arXiv:math/0005026v1 [math.GM] 3 May 2000

ON THE COMPLETE SOLUTION TO THE MOST GENERAL FIFTH DEGREE POLYNOMIAL

Richard J. Drociuk

Physics Department

Simon Fraser University

Burnaby British Columbia, Canada.

April 10, 2000.

Dedicated to Erland Samuel Bring
The first great pioneer into the solution to the equation to the fifth degree.

ABSTRACT

The motivation behind this note, is due to the non success in finding the complete solution to the General Quintic Equation. The hope was to have a solution with all the parameters precisely calculated in a straight forward manner. This paper gives the closed form solution for the five roots of the General Quintic Equation. They can be generated on Maple V, or on the new version Maple VI. On the new version of maple, Maple VI, it may be possible to insert all the substitutions calculated in this paper, into one another, and construct one large equation for the Tschirnhausian Transformation. The solution also uses the Generalized Hypergeometric Function which Maple V can calculate, robustly.

INTRODUCTION

It has been known since about 2000 BC, that the Mesopotamians have been able to solve the Quadratic Equation with the Quadratic Formula[Young, 1]. It took until 1545 AD, for Cardano to publish his solution for the Cubic Equation, in his " Artis magnae sive de regulis algebraicis". But it was actually Tartaglia who did the original work to solve the cubic. Cardano's roommate, Ferrari (in Cardano's Ars magna), solved the Quartic Equation at about the same time Cardano solved the Cubic Equation. Tartaglia fought ferociously against Cardano, Ferrari, and Sciopone Ferro, for stealing his solution of the Cubic Equation. This situation was filled with perjury, disputation, and bitterness. Finally, Cardano was thrown into prison by the inquisition for heresy, for making the horoscope of Christ[Guerlac, 2].

Erland Samuel Bring (1786), was the first person to perform a Tschirnhausian Transformation to a quintic equation, successfully. He transformed a quintic with the fourth and third order terms missing, i.e. x^5+px^2+qx+r=0, to the Bring Form x^5-x-s=0 [Bring, 3]. This work was disputed by the University of Lund, and was lost in the university's archives. I do not know if an original

arXiv:nlin/0011038v2 [nlin.CD] 11 Sep 2001

Classical and Quantum Hamiltonian Ratchets

Holger Schanz,[1] Marc-Felix Otto,[1] Roland Ketzmerick,[1] and Thomas Dittrich[2]
[1] *Max-Planck-Institut für Strömungsforschung and Institut für Nichtlineare Dynamik der Universität Göttingen, Bunsenstraße 10, 37073 Göttingen, Germany*
[2] *Departamento de Física, Universidad Nacional, Santafé de Bogotá, Colombia*
(June 10, 2001)

We explain the mechanism leading to directed chaotic transport in Hamiltonian systems with spatial and temporal periodicity. We show that a mixed phase space comprising both regular and chaotic motion is required and derive a classical sum rule which allows to predict the chaotic transport velocity from properties of regular phase-space components. Transport in quantum Hamiltonian ratchets arises by the same mechanism as long as uncertainty allows to resolve the classical phase-space structure. We derive a quantum sum rule analogous to the classical one, based on the relation between quantum transport and band structure.

Stimulated by the biological task of explaining the functioning of molecular motors, the study of ratchets [1] has widened to a general exploration of "self-organized" transport, i.e., transport without external bias, in nonlinear systems [2]. Along with this process, there has been a tendency to reduce the models under investigation from realistic biophysical machinery to the minimalist systems customary in nonlinear dynamics. External noise, for example, which originally served to account for the fluctuating environment of molecular motors, has been replaced by deterministic chaos. This required to include inertia terms in the equations of motion, thus leaving the regime of overdamped dynamics and leading to deterministic inertia ratchets with dissipation [3,4]. It is then a consequent but radical step to abandon friction altogether. Indeed, transport in *Hamiltonian ratchets* was observed numerically if all symmetries were broken that generate to each trajectory a countermoving partner [5,6].

As a parallel development, the desire to realize ratchets in artificial, nanostructured electronic systems, required to consider quantum effects [7,6]. *Quantum Hamiltonian ratchets*, however, have been studied only in the framework of one-band systems where no transport occurs [6].

In this paper we explain how a Hamiltonian ratchet works. We rely on methods which—although well established in studies of deterministic dynamics—have never before been applied to ratchets. We derive a classical and an analogous quantum sum rule for transport allowing the following conclusions: (i) Directed transport is a property associated with individual invariant sets of the dynamics. A necessary condition for non-zero transport is a mixed phase space with coexisting regular and chaotic regions. (ii) Transport in *chaotic* regions can be described quantitatively by using topological and further properties of adjacent *regular* regions only. (iii) Quantum transport persists for all times and approaches the classical transport when $\hbar$ is small compared to the major invariant sets of the classical phase space.

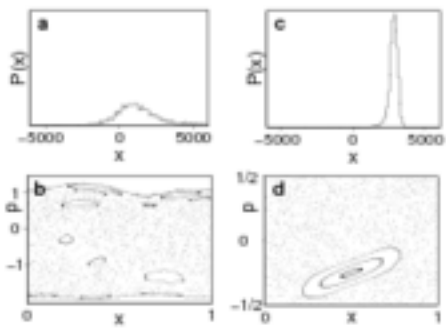


FIG. 1. (a) Spatial distribution $P(x)$ of a continuously driven system [8] after 20,000 time periods showing the directed transport in a Hamiltonian ratchet. Initially, 10^4 trajectories were started at random on the line $p = 0$, $x \in [0, 1)$ in the chaotic sea. (b) Poincaré section p vs x of a unit cell at integer times showing the main chaotic sea, the upper and lower limiting KAM-tori, and the major embedded regular islands. (c,d) As (a,b), but for the kicked Hamiltonian (4) showing a much more pronounced directed transport.

We consider a Hamiltonian of the form $H(x, p, t) = T(p) + V(x, t)$, where $T(p)$ is the kinetic energy. The force $-V'$ is periodic in space and time, $V'(x+1, t) = V'(x, t+1) = V'(x, t)$, and has zero mean $\int_0^1 dt \int_0^1 dx\, V'(x, t) = 0$. Usually directed transport is demonstrated by following selected trajectories over very long times [5,6] or an ensemble of trajectories which generates spatial distributions as shown in Fig. 1a,c. While this is easily implemented numerically, it gives no clue about the origin of the transport (but see Ref. [9]). Instead, we shall exploit the periodicity of the dynamics with respect to space and time and analyze transport in terms of the invariant sets of phase space, *reduced to the spatio-temporal unit cell* $x, t \in [0, 1)$. For any finite invariant set M we define ballistic transport as phase-space volume times average

arXiv:math/0011193v1 [math.QA] 23 Nov 2000

NONCOMMUTATIVE GEOMETRY YEAR 2000

Alain CONNES,[1]

[1] Collège de France, 3, rue Ulm, 75005 PARIS
and
I.H.E.S., 35, route de Chartres, 91440 BURES-sur-YVETTE

Abstract

Our geometric concepts evolved first through the discovery of NonEuclidean geometry. The discovery of quantum mechanics in the form of the noncommuting coordinates on the phase space of atomic systems entails an equally drastic evolution. We describe a basic construction which extends the familiar duality between ordinary spaces and commutative algebras to a duality between Quotient spaces and Noncommutative algebras. The basic tools of the theory, K-theory, Cyclic cohomology, Morita equivalence, Operator theoretic index theorems, Hopf algebra symmetry are reviewed. They cover the global aspects of noncommutative spaces, such as the transformation $\theta \to 1/\theta$ for the noncommutative torus $\mathbf{T}^2_\theta$ which are unseen in perturbative expansions in θ such as star or Moyal products. We discuss the foundational problem of "what is a manifold in NCG" and explain the fundamental role of Poincare duality in K-homology which is the basic reason for the spectral point of view. This leads us, when specializing to 4-geometries to a universal algebra called the "Instanton algebra". We describe our joint work with G. Landi which gives noncommutative spheres S^4_θ from representations of the Instanton algebra. We show that any compact Riemannian spin manifold whose isometry group has rank $r \geq 2$ admits isospectral deformations to noncommutative geometries. We give a survey of several recent developments. First our joint work with H. Moscovici on the transverse geometry of foliations which yields a diffeomorphism invariant (rather than the usual covariant one) geometry on the bundle of metrics on a manifold and a natural extension of cyclic cohomology to Hopf algebras. Second, our joint work with D. Kreimer on renormalization and the Riemann-Hilbert problem. Finally we describe the spectral realization of zeros of zeta and L-functions from the noncommutative space of Adele classes on a global field and its relation with the Arthur-Selberg trace formula in the Langlands program. We end with a tentalizing connection between the renormalization group and the missing Galois theory at Archimedian places.

Escape in Hill's Problem

Douglas C Heggie

University of Edinburgh, UK

arXiv:astro-ph/0011294v1 15 Nov 2000

1 Introduction and Motivation

In the 19th century the American mathematician G.W. Hill devised a simple and useful approximation for the motion of the moon around the earth with perturbations by the sun. To most dynamical astronomers "Hill's Problem" still means a model for motions in the solar system in which two nearby bodies move in nearly circular orbits about another much larger body at a great distance. These lectures have, however, been motivated by a problem in stellar dynamics.

Consider a star in a star cluster which is itself in orbit about a galaxy (Figure 2). The star, cluster and galaxy take the place of the moon, earth and sun, respectively. The potentials of the cluster and galaxy are not those of a point mass, and the galactic orbits of the star and cluster may be far from circular. Nevertheless Hill's problem is a good starting point, and it can be modified easily to accommodate the differences. In section 2 we outline a derivation of Hill's equations, and in section 3 we summarise the appropriate extensions.

Stars gradually escape from star clusters. This has been expected on theoretical grounds for many years, ever since a paper by Ambartsumian (1938). Recently, deep observations have confirmed this (e.g. Leon et al 2000), by revealing faint streams of stars around a number of the globular clusters of our Galaxy.

Loosely speaking we can say that a star can only escape if its energy exceeds some critical energy. The energies of stars change slightly as a result of two-body gravitational encounters within clusters, though the time scale on which this happens (the *relaxation time scale*) is very long, of order 10^9yr. But the orbital motions of stars within clusters have much smaller time scales of order 10^6yr, and until recently it was thought that escaping stars would leave on a similar time scale. With this assumption, relaxation is the bottleneck, and so the escape time scale (e.g. the time taken for half the stars to escape) should vary with the relaxation time.

Nowadays it is possible to simulate the evolution of modest-sized star clusters with 3×10^4 or more members, and the predicted escape time scale can be checked empirically. Unfortunately the results contradict the theory (Figure 1). As these simulations require

Beyond Turing: Hypercomputation and Quantum Morphogenesis

Ignazio Licata

1. "Purely Mechanical"

One of the most innovative areas in contemporary research is the study of the deep conceptual connection between physics, information and the "counting" of information, i.e. a search for a computation model for physical systems. Any physical system can be considered as an information processor in dialogue with the external environment. The initial values are transformed into the final ones by the system's internal dynamics. The Church–Turing Thesis (CTT), in its strong form, states that any processing of syntactic information can be described by means of a suitable Turing Machine (TM).

The analogy between a quantum of action and a bit seems very natural (minimum action necessary to cause an observable change in a physical system), and so the CTT, as it is maintained — quite imprecisely — is considered a "statement on the physical world".

Here we ask the question: Is this statement really valid? Is the CT thesis so naturally and obviously applicable to physics?

In recent years the critical debate on the limit of application of recursive functions in physics has grown and, in this direction, the two most important research areas are hypercomputation and quantum information theory.

Some classical works have strengthened the idea that the behaviour of a mechanical discrete system evolving according to local laws is recursive. Such works have shown the relations between the classical computation theory and the physical deterministic systems. In particular, it can be noted a strong analogy between a TM's asymptotic unpredictable behaviours and deterministic chaos; in both cases the local rules do not imply a long-term predictable behaviour, indeed [28, 10, 27, 15]. Different strategies have been proposed to apply such computational scheme to the continuous language of differential equations [22].

The general reasons taken into consideration to justify the use of TM in physics can be summarised as follows:

(a) A fundamental discretisation of the physical world (for example Beckenstein limit: a system cannot handle more information than that it contains);

(b) Relativity: the whole tape is not available in its whole at each computational instant,

and, finally:

(c) The infinity of the tape lets us suppose that there are no limitations to the possible implementations of the Kleene Theorem (for example: asynchronous and parallel computation, cellular automata and so on).

We note, in particular, that the first point refers to a generic discrete structure of the world, but contains no specific information on the proper dynamics of quantum processes, and point (b) is connected to a locality principle. Finally, point (c) stresses the universality of the Turing scheme, with respect to other kinds of computation formally equivalent to the first one, but with a different attitude towards the space-time patterns [40].

In general, the question, if any physical model is Turing computable, collides with a large number of counter examples. These are rather sophisticated questions related to exotic limit-cases of classical, relativistic and gravitational physics (see, for example, [16]), but strong enough to suggest to us that perhaps it would be useful to substitute CT Thesis with a computational paradigm for each specific class of physical problems with the suitable modifications to the (a), (b) and (c) conditions: for example the Friedkin–Totfoli billiard-machine class for mechanical processes, or the class of space time topologies for relativistic computers, or the class of differential equations showing "pathological" boundary conditions with respect to computability.

So the TM remains a notion which was born within a classical and mechanistic conception of the physical world and the Hilbertian axiomatic. As Alan Turing himself writes: "TMs can do anything that could be described as a 'rule of thumb' or 'purely mechanical', so that 'calculable by means of a TM' is the correct

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/228883978

Feynman integrals, diffusion processes and quantum symplectic two-forms

Article in Journal of the Korean Mathematical Society · January 2001

CITATIONS
6

READS
28

1 author:

Jean Claude Zambrini
University of Lisbon
35 PUBLICATIONS 330 CITATIONS

SEE PROFILE

All content following this page was uploaded by Jean Claude Zambrini on 28 May 2014.

The user has requested enhancement of the downloaded file.

ResearchGate

See discussions, stats, and author profiles for this publication at:
https://www.researchgate.net/publication/38330256

Resonances in chaotic dynamics

Article *in* Communications in Mathematical Physics · June 1988

DOI: 10.1007/BF01212260 · Source: OAI

CITATIONS
33

READS
30

1 author:

Stefano Isola
University of Camerino
77 PUBLICATIONS **778** CITATIONS

SEE PROFILE

All content following this page was uploaded by Stefano Isola on 12 February 2014.

The user has requested enhancement of the downloaded file.

Progress In Electromagnetics Research, PIER 32, 1–44, 2001

FINITE FORMULATION OF THE ELECTROMAGNETIC FIELD

E. Tonti

Università di Trieste, 34127 Trieste, Italy

Abstract—The objective of this paper is to present an approach to electromagnetic field simulation based on the systematic use of the global (i.e. integral) quantities. In this approach, the equations of electromagnetism are obtained directly in a finite form starting from experimental laws without resorting to the differential formulation. This finite formulation is the natural extension of the network theory to electromagnetic field and it is suitable for computational electromagnetics.

1 Introduction

2 Finite Formulation: the Premises
- 2.1 Configuration, Source and Energy Variables
- 2.2 Global Variables and Field Variables

3 Physical Variables and Geometry
- 3.1 Inner and Outer Orientation
- 3.2 Time Elements
- 3.3 Global Variables and Space-time Elements
- 3.4 Operational Definition of Six Global Variables
- 3.5 Physical Laws and Space-time Elements
- 3.6 The Field Laws in Finite Form

4 Cell Complexes in Space and Time
- 4.1 Classification Diagram of Space-time Elements
- 4.2 Incidence Numbers
- 4.3 Constitutive Laws in Finite Form
- 4.4 Computational Procedure
- 4.5 Classification Diagrams of Physical Variables

THE DEMOCRATIC NATIONAL COMMITTEE

WEEKLY UPDATE

BROUGHT TO YOU BY THE DNC COMMUNICATIONS DEPARTMENT

January 6, 2012

This week, the President addressed enthusiastic Democratic caucus-goers across the state during Iowa's caucuses on Tuesday night. He was also in Ohio to speak about the economy, where he announced his appointment of former Ohio Attorney General Richard Cordray as head of the Consumer Financial Protection Bureau – noting that America's working families can no longer wait for Republicans in the Senate who have stood in the way of consumer protection by holding up Cordrey's nomination. On Thursday, President Obama delivered remarks at the Pentagon on the Defense Strategic Review, which followed a comprehensive review of our defense strategy and budget priorities by the President, America's civilian and uniformed military leadership, and the Administration's national security team. On Friday, the Bureau of Labor Statistics released its monthly jobs numbers, saying that the economy added 212,000 private sector jobs in December and that the unemployment rate fell to 8.5 percent.

And with the Republican candidates for president competing for the nomination in Iowa, New Hampshire, South Carolina and beyond, the Democratic National Committee and local, state and national Democratic leaders across the country worked to hold Mitt Romney and the rest of the GOP field accountable for their failed policies and lack of vision – including Romney's recent out-of-touch statement that he would veto the DREAM Act if he were president and Congress had passed the bill.

Economy Adds Private Sector Jobs in December

On Friday, the Bureau of Labor Statistics released jobs numbers for December, showing that the private sector added 212,000 private sector jobs in December and that the unemployment rate fell to 8.5 percent. This is now the 22nd consecutive month of private sector job growth and a sign that the economy is headed in the right direction, though the President believes we need faster economic growth.

Democrats Show Enthusiastic Turnout as the President Addresses Participants on Iowa Caucus Night

As Iowa voters headed to the caucuses on Tuesday night, President Obama spoke via video teleconference to Democratic caucus-goers across the state, letting them know that he will keep fighting for Iowa's working families and all Americans. The results showed enthusiastic support for the President's re-election, with 25,000 Iowans turning out for the Democratic caucuses and 7,500 pledging to volunteer and work for the campaign. During the President's address to caucus-goers, he said:

> "Although we've passed health care reform, we've passed Wall Street reform, there are a lot of forces that want to push back against us and want to undo some of those changes. And we're battling millions of dollars of negative advertising and lobbyists and special interests who don't want to see the change that you worked so hard to fully take root. And that's why this time out is going to be in some ways more important than the first time out. Mitch is right. Change is never easy. The

Paid for and authorized by the Democratic National Committee, www.democrats.org. This communication is not authorized by any candidate or candidate's committee.

arXiv:hep-th/0110067v2 13 Jan 2006

Heterotic, Open and Unoriented String Theories from Topological Membrane

Pedro Castelo Caetano Ferreira

Department of Physics
Keble College
University of Oxford

Thesis submitted for the degree of Doctor of Philosophy

in the University of Oxford

Supervisor: Ian I. Kogan

5th October 2001, Michaelmas term

Complex Systems **1** (1987) 923–938

Quantum Fractals

Siamak Amir-Azizi
Anthony J. G. Hey
Timothy R. Morris
Department of Electronics and Computer Science,
University of Southampton, Southampton SO9 5NH, England

Abstract. The fractal nature of quantum paths contributing to Feynman path integral formulation of quantum mechanics is investigated. A computer simulation of both one- and two-dimensional quantum harmonic oscillators yields results in agreement with rigorous results on the Hausdorff-Besicovitch dimension for Brownian motion.

1. Introduction

It is well known that classical mechanics can be reformulated in terms of a minimum principle. The Euler-Lagrange equations of motion follow from demanding that the action

$$S[x(t)] = \int_{t_i}^{t_f} L(x, \dot{x}) dt$$

be stationary with respect to variations in the path $x(t)$ taken between $x(t_i) = x_i$ and $x(t_f) = x_f$. An alternative formulation of quantum mechanics, due to Feynman [1], is in terms of a kernel, $F(x_f, t_f; x_i, t_i)$, defined by

$$\Psi(x_f, t_f) = \int dx_i F(x_f, t_f; x_i, t_i)\, \Psi(x_i, t_i)$$

The kernel is expressed as a "path integral": the path integral sums over all possible trajectories $x(t)$ from $x(t_i) = x_i$ to $x(t_f) = x_f$ with an amplitude which depends on the classical action for that path. Formally, this is written as

$$F(x_f, t_f; x_i, t_i) = (\text{const}) \int_{x(t_i)=x_i}^{x(t_f)=x_f} \mathcal{D}x(t) \exp[\frac{i}{\hbar} S[x(t)]]$$

where the symbol $\mathcal{D}x(t)$ is Feynman's famous "sum over all paths", and the overall constant does not concern us here. The sum over all paths may be defined more precisely by introducing a time lattice and dividing up the time interval, $t_f - t_i$, into equal time slices, ε apart, and integrating over all x_n at each time slice t_n.

© 1987 Complex Systems Publications, Inc.

SMARTPOOL: Practical Decentralized Pooled Mining

Loi Luu
National University of Singapore
loiluu@comp.nus.edu.sg

Yaron Velner
The Hebrew University of Jerusalem
yaron.velner@mail.huji.ac.il

Jason Teutsch
TrueBit Foundation
jt@truebit.io

Prateek Saxena
National University of Singapore
prateeks@comp.nus.edu.sg

Abstract

Cryptocurrencies such as Bitcoin and Ethereum are operated by a handful of mining pools. Nearly 95% of Bitcoin's and 80% of Ethereum's mining power resides with less than ten and six mining pools respectively. Although miners benefit from low payout variance in pooled mining, centralized mining pools require members to trust that pool operators will remunerate them fairly. Furthermore, centralized pools pose the risk of transaction censorship from pool operators, and open up possibilities for collusion between pools for perpetrating severe attacks.

In this work, we propose SMARTPOOL, a novel protocol design for a decentralized mining pool. Our protocol shows how one can leverage *smart contracts*, autonomous blockchain programs, to decentralize cryptocurrency mining. SMARTPOOL gives transaction selection control back to miners while yielding low-variance payouts. SMARTPOOL incurs mining fees lower than centralized mining pools and is designed to scale to a large number of miners. We implemented and deployed a robust SMARTPOOL implementation on the Ethereum and Ethereum Classic networks. To date, our deployed pools have handled a peak hashrate of 30 GHs from Ethereum miners, resulting in 105 blocks, costing miners a mere 0.6% of block rewards in transaction fees.

1 Introduction

Cryptocurrencies such as Bitcoin and Ethereum offer the promise of a digital currency that lacks a centralized issuer or a trusted operator. These cryptocurrency networks maintain a distributed ledger of all transactions, agreed upon by a large number of computation nodes (or *miners*). The most widely used protocol for agreement is Nakamoto consensus, which rewards one miner every epoch (lasting, say, 10 minutes as in Bitcoin) who exhibits a solution to a probabilistic computation puzzle called a "proof-of-work" (or PoW) puzzle [1]. The winning miner's solution includes a transaction *block*, which is appended to the distributed ledger that all miners maintain. The reward is substantial (e.g. 12.5 BTC in Bitcoin, or 30,000 USD at present), incentivizing participation.

Nakamoto-based cryptocurrencies, such as Bitcoin and Ethereum, utilize massive computational resources for their mining. Finding a valid solution to a PoW puzzle is a probabilistic process, which follows a Poisson distribution, with a miner's probability of finding a solution within an epoch determined by the fraction of computation power it possesses in the network. Miners with modest computational power can have extremely high variance. A desktop CPU would mine 1 Bitcoin block in over a thousand years, for instance [2]. To reduce variance, miners join *mining pools* to mine blocks and share rewards together. In a mining pool, a designated pool *operator* is responsible for distributing computation sub-puzzles of lower difficulty than the full PoW block puzzle to its members. Each solution to a sub-puzzle has a probability of yielding a solution to the full PoW block puzzle—so if enough miners solve them, some of these solutions are likely to yield blocks. When a miner's submitted solution yields a valid block, the pool operator submits it to the network and obtains the block reward. The reward is expected to be fairly divided among all pool members proportional to their contributed solutions.

Problem. Centralized pool operators direct the massive computational power of their pools' participants. At the time of this writing, Bitcoin derives at least 95% of its mining power from only 10 mining pools; the Ethereum network similarly has 80% of its mining power emanating from 6 pools. Previous works have raised concerns about consolidation of power on Bitcoin [3,4]. Recent work by Apostolaki *et al.* has demonstrated large-scale network attacks on cryptocurrencies, such as double spending and network partitioning, which exploit centralized mining status quo [5]. By design, if a single pool operator controls more than half of the network's total mining power, then a classical 51% attack threat-

Physics 6010, Fall 2010

Introduction. Configuration space. Equations of Motion. Velocity Phase Space.

Relevant Sections in Text: §1.1–1.3

Introduction

This course principally deals with the variational principles of mechanics, particularly the Lagrangian and Hamiltonian descriptions of dynamical systems. So, this won't be a course in which we spend a lot of time doing things like solving for the motion of a triple pendulum coupled by springs while sliding on an inclined plane with friction in a viscous fluid as viewed in a rotating reference frame. To be sure, we will analyze the motion of some important dynamical systems. But the emphasis will be more on formalism – the Lagrangian and Hamiltonian approaches, in particular – and less on solving equations. There are many reasons for this; here are a few.

First of all, when analyzing a dynamical system the first task is to figure out what is the correct mathematical description, what are the equations of motion, etc. The Lagrangian and Hamiltonian formalisms are the most powerful ways to do this. Next, as I shall repeatedly emphasize, most interesting dynamical systems are simply too complex in their behavior for one to find closed-form, analytical expressions for their motion. In other words, the solutions to the equations of motion exist, but you will never be able to write them down in practice. How then to extract physical information about the system? There are a variety of sophisticated methods for getting at aspects of the physical behavior. Many of these methods stem from the powerful vantage point provided by the Lagrangian and/or Hamiltonian formulations of mechanics. Finally, one can view "classical mechanics" as an approximation to the more fundamental "quantum mechanics", this approximation being valid, *e.g.*, for macroscopic systems. A key link between these two descriptions of dynamics is made via the Lagrangian and Hamiltonian formalisms. Indeed, a lot of the structural features of quantum mechanics have clear classical analogs, and these are uncovered via the Lagrangian and Hamiltonian formulations. One might say the Lagrangian and Hamiltonian forms of mechanics are a classical imprint of the quantum world. So, by learning these techniques you are better prepared to study quantum mechanics and you are acquiring tools which can handle all kinds of dynamics – classical and/or quantum.

In mechanics we have four principal tasks: (1) determine the *configuration space* or the *phase space* for the system of interest; (2) find the underlying *dynamical law* – the equations of motion – governing the motion of a system; (3) use the dynamical law to find the allowed motions of a system; (4) out of all allowed motions find those which describe the physical situations of interest. Let us now briefly discuss each of these tasks.

arXiv:quant-ph/0202026v1 5 Feb 2002

Nonlinear QM as a fractal Brownian motion with complex diffusion constant

Carlos Castro[1], Jorge Mahecha[2] and Boris Rodríguez[2]

[1] *Center for Theoretical Studies of Physical Systems, Clark Atlanta University, Atlanta, Georgia, USA*

[2] *Institute of Physics, University of Antioquia, Medellín, Colombia*

February 1, 2008

Abstract

A new nonlinear Schrödinger equation is obtained explicitly from the fractal Brownian motion of a massive particle with a complex-valued diffusion constant. Real-valued energy (momentum) plane wave and soliton solutions are found in the free particle case. The hydro-dynamical model analog yields another (new) nonlinear QM wave equation with physically meaningful soliton solutions. One remarkable feature of this nonlinear Schrödinger equation based on a fractal Brownian motion model, over all the other nonlinear QM models, is that the quantum-mechanical energy functional coincides with the field theory one.

1 Introduction

The theoretical study of quantum chaos has been developed mainly in two areas: The phenomenological characterization of the spacing of the energy levels of bound and quasi-bound quantum physical systems, whose main analytical tool is the random matrix theory [6], and the semi-classical limit of chaotic classical systems [7]. The semi-classical approach pretends to seek solutions of the Schrödinger equation and to read in the wave functions any fingerprints of classical chaos. Due to the linearity of the Schrödinger equation there is no place where the sensibility to the initial conditions can be made manifest, which is present in nonlinear chaotic systems. The Riemann zeta function has been considered as a unifying link between those two approaches [8].

We believe that quantum chaos is truly a new paradigm in physics associated with non-unitary and nonlinear QM processes based on non-Hermitian operators (implementing time symmetry breaking). This chaotic behavior stems directly from the nonlinear Schrödinger equation without any reference to the nonlinear behavior of the classical limit. See [9]. For this reason, the genuine quantum chaos should be exhibited only by systems whose behavior is correctly described by a nonlinear Schrödinger equation.

The nonlinear QM has a practical importance in different fields, like condensed matter, quantum optics and atomic and molecular physics; even quantum gravity may involve nonlinear QM. Another important example is in the modern field of quantum computing. If quantum states exhibit small nonlinearities during their temporal evolution, then quantum computers can be used to solve NP-complete (non polynomial) and #P problems in polynomial time.

arXiv:math/0206229v2 [math.DG] 13 Dec 2002

EINSTEIN METRICS AND COMPLEX SINGULARITIES

DAVID M. J. CALDERBANK AND MICHAEL A. SINGER

ABSTRACT. This paper is concerned with the construction of special metrics on non-compact 4-manifolds which arise as resolutions of complex orbifold singularities. Our study is close in spirit to the construction of the hyperkähler gravitational instantons, but we focus on a different class of singularities. We show that any resolution X of an isolated cyclic quotient singularity admits a complete scalar-flat Kähler metric (which is hyperkähler if and only if $c_1(X) = 0$), and that if $c_1(X) < 0$ then X also admits a complete (non-Kähler) self-dual Einstein metric of negative scalar curvature. In particular, complete self-dual Einstein metrics are constructed on simply-connected non-compact 4-manifolds with arbitrary second Betti number.

Deformations of these self-dual Einstein metrics are also constructed: they come in families parameterized, roughly speaking, by free functions of one real variable.

All the metrics constructed here are *toric* (that is, the isometry group contains a 2-torus) and are essentially explicit. The key to the construction is the remarkable fact that toric self-dual Einstein metrics are given quite generally in terms of *linear* partial differential equations on the hyperbolic plane.

1. INTRODUCTION AND MAIN THEOREMS

If Γ is a finite subgroup of $SU(2)$, then the complex orbifold $\mathbb{C}^2/\Gamma$ has a canonical resolution X with $c_1(X) = 0$. This non-compact complex surface carries a family of asymptotically locally euclidean (ALE) hyperkähler metrics, the so-called gravitational instantons of Gibbons, Hawking, Hitchin and Kronheimer [10, 12, 18]. In this paper, we extend this picture by looking for 'optimal' metrics on complex resolutions of other surface singularities. Our methods apply to finite cyclic subgroups $\Gamma \subset U(2)$ with the property that $\mathbb{C}^2/\Gamma$ has an isolated singular point, the image of the origin in $\mathbb{C}^2$. These varieties are *toric*: there is a $\mathbb{C}^\times \times \mathbb{C}^\times$ subgroup of $\mathrm{GL}_2(\mathbb{C})$ commuting with Γ, which acts on $\mathbb{C}^2/\Gamma$ and the resolution X. If $\Gamma \not\subset SU(2)$ then $c_1(X) \neq 0$ and so X cannot carry a hyperkähler metric. However we shall find ALE Kähler metrics with zero scalar curvature, and if $c_1(X)$ is negative definite, complete asymptotically (locally) hyperbolic self-dual Einstein metrics (with respect to the opposite orientation of X).

The situation is simplest if Γ acts by scalar multiples of the identity on $\mathbb{C}^2$. Then if $|\Gamma| = p$, X is the total space of the complex line bundle $\mathcal{O}(-p) \to \mathbb{C}P^1$ and for each p (including $p = 1$, the blow up of $\mathbb{C}^2$) there is a $U(2)$-invariant ALE scalar-flat Kähler (SFK) metric on X: this is due to Burns if $p = 1$, to Eguchi–Hanson if $p = 2$, and to LeBrun for $p > 2$ (see [20]). Note that among these metrics, only Eguchi–Hanson is hyperkähler, corresponding to $\Gamma = \{\pm 1\} \subset SU(2)$. However, the Burns metric is conformal to the Fubini–Study metric on the punctured projective plane $\mathbb{C}P^2 \setminus \{\infty\}$, which is a self-dual Einstein (SDE) metric of positive scalar curvature, whereas the LeBrun metrics are (in suitable domains) conformal to Fodersen metrics [25], which are AH self-dual Einstein metrics of negative scalar curvature (see [13, 7]).

Our main results show that a similar picture continues to hold for more general cyclic subgroups of $U(2)$. We begin with the SFK metrics.

Date: February 2008.

arXiv:math/0207258v1 [math.GM] 27 Jul 2002

On the Root Ambiguity in the Complete Solution to the Most General Fifth Degree Polynomial

Richard Drociuk

November 9, 2013

1 Abstract

Starting from the solution to Bring's equation the root ambiguity is removed from the solution to the quintic equation. This gives the five complex roots of the quintic equation as indicated by Gauss's Fundamental Theorem of Algebra.

2 Introduction

In the previous paper[Drociuk,1], the solution to the quintic was given, but the root ambiguity was not correctly removed. This problem arises because Ferrari's method for solving the quartic equation does not introduce all possible roots. Instead if one uses a Tshirnhausen transformation as demonstrated[Drociuk,1], to the quartic equation, the five correct roots of the quintic equation,

$$x^5 + mx^4 + nx^3 + px^2 + qx + r = 0 \tag{1}$$

are selcted for arbitrary coefficients m, n, p, q, and r. The roots are selected from all possible roots using conditional loops to an arbitrary precission, ϵ.

3 Ambiguity in the Quartic Solution

The quartic equation,

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \tag{2}$$

is transformed with,

$$Tsh2 = x^3 + b_2x^2 + b_1x + b_0 + y_n \tag{3}$$

to the quadratic in y_n^2,

$$y_n^4 + B_2y_n^2 + B_0 = 0 \tag{4}$$

whose four roots are,

$$y_1 = \frac{1}{2}(-2B_2 + 2(B_2^2 - 4B_0)^{\frac{1}{2}})^{\frac{1}{2}} \tag{5}$$

7.8 SURFACE EQUIVALENCE THEOREM: HUYGENS'S PRINCIPLE

The *surface equivalence* theorem is a principle by which actual sources, such as an antenna and transmitter, are replaced by equivalent sources. The fictitious sources are said to be equivalent within a region because they produce within that region the same fields as the actual sources. The formulations of scattering and diffraction problems by the surface equivalence theorem are more suggestive of approximations.

The surface equivalence was introduced in 1936 by Schelkunoff [11], and it is a more rigorous formulation of Huygens's principle [12], which states [13] that "each point on a primary wavefront can be considered to be a new source of a secondary spherical wave and that a secondary wavefront can be constructed as the envelope of these secondary spherical waves." The surface equivalence theorem is based on the uniqueness theorem of Section 7.3, which states [1] that "a field in a lossy region is uniquely specified by the sources within the region plus the tangential components of the electric field over the boundary, or the tangential components of the magnetic field over the boundary, or the former over part of the boundary and the latter over the rest of the boundary." The fields in a lossless medium are considered to be the limit, as the losses go to zero, of the corresponding fields in a lossy medium. Thus if the tangential electric and magnetic fields are completely known over a closed surface, the fields in the source-free region can be determined.

By the surface equivalence theorem, the fields outside an imaginary closed surface are obtained by placing, over the closed surface, suitable electric and magnetic current densities that satisfy the boundary conditions. The current densities are selected so that the fields inside the closed surface are zero and outside are equal to the radiation produced by the actual sources. Thus the technique can be used to obtain the fields radiated outside a closed surface by sources enclosed within it. The formulation is exact but requires integration over the closed surface. The degree of accuracy depends on the knowledge of the tangential components of the fields over the closed surface.

In the majority of applications, the closed surface is selected so that most of it coincides with the conducting parts of the physical structure. This is preferred because the tangential electric field components vanish over the conducting parts of the surface, which results in reduction of the physical limits of integration.

The surface equivalence theorem is developed by considering an actual radiating source, which is represented electrically by current densities $\mathbf{J}_1$ and $\mathbf{M}_1$, as shown in Figure 7-7*a*. The source radiates fields $\mathbf{E}_1$ and $\mathbf{H}_1$ everywhere. However, we wish to develop a method that will yield the fields outside a closed surface. To accomplish this, a closed surface S is chosen, shown dashed in Figure 7-7*a*, which encloses the current densities $\mathbf{J}_1$ and $\mathbf{M}_1$. The volume within S is denoted by V_1 and outside S by V_2. The primary task is to replace the original problem, shown in Figure 7-7*a*, with an equivalent that will yield the same fields $\mathbf{E}_1$ and $\mathbf{H}_1$ outside S (within V_2). The formulation of the problem can be aided immensely if the closed surface is chosen judiciously so that fields over most, if not the entire surface, are known a priori.

An equivalent problem to Figure 7-7*a* is shown in Figure 7-7*b*. The original sources $\mathbf{J}_1$ and $\mathbf{M}_1$ are removed, and we assume that there exist fields $\mathbf{E}, \mathbf{H}$ inside S and fields $\mathbf{E}_1, \mathbf{H}_1$ outside S. For these fields to exist within and outside S, they must satisfy the boundary conditions on the tangential electric and magnetic field components of Table 1-5. Thus on the imaginary surface S there must exist the

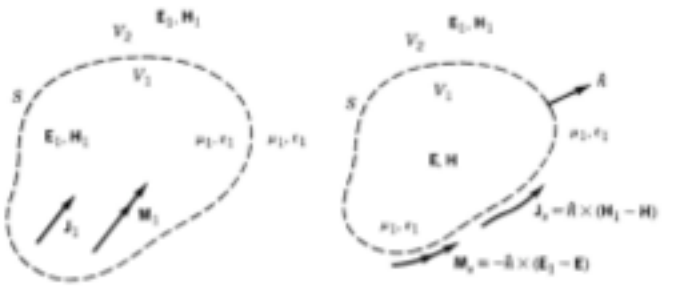


FIGURE 7-7 (*a*) Actual and (*b*) equivalent problem models (*Source:* C. A. Balanis, *Antenna Theory: Analysis and Design*. Copyright © 1982, John Wiley & Sons, Inc. Reprinted with permission of John Wiley & Sons, Inc.)

equivalent sources

$$\mathbf{J}_s = \hat{n} \times (\mathbf{H}_1 - \mathbf{H}) \tag{7-42a}$$

$$\mathbf{M}_s = -\hat{n} \times (\mathbf{E}_1 - \mathbf{E}) \tag{7-42b}$$

which radiate into an unbounded space (same medium everywhere). The current densities of (7-42a) and (7-42b) are said to be equivalent only within V_2, because they will produce the original field $(\mathbf{E}_1, \mathbf{H}_1)$ only outside S. A field $\mathbf{E}, \mathbf{H}$, different from the original $(\mathbf{E}_1, \mathbf{H}_1)$ will result within V_1. Since the currents of (7-42a) and (7-42b) radiate in an unbounded space, the fields can be determined using (6-30) through (6-35a) and the geometry of Figure 6-3*a*. In Figure 6-3*a*, R is the distance from any point on the surface S, where $\mathbf{J}_s$ and $\mathbf{M}_s$ exist, to the observation point.

So far, the tangential components of both $\mathbf{E}$ and $\mathbf{H}$ have been used to set up the equivalent problem. From electromagnetic uniqueness concepts, we know that the tangential components of only $\mathbf{E}$ or $\mathbf{H}$ are needed to determine the field. It will be demonstrated that equivalent problems that require only magnetic currents (tangential $\mathbf{E}$) or only electric currents (tangential $\mathbf{H}$) can be found. This will require modifications to the equivalent problem of Figure 7-7*b*.

Since the fields $\mathbf{E}, \mathbf{H}$ within S, which is not the region of interest, can be anything, it can be assumed that they are zero. Then the equivalent problem of Figure 7-7*b* reduces to that of Figure 7-8*a* with equivalent current densities equal to

$$\mathbf{J}_s = \hat{n} \times (\mathbf{H}_1 - \mathbf{H})\big|_{\mathbf{H}=0} = \hat{n} \times \mathbf{H}_1 \tag{7-43a}$$

$$\mathbf{M}_s = -\hat{n} \times (\mathbf{E}_1 - \mathbf{E})\big|_{\mathbf{E}=0} = -\hat{n} \times \mathbf{E}_1 \tag{7-43b}$$

This form of the field equivalence principle is known as *Love's equivalence principle* [7, 14]. Since the current densities of (7-43a) and (7-43b) radiate in an unbounded medium, that is, have the same μ_1, ϵ_1 everywhere, they can be used in conjunction with (6-30) through (6-35a) to find the fields everywhere.

Love's equivalence principle in Figure 7-8*a* produces a null field within the imaginary surface S. Since the value of the $\mathbf{E} = \mathbf{H} = 0$ within S cannot be disturbed if the properties of the medium within it are changed, let us assume that it is

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/226976724

Quantum Phenomena Within a New Theory of Time

Chapter · March 2006

DOI: 10.1007/3-540-26669-0_17

CITATIONS
20

READS
66

2 authors:

Avshalom C Elitzur
Iyar
80 PUBLICATIONS **1,162** CITATIONS

SEE PROFILE

Shahar Dolev
Tel Aviv University
23 PUBLICATIONS **207** CITATIONS

SEE PROFILE

All content following this page was uploaded by Shahar Dolev on 26 May 2014.

The user has requested enhancement of the downloaded file.

Nautilus: A Concurrent Anticipatory Programming Language

P. Blauth Menezes[*], Simone A. Costa[†], Júlio P. Machado[*] and Jaime Ramos[†]

[*]*Instituto de Informática, UFRGS, Av. Bento Gonçalves 9500, Campus do Vale, Bloco IV, CEP 91501-970, Caixa Postal: 15064, Porto Alegre, Brasil. {blauth,jmachado}@inf.ufrgs.br*

[†]*Centro de Ciências Exatas e Tecnológicas, UNISINOS, Av. Unisinos 950, CEP 93022-000, São Leopoldo, Brasil. sacosta,jaime@exatas.unisinos.br*

[†]*CLC, Departamento de Matemática, IST, Av. Rovisco Pais, 1049-001, Lisbon, Portugal. jaime@math.ist.utl.pt*

Abstract. Nautilus is a concurrent anticipatory programming language based on the principles of the language CNOMI which is a simplified and revised version of OBLOG. A semantics for Nautilus is given by Nonsequential Automata, that is a categorial semantic domain based on labeled transition systems with full concurrency, where a class of morphisms stands for anticipations. The semantics of an object in Nautilus is given by an anticipation morphism which is viewed as a special automatic morphism whose target automata, called base, is determined by the computations of a freely generated automata able to simulate any object specifier over the involved attributes, and the source automata is a relabelled restriction of the base. In order to introduce the anticipation of Nautilus, some examples are presented depicting the features of the language.

Keywords: anticipation, nonsequential automata, programming language, category theory.

1 INTRODUCTION

The main purpose of this paper is to present Nautilus as a concurrent anticipatory programming language, i.e., its semantic is on an anticipatory system that involves "its future", inspired by [5] and based on [8, 9,]. An anticipatory system [5] is a system for which the present behavior is based on past and/or present events but also on future events built from these past, present and future events. Nautilus [8, 7, 9] is a general purpose concurrent object-based language, originally based on the language Cronus [10, 11, 14], and introduces some special features inspired by the semantic domain such as anticipation. A semantics for Nautilus is given by Nonsequential Automata [8, 7, 9, 6], which constitute a categorial [1] semantic domain based on labeled transition system with full concurrency, where a class of morphisms stands for anticipation. It is a model which satisfies the diagonal compositionality requirement, i.e., anticipations compose and distribute over system combinators.

In Nautilus, an object can be specified either as a simple object or the resulting object of an encapsulation, aggregation, anticipation or parallel composition. An action of an object in Nautilus may be a sequential or concurrent composition of clauses, executed in an atomic way. The semantics of an object in Nautilus is given by an anticipation morphism where the target automata, called base, is determined by the computations of a freely generated automata able to simulate any object specifier over the involved attributes, and the source automata is a relabelled restriction of the base. An anticipation maps transitions into connections reflecting the implementation of an automaton on top of another. Therefore, an anticipation mapping is viewed as a special automatic morphism (a kind of implementation morphism [7] where the target object is closed under composition, i.e., the target (more concrete) automaton is enriched with all the conceivable sequential and nonsequential compositions that can be split into permutations of original transitions. Accordingly, the anticipation of an object is specified over an existing object (an action may be mapped into a complex action of the target object). Also, an action may be mapped according to several alternatives, that is, an anticipation may be state dependent. Thus, we say a more abstract object is "implemented" over a more concrete object, possibly specifying alternative "implementations". In other words, an

CASYS, Computing Anticipatory Systems: CASYS'2000 – 4th International Conference, edited by D. M. Dubois
© 2001 American Institute of Physics 0-7354-0088-4/01/$19.00

Downloaded 27 Nov 2002 to 192.58.150.40. Redistribution subject to AIP license or copyright, see http://proceedings.aip.org/proceedings/cpcr.jsp

arXiv:quant-ph/0303034v1 7 Mar 2003

The Feynman Path Integral: An Historical Slice

John R. Klauder *
Departments of Physics and Mathematics
University of Florida
Gainesville, FL 32611

Abstract

Efforts to give an improved mathematical meaning to Feynman's path integral formulation of quantum mechanics started soon after its introduction and continue to this day. In the present paper, one common thread of development is followed over many years, with contributions made by various authors. The present version of this line of development involves a continuous-time regularization for a general phase space path integral and provides, in the author's opinion at least, perhaps the optimal formulation of the path integral.

The Feynman Path Integral, 1948

Much has already been written about Feynman path integrals, and, no doubt, much more will be written in the future. A comprehensive survey after more than fifty years since their introduction would be a major undertaking, and this paper is not such a survey. Rather, it is an attempt to follow one relatively narrow development regarding a special form of regularization used in the definition of path integrals. Since we deal with several different approaches, this paper does not go too deeply into any one of them; it is intended more as a conceptual overview rather than a detailed exposition.

*Electronic mail: klauder@phys.ufl.edu

arXiv:quant-ph/0306042v1 5 Jun 2003

Multi-Party Pseudo-Telepathy

Gilles Brassard*, Anne Broadbent**, and Alain Tapp***

Département IRO, Université de Montréal, C.P. 6128, succursale centre-ville,
Montréal (Québec), Canada H3C 3J7
{brassard, broadbea, tappa}@iro.umontreal.ca

Abstract. Quantum entanglement, perhaps the most non-classical manifestation of quantum information theory, cannot be used to transmit information between remote parties. Yet, it can be used to reduce the amount of communication required to process a variety of distributed computational tasks. We speak of *pseudo-telepathy* when quantum entanglement serves to *eliminate* the classical need to communicate. In earlier examples of pseudo-telepathy, classical protocols could succeed with high probability unless the inputs were very large. Here we present a simple multi-party distributed problem for which the inputs and outputs consist of a single bit per player, and we present a perfect quantum protocol for it. We prove that no classical protocol can succeed with a probability that differs from $1/2$ by more than a fraction that is exponentially small in the number of players. This could be used to circumvent the detection loophole in experimental tests of nonlocality.

1 Introduction

It is well-known that quantum mechanics can be harnessed to reduce the amount of communication required to perform a variety of distributed tasks [3], through the use of either quantum communication [13] or quantum entanglement [6]. Consider for example the case of Alice and Bob, who are very busy and would like to find a time when they are simultaneously free for lunch. They each have an engagement calendar, which we may think of as n–bit strings a and b, where $a_i = 1$ (resp. $b_i = 1$) means that Alice (resp. Bob) is free for lunch on day i. Mathematically, they want to find an index i such that $a_i = b_i = 1$ or establish that such an index does not exist. The obvious solution is for Alice, say, to communicate her entire calendar to Bob, so that he can decide on the date: this requires roughly n bits of communication. It turns out that this is optimal in the worst case, up to a constant factor, according to classical information theory [8], even when the answer is only required to be correct with probability at least $2/3$. Yet, this problem can be solved with arbitrarily high success probability with the exchange of a number of *quantum* bits—known as *qubits*—in the order

* Supported in part by Canada's NSERC, Québec's FCAR, the Canada Research Chair Programme, and the Canadian Institute for Advanced Research.
** Supported in part by a scholarship from Canada's NSERC.
*** Supported in part by Canada's NSERC and Québec's FCAR.

arXiv:quant-ph/0309107v1 13 Sep 2003

Universal Signature of Non-Quantum Systems

Antony Valentini[1]

Perimeter Institute for Theoretical Physics, 35 King Street North, Waterloo, Ontario N2J 2W9, Canada.[2]
Theoretical Physics Group, Blackett Laboratory, Imperial College, Prince Consort Road, London SW7 2BZ, England.
Augustus College, 14 Augustus Road, London SW19 6LN, England.[3]

It is shown that 'non-quantum systems', with anomalous statistical properties, would carry a distinctive experimental signature. Such systems can exist in deterministic hidden-variables theories (such as the pilot-wave theory of de Broglie and Bohm). The signature consists of non-additive expectations for non-commuting observables, breaking the sinusoidal modulation of quantum probabilities for two-state systems. This effect is independent of the quantum state (pure or mixed), or of the details of the hidden-variables model. Experiments are proposed, testing polarisation probabilities for single photons.

[1]email: avalentini@perimeterinstitute.ca
[2]Corresponding address.
[3]Permanent address.

arXiv:hep-th/0310145v1 15 Oct 2003

Noncommutative geometry and the standard model

Encyclopedia of Mathematical Physics, J.-P. Francoise, G. Naber & Tsou Sheung Tsun (eds.), Elsevier Science

1 Introduction

The aim of this contribution is to explain how Connes derives the standard model of electromagnetic, weak and strong forces from noncommutative geometry. The reader is supposed to be aware of two other derivations in fundamental physics: the derivation of the Balmer-Rydberg formula for the spectrum of the hydrogen atom from quantum mechanics and Einstein's derivation of gravity from Riemannian geometry.

At the end of the 19th century, new physics was discovered in atoms, their discrete spectra. Balmer and Rydberg succeeded to put order into the fast growing set of experimental numbers with the help of a phenomenological ansatz for the frequencies ν of the spectral rays of e.g. the hydrogen atom,

$$\nu = g(n_2^q - n_1^q), \quad n_j \in \mathbb{N}, \quad q \in \mathbb{Z}, \quad g \in \mathbb{R}. \tag{1}$$

The integer variables n_1 and n_2 reflect the discreteness of the spectrum. On the other hand the discrete parameter q and the continuous parameter g were fitted by experiment: $q = -2$ and $g = 3.289\ 10^{15}$ Hz, the famous Rydberg constant. Later quantum mechanics was discovered and allowed to derive the Balmer-Rydberg ansatz and to constrain its parameters:

$$q = 2 \quad \text{and} \quad g = \frac{m_e}{4\pi\hbar^3}\frac{e^4}{(4\pi\epsilon_0)^2}, \tag{2}$$

in beautiful agreement with the anterior experimental fit.

2 The standard model

We propose to introduce the standard model in analogy with the Balmer-Rydberg formula, Tab. 1.

2.1 The Yang-Mills-Higgs ansatz

The variables of this Lagrangian ansatz are spin 1 particles A, spin $\frac{1}{2}$ particles decomposed into left- and right-handed components $\psi = (\psi_L, \psi_R)$ and spin 0 particles φ. There are four discrete parameters, a compact real Lie group G, and three unitary representations on complex Hilbert spaces $\mathcal{H}_L$, $\mathcal{H}_R$, and $\mathcal{H}_S$. The spin 1 particles come in a multiplet living in the complexified of the Lie algebra of G, $A \in \mathrm{Lie}(G)^{\mathbb{C}}$. The left-handed and right-handed spinors come in multiplets living in the Hilbert spaces, $\psi_L \in \mathcal{H}_L$, $\psi_R \in \mathcal{H}_R$. The (Higgs) scalar is another

arXiv:quant-ph/0311039v4 15 Jul 2004

Multilinear Formulas and Skepticism of Quantum Computing

Scott Aaronson*

Abstract

Several researchers, including Leonid Levin, Gerard 't Hooft, and Stephen Wolfram, have argued that quantum mechanics will break down before the factoring of large numbers becomes possible. If this is true, then there should be a natural set of quantum states that can account for all quantum computing experiments performed to date, but *not* for Shor's factoring algorithm. We investigate as a candidate the set of states expressible by a polynomial number of additions and tensor products. Using a recent lower bound on multilinear formula size due to Raz, we then show that states arising in quantum error-correction require $n^{\Omega(\log n)}$ additions and tensor products even to approximate, which incidentally yields the first superpolynomial gap between general and multilinear formula size of functions. More broadly, we introduce a complexity classification of pure quantum states, and prove many basic facts about this classification. Our goal is to refine vague ideas about a breakdown of quantum mechanics into specific hypotheses that might be experimentally testable in the near future.

1 Introduction

> QC of the sort that factors long numbers seems firmly rooted in science fiction ... The present attitude would be analogous to, say, Maxwell selling the Daemon of his famous thought experiment as a path to cheaper electricity from heat. —Leonid Levin [35]

Quantum computing presents a dilemma: is it reasonable to study a type of computer that has never been built, and might never be built in one's lifetime? Some researchers strongly believe the answer is 'no.' Their objections generally fall into four categories:

(A) There is a fundamental physical reason why large quantum computers can never be built.

(B) Even if (A) fails, large quantum computers will never be built in practice.

(C) Even if (A) and (B) fail, the speedup offered by quantum computers is of limited theoretical interest.

(D) Even if (A), (B), and (C) fail, the speedup is of limited practical value.[1]

*University of California, Berkeley. Email: aaronson@cs.berkeley.edu. Part of this work was done at the Perimeter Institute (Waterloo, Canada). Supported by an NSF Graduate Fellowship and by the Defense Advanced Research Projects Agency (DARPA).

[1] Because of the 'even if' clauses, the objections seem to us logically independent, so that there are 16 possible positions regarding them (or 15 if one is against quantum computing). We ignore the possibility that no speedup exists, in other words that BPP = BQP. By 'large quantum computer' we mean any computer much faster than its best classical simulation, as a result of asymptotic complexity rather than the speed of elementary operations. Such a computer need not be universal; it might be specialized for (say) factoring.

arXiv:quant-ph/0401062v2 17 Mar 2004

Is Quantum Mechanics An Island In Theoryspace?

Scott Aaronson*

Abstract

This recreational paper investigates what happens if we change quantum mechanics in several ways. The main results are as follows. First, if we replace the 2-norm by some other p-norm, then there are no nontrivial norm-preserving linear maps. Second, if we relax the demand that norms be preserved, we end up with a theory that allows rapid solution of PP-complete problems (as well as superluminal signalling). And third, if we restrict amplitudes to be real, we run into a difficulty much simpler than the usual one based on parameter-counting of mixed states.

1 Introduction

"It is striking that it has so far not been possible to find a logically consistent theory that is close to quantum mechanics, other than quantum mechanics itself." —Steven Weinberg, *Dreams of a Final Theory* [13]

The title of this paper should be self-explanatory, but if it isn't: "theoryspace" is the space of logically conceivable physical theories, with two theories close to each other if they differ in few respects. An "island" in theoryspace is a natural and interesting theory, whose neighbors are all somehow perverse or degenerate.[1] The Standard Model isn't an island, because we don't know any compelling (non-anthropic) reason why the masses and coupling constants should have the values they do.[2] Likewise, general relativity is probably not an island, because of alternatives such as the Brans-Dicke theory.

To many physicists, however, quantum mechanics *does* seem like an island: change any one aspect, and the whole structure collapses. This view is buttressed by three types of results:

(1) **"Derivations" of the $|\psi|^2$ probability rule.** Gleason's Theorem [9] shows that, in a Hilbert space of dimension 3 or higher, the usual quantum probability rule is the only one consistent with a requirement of noncontextuality. Deutsch [7] and Zurek [14] derived the rule from other assumptions.

(2) **Arguments for complex amplitudes.** If $f(n)$ is the number of real parameters needed to specify an n-dimensional mixed state, then only when amplitudes are complex numbers does $f(n_A n_B) = f(n_A) f(n_B)$ (since $f(n) = n^2$). With real amplitudes, $f(n) = n(n+1)/2$ and thus $f(n_A n_B) > f(n_A) f(n_B)$. With quaternionic amplitudes, $f(n) = 2n^2 - n$ and thus $f(n_A n_B) < f(n_A) f(n_B)$. Caves, Fuchs, and Schack [6] exploited this observation to show that a "quantum de Finetti Theorem" (which justifies Bayesian reasoning) works only if amplitudes are complex. Hardy [10] also made essential use of the observation in his derivation of quantum mechanics from "five simple axioms."

(3) **"Perverse" consequences of nonlinearity.** After Weinberg [12] proposed nonlinear variants of the Schrödinger equation, Gisin [8] and Polchinski [11] independently observed that almost all such

*University of California, Berkeley. Email: aaronson@cs.berkeley.edu. Supported by an NSF Graduate Fellowship, by NSF ITR Grant CCR-0121555, and by the Defense Advanced Research Projects Agency (DARPA).

[1] A bit of pedantry: a physicist might call the neighbors of quantum mechanics I'll discuss "inconsistent," since they contradict auxiliary assumptions that the physicist considers obvious. I'll stick to milder epithets like "perverse."

[2] More pedantry: whether a theory is an island is therefore a function of our knowledge, not just of the theory itself.

arXiv:quant-ph/0404072v1 12 Apr 2004

ON THE NOTION OF PHASE IN MECHANICS

Maurice A de Gosson
BTH-Karlskrona
SE-371 79 Karlskrona

July 23, 2013

Abstract

The notion of phase plays an essential role in both semiclassical and quantum mechanics. But what is exactly a phase, and how does it change with time? It turns out that the most universal definition of a phase can be given in terms of Lagrangian manifolds by exploiting the properties of the Poincaré–Cartan form. Such a phase is defined, not in configuration space, but rather in phase space and is thus insensitive to the appearance of caustics. Surprisingly enough this approach allows us to recover the Heisenberg–Weyl formalism without invoking commutation relations for observables.

Contents

1 Introduction **2**

2 Lagrangian Manifolds in Mechanics **5**

3 The Phase of a Lagrangian Submanifold **6**

4 The Local Expression of the Phase **10**

5 Symplectic Frames and Lagrangian Phases **11**

6 Hamiltonian Motions and Phase **14**

7 Phase and Heisenberg–Weyl Operators **18**

arXiv:quant-ph/0404134v2 3 Feb 2005

Are All Particles Real?

Sheldon Goldstein*, James Taylor†,
Roderich Tumulka‡ and Nino Zanghì§

September 27, 2004

Abstract

In Bohmian mechanics elementary particles exist objectively, as point particles moving according to a law determined by a wavefunction. In this context, questions as to whether the particles of a certain species are real—questions such as, Do photons exist? Electrons? Or just the quarks?—have a clear meaning. We explain that, whatever the answer, there is a corresponding Bohm-type theory, and no experiment can ever decide between these theories. Another question that has a clear meaning is whether particles are intrinsically distinguishable, i.e., whether particle world lines have labels indicating the species. We discuss the intriguing possibility that the answer is no, and particles are points—*just points*.

PACS number: 03.65.Ta (foundations of quantum mechanics)
Key words: Bohmian mechanics, ontology, empirical equivalence, fundamental limitations of science, particle trajectories in quantum physics

1 Introduction

We address in this paper rather basic but intimidating questions about the ontology in Bohmian mechanics and similar theories, using two specific questions as a case study. What is intimidating about these questions is that they cannot be answered experimentally. However, as we shall explain, this does not mean they cannot be answered. Most, if not all, of what we point out in this paper has surely been known to some experts. However, we have found no clear discussion of the matter in the literature.

*Departments of Mathematics, Physics and Philosophy, Hill Center, Rutgers, The State University of New Jersey, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019, USA. E-mail: oldstein@math.rutgers.edu

†Department of Mathematics, Iowa State University, Carver Hall, Ames, IA 50010, USA. E-mail: jostylr@member.ams.org

‡Dipartimento di Fisica dell'Università di Genova and INFN sezione di Genova, Via Dodecaneso 33, 16146 Genova, Italy. E-mail: tumulka@mathematik.uni-muenchen.de

§Dipartimento di Fisica dell'Università di Genova and INFN sezione di Genova, Via Dodecaneso 33, 16146 Genova, Italy. E-mail: zanghi@ge.infn.it

arXiv:quant-ph/0405039v2 3 Feb 2005

Are All Particles Identical?

Sheldon Goldstein*, James Taylor†,
Roderich Tumulka‡ and Nino Zanghì§

September 28, 2004

Abstract

We consider the possibility that all particles in the world are fundamentally identical, i.e., belong to the same species. Different masses, charges, spins, flavors, or colors then merely correspond to different quantum states of the same particle, just as spin-up and spin-down do. The implications of this viewpoint can be best appreciated within Bohmian mechanics, a precise formulation of quantum mechanics with particle trajectories. The implementation of this viewpoint in such a theory leads to trajectories different from those of the usual formulation, and thus to a version of Bohmian mechanics that is inequivalent to, though arguably empirically indistinguishable from, the usual one. The mathematical core of this viewpoint is however rather independent of the detailed dynamical scheme Bohmian mechanics provides, and it amounts to the assertion that the configuration space for N particles, even N "distinguishable particles," is the set of all N-point subsets of physical 3-space.

PACS numbers: 03.65.Ta (foundations of quantum mechanics)

1 Introduction and Overview

It is not a new idea that what appear to be two different species of particles may in fact be two different states of the same species. It is particularly obvious that spin-up and

*Departments of Mathematics, Physics and Philosophy, Hill Center, Rutgers, The State University of New Jersey, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019, USA. E-mail: oldstein@math.rutgers.edu

†Department of Mathematics, Iowa State University, Carver Hall, Ames, IA 50010, USA. E-mail: jostylr@member.ams.org

‡Dipartimento di Fisica dell'Università di Genova and INFN sezione di Genova, Via Dodecaneso 33, 16146 Genova, Italy. E-mail: tumulka@mathematik.uni-muenchen.de

§Dipartimento di Fisica dell'Università di Genova and INFN sezione di Genova, Via Dodecaneso 33, 16146 Genova, Italy. E-mail: zanghi@ge.infn.it

arXiv:quant-ph/0406205v1 27 Jun 2004

Almost Certain Escape from Black Holes

Seth Lloyd*
MIT Mechanical Engineering

Abstract: Recent models of the black-hole final state suggest that quantum information can escape from a black hole by a process akin to teleportation. These models require a specific final state and restrictions on the interaction between the collapsing matter and the incoming Hawking radiation for quantum information to escape. This paper investigates escape from black holes for arbitrary final states and for generic interactions between matter and Hawking radiation. Classical information, including the result of any computation performed by the matter inside the hole, escapes from the hole with certainty. Quantum information escapes with fidelity $\approx (8/3\pi)^2$: only half a bit of quantum information is lost on average, independent of the number of bits that escape from the hole.

It has been proposed that black holes could function as quantum computers [1-2]; the computational capacity of black holes can be calculated in terms of their mass and lifetime [1-3]. In order to function as a useful computer, however, a black hole must permit information to escape as the black hole evaporates. Recently, Horowitz and Maldacena proposed a model of black hole evaporation that imposes a final state boundary condition at the black-hole singularity [4]. The result is a nonlinear time evolution for the quantum states in and outside of the black hole, which permits quantum information to escape from the black hole by a process akin to teleportation. Because it allows information to escape, such a model naturally allows the black hole to function as a computer whose output is written in the outgoing Hawking radiation produced during evaporation, as envisioned in [1]. The Horowitz-Maldacena model requires a specific final state which is perfectly entangled between the matter that formed the black hole and the incoming Hawking radiation. Whether or not quantum gravity supports such a final state remains

arXiv:quant-ph/0406216v1 29 Jun 2004

New quantum algorithm for studying NP-complete problems

Masanori Ohya
Tokyo University of Science,
Department of Information Sciences,
Noda City, Chiba 278-8510, Japan
e-mail: ohya@is.noda.tus.ac.jp

Igor V. Volovich
Steklov Mathematical Institute,
Gubkin St. 8, 117966 Moscow, Russia
e-mail: volovich@mi.ras.ru

February 1, 2008

Abstract

Ordinary approach to quantum algorithm is based on quantum Turing machine or quantum circuits. It is known that this approach is not powerful enough to solve NP-complete problems. In this paper we study a new approach to quantum algorithm which is a combination of the ordinary quantum algorithm with a chaotic dynamical system. We consider the satisfiability problem as an example of NP-complete problems and argue that the problem, in principle, can be solved in polynomial time by using our new quantum algorithm.

keywords: Quantum Algorithm, NP-complete problem, Chaotic Dynamics

1 Introduction

Ordinary approach to quantum algorithm is based on quantum Turing machine or quantum circuits [1, 2, 3]. It is known that this approach is not powerful enough to solve NP-complete problems [4, 5]. In [6] we have proposed a new approach to quantum algorithm which goes beyond the standard quantum computation paradigm. This new approach is a sort of combination of the ordinary quantum algorithm and a chaotic dynamics. This approach was based on the results obtained in the paper [7].

There are important problems such as the knapsack problem, the traveling salesman problem, the integer programming problem, the subgraph isomorphism problem, the satisfiability problem that have been studied for decades

Black hole entropy from Quantum Geometry

Marcin Domagala[1] and Jerzy Lewandowski[1,2,3]

1. Instytut Fizyki Teoretycznej, Uniwersytet Warszawski, ul. Hoża 69, 00-681 Warszawa, Poland

2. Physics Department, 104 Davey, Penn State, University Park, PA 16802, USA

3. Max Planck Institut für Gravitationsphysik, Albert Einstein Institut, 14476 Golm, Germany

arXiv:gr-qc/0407051v2 23 Aug 2004

Abstract

Quantum Geometry (the modern Loop Quantum Gravity using graphs and spin-networks instead of the loops) provides microscopic degrees of freedom that account for the black-hole entropy. However, the procedure for state counting used in the literature contains an error and the number of the relevant horizon states is underestimated. In our paper a correct method of counting is presented. Our results lead to a revision of the literature of the subject. It turns out that the contribution of spins greater then 1/2 to the entropy is not negligible. Hence, the value of the Barbero-Immirzi parameter involved in the spectra of all the geometric and physical operators in this theory is different than previously derived. Also, the conjectured relation between Quantum Geometry and the black hole quasi-normal modes should be understood again.

Pacs 04.60Pp, 04.60.Ds, 04.60.Nc, 03.65.Sq

arXiv:quant-ph/0407221v3 22 Nov 2004

Quantum Pseudo-Telepathy

Gilles Brassard [*] Anne Broadbent [†] Alain Tapp [‡]

Département IRO, Université de Montréal
C.P. 6128, succursale centre-ville
Montréal (Québec), H3C 3J7 Canada

{brassard, broadbea, tappa}@iro.umontreal.ca

Abstract

Quantum information processing is at the crossroads of physics, mathematics and computer science. It is concerned with that we can and cannot do with quantum information that goes beyond the abilities of classical information processing devices. Communication complexity is an area of classical computer science that aims at quantifying the amount of communication necessary to solve distributed computational problems. *Quantum* communication complexity uses quantum mechanics to reduce the amount of communication that would be classically required.

Pseudo-telepathy is a surprising application of quantum information processing to communication complexity. Thanks to entanglement, perhaps the most nonclassical manifestation of quantum mechanics, two or more quantum players can accomplish a distributed task with no need for communication whatsoever, which would be an impossible feat for classical players.

After a detailed overview of the principle and purpose of pseudo-telepathy, we present a survey of recent and no-so-recent work on the subject. In particular, we describe and analyse all the pseudo-telepathy games currently known to the authors.

Keywords: Entanglement, Nonlocality, Bell's theorem, Quantum information processing, Quantum communication complexity, Pseudo-telepathy.

[*] Supported in part by Canada's NSERC, Québec's FQRNT, the Canada Research Chair programme, the Canadian Institute for Advanced Research (CIAR), the Mathematics of Information Technology and Complex Systems Network (MITACS) and the Canadian Institute for Photonic Innovations (CIPI).

[†] Supported in part by a scholarship from Canada's NSERC.

[‡] Supported in part by Canada's NSERC, Québec's FQRNT, the CIAR and MITACS.

The roots of any polynomial equation

G.A.Uytdewilligen,
Bergen op Zoomstraat 76, 5652 KE Eindhoven, g.a.uytdewilligen@connect.nl

Abstract
We provide a method for solving the roots of the general polynomial equation

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_1 \cdot x + s = 0 \tag{1}$$

To do so, we express x as a powerseries of s, and calculate the first n-2 coefficients. We turn the polynomial equation into a differential equation that has the roots as solutions. Then we express the powerseries' coefficients in the first n-2 coefficients. Then the variable s is set to a0. A free parameter is added to make the series convergent. © 2004 G.A.Uytdewilligen. All rights reserved.

Keywords: Algebraic equation

The method

The method is based on [1]. Let's take the first n-1 derivatives of (1) to s. Equate these derivatives to zero. Then find $\frac{d^i}{ds^i} x(s)$ in terms of x(s) for i from 1 to n-1. Now make a new differential equation

$$m1 \frac{d^{n-1}}{ds^{n-1}} x(s) + m2 \frac{d^{n-2}}{ds^{n-2}} x(s) + \ldots + m_n \cdot x(s) + m_{n+1} = 0 \tag{2}$$

and fill in our $\frac{d^i}{ds^i} x(s)$ in (2). Multiply by the denominator of the expression. Now we have a polynomial in x(s) of degree higher then n. Using (1) as property, we simplify this polynomial to the degree of n. Set it equal to (1) and solve $m_1 .. m_{n+1}$ in terms of s and $a_1 .. a_n$. Substituting these in (2) gives a differential equation that has the zeros of (1) among its solutions. We then insert

$$x(s) = y(s) - \frac{a_{n-1}}{n \cdot a_n} \tag{3}$$

in (2). Multiplying by the denominator we get a differential equation of the linear form:

$$p1 \frac{d^{n-1}}{ds^{n-1}} y(s) + p2 \frac{d^{n-2}}{ds^{n-2}} y(s) + \ldots + p_n \cdot y(s) = 0 \tag{4}$$

With $p_1(s)..p_n(s)$ polynomials in s. If we substitute our powerseries, all the coefficients are determined by the first n-1 coefficients. The first coefficients are calculated as follows: A powerseries is filled in in (1).

$$x(s) = \sum_{i=0}^{n-2} b_i \cdot s^i - \frac{a_n}{n \cdot a_{n-1}} \tag{5}$$

and it should be zero for all s. From this, we calculate b_i for i from 0 to n-2.b_0 Is a root af an n-1 degree polynomial and the other b_i are expressed in b_0 Now a powerseries is inserted in (4):

Hydrodynamic construction of the electromagnetic field

Peter Holland

Green College
University of Oxford
Oxford OX2 6HG
England

peter.holland@green.ox.ac.uk

11th June 2005

Abstract

We present an alternative Eulerian hydrodynamic model for the electromagnetic field in which the discrete vector indices in Maxwell's equations are replaced by continuous angular freedoms, and develop the corresponding Lagrangian picture in which the fluid particles have rotational and translational freedoms. This enables us to extend to the electromagnetic field the exact method of state construction proposed previously for spin 0 systems, in which the time-dependent wavefunction is computed from a single-valued continuum of deterministic trajectories where two spacetime points are linked by at most a single orbit. The deduction of Maxwell's equations from continuum mechanics is achieved by generalizing the spin 0 theory to a general Riemannian manifold from which the electromagnetic construction is extracted as a special case. In particular, the flat-space Maxwell equations are represented as a curved-space Schrödinger equation for a massive system. The Lorentz covariance of the Eulerian field theory is obtained from the non-covariant Lagrangian-coordinate model as a kind of collective effect. The method makes manifest the electromagnetic analogue of the quantum potential that is tacit in Maxwell's equations. This implies a novel definition of the "classical limit" of Maxwell's equations that differs from geometrical optics. It is shown that Maxwell's equations may be obtained by canonical quantization of the classical model. Using the classical trajectories a novel expression is derived for the propagator of the electromagnetic field in the Eulerian picture. The trajectory and propagator methods of solution are illustrated for the case of a light wave.

PACS: 03.50.De; 03.65.Ta

"…it is a good thing to have two ways of looking at a subject, and to admit that there *are* two ways of looking at it." [1]

1. INTRODUCTION

In a recent article [2] a method was described that provides an exact scheme to calculate the time-dependent wavefunction for a spin 0 system from a single-valued continuum of deterministic trajectories where two spacetime points are linked by at most a single orbit. A

arXiv:quant-ph/0412063v1 8 Dec 2004

Quantum Information Theory and The Foundations of Quantum Mechanics

Christopher Gordon Timpson
The Queen's College

A thesis submitted for the degree of Doctor of Philosophy
at the University of Oxford

Trinity Term 2004

arXiv:quant-ph/0412078v1 10 Dec 2004

Quantum-Enhanced Measurements: Beating the Standard Quantum Limit

Vittorio Giovannetti[1], **Seth Lloyd**[2], **Lorenzo Maccone**[3]

[1] *NEST-INFM & Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126, Pisa, Italy.*

[2] *MIT, Research Laboratory of Electronics and Dept. of Mechanical Engineering, 77 Massachusetts Ave., Cambridge, MA 02139, USA.*

[3] *QUIT - Quantum Information Theory Group, Dip. di Fisica "A. Volta", Università di Pavia, via A. Bassi 6 I-27100, Pavia, Italy.*

One sentence summary: **To attain the limits to measurement precision imposed by quantum mechanics, 'quantum tricks' are often required.**

Abstract: Quantum mechanics, through the Heisenberg uncertainty principle, imposes limits to the precision of measurement. Conventional measurement techniques typically fail to reach these limits. Conventional bounds to the precision of measurements such as the shot noise limit or the standard quantum limit are not as fundamental as the Heisenberg limits, and can be beaten using quantum strategies that employ 'quantum tricks' such as squeezing and entanglement.

Measurement is a physical process, and the accuracy to which measurements can be performed is governed by the laws of physics. In particular, the behavior of systems at small scales is governed by the laws of quantum mechanics, which place limits on the accuracy to which measurements can be performed. These limits to accuracy take two forms. First, the Heisenberg uncertainty relation [1] imposes an intrinsic uncertainty in the values of measurement results of complementary observables such as position and momentum, or the different components of the angular momentum of a rotating object (Fig. 1). Second, every measurement apparatus is itself a quantum system: as a result, the uncertainty relations together with other quantum constraints on the speed of evolution (such as the Margolus-Levitin theorem [2]) impose limits on how accurately we can measure quantities given the amount of physical resources, e.g. energy, at hand to perform the measurement.

One important consequence of the physical nature of measurement is the so-called 'quantum back action': the extraction of information from a system can give rise to a feedback effect in which the system configuration after the measurement is determined by the measurement outcome. For example, the most extreme case (the so-called von Neumann or projective measurement) produces a complete determination of the post-measurement state. When

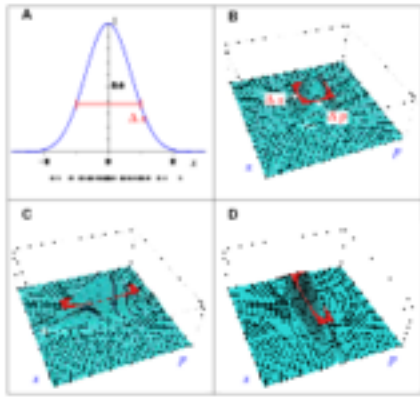


Figure 1: The Heisenberg uncertainty relation. In quantum mechanics the outcomes x_1, x_2, *etc.* of the measurements of a physical quantity x are statistical variables; that is, they are randomly distributed according to a probability determined by the state of the system. A measure of the "sharpness" of a measurement is given by the spread Δx of the outcomes: An example is given in **(A)**, where the outcomes (tiny triangles) are distributed according to a Gaussian probability with standard deviation Δx. The Heisenberg uncertainty relation states that when simultaneously measuring incompatible observables such as position x and momentum p the product of the spreads is lower bounded: $\Delta x\,\Delta p \geq \hbar/2$, where $\hbar$ is the Planck constant. The same is true when measuring one of the observables (say x) on a set of particles prepared with a spread Δp on the other observable. [In the general case when we are measuring two observables A and B, the lower bound is given by the expectation value of the commutator between the quantum operators associated to A and B.] In **(B)** we see a coherent state (depicted through its Wigner function): it has the same spreads in position and momentum $\Delta x = \Delta p$. In **(C)** and **(D)**, squeezed states are shown: they have reduced fluctuations in one of the two incompatible observables [*i.e.* x for **(C)** and p for **(D)**] at the expense of increased fluctuations in the other. The Heisenberg relation states that the red areas in the plots (given by the product $\Delta x\Delta p$) must have a surface larger than $\hbar/2$. In quantum optics, the observables x and p are replaced by the in-phase and out-of-phase amplitudes of the electromagnetic field, i.e. by its "quadratures". The Heisenberg principle is so called only for historical reasons: it is not a principle in modern quantum mechanics, since it is a consequence of the measurement postulate [1]. Moreover, Heisenberg's formulation of a dynamical disturbance necessarily induced on a system by a measurement was experimentally proven wrong [3]: it is possible to devise experiments where the disturbance is totally negligible, but where the Heisenberg relations are still valid. They are enforced by the complementarity of quantum mechanics.

Tools of the Hardware Hacking Trade

Black Hat Webcast, April 23, 2014

Joe Grand (@joegrand)

CDD: 115

THE NOTION OF PROCESS IN NONSTANDARD THEORY AND IN WHITEHEADIAN METAPHYSICS

STATHIS LIVADAS
Mesologgiou 66, 26222
Patras
GREECE

livadas@math.upatras.gr

Received: 10.03.2012; Revised: 07.09.2012; Accepted: 21.12.2012

Abstract: In this article I intend to show that certain aspects of A.N. Whitehead's philosophy of organism and especially his epochal theory of time, as mainly exposed in his well-known work *Process and Reality*, can serve in clarify the underlying assumptions that shape nonstandard mathematical theories as such and also as metatheories of quantum mechanics. Concerning the latter issue, I point to an already significant research on nonstandard versions of quantum mechanics; two of these approaches are chosen to be critically presented in relation to the scope of this work. The main point of the paper is that, insofar as we can refer a nonstandard mathematical entity to a kind of axiomatical formalization essentially 'codifying' an underlying mental process indescribable as such by analytic means, we can possibly apply certain principles of Whitehead's metaphysical scheme focused on the key notion of process which is generally conceived as the becoming of actual entities. This is done in the sense of a unifying approach to provide an interpretation of nonstandard mathematical theories as such and also, in their metatheoretical status, as a formalization of the empirical-experimental context of quantum mechanics.

Keywords: Actual entity. Concrescence. Coordinate division. Divisibility relation. Genetic division. Infinitesimal. Nonstandard hull. Prehension. Process. Standard. Ulten eigenvector.

Types and Forms of Emergence

Jochen Fromm

Distributed Systems Group,
Electrical Engineering & Computer Science,
Universität Kassel, Germany

Abstract. The knowledge of the different types of emergence is essential if we want to understand and master complex systems in science and engineering, respectively. This paper specifies a universal taxonomy and comprehensive classification of the major types and forms of emergence in Multi-Agent Systems, from simple types of intentional and predictable emergence in machines to more complex forms of weak, multiple and strong emergence.

1. Introduction

The emergence of order and organization in systems composed of many autonomous entities or agents is a very fundamental process. The process of emergence deals with the fundamental question: "how does an entity come into existence?" In a process of emergence we observe something (for instance the appearance of order or organization) and ask how this is possible, since we assume causality: every effect should have a cause. The surprising aspect in a process of emergence is the observation of an effect without an apparent cause. Although the process of emergence might look mysterious, there is nothing mystical, magical or unscientific about it.

If we consider the world of emergent properties, the deepest mysteries are as close as the nearest seedling, ice cube, grain of salt or pile of sand, as Laughlin explains in his book [Laughlin05]. It is doubtful that the ultimate laws can be found at inconceivable high energies or extreme scales, if we do not understand things at our own scale well enough. In other words we must step back and look at the patterns and the interactions of everyday objects to discover the nature of our universe.

Emergent properties are amazing and paradox: they are very fundamental and yet familiar. Emergent phenomena in generated systems are according to John H. Holland typically persistent patterns with changing components [Holland98], i.e. they are changeless *and* changing, constant *and* fluctuating, persistent *and* shifting, inevitable *and* unpredictable. Moreover an emergent property is a part of the system and at the same time it is not a part of the system, it depends on a system because it appears in it and is yet independent from it to a certain degree. According to the Stanford Encyclopedia of Philosophy, "emergent entities (properties or substances) 'arise' out of more fundamental entities and yet are 'novel' or

arXiv:quant-ph/0506115v2 14 Oct 2005

Generalizations of Quantum Mechanics

Philip Pearle
Hamilton College
Clinton, NY 13323, USA
e-mail: ppearle@hamilton.edu

Antony Valentini
Perimeter Institute for Theoretical Physics
31 Caroline Street North, Waterloo, Ontario N2L 2Y5, Canada
e-mail: avalentini@perimeterinstitute.ca

Abstract

We review realistic models that reproduce quantum theory in some limit and yield potentially new physics outside that limit. In particular, we consider deterministic hidden-variables theories (such as the pilot-wave model) and their extension to "quantum nonequilibrium," and we consider the continuous spontaneous localization model of wave function collapse. Other models are briefly discussed.

CONTENTS

1 Introduction
2 Hidden Variables and Quantum Nonequilibrium
– 2.1 Pilot-Wave Theory
– 2.2 H-Theorem: Relaxation to Equilibrium
– 2.3 Nonlocal Signaling
– 2.4 Subquantum Measurement
– 2.5 Subquantum Information and Computation
– 2.6 Extension to All Deterministic Hidden-Variables Theories
3 Continuous Spontaneous Localization Model (CSL)
– 3.1 Requirements for Stochastic Collapse Dynamics
– 3.2 CSL in Essence
– 3.3 CSL
– 3.4 Consequences of CSL
– 3.5 Further Remarks
– 3.6 Spontaneous Localization Model (SL)
4 Other Models

To be published in: *Encyclopaedia of Mathematical Physics*, eds. J.-P. Françoise, G. Naber and T. S. Tsun (Elsevier, 2006).

arXiv:quant-ph/0508211v3 30 Nov 2006

Information processing in generalized probabilistic theories

Jonathan Barrett*
Perimeter Institute for Theoretical Physics, 31 Caroline Street N, Waterloo, Ontario N2L 2Y5, Canada

I introduce a framework in which a variety of probabilistic theories can be defined, including classical and quantum theories, and many others. From two simple assumptions, a tensor product rule for combining separate systems can be derived. Certain features, usually thought of as specifically quantum, turn out to be generic in this framework, meaning that they are present in all except classical theories. These include the non-unique decomposition of a mixed state into pure states, a theorem involving disturbance of a system on measurement (suggesting that the possibility of secure key distribution is generic), and a no-cloning theorem. Two particular theories are then investigated in detail, for the sake of comparison with the classical and quantum cases. One of these includes states that can give rise to arbitrary non-signalling correlations, including the super-quantum correlations that have become known in the literature as Nonlocal Machines or Popescu-Rohrlich boxes. By investigating these correlations in the context of a theory with well-defined dynamics, I hope to make further progress with a question raised by Popescu and Rohrlich, which is, why does quantum theory not allow these strongly nonlocal correlations? The existence of such correlations forces much of the dynamics in this theory to be, in a certain sense, classical, with consequences for teleportation, cryptography and computation. I also investigate another theory in which all states are local. Finally, I raise the question of what further axiom(s) could be added to the framework in order uniquely to identify quantum theory, and hypothesise that quantum theory is optimal for computation.

PACS numbers: 03.67.-a, 03.65.Ta

I. INTRODUCTION

The question is periodically raised, what is responsible for the power of quantum computation (or cryptography, or information processing in general)? At a recent meeting in Konstanz [1], speakers referred to quantum entanglement; the superposition principle; the exponentially growing size of Hilbert space with the number of qubits; nonlocality and contextuality; the possibility of continuous reversible transformations between pure states; and the so-called sign problem in Monte Carlo simulations of certain types of quantum system [2]. It is perhaps unsurprising that there are so many different answers. The problem is that the results of quantum information theory are already well understood as consequences of the quantum formalism, and it is not clear that simply pointing to aspects of that formalism tells us anything new. What we are really looking for is a better understanding of the connections between information processing and physical principles in general.

Such an understanding could be gained by studying information processing in a broader range of theories than classical and quantum, where different physical principles may hold. For any theory, whether it applies to Nature or not, one can consider the information processing possibilities of this theory, the differences from those of classical or quantum theory, and attempt to trace these possibilities back to the fundamental features of the theory. Some authors have indeed investigated unrealistic theories, with a view to understanding the relevant features [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13].

To make further progress along these lines, I introduce an operational framework for probabilistic theories in which a broad range of different theories can be defined. The framework, described in Sections II, III and IV, is based on that used by Hardy in his derivation of quantum theory from simple axioms [14]. The basic idea is that a state is represented as a vector of probabilities of measurement outcomes. Transformations of a system must correspond to linear transformations of this vector. By including probabilistic, that is normalization-decreasing, transformations, a unified account of transformations and measurements can be given. Rather than employ any of Hardy's axioms, I introduce two assumptions that concern how separate systems combine to form a joint system. The first is that operations on the separate systems commute (this implies a no-signalling principle), and the second is that the state of the joint system can be completely specified by joint probabilities for local measurements. From these assumptions a tensor product rule can be derived. This removes at least some of the mystery from the quantum tensor product rule and generalizes a derivation by Fuchs [15].

The resulting framework includes classical probabilistic theories, quantum theory, and many other theories besides. The first thing one notices is that certain phenomena, usually thought of as specifically quantum, are in fact generic. This means that they either appear in all theories, or they appear in all theories except classical theories, which emerge as a very special case. As shown in Section V, these phenomena include the non-unique decomposition of a mixed state into pure states, a

*Electronic address: jbarrett@perimeterinstitute.ca

arXiv:math/0508341v2 [math.DG] 18 Aug 2005

DISCRETE EXTERIOR CALCULUS

MATHIEU DESBRUN, ANIL N. HIRANI, MELVIN LEOK, AND JERROLD E. MARSDEN

ABSTRACT. We present a theory and applications of discrete exterior calculus on simplicial complexes of arbitrary finite dimension. This can be thought of as calculus on a discrete space. Our theory includes not only discrete differential forms but also discrete vector fields and the operators acting on those objects. This allows us to address the various interactions between forms and vector fields (such as Lie derivatives) which are important in applications. Previous attempts at discrete exterior calculus have addressed only differential forms. We also introduce the notion of a circumcentric dual of a simplicial complex. The importance of dual complexes in this field has been well understood, but previous researchers have used barycentric subdivision or barycentric duals. We show that the use of circumcentric duals is crucial in arriving at a theory of discrete exterior calculus that admits both vector fields and forms.

CONTENTS

1. Introduction 1
2. History and Previous Work 4
3. Primal Simplicial Complex and Dual Cell Complex 4
4. Local and Global Embeddings 10
5. Differential Forms and Exterior Derivative 12
6. Hodge Star and Codifferential 14
7. Maps between 1-Forms and Vector Fields 15
8. Wedge Product 17
9. Divergence and Laplace–Beltrami 22
10. Contraction and Lie Derivative 24
11. Discrete Poincaré Lemma 27
12. Discrete Variational Mechanics and DEC 38
13. Extensions to Dynamic Problems 44
13.1. Groupoid Interpretation of Discrete Variational Mechanics 44
13.2. Discrete Diffeomorphisms and Discrete Flows 46
13.3. Push-Forward and Pull-Back of Discrete Vector Fields and Discrete Forms 48
14. Remeshing Cochains and Multigrid Extensions 49
15. Conclusions and Future Work 50
References 51

1. INTRODUCTION

This work presents a theory of ***discrete exterior calculus*** (DEC) motivated by potential applications in computational methods for field theories such as elasticity, fluids, and electromagnetism. In addition, it provides much needed mathematical machinery to enable a systematic development of numerical schemes that mirror the approach of geometric mechanics.

arXiv:cond-mat/0510774v2 [cond-mat.stat-mech] 17 Nov 2005

Quantum dynamics in strong fluctuating fields

Igor Goychuk* and Peter Hänggi,
Universität Augsburg, Institut für Physik, Universitätsstr. 1,
D-86135 Augsburg, Germany

February 2, 2008

Abstract

A large number of multifaceted quantum transport processes in molecular systems and physical nanosystems, such as e.g. nonadiabatic electron transfer in proteins, can be treated in terms of quantum relaxation processes which couple to one or several fluctuating environments. A thermal equilibrium environment can conveniently be modelled by a thermal bath of harmonic oscillators. An archetype situation provides a two-state dissipative quantum dynamics, commonly known under the label of a spin-boson dynamics. An interesting and nontrivial physical situation emerges, however, when the quantum dynamics evolves far away from thermal equilibrium. This occurs, for example, when a charge transferring medium possesses nonequilibrium degrees of freedom, or when a strong time-dependent control field is applied externally. Accordingly, certain parameters of underlying quantum subsystem acquire stochastic character. This may occur for example for the tunnelling coupling between the donor and acceptor states of transferring electron, or for the corresponding energy difference between electronic states which assume via the coupling to the fluctuating environment an explicit stochastic or deterministic time-dependence. Herein, we review the general theoretical framework which is based on the method of projector operators, yielding the quantum master equations for systems that are exposed to strong external fields. This allows one to investigate on a common basis the influence of nonequilibrium fluctuations and periodic electrical fields on those already mentioned dynamics and related quantum transport processes. Most importantly, such strong fluctuating fields induce a whole variety of nonlinear and nonequilibrium phenomena. A characteristic feature of such dynamics is the absence of thermal (quantum) detailed balance.

*Corresponding author, e-mail: goychuk@physik.uni-augsburg.de

arXiv:physics/0511138v1 [physics.class-ph] 16 Nov 2005

Dynamics with Low-Level Fractionality

Vasily E. Tarasov[1,2] and George M. Zaslavsky[1,3]

1) *Courant Institute of Mathematical Sciences, New York University*
251 Mercer Street, New York, NY 10012, USA
2) *Skobeltsyn Institute of Nuclear Physics,*
Moscow State University, Moscow 119992, Russia
3) *Department of Physics, New York University,*
2-4 Washington Place, New York, NY 10003, USA

Abstract

The notion of fractional dynamics is related to equations of motion with one or a few terms with derivatives of a fractional order. This type of equation appears in the description of chaotic dynamics, wave propagation in fractal media, and field theory. For the fractional linear oscillator the physical meaning of the derivative of order $\alpha < 2$ is dissipation. In systems with many spacially coupled elements (oscillators) the fractional derivative, along the space coordinate, corresponds to a long range interaction. We discuss a method of constructing a solution using an expansion in $\varepsilon = n - \alpha$ with small ε and positive integer n. The method is applied to the fractional linear and nonlinear oscillators and to fractional Ginzburg-Landau or parabolic equations.

PACS: 45.10.Hj; 45.05.+x; 45.50.-j

Keywords: Fractional equations, Fractional oscillator, Ginzburg-Landau equation

1 Introduction

It became clear in the last decade that many physical processes can be adequately described by equations that consist of derivatives of fractional order. In a fairly short period of time,

arXiv:hep-th/0512351v4 28 Feb 2006

hep-th/0512351 v4

Hawking radiation as tunneling from the Kerr and Kerr-Newman black holes

Qing-Quan Jiang *
College of Physical Science and Technology, Central China Normal University, Wuhan, Hubei 430079, People's Republic of China and Institute of Theoretical Physics, China West Normal University, Nanchong, Sichuan 637002, People's Republic of China

Shuang-Qing Wu †
College of Physical Science and Technology, Central China Normal University, Wuhan, Hubei 430079, People's Republic of China

Xu Cai ‡
Institute of Particle Physics, Central China Normal University, Wuhan, Hubei 430079, People's Republic of China

(Revised February 1, 2008)

Recent work, which treats the Hawking radiation as a semi-classical tunneling process at the horizon of the Schwarzschild and Reissner-Nordström spacetimes, indicates that the exact radiant spectrum is no longer pure thermal after considering the black hole background as dynamical and the conservation of energy. In this paper, we extend the method to investigate Hawking radiation as massless particles tunneling across the event horizon of the Kerr black hole and that of charged particles from the Kerr-Newman black hole by taking into account the energy conservation, the angular momentum conservation, and the electric charge conservation. Our results show that when self-gravitation is considered, the tunneling rate is related to the change of Bekenstein-Hawking entropy and the derived emission spectrum deviates from the pure thermal spectrum, but is consistent with an underlying unitary theory.

PACS numbers: 04.70.Dy, 04.62.+v, 03.65.Sq

I. INTRODUCTION

The "no hair" theorem stated that all information about the collapsing body was lost from the outside region apart from three conserved quantities: the mass, the angular momentum, and the electric charge. In other words, this implied that the only stationary rotating black hole solutions of the Einstein-Maxwell equations in four dimensions are the Kerr-Newman metrics. In the classical theory, the loss of information was not a serious problem since the information could be thought of as preserved inside the black hole but just not very accessible. However, taking the quantum effect into consideration, the situation is changed. With the emission of thermal radiation [1], black holes could lose energy, shrink, and eventually evaporate away completely. Since the radiation with a precise thermal spectrum carries no information, the information carried by a physical system falling toward black hole singularity has no way to be recovered after a black hole has disappeared completely. This is the so-called "information loss paradox" [2], which means that pure quantum states (the original matter that forms the black hole) can evolve into mixed states (the thermal spectrum at infinity). Such an evolution violates the fundamental principles of quantum theory, as these prescribe a unitary time evolution of basis states. While the information paradox can perhaps be attributed to the semi-classical nature of the investigations of Hawking radiation, researches in string theory indeed support the idea that Hawking radiation can be described within a manifestly unitary theory, however, it still remains a mystery how information is recovered. Although a complete resolution of the information loss paradox might be within a unitary theory of quantum gravity or string/M-theory, it is argued that the information could come out if the outgoing radiation were not exactly thermal but had subtle corrections [2].

On the other hand, the mechanism of black hole radiance remains shrouded in some degree of mystery. In the original derivation of black hole evaporation, Hawking described the thermal radiation as a quantum tunneling process [3] triggered by vacuum fluctuations near the event horizon. According to this scenario, a pair of particles is spontaneously created just inside the horizon, the positive energy particle then tunnels out to the infinity, and the negative energy "partner" remains behind and effectively lowers the mass of the black hole. This tunneling picture can be depicted in another manner, that is, a particle/anti-particle pair is created just outside the horizon, the negative energy particle tunnels into the horizon because the negative energy orbit exists only inside the horizon, the positive energy "partner" is left outside and emerges at infinity.

In fact, the above viewpoint that regards the radiation

*E-mail address: jiangqingquan@126.com
†E-mail address: sqwu@phy.ccnu.edu.cn (Corresponding author)
‡E-mail address: xcai@mail.ccnu.edu.cn

arXiv:math/0603097v2 [math.GT] 25 Jul 2007

A VARIATIONAL PRINCIPLE FOR WEIGHTED DELAUNAY TRIANGULATIONS AND HYPERIDEAL POLYHEDRA

BORIS A. SPRINGBORN

Abstract. We use a variational principle to prove an existence and uniqueness theorem for planar weighted Delaunay triangulations (with non-intersecting site-circles) with prescribed combinatorial type and circle intersection angles. Such weighted Delaunay triangulations may be interpreted as images of hyperbolic polyhedra with one vertex on and the remaining vertices beyond the infinite boundary of hyperbolic space. Thus the main theorem states necessary and sufficient conditions for the existence and uniqueness of such polyhedra with prescribed combinatorial type and dihedral angles. More generally, we consider weighted Delaunay triangulations in piecewise flat surfaces, allowing cone singularities with prescribed cone angles in the vertices. The material presented here extends work by Rivin on Delaunay triangulations and ideal polyhedra.

1. Introduction

1.1. **Overview.** Rivin developed a variational method to prove the existence and uniqueness of ideal hyperbolic polyhedra with prescribed combinatorial type and dihedral angles, or equivalently, of planar Delaunay triangulations with prescribed combinatorial type and circumcircle intersection angles [28]. The purpose of this article is to extend this method to hyperideal polyhedra and to weighted Delaunay triangulations. Consider a finite set of disjoint circular disks in the plane. For every triple of such disks there exists a circle that intersects the boundaries of the disks orthogonally. The weighted Delaunay triangulation induced by the disks consists of the triangles whose vertices are the centers of a triple of disks such that the orthogonal circle of this triple intersects no other disk more than orthogonally (see Figure 2). Such weighted Delaunay triangulations correspond to hyperbolic polyhedra with one vertex on the infinite boundary and all other vertices outside. The dihedral angles correspond to the intersection angles of the orthogonal circles. More generally, we allow cone singularities at the centers of the disks, and we call such weighted Delaunay triangulation with cone singularities euclidean hyperideal circle patterns. The question we consider is: Given an abstract triangulation T with vertex set V, edge set E, and face set $\mathcal{T}$, and given intersection angles θ as a function on the edges and cone angles Ξ as a function on the vertices, does there exist a corresponding euclidean hyperideal circle pattern, and is it unique? The main result is the following.

Theorem 1. *A euclidean hyperideal circle pattern with triangulation T, intersection angles $\theta : E \to [0, \pi)$ and cone/boundary angles $\Xi : V \to (0, \infty)$ exists if and only if the set of coherent angle systems $\mathcal{A}(T, \theta, \Xi)$ is not empty. In this case, the circle pattern is unique up to scale.*

Section 2 contains the basic definitions and a precise statement of the "circle pattern problem" under consideration. The set of coherent angle systems $\mathcal{A}(T, \theta, \Xi)$

2000 *Mathematics Subject Classification.* Primary 51M20; Secondary 52C26, 57M50.
Supported by the DFG Research Center MATHEON in Berlin.

EPJ manuscript No.
(will be inserted by the editor)

A fundamental threat to quantum cryptography: gravitational attacks

R. Plaga[1a]

Federal Office for Information Security (BSI), 53175 Bonn, Germany

Received: date / Revised version: date

Abstract. An attack on the "Bennett-Brassard 84"(BB84) quantum key-exchange protocol in which Eve exploits the action of gravitation to infer information about the quantum-mechanical state of the qubit exchanged between Alice and Bob, is described. It is demonstrated that the known laws of physics do not allow to describe the attack. Without making assumptions that are not based on broad consensus, the laws of quantum gravity, unknown up to now, would be needed even for an approximate treatment. Therefore, it is currently not possible to predict with any confidence if information gained in this attack will allow to break BB84. Contrary to previous belief, a proof of the perfect security of BB84 cannot be based on the assumption that the known laws of physics are strictly correct, yet.
A speculative parameterization that characterizes the time-evolution operator of quantum gravity for the gravitational attack is presented. It allows to evaluate the results of gravitational attacks on BB84 quantitatively. It is proposed to perform state-of-the-art gravitational attacks, both for a complete security assurance of BB84 and as an unconventional search for experimental effects of quantum gravity.

PACS. 03.67.Dd Quantum cryptography – 04.80.-n Quantum gravity – 03.65.Ta Foundations of quantum mechanics, measurement theory

arXiv:quant-ph/0603234v1 26 Mar 2006

1 Introduction

Quantum key-distribution (QKD) protocols, often collectively called "quantum cryptography", exploit the principles of quantum mechanics to enable the secure distribution of information[1]. It is a common belief that the perfect secrecy of keys exchanged by such protocols is guaranteed if the "known laws of physics"[1] are assumed to be strictly correct[2,3]. This would be a major advantage of quantum cryptography because an analogous security guarantee for classical cryptography - based on the correctness of proven, or at least highly plausible, mathematical theorems[2] - is not possible, yet[4].
Section 2 presents a novel attack procedure against the first and best known QKD protocol, the "Bennett-Brassard 84" (BB84) protocol[1], in which the attacker exploits the action of gravity. I demonstrate in section 3 that this attack cannot be modelled - not even to any approximation - on the basis of the known laws of physics without making assumptions that are not based on broad consensus.
Even though its security proof is shown to be incomplete, BB84 retains its great value because it rests on completely different foundations than its classical counterparts. However, for a complete security assurance one needs to attack the protocol experimentally. In section 4 I propose a framework in which the results of gravitational attacks on BB84 can be evaluated quantitatively. In this framework Eve breaks BB84 via gravitationally cloning a qubit, section 5 studies if this indirectly violates special relativity. Section 6 concludes.

2 The "gravitational-attack" protocol

In the BB84 protocol the honest party ("Alice") encodes a bit of the key to be distributed by preparing a qubit "Q" either in one of the four quantum-mechanical states $|\Psi> = |0>$, $|\Psi> = |1>$, $|\Psi> = |+> = \frac{1}{\sqrt{2}}(|0> + |1>)$ or $|\Psi> = |-> = \frac{1}{\sqrt{2}}(|0> - |1>)$. She then sends Q to its designated receiver ("Bob"). Rigorous proofs of the security of BB84[5,6] are based on the assumption that the laws of quantum physics are correct. However, these proofs ignore gravitation. Implicitly they assume that attackers only employ the resources of quantum physics in flat space time. However, it seems overly optimistic to "require" eavesdroppers to avoid the profound difficulties that still beset any attempt to definitely answer the question: "What gravitational field corresponds to a given quantum state?"

[a] *E-mail:* rainer.plaga@bsi.bund.de

[1] Defined here as an expression that was derived from a consistent mathematical framework (a "theory of physics") and has been confirmed by repeated scientific experiments.

[2] The analogues to laws of physics.

arXiv:hep-th/0605162v2 22 May 2006

hep-th/0605162

Opening Mirror Symmetry on the Quintic

Johannes Walcher

School of Natural Sciences, Institute for Advanced Study
Princeton, New Jersey, USA

Abstract

Aided by mirror symmetry, we determine the number of holomorphic disks ending on the real Lagrangian in the quintic threefold. The tension of the domainwall between the two vacua on the brane, which is the generating function for the open Gromov-Witten invariants, satisfies a certain extension of the Picard-Fuchs differential equation governing periods of the mirror quintic. We verify consistency of the monodromies under analytic continuation of the superpotential over the entire moduli space. We reproduce the first few instanton numbers by a localization computation directly in the A-model, and check Ooguri-Vafa integrality. This is the first exact result on open string mirror symmetry for a compact Calabi-Yau manifold.

May 2006

How to Introduce Time Operator

Zhi-Yong Wang*, Cai-Dong Xiong

School of Physical Electronics, University of Electronic Science and Technology of China, Chengdu 610054

Abstract

Time operator can be introduced by three different approaches: by pertaining it to dynamical variables; by quantizing the classical expression of time; taken as the restriction of energy shift generator to the Hilbert space of a physical system.

PACS: 03.65.Ca; 03.65.Ta; 03.65.Xp

Keywords: time operator; self-adjointness; energy shift; time-energy uncertainty

1. Introduction

Traditionally, time enters quantum mechanics as a parameter rather than a dynamical operator. As a consequence, the investigations on tunneling time, arrival time and traversal time, etc., still remain controversial today [1-19]. On the one hand, one imposes self-adjointness as a requirement for any observable; on the other hand, according to Pauli's argument [20-23], there is no self-adjoint time operator canonically conjugating to a Hamiltonian if the Hamiltonian spectrum is bounded from below. A way out of this dilemma set by Pauli's objection is based on the use of positive operator valued measures (POVMs) [19, 22-26]: quantum observables are generally positive operator valued measures, e.g., quantum observables are extended to maximally symmetric but not necessarily self-adjoint operators, in such a way one preserves the requirement that time operator be conjugate to the Hamiltonian but abandons the self-adjointness of time operator.

In this paper, general time operators are constructed by three different approaches. In the following, the natural units of measurement ($\hbar = c = 1$) is applied.

* *E-mail address*: zywang@uestc.edu.cn

DENSITIES OF STATES, MOMENTS, AND MAXIMALLY BROKEN TIME-REVERSAL SYMMETRY

Roger Haydock and C. M. M. Nex,

Department of Physics and Materials Science Institute,

1274 University of Oregon, OR 97403-1274, USA.

Power moments, modified moments, and optimized moments are powerful tools for solving microscopic models of macroscopic systems; however the expansion of the density of states as a continued fraction does not converge to the macroscopic limit point-wise in energy with increasing numbers of moments. In this work the moment problem is further constrained by minimal lifetimes or maximal breaking of time-reversal symmetry, to yield approximate densities of states with point-wise macroscopic limits. This is applied numerically to models with one and two finite bands with various singularities, as well as to a model with infinite band-width, and the results are compared with the maximum entropy approximation where possible.

PACS number(s): 71.15.-m, 02.60.-x, 71.15.Dx

arXiv:0705.0901v2 [math.GM] 10 May 2007

HOW TO RELEASE FREGE'S SYSTEM FROM RUSSELL'S ANTINOMY

PAOLA CATTABRIGA

ABSTRACT. The conditions for proper definitions in mathematics are given, in terms of the theory of definition, on the basis of the criterions of eliminability and non-creativity. As a definition, Russell's antinomy is a violation of the criterion of eliminability (Behmann, 1931, [1]; Beeboer, 1943, [2]). Following the path of the criterion of non-creativity, this paper develops a new analysis of Comprehension schema and, as a consequence, proof that Russell's antinomy argumentation, despite the words of Frege himself, does not hold in Grundgesetze der Arithmetik. According to Basic Law (III), the class of classes not belonging to themselves is a class defined by a function which can not take as argument its own course of value,

$$\neg\Big(\forall = \varepsilon\big(\forall^{1}\neg\big(\varepsilon(\varepsilon) \longrightarrow \varepsilon \;\rightarrow\; \varphi(\varepsilon)\big)\big)\Big),$$

in other words, the class of classes not belonging to themselves is a class whose classes are not identical to the class itself [6].

INTRODUCTION

Recently, a considerable attention has been devoted to the discovery of new ways for repairing Frege's system from the damage produced by Russell's antinomy. All these attempts share a common aptitude in finding new restrictive forms or applications of the comprehension principle [4, 16, 20, 22, 23], either offer a revised interpretation of Basic Law (V) [3].

The present note proposes a completely new way to restore Frege's system, neither restrictive nor revising, rising from the logical inquiry in the theory of definition and the author's investigations in self-reference procedures [7, 9]. Partially in agreement with their constructive attitude, the result we are concerned with draws its first inspiration from Jules-Henri Poincaré's writings about the significance and riskiness of impredicative definitions in mathematics.

> *The fact is that such a procedure is* not *applicable. Why? Because their definitions are* not *predicative and contain within such a vicious circle I already mentioned above; not predicative definitions* can not be substituted to defined terms. *In this condition, logistics is* no *longer sterile: it generates contradictions.* (1902, [21], 211, our translation)

With these words Poincaré was directly referring to Cantor's famous diagonalization argument for reaching more-than-denumerable sets, criticizing the underlying belief of the existence of the actual infinite. Russell's antinomy and Cantor's diagonalization are both self-referring procedures, and by admission of Russell himself his discovery is due to his reflections about Cantor's argument.

Maxwell Equations with Accounting of Tensor Properties of Time

Vlokh R. and Kvasnyuk O.

Institute of Physical Optics, 23 Dragomanov St., 79005 Lviv, Ukraine, e-mail: vlokh@ifo.lviv.ua

Received: 21.05.2007

Abstract

The Maxwell equations with accounting for tensors properties of time have been considered. The effects that follow from such consideration are described. These are the appearance of vacuum polarization, anisotropy of electromagnetic wave velocity in vacuum, anisotropy of the vacuum dielectric permittivity, rotation of light polarization plane, as well as the existence of longitudinal components of electromagnetic wave and the rotational (non-potential) component of electric field caused by electric charges.

Key words: Maxwell equations, time, speed of light, physical vacuum

PACS: 03.50.De, 42.25.Bs, 95.30.Sf

Introduction

One of the commonly used notations of Maxwell equations for vacuum is as follows (see, e.g., [1]):

$$\begin{cases} \varepsilon_0 \dfrac{\partial E}{\partial t} = rot H \\ -\mu_0 \dfrac{\partial H}{\partial t} = rot E \\ div E = 0 \\ div H = 0 \end{cases}, \qquad (1)$$

where E and H are respectively polar and axial vectors of electric and magnetic fields, t is time represented by scalar quantity and ε_0 and μ_0 stand respectively for electric permittivity and magnetic permeability of vacuum. The first two relations in Eq. (1) are known as the Faraday's and Ampere's laws, respectively, while the last two as the Coulomb's and Gauss's laws. In order to describe electromagnetic wave propagation in material media with certain electric and magnetic properties, the relations (1) are supplemented with the constitutive relations

LPTENS-08/05
January 2008

Lectures on Anomalies*

Adel Bilal

Laboratoire de Physique Théorique, École Normale Supérieure - CNRS UMR8549†
24 rue Lhomond, 75231 Paris Cedex 05, France

arXiv:0802.0634v1 [hep-th] 5 Feb 2008

Abstract

These lectures on anomalies are relatively self-contained and intended for graduate students in theoretical high-energy physics who are familiar with the basics of quantum field theory. More elaborate concepts are introduced when needed.
We begin with several derivations of the abelian anomaly: anomalous transformation of the measure, explicit computation of the triangle Feynman diagram, relation to the index of the Euclidean Dirac operator. The chiral (non-abelian) gauge anomaly is derived by evaluating the anomalous triangle diagram with three non-abelian gauge fields coupled to a chiral fermion. We discuss in detail the relation between anomaly, current non-conservation and non-invariance of the effective action, with special emphasis on the derivation of the anomalous Slavnov-Taylor/Ward identities. We show why anomalies always are finite and local. A general characterization is given of gauge groups and fermion representations which may lead to anomalies in four dimensions, and the issue of anomaly cancellation is discussed, in particular the classical example of the standard model.
Then, in a second part, we move to more formal developments and arbitrary even dimensions. After introducing a few basic notions of differential geometry, in particular the gauge bundle and characteristic classes, we derive the descent equations. We prove the Wess-Zumino consistency condition and show that relevant anomalies correspond to BRST cohomologies at ghost number one. We discuss why and how anomalies are related via the descent equations to characteristic classes in two more dimensions. The computation of the anomalies in terms of the index of an appropriate Dirac operator in these higher dimensions is outlined. Finally we derive the gauge and gravitational anomalies in arbitrary even dimensions from the appropriate index and explain the anomaly cancellations in ten-dimensional IIB supergravity and in the field theory limits of type I and heterotic superstrings.

*Based on lectures given at the joint Amsterdam-Brussels-Paris graduate school in theoretical high-energy physics
†Unité mixte du CNRS et de l'École Normale Supérieure associée à l'UPMC Univ Paris 06 (Pierre et Marie Curie)

arXiv:0802.2728v1 [quant-ph] 19 Feb 2008

Zitterbewegung in Quantum Mechanics – a research program

David Hestenes
*Department of Physics, Arizona State University, Tempe, Arizona 85287-1504**

Spacetime Algebra (STA) provides unified, matrix-free spinor methods for rotational dynamics in classical theory as well as quantum mechanics. That makes it an ideal tool for studying particle models of *zitterbewegung* and using them to study zitterbewegung in the Dirac theory. This paper develops a self-contained dynamical model of the electron as a lightlike particle with helical zitterbewegung and electromagnetic interactions. It attributes to the electron an electric dipole moment oscillating with ultrahigh frequency, and the possibility of observing this directly as a resonance in electron channeling is analyzed in detail. A modification of the Dirac equation is suggested to incorporate the oscillating dipole moment. That enables extension of the Dirac equation to incorporate electroweak interactions in a new way.

Keywords: zitterbewegung, geometric algebra, electron channeling, de Broglie frequency

I. INTRODUCTION

This paper continues a research program investigating implications of the *Real Dirac Equation* for the interpretation and extension of quantum mechanics. Details of the program have been reviewed elsewhere [1–3], so it suffices here to state the main ideas and conclusions to set the stage for the present study.

The program began with a reformulation of the Dirac equation in terms of *Spacetime Algebra* (Section II), which revealed geometric structure that is suppressed in the standard matrix version. In particular, it revealed that the generator of phase and electromagnetic gauge transformations is a spacelike bivector specified by electron spin. In other words, spin and phase are inseparably related — spin is not simply an add-on, but an essential feature of quantum mechanics. However, physical implications of this fact depend critically on relations of the Dirac wave function to physical observables, which are not specified by the Dirac equation itself. That started the present research program to investigate various possibilities.

A standard observable in Dirac theory is the Dirac current, which doubles as a probability current and a charge current. However, this does not account for the magnetic moment of the electron, which many investigators conjecture is due to a circulation of charge. But what is the nature of this circulation? After a lengthy analysis of the Dirac equation Bohm and Hiley conclude [4]: "the electron must still be regarded as a simple point particle whose only intrinsic property is its position." Under this assumption, spin and phase must be kinematical features of electron motion. The charge circulation that generates the magnetic moment can then be identified with the *zitterbewegung* of Schroedinger [5].

This raises the central question of the present research: Is the zitterbewegung, so construed, a real physical phenomenon, or is it merely a colorful metaphor? Although this question was motivated by structural features of the Dirac equation, it cannot be answered without attributing substructure to electron motion that is not specified by standard Dirac theory.

The main purpose of this paper is to formulate and study a well-defined particle model of the electron with *spin and zitterbewegung dynamics* motivated by the Dirac equation. Since the term *zitterbewegung* is quite a mouthful, I often abbreviate it to *zitter*, especially when it is used as an adjective.

We study the structure of the *zitter model* in considerable detail with the aim of identifying new experimental implications. The main conclusion is that the electron is the seat of a rapidly rotating electric dipole moment fluctuating with the zitter frequency of Schroedinger. As this frequency is so rapid, it is observable only under resonance conditions. It is argued that many familiar quantum mechanical effects may be attributable to zitter resonance. Moreover, the new possibility of observing zitter directly as a resonance in electron channeling is analyzed in detail, because the prospects of crucial experimental tests are very promising.

The relation of the zitter particle model to the Dirac equation is also studied. The main conclusion is that, though zitter oscillations are inherent in the Dirac equation, they will not be manifested as an oscillating electric dipole without altering the definition of charge current. A simple modification of the Dirac equation to incorporate the altered definition is proposed. Remarkably, that opens the door for incorporating electroweak interactions into the Dirac equation in a novel way.

In conclusion, the relation of the zitter particle model to the Dirac equation can be considered from two different perspectives. On the one hand, it can be regarded as a "quasiclassical" approximation that embodies structural features of the Dirac equation in a convenient form for analysis. On the other hand, it can be regarded as formulating fundamental properties of the electron that are manifested in the Dirac equation in some kind of average form. The choice of perspective is left to the reader.

*Electronic address: hestenes@asu.edu; URL: http://modelingnts.la.asu.edu/

arXiv:0803.0119v1 [math.GM] 2 Mar 2008

Glimpses of the Octonions and Quaternions History and Today's Applications in Quantum Physics (*)

A.Krzysztof Kwaśniewski
the Dissident
- relegated by Białystok University authorities
from the Institute of Computer Sciences
organized by the author
to Faculty of Physics
ul. Lipowa 41, 15 424 Białystok, Poland
e-mail: kwandr@gmail.com, http://ii.uwb.edu.pl/akk/publ1.htm

March 3, 2008

Abstract

Before we dive into the accessibility stream of nowadays indicatory applications of octonions to computer and other sciences and to quantum physics let us focus for a while on the crucially relevant events for today's revival on interest to nonassociativity. Our reflections keep wandering back to the Brahmagupta-Fibonacci Two-Square Identity and then via the Euler Four-Square Identity up to the Degen-Graves-Cayley Eight-Square Identity. These glimpses of history incline and invite us to re-tell the story on how about one month after quaternions have been carved on the Brougham bridge octonions were discovered by John Thomas Graves (1806-1870), jurist and mathematician - a friend of William Rowan Hamilton (1805-1865). As for today we just mention en passant quaternionic and octonionic quantum mechanics, generalization of Cauchy-Riemann equations for octonions and Triality Principle and G_2 group in spinor language in a descriptive way in

bioRxiv preprint first posted online Oct. 13, 2016; doi: http://dx.doi.org/10.1101/080697. The copyright holder for this preprint (which was not peer-reviewed) is the author/funder. All rights reserved. No reuse allowed without permission.

Liberation from equations: An equation-free method reveals the ecological interaction networks within complex microbial ecosystems

*Kenta Suzuki[1], Katsuhiko Yoshida[1], Yumiko Nakanishi[2,3] and Shinji Fukuda[2,4]

[1]Biodiversity Conservation Planning Section, Center for Environmental Biology and Ecosystem Studies, National Institute for Environmental Studies, 16-2 Onogawa, Tsukuba, Ibaraki, 305-8506 Japan.
[2]Institute for Advanced Biosciences, Keio University, 246-2 Mizukami, Kakuganji, Tsuruoka, Yamagata 997-0052, Japan
[3]RIKEN Center for Integrative Medical Sciences, 1-7-22 Suehiro-cho, Tsurumi-ku, Yokohama, Kanagawa 230-0045, Japan
[4]PREST, Japan Science and Technology Agency, 4-1-8 Honcho Kawaguchi, Saitama 332-0012, Japan

*Corresponding author: Kenta Suzuki
Tel.: +81-029-850-2747
E-mail: suzuki.kenta@nies.go.jp

Abstract

Mapping the network of ecological interactions is key to understanding the composition, stability, function and dynamics of microbial communities. These ecosystem properties provide the mechanistic basis for understanding and designing microbial treatments that attempt to promote human health and provide environmental services. In recent years various approaches have been used to reveal microbial interaction networks, inferred from metagenomic sequencing data using time-series analysis, machine learning and statistical techniques. Despite these efforts it is still not possible to capture details of the ecological interactions behind complex microbial dynamics. Here, we develop the sparse S-map method (SSM), which generates a sparse interaction network from a multivariate ecological time-series without presuming any mathematical formulation for the underlying microbial processes. We show that this method outperforms a comparative equation-based method and that the results were robust to the range of observational errors and quantity of data that we tested. We then applied the method to the microbiome data of six mice and found that the mice had similar interaction networks when they were middle- to old-aged (36-72 week-old), characterized by the high connectivity of an unclassified Clostridiales. However, there was almost no shared network patterns when they were young- to middle-aged (4-36 week-old). The results shed light on the universality of microbial interactions during the lifelong dynamics of mouse gut-microbiota. The complexity of microbial relationships impede detailed equation-based modeling, and our method provides a powerful alternative framework to infer ecological interaction networks of microbial communities in various environments.

NEGATIVE ENERGIES AND FIELD THEORY

Gerald E. Marsh
Argonne National Laboratory (Ret)
5433 East View Park
Chicago, IL 60615

E-mail: gemarsh@uchicago.edu

Abstract: The assumption that the vacuum is the minimum energy state, invariant under unitary transformations, is fundamental to quantum field theory. However, the assertion that the conservation of charge implies that the equal time commutator of the charge density and its time derivative vanish for two spatially separated points is inconsistent with the requirement that the vacuum be the lowest energy state. Yet, for quantum field theory to be gauge invariant, this commutator *must* vanish. This essay explores how this conundrum is resolved in quantum electrodynamics.

PACS: 03.65-w, 11.10-z.
Key words: Negative Energy, Field Theory.

arXiv:0810.1543v1 [math-ph] 8 Oct 2008

On the nonlocality of the fractional Schrödinger equation

M. Jeng[1*], S.-L.-Y. Xu[1†], E. Hawkins[2‡] and J. M. Schwarz[1§]
[1] *Physics Department, Syracuse University, Syracuse, NY, 13244, USA* [2] *Department of Mathematics, University of York, UK*

A number of papers over the past eight years have claimed to solve the fractional Schrödinger equation for systems ranging from the one-dimensional infinite square well to the Coulomb potential to one-dimensional scattering with a rectangular barrier. However, some of the claimed solutions ignore the fact that the fractional diffusion operator is inherently nonlocal, preventing the fractional Schrödinger equation from being solved in the usual piecewise fashion. We focus on the one-dimensional infinite square well and show that the purported groundstate, which is based on a piecewise approach, is definitely not a solution of the fractional Schrödinger equation for general fractional parameters α. On a more positive note, we present a solution to the fractional Schrödinger equation for the one-dimensional harmonic oscillator with $\alpha = 1$.

I. INTRODUCTION

A wide variety of stochastic processes are more general than the familiar Brownian motion, but presumably can still be described by modifying the diffusion equation using a fractional Laplacian operator [1, 2]. Such "fractional diffusion" is now a large and active field, and a number of books have been written on the mathematics and physics of fractional diffusion operators [3, 4, 5]. In 2000, Laskin introduced the fractional Schrödinger equation, in which the normal Schrödinger equation is modified in analogy with fractional diffusion [6, 7, 8]. Laskin claimed to exactly solve this equation in the case of the one-dimensional infinite square well [6]. A more recent (2006) work claimed to find solutions again for the infinite one-dimensional square well (agreeing with Laskin's original solution), and for one-dimensional scattering off of a barrier potential [9]. A 2007 work used a different method of analysis to claim solutions for the linear, delta function, and Coulomb potentials in one dimension [10]. Laskin also recently built on the same claimed solution to derive properties of the quantum kernel [11]. The purpose of this work is to point out that of the many purported exact solutions presented in the literature, only the one for the delta function potential is correct.

The one-dimensional fractional Schrödinger equation [6] is

$$i\hbar\frac{\partial\psi(x,t)}{\partial t} = D_\alpha\left(-\hbar^2\triangle\right)^{\alpha/2}\psi(x,t) + V(x,t)\,\psi(x,t), \tag{1}$$

where D_α is a constant, $\Delta \equiv \partial^2/\partial x^2$ is the Laplacian, and $\left(-\hbar^2\triangle\right)^{\alpha/2}$ is the quantum Riesz fractional derivative:

$$\left(-\hbar^2\triangle\right)^{\alpha/2}\psi(x,t) \equiv \frac{1}{2\pi\hbar}\int_{-\infty}^{+\infty} dp\; e^{ipx/\hbar}\,|p|^\alpha\,\phi(p,t). \tag{2}$$

Here, $\phi(p,t)$ is the Fourier transform of the wavefunction,

$$\phi(p,t) = \int_{-\infty}^{+\infty} dx\;\psi(x,t)e^{-ipx/\hbar}. \tag{3}$$

When $\alpha = 2$, the quantum Riesz fractional derivative becomes equivalent to an ordinary Laplacian, and we recover the ordinary Schrödinger equation.

We focus on the case where the potential is independent of time, so we are interested in solutions of the following equation:

$$D_\alpha\left(-\hbar^2\triangle\right)^{\alpha/2}\psi(x) + V(x)\,\psi(x) = E\psi(x). \tag{4}$$

* mjeng@physics.syr.edu
† xuxu01@physics.syr.edu
‡ enrmacon@mac.com
§ jschwarz@physics.syr.edu

arXiv:0810.5317v2 [quant-ph] 30 Nov 2009

Can quantum mechanics help distributed computing?

Anne Broadbent Alain Tapp

Abstract

We present a brief survey of results where quantum information processing is useful to solve distributed computation tasks. We describe problems that are impossible to solve using classical resources but that become feasible with the help of quantum mechanics. We also give examples where the use of quantum information significantly reduces the need for communication. The main focus of the survey is on communication complexity but we also address other distributed tasks.

Keywords: pseudo-telepathy, communication complexity, quantum games, simulation of entanglement

Quantum computation and entanglement

This survey is aimed at researchers having very limited knowledge of quantum computation, but that have a basic understanding of complexity from the theoretical computer science perspective. We address the topics of communication complexity and pseudo-telepathy, as well as other problems of interest in the field of distributed computation. The goal of this survey is not to be exhaustive but rather to cover many different aspects and give the highlights and intuition into the power of distributed quantum computation. Other relevant surveys are available [53, 15, 21, 17].

In classical computation, the basic unit of information is the bit. In quantum computation, which is based on quantum mechanics, the basic unit of information is the *qubit*. A string of bits can be described by a string of zeroes and ones; quantum information can also be in a classical state represented by a binary string, but in general it can be in *superposition* of all possible strings with different *amplitudes*. Amplitudes are complex numbers and thus the complete description of a string of n qubits requires 2^n complex numbers. The fact that quantum information uses a continuous notation does not mean that qubits are somewhat equivalent to analog information: although the description of a quantum state is continuous, quantum measurement, the method of extracting classical information from a quantum state, is discrete. Only n bits of information can be extracted from an n-qubit state. Depending of the choice of measurement, different properties of the state can be extracted but the rest is lost forever. Another way to see this is that measurement disturbs a quantum state irreversibly. In quantum algorithms, it is possible to compute a

Localized closed timelike curves can perfectly distinguish quantum states

Todd A. Brun,[1] Jim Harrington,[2] and Mark M. Wilde[1,3]

[1]*Communication Sciences Institute, Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089, USA*
[2]*Applied Modern Physics (P-21), MS D454, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[3]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

(Dated: January 31, 2009)

We show that qubits traveling along closed timelike curves are a resource that a party can exploit to distinguish perfectly any set of quantum states. As a result, an adversary with access to closed timelike curves can break any prepare-and-measure quantum key distribution protocol. Our result also implies that a party with access to closed timelike curves can violate the Holevo bound.

PACS numbers: 03.65.Wj, 03.67.Dd, 03.67.Hk, 04.20.Cv

arXiv:0811.1209v2 [quant-ph] 31 Jan 2009

Introduction—The theory of general relativity points to the possible existence of closed timelike curves (CTCs) [1, 2]. The *grandfather paradox* is one criticism raised to their existence, but Deutsch resolved this paradox by presenting a method for finding self-consistent solutions of CTC interactions [3].

Recently, several quantum information researchers have assumed that CTCs exist and have examined the consequences of this assumption for *computation* [4, 5, 6]. Brun showed that a classical treatment (assuming a lack of contradictions) allows NP-hard problems to be computed with a polynomial number of gates [4]. Bacon followed with a purely quantum treatment that demonstrates the same reduction of NP-hard problems to P, along with a sketch of how to perform this reduction in a fault-tolerant manner [5]. Aaronson and Watrous have recently established that either classical or quantum computers interacting with closed timelike curves can compute any function in PSPACE in polynomial time [6].

In this Letter, we show how a party with access to CTCs, or a "CTC-assisted" party, can perfectly distinguish among a set of non-orthogonal quantum states. The result has implications for fundamental protocols in quantum *communication* because a simple corollary is that a CTC-assisted party can break any prepare-and-measure quantum key distribution protocol [7, 8, 9]. (The security of such a scheme relies on the information-disturbance tradeoff for identifying quantum states.) Furthermore, the capacity for quantum systems to carry classical information becomes unbounded.

Our work here raises fundamental questions concerning the nature of a physical world in which closed timelike curves exist because it challenges the postulate of quantum mechanics that non-orthogonal states cannot be perfectly distinguished. A full theory of quantum gravity would have to resolve this apparent contradiction between the implication of CTCs and the laws of quantum mechanics. Note that any alternative source of nonlinearity would raise similar questions.

We structure this Letter as follows. First, we give some background on Deutsch's formalism regarding CTCs in quantum information theory [3]. We then show how to distinguish the non-orthogonal states $|0\rangle$ and $|-\rangle$ where $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$ and follow by showing how to distinguish the "BB84" states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ where $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$. Our main theorem then shows that a CTC-assisted party can perfectly distinguish among an arbitrary set of states. We end by discussing how a CTC-assisted party can break Holevo's bound [10].

Background—Qubits traveling around closed timelike curves (CTC qubits) may give rise to highly nonintuitive behavior, but Deutsch showed how to avoid certain paradoxes by imposing a self-consistency condition [3]. This self-consistency condition requires that the input density matrix of a CTC quantum system match its output density matrix following its interaction with another system:

$$\rho_{\text{CTC}} = \text{Tr}_{\text{sys}}\{V\left(|\psi\rangle\langle\psi| \otimes \rho_{\text{CTC}}\right)V^\dagger\}, \tag{1}$$

where $|\psi\rangle$ is the input state of the chronology-respecting system, the matrix ρ_{CTC} is the initial density matrix of the CTC quantum system before the two systems interact, and V is the interaction unitary. The expression on the right hand side of (1) is the partial density matrix of the CTC system after the interaction. The output state of the chronology-respecting system is then

$$\rho_{\text{out}} = \text{Tr}_{\text{CTC}}\{V\left(|\psi\rangle\langle\psi| \otimes \rho_{\text{CTC}}\right)V^\dagger\}. \tag{2}$$

The output state is in general a nonlinear function of the input state $|\psi\rangle$, because ρ_{out} depends on both $|\psi\rangle$ and ρ_{CTC}, and ρ_{CTC} also depends on $|\psi\rangle$. It is this nonlinearity that enables us to transcend the usual limitations of quantum mechanics.

Deutsch showed in Ref. [3] that there always exists a self-consistent solution to Eq. (1), but it does not necessarily have to be unique. In the examples and main theorem of this Letter, we construct an interaction and measurement scheme to distinguish perfectly any set of non-orthogonal states. To achieve this result, we engineer the density matrix of the CTC system to be unique as well as self-consistent.

Distinguishing two non-orthogonal states—We first show how to distinguish the non-orthogonal states $|0\rangle$

Securely Implementing Network Protocols: Detecting and Preventing Logical Flaws

Mathy Vanhoef (KU Leuven)

Black Hat Webcast, 24 August 2017

@vanhoefm

DistriNet

arXiv:0901.4968v3 [math.DS] 30 Jul 2009

Complex Singularities and the Lorenz Attractor

Divakar Viswanath* Sönmez Şahutoğlu†

August 13, 2013

Abstract

The Lorenz attractor is one of the best known examples of applied mathematics. However, much of what is known about it is a result of numerical calculations and not of mathematical analysis. As a step toward mathematical analysis, we allow the time variable in the three dimensional Lorenz system to be complex, hoping that solutions that have resisted analysis on the real line will give up their secrets in the complex plane. Knowledge of singularities being fundamental to any investigation in the complex plane, we build upon earlier work and give a complete and consistent formal development of complex singularities of the Lorenz system using *psi series*. The psi series contain two undetermined constants. In addition, the location of the singularity is undetermined as a consequence of the autonomous nature of the Lorenz system. We prove that the psi series converge, using a technique that is simpler and more powerful than that of Hille, thus implying a two-parameter family of singular solutions of the Lorenz system. We pose three questions, answers to which may bring us closer to understanding the connection of complex singularities to Lorenz dynamics.

Keywords: Lorenz attractor, psi series, complex singularities.
AMS: 34M35, 37D45.

1 Introduction

The nonlinear system of equations

$$\begin{aligned}\frac{dx}{dt} &= 10(y-x)\\ \frac{dy}{dt} &= 28x - y - xz\\ \frac{dz}{dt} &= -8z/3 + xy,\end{aligned} \tag{1.1}$$

which is named after Lorenz, gives the best known example of a strange attractor. Lorenz [21, 22] derived this system to argue that the unpredictability of weather is due to the nature of the solutions of the Navier-Stokes equations and not due to stochastic terms of unknown origin, his point being that a deterministic system could possess an attracting and invariant set on which the dynamics

*Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109. Partly supported by NSF grants DMS-0407710 and DMS-0713510.

†Department of Mathematics, University of Toledo, Toledo, OH 43606. Partly supported by NSF grant DMS-0802191.

arXiv:0902.1305v2 [physics.gen-ph] 22 Aug 2009

Polarizable vacuum analysis of electric and magnetic fields

Xing-Hao Ye*
Department of Applied Physics, Hangzhou Dianzi University, Hangzhou 310018, China
(Dated: August 22, 2009)

The electric and magnetic fields are investigated on the basis of quantum vacuum. The analysis of the electromagnetic energy and force indicates that an electric field is a polarized distribution of the vacuum virtual dipoles, and that a magnetic field in vacuum is a rearrangement of the vacuum polarization. It means that an electromagnetic wave is a successional changing of the vacuum polarization in space. Also, it is found that the average half length of the virtual dipoles around an elementary charge is $a = 2.8 \times 10^{-15}$m. The result leads to the step distribution of the field energy around an electron, the relation between the fine structure constant and the vacuum polarization distribution, and an extremely high energy density of the electromagnetic field.

PACS numbers: 03.50.De, 41.20.Cv, 41.20.Gz

The quantum theory and experiments have approved that vacuum can be polarized. The vacuum polarization can be used to interpret the gravitation [1, 2, 3], which reaches an insightful description of the vacuum around the gravitational matter with changeable permittivity ε and permeability μ [1, 2, 3] or graded refractive index n [1, 2, 3, 4, 5, 6, 7, 8, 9]. A vacuum polarization interpretation of the gravitational field endows the space of vacuum with physical qualities. It is just what Einstein hoped and predicted [10]. A reasonable extrapolation is that the electromagnetic fields can also be interpreted as the effects of vacuum polarization. Such an interpretation claims for a vacuum whose properties are somewhat like those of dielectric medium [11].

Exhilaratingly, facts and theories all indicate that vacuum is actually a special kind of medium [12, 13]. Casimir effect[14, 15] tells that vacuum is not just a void, but a special physical existence full of zero-point energy. Vacuum can be polarized by electromagnetic field, which leads to the well-known effects of Lamb shift and anomalous magnetic moment of the electron [12]. If the electromagnetic field is extremely powerful, the vacuum will be excited to produce $e^- - e^+$ pairs [16]. Deputs et al. pointed out that the optical properties of quantum vacuum could be modified by magnetic field, witch will influence the propagation of light emitted by a magnetized neutron star [13]. Rikken and Rizzo predicted that magnetoelectric birefringence will occur in vacuum when magnetic and electric fields are perpendicularly applied [17]. The phenomena that the propagation of light can be modified by applying electromagnetic fields to the vacuum are just similar to the Kerr electro-optic effect and the Faraday magneto-optic effect in dielectric medium. This similarity between the vacuum and the dielectric medium implies that vacuum must also have its inner structure, which could be influenced by electric charges or currents.

In this letter, both the electric field and magnetic field will be analysed on the basis of vacuum polarization. The energy of electric and magnetic fields will be figured out by using the intensity of vacuum polarization. The electrical and magnetic forces will be discussed considering the action of the nearby virtual dipoles in vacuum. By doing this, the relation between the electromagnetic fields and the quantum vacuum will be clarified. The electromagnetic wave will then be described as an effect of successional changing of vacuum polarization. Also, it will be shown that the virtual dipoles around an elementary charge have a characteristic half length on average, which leads to some interesting findings further.

First, examining the electric displacement vector $\mathbf{D}$ in a dielectric medium:

$$\mathbf{D} = \mathbf{P} + \varepsilon_0 \mathbf{E}, \tag{1}$$

where $\mathbf{P}$ represents the polarization of dielectric medium, ε_0 is the permittivity of vacuum, $\mathbf{E}$ denotes the electric field intensity in the medium. It is noticed that in the equation $\varepsilon_0 \mathbf{E}$ can be interpreted as the polarization of vacuum $\mathbf{P}'$ [1, 2], that is

$$\mathbf{P}' = \varepsilon_0 \mathbf{E}. \tag{2}$$

The vacuum polarization is based on the knowledge that there are virtual positive-negative charges, for example, but not limited to, virtual $e^- - e^+$ pairs, being randomly created and annihilated in vacuum. Similar to a dielectric medium, the virtual charge pairs in a vacuum will be polarized and aligned by the real charges, or by the so-called "external electric field". For example, a vacuum will be polarized in a spherical symmetry by a positive electric charge $+Q$ as shown in Fig. 1, where the solid $\bigoplus$ denotes the real charge $+Q$, the dashed $\ominus\oplus$ is a simplified representation of a polarized virtual charge pair in the vacuum, and the direction from the negative virtual charge to the positive one indicates the direction of the electric field.

The intensity of vacuum polarization can be defined as $\mathbf{P}' = \sum \mathbf{p}'/V$, where $\mathbf{p}'$ is the electrical dipole moment of a single polarized virtual charge pair, and V is a volume. If there are N virtual vacuum dipoles in volume V, each dipole has an electrical dipole moment $\mathbf{p}' = q' \cdot 2\mathbf{a}$ ($2a$ is the average distance between the two vacuum virtual charges $\pm q'$ — the reason we say "average" here is that, for an individual virtual dipole, the length $2a$ can be quite different due to the uncertainties in quantum mechanics), we have

$$\mathbf{P}' = \frac{N}{V} q' \cdot 2\mathbf{a}. \tag{3}$$

The fundamental limit on the rate of quantum dynamics: the unified bound is tight

Lev B. Levitin and Tommaso Toffoli

arXiv:0905.3417v2 [quant-ph] 17 Jun 2009

The question of how fast a quantum state can evolve has attracted a considerable attention in connection with quantum measurement, metrology, and information processing. Since only orthogonal states can be unambiguously distinguished, a transition from a state to an orthogonal one can be taken as the elementary step of a computational process.[1] Therefore, such a transition can be interpreted as the operation of "flipping a qubit", and the number of orthogonal states visited by the system per unit time can be viewed as the maximum rate of operation.

A lower bound on the orthogonalization time, based on the energy spread ΔE, was found by Mandelstam and Tamm.[2] Another bound, based on the average energy E, was established by Margolus and Levitin.[3] The bounds coincide, and can be exactly attained by certain initial states if $\Delta E = E$. However, the problem remained open of what the situation is when $\Delta E \neq E$.

Here we consider the unified bound that takes into account both ΔE and E. We prove that there exist no initial states that saturate the bound if $\Delta E \neq E$. However, the bound remains tight: for any given values of ΔE and E, there exists a one-parameter family of initial states that can approach the bound arbitrarily close when the parameter approaches its limit value. The relation between the largest energy level, the average energy, and the orthogonalization time is also discussed. These results establish the fundamental quantum limit on the rate of operation of any information-processing system.

Starting with the classical result of Mandelstam and Tamm,[2] it was later shown by Fleming,[4] Anandan and Aharonov,[5] and Vaidman[6] that the minimum time τ required for arriving to an orthogonal state is bounded by

$$\tau \geq \hbar/4\Delta E, \tag{1}$$

where $(\Delta E)^2 = \langle\psi|H^2|\psi\rangle - (\langle\psi|H|\psi\rangle)^2$, H is the Hamiltonian, and $|\psi\rangle$ the wavefunction of the system. A different bound was obtained in,[3] namely,

$$\tau \geq \hbar/4E. \tag{2}$$

Here, $E = \langle\psi|H|\psi\rangle$ is the quantum-mechanical average energy of the system (the energy of the ground state is taken to be zero). Both bounds (1) and (2) are tight, and achieved for a quantum state such that $\Delta E = E$.

Since then, a vast literature has been devoted to various aspects of this problem. In particular, inequality (2) has been proved for mixed states and for composite systems both in separable and in entangled states (e.g., Giovannetti et al.,[7,8] Zander et al.[9]). Bound (2) obtained for an isolated system has been generalized to a system driven by an external Hamiltonian (a "quantum gate") in.[10,11] Various derivations of (1) and (2) (e.g.,[12–14]), bounds based on energy-distribution moments,[15] more general problems of time-optimal quantum evolution,[13,16–24] and the ultimate limits of computation[25,26] have been considered.

However, what remained unnoticed is the paradoxical situation of the existence of two bounds based on two different characteristics of the quantum state, seemingly independent of one another. Since the average energy E and the energy uncertainty ΔE play the most determinative role in quantum evolution, it is important to have a unified bound that would take into account both of these characteristics.

In all known cases where bounds (1) and (2) can be exactly attained, the ratio $\alpha = \frac{\Delta E}{E}$ equals 1. A question arises: what happens if $\alpha \neq 1$? Some authors just assumed without justification that the minimum orthogonalization time is

$$\tau_{\min} = \max\left(\frac{h}{4E}, \frac{h}{4\Delta E}\right) = \frac{h}{2[E + \Delta E - |E - \Delta E|]}. \tag{3}$$

In fact, the situation is not so simple. Bound (3), indeed, can only be achieved for $\alpha = 1$. However, this bound remains tight when $\alpha \neq 1$ as well, though in this case it is only asymptotically attainable.

Theorem 1 *Under the assumption that the smallest (ground) energy of a quantum system is zero,*

1. *The only state that attains bound (1) is the two-level state*

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle + |\psi_1\rangle), \tag{4}$$

where $H|\psi_k\rangle = kE_1$ for $k = 0, 1$;

2. *The only state that attains bound (2) is likewise state (4). State (4) is unique up to degeneracy of the energy level E_1 and arbitrary phase factors for $|\psi_0\rangle$ and $|\psi_1\rangle$.*

Proof. To prove the first statement we shall use the trigonometric inequality

$$\cos x \geq 1 - \frac{4}{\pi^2} x \sin x - \frac{2}{\pi^2} x^2, \tag{5}$$

which is valid for any real x. Note that (5) turns into an equality iff $x = 0$ or $x = \pm\pi$.

Let the initial state be

$$|\psi(0)\rangle = \sum_{n=0}^{\infty} c_n |E_n\rangle, \tag{6}$$

where the $|E_n\rangle$ are energy eigenstates of the system and $\sum_{n=0}^{\infty} |c_n|^2 = 1$. Then

$$\begin{aligned} |S(t)|^2 &= |\langle\psi(0)|\psi(t)\rangle|^2 \\ &= \sum_{n,n'=0}^{\infty} |c_n|^2 |c_{n'}|^2 e^{-i\frac{E_n - E_{n'}}{\hbar/t}} \\ &= \sum_{n,n'=0}^{\infty} |c_n|^2 |c_{n'}|^2 \cos\frac{E_n - E_{n'}}{\hbar/t}. \end{aligned} \tag{7}$$

Using inequality (5), we obtain

$$\begin{aligned} |S(t)|^2 &\geq 1 - \frac{4}{\pi^2} \sum_{n,n'=0}^{\infty} |c_n|^2 |c_{n'}|^2 \frac{E_n - E_{n'}}{\hbar/t} \sin\frac{E_n - E_{n'}}{\hbar/t} \\ &\quad - \frac{2}{\pi^2} \sum_{n,n'=0}^{\infty} |c_n|^2 |c_{n'}|^2 \left(\frac{E_n - E_{n'}}{\hbar/t}\right)^2 \\ &= 1 + \frac{4t}{\pi^2} \frac{d\,|S(t)|^2}{dt} - \frac{1}{\pi^2}\left(\frac{\Delta E}{\hbar/2t}\right)^2. \end{aligned} \tag{8}$$

Since $|S(t)|^2 \geq 0$, it follows that $\frac{d\,|S(t)|^2}{dt} = 0$ whenever $S(t) = 0$. Thus, at a time τ such that $S(\tau) = 0$, the second term in (8) vanishes, and we obtain

$$0 \geq 1 - \frac{4\tau^2}{\pi^2\hbar^2}(\Delta E)^2, \tag{9}$$

Attacking an OT-Based Blind Signature Scheme

Stylianos Basagiannis, Panagiotis Katsaros and Andrew Pombortsis

***Abstract*—In this paper, we describe an attack against one of the Oblivious-Transfer-based blind signatures scheme, proposed in [1]. An attacker with a primitive capability of producing specific-range random numbers, while exhibiting a partial MITM behavior, is able to corrupt the communication between the protocol participants. The attack is quite efficient as it leads to a protocol communication corruption and has a sound-minimal computational cost. We propose a solution to fix the security flaw.**

***Index Terms*—Oblivious Transfer, blind signatures.**

I. Introduction

Oblivious Transfer (OT) constitutes a powerful tool used today in modern cryptography. In the first introduction of the OT_1^2 mechanism by Rabin [2], it is assumed that in a communication system, Alice transmit to Bob a two-part message, where only the one part is the secret that Alice wants to share. From Bob's side, Bob does not know which one of the two is the real secret, so he selects one of them with probability ½ of success (or ½ of failure).

In the related bibliography, OT based security protocols [3] [4] that aim to guarantee a variety of security properties such as anonymity or privacy of the participants, especially when OT is combined with other cryptographic primitives, e.g. blind signatures [5]. Through these works, OT has been involved into several improvements regarding efficiency and of the OT-based communication systems. The basic OT_1^2, described above, has been replaced by mechanisms of OT_1^n shown in [3], where the *Sender* dispatch N message to the *Chooser*, and the *Chooser* selects the appropriate message without knowing the initial selection of the *Sender*.

In reports [6] and [7], the OT mechanism is combined with various cryptographic techniques, in order to provide the involved participants with even more security guarantees. OT is combined with signature schemes providing strong fairness, anonymity and privacy of the communication. Both of the reports also provide a detailed analysis of the protocol in terms of anonymity and privacy. There are also reports like [8], where security threats over the OT-based protocol schemes have been classified into high and low cost attacks. All these kinds of security threats are managed to succeed regarding the computational cost of the encryption used between the protocols' participants, where an adversary is consider containing the maximum computational power, performing a variety of attack actions.

In this paper, we present an attack against the OT-based double blind signature scheme protocol described in [1]. More precisely, we show that a partial MITM intruder with a low computational cost can corrupt the protocol's communication by integrity violating one of the protocols' exchanged messages (by tagging specific random numbers). As a result the protocols' agents will accept the corruption occurred, which misinterprets the overall communication.

The authors are with the Dept. of Informatics, Aristotle University of Thessaloniki, 541 24, Greece. Email: {basagis, katsaros, apombo}@csd.auth.gr.

II. The OT-based blind signature protocol

This paper focuses on the analysis of a variant *1*-out-of-*n* Oblivious Transfer (OT_1^n) based on blind signatures protocol. The specific protocol incorporates a blind mechanism from both the *Sender*'s and the *Chooser*'s side. To achieve cryptographic efficiency the protocol involves a series of security perspectives such as public key cryptography, blind signatures and a keyed hash function. A random number generator for both of the participants is also used in order to overcome predictability attacks caused by an *Intruder*. The following notation is used throughout the paper:

N	RSA modulus
$\{S_0,\ldots,S_{n-1}\}$	*Sender* posses initially n secret strings S_i
σ	*Chooser* posses initially an integer $\sigma \in [0..n-1]$
H	Pre-agreed Hash Function
$SK < N,d >$	Secret Key
$PK < N,e >$	Public Key
$\{U_0,\ldots,U_{n-1}\}$	Random numbers $U_0,\ldots,U_{n-1} \in Z^*_N$
$SP()$	Secure padding scheme for RSA
C	Random number $C \in Z^*_N$
R	Random number $R \in Z^*_N$
Y_σ	Blind Signature for the *Sender*
$K_{j=0..n-1}$	Encryption Keys for the *Sender*
$\oplus$	XOR operator
$d1>>d2$	Right shift-bit operator

The *Sender* has n input secret strings, $\{S_0,\ldots,S_{n-1}\}$ and the *Chooser*'s input is an integer $\sigma \in [0..n-1]$. Because of the OT_1^n, the *Chooser* should learn a secret S_σ and nothing on any other $\{S_0,\ldots,S_{n-1}\}-\{S_\sigma\}$. On the other hand, the *Sender* should learn nothing about σ. The protocol described here provides unconditional protection for the *Chooser* and computational protection in the random oracle model for the *Sender*. Due to the OT operability, the specific protocol may be often invoked multiple times between the participants.

The basic steps of the described protocol are illustrated in Fig.1 and can be summarized as follows:

arXiv:0908.3023v2 [quant-ph] 15 Oct 2009

Can closed timelike curves or nonlinear quantum mechanics improve quantum state discrimination or help solve hard problems?

Charles H. Bennett,[1,*] Debbie Leung,[2,†] Graeme Smith,[1,‡] and John A. Smolin[1,§]

[1]*IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA*

[2]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada. N2L 3G1.*

(Dated: October 15, 2009)

We study the power of closed timelike curves (CTCs) and other nonlinear extensions of quantum mechanics for distinguishing nonorthogonal states and speeding up hard computations. If a CTC-assisted computer is presented with a labeled mixture of states to be distinguished—the most natural formulation—we show that the CTC is of no use. The apparent contradiction with recent claims that CTC-assisted computers can perfectly distinguish nonorthogonal states is resolved by noting that CTC-assisted evolution is nonlinear, so the output of such a computer on a mixture of inputs is not a convex combination of its output on the mixture's pure components. Similarly, it is not clear that CTC assistance or nonlinear evolution help solve hard problems if computation is defined as we recommend, as correctly evaluating a function on a labeled mixture of orthogonal inputs.

Introduction: Physicists and science fiction writers have long been interested in time travel, wherein a person or object travels backward in time to interact with a younger version of itself. The many studies of such closed timelike curves have led to the general conclusion that, while conditions for their creation may not arise in typical astrophysical or cosmological settings, in principle there seems to be no barrier to their existence[1–5].

In the context of quantum computation, the most widely accepted model of time travel, due to Deutsch [6], involves a unitary interaction U of a causality-respecting (CR) register with a register that traverses a CTC. The physical states of Deutsch's theory are the density matrices of quantum mechanics, but the dynamics are augmented from the usual linear evolution. For each initial mixed state ρ_{CR} of the CR register, the CTC register is postulated to find a fixed point ρ_{CTC} such that

$$\mathrm{Tr}_{CR}(U\rho_{CR}\otimes\rho_{CTC}U^\dagger)=\rho_{CTC}. \qquad (1)$$

The final state of the CR register is then defined in terms of the fixed point as

$$\rho'_{CR}=\mathrm{Tr}_{CTC}(U\rho_{CR}\otimes\rho_{CTC}U^\dagger). \qquad (2)$$

The induced mapping $\rho_{CR}\to\rho'_{CR}$ is nonlinear because the fixed point ρ_{CTC} depends on the initial state ρ_{CR}. The nonlinear evolution leads to various puzzling consequences considered below, but, because the fixed point is allowed to be a mixed state, it always exists [6], thereby avoiding the notorious "grandfather paradox" wherein some initial conditions lead to no consistent future [7].

In Deutsch's model, the mixed-state fixed point ρ_{CTC} explicitly begins in a product state with the CR register. Thus, the universe may evolve from a pure to mixed state, which is not normally allowed by quantum mechanics. To recover a pure state picture Deutsch appeals to the multiverse of the many-worlds interpretation, where the CTC system in our world is entangled with other worlds' CTC and CR systems. This kind of mixed state runs counter to the "church of the larger Hilbert space" philosophy applicable to CTC-free quantum mechanics, which views mixed states as always being subsystems of larger entangled pure systems in *this* universe.

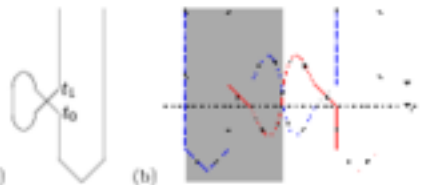


FIG. 1: Sending half of an EPR pair along a CTC. (a) Single universe picture. An EPR pair is created in the distant past. At time t_0 a qubit emerges from the CTC and at time t_1 half of the EPR pair is put into the CTC. According to Deutsch's prescription the density matrix of the CTC system at t_0 is equal to the CTC density matrix at t_1. Nevertheless the joint state at any time after t_1 is a product state. (b) Multiple universe picture. In both universes an EPR pair is created in the distant past. At time t_0 a qubit emerges from the CTC in each universe. At time t_1 in each universe half of an EPR pair is put into the CTC and goes back in time to emerge at t_0 in the other universe. Each EPR particle originally created is entangled with a partner in the other universe and in a product state with the other particle in its own universe.

To illustrate Deutsch's model, consider putting half of a maximally entangled state into a CTC (FIG. 1). There are now two causality respecting qubits, A and B, and a single CTC qubit. The unitary of Eq. (1) is the swap operation between CTC and B. Finding the fixed point gives $\rho_{CTC}=\frac{1}{2}I$, which along with Eq. (2) gives a final state of $\rho'_{AB}=\frac{1}{4}I_A\otimes I_B$ on the causality respecting qubits. Strangely, not only does the CTC cause an evolution from a pure to mixed state but the simple act of sending B along a CTC disentangles it from A. A pure state is recovered by considering both our initial universe and the universe with which the CTC interacts.

In: Daniel M. Dubois (Ed.) *Proceedings of the 8th Intern. Conf. on Computing Anticipatory Systems CASYS'07*, Liège, Belgium, 6-11 August 2007. Melville, NY: *American Institute of Physics Conference Proceedings*, Vol. 1051 (2008) pp. 33-49.

The Communication of Meaning in Anticipatory Systems: A Simulation Study of the Dynamics of Intentionality in Social Interactions

Loet Leydesdorff

Amsterdam School of Communications Research (ASCoR), University of Amsterdam, Kloveniersburgwal 48, 1012 CX Amsterdam, The Netherlands; http://www.leydesdorff.net ; loet@leydesdorff.net

Abstract. Psychological and social systems provide us with a natural domain for the study of anticipations because these systems are based on and operate in terms of intentionality. Psychological systems can be expected to contain a model of themselves and their environments; social systems can be strongly anticipatory and therefore co-construct their environments, for example, in techno-economic (co-)evolutions. Using Dubois' hyper-incursive and incursive formulations of the logistic equation, these two types of systems and their couplings can be simulated. In addition to their structural coupling, psychological and social systems are also coupled by providing meaning reflexively to each other's meaning-processing. Luhmann's distinctions among (1) interactions between intentions at the micro-level, (2) organization at the meso-level, and (3) self-organization of the fluxes of meaningful communication at the global level can be modeled and simulated using three hyper-incursive equations. The global level of self-organizing interactions among fluxes of communication is retained at the meso-level of organization. In a knowledge-based economy, these two levels of anticipatory structuration can be expected to propel each other at the supra-individual level.

Keywords: anticipation, social system, meaning, communication, incursion, double contingency
PACS: 87.23.Ge; 89.65.-s; 89.70.+c; 89.75.Fb

1. INTRODUCTION

The hyper-incursive formulation of the logistic equation—$x_t = ax_{t-1}(1 - x_{t+1})$ [1]—provides us with an operationalization of the concept of "double contingency" which has been central to the theory of social systems [2-7]. According to Luhmann [5:70], "double contingency" can be considered as the auto-catalyst of social processes between reflexive individuals.

The concept of double contingency was first formulated by the American sociologist Talcott Parsons, who defined "double contingency" in 1951 as follows:

> The expectation is not defined "*Being* what I am, alter's treatment of me must take one of the following alternatives" but "Depending on *which of several alternatives open to me I take*, I will set *alter* a problem to which he will react in terms of the alternative system of his own which is oriented to my action."[2:94]

According to Parsons [3: 436], the theory of games could be considered as a most sophisticated analysis of the implications of double contingency. However, one can also specify the dynamics of expectations in terms of the theory of strongly anticipatory systems [8,9] and provide the above (formal) equation with the following (substantive) interpretation: *Ego* (at x_t) operates on the basis of an expectation of its own next state (x_{t+1}) and the next state of an *Alter* ($1 - x_{t+1}$). Note that *Alter* is now defined in terms of *Ego*'s expectations; the relationship between expectations constructed in each human mind precedes a possible interaction between *Ego* and *Alter*.

While Parsons based his definition mainly on American pragmatism [2,9], the German sociologist Niklas Luhmann elaborated on double contingency in the continental tradition. He based himself on Edmund Husserl's transcendental phenomenology. Husserl had concluded that "intersubjectivity" provides us with an intentionality different from and transcendental to subjectivity [10:144]. While subjective intentionality is a natural consequence

PARADOXES OF THERMODYNAMICS AND STATISTICAL PHYSICS

DRAGOLJUB CUCIĆ
Regional centre for talents Mihajlo Pupin, Pančevo, Serbia, rctpupin@panet.rs

ABSTRACT

The paradoxes of thermodynamics and statistical physics are unavoidable in the study of physical paradoxes because of their importance at the time they came to be as well as the frequency of their appearance in historical studies of physics. In this work paradoxes are presented together with the historical studies of their creation, their solutions are given and they are analysed according to a number of characteristics: is it an exparadox, is it of theoretic or experimental nature, is it a thought experiment and the type of paradox it belongs to.

Key words: paradox, thermodynamics, statistical physics

Introduction

The subject of this work are paradoxes of thermodynamics and statistical physics. In the professional literature one can find a lot of texts dealing with the paradoxes in this branch of physics, but they are all solved and processed individually. In scientific works of this kind the solutions of each of the paradoxes are presented more thoroughly than here.
There is no text, or at least I haven't had the opportunity to find one, that synthesizes all more familiar paradoxes of thermodynamics and statistical physics according to common characteristics. This is the very aim of this work; to clearly number the paradoxes of thermodynamics and statistical physics that are considered by the author as worthy of attention; to show the historical conditions prior to paradox formulation; to give the current paradox solutions, if any exist, without in-depth explanations, since to solve certain paradoxes a very specific professional knowledge is needed and finally to gain a general insight into the paradoxes according to the following characteristics: is there a solution to the paradox, is it of theoretic or experimental nature, is the paradox a thought experiment and the paradox type.
This kind of analysis will provide a quantitative understanding and the opportunity to draw a conclusion concerning a possible special nature of paradoxes of thermodynamics and statistical physics. The results will be given, for better clarity, in graphical and tabular form.
This kind of analysis provides an approach to the phenomenon of paradox from the perspective of this branch of physics in order to get as complete picture of them as possible. A clear formulation of the causes of paradox in physics provides an easier path to their solutions if the paradoxes are equivalent in certain characteristics.

Paradoxes of thermodynamics and statistical physics

Thermodynamics is a branch of physics that, like other branches of the science, has its origins in Ancient Greek philosophy. The breakthroughs in the study of heat phenomena date back to the middle ages with the attempts of scale standardisation and physical realisation of measuring device. The invention of the thermometer in the 17th century enables the heat to be studied quantitatively as well as qualitatively and thermodynamics begins clearly to take shape.

Reasons for Cybersecurity Circumvention*

A Study and a Model

Sean Smith
PhD
Department of Computer Science
Dartmouth College
sws@cs.dartmouth.edu

Ross Koppel
PhD, FACMI
Department of Sociology
University of Pennsylvania
rkoppel@sas.upenn.edu

Jim Blythe
PhD
Information Sciences Institute
University of Southern California
blythe@isi.edu

Vijay Kothari
PhD Student
Department of Computer Science
Dartmouth College
vijaya@cs.dartmouth.edu

* This poster is an adaptation of an earlier paper, Mismatches: a Semiotic Model of Computer Security Circumvention, Smith et al., WASA 2015

Introduction

Users often work around security controls. We can pretend this doesn't happen, but it does.

In our research, we address this problem via observation and grounded theory (Bernard and Ryan, 2010; Charmaz, 2003; Pettigrew, 2009). Rather than assuming that users behave perfectly or that we're bad users de bad things, we instead observe and record what really goes on compared to the various expectations. Then, after reviewing data, we develop structure and models, and bring in additional data to support, reject and refine these models.

A Semiotic Model for IT Usability Trouble

In their seminal work on the meaning of language, Ogden and Richards (1927) constructed what is sometimes called the **semiotic triad**. The vertices are the three principal objects: what the speaker (or listener/reader) **thinks**, what **symbol** they use, and the actual item to which they are **referring**.

We Ask Why Circumvention Occurs and How It Can Be Reduced

We extend the Ogden and Richards (1927) semiotic model to examine reasons for workarounds.

We now extend to security:

- *Referent* → *thought*: the admin constructs a mental model of what she imagines are the actual enterprise workflow requirements.
- *Thought* → *symbol*: the admin reasons about security and work goals and constructs a system configuration that she believes achieves these goals.
- *Symbol* → *referent*: this configuration in practice then generates some actual reality.

Policy creation:
- *Referent* → *thought*: Admin perceives risk from unattended computers in hospital.
- *Thought* → *symbol*: Admin adds proximity detectors and automatic logout after timeout.
- *Symbol* → *referent*: Machines time out when clinician turns away or detector is poorly wiring.

Policy circumvention:
- *Referent* → *thought*: Clinicians perceive this system as not matching their desired workflow.
- *Thought* → *symbol*: Clinicians place inverted styrofoam cups over detectors.
- *Symbol* → *referent*: Net exposure is even worse.

Loss of Static Properties Result in Greater Vulnerabilities

Lost Workflow Properties:
•Electronic health records (EHRs) list oldest tests first.
•Computer physician order entry (CPOE) imposes "linear workflow" (Harrison et al., 2007).
•EHR limits box to N chars; no way for reader to know there's another box.
•IEEE editing portal does not allow summary rejection.
•Network flow anomaly tool fails to recognize only abuse.
•Bona fide user cannot authenticate to credit bureau — because it uses knowledge-based authentication, based on data corrupted by identity theft.
•Policy requires nurses witness disposal of extra meds before disposal can happen.

Invariants Made False:
•"EHR reflects needed dose, not lethal dose."
•"IT system reflects actual IV dosage patient has received."
•"smart pump IT represents actual drug, dose, patient weight."
•"EHR reflects actual diagnosis, not insurance trick"
•"the EHR record's author field indicates the author."
•"university travel portal for user A records only A's travel."

Provisioning:
•Unix sysadmins confidently creating wrong access controls.
•Users at universities, govt, and P2P accidentally make private files world readable (Maxion and Reeder, 2005).
•Investment bank employees unable to understand their own entitlements.
•Barrier to automated role mining is "interpretability" (Xu and Stoller, 2012)

User Circumvention of Authentication Protocols

Users are often obliged to work around authentication protocols to perform their tasks.

Adding Functionality:
•Sticky notes, shared passwords.
•US nuclear missiles had launch code "00000000" (Nichols, 2013).

Removing Functionality:
- smart key in Faraday foil (Paul and MacNaughton, 2014).
- code silently removed by compilers (Wang et al., 2013).

Shadow Systems:
- Password-free telephone instead of online (Heckle,2011).
- Exfiltration by turning docs into images.
- Screen scraping images into PowerPoint.
- Dropbox instead of official Sharepoint.
- Work docs sent to home email.
- Government users tunneling to university system.
- Government users working from Starbucks.

Turning Security Knobs Has Unintended Consequences

When security rules tighten, users who view them as incongruent with workflow needs are obliged to circumvent them, thereby creating a dip in actual security.

Loss of Monotonicity

We implicitly have some numeric function S that maps a tunable parameter (e.g., password length) to the level of security achieved. The intention of the human is to tune the parameter x so as to maximize S(x). However, if the mappings across the triad nodes fail to preserve crucial properties of this x vs S(x) curve, unfortunate things can happen.

Uncanny Descent: Dialing security **up** can make the reality **worse**.
- requiring strong passwords leads to writing them down or relying on security questions.
- adding computerized controls to medicine hurts patients by disrupting workflow (many examples).
- adding S/MIME led to worse trust decisions (Masone, 2008).
- adding effective security controls leads to them being disabled by default.
- limiting message size leads to accidental exfiltration.

Uncanny Ascent: Dialing security **down** can make the reality **better**
- eliminating unique passwords led to reduction in sharing.
- shortening Gmail passwords can make them more secure.
- having browser remember critical site password stopped phishing.

Uncanny nop: Dialing security **up or down** has **no effect** on the reality.
•passwords must be distinct from last 4—but users know they checked via hash.
•adding privileged secure WiFi—but users all use the public one.
•educating users about good behavior doesn't change behavior (e.g., Riley, 2006; Yan et al., 2005; Dhamija and Perrig, 2000; Heckle, 2011).
•deleting material by deleting link.

The system is as weak as its weakest link. With greater complexity, there are more vulnerabilities.

Loss of Continuity

Small changes in configuration can yield surprisingly big changes in security reality.

Domain and Range Trouble

Reality may have more parameters and consequences.

Example: loss of locality of control. The actual security at S1 can change because of a policy change by the admin at a different S2!
- password reuse + leak.
- training users to accept self-signed SSL certificates.
- training users to accept basic authentication.
- requiring users to change passwords.

For more information on this and our other project work, visit http://shucs.org

Visit shucs.org to learn more about the Science of Human Circumvention of Security

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency

INFORMATION TRUST INSTITUTE

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/263490183

Hamiltonian Flows and the Holomovement

Article in Mind and Matter · January 2013

CITATIONS
3

READS
92

2 authors:

Maurice A de Gosson
University of Vienna
209 PUBLICATIONS **1,353** CITATIONS

SEE PROFILE

B. J. Hiley
University College London
132 PUBLICATIONS **3,508** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Pseudodifferential operators and quantum mechanics View project

LOCATIF - Local Aspects of Time-Frequency analysis View project

All content following this page was uploaded by Maurice A de Gosson on 03 July 2014.

The user has requested enhancement of the downloaded file.

arXiv:1409.5338v5 [physics.hist-ph] 30 Nov 2015

Minkowski Spacetime and QED from Ontology of Time

C. Baumgarten[1]
5244 Birrhard, Switzerland[a)]

[Dated: 1 December 2015)

Classical mechanics, relativity, electrodynamics and quantum mechanics are often depicted as separate realms of physics, each with its own formalism and notion. This remains unsatisfactory with respect to the unity of nature and to the necessary number of postulates. We uncover the intrinsic connection of these areas of physics and describe them using a common symplectic Hamiltonian formalism. Our approach is based on a proper distinction between variables and constants, i.e. on a basic but rigorous ontology of time. We link these concept with the obvious conditions for the possibility of measurements. The derived consequences put the measurement problem of quantum mechanics and the Copenhagen interpretation of the quantum mechanical wavefunction into perspective. According to our (onto-) logic we find that spacetime can not be fundamental. We argue that a geometric interpretation of symplectic dynamics emerges from the isomorphism between the corresponding Lie algebra and the representation of a Clifford algebra. Within this conceptional framework we derive the dimensionality of spacetime, the form of Lorentz transformations and of the Lorentz force and fundamental laws of physics as the Planck-Einstein relation, the Maxwell equations and finally the Dirac equation.

PACS numbers: 01.70.+w, *43.10.Mq, 05.45.Xt, 03.50.De, 03.65.Pm, 45.20.Jj, 47.10.Df, 05.45.Xt
Keywords: Philosophy of physics, Lorentz transformation, Electrodynamics, Dirac equation, Hamiltonian mechanics, coupled oscillators

I. OVERTURE

Schrödinger wrote that "In Einstein's theory of gravitation matter and its dynamical interaction are based on the notion of an intrinsic geometric structure of the space-time continuum"[1]. What we will discuss in this article will force us to conjecture the reverse statement, *i.e.* that the intrinsic geometric structure of spacetime is based on the very notion of matter and its dynamical interaction. The idea that spacetime is not fundamental but emergent has been proposed in the past by several authors[2–12]. Some authors discussed the relation between spacetime and quantum communication[13]. This conjecture will guide us towards a different, almost classical, notion of quantum mechanics, closely connected to the phase space picture of classical statistical mechanics. A significant number of publications support our directions of thought[14–25].

We shall start from pure logical reasoning based on "the method of physics" and the distinction of variables and constants, i.e. from the (onto-)logic of time. Consider the basic quantummechanical relationship

$$i\hbar\partial_t\psi = E\,\psi\,. \tag{1}$$

The left side is the rate of change of a wavefunction ψ and the equation expresses that this rate of change is equal to the energy of the system. "Energy" is probably the most fundamental concept in physics. The conservation of energy has no serious exception and physics assigns to the energy the role of substance. Any entity that falls under the notion of "object" has energy and therefore also a rate of change $\omega = E/\hbar$. What exists The rate of change is what we call the "passage of time". This is the meaning of saying that time and energy are conjugate quantities. We measure the passage of time by clocks, i.e. by the rate of change of some reference device. Of cause - according to Eq. 1 - any real system is itself a clock. Metaphorically we say it exists *in time*.

It is part of the postulates of quantum mechanics that composed systems are described by a composed wavefunction. There is no limit in principle for the size of systems that are described by a common wavefunction - including the whole universe. Furthermore the wavefunction is considered to be *the* fundamental description of reality. The wavefunction for composed systems has more than just one real and an one imaginary part - it consists of several components. But no matter how large the system is - according to quantum mechanics it can finally be described by $2n$ real fundamental variables that form the real and the imaginary part of ψ.

We write the real and imaginary part separately $\psi = X + i\,Y$ with $E/\hbar = \omega$:

$$\begin{aligned}\dot{\psi} &= \dot{X} + i\,\dot{Y} = -i\omega(X + iY)\\ \dot{X} &= \omega\,Y\\ \dot{Y} &= -\omega\,X\,,\end{aligned} \tag{2}$$

where the dot indicates the temporal derivative. In ma-

a)Electronic mail: christian-baumgarten@gmx.net

Progress In Electromagnetics Research, PIER 32, 247–269, 2001

DISCRETE HODGE-OPERATORS: AN ALGEBRAIC PERSPECTIVE

R. Hiptmair

Sonderforschungsbereich 382
Universität Tübingen
72076 Tübingen, Germany

Abstract—Discrete differential forms should be used to deal with the discretization of boundary value problems that can be stated in the calculus of differential forms. This approach preserves the topological features of the equations. Yet, the discrete counterparts of the metric-dependent constitutive laws remain elusive.

I introduce a few purely algebraic constraints that matrices associated with discrete material laws have to satisfy. It turns out that most finite element and finite volume schemes comply with these requirements. Thus convergence analysis can be conducted in a unified setting. This discloses basic sufficient conditions that discrete material laws have to meet in order to ensure convergence in the relevant energy norms.

1 Introduction

2 Discrete Differential Forms

3 Discrete Hodge Operators

4 Examples

5 Abstract Error Analysis

6 Estimation of Consistency Errors

References

1. INTRODUCTION

The focus of this paper is on linear stationary boundary value problems that can be expressed in the calculus of differential forms (For

arXiv:1002.1722v2 [hep-th] 17 Feb 2010

Introduction to Holographic Superconductors

Gary T. Horowitz

Abstract These lectures give an introduction to the theory of holographic superconductors. These are superconductors that have a dual gravitational description using gauge/gravity duality. After introducing a suitable gravitational theory, we discuss its properties in various regiemes: the probe limit, the effects of backreaction, the zero temperature limit, and the addition of magnetic fields. Using the gauge/gravity dictionary, these properties reproduce many of the standard features of superconductors. Some familiarity with gauge/gravity duality is assumed. A list of open problems is included at the end.

1 Introduction

The name "holographic superconductor" suggests that one can look at a two (spatial) dimensional superconductor and see a three dimensional image. We will see that there is a class of superconductors for which this is true, but the image one "sees" is quite striking. It involves a charged black hole with nontrivial "hair". This remarkable connection between condensed matter and gravitational physics was discovered just a few years ago. It grew out of the gauge/gravity duality which has emerged from string theory [47, 21, 61]. Although this duality was first formulated as a equivalence between a certain gauge theory and a theory of quantum gravity (and provided new insights into each of these theories), over the past decade it has been applied with notable success to other areas of physics as well. Many of these new applications are discussed in other lectures in this school. I will focus on the application to superconductivity. These lectures will be heavily based on [29, 30, 37, 38]. For a more general discussion of applying gauge/gravity duality

Gary T. Horowitz
Physics Department, UCSB, Santa Barbara, CA 93106, USA, e-mail: gary@physics.ucsb.edu

arXiv:1003.3303v2 [quant-ph] 18 Jul 2010

Quantum anomalies and linear response theory

Itamar Sela[1], **James Aisenberg**[2], **Tsampikos Kottos**[2], **Doron Cohen**[1]

[1]Department of Physics, Ben-Gurion University, Beer-Sheva 84105, Israel
[2]Department of Physics, Wesleyan University, Middletown, CT 06459, USA

Abstract. The analysis of diffusive energy spreading in quantized chaotic driven systems, leads to a universal paradigm for the emergence of a quantum anomaly. In the classical approximation a driven chaotic system exhibits stochastic-like diffusion in energy space with a coefficient D that is proportional to the intensity ϵ^2 of the driving. In the corresponding quantized problem the coherent transitions are characterized by a generalized Wigner time t_φ, and a self-generated (intrinsic) dephasing process leads to non-linear dependence of D on ϵ^2.

A major theme in mechanics concerns the response of a system to a driving source $f(t)$, given that the interaction term is $\mathcal{H}_{\rm ext} = f(t)V$. This leads to the well known framework of linear response theory (LRT) with its celebrated fluctuation-dissipation relation. Below we assume a stationary driving source which is characterized by a power spectrum $\tilde{S}(\omega) = \mathbf{FT}[\langle f(t)f(0)\rangle]$, where $\mathbf{FT}$ stands for Fourier transform. In the absence of driving the stationary fluctuations of the system are characterized by the spectral function $\tilde{C}(\omega) = \mathbf{FT}[\langle V(t)V(0)\rangle]$. In the presence of driving the main three effects are: the *decay* of the initial preparation; the spreading and eventually the *diffusion* in energy space; and the associated *heating*.

1. LRT and Kubo

Strict LRT behavior means that the diffusion in energy space [1] and the related absorption coefficient [2, 3, 4] are *linear functional* of the spectral function $\tilde{S}(\omega)$. Specifically, the Kubo formula for the diffusion coefficient in energy space is

$$D \;=\; \frac{1}{2}\int_{-\infty}^{\infty} \omega^2 d\omega\; \tilde{C}(\omega)\tilde{S}(\omega) \tag{1}$$

It follows that the diffusion is proportional to the intensity of the driving ϵ^2 as defined below. We are going to consider on equal footing driving by a quasi-constant perturbation $f(t)\sim$const, and quasi-linear DC driving with $\dot{f}(t)\sim$const. The notation "$\sim$const" means that it is constant over large time intervals of duration t_φ, with some characteristic RMS value that we call ϵ. Accordingly the associated spectral functions is

$$\tilde{S}(\omega) \;=\; \epsilon^2\omega^{-\sigma}\delta_\gamma(\omega) \tag{2}$$

where $\delta_\gamma(\omega) = (\gamma/\pi)/(\omega^2+\gamma^2)$ with $\gamma = 1/t_\varphi$, while the spectral exponent is $\sigma{=}0$ for quasi-constant perturbation, and $\sigma{=}2$ for quasi linear DC driving.

The quantum mechanics of time travel through post-selected teleportation

Seth Lloyd[1], Lorenzo Maccone[1], Raul Garcia-Patron[1], Vittorio Giovannetti[2], Yutaka Shikano[1,3]
[1]*zQIT,Massachusetts Institute of Technology, 77 Mass Ave., Cambridge MA.*
[2]*NEST-CNR-INFM & Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126, Pisa, Italy.*
[3]*Dep. Physics, Tokyo Institute of Technology, 2-12-1 Oh-Okayama, Meguro, Tokyo, 152-8551, Japan.*

This paper discusses the quantum mechanics of closed timelike curves (CTCs) and of other potential methods for time travel. We analyze a specific proposal for such quantum time travel, the quantum description of CTCs based on post-selected teleportation (P-CTCs). We compare the theory of P-CTCs to previously proposed quantum theories of time travel: the theory is physically inequivalent to Deutsch's theory of CTCs, but it is consistent with path-integral approaches (which are the best suited for analyzing quantum field theory in curved spacetime). We derive the dynamical equations that a chronology-respecting system interacting with a CTC will experience. We discuss the possibility of time travel in the absence of general relativistic closed timelike curves, and investigate the implications of P-CTCs for enhancing the power of computation.

PACS numbers: 03.67.-a,03.65.Ud,04.60.Cf,04.62.+v,04.60.-m

arXiv:1007.2615v2 [quant-ph] 19 Jul 2010

Einstein's theory of general relativity allows the existence of closed timelike curves, paths through spacetime that, if followed, allow a time traveler – whether human being or elementary particle – to interact with her former self. The possibility of such closed timelike curves (CTCs) was pointed out by Kurt Gödel [1], and a variety of spacetimes containing closed timelike curves have been proposed [2, 3]. Reconciling closed timelike curves with quantum mechanics is a difficult problem that has been addressed repeatedly, for example, using path integral techniques [4–9]. This paper explores a particular version of closed timelike curves based on combining quantum teleportation with post-selection. The resulting post-selected closed timelike curves (P-CTCs) provide a self-consistent picture of the quantum mechanics of time-travel. P-CTCs offer a theory of closed timelike curves that is physically inequivalent to other Hilbert-space based theories, e.g., that of Deutsch [10]. As in all versions of time travel, closed timelike curves embody apparent paradoxes, such as the grandfather paradox, in which the time traveller inadvertently or on purpose performs an action that causes her future self not to exist. Einstein (a good friend of Gödel) was himself seriously disturbed by the discovery of CTCs [11]. Because the theory of P-CTCs rely on post-selection, they provide self-consistent resolutions to such paradoxes: anything that happens in a P-CTC can also happen in conventional quantum mechanics with some probability. Similarly, the post-selected nature of P-CTCs allows the predictions and retrodictions of the theory to be tested experimentally, even in the absence of an actual general-relativistic closed timelike curve.

Time travel is a subject that has fascinated human beings for thousands of years. In the Hindu epic, the Mahabarata, for example, King Revaita accepts an invitation to visit Brahma's palace. Although he stays for only a few days, when he returns to earth he finds that many eons have passed. The Japanese fisherman in the folk tale Urashima Taro, having saved a sea turtle, is invited to the palace of the sea-king; upon returning home discovers on the beach a crumbling monument, centuries old, memorializing him. The Gaelic hero Finn McCool suffers a similar fate. These stories also dwell on the dangers of time travel. Urashima Taro is given a magic box and told not to open it. Finn receives the gift of a magic horse and told not to dismount. When, inevitably, Taro opens the box, and Fian's toe touches the ground, they instantaneously age and crumble into dust.

These tales involve time travel to the future. Perhaps because of the various paradoxes to which it gives rise, the concept of travel to the past is a more recent invention. Starting in the late eighteenth century, a few narratives take a stab at time travel to the past, the best known being Charles Dickens's *A Christmas Carol*, and Mark Twain's *A Connecticut Yankee in King Arthur's Court*. The contemporary notion of time travel, together with all its attendant paradoxes, did not come into being until H.G. Wells' masterpiece, *The Time Machine*, which is also the first book to propose an actual device that can be used to travel back and forth in time.

As frequently happens, scientific theories of time travel lagged behind the fictional versions. Although Einstein's theory of general relativity implicitly allows travel to the past, it took several decades before Gödel proposed an explicit space-time geometry containing closed timelike curves (CTCs). The Gödel universe consists of a cloud of swirling dust, of sufficient gravitational power to support closed timelike curves. Later, it was realized that closed timelike curves are a generic feature of highly curved, rotating spacetimes: the Kerr solution for a rotating black hole contains closed timelike curves within the black hole horizon; and massive rapidly rotating cylinders typically are associated with closed timelike curves [2, 8, 12]. The topic of closed timelike curves in general relativity continues to inspire debate: Hawking's chronology protection postulate, for example, suggests that the conditions needed to create closed timelike curves cannot arise in any physically realizable spacetime [13]. For example, while Gott showed that cosmic string geometries can contain closed timelike curves [3], Deser *et al.* showed that

arXiv:1009.3786v1 [quant-ph] 20 Sep 2010

Chapter 1

A universe of processes and some of its guises

Bob Coecke

Oxford University Computing Laboratory
OX1 3QD Oxford, UK
coecke@comlab.ox.ac.uk

1.1 Introduction

Our starting point is a particular 'canvas' aimed to 'draw' theories of physics, which has *symmetric monoidal categories* as its mathematical backbone. In this paper we consider the *conceptual foundations* for this canvas, and how these can then be converted into mathematical structure.

With very little structural effort (i.e. in very abstract terms) and in a very short time span the *categorical quantum mechanics* (CQM) research program, initiated by Abramsky and the author in [6], has reproduced a surprisingly large fragment of quantum theory [45, 171, 180, 61, 57, 62, 49, 3, 63]. It also provides new insights both in *quantum foundations* and in *quantum information*, for example in [59, 60, 50, 51, 80, 65, 52, 81], and has even resulted in automated reasoning software called `quantomatic` [76, 77, 75] which exploits the deductive power of CQM, which is indeed a *categorical quantum logic* [78].

In this paper we complement the available material by not requiring prior knowledge of category theory, and by pointing at connections to previous and current developments in the foundations of physics.

This research program is also in close synergy with developments elsewhere, for example in representation theory [73], quantum algebra [177], knot theory [188], topological quantum field theory [133] and several other areas.

arXiv:1011.0723v1 [physics.data-an] 2 Nov 2010

Entropic Inference*

Ariel Caticha
Department of Physics, University at Albany-SUNY,
Albany, NY 12222, USA.

Abstract

In this tutorial we review the essential arguments behing entropic inference. We focus on the epistemological notion of information and its relation to the Bayesian beliefs of rational agents. The problem of updating from a prior to a posterior probability distribution is tackled through an eliminative induction process that singles out the logarithmic relative entropy as the unique tool for inference. The resulting method of Maximum relative Entropy (ME), includes as special cases both MaxEnt and Bayes' rule, and therefore unifies the two themes of these workshops – the Maximum Entropy and the Bayesian methods – into a single general inference scheme.

1 Introduction

Our subject is inductive inference. Our goal in this tutorial paper is to review the problem of updating from a prior probability distribution to a posterior distribution when new information becomes available.

First we tackle the question of the nature of information itself: What is information? It is clear that data "contains" or "conveys" information, but what does this precisely mean? Is information physical? We discuss how in a properly Bayesian framework one can usefully adopt a concept of information that is more directly related to the epistemological concerns of rational agents.

Then we turn to the actual methods to process information. We argue for the uniqueness and universality of the Method of Maximum relative Entropy (ME) and then we discuss its relation to Bayesian methods. At first sight Bayesian and Maximum Entropy methods appear unrelated. Bayes' rule is the natural way to update probabilities when the new information is in the form of data. On the other hand, Jaynes' method of maximum entropy, MaxEnt, is designed to handle information in the form of constraints [1]. An important question is whether they are compatible with each other. We show that the ME method includes both MaxEnt and Bayesian methods as special cases and

*Presented at MaxEnt 2010, the 30th International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering (July 4-9, 2010, Chamonix, France).

The quantum Gaussian well

Saikat Nandi*

Tata Institute of Fundamental Research, Mumbai-400005, India

Abstract

Different features of a potential in the form of a Gaussian well have been discussed extensively. Although the details of the calculation are involved, the general approach uses a variational method and WKB approximation, techniques which should be familiar to advanced undergraduates. A numerical solution of the Schrödinger equation through diagonalization has been developed in a self-contained way, and physical applications of the potential are mentioned.

arXiv:1011.3637v1 [quant-ph] 16 Nov 2010

arXiv:1011.4031v1 [math-ph] 17 Nov 2010

The Clifford Algebra approach to Quantum Mechanics A: The Schrödinger and Pauli Particles.

B. J. Hiley* and R. E. Callaghan.

TPRU, Birkbeck, University of London, Malet Street, London WC1E 7HX.

Abstract

In this paper we show how all the quantum properties of Schrödinger and Pauli particles can be described entirely from within a Clifford algebra taken over the reals. There is no need to appeal to any 'wave function'. To describe a quantum system, we define the Clifford density element [CDE], $\rho_r = \Phi_L\tilde{\Phi}_L$, as a product of an element of a minimal left ideal, Φ_L, and its Clifford conjugate. The properties of the system are then completely specified in terms of bilinear invariants of the first and second kind calculated using the CDE. Thus the quantum properties of a system can be completely described from within the algebra without the need to appeal to any Hilbert space representation.

Furthermore we show that the essential bilinear invariants of the second kind are simply the Bohm energy and the Bohm momentum, entities that make their appearance in the Bohm interpretation. We also show how these parameters emerge from standard quantum field theory in the low energy, single particle approximation. There is no need to appeal to classical mechanics at any stage. This clearly shows that the Bohm approach is entirely within the standard quantum formalism. The method has enabled us to lay the foundations of an approach that can be extended to provide a complete relativistic version of Bohm model. In this paper we confine our attention to the details of the non-relativistic case and will present its relativistic extension in a subsequent paper.

*E-mail address b.hiley@bbk.ac.uk.

A Classification Diagram for Physical Variables

(preliminary draft)

comments and suggestions are highly welcome

diagrammi.tex

tonti@units.it

Enzo Tonti

September 8, 2003

Noname manuscript No.
(will be inserted by the editor)

Recent progress on the elliptic curve discrete logarithm problem

Steven D. Galbraith · Pierrick Gaudry

Received: date / Accepted: date

Abstract We survey recent work on the elliptic curve discrete logarithm problem. In particular we review index calculus algorithms using summation polynomials, and claims about their complexity.

Keywords Elliptic curve discrete logarithm problem (ECDLP) · Summation polynomials · Pollard rho · Index calculus

Mathematics Subject Classification (2000) 11Y16 · 11G20 · 14G15 · 13P10 · 14G50 · 11T71 · 14H52

1 Introduction

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, where $q = p^n$ and p is prime. The *elliptic curve discrete logarithm problem (ECDLP)* is the following computational problem: Given points $P, Q \in E(\mathbb{F}_q)$ to find an integer a, if it exists, such that $Q = aP$. This problem is the fundamental building block for elliptic curve cryptography and pairing-based cryptography, and has been a major area of research in computational number theory and cryptography for several decades.

There are many excellent books that provide a detailed background to elliptic curve cryptography, for example [3, 12, 13, 42, 58, 114]. Hence, the goal of this article is to survey developments from within the last five years or so. In particular we wish to highlight some open questions and areas where more work is needed. We assume the reader already has a good knowledge of elliptic curves and algorithms. We focus on the case of elliptic curves, but occasionally this involves mention of higher genus curves and their divisor class groups. However, we do not attempt to discuss all recent work regarding the DLP for curves of genus greater than one.

S. D. Galbraith
University of Auckland, New Zealand.
E-mail: s.galbraith@math.auckland.ac.nz

P. Gaudry
CNRS, Université de Lorraine and Inria, Nancy, France.
E-mail: pierrick.gaudry@loria.fr

Are All Probabilities Fundamentally Quantum Mechanical?

Rajat Kumar Pradhan*
Rajendra College, Bolangir, Orissa, India-767002.

(Date: 10.05.2011)

Abstract

The subjective and the objective aspects of probabilities are incorporated in a simple duality axiom inspired by observer participation in quantum theory. Transcending the classical notion of probabilities, it is proposed and demonstrated that all probabilities may be fundamentally quantum mechanical in the sense that they may all be derived from the corresponding amplitudes. The classical coin-toss and the quantum double slit interference experiments are discussed as illustrative prototype examples. Absence of multi-order quantum interference effects in multiple-slit experiments and the Experimental tests of complementarity in Wheeler's delayed-choice type experiments are explained using the involvement of the observer.

Key words: probability theory; quantum theory; coin toss; double slit interference; subject-object duality; Born rule.
PACS numbers: 02.50.Cw, 03.65.-w

*email: rajat@iopb.res.in

Analytic Modeling of Starshades

Webster Cash

Center for Astrophysics and Space Astronomy,

University of Colorado, Boulder, CO 80309, USA

ABSTRACT

External occulters, otherwise known as starshades, have been proposed as a solution to one of the highest priority yet technically vexing problems facing astrophysics - the direct imaging and characterization of terrestrial planets around other stars. New apodization functions, developed over the past few years, now enable starshades of just a few tens of meters diameter to occult central stars so efficiently that the orbiting exoplanets can be revealed and other high contrast imaging challenges addressed. In this paper an analytic approach to analysis of these apodization functions is presented. It is used to develop a tolerance analysis suitable for use in designing practical starshades. The results provide a mathematical basis for understanding starshades and a quantitative approach to setting tolerances.

Keywords: coronagraphs, exoplanets, diffraction

I. Introduction

Nearly everybody wants to know if Earth-like planets abound in the Universe. Are warm, watery paradises common, and does life arise everywhere it is given a chance? To answer these age-old questions requires a very good telescope capable of pulling the signal from a faint Earth-like planet out of the glare of its parent star. It will probably be necessary to look out to distances of 10 parsecs or more to have a good chance of finding such an Earth twin (Turnbull et al, 2011). But at that distance, the Earth is only thirtieth magnitude and hovers less than 0.1 arcseconds from the star.

This is a daunting challenge for telescope builders. An m=30 object, at 0.1 arcsecond angular separation, is at both the sensitivity limit and angular resolution limit of the Hubble Space Telescope. So an Earth-searching telescope has to be expensive and high quality if it is to be able to resolve and study the planetary system - even if there is no glare from the star.

The Terrestrial Planet Finder program encapsulated NASA's response. Two approaches were developed to building telescopes that could null out the parent star and

arXiv:1107.5436v1 [nlin.CD] 27 Jul 2011

Communications in Nonlinear Science and Numerical Simulation 11 (2006) 885-898

Fractional dynamics of systems with long-range interaction

Vasily E. Tarasov[1,2] **and George M. Zaslavsky**[2,3]

1) *Skobeltsyn Institute of Nuclear Physics,*
Moscow State University, Moscow 119992, Russia
2) *Courant Institute of Mathematical Sciences, New York University*
251 Mercer Street, New York, NY 10012, USA,
3) *Department of Physics, New York University,*
2-4 Washington Place, New York, NY 10003, USA

Abstract

We consider one-dimensional chain of coupled linear and nonlinear oscillators with long-range power wise interaction defined by a term proportional to $1/|n-m|^{\alpha+1}$. Continuous medium equation for this system can be obtained in the so-called infrared limit when the wave number tends to zero. We construct a transform operator that maps the system of large number of ordinary differential equations of motion of the particles into a partial differential equation with the Riesz fractional derivative of order α, when $0 < \alpha < 2$. Few models of coupled oscillators are considered and their synchronized states and localized structures are discussed in details. Particularly, we discuss some solutions of time-dependent fractional Ginzburg-Landau (or nonlinear Schrodinger) equation.

PACS: 05.45.-a; 45.05.+x; 45.50.-j

Keywords: Long-range interaction, Fractional oscillator, Synchronization, Fractional Ginzburg-Landau equation

arXiv:1107.6019v1 [gr-qc] 29 Jul 2011

Causal categories: relativistically interacting processes

Bob Coecke and Raymond Lal

University of Oxford, Computer Science, Quantum Group,
Wolfson Building, Parks Road, Oxford OX1 3QD, UK.
coecke/rayl@cs.ox.ac.uk

Abstract

A symmetric monoidal category naturally arises as the mathematical structure that organizes physical systems, processes, and composition thereof, both sequentially and in parallel. This structure admits a purely graphical calculus. This paper is concerned with the encoding of a fixed causal structure within a symmetric monoidal category: causal dependencies will correspond to topological connectedness in the graphical language. We show that correlations, either classical or quantum, force terminality of the tensor unit. We also show that well-definedness of the concept of a global state forces the monoidal product to be only partially defined, which in turn results in a relativistic covariance theorem. Except for these assumptions, at no stage do we assume anything more than purely compositional symmetric-monoidal categorical structure. We cast these two structural results in terms of a mathematical entity, which we call a *causal category*. We provide methods of constructing causal categories, and we study the consequences of these methods for the general framework of categorical quantum mechanics.

Contents

1 Introduction **2**

2 Processes as pictures **3**
2.1 Symmetric monoidal categories 3
2.2 Elements of Categorical Quantum Mechanics 9
2.3 A pitfall 11

3 Terminality of the tensor unit from correlations **12**
3.1 Causality as information flow, formalised by connectedness 12
3.2 Terminality of I as 'no correlation-induced signaling' 15

4 Partiality of the tensor from global state **19**

arXiv:1110.1520v3 [math.AT] 12 Jun 2013

ARRANGEMENTS OF SUBMANIFOLDS AND THE TANGENT BUNDLE COMPLEMENT

PRIYAVRAT DESHPANDE

ABSTRACT. Drawing parallels with hyperplane arrangements, we develop the theory of arrangements of submanifolds. Given a smooth, finite dimensional, real manifold X we consider a finite collection $\mathcal{A}$ of locally flat, codimension-1 submanifolds that intersect like hyperplanes. To such a collection we associate two combinatorial objects: the face category and the intersection poset. We also associate a topological space to the arrangement called the tangent bundle complement. It is the complement of union of tangent bundles of these submanifolds inside the tangent bundle of the ambient manifold. Our aim is to investigate the relationship between the combinatorics of the arrangement and the topology of the complement. In particular we show that the tangent bundle complement has the homotopy type of a finite cell complex. We generalize the classical theorem of Salvetti for hyperplane arrangements and show that this particular cell complex is completely determined by the face category.

INTRODUCTION

An arrangement of hyperplanes is a finite set $\mathcal{A}$ of hyperplanes in $\mathbb{R}^l$. These hyperplanes and their intersections induce a stratification of the ambient space. These strata form a poset when ordered by topological inclusion known as the *face poset*. The set of all possible intersections also forms a poset known as the *intersection poset* (usually ordered by reverse inclusion). These two posets contain combinatorial information about the arrangement. The topological spaces associated with an arrangement $\mathcal{A}$ are the *real complement* $\mathcal{C}(\mathcal{A})$ and the *complexified complement* $M(\mathcal{A})$. The real complement is the complement of the union of hyperplanes in $\mathbb{R}^l$, whereas the complexified complement is the complement of the union of the complexified hyperplanes in $\mathbb{C}^l$. One of the aspects of the theory of arrangements is to understand the interaction between the combinatorial data of an arrangement and the topology of these complements. For example, one would like to comprehend to what extent the combinatorial data of an arrangement control the topological invariants, such as (co)homology or homotopy groups etc., of these complements.

In this paper we introduce a generalization of real hyperplane arrangements which we call the *arrangements of submanifolds of codimension*-1. We consider situations in which finitely many submanifolds of a given manifold intersect in a way that the local information is same as that of a hyperplane arrangement but the global picture is different. Intuitively, it means that for every point of the manifold there exists a coordinate neighborhood homeomorphic to an arrangement of real hyperplanes. We also introduce an analogue of the complexified complement in this new setting and call it *the tangent bundle complement*. This paper is an attempt to answer the following question: *how does the combinatorics of the intersections of these submanifolds help determine the topology of the tangent bundle complement?*

2010 *Mathematics Subject Classification.* 52C35, 57N80, 05E45.

Key words and phrases. Hyperplane arrangements, Salvetti complex, Nerve lemma, Acyclic categories.

bioRxiv preprint first posted online Mar. 8, 2017; doi: http://dx.doi.org/10.1101/115063. The copyright holder for this preprint (which was not peer-reviewed) is the author/funder. It is made available under a CC-BY-NC-ND 4.0 International license.

High-resolution TADs reveal DNA sequences underlying genome organization in flies

Fidel Ramírez[1*], Vivek Bhardwaj[1,5,*], José Villaveces[2], Laura Arrigoni[3], Björn A. Grüning[4], Kin Chung Lam[1], Bianca Habermann[2], Asifa Akhtar[1], Thomas Manke[1#]

[1]Max Planck Institute of Immunobiology and Epigenetics. Bioinformatics Unit. Stübeweg 51, 79108 Freiburg Germany

[2]Max Planck Institute of Biochemistry. Computational Biology. Am Klopferspitz 18, 82152 Martinsried Germany

[3]Max Planck Institute of Immunobiology and Epigenetics. Sequencing Facility. Stübeweg 51, 79108 Freiburg Germany

[4]University of Freiburg, Department of Computer Science, Georges-Köhler-Allee 106, 79110 Freiburg, Germany

[5]Faculty of Biology, University of Freiburg, Schänzlestraße 1, 79104 Freiburg, Germany

* These authors contributed equally
# Corresponding author
manke@ie-freiburg.mpg.de
+49 (0)761 5108738

arXiv:1201.0907v3 [math-ph] 16 Jul 2013

A Geometrical Method of Decoupling

C. Baumgarten[1]
Paul Scherrer Institute, Switzerland[a)]

[Dated: 17 July 2013]

The computation of tunes and matched beam distributions are essential steps in the analysis of circular accelerators. If certain symmetries – like midplane symmetry – are present, then it is possible to treat the betatron motion in the horizontal, the vertical plane and (under certain circumstances) the longitudinal motion separately using the well-known Courant-Snyder theory, or to apply transformations that have been described previously as for instance the method of Teng and Edwards[1,2]. In a preceding paper it has been shown that this method requires a modification for the treatment of isochronous cyclotrons with non-negligible space charge forces[3]. Unfortunately the modification was numerically not as stable as desired and it was still unclear, if the extension would work for all conceivable cases. Hence a systematic derivation of a more general treatment seemed advisable.

In a second paper the author suggested the use of real Dirac matrices as basic tools for coupled linear optics and gave a straightforward recipe to decouple positive definite Hamiltonians with imaginary eigenvalues[4]. In this article this method is generalized and simplified in order to formulate a straightforward method to decouple Hamiltonian matrices with eigenvalues on the real and the imaginary axis. The decoupling of symplectic matrices which are exponentials of such Hamiltonian matrices can be deduced from this in a few steps. It is shown that this algebraic decoupling is closely related to a geometric "decoupling" by the orthogonalization of the vectors $\vec{E}$, $\vec{B}$ and $\vec{P}$, that were introduced with the so-called "electromechanical equivalence"[4].

A mathematical analysis of the problem can be traced down to the task of finding a structure-preserving block-diagonalization of symplectic or Hamiltonian matrices. Structure preservation means in this context that the (sequence of) transformations must be symplectic and hence canonical.

When used iteratively, the decoupling algorithm can also be applied to n-dimensional systems and requires $\mathcal{O}(n^2)$ iterations to converge to a given precision.

PACS numbers: 45.20.Jj, 05.45.Xt, 41.85.-p, 03.30.+p
Keywords: Hamiltonian mechanics, coupled oscillators, beam optics, Lorentz transformation

I. INTRODUCTION

The significance of the symplectic groups in Hamiltonian dynamics has been emphasized for instance by A. Dragt[5], and it has long been known[6] that the Dirac matrices are generators of the symplectic group $Sp(4,R)$. In Ref.[4] the author presented a toolbox for the treatment of two coupled harmonic oscillators that is based on the use of the real Dirac matrices (RDMs) as generators of the symplectic group $Sp(4,R)$ and a systematic survey of symplectic transformations in two dimensions. This toolbox enabled the development of a straightforward recipe for the decoupling of positive definite two-dimensional harmonic oscillators. Here we present an improvement of the method that is based on geometric arguments, i.e. on the orthogonalization of 3-dimensional vectors associated via the electromechanical equivalence (EMEQ) to certain linear combinations of matrix elements.

There is a long history of publications covering the diagonalization (and related) problems in linear algebra as well as in linear coupled optics, linear Hamiltonian dynamics and control theory. A (non-exhaustive) list is given in the bibliography (see Refs.[10–26], but also Ref.[3,4] and references therein). However, none of the previous works (known to the author) takes full advantage of the group structure of the generators of $Sp(4)$. The conceptually closest approach uses "quaternions", the representations of which seems to be identical to the RDMs[27], but seems to be limited to orthogonal symplectic transformations. The decoupling method of Teng and Edwards has been the starting point for this work, as it turned out to fail in some special cases (see Ref.[3] and App. D).

The method that we present here, is based on a survey of all symplectic similarity transformations. We do not make specific assumptions about the Hamiltonian other than that it is a symmetric quadratic form and we present a geometric interpretation via the EMEQ, which provides a physical notation of otherwise complicated and non-descriptive algebraic expressions [1]. Furthermore we believe that the use of the EMEQ is an interesting example of how elements of classical physics, quantum mechanics, special relativity, electrodynamics, group theory, geometric algebra, statistics[28] and last but not least symplectic theory fit together and allow to use a common formalism.

The simplest classical linear dynamical system with interaction (coupling) has two degrees of freedom and

a)Electronic mail: christian.baumgarten@psi.ch

[1] Compare for instance Ref.[20].

The Principle of Least Action as interpreted by Nature and by the Observer

Michel Gondran

*University Paris Dauphine, Lamsade, 75 016 Paris, France**

Alexandre Gondran

École Nationale de l'Aviation Civile, 31000 Toulouse, France†

arXiv:1203.2736v4 [quant-ph] 12 May 2015

Abstract

In this paper, we show that the difficulties of interpretation of the principle of least action concerning "final causes" or "efficient causes" are due to the existence of two different actions, the "Euler-Lagrange action" (or classical action) and the "Hamilton-Jacobi action". These two actions, which are not clearly differentiated in the texbooks, are solutions to the same Hamilton-Jacobi equation, but with very different initial conditions: smooth conditions for the Hamilton-Jacobi action, singular conditions for the Euler-Lagrange action. There are related by the Minplus Path Integral which is the analog in classical mechanics of the Feynmann Path Integral in quantum mechanics. Finally, we propose a clear-cut interpretation of the principle of least action: the Hamilton-Jacobi action does not use "final causes" and seems to be the action used by Nature; the Euler-Lagrange action uses "final causes" and is the action used by an observer to retrospectively determine the trajectory of the particle.

arXiv:1203.4988v2 [quant-ph] 27 Apr 2012

Strong Complementarity and Non-locality in Categorical Quantum Mechanics

Bob Coecke[1] Ross Duncan[2] Aleks Kissinger[1] Quanlong Wang[3]

[1]University of Oxford, Department of computer science,
Wolfson Building, Parks Road, Oxford OX1 3QD, UK.
coecke|aleks@cs.ox.ac.uk
[2]Université Libre de Bruxelles, Laboratoire d'Information Quantique
Campus Plaine, Boulevard du Triomphe, 1050 Brussels, Belgium
rduncan@ulb.ac.be
[3]Beihang University, School of Mathematics and System Sciences
XueYuan Road No.37, HaiDian District, Beijing, China
qlwang@buaa.edu.cn

Abstract—**Categorical quantum mechanics studies quantum theory in the framework of dagger-compact closed categories.**

Using this framework, we establish a tight relationship between two key quantum theoretical notions: non-locality and complementarity. In particular, we establish a direct connection between Mermin-type non-locality scenarios, which we generalise to an arbitrary number of parties, using systems of arbitrary dimension, and performing arbitrary measurements, and, a new stronger notion of complementarity which we introduce here.

Our derivation of the fact that strong complementarity is a necessary condition for a Mermin scenario provides a crisp operational interpretation for strong complementarity. We also provide a complete classification of strongly complementary observables for quantum theory, something which has not yet been achieved for ordinary complementarity.

Since our main results are expressed in the (diagrammatic) language of dagger-compact categories, they can be applied outside of quantum theory, in any setting which supports the purely algebraic notion of strongly complementary observables. We have therefore introduced a method for discussing non-locality in a wide variety of models in addition to quantum theory.

The diagrammatic calculus substantially simplifies (and sometimes even trivialises) many of the derivations, and provides new insights. In particular, the diagrammatic computation of correlations clearly shows how local measurements interact to yield a global overall effect. In other words, we *depict non-locality*.

I. Introduction

This paper is concerned with two central notions in quantum foundations and quantum computation, *non-locality* and *complementarity*, and the study of their relationship.

Non-locality is what Einstein notoriously referred to as 'spooky action at a distance'. It was formally substantiated for the first time by Bell's theorem, and experimentally verified by testing Bell-inequalities. It states that the correlations observed when measuring spatially quantum separated systems cannot be explained by means of classical probabilities, *i.e.* that there is no underlying *hidden variable theory*. Complementarity, informally put, states that if one knows the value of one observable sharply (e.g. position), then there is complete uncertainty about the other observable (e.g. momentum).

These two concepts underpin what is arguably the most successful endeavour towards quantum information technologies: quantum cryptography. Indeed, in a quantum key distribution protocol, encoding data in either of two complementary observables will enable the parties to detect interception by an adversary [7], while non-locality allows one to verify the authenticity of the shared entangled resource by means of which key sharing is established [23].

This research applies methods of computer science and logic to investigations in quantum foundations. It is moreover strongly aligned with the current trend in the broader quantum information community: understanding quantum information processing within a larger space of hypothetical information processing theories in order to understand what is particular about quantum theory.

Until now, this area has been characterised by the study of *generalised probabilistic theories* [6], a space of theories which includes quantum probability theory, classical probability theory, as well as theories which are even more non-local than quantum theory. A topic of particular focus has been the search for peculiarities of quantum non-locality, within the larger space of non-local theories, e.g. [38], [5].

Of course, a space of more general theories can be conceived as abstracting away certain concrete features of quantum theory, hence encompassing a broader class of theories, and the words 'generalised' and 'abstract' can be treated as synonymous. While the generalised probabilistic theories discussed above abstract away all but convex probabilistic structure, our focus is on the *compositional structure on processes*, say *generalised process theories*.

While having composition play a leading role evidently draws form computer science practice, it also appeals to Schrödinger's conviction that what mostly characterises quantum theory is the manner in which systems compose [39].

This compositional paradigm was the main motivation for

arXiv:1204.2779v3 [math.RT] 17 Oct 2013

Umbral Moonshine*

Miranda C. N. Cheng†
John F. R. Duncan‡
Jeffrey A. Harvey§

2013 October 13

Abstract

We describe surprising relationships between automorphic forms of various kinds, imaginary quadratic number fields and a certain system of six finite groups that are parameterised naturally by the divisors of twelve. The Mathieu group correspondence recently discovered by Eguchi–Ooguri–Tachikawa is recovered as a special case. We introduce a notion of extremal Jacobi form and prove that it characterises the Jacobi forms arising by establishing a connection to critical values of Dirichlet series attached to modular forms of weight two. These extremal Jacobi forms are closely related to certain vector-valued mock modular forms studied recently by Dabholkar–Murthy–Zagier in connection with the physics of quantum black holes in string theory. In a manner similar to monstrous moonshine the automorphic forms we identify constitute evidence for the existence of infinite-dimensional graded modules for the six groups in our system. We formulate an umbral moonshine conjecture that is in direct analogy with the monstrous moonshine conjecture of Conway–Norton. Curiously, we find a number of Ramanujan's mock theta functions appearing as McKay–Thompson series. A new feature not apparent in the monstrous case is a property which allows us to predict the fields of definition of certain homogeneous submodules for the groups involved. For four of the groups in our system we find analogues of both the classical McKay correspondence and McKay's monstrous Dynkin diagram observation manifesting simultaneously and compatibly.

*MSC2010: 11F22, 11F37, 11F46, 11F50, 20C34, 20C35

†Université Paris 7, UMR CNRS 7586 and LPTHE, Université Paris 6, Paris, France.
E-mail: chengm@math.jussieu.fr

‡Department of Mathematics, Case Western Reserve University, Cleveland, OH 44106, U.S.A.
E-mail: john.duncan@case.edu

§Enrico Fermi Institute and Department of Physics, University of Chicago, Chicago, IL 60637, U.S.A.
E-mail: j-harvey@uchicago.edu

Ciphers and Commuting Algebras of Hilbert Spaces in Music

Dr. Terry Allen (principle investigator; musician-mathematician)
tallen@wildblue.net

Daniel Branscombe (mathematician)
daniel.branscombe@gmail.com

Jim Bury (musician and guitar technical advisor)
92scooter@comcast.net

May 5, 2012

arXiv:1209.1737v3 [quant-ph] 4 Mar 2013

Quantum speed limits in open system dynamics

A. del Campo,[1,2] I. L. Egusquiza,[3] M. B. Plenio,[4,5] and S. F. Huelga[4,5]

[1]*Theoretical Division, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[2]*Center for Nonlinear Studies, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[3]*Department of Theoretical Physics and History of Science, UPV-EHU, 48080 Bilbao, Spain*
[4]*Institut für Theoretische Physik, Albert-Einstein Allee 11, Universität Ulm, D-89069 Ulm, Germany*
[5]*Institut for Integrated Quantum Science and Technology, Albert-Einstein Allee 11, Universität Ulm, D-89069 Ulm, Germany*

Bounds to the speed of evolution of a quantum system are of fundamental interest in quantum metrology, quantum chemical dynamics and quantum computation. We derive a time-energy uncertainty relation for open quantum systems undergoing a general, completely positive and trace preserving (CPT) evolution which provides a bound to the quantum speed limit. When the evolution is of the Lindblad form, the bound is analogous to the Mandelstam-Tamm relation which applies in the unitary case, with the role of the Hamiltonian being played by the adjoint of the generator of the dynamical semigroup. The utility of the new bound is exemplified in different scenarios, ranging from the estimation of the passage time to the determination of precision limits for quantum metrology in the presence of dephasing noise.

PACS numbers: 03.65.-w, 03.65.Yz, 03.67.Lx

How fast can a quantum system evolve? Quantum mechanics acts as a legislative body imposing speed limits to the evolution of quantum systems. While these limits are both ultimate and fundamental, at the same time, their existence is at the center of a surge of activity, as a result of their manifold applications, including the identification of precision bounds in quantum metrology [1], the formulation of computational limits of physical systems [2], and the development of quantum optimal control algorithms [3].

Bounds on the speed of evolution are intimately related to the concept of the passage time τ_p, which is the required time for a given pure state $|\chi\rangle$ to become orthogonal to itself under unitary dynamics [4]. One of the early answers to this problem was provided by Mandelstam and Tamm (MT), who showed that the passage time can be lower-bounded by the inverse of the variance in the energy of the system so that

$$\tau \geq \frac{\pi}{2}\frac{\hbar}{\Delta H}, \qquad (1)$$

where $\Delta H = \langle H^2\rangle - \langle H\rangle^2)^{1/2}$, whenever the dynamics under study is governed by an Hermitian Hamiltonian H [5–13]. A simple geometric interpretation of this result was provided by Brody using the Fubini-Study metric in the Hilbert space spanned by the initial state and its orthogonal complement [14]. Indeed, the passage time problem can be posed as a quantum brachistochrone problem. From this perspective, a particularly exciting result was found: whenever the Hamiltonian is non-Hermitian $\mathcal{PT}$-symmetric, the passage time can be made arbitrarily small without violating the time-energy uncertainty principle [15, 16]. A second bound, due to Margolus and Levitin (ML), takes the simpler form $\tau \geq \frac{\pi}{2}\frac{\hbar}{\langle H\rangle - E_0}$ where the zero of energy is generally shifted to the ground state energy so that $E_0 = 0$ [17]. This bound has been applied to ascertain fundamental computational limits in nature [2, 18].

Despite the growing body of literature on the subject, the analysis has almost exclusively been focused on unitary dynamics of isolated quantum systems. An analogous bound for open quantum systems is highly desirable, since ultimately all systems are coupled to an environment [19, 20]. As an example, such a bound on the evolution of an open system would help to address the robustness of quantum simulators and computers against decoherence [21], as well as the relevance of the specific nature of the noise, and in particular whether or not it is Markovian, in phase estimation problems of interest in metrology and precision spectroscopy [22, 23].

The MT bound can be derived by considering the time evolution of the overlap $\alpha = |\langle\psi_t|\psi_0\rangle|$ between the initial state $|\psi_0\rangle$ and the quantum state $|\psi_t\rangle$ at time t subject to a unitary evolution $U(t) = \exp\{-iHt/\hbar\}$. It can be shown that the MT-limit (eq. 1) is achievable, as for a suitable Hamiltonian H we can satisfy the differential equation $\hbar\frac{d\alpha^2}{dt} = -2\Delta H\,\alpha\sqrt{1-\alpha^2}$ which for $\alpha = \cos\phi$ is easily seen to result in $\hbar\dot{\phi} = \Delta H$ thus matching the MT bound [24].

In the case of open system dynamics we need to consider general non-unitary quantum evolutions and have the freedom to choose a variety of distance measures between quantum states. One natural choice here is the fidelity between two mixed states ρ and σ, which is given by $F(\rho,\sigma) = \mathrm{tr}[\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}]$. The quantum speed limit then provides a lower bound on the time τ that is required to achieve, for a given initial state $\rho(0)$ and a target fidelity f_{target}, the condition $F(\rho_\tau,\rho_0) < f_{target}$ subject to an open system evolution. Ideally, such bounds should reduce to the MT bound in the case of unitary dynamics on pure states and/or be easy to compute.

Bounds on τ may be derived by taking inspiration from the variational characterization of the fidelity $F(\rho^S,\sigma^S) = \max|\langle\psi^{SE}|\phi^{SE}\rangle|$ [25], where the maximization is over all $|\psi^{SE}\rangle$ ($|\phi^{SE}\rangle$) on a larger Hilbert space $\mathcal{H}^{SE}$ that are purifications of the mixed states ρ^S (σ^S) on the smaller system S, that is $\mathrm{tr}_E[|\psi^{SE}\rangle\langle\psi^{SE}|] = \rho^S$ ($\mathrm{tr}_E[|\phi^{SE}\rangle\langle\phi^{SE}|] = \sigma^S$). Then for any specific purification the inequality $F(\rho^S,\sigma^S) \geq |\langle\psi^{SE}|\phi^{SE}\rangle|$

High order gradient, curl and divergence conforming spaces, with an application to compatible NURBS-based IsoGeometric Analysis

R.R. Hiemstra[a], R.H.M. Huijsmans[a], M.I.Gerritsma[b]

[a]*Department of Marine Technology, Mekelweg 2, 2628CD Delft*
[b]*Department of Aerospace Technology, Kluyverweg 2, 2629HT Delft*

Abstract

Conservation laws, in for example, electromagnetism, solid and fluid mechanics, allow an exact discrete representation in terms of line, surface and volume integrals. We develop high order interpolants, from any basis that is a partition of unity, that satisfy these integral relations exactly, at cell level. The resulting gradient, curl and divergence conforming spaces have the property that the conservation laws become completely independent of the basis functions. This means that the conservation laws are exactly satisfied even on curved meshes. As an example, we develop high order gradient, curl and divergence conforming spaces from NURBS - non uniform rational B-splines - and thereby generalize the compatible spaces of B-splines developed in [1]. We give several examples of 2D Stokes flow calculations which result, amongst others, in a point wise divergence free velocity field.

Keywords:
Compatible numerical methods, Mixed methods, NURBS, IsoGeometric Analyis

> *Be careful of the naive view that a physical law is a mathematical relation between previously defined quantities. The situation is, rather, that a certain mathematical structure represents a given physical structure. Burke [2]*

1. Introduction

In deriving mathematical models for physical theories, we frequently start with analysis on finite dimensional geometric objects, like a control volume and its bounding surfaces. We assign global, 'measurable', quantities to these different geometric objects and set up balance statements. Take for example the global balance in (1), where the total mass/momentum/energy E inside a control volume V is only conserved (no change in time) if the in- and outgoing mass/momentum/energy fluxes Q over the bounding surfaces ∂V cancel.

$$\underbrace{\frac{d}{dt}E(V) = Q(\partial V)}_{\text{(discrete or global)}} \xrightarrow{\lim V \to P} \underbrace{\frac{\partial}{\partial t}e = \operatorname{div} \mathbf{q}}_{\text{(differential or local)}}. \tag{1}$$

This is exactly Gauss divergence theorem, depicted in Figure 1c. Other balance equations in $\mathbb{R}^3$ involve the fundamental theorem of calculus, relating a global quantity associated with a curve L, to the values of a quantity at the boundary points ∂L, and Stokes circulation theorem, which relates the amount of rotation in a surface S to the amount of circulation around the bounding curve ∂S.

While the association of physical quantities with geometry is clear in the global sense, it remains obscured when the mathematical model is written in local form, in (1), as a differential equation. The local variables, i.e. the source field $\mathbf{q}$ and density e, obtained from a limiting process by shrinking the integration domain V up to a point P, although mathematically well defined, seem to have lost their geometric significance.

Email addresses: R.R.Hiemstra@tudelft.nl (R.R. Hiemstra), R.H.M.Huijsmans@tudelft.nl (R.H.M. Huijsmans), M.I.Gerritsma@tudelft.nl (M.I.Gerritsma)

arXiv:1210.5658v1 [math.LO] 20 Oct 2012

HOMOTOPY TYPE THEORY AND VOEVODSKY'S UNIVALENT FOUNDATIONS

Álvaro Pelayo and Michael A. Warren

Abstract. Recent discoveries have been made connecting abstract homotopy theory and the field of type theory from logic and theoretical computer science. This has given rise to a new field, which has been christened "homotopy type theory". In this direction, Vladimir Voevodsky observed that it is possible to model type theory using simplicial sets and that this model satisfies an additional property, called the *Univalence Axiom*, which has a number of striking consequences. He has subsequently advocated a program, which he calls *univalent foundations*, of developing mathematics in the setting of type theory with the Univalence Axiom and possibly other additional axioms motivated by the simplicial set model. Because type theory possesses good computational properties, this program can be carried out in a computer proof assistant. In this paper we give an introduction to homotopy type theory in Voevodsky's setting, paying attention to both theoretical and practical issues. In particular, the paper serves as an introduction to both the general ideas of homotopy type theory as well as to some of the concrete details of Voevodsky's work using the well-known proof assistant Coq. The paper is written for a general audience of mathematicians with basic knowledge of algebraic topology; the paper does not assume any preliminary knowledge of type theory, logic, or computer science.

1. Introduction

Type theory is a branch of mathematical logic which developed out of the work of Church [9, 10, 11] and which has subsequently found many applications in theoretical computer science, especially in the theory of programming languages [19]. For instance, the notion of *data type* in programming languages derives from the type theoretic notion of *type*. Recently, a number of deep and unexpected connections between a form of type theory (introduced by Martin-Löf [40, 43, 44, 45]) and homotopy theory have been discovered, opening the way to a new area of research in mathematics and theoretical computer science which has recently been christened *homotopy type theory*. Due to the nature of the mathematical results in this area, we believe that there is great potential for the future research in this area to have a considerable impact on a number of areas of pure and applied mathematics, as well as on the practice of mathematicians.

Date: October 23, 2012.

2010 *Mathematics Subject Classification.* Primary 03-02. Secondary 03-B15, 68N18 and 55P99.

Pelayo is partly supported by NSF CAREER Award DMS-1055897, Spain Ministry of Science Grant MTM 2010-21186-C02-01, and Spain Ministry of Science Sev-2011-0087. Pelayo also received support from NSF Grant DMS-0635607 during the preparation of this paper.

Warren is supported by the Oswald Veblen Fund and also received support from NSF Grant DMS-0635607 during the preparation of this paper.

arXiv:1211.2098v1 [quant-ph] 9 Nov 2012

On the Relationship between the Moyal Algebra and the Quantum Operator Algebra of von Neumann.

B. J. Hiley.

TPRU, Birkbeck, University of London, Malet Street, London WC1E 7HX.

[b.hiley@bbk.ac.uk]

Abstract

The primary motivation for Moyal's approach to quantum mechanics was to develop a phase space formalism for quantum phenomena by generalising the techniques of classical probability theory. To this end, Moyal introduced a quantum version of the characteristic function which immediately provides a probability distribution. The approach is sometimes perceived negatively merely as an attempt to return to classical notions, but the mathematics Moyal develops is simply a re-expression of what is at the heart of quantum mechanics, namely the non-commutative algebraic structure first introduced by von Neumann in 1931. In this paper we will establish this relation and show that the "distribution function", $F(P,X,t)$ is simply the quantum mechanical density matrix for a single particle. The coordinates, X and P, are not the coordinates of the particle but the mean co-ordinates of a cell structure (a 'blob') in phase space, giving an intrinsically non-local description of each individual particle, which becomes a point in the limit to order $\hbar^2$. We discuss the significance of this non-commutative structure on the symplectic geometry of the phase space for quantum processes.

1 Introduction.

As is well known, the Wigner-Moyal approach has its origins in an early attempt of Wigner [48] to find quantum corrections to the statistical properties of thermodynamic quantum systems. A major contribution to the

arXiv:1211.2107v1 [quant-ph] 9 Nov 2012

Process, Distinction, Groupoids and Clifford Algebras: an Alternative View of the Quantum Formalism.

B. J. Hiley.

TPRU, Birkbeck, University of London, Malet Street, London WC1E 7HX.

Abstract

In this paper we start from a basic notion of process, which we structure into two groupoids, one orthogonal and one symplectic. By introducing additional structure, we convert these groupoids into orthogonal and symplectic Clifford algebras respectively. We show how the orthogonal Clifford algebra, which include the Schrödinger, Pauli and Dirac formalisms, describe the *classical* light-cone structure of space-time, as well as providing a basis for the description of quantum phenomena. By constructing an orthogonal Clifford bundle with a Dirac connection, we make contact with quantum mechanics through the Bohm formalism which emerges quite naturally from the connection, showing that it is a structural feature of the mathematics. We then generalise the approach to include the symplectic Clifford algebra, which leads us to a non-commutative geometry with projections onto shadow manifolds. These shadow manifolds are none other than examples of the phase space constructed by Bohm. We also argue that this provides us with a mathematical structure that fits the implicate-explicate order proposed by Bohm.

1 The Algebra of Process.

Traditionally basic theories of quantum phenomena are described in terms of the dynamical properties of particles-in-interaction, or more basically, fields-in-interaction built on an *a priori* given manifold. Special relativity demands this manifold is a Minkowski space-time, while general relativity demands a more general manifold with a metric carrying the properties of the gravitational field. In this paper we explore the possibility of starting

Effective Fokker-Planck Equation for Birhythmic Modified van der Pol Oscillator

R. Yamapi,[1,*] G. Filatrella,[2] M. A. Aziz-Alaoui,[3] and Hilda A. Cerdeira[4]

[1]*Fundamental Physics Laboratory, Department of Physics, Faculty of Science, University of Douala, Box 24 157 Douala, Cameroon and Salerno unit of CNSIM, Dept. of Physics, Univ. of Salerno,I-84081 Fisciano, Italy*

[2]*Dept. of Sciences for Biological, Geological, and Environmental Studies and Salerno unit of CNSIM, University of Sannio, Via Port'Arsa 11, I-82100 Benevento, Italy*

[3] *Applied Mathematics Laboratory, University of Le Havre, 25 rue ph. Lebon, B.P 540, Le Havre, Cedex, France*

[4] *Instituto de Física Teórica, Universidade Estadual Paulista, Rua Dr. Bento Teobaldo Ferraz, 271, Bloco II - Barra Funda, 01140-070 São Paulo, Brazil.*

arXiv:1212.0098v1 [nlin.CD] 1 Dec 2012

arXiv:1212.5605v2 [hep-th] 17 Mar 2014

Preprint typeset in JHEP style - HYPER VERSION

PUPT-2435

Scattering Amplitudes and the Positive Grassmannian

N. Arkani-Hamed[a], J. Bourjaily[b], F. Cachazo[c], A. Goncharov[d], A. Postnikov[e], and J. Trnka[a,f]

[a] *School of Natural Sciences, Institute for Advanced Study, Princeton, NJ*
[b] *Department of Physics, Harvard University, Cambridge, MA*
[c] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario, CA*
[d] *Department of Mathematics, Yale University, New Haven CT*
[e] *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA*
[f] *Department of Physics, Princeton University, Princeton, NJ*

Abstract: We establish a direct connection between scattering amplitudes in planar four-dimensional theories and a remarkable mathematical structure known as the *positive* Grassmannian. The central physical idea is to focus on on-shell diagrams as objects of fundamental importance to scattering amplitudes. We show that the all-loop integrand in $\mathcal{N}=4$ super Yang-Mills (SYM) is naturally represented in this way. On-shell diagrams in this theory are intimately tied to a variety of mathematical objects, ranging from a new graphical representation of permutations to a beautiful stratification of the Grassmannian $G(k,n)$ which generalizes the notion of a simplex in projective space. All physically important operations involving on-shell diagrams map to canonical operations on permutations—in particular, BCFW deformations correspond to simple adjacent transpositions. Each cell of the positive Grassmannian is naturally endowed with "positive" coordinates α_i and an invariant measure of the form $\prod_i d\log\alpha_i$ which determines the on-shell function associated with the diagram. This understanding allows us to classify and compute all on-shell diagrams, and give a geometric understanding for all the non-trivial relations among them. The Yangian invariance of scattering amplitudes is transparently represented by diffeomorphisms of $G(k,n)$ which preserve the positive structure. Scattering amplitudes in (1+1)-dimensional integrable systems and the ABJM theory in (2+1) dimensions can both be understood as special cases of these ideas. On-shell diagrams in theories with less (or no) supersymmetry are associated with exactly the same structures in the Grassmannian, but with a measure deformed by a factor encoding ultraviolet singularities. The Grassmannian representation of on-shell processes also gives a new understanding of the all-loop integrand for scattering amplitudes—presenting all integrands in a novel "dlog" form which is a direct reflection of the underlying positive structure.

arXiv:1302.2323v1 [quant-ph] 10 Feb 2013

Time and the Algebraic Theory of Moments.

B. J. Hiley*

TPRU, Birkbeck, University of London, Malet Street,
London WC1E 7HX.

Abstract

We introduce the notion of an extended moment in time, the duron. This is a region of temporal ambiguity which arises naturally in the nature of process which we take to be basic. We introduce an algebra of process and show how it is related to, but different from, the monoidal category introduced by Abramsky and Coecke. By considering the limit as the duration of the moment approaches the infinitesimal, we obtain a pair of dynamical equations, one expressed in terms of a commutator and the other which is expressed in terms of an anti-commutator. These two coupled real equations are equivalent to the Schrödinger equation and its dual.

We then construct a bi-algebra, which allows us to make contact with the thermal quantum field theory introduced by Umezawa. This allows us to link quantum mechanics with thermodynamics. This approach leads to two types of time, one is Schrödinger time, the other is an irreversible time that can be associated with a movement between inequivalent vacuum states. Finally we discuss the relation between our process algebra and the thermodynamic origin of time.

1 Introduction.

In this paper we address the question of time in quantum mechanics. The first and more commonly chosen option is to treat time as an external parameter as one does in the Schrödinger and Heisenberg equations of motion. In the relativistic domain time is treated as the fourth component of a four-vector. In non-relativistic quantum mechanics, the three space components are regarded as operators, why keep time as a parameter? Surely it should be treated as an operator. However the attempt to treat time as an operator is regarded as a failure for the reasons discussed by Pauli [57] in his seminal paper on this topic. As a caveat, we should point out that recently there have been two papers [29], [30] that have challenged this conclusion.

*E-mail address b.hiley@bbk.ac.uk.

arXiv:1304.6295v2 [math-ph] 1 May 2013

EMERGENT QUANTUM MECHANICS AS A THERMAL ENSEMBLE

P. Fernández de Córdoba[1,a], **J.M. Isidro**[1,b] **and Milton H. Pena**[1,2,c]
[1]Instituto Universitario de Matemática Pura y Aplicada,
Universidad Politécnica de Valencia, Valencia 46022, Spain
[2]Departamento de Matemáticas y Física, Universidad Tecnológica
del Chocó, Colombia
[a]pfernandez@mat.upv.es, [b]joimsan@mat.upv.es
[c]milpecr@posgrado.upv.es

Abstract It has been argued that gravity acts dissipatively on quantum–mechanical systems, inducing thermal fluctuations that become indistinguishable from quantum fluctuations. This has led some authors to demand that some form of time irreversibility be incorporated into the formalism of quantum mechanics. As a tool towards this goal we propose a thermodynamical approach to quantum mechanics, based on Onsager's classical theory of irreversible processes and on Prigogine's nonunitary transformation theory. An entropy operator replaces the Hamiltonian as the generator of evolution. The canonically conjugate variable corresponding to the entropy is a dimensionless evolution parameter. Contrary to the Hamiltonian, the entropy operator is not a conserved Noether charge. Our construction succeeds in implementing gravitationally–induced irreversibility in the quantum theory.

1 Introduction

It has been known for long that weak interactions violate CP–invariance [10]. By the CPT theorem of quantum field theory, time invariance must also be violated in weak interactions; recent observations [32] confirm this expectation. Now quantum field theory is an extension of quantum mechanics. Since time invariance is naturally implemented in the latter, it would appear that only CP–violating quantum field theories can also violate time invariance, because quantum mechanics as we know it is symmetric under time reversal.

Actually such is not the case. A number of firmly established quantum–gravity effects have been shown to be intrinsically irreversible; for background see, *e.g.*, [23, 30, 51, 52, 55] and references therein. From the independent perspective of statistical physics [40] it has also been suggested that time irreversibility should be taken into account at the more fundamental level of the differential equations governing mechanical processes. This is in sharp contrast with standard thinking, where irreversibility is thought to arise through *time–irreversible* initial conditions imposed on the solutions to *time–reversible* evolution equations. In view of this situation, a number of authors have called for the due modifications to the standard quantum–mechanical formalism (for a

Derivation of the String Tension Formalism from Inherent Parameters of a Holographic Anthropic Multiiverse (HAM)

R.L. Amoroso* & E.A. Rauscher°
*Noetic Advanced Studies Institute, 608 Jean St, Oakland, CA 94610-1422 USA
°Tecnic *Research Labr, 3500 S. Tomahawk Rd, Bldg. 188, Apache Junction, AZ 85219 USA*
Email: cerebroscopic@mindspring.com

Abstract. In Holographic Anthropic Multiverse (HAM) cosmology observed temporal reality is a 3(4)D virtual subspace of an 11(12)D eternity in correspondence with the tenets of the F-Theory incarnation of M-Theory; 12D being the minimum number of dimensions (D) to signify causal separation from temporality. Succinctly HAM cosmology postulates an infinite number of nested Hubble spheres each with their own laws of physics; this and other details of the HAM will be discussed in detail. The HAM present is a dynamic instant, a continuous-state standing wave of the least cosmological unit of the 12D Superspace undergoing a Continuous Dimensional Reduction / Compactification Process (CDRCP) based on extensions of the Wheeler-Feynman-Cramer transactional models. This HAM dynamic entails an energy dependent spacetime metric as 1* proposed by Einstein. This means that HD properties of the CDRCP standing wave metric entail a form of future-past hysteresis loop. The energetics of this so-called hysteresis loop of the 12D least unit reveal a new action principle driving the evolution of the HAM which is itself a form of self-organized complex system. Since the HAM is scale invariant these energetics also apply to self-organized Autopoietic living systems. This new teleological or noetic action principle is shown to be associated with the unitary physical field and a form of 'super quantum potential' as postulated by de Broglie and Bohm. Using these parameters an alternate derivation of the string tension formalism is derived. It is anticipated that this form of the string tension formalism may shed light on recalculating Planck's constant and lead to a program for completing quantum theory. HAM cosmology is empirically testable and an experimental protocol for isolation of the new energy dynamics is presented.

1. Introduction – Relevant Cosmological and Superstring Context

The evolutionary search for the fundamental background independent string vacuum has been cast recently in a Twelve Dimensional (12D) form called F-Theory. Generally String Theory is still aligned with naturalistic Big Bang Cosmology not perceived as compatible with a covariant Dirac polarized vacuum essential for extended electromagnetic theory and finite photon mass m_γ. A recently formulated highly symmetric continuous-state cosmology called the Holographic Anthropic Multiverse (HAM) utilizes a 12D energy dependent standing wave superspace based on extensions of the Wheeler-Feynman-Cramer transactional model providing a context where scale-invariant least cosmological units of the Superspace act as a complex self-organized system. These fundamental least-unit entail a form of incursive oscillator inherent in the continuous-state topology of HAM spacetime. Simulated application of the Incursive Oscillator (IO) is shown to produce a natural emergence of generalized F-Theory 2-branes from the superspace backdrop potentially bringing the IO program into closer alignment with mainstream physical cosmology which could be instrumental in solving the problem of deriving parameters of the fundamental string vacuum, especially emergence of a new action principle driving the evolution of its self-organization.

Over the last decade the cosmology of a continuous-state Holographic Anthropic Multiiverse (HAM) has been developed [1-4]. The HAM cosmology is highly ordered and symmetric such that the Euclidian-Minkowski $E_3 - \dot{M}_4$ present is a form of a harmonic oscillator, that is a virtual standing-wave topology of Higher Dimensional (HD) future-past elements. This condition is based on an extension of the Transactional Interpretation of quantum theory [5] to the topology of spacetime itself [1-4]. The transactional Interpretation is based on the Wheeler-Feynman absorber theory of radiation where events are transactions based on the interaction of future-past elements. The HAM cosmology is a form of self-organized complex system, a supposition suggesting properties

Ca Valtpa, I. Dientes & R.L. Amoroso (eds.) Unified Theories, 35-46. © 2005 The Noetic Press, Printed in the USA.

Riemannian Quantum Circuit

R. V. Ramos and F. V. Mendes
rubens@deti.ufc.br, fernandovm@deti.ufc.br

Lab. of Quantum Information Technology, Department of Teleinformatic Engineering – Federal University of Ceara - DETI/UFC, C.P. 6007 – Campus do Pici - 60455-970 Fortaleza-Ce, Brazil.

In this work we present the theory of a unitary matrix related to a finite number of zeros of the Riemann-zeta function. The equivalent quantum circuit and the calculation of the entanglement of a multipartite quantum state produced by the Riemannian quantum circuit are also shown.

1. Introduction

Recently, there has been a growing interest in quantum systems related to number theory problems [1-3]. Such interest comes from the early days of quantum mechanics, when Hilbert and Pólya discussed a possible physical solution for Riemann's hypothesis: the zeros of the Riemann-zeta function could be the spectrum of an operator $R = I/2 + iH$, where H is self-ajoint and interpreted as a Hamiltonian. Nowadays, several physical systems related to the zeros of the Riemann-zeta function have been discussed [4,5]. In particular, in [6] the authors, having a finite number of zeros of the Riemann-zeta function, used a numerical method for finding a quantum potential able to reproduce those zeros as energy eigenvalues.

In this work, we show how to construct a quantum circuit, hereafter named Riemannian quantum circuit, whose equivalent unitary matrix has eigenvalues related to the zeros (the amount of zeros considered is equal to the dimension of the unitary matrix) of the Riemann-zeta function. The existence of such quantum circuit implies that, at least in principle, it is always possible to construct a physical system related to any finite amount of zeros using a quantum computer. Additionally, we also show a quantum algorithm based on the Riemannian quantum circuit and we briefly discuss the amount of bipartite entanglement generated by the Riemannian quantum circuit for a particular state having up to 16 qubits.

The present work is outlined as follows: Section 2 brings the procedure for building a unitary matrix whose eigenvalues are related to the zeros of the Riemann-zeta function; Section 3 discusses some applications of the Riemannian quantum circuit; Section 4 shows a quantum circuit related to the unitary matrix obtained in Section 2; at last, conclusions are drawn in Section 5.

2. Procedure to construct the Riemannian unitary matrix

Let s_1, s_2, s_3, …, s_k, be a set of the first k non-trivial zeros of the Riemann-zeta

CUDA Leaks: Information Leakage in GPU Architectures

Roberto Di Pietro* Flavio Lombardi* Antonio Villani*
* Department of Maths and Physics
Roma Tre University
Rome, Italy
Email: {dipietro,lombardi,villani}@mat.uniroma3.it

arXiv:1305.7383v2 [cs.CR] 15 Jul 2013

Abstract

Graphics Processing Units (GPUs) are deployed on most present server, desktop, and even mobile platforms. Nowadays, a growing number of applications leverage the high parallelism offered by this architecture to speed-up general purpose computation. This phenomenon is called GPGPU computing (General Purpose GPU computing). The aim of this work is to discover and highlight security issues related to CUDA, the most widespread platform for GPGPU computing. In particular, we provide details and proofs-of-concept about a novel set of vulnerabilities CUDA architectures are subject to, that could be exploited to cause severe information leak. Following (detailed) intuitions rooted on sound engineering security, we performed several experiments targeting the last two generations of CUDA devices: Fermi and Kepler. We discovered that these two families do suffer from information leakage vulnerabilities. In particular, some vulnerabilities are shared between the two architectures, while others are idiosyncratic of the Kepler architecture. As a case study, we report the impact of one of these vulnerabilities on a GPU implementation of the AES encryption algorithm. We also suggest software patches and alternative approaches to tackle the presented vulnerabilities. To the best of our knowledge this is the first work showing that information leakage in CUDA is possible using just standard CUDA instructions. We expect our work to pave the way for further research in the field.[1]

Index Terms

Security; GPU; Information Leakage.

I. Introduction

Graphics Processing Units (GPUs) are a widespread and still underutilized resource. They are available on most present Desktop PCs, laptops, servers and even mobile phones and tablets. They are often used as cost-effective High Performance Computing (HPC) resources, as in computing clusters [1].

CUDA (Compute Unified Device Architecture - NVIDIA™) is by far the most widespread GPU platform, OpenCL (by AMD™) being its only competitor. Most present applications leverage CUDA for speeding-up scientific computing-intensive tasks or for computational finance operations [2]. GPU computational power is also employed to offload the CPU from security sensitive computations. As an example, various cryptographic algorithms have been ported to GPUs [3]–[9]. Such applications require the encryption key or other sensitive data to be present on the GPU device where they are potentially exposed to unauthorized access. Any kind of information leakage from such applications would seriously hurt the success of the shared-GPU computing model, where the term shared-GPU indicates all those scenarios where the GPU resource is actually shared among different users, whether it is on a local server, on a cluster machine or on a GPU cloud [10] (originating the GPU-as-a-Service —a specialization of the more general class Computing-as-a-Service).

GPUs are increasingly deployed as Computing-as-a-Service on the Cloud [11], [12]. In fact, sharing GPU resources brings several benefits such as sparing the cost involved in building and maintaining a HW/SW GPU

[1] This paper has been subject to a review process. The timeline is reported below:
2012-11-04: Submission to Transactions on Information Forensics And Security
2013-01-16: Decision to REVISE and RESUBMIT (T-IFS-03001-2012)
2013-02-27: Revised Manuscript Submitted (T-IFS-03001-2012.R1)
2013-05-28: REJECT AND RESUBMIT (RR) AS A REGULAR PAPER (T-IFS-03001-2012.R1)
2013-07-05: Withdrawn from IEEE TIFS, enhanced and submitted to Another Top Notch Transaction

arXiv:1308.0291v2 [math-ph] 12 Oct 2013

Schrödinger Equation on Fractals Curves Imbedding in R^3

Alireza Khalili Golmankhaneh [a†]
Dumitru Baleanu [b,c,d *]
[a]*Department of Physics, Islamic Azad University, Urmia Branch, PO Box 969, Urmia, Iran*
[†]E-mail:alirezakhalili2005@gmail.com
[b]*Department of Mathematics and Computer Science Çankaya University, 06530 Ankara, Turkey*
[c]*Institute of Space Sciences, P.O.BOX, MG-23, R76900, Magurele-Bucharest, Romania*
[d]*Department of Chemical and Materials Engineering, Faculty of Engineering, King Abdulaziz University, P.O. Box: 80204, Jeddah, 21589, Saudi Arabia*

October 15, 2013

Abstract

In this paper we have generalized the quantum mechanics on fractal time-space. The time is changing on Cantor-set like but space is considered as fractal curve like Von-Koch curve. The Feynman path method in quantum mechanics has been suggested on fractal curve. Using F^α-calculus and Feynman path method we found the Schrödinger on fractal time-space. The Hamiltonian operator and momentum operator has been derived. More, the continuity equation and the probability density is given in generalized formulation.

Keywords:Feynman path method, Schrödinger on fractal time-space,continuity equation

1 Introduction

Fractal is objects that are very fragmented and irregular at all scales. Their important properties are non-differentiability and having non-integer dimension. Fractal has topological dimension less than Hausdorff-Besicovitch, box-counting, and similarity dimensions. In general, dimension of fractal can be integer or not well-defined dimension [1–7]. Fractional local calculus and nonlocal has applied to model the process with memory and fractal structure [8–14]. The electric and magnetic fields are derived using fractional integrals as a approximation method on fractals [15]. The quantum space-time on the basis of relativity principle and geometrical concept of fractals is introduced [16].The probability density of quantum wave function with by Dirichlet boundary conditions in a D-dimensional spaces has been studied [17]. The fractal concept to quantum physics and the relationships between fractional integral and Feynman path integral method is developed [18,19]. The generalized wave functions is introduced to fractal dimension, a wide class of quantum problems, including the infinite potential well, harmonic oscillator, linear potential, and free particle [20].Fratal path in quantum mechanics and their contributing in Feynman path integral is investigated [21]. The classical mechanics is derived without the need of the least-action principle using path-integral approach [22]. The calculus on the fractals has been studied in different methods like probabilistic approach method, sequence of discrete Laplacians, measure-theoretical method, time scale calculus [23].Riemann integration like method has been studied since that is useful and algorithmic [24–29].Using the calculus on fractals the Newtonian mechanics, Lagrange and Hamilton mechanics, and Maxwell equations has been generalized [30–32]. As a pursue theses research we generalized the quantum mechanics on fractals.

The plan of this paper is as following:

Section 2 we review the fractal calculus. In section 3 we defined the gradient, divergent and Laplacian on fractal space. Section 4 is explained the quantum mechanics on fractals curves. In section 5 we suggested the probability density and continuity equation on the generalized quantum formalism. Finally, section 6 is devoted to conclusion.

*Tel:+903122844500, Fax:+903122868662
E-mail address: dumitru@cankaya.edu.tr

Has our brain grown too big to think effectively?

Konrad R. Fialkowski

University of Warsaw, Poland.

Mailing address: An den Langen Luessen 9/1/3; 1190 Wien, Austria
Fax: 431 3288689
e-mail: fialkows@aol.com

Abstract.

A variant of *microcephalin*, *MCPH1* gene, was introgressed about **37,000** years ago into *Homo sapiens* genetic pool from an archaic (*Homo erectus*) lineage and rose to exceptionally high frequency of around **70 percent worldwide** today. It is involved in regulating neuroblast proliferation and its changes alter the rate of division and/or differentiation of neuroblasts during the neurogenic phase of embriogenesis, which could alter the size and structure of the resulting brain.

At the time of introgression, images had already been painted on the walls of caves and speech has been in use for over 100,000 years, as had been abstract thinking. Like today, reasoning and thinking were the primary faculties of individuals. *Homo erectus* either did not possess those faculties or was markedly inferior to *Homo sapiens* in them. Its brain was smaller and the cortex was apparently less convoluted. Thus, introgressed *microcephalin* allele directed neurogenesis evolutionary back to less complicated brain structure typical for our evolutionary forefathers, slightly decreasing the level of complexity already achieved by *Homo sapiens* 37,000 years ago. Despite that, it proliferated at a rapid pace.

It yields a supposition: 37,000 years ago the brains of *Homo sapiens* were too big and too complicated for the kind of thinking needed for the highest fitness of individuals. Since adaptation cannot by definition surpass selection requirements, **the volume and complication of the human brain did not originate under selective pressure to improve effective thinking** and they cannot **be explained in terms of such selection.**

A proposal to solve this quandary is presented, claiming **that *Homo sapiens* originated just by chance**. Endurance running led to the emergence of *Homo sapiens*. The human mind and larynx used for speech are side-effects of more than a million years of endurance running by pre-human hunters.

arXiv:1311.1086v2 [cond-mat.mes-hall] 22 Jan 2014

Tunable transport with broken space-time symmetries

Sergey Denisov[a,b,*], Sergej Flach[c], Peter Hänggi[b,d,e]

[a] *Sumy State University, Rimsky-Korsakov Street 2, 40007 Sumy, Ukraine*

[b] *Institut für Physik, Universität Augsburg, Universitätsstr.1, 86135 Augsburg, Germany*

[c] *New Zealand Institute for Advanced Study, Centre for Theoretical Chemistry and Physics, Massey University, Private Bag 102 904 NSMCS, 0746 Auckland, New Zealand*

[d] *Center for Phononics and Thermal Energy Science, School of Physics Science and Engineering, Tongji University, 200092 Shanghai, China*

[e] *Nanosystems Initiative Munich, Schellingstr. 4, D-80799 München, Germany*

Abstract

Transport properties of particles and waves in spatially periodic structures that are driven by external time-dependent forces manifestly depend on the space-time symmetries of the corresponding equations of motion. A systematic analysis of these symmetries uncovers the conditions necessary for obtaining directed transport. In this work we give a unified introduction into the symmetry analysis and demonstrate its action on the motion in one-dimensional periodic, both in time and space, potentials. We further generalize the analysis to quasi-periodic drives, higher space dimensions, and quantum dynamics. Recent experimental results on the transport of cold and ultracold atomic ensembles in ac-driven optical potentials are reviewed as illustrations of theoretical considerations.

Keywords: nonlinear dynamics, ratchet effect, Hamiltonian chaos, Floquet theory, quantum optics

Contents

1 Introduction **3**

2 Symmetries in a nutshell **4**

2.1 Symmetries of periodic functions 5

2.2 Symmetries of quasiperiodic functions 6

2.3 An example: Hamiltonian ratchets 7

*Corresponding author. Tel.: +49-821-598-3228

E-mail address: sergey.denisov@physik.uni-augsburg.de

arXiv:1312.1027v3 [cs.CC] 11 Dec 2013

A Note on the Quantum Collision and Set Equality Problems

Mark Zhandry
Stanford University, USA
mzhandry@stanford.edu

Abstract

The results showing a quantum query complexity of $\Theta(N^{1/3})$ for the collision problem do not apply to random functions. The issues are two-fold. First, the $\Omega(N^{1/3})$ lower bound only applies when the range is no larger than the domain, which precludes many of the cryptographically interesting applications. Second, most of the results in the literature only apply to r-to-1 functions, which are quite different from random functions.

Understanding the collision problem for random functions is of great importance to cryptography, and we seek to fill the gaps of knowledge for this problem. To that end, we prove that, as expected, a quantum query complexity of $\Theta(N^{1/3})$ holds for all interesting domain and range sizes. Our proofs are simple, and combine existing techniques with several novel tricks to obtain the desired results.

Using our techniques, we also give an optimal $\Omega(N^{1/3})$ lower bound for the set equality problem. This new lower bound can be used to improve the relationship between classical randomized query complexity and quantum query complexity for so-called permutation-symmetric functions.

1 Introduction

A *collision* for a function f consists of two distinct inputs $x_1, x_2, x_1 \neq x_2$ that map to the same value: $f(x_1) = f(x_2)$. In this note, we explore the difficulty of computing collisions in the quantum query model: how many quantum queries to an unknown function f are required to produce a collision? Let M be the size of the domain of f, and N be the size of the codomain.

Brassard, Høyer, and Tapp [BHT97] give a quantum algorithm (henceforth called the BHT algorithm) requiring $O(M^{1/3})$ quantum queries to any two-to-one function f to produce a collision with overwhelming probability. Ambainis [Amb03] gives an $O(M^{2/3})$ algorithm (which we will call Ambainis's algorithm) for finding a collision in an arbitrary function f, guaranteed that it contains at least one collision. This latter problem is related to the so-called element distinctness problem, where one is asked to distinguish between an injective function and a function with a single collision.

On the lower bound side, most of the prior work has also focused on two-to-one functions. In the case where the domain and co-domain are the same, Aaronson and Shi [AS04] and Ambainis [Amb05] prove an $\Omega(N^{1/3}) = \Omega(M^{1/2})$ lower bound for two-to-one functions. The results also generalize to r-to-one functions. These results also imply an $\Omega(M^{2/3})$ lower bound for the element distinctness problem.

While the above results provide matching upper and lower bounds for the problems they analyze, they have a couple crucial limitations:

arXiv:1312.3395v1 [quant-ph] 12 Dec 2013

Local $\mathcal{PT}$ symmetry violates the no-signaling principle

Yi-Chan Lee,[1,2,*] Min-Hsiu Hsieh,[2] Steven T. Flammia,[3] and Ray-Kuang Lee[1,4]

[1]*Physics Department, National Tsing-Hua University, Hsinchu City 300, Taiwan*
[2]*Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology, Sydney, NSW 2007, Australia*
[3]*School of Physics, University of Sydney, Sydney, NSW 2006, Australia*
[4]*Institute of Photonics Technologies, National Tsing-Hua University, Hsinchu City 300, Taiwan*

(Dated: December 13, 2013)

Bender *et al.* [1] have developed $\mathcal{PT}$-symmetric quantum theory as an extension of quantum theory to non-Hermitian Hamiltonians. We show that when this model has a local $\mathcal{PT}$ symmetry acting on composite systems it violates the no-signaling principle of relativity. Since the case of global $\mathcal{PT}$ symmetry is known to reduce to standard quantum mechanics [2], this shows that the $\mathcal{PT}$-symmetric theory is either a trivial extension or likely false as a fundamental theory.

The Hermiticity of Hamiltonians—and indeed observables in general—is one of the fundamental postulates of quantum mechanics. There are two reasons for this restriction: first, a Hermitian Hamiltonian guarantees that the energy of the physical system described by it is always real. Second, based on the Schrödinger equation, the Hermiticity implies that the time-evolution operator generated by a Hamiltonian is unitary, which ensures conservation of probabilities for the time-evolved quantum state.

Nonetheless, non-Hermitian Hamiltonians are still useful in theoretical work and are a mathematical tool for studying open quantum systems in nuclear physics [3] or quantum optics [4], among others. In these fields, the whole physical system is still considered to obey conventional quantum mechanics, and the non-Hermitian Hamiltonian only comes out as an effective subsystem within a projective subspace.

In 1998, Bender and colleagues proposed a class of non-Hermitian Hamiltonians with a real energy spectrum as a fundamental, non-effective model beyond standard quantum theory [1]. By redefining the inner product, the time evolution operator generated by such a Hamiltonian could be unitary [5]. Their proposal reveals the possibility to remove the restriction of Hamiltonians from Hermiticity to a weaker parity-time ($\mathcal{PT}$) symmetry, where parity-time means spatial reflection and time reversal. In other words, it might be possible to have a physical system described by a non-Hermitian Hamiltonian. They showed that when the eigenstates of a $\mathcal{PT}$-symmetric system are also $\mathcal{PT}$ symmetric, the energy eigenvalues are always real. When the eigenstates are no longer $\mathcal{PT}$ symmetric, the energy becomes complex and is called spontaneous ($\mathcal{PT}$) symmetry breaking.

This proposal led to a flurry of activity investigating the strange properties of $\mathcal{PT}$-symmetric Hamiltonians. Especially in optical systems, since the paraxial equation is equivalent to Schrödinger's equation, various *effective* models were proposed to simulate $\mathcal{PT}$-symmetric Hamiltonian dynamics [6]. A $\mathcal{PT}$-symmetric Hamiltonian was successfully simulated in optics experiments by using coupling optical channels in 2010, and the spontaneous breaking of $\mathcal{PT}$ symmetry was also observed in this system [7]. Besides these discoveries, many optical applications of $\mathcal{PT}$-symmetric Hamiltonians were also proposed, such as unidirectional optical valves [8], perfect laser absorbers [9], unidirectional invisible media [10], and spatial optical switches [11]. The applications of $\mathcal{PT}$-symmetric Hamiltonians in these optical systems are all classical and, to the extent that they were realized, were effective models. However, in the quantum regime Bender and others proposed two interesting applications related to quantum computation: ultrafast quantum state transformation [12] and quantum state discrimination with single-shot measurement [13], which also inspired much investigation of "shortcut" quantum time evolution [14, 15].

It is well known that in conventional quantum mechanics the time to evolve between two orthogonal states is limited by the uncertainty principle [16, 17], and only orthogonal states can be distinguished perfectly with a single-copy measurement [18]. Both of these limitations are entirely absent in $\mathcal{PT}$-symmetric quantum theory because the following two assumptions are built in:

1. There exists an local quantum system described by a $\mathcal{PT}$-symmetric Hamiltonian and it can coexist with a conventional quantum system.

2. Post-measurement probability distributions are computed using conventionally normalized quantum states.

These two assumptions are implicitly made in [12, 13] and present a clear departure from standard quantum mechanics, but so far have not been tested. The existing experimental realizations of $\mathcal{PT}$-symmetric evolutions are either classical simulations or conditioned evolution in conventional quantum theory [7, 19]. Some theoretical scrutiny has shown that a *globally* $\mathcal{PT}$-symmetric system is conventional quantum mechanics in disguise with a different inner product definition, and in finite-dimensional systems $\mathcal{PT}$-symmetric Hamiltonians are actually a specific class of pseudo-Hermitian Hamiltonians in one-to-one correspondence with Hermitian Hamiltonians via a similarity transformation [2]. This equivalence indicates that if $\mathcal{PT}$-symmetric quantum symmetry can only describe physical systems globally then it would be unnecessary for us to consider this theory except for potentially simplifying calculations. From this point of view, whether $\mathcal{PT}$-symmetric

SoK: Eternal War in Memory

László Szekeres[†], Mathias Payer[‡], Tao Wei[*‡], Dawn Song[‡]
[†]*Stony Brook University*
[‡]*University of California, Berkeley*
[*]*Peking University*

***Abstract*—Memory corruption bugs in software written in low-level languages like C or C++ are one of the oldest problems in computer security. The lack of safety in these languages allows attackers to alter the program's behavior or take full control over it by hijacking its control flow. This problem has existed for more than 30 years and a vast number of potential solutions have been proposed, yet memory corruption attacks continue to pose a serious threat. Real world exploits show that all currently deployed protections can be defeated.**

This paper sheds light on the primary reasons for this by describing attacks that succeed on today's systems. We systematize the current knowledge about various protection techniques by setting up a general model for memory corruption attacks. Using this model we show what policies can stop which attacks. The model identifies weaknesses of currently deployed techniques, as well as other proposed protections enforcing stricter policies.

We analyze the reasons why protection mechanisms implementing stricter polices are not deployed. To achieve wide adoption, protection mechanisms must support a multitude of features and must satisfy a host of requirements. Especially important is performance, as experience shows that only solutions whose overhead is in reasonable bounds get deployed.

A comparison of different enforceable policies helps designers of new protection mechanisms in finding the balance between effectiveness (security) and efficiency. We identify some open research problems, and provide suggestions on improving the adoption of newer techniques.

I. Introduction

Memory corruption bugs are one of the oldest problems in computer security. Applications written in low-level languages like C or C++ are prone to these kinds of bugs. The lack of memory safety (or type safety) in such languages enables attackers to exploit memory bugs by maliciously altering the program's behavior or even taking full control over the control-flow. The most obvious solution would be to avoid these languages and to rewrite vulnerable applications in type-safe languages. Unfortunately, this is unrealistic not only due to the billions of lines of existing C/C++ code, but also due to the low-level features needed for performance critical programs (e.g. operating systems).

The war in memory is fought on one side by offensive research that develops new attacks and malicious attackers, and on the other side by defensive researchers who develop new protections and application programmers who try to write safe programs. The memory war effectively is an arms race between offense and defense. According to the MITRE ranking [1], memory corruption bugs are considered one of the top three most dangerous software errors. Google Chrome, one of the most secure web browsers written in C++, was exploited four times during the Pwn2Own/Pwnium hacking contests in 2012.

In the last 30 years a set of defenses has been developed against memory corruption attacks. Some of them are deployed in commodity systems and compilers, protecting applications from different forms of attacks. Stack cookies [2], exception handler validation [3], Data Execution Prevention [4] and Address Space Layout Randomization [5] make the exploitation of memory corruption bugs much harder, but several attack vectors are still effective under all these currently deployed basic protection settings. Return-Oriented Programming (ROP) [6], [7], [8], [9], [10], [11], information leaks [12], [13] and the prevalent use of user scripting and just-in-time compilation [14] allow attackers to carry out practically any attack despite all protections.

A multitude of defense mechanisms have been proposed to overcome one or more of the possible attack vectors. Yet most of them are not used in practice, due to one or more of the following factors: the *performance* overhead of the approach outweighs the potential protection, the approach is not *compatible* with all currently used features (e.g., in legacy programs), the approach is not *robust* and the offered protection is not complete, or the approach *depends* on changes in the compiler toolchain or in the source-code while the toolchain is not publicly available.

With all the diverse attacks and proposed defenses it is hard to see how effective and how efficient different solutions are and how they compare to each other and what the primary challenges are. The motivation for this paper is to systematize and evaluate previously proposed approaches. The systematization is done by setting up a general model for memory corruption vulnerabilities and exploitation techniques. The defense techniques are classified by the exploits they mitigate and by the particular phase of exploit they try to inhibit. The evaluation is based on robustness, performance and compatibility. Using this evaluation, we also discuss common criteria that need to be fulfilled for successful deployment of a new software defense.

*Corresponding author.

arXiv:1401.2026v2 [gr-qc] 10 Jun 2014

Quantum fields in curved spacetime

June 11, 2014

Abstract

We review the theory of quantum fields propagating in an arbitrary, classical, globally hyperbolic spacetime. Our review emphasizes the conceptual issues arising in the formulation of the theory and presents known results in a mathematically precise way. Particular attention is paid to the distributional nature of quantum fields, to their local and covariant character, and to microlocal spectrum conditions satisfied by physically reasonable states. We review the Unruh and Hawking effects for free fields, as well as the behavior of free fields in deSitter spacetime and FLRW spacetimes with an exponential phase of expansion. We review how nonlinear observables of a free field, such as the stress-energy tensor, are defined, as well as time-ordered-products. The "renormalization ambiguities" involved in the definition of time-ordered products are fully characterized. Interacting fields are then perturbatively constructed. Our main focus is on the theory of a scalar field, but a brief discussion of gauge fields is included. We conclude with a brief discussion of a possible approach towards a nonperturbative formulation of quantum field theory in curved spacetime and some remarks on the formulation of quantum gravity.

[1]Universität Leipzig, Institut für Theoretische Physik, Brüderstrasse 16, D-04103 Leipzig, FRG

[2]Enrico Fermi Institute and Department of Physics, University of Chicago, Chicago, IL 60637, USA

arXiv:1401.4356v1 [quant-ph] 16 Jan 2014

Why bouncing droplets are a pretty good model of quantum mechanics

Robert Brady and Ross Anderson
University of Cambridge Computer Laboratory
JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
{robert.brady,ross.anderson}@cl.cam.ac.uk

January 20, 2014

Abstract

In 2005, Couder, Protière, Fort and Badoual showed that oil droplets bouncing on a vibrating tray of oil can display nonlocal interactions reminiscent of the particle-wave associations in quantum mechanics; in particular they can move, attract, repel and orbit each other. Subsequent experimental work by Couder, Fort, Protière, Eddi, Sultan, Moukhtar, Rossi, Moláček, Bush and Sbitnev has established that bouncing drops exhibit single-slit and double-slit diffraction, tunnelling, quantised energy levels, Anderson localisation and the creation/annihilation of droplet/bubble pairs.

In this paper we explain why. We show first that the surface waves guiding the droplets are Lorentz covariant with the characteristic speed c of the surface waves; second, that pairs of bouncing droplets experience an inverse-square force of attraction or repulsion according to their relative phase, and an analogue of the magnetic force; third, that bouncing droplets are governed by an analogue of Schrödinger's equation where Planck's constant is replaced by an appropriate constant of the motion; and fourth, that orbiting droplet pairs exhibit spin-half symmetry and align antisymmetrically as in the Pauli exclusion principle. Our analysis explains the similarities between bouncing-droplet experiments and the behaviour of quantum-mechanical particles. It also enables us to highlight some differences, and to predict some surprising phenomena that can be tested in feasible experiments.

1 Introduction

In 1978 Walker reported that a droplet of soapy water could bounce for several minutes on a vibrating dish of the same fluid [1]. In 2005 Couder, Protière, Fort and Badouad started the systematic study of this phenomenon using droplets of silicone oil; the droplets can be made to bounce indefinitely on an oil surface that is vibrated vertically, and with the right amplitude and frequency of vibration, droplets can move laterally or 'walk' [2]. A thin film of air between the droplet and the surface prevents coalescence.

Figure 1 illustrates the apparatus, figure 2 has six photographs of a bouncing droplet, and figure 3 illustrates the vertical motion as a function of time. Here the droplet touches down every other cycle; at lower driving amplitudes there are less interesting modes of bouncing, where the droplet grazes off the peak near f in the figure or touches down every cycle.

These experiments have since been reproduced in laboratories around the world, such as by Moláček and Bush [3], and have appeared on TV [4]. They are of interest because the droplets exhibit much of the behaviour that had

arXiv:1402.3668v3 [math.NT] 12 Jun 2014

Breaking '128-bit Secure' Supersingular Binary Curves*

(or how to solve discrete logarithms in $\mathbb{F}_{2^{4\cdot 1223}}$ and $\mathbb{F}_{2^{12\cdot 367}}$)

Robert Granger[1], Thorsten Kleinjung[1], and Jens Zumbrägel[2]

[1] Laboratory for Cryptologic Algorithms, EPFL, Switzerland
[2] Institute of Algebra, TU Dresden, Germany
robbiegranger@gmail.com, thorsten.kleinjung@epfl.ch, jens.zumbragel@uc0.te

Abstract. In late 2012 and early 2013 the discrete logarithm problem (DLP) in finite fields of small characteristic underwent a dramatic series of breakthroughs, culminating in a heuristic quasi-polynomial time algorithm, due to Barbulescu, Gaudry, Joux and Thomé. Using these developments, Adj, Menezes, Oliveira and Rodríguez-Henríquez analysed the concrete security of the DLP, as it arises from pairings on (the Jacobians of) various genus one and two supersingular curves in the literature, which were originally thought to be 128-bit secure. In particular, they suggested that the new algorithms have no impact on the security of a genus one curve over $\mathbb{F}_{2^{1223}}$, and reduce the security of a genus two curve over $\mathbb{F}_{2^{367}}$ to 94.6 bits. In this paper we propose a new field representation and efficient general descent principles which together make the new techniques far more practical. Indeed, at the '128-bit security level' our analysis shows that the aforementioned genus one curve has approximately 59 bits of security, and we report a total break of the genus two curve.

Keywords: Discrete logarithm problem, finite fields, supersingular binary curves, pairings

1 Introduction

The role of small characteristic supersingular curves in cryptography has been a varied and an interesting one. Having been eschewed by the cryptographic community for succumbing spectacularly to the subexponential MOV attack in 1993 [40], which maps the DLP from an elliptic curve (or more generally, the Jacobian of a higher genus curve) to the DLP in a small degree extension of the base field of the curve, they made a remarkable comeback with the advent of pairing-based cryptography in 2001 [42,31,9]. In particular, for the latter it was reasoned that the existence of a subexponential attack on the DLP does not *ipso facto* warrant their complete exclusion; rather, provided that the finite field DLP into which the elliptic curve DLP embeds is sufficiently hard, this state of affairs would be acceptable.

Neglecting the possible existence of native attacks arising from the supersingularity of these curves, much research effort has been expended in making instantiations of the required cryptographic operations on such curves as efficient as possible [6,17,14,28,27,5,30,7,11,18,3,1], to name but a few, with the associated security levels having been estimated using Coppersmith's algorithm from 1984 [12,39]. Alas, a series of dramatic breakthrough results for the DLP in finite fields of small characteristic have potentially rendered all of these efforts in vain.

The first of these results was due to Joux, in December 2012, and consisted of a more efficient method — dubbed 'pinpointing' — to obtain relations between factor base elements [32]. For medium-sized base fields, this technique has heuristic complexity as low as $L(1/3, 2^{1/3}) \approx L(1/3, 1.260)$[†], where as usual $L(\alpha, c) = L_Q(\alpha, c) = \exp((c + o(1))(\log Q)^{\alpha}(\log\log Q)^{1-\alpha})$, with

* The second author acknowledges the support of the Swiss National Science Foundation, via grant numbers 200021-128727 and 200020-132160, while the third author acknowledges the support of the Irish Research Council, grant number ELEVATEPD/2013/82.

† The original paper states a complexity of $L(1/3, (8/9)^{1/3}) \approx L(1/3, 0.961)$; however, on foot of recent communications the constant should be as stated.

arXiv:1404.1207v1 [gr-qc] 4 Apr 2014

Spontaneous creation of the universe from nothing

Dongshan He,[1,2] Dongfeng Gao,[1] and Qing-yu Cai[1,*]

[1]State Key Laboratory of Magnetic Resonances and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan 430071, China
[2]Graduate University of the Chinese Academy of Sciences, Beijing 100049, China

An interesting idea is that the universe could be spontaneously created from nothing, but no rigorous proof has been given. In this paper, we present such a proof based on the analytic solutions of the Wheeler-DeWitt equation (WDWE). Explicit solutions of the WDWE for the special operator ordering factor $p = -2$ (or 4) show that, once a small true vacuum bubble is created by quantum fluctuations of the metastable false vacuum, it can expand exponentially no matter whether the bubble is closed, flat or open. The exponential expansion will end when the bubble becomes large and thus the early universe appears. With the de Broglie-Bohm quantum trajectory theory, we show explicitly that it is the quantum potential that plays the role of the cosmological constant and provides the power for the exponential expansion of the true vacuum bubble. So it is clear that the birth of the early universe completely depends on the quantum nature of the theory.

PACS numbers: 98.80.Cq, 98.80.Qc

I. INTRODUCTION

With the lambda-cold dark matter (ΛCDM) model and all available observations (cosmic microwave background, abundance of light elements), it has been widely accepted that the universe was created in a big bang. However, there are still some puzzles, such as problems of the flatness, the horizon, the monopole, and the singularity [1]. Quantum mechanics has been applied to cosmology to study the formation of the universe and its early evolution. In particular, inflation theories, which suggest that the universe experienced an exponential expansion period, were proposed to solve puzzles of the early universe [2–4]. In quantum cosmology theory, the universe is described by a wave function rather than the classical spacetime. The wave function of the universe should satisfy the Wheeler-DeWitt equation (WDWE) [5]. With the development of quantum cosmology theory, it has been suggested that the universe can be created spontaneously from nothing, where "nothing" means there is neither matter nor space or time [6], and the problem of singularity can be avoided naturally.

Although the picture of the universe created spontaneously from nothing has emerged for a long time, a rigorous mathematical foundation for such a picture is still missing. According to Heisenberg's uncertainty principle, a small empty space, also called a small true vacuum bubble, can be created probabilistically by quantum fluctuations of the metastable false vacuum. But if the small bubble cannot expand rapidly, it will disappear soon due to quantum fluctuations. In this case, the early universe would disappear before it grows up. On the other side, if the small bubble expands rapidly to a large enough size, the universe can then be created irreversibly.

In this paper, we obtain analytic solutions of the WDWE of the true vacuum bubble. With the de Broglie-Bohm quantum trajectory theory, we prove that once a small true vacuum bubble is created, it has the chance to expand exponentially when it is very small, *i.e.*, $a \ll 1$. The exponential expansion will end when the true vacuum bubble becomes very large, *i.e.*, $a \gg 1$. It is the quantum potential of the small true vacuum bubble that plays the role of the cosmological constant and provides the power for its exponential expansion. This explicitly shows that the universe can be created spontaneously by virtue of a quantum mechanism.

II. WDWE FOR THE SIMPLEST MINISUPERSPACE MODEL

Heisenberg's uncertainty principle indicates that a small true vacuum bubble can be created probabilistically in a metastable false vacuum. The small bubble has 1 degree of freedom, the bubble radius. We can assume that the bubble is nearly spherical, isotropic and homogeneous, since it is a small true vacuum bubble. As we will show below, the small bubble will expand exponentially after its birth and all asymmetries will be erased by the inflation.

Since the small true vacuum bubble is nearly spherical, it can be described by a minisuperspace model [7–9] with one single parameter of the scalar factor a. The action of the minisuperspace can be written as

$$S = \frac{1}{16\pi G}\int R\sqrt{-g}d^4x. \tag{1}$$

Since the bubble is homogeneous and isotropic, the metric in the minisuperspace model is given by

$$ds^2 = \sigma^2[N^2(t)dt^2 - a^2(t)d\Omega_3^2]. \tag{2}$$

Here, $N(t)$ is an arbitrary lapse function, $d\Omega_3^2$ is the metric on a unit three-sphere, and $\sigma^2 = 2G/3\pi$ is a normalizing factor chosen for later convenience. Substituting Eq.

*Corresponding author. Electronic address: qycai@wipm.ac.cn

arXiv:1404.6551v2 [quant-ph] 13 Aug 2014

Differentiable-Path Integrals in Quantum Mechanics

Benjamin Koch* and Ignacio Reyes*
* *Instituto de Física,*
Pontificia Universidad Católica de Chile,
Av. Vicuña Mackenna 4860,
Santiago, Chile

(Dated: August 14, 2014)

A method is presented which restricts the space of paths entering the path integral of quantum mechanics to subspaces of C^n, by only allowing paths which possess at least n derivatives. The method introduces two external parameters, and induces the appearance of a particular time scale ϵ_D such that for time intervals longer than ϵ_D the model behaves as usual quantum mechanics. However, for time scales smaller than ϵ_D, modifications to standard formulation of quantum theory occur. This restriction renders convergent some quantities which are usually divergent in the time-continuum limit $\epsilon \to 0$. We illustrate the model by computing several meaningful physical quantities such as the mean square velocity $\langle v^2 \rangle$, the canonical commutator, the Schrodinger equation and the energy levels of the harmonic oscillator. It is shown that an adequate choice of the parameters introduced makes the evolution unitary.

PACS numbers:

I. INTRODUCTION

What are the relevant trajectories in the path integral approach to quantum mechanics? The path integral (PI) method, envisioned by Dirac and developed by Feynman [1, 2] is defined by a summation over all possible histories or configurations going from an initial to a final state. For the case of quantum mechanics this means a summation over all continuos functions connecting two events in space-time. However some natural questions arise at a very early stage, for example: are all paths relevant, important, or even necessary to define a consistent quantum theory? How do different "classes" of paths contribute to the path integral? What is the effect of leaving some paths out? Specifically, what is the role of the highly irregular/nowhere-differentiable paths in this summation? The topic regarding this last question was already discussed in [2], and thereafter further developed by many others [2–8]: *"The important paths for a quantum mechanical particle are not those which have a definite slope (or velocity)... Typical paths of a quantum mechanical particle are highly irregular on a fine scale... In other words, the paths are nondifferentiable."*[2]

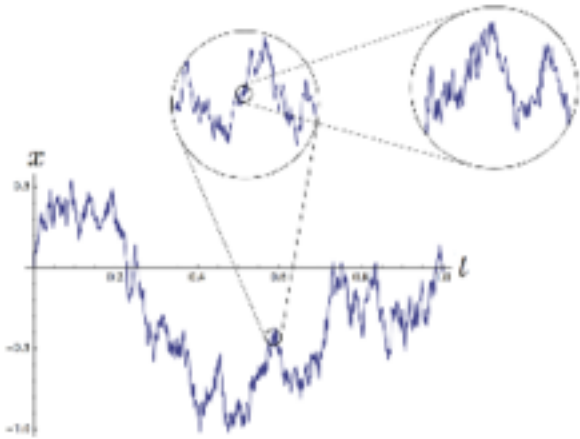


FIG. 1: typical quantum trajectory in Feynman's approach: curves are continuos but nowhere-differentiable.

From this analysis there has arisen a mainstream point of view, which may be summarized in three key statements:

arXiv:1404.6898v2 [quant-ph] 19 Oct 2014

Quantum Attacks on Classical Proof Systems

The Hardness of Quantum Rewinding

Andris Ambainis
University of Latvia and
Institute for Advanced Study
Princeton

Ansis Rosmanis
Institute for Quantum Computing
School of Computer Science
University of Waterloo

Dominique Unruh
University of Tartu

October 21, 2014

Abstract. Quantum zero-knowledge proofs and quantum proofs of knowledge are inherently difficult to analyze because their security analysis uses rewinding. Certain cases of quantum rewinding are handled by the results by Watrous (SIAM J Comput, 2009) and Unruh (Eurocrypt 2012), yet in general the problem remains elusive. We show that this is not only due to a lack of proof techniques: relative to an oracle, we show that classically secure proofs and proofs of knowledge are insecure in the quantum setting.

More specifically, sigma-protocols, the Fiat-Shamir construction, and Fischlin's proof system are quantum insecure under assumptions that are sufficient for classical security. Additionally, we show that for similar reasons, computationally binding commitments provide almost no security guarantees in a quantum setting.

To show these results, we develop the "pick-one trick", a general technique that allows an adversary to find one value satisfying a given predicate, but not two.

Contents

1 Introduction **2**

2 Preliminaries **8**
2.1 Security definitions 9

3 State creation oracles **12**

4 The pick-one trick **14**
4.1 Additional oracles 15

5 Attacking commitments **17**

6 Attacking sigma-protocols **19**
6.1 The computational case . 21

7 Attacking Fiat-Shamir **22**
7.1 The computational case . 23

8 Attacking Fischlin's scheme **23**
8.1 The computational case . 24

References **25**

Symbol index **28**

Keyword index **30**

A Auxiliary lemmas **31**

arXiv:1405.4772v3 [quant-ph] 28 Nov 2014

Bohm's approach and individuality.

P. Pylkkänen[1,2], B. J. Hiley[3] and I. Pättiniemi[1].

1. Department of Philosophy, History, Culture and Art Studies & The Finnish Center of Excellence in the Philosophy of the Social Sciences (TINT), University of Helsinki, Finland
2. Department of Cognitive Neuroscience and Philosophy, University of Skövde, Sweden
3. TPRU, Birkbeck, University of London, Malet Street, London WC1E 7HX.

(15 November 2014)

Abstract

Ladyman and Ross (LR) argue that quantum objects are not individuals (or are at most weakly discernible individuals) and use this idea to ground their metaphysical view, ontic structural realism, according to which relational structures are primary to things. LR acknowledge that there is a version of quantum theory, namely the Bohm theory (BT), according to which particles do have definite trajectories at all times. However, LR interpret the research by Brown *et al.* as implying that "raw stuff" or *haecceities* are needed for the individuality of particles of BT, and LR dismiss this as idle metaphysics. In this paper we note that Brown *et al.*'s research does not imply that *haecceities* are needed. Thus BT remains as a genuine option for those who seek to understand quantum particles as individuals. However, we go on to discuss some problems with BT which led Bohm and Hiley to modify it. This modified version underlines that, due to features such as context-dependence and non-locality, Bohmian particles have a very limited autonomy in situations where quantum effects are non-negligible. So while BT restores the possibility of quantum individuals, it also underlines the primacy of the whole over the autonomy of the parts. The later sections of the paper also examine the Bohm theory in the general mathematical context of symplectic geometry. This provides yet another way of understanding the subtle, holistic and dynamic nature of Bohmian individuals. We finally briefly consider Bohm's other main line of research, the "implicate order", which is in some ways similar to LR's structural realism.

arXiv:1406.2310v3 [quant-ph] 12 Mar 2015

First Quantized Pair Interactions

A. F. Bennett*

College of Earth, Ocean and Atmospheric Sciences

Oregon State University

104 CEOAS Administration Building

Corvallis, OR 97331-5503, USA

(Dated: March 13, 2015)

The parametrized Dirac wave equation for multiple particles is shown here to yield the standard cross sections for creation and annihilation of fermion pairs, while avoiding the paradoxes arising from the standard single-particle Dirac equation and hole theory. These paradoxes were originally overcome with Quantum Field Theory. The creation and annihilation operators of Quantum Field Theory are subject to causality conditions which preclude entanglement across distances greater than the order of the Compton wavelength. The parametrized first-quantized formalism requires no causality condition for fermions, and it admits fermion entanglement across all of space and time, while ensuring covariant Dyson series and $\mathcal{TPC}$ invariance.

* afbennett97330@post.harvard.edu

ANALYSIS OF RSA ALGORITHM USING GPU PROGRAMMING

Sonam Mahajan[1] and Maninder Singh[2]
[1]Department of Computer Science Engineering, Thapar University, Patiala, India
sonam_mahajan1990@yahoo.in
[2] Department of Computer Science Engineering, Thapar University, Patiala, India
msingh@thapar.edu

ABSTRACT

Modern-day computer security relies heavily on cryptography as a means to protect the data that we have become increasingly reliant on. The main research in computer security domain is how to enhance the speed of RSA algorithm. The computing capability of Graphic Processing Unit as a co-processor of the CPU can leverage massive-parallelism. This paper presents a novel algorithm for calculating modulo value that can process large power of numbers which otherwise are not supported by built-in data types. First the traditional algorithm is studied. Secondly, the parallelized RSA algorithm is designed using CUDA framework. Thirdly, the designed algorithm is realized for small prime numbers and large prime number . As a result the main fundamental problem of RSA algorithm such as speed and use of poor or small prime numbers that has led to significant security holes, despite the RSA algorithm's mathematical soundness can be alleviated by this algorithm.

KEYWORDS

CPU, GPU, CUDA, RSA, Cryptographic Algorithm.

1. INTRODUCTION

RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman [1]) is a public key encryption scheme. This algorithm relies on the difficulty of factoring large numbers which has seriously affected its performance and so restricts its use in wider applications. Therefore, the rapid realization and parallelism of RSA encryption algorithm has been a prevalent research focus. With the advent of CUDA technology, it is now possible to perform general-purpose computation on GPU [2]. The primary goal of our work is to speed up the most computationally intensive part of their process by implementing the GCD comparisons of RSA keys using NVIDIA's CUDA platform.

The reminder of this paper is organized as follows. In section 2,3,4, we study the traditional RSA algorithm. In section 5, we explained our system hardware. In section 6,7,8, 9 we explained the design and implementation of parallelized algorithm. Section 10 gives the result of our parallelized algorithm and section 12 concludes the paper.

2. TRADITIONAL RSA ALGORITHM[1]

RSA is an algorithm for public-key cryptography [1] and is considered as one of the great advances in the field of public key cryptography. It is suitable for both signing and encryption. Electronic commerce protocols mostly rely on RSA for security. Sufficiently long keys and up-to-date implementation of RSA is considered more secure to use.

RSA is an asymmetric key encryption scheme which makes use of two different keys for encryption and decryption. The public key that is known to everyone is used for encryption. The messages encrypted using the public key can only be decrypted by using private key. The key generation process of RSA algorithm is as follows:

The public key is comprised of a modulus n of specified length (the product of primes p and q), and an exponent e. The length of n is given in terms of bits, thus the term "8-bit RSA key" refers to the number of bits which make up this value. The associated private key uses the same n, and another value d such that $d*e = 1 \bmod \varphi(n)$ where $\varphi(n) = (p - 1)*(q - 1)$ [3]. For a plaintext M and cipher text C, the encryption and decryption is done as follows:

$$C = M^e \bmod n,\ M = C^d \bmod n.$$

arXiv:1407.5886v1 [math-ph] 22 Jul 2014

Purely non-local Hamiltonian formalism, Kohno connections and ∨-systems

Alessandro Arsie* and Paolo Lorenzoni**

*Department of Mathematics and Statistics

University of Toledo, 2801 W. Bancroft St., 43606 Toledo, OH, USA

**Dipartimento di Matematica e Applicazioni

Università di Milano-Bicocca, Via Roberto Cozzi 53, I-20125 Milano, Italy

*alessandro.arsie@utoledo.edu, **paolo.lorenzoni@unimib.it

Abstract

In this paper, we extend purely non-local Hamiltonian formalism to a class of Riemannian F-manifolds, without assumptions on the semisimplicity of the product $\circ$ or on the flatness of the connection ∇. In the flat case we show that the recurrence relations for the principal hierarchy can be re-interpreted using a local and purely non-local Hamiltonian operators and in this case they split into two Lenard-Magri chains, one involving the even terms, the other involving the odd terms. Furthermore, we give an elementary proof that the Kohno property and the ∨-system condition are equivalent under suitable conditions and we show how to associate a purely non-local Hamiltonian structure to any ∨-system, including degenerate ones.

1 Introduction

The study of Frobenius manifolds is an important branch of modern mathematics, with relations with many areas, ranging from singularity theory and Coxeter groups to Gromov-Witten invariants and hierarchies of integrable PDEs (see [6]).

Frobenius manifolds are given by the data $(M, \eta, \circ, e, E)$, where M is a smooth manifold, η a nondegenerate metric, $\circ$ is a smooth commutative associative product on sections of TM, e is the unit vector field of $\circ$ and E is the Euler vector field. These structures are required to satisfy some further compatibility axioms.

arXiv:1408.5697v1 [quant-ph] 25 Aug 2014

Quantum Mechanics: Harbinger of a Non-Commutative Probability Theory?

B. J. Hiley*

TPRU, Birkbeck, University of London, Malet Street,
London WC1E 7HX.

Abstract

In this paper we discuss the relevance of the algebraic approach to quantum phenomena first introduced by von Neumann before he confessed to Birkoff that he no longer believed in Hilbert space. This approach is more general and allows us to see the structure of quantum processes in terms of non-commutative probability theory, a non-Boolean structure of the implicate order which contains Boolean substructures which accommodates the explicate classical world. We move away from mechanical 'waves' and 'particles' and take as basic what Bohm called a *structure process*. This enables us to learn new lessons that can have a wider application in the way we think of structures in language and thought itself.

1 Introduction

As Murry Gell-Mann [1] once wrote:-

> Quantum mechanics, that mysterious, confusing discipline, which none of us really understands but which we know how to use. It works perfectly, as far as we can tell, in describing physical reality, but it is a 'counter-intuitive' discipline, as social scientists would say. Quantum mechanics is not a theory, but rather a framework within which we believe a correct theory must fit.

The professional physicist still finds explaining exactly what the quantum formalism is telling us about Nature very difficult. We know that it is

*E-mail address b.hiley@bbk.ac.uk.

arXiv:1409.0213v2 [quant-ph] 4 Dec 2014

Classical entanglement: Oxymoron or resource?

Andrea Aiello[1,2,*] Falk Töppel[1,2,3], Christoph Marquardt[1,2], Elisabeth Giacobino[1,4], and Gerd Leuchs[1,2]
[1] *Max Planck Institute for the Science of Light, Günther-Scharowsky-Straße 1/Bau24, 91058 Erlangen, Germany*
[2] *Institute for Optics, Information and Photonics, University of Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany*
[3] *Erlangen Graduate School in Advanced Optical Technologies (SAOT), Paul-Gordan-Straße 6, 91052 Erlangen, Germany and*
[4] *Laboratoire Kastler Brossel, Université Pierre et Marie Curie, Ecole Normale Supérieure, CNRS, 4 place Jussieu, 75252 Paris Cedex 05, France*
(Dated: December 5, 2014)

In this work we review and further develop the controversial concept of "classical entanglement" in optical beams. We present a unified theory for different kinds of light beams exhibiting classical entanglement and we indicate several possible extensions of the concept. Our results shed new light upon the physics at the debated border between the classical and the quantum representations of the world.

I. INTRODUCTION

A composite physical system, namely one made of at least two identifiable parts, say A and B, which are denoted subsystems, can be prepared in such a way that the latter are not independent. In the realm of classical physics this means, for example, that the probability $P(a \in A, b \in B)$ for the events a, b associated to subsystems A, B, respectively, cannot be factored as $P(a \in A, b \in B) = P(a \in A)P(b \in B)$ [1]. Conversely, for a composite quantum system, statistical dependence of the subsystems A, B means that the state vector $|\Psi\rangle$ describing a physical state of the whole system, cannot be decomposed in the tensor product

$$|\Psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle, \tag{1}$$

where $|\psi_A\rangle$ represents the state of the subsystem A and $|\psi_B\rangle$ represents the state of the subsystem B. Here, we are not interested in the deep conceptual implications of Eq. (1) but follow, rather, the "die-hard pragmatist's" approach [2] and denote as *entangled* any state vector that does not factorizes as in Eq. (1); namely,

$$entangled \;=\; non\text{–}separable. \tag{2}$$

Traditionally, entanglement has been regarded either as a peculiar feature of quantum mechanics or, instead, as a powerful resource especially for quantum information science [3]. In this paper we adhere to the latter view and aim at showing how some potentially useful characteristics of *quantum* entanglement can be replicated in *classical* systems. In fact, our ultimate goal is *not* to replace or simulate entangled quantum systems with classical ones in some actual operations. Instead, the aim is to study how to make quantum entanglement potentialities accessible to classical physics applications as recently demonstrated, e.g., in classical polarization metrology [4].

Thus, the main purpose of this paper is to revisit the concept of the so-called "classical entanglement" in optics [5, 6], and to present a brief but comprehensive overview of it. We would like to stress that "classical entanglement" is *not* substitutive of bona fide quantum entanglement, but is a feature exhibited by some classical systems. In a sense, which will become more clear later, the name *classical entanglement* denotes the occurrence of some mathematical and physical aspects of quantum entanglement in classical beams of light. In this sense, classical entanglement should not be confused with "entanglement simulations in classical optics", namely the use of classical fields to reproduce non-classical correlations between distinct measurement apparatuses [7, 8]. In any case, classical entanglement does not belong to the rich field of studies denoted by the name "quantum-classical analogies" [9–11]. A precise definition of what is usually meant with "classical entanglement", will be given in Sect. 2.

As a final important remark, the term "classical" in the name *classical entanglement*, indicates the non-quantum nature of the excitation of the electromagnetic field. In this paper, typically, we deal with bright beams of light as, e.g., laser beams. However, whether the beam is very intense or very weak, is a factor that has not influence upon classical entanglement, as it will be shown in Sect. 2. Yet, it should be noticed that single-photon excitations permit only the quantum mechanical representation as Fock states and, therefore, will not be considered here. However, it has been recently demonstrated that single photons can be prepared in a quantum state entangled with the vacuum [12–16]. Single-photon-vacuum entanglement resembles classical entanglement in that there is only one individual physical system, a single-photon in the quantum case and a single bright beam in the classical one, and two (or more) entangled modes of the electromagnetic field [17–19]. This concept will be further discussed in the next section.

* andrea.aiello@mpl.mpg.de

arXiv:1409.3727v1 [cond-mat.quant-gas] 12 Sep 2014

Phase space manipulations of many-body wavefunctions

G. Condon, A. Fortun, J. Billy, and D. Guéry-Odelin
Université de Toulouse ; UPS ; Laboratoire Collisions Agrégats Réactivité, IRSAMC ; F-31062 Toulouse, France and CNRS ; UMR 5589 ; F-31062 Toulouse, France

We explore the manipulation in phase space of many-body wavefunctions that exhibit self-similar dynamics, under the application of sudden force and/or in the presence of a constant acceleration field. For this purpose, we work out a common theoretical framework based on the Wigner function. We discuss squeezing in position space, phase space rotation and its implications in cooling for both non-interacting and interacting gases, and time reversal operation. We discuss various optical analogies and calculate the role of spherical-like aberration in cooling protocols. We also present the equivalent of a spin-echo technique to improve the robustness of velocity dispersion reduction protocols.

Phase space manipulations are at the heart of astonishing developments in atomic and molecular physics. Laser cooling of cold atom samples provides a spectacular example with the increase of the phase space density by populating a large number of photon modes through the dissipative mechanism provided by spontaneous emission [1]. Alternatively, evaporative cooling exploits the irreversible nature of 3D elastic collisions to increase the phase space density of a sub-ensemble of confined particles. The phase space density of atomic beams has also been increased with similar techniques [2, 3]. The demonstration of Maxwell's Demon devices that combined conservative potentials with an irreversible step belongs to the same kind of phase space manipulations [4, 5]. In the absence of dissipative mechanisms, the phase space volume is conserved. The manipulations that can be carried out in phase space with well engineered time-dependent conservative potentials involve separately or in combination: translation (used for instance in the slowing down of atomic or molecular packets [6–10]) and deformation [7, 11, 12] including compressions either in position or momentum space [11, 13–18] or magnification [19, 20]. Such methods are quite general, they do not rely on a specific internal structure and can therefore be applied to a large class of particles including neutrons [21, 22].

In Ref. [14], the authors proposed a phase space manipulation for velocity dispersion reduction of a non-interacting wave packet based on phase imprinting. This method has proven to cool very efficiently thermal and Bose-condensed atomic samples, leading recently to temperatures as low as 50 pK [23]. This efficient narrowing of the velocity dispersion is of great interest in metrology measurements based on atom interferometry [24, 25] and also for realizing quantum simulations [26].

Only very recently, such techniques have started to be applied to strongly interacting atoms [19]. In this paper, we precisely investigate the generalization of such a cooling concept for manipulating in phase space many-body quantum systems that exhibit self-similar dynamics [27–33, 35–40].

This paper is arranged as follows. The scaling formalism applied to the Wigner function and the class of many-body systems for which it is valid are presented in Sec. I. Section II derives the maximum compression factor in space that one can obtain for a given kick force depending on the evolution law of the dilation factor. In Sec. III, we provide the Wigner formalism for a general compression and displacement in momentum space. We also show how a time reversal operator can be applied. Section IV provides a concrete comparison between non interacting and interacting cases. The issue of anharmonicities is investigated in Sec. V. The last section explores more involved phase space manipulations for improving the robustness of compression protocols.

I. WIGNER FUNCTION FOR SELF-SIMILAR MANY-BODY SYSTEMS

The many-body quantum systems that exhibit self-similar dynamics include the Calogero-Sutherland model [30], the Tonks Girardeau gas [31, 32], certain Lieb-Liniger states [34], Bose-Einstein condensates [33, 35] even in the presence of dipolar interactions [36], strongly interacting gas mixtures [37], strongly interacting quantum gases whose collisions are described by the unitary limit [38], etc. A non-interacting classical gas described by its phase space distribution function governed by the Boltzmann equation belongs also to the same class of problems [39].

The formalism that we use relies on the Wigner function W associated with the many-body wavefunction. It is defined via the one-body reduced density matrix $g_1(x, y; t)$:

$$W(x, p; t) = \frac{1}{\pi\hbar} \int g_1(x + y, x - y; t) e^{2ipy/\hbar} \mathrm{d}y. \quad (1)$$

The self-similar dynamics after phase imprinting or in the presence of a constant acceleration field g involve two time-dependent parameters, $\alpha(t)$ and $\eta(t)$ [41]:

$$g_1(x, y; t) = \frac{1}{\alpha} g_1\left(\frac{x - \eta}{\alpha}, \frac{y - \eta}{\alpha}; 0\right) e^{i(S(x,t) - S(\eta,t))}, \quad (2)$$

where the time-dependent dilation factor fulfills $\ddot{\alpha} = \omega_0^2/\alpha^\xi$ (the exponent ξ depends on the specific system that is considered) for a free propagation of a many-body

arXiv:1409.5338v6 [physics.hist-ph] 27 Jun 2017

Minkowski Spacetime and QED from Ontology of Time

C. Baumgarten
*3244 Bärhard, Switzerland**
(Dated: June 28, 2017)

Classical mechanics, relativity, electrodynamics and quantum mechanics are often depicted as separate realms of physics, each with its own formalism and notion. This remains unsatisfactory with respect to the unity of nature and to the necessary number of postulates. We uncover the intrinsic connection of these areas of physics and describe them using a common symplectic Hamiltonian formalism. Our approach is based on a proper distinction between variables and constants, i.e. on a basic but rigorous ontology of time. We link these concepts with the obvious conditions for the possibility of measurements. The derived consequences put the measurement problem of quantum mechanics and the Copenhagen interpretation of the quantum mechanical wavefunction into perspective. According to our (onto-) logic we find that spacetime can not be fundamental. We argue that a geometric interpretation of symplectic dynamics emerges from the isomorphism between the corresponding Lie algebra and the representation of a Clifford algebra. Within this conceptional framework we derive the dimensionality of spacetime, the form of Lorentz transformations and of the Lorentz force and fundamental laws of physics as the Planck-Einstein relation, the Maxwell equations and finally the Dirac equation.

I. INTRODUCTION

A. Spacetime vs. Proper Time

Schrödinger once wrote that "In Einstein's theory of gravitation matter and its dynamical interaction are based on the notion of an intrinsic geometric structure of the space-time continuum"[1]. What we will discuss in this article suggests to conjecture the reverse statement, i.e. that the intrinsic geometric structure of spacetime is based on the very notion of matter and its dynamical interaction. The idea that spacetime is not fundamental but emergent has been proposed in the past by several authors [2–12]. Some discussed the relation between spacetime and quantum communication [13]. Our conjecture results from a different, almost classical, notion of quantum mechanics, closely connected to the phase space picture of classical statistical mechanics. A significant number of publications support our direction of thought [14–24].

We shall start with the distinction of variables and constants, i.e. from an (onto-)logic of time. Consider the basic quantummechanical relationship

$$i\hbar\partial_t\psi = E\,\psi\,. \tag{1}$$

The left side is the rate of change of a wavefunction ψ and the equation expresses that this rate of change is equal to the energy of the system. "Energy" is probably the most fundamental concept in physics. The conservation of energy has no serious exception and physics assigns to the energy the role of substance. Any entity that falls under the notion of "object" is "charged" with a certain amount of energy and is therefore subject to change with a frequency $\omega = E/\hbar$. The rate of change is what quantifies the "passage of time". This is the meaning of saying that time and energy are conjugate quantities. The passage of time is measured by clocks, i.e. by the rate of change of a reference device. And any system that can be described by Eq. 1 is a clock in itself. Metaphorically we say it exists *in time*.

Seen by light, Eq. 1 is nothing but the equation of motion (EQOM) of an harmonic oscillator. If we write the real and imaginary part of the so-called "wave-function" separately $\psi = X + iY$, then we obtain with $E/\hbar = \omega$:

$$\begin{aligned}\dot{\psi} &= \dot{X} + i\dot{Y} = -i\omega(X + iY)\\ \dot{X} &= \omega Y\\ \dot{Y} &= -\omega X\,,\end{aligned} \tag{2}$$

where the dot indicates the temporal derivative. In matrix form this reads[1]:

$$\begin{pmatrix}\dot{X}\\ \dot{Y}\end{pmatrix} = \omega\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}X\\ Y\end{pmatrix}. \tag{3}$$

The interpretation of the use of the unit imaginary in Eq. 1 seems to be the litmus test of our attitude towards quantum mechanics. It is as often presented as a necessary ingredient as its necessity is strictly denied. We believe that the unit imaginary is nothing mysterious or magical that distinguishes quantum from classical mechanics. It is just a compact form of writing Hamilton's equations of motion (EQOM) of a classical harmonic oscillator (CHO). However, Eq. 3 is the *normal form* of an algebraically more general equation and it is in this respect an unmotivated limitation of the EQOM - as we are going to show in this essay.

* christian-baumgarten@gmx.net

[1] The equality of Eq. 1 and Eq. 3 is known for long (see for instance Ref. ([15])), but the way of understanding and teaching quantum mechanics has not changed.

arXiv:1411.3989v4 [math.SG] 5 Apr 2016

Symplectic non-squeezing in Hilbert space and discrete Schrödinger equations

Alexandre Sukhov* and Alexander Tumanov**

* Université des Sciences et Technologies de Lille, Laboratoire Paul Painlevé, U.F.R. de Mathématique, 59655 Villeneuve d'Ascq, Cedex, France. The author is partially supported by Labex CEMPI. E-mail address: sukhov@math.univ-lille1.fr

** University of Illinois, Department of Mathematics, 1409 West Green Street, Urbana, IL 61801, USA. The author is partially supported by Simons Foundation grant. E-mail address: tumanov@illinois.edu

Abstract. We prove a generalization of Gromov's symplectic non-squeezing theorem for the case of Hilbert spaces. Our approach is based on filling almost complex Hilbert spaces by complex discs partially extending Gromov's results on existence of J-complex curves. We apply our result to the flow of the discrete nonlinear Schrödinger equation.

MSC: 32H02, 53C15.

Key words: symplectic diffeomorphism, Hilbert space, Hamiltonian PDE, almost complex structure, J-complex disc, discrete nonlinear Schrödinger equation.

Contents

1 Introduction **2**

2 Almost complex structures on Hilbert spaces **3**
2.1 Almost complex and symplectic structures 3
2.2 Symplectomorphisms 4
2.3 Hilbert scales 6
2.4 Vector-valued Sobolev spaces 7

3 Main results **8**

4 Cauchy integral for vector functions **10**
4.1 Cauchy integral and related operators 10
4.2 Operators on spaces of vector functions 12

5 Proof of Theorem 3.2 **14**

Noncommutative geometry and stochastic processes

Marco Frasca*

Via Erasmo Gattamelata, 3

00176 Roma (Italy)

arXiv:1412.4693v4 [quant-ph] 14 Jul 2017

Abstract

The recent analysis on noncommutative geometry, showing quantization of the volume for the Riemannian manifold entering the geometry, can support a view of quantum mechanics as arising by a stochastic process on it. A class of stochastic processes can be devised, arising as fractional powers of an ordinary Wiener process, that reproduce in a proper way a stochastic process on a noncommutative geometry. These processes are characterized by producing complex values and so, the corresponding Fokker–Planck equation resembles the Schrödinger equation. Indeed, by a direct numerical check, one can recover the kernel of the Schrödinger equation starting by an ordinary Brownian motion. This class of stochastic processes needs a Clifford algebra to exist. In four dimensions, the full set of Dirac matrices is needed and the corresponding stochastic process in a noncommutative geometry is easily recovered as is the Dirac equation in the Klein–Gordon form being it the Fokker–Planck equation of the process.

* marcofrasca@mclink.it

arXiv:1412.5629v1 [quant-ph] 17 Dec 2014

Entropic Dynamics: from Entropy and Information Geometry to Hamiltonians and Quantum Mechanics*

Ariel Caticha, Daniel Bartolomeo
Physics Department, University at Albany-SUNY, Albany, NY 12222, USA.

Marcel Reginatto
Physikalisch-Technische Bundesanstalt, 38116 Braunschweig, Germany

Abstract

Entropic Dynamics is a framework in which quantum theory is derived as an application of entropic methods of inference. There is no underlying action principle. Instead, the dynamics is driven by entropy subject to the appropriate constraints. In this paper we show how a Hamiltonian dynamics arises as a type of non-dissipative entropic dynamics. We also show that the particular form of the "quantum potential" that leads to the Schrödinger equation follows naturally from information geometry.

1 Introduction

In the standard view quantum theory (QT) is a type of mechanics and it is natural to postulate that its dynamical laws are given by an action principle. In contrast, Entropic Dynamics (ED) views quantum theory as an application of entropic methods of inference and there is no underlying action principle. The dynamics is generated by continuously maximizing an entropy as constrained by the appropriate relevant information — it is through these constraints that the "physics" is introduced. [1][2] The ED approach allows a fresh perspective on familiar notions such as time and mass and on long-standing conceptual difficulties, such as indeterminism and the problem of measurement.

The early formulations of ED involved assumptions that were justified only by their pragmatic success — they led to the right answers. For example, use was made of auxiliary variables the physical interpretation of which remained obscure and there were further assumptions about the configuration space metric

*Presented at MaxEnt 2014, the 34th International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering (September 21–26, 2014, Amboise, France).

arXiv:1502.02028v1 [math-ph] 8 Feb 2015

Symplectic transformations of a beam matrix with real Pauli and Dirac matrices

Herbert E. Müller
http://herbert-mueller.info/

Abstract

A basic problem in linear particle optics is to find a symplectic transformation that brings a symmetric matrix $\mathbf{\Sigma}$ (the beam or bunch matrix) to a special diagonal form, called normal form. The conventional way to do this involves an eigenvalue-decomposition of a matrix related to $\mathbf{\Sigma}$, and may be applied to the case of 1, 2 or 3 particle degrees of freedom. For 2 degrees of freedom, a different normalization method involving "real Dirac matrices" has recently been proposed [1], [2]. In the present article, the mathematics of real Dirac matrices is presented differently. Another normalization recipe is given, and more general decoupling problems are solved. A 3D visual representation of $\mathbf{\Sigma}$ is provided. The corresponding normalization method for 1 degree of freedom involving "real Pauli matrices" is also given.

Axioms **2013**, *xx*, 1-x; doi:10.3390/——

OPEN ACCESS

axioms

ISSN 2075-1680

www.mdpi.com/journal/axioms

Communication

On transcendental numbers: new results and a little history

Solomon Marcus[1] **and Florin F. Nichita**[1,*]

[1] Institute of Mathematics of the Romanian Academy, 21 Calea Grivitei Street, 010702 Bucharest, Romania

* Author to whom correspondence should be addressed; E-Mail: Florin.Nichita@imar.ro; Tel: (+40) (0) 21 319 65 06; Fax: (+40) (0) 21 319 65 05

Received: xx / Accepted: xx / Published: xx

arXiv:1502.05637v1 [math.HO] 19 Feb 2015

Abstract: Attempting to create a general framework for studying new results on transcendental numbers, this paper begins with a survey on transcendental numbers and transcendence, it then presents several properties of the transcendental numbers e and π, and then it gives the proofs of new inequalities and identities for transcendental numbers. Also, in relationship with these topics, we study some implications for the theory of the Yang-Baxter equations, and we propose some open problems.

Keywords: Euler's relation, transcendental numbers; transcendental operations / functions; transcendence; Yang-Baxter equation

Classification: MSC 01A05; 11D09; 11T23; 33B10; 16T25

1. Introduction

One of the most famous formulas in mathematics, the Euler's relation:

$$e^{\pi i} + 1 = 0\,, \tag{1}$$

contains the transcendental numbers e and π, the imaginary number i, the constants 0 and 1, and (transcendental) operations. Beautiful, powerful and surprising, it has changed the mathematics forever.

We will unveil profound aspects related to it, and we will propose a counterpart:

$$|e^i - \pi| < e\,, \tag{2}$$

arXiv:1502.05926v1 [quant-ph] 20 Feb 2015

Maxwell's fluid model of magnetism

Robert Brady and Ross Anderson
University of Cambridge Computer Laboratory
JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
{robert.brady,ross.anderson}@cl.cam.ac.uk

February 23, 2015

Abstract

In 1861, Maxwell derived two of his equations of electromagnetism by modelling a magnetic line of force as a 'molecular vortex' in a fluid-like medium. Later, in 1980, Berry and colleagues conducted experiments on a 'phase vortex', a wave geometry in a fluid which is analogous to a magnetic line of force and also exhibits behaviour corresponding to the quantisation of magnetic flux. Here we unify these approaches by writing down a solution to the equations of motion for a compressible fluid which behaves in the same way as a magnetic line of force. We then revisit Maxwell's historical inspiration, namely Faraday's 1846 model of light as disturbances in lines of force. Using our unified model, we show that such disturbances resemble photons: they are polarised, absorbed discretely, obey Maxwell's full equations of electromagnetism to first order, and quantitatively reproduce the correlation that is observed in the Bell tests.

In 1746 Euler modelled light as waves in a frictionless compressible fluid; a century later in 1846, Faraday modelled it as vibrations in 'lines of force' as in figure 1 [1–4].

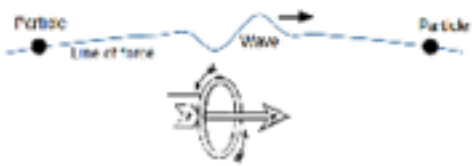


Figure 1: *Faraday's 1846 model of light as waves in lines of force, and Maxwell's 1861 figure showing his extension to a magnetic line of force.*

Fifteen years later Maxwell combined these approaches, proposing that a magnetic line of force is a 'molecular vortex' (see the diagram from his 1861 paper in figure 1 [5–7]). A fluid-like medium flows around the line, and centrifugal forces reduce the pressure near the centre, giving a 'tension' along the axis which accounts for the forces between the poles of magnets.

Maxwell then derived two of his equations of electromagnetism. Suppose the mean momentum per unit volume of fluid is $\overline{\mathbf{p}}(\mathbf{x})$. In modern notation with unit charge, the magnetic field is $\mathbf{B} = \nabla \times \overline{\mathbf{p}}$, and it obeys Gauss's law for magnetism $\nabla.\mathbf{B} = 0$, since $\nabla.(\nabla \times \overline{\mathbf{p}})$ is identically zero. Defining the magnetic flux by $\phi = \int \mathbf{B}.d\mathbf{s}$ where $d\mathbf{s}$ is a surface element, Stokes's theorem shows that $\phi = \oint \overline{\mathbf{p}}.d\boldsymbol{\ell} \neq 0$ where the path $d\boldsymbol{\ell}$ encircles the centre. If the fluid exerts a mean force density $\mathbf{E}$ on an external system then it must lose momentum, $\mathbf{E} = -\partial\overline{\mathbf{p}}/\partial t$. Faraday's law of induction follows immediately: $\nabla \times \mathbf{E} = -\partial\mathbf{B}/\partial t$. Feynman later rediscovered a similar derivation [8]. On later interpretations, the momentum density $\overline{\mathbf{p}}$ corresponds to the magnetic vector potential.

Maxwell's magnetic line of force can be almost any axis with mass flow around it ($\oint \overline{\mathbf{p}}.d\boldsymbol{\ell} \neq 0$). An ordinary vortex in a fluid is not a good exam-

arXiv:1502.07002v3 [quant-ph] 14 Mar 2015

Effective Simulation of Quantum Entanglement using Classical Fields Modulated with Pseudorandom Phase Sequences

Jian Fu, Xingkun Wu

State Key Lab of Modern Optical Instrumentation,

Department of Optical Engineering,

*Zhejiang University, Hangzhou 310027, China**

(Dated: today)

Abstract

An effective simulation of quantum entanglement is presented using classical fields modulated with n pseudorandom phase sequences (PPSs) that constitute a $n2^n$-dimensional Hilbert space with a tensor product structure. Applications to classical fields are exampfied by effective simulation of both Bell and GHZ states, and a correlation analysis was performed to characterize the simulation. Results that strictly comply with criteria of quantum entanglement were obtained and the approach was also shown to be applicable to a system consisting of n quantum particles.

PACS numbers: 03.67.Lx, 03.65.Bz, 42.50.2p, 42.79.Ta

arXiv:1504.05255v4 [cs.CR] 1 Jun 2016

Semantic Security and Indistinguishability in the Quantum World

June 2, 2016*

Tommaso Gagliardoni[1], Andreas Hülsing[2], and Christian Schaffner[3,4,5]

[1] CASED, Technische Universität Darmstadt, Germany
tommaso@gagliardoni.net
[2] TU Eindhoven, The Netherlands
andreas@huelsing.net
[3] Institute for Logic, Language and Computation (ILLC), University of Amsterdam, The Netherlands
c.schaffner@uva.nl
[4] Centrum Wiskunde & Informatica (CWI) Amsterdam, The Netherlands
[5] QuSoft, The Netherlands

Abstract. At CRYPTO 2013, Boneh and Zhandry initiated the study of quantum-secure encryption. They proposed first indistinguishability definitions for the quantum world where the actual indistinguishability only holds for classical messages, and they provide arguments why it might be hard to achieve a stronger notion. In this work, we show that stronger notions are achievable, where the indistinguishability holds for quantum superpositions of messages. We investigate exhaustively the possibilities and subtle differences in defining such a quantum indistinguishability notion for symmetric-key encryption schemes. We justify our stronger definition by showing its equivalence to novel quantum semantic-security notions that we introduce. Furthermore, we show that our new security definitions cannot be achieved by a large class of ciphers – those which are quasi-preserving the message length. On the other hand, we provide a secure construction based on quantum-resistant pseudorandom permutations; this construction can be used as a generic transformation for turning a large class of encryption schemes into quantum indistinguishable and hence quantum semantically secure ones. Moreover, our construction is the first completely classical encryption scheme shown to be secure against an even stronger notion of indistinguishability, which was previously known to be achievable only by using quantum messages and arbitrary quantum encryption circuits.

1 Introduction

Quantum computers [NC00] threaten many cryptographic schemes. By using Shor's algorithm [Sho94] and its variants [Wat01], an adversary in possession of a quantum computer can break the security of every scheme based on factorization and discrete logarithms, including RSA, ElGamal, elliptic-curve primitives and many others. Moreover, longer keys and output lengths are required in order to

* An extended abstract of this work appears in the proceedings of CRYPTO 2016. This is the full version.

arXiv:1504.05625v4 [math.CT] 28 Sep 2016

A Compositional Framework for Passive Linear Networks

John C. Baez

Department of Mathematics
University of California
Riverside CA, USA 92521
and
Centre for Quantum Technologies
National University of Singapore
Singapore 117543

Brendan Fong

Department of Computer Science
University of Oxford
United Kingdom OX1 3QD

email: baez@math.ucr.edu, brendan.fong@cs.ox.ac.uk

September 29, 2016

Abstract

Passive linear networks are used in a wide variety of engineering applications, but the best studied are electrical circuits made of resistors, inductors and capacitors. We describe a category where a morphism is a circuit of this sort with marked input and output terminals. In this category, composition describes the process of attaching the outputs of one circuit to the inputs of another. We construct a functor, dubbed the 'black box functor', that takes a circuit, forgets its internal structure, and remembers only its external behavior. Two circuits have the same external behavior if and only if they impose same relation between currents and potentials at their terminals. The space of these currents and potentials naturally has the structure of a symplectic vector space, and the relation imposed by a circuit is a Lagrangian linear relation. Thus, the black box functor goes from our category of circuits to the category of symplectic vector spaces and Lagrangian linear relations. We prove that this functor is a symmetric monoidal dagger functor between dagger compact categories. We assume the reader has some familiarity with category theory, but none with circuit theory or symplectic linear algebra.

Contents

1 Introduction **3**
1.1 Finding your way through this paper 8

I Passive Linear Circuits **9**

2 Circuits of linear resistors **10**
2.1 Circuits as labelled graphs 10
2.2 Ohm's law, Kirchhoff's laws, and the principle of minimum power 11
2.3 A Dirichlet problem 13
2.4 Equivalent circuits 15
2.5 Dirichlet forms 18

arXiv:1506.00398v3 [quant-ph] 13 Mar 2016

Quantum from principles

Giulio Chiribella[1]

Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, 100084

Giacomo Mauro D'Ariano

QUIT Group, *Dipartimento di Fisica, Università di Pavia, via Bassi 6, 27100 Pavia, Italy*

INFN sezione di Pavia, via Bassi 6, 27100 Pavia, Italy

Paolo Perinotti

QUIT Group, *Dipartimento di Fisica, Università di Pavia, via Bassi 6, 27100 Pavia, Italy*

INFN sezione di Pavia, via Bassi 6, 27100 Pavia, Italy

Abstract

Quantum theory was discovered in an adventurous way, under the urge to solve puzzles—like the spectrum of the blackbody radiation—that haunted the physics community at the beginning of the 20th century. It soon became clear, though, that quantum theory was not just a theory of specific physical systems, but rather a new language of universal applicability. Can this language be reconstructed from first principles? Can we arrive at it from logical reasoning, instead of *ad hoc* guesswork? A positive answer was provided in Refs. [1, 2], where we put forward six principles that identify quantum theory uniquely in a broad class of theories. We first defined a class of "theories of information", constructed as extensions of probability theory in which events can be connected into networks. In this framework, we formulated the six principles as rules governing the control and the accessibility of information. Directly from these rules, we reconstructed a number of quantum information features, and eventually, the whole Hilbert space framework. In short, our principles characterize quantum theory as the theory of information that allows for maximal control of randomness.

1. Introduction

Quantum foundations is an old field—as old as quantum mechanics itself. Among the early works stand out the seminal papers by Einstein, Podolski, and

[1]Corresponding author: giulio@tsinghua.edu.cn

Advancing the case for PT Symmetry – the Hamiltonian is always PT Symmetric

Philip D. Mannheim
Department of Physics, University of Connecticut, Storrs, CT 06269, USA. email: philip.mannheim@uconn.edu
(Dated: June 28, 2015)

While a Hamiltonian can be both Hermitian and PT symmetric, it is PT symmetry that is the more general, as it can lead to real energy eigenvalues even if the Hamiltonian is not Hermitian. We discuss some specific ways in which PT symmetry goes beyond Hermiticity and is more far reaching than it. We show that simply by virtue of being the generator of time translations, the Hamiltonian must always be PT symmetric, *regardless* of whether or not it *might* be Hermitian. We show that the reality of the Euclidean time path integral is a necessary and sufficient condition for PT symmetry of a quantum field theory, with Hermiticity only being a sufficient condition. We show that in order to construct the correct classical action needed for a path integral quantization one must impose PT symmetry on each classical path, a requirement that has no counterpart in any Hermiticity condition since Hermiticity of a Hamiltonian is only definable after the quantization has been performed and the quantum Hilbert space has been constructed. With the spacetime metric being PT even we show that a covariant action must always be PT symmetric. Unlike Hermiticity, PT symmetry does not need to be postulated as it is derivable from Poincare invariance. Hermiticity is just a particular realization of PT symmetry, one in which the eigenspectrum is real and complete.

arXiv:1506.08432v1 [quant-ph] 28 Jun 2015

I. INTRODUCTION AND BACKGROUND

Hermiticity of the Hamiltonian has been a cornerstone of quantum mechanics ever since its inception. Nonetheless, while the eigenvalues of a Hermitian Hamiltonian are all real, Hermiticity of a Hamiltonian is only a sufficient condition for such reality. As is for instance manifested in the matrix given in [1], viz.

$$M=\begin{pmatrix} 1+i & s \\ s & 1-i \end{pmatrix}, \tag{1}$$

we see that Hermiticity is not a necessary condition, since even though this M is not Hermitian, its eigenvalues are given by $E_\pm = 1 \pm (s^2-1)^{1/2}$, and both of these eigenvalues are real if s is real and greater than one.

A more general condition for the reality of eigenvalues has been identified by Bender and collaborators, and in a sense it is surprising since it involves an operator, time reversal $\mathcal{T}$, that acts anti-linearly in the space of states rather than linearly, and is thus not ordinarily considered in linear algebra studies. The explicit condition that was found [2, 3] was that the Hamiltonian has to be PT symmetric where P is the parity operator, and this has engendered a large number of PT studies in recent years, as described for instance in [1, 4, 5]. (In our example above, if we set $P=\sigma_1$ and $\mathcal{T}=K$ where K denotes complex conjugation we obtain $PTMT^{-1}P^{-1}=M$.)

While PT symmetry encompasses Hermiticity (Hermitian Hamiltonians can also be PT symmetric), it allows for more possibilities. The matrix M given in (1) is PT symmetric for any value of the real parameter s. However, if $s^2<1$ the energy eigenvalues form a complex conjugate pair. And while the energy eigenvalues would be real and degenerate at the crossover point where $s=1$, at this point the matrix becomes of non-diagonalizable Jordan-block form with M only possessing one eigenvector [6]. Neither of these possible outcomes is achievable with Hermitian Hamiltonians.

The utility in having a complex conjugate pair of energy eigenvalues is that when a state $|A\rangle$ (the state whose energy has a negative imaginary part) decays into some other state $|B\rangle$ (the one whose energy has a positive imaginary part), as the population of state $|A\rangle$ decreases that of $|B\rangle$ increases in proportion. In a PT-symmetric theory this interplay between the two states is found [6] to lead to unitary time evolution. In contrast, in theories based on Hermitian Hamiltonians, to describe a decay one essentially by hand adds a non-Hermitian term to a Hamiltonian, and again by hand chooses its sign so that only the decaying mode appears.

As regards the Jordan-Block case, we recall that in matrix theory Jordan showed that via a sequence of similarity transformations any matrix can be brought either to a diagonal form or to the Jordan canonical form in which all the eigenvalues are on the diagonal, in which the only non-zero off-diagonal elements fill one of the diagonals next to the leading diagonal, and in which all non-zero elements in the matrix are all equal to each other. To see this explicitly for our example, when $s=1$ we note that by means of a similarity transformation we can bring M to the Jordan-block form

$$\begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}\begin{pmatrix} 1+i & 1 \\ 1 & 1-i \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -i & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \tag{2}$$

with the transformed M being found to only possess one eigenvector, viz. $\widetilde{(1,0)}$, where the tilde symbol denotes transpose, even though the secular equation $|M-\lambda I|=0$ has two solutions, both with $\lambda=1$. (Since the energy eigenvalues have to share the only eigenvector available in the Jordan-block case, they must be degenerate.) Such lack of diagonalizability cannot occur for Hermitian matrices, to show that PT symmetry is richer than Hermiticity. Just such lack of diagonalizability has been found to occur in fourth-order derivative theories, with

Antimatter in the direct-action theory of fields

Ruth E. Kastner

13 September 2015

ABSTRACT. One of Feynman's greatest contributions to physics was the interpretation of negative energies as antimatter in quantum field theory. A key component of this interpretation is the Feynman propagator, which seeks to describe the behavior of antimatter at the virtual particle level. Ironically, it turns out that one can dispense with the Feynman propagator in a direct-action theory of fields, while still retaining the interpretation of negative energy solutions as antiparticles.

1. Introduction

This issue salutes the profound contributions by Richard P. Feynman. Feynman is known for the Wheeler-Feynman (W-F) 'direct-action' theory of classical electromagnetism [1]. Another of his contributions is the interpretation of the negative energy field equation solutions as antiparticles, and the invention of the 'Feynman propagator' which incorporates the antiparticle concept into virtual propagation. In this paper, I examine these key features of Feynman's work and attempt to elucidate their relationship to my recent development of the Transactional Interpretation (TI) of quantum theory, which is based on the W-F direct-action theory. The first three sections are review, while sections 4 and 5 are original research.

John G. Cramer used the Wheeler-Feynman theory as the basis of TI [2]. I have proposed a relativistic extension of TI [3] based on the direct-action theory of QED elaborated by Davies [4]. I call this relativistic version of TI the 'Possibilist Transactional Interpretation' (PTI), because the quantum states are interpreted as extra-spatiotemporal possibilities. (For the specific details of this suggested ontology, the reader is invited to consult [3], Chapter 7.) In the Davies theory, and accordingly in PTI, virtual particle processes are described not by the Feynman propagator, but by the time-symmetric propagator. The question then naturally arises: what exactly is an antiparticle in PTI? This paper will addressed that question, as well as the historically curious fact that Feynman abandoned his own direct-action theory. In what follows, I

Title: Revisiting time reversal and holography with spacetime transformations.

Authors:

Vincent Bacot[1], Matthieu Labousse[1,+], Antonin Eddi[2], Mathias Fink[1*], Emmanuel Fort[1*]

Addresses:

[1]Institut Langevin, ESPCI, CNRS, PSL Research University, 1 rue Jussieu, 75005, Paris, France.

[2]Laboratoire de Physique et Mécanique des Milieux Hétérogènes, ESPCI, CNRS, PSL Research University, 10 rue Vauquelin, 75005, Paris, France.

[+] Current address: Laboratoire Matériaux et Phénomènes Quantiques, Université Paris Diderot, Sorbonne Paris Cité, 10 rue A. Domon et L. Duquet, 75013 Paris, France.

[*] These authors contributed equally to this work.

arXiv:1511.00126v1 [physics.flu-dyn] 31 Oct 2015

Intermittency at Fine Scales and Complex Singularities of Turbulent Couette Flow

Andre Souza and Divakar Viswanath

Department of Mathematics, University of Michigan (sandre/divakar@umich.edu).

Abstract

Fine scales of turbulent velocity fields, beyond the inertial range and well into the dissipative range, are highly intermittent. It has been hypothesized that complex phase singularities are the principal mechanism behind fine scale intermittency. In this article, we view the velocity field of a turbulent flow as an analytic function of time. Although the function is only available for real values of time, we present a numerical technique to analytically continue the function to complex values of time, and with sufficient fidelity to locate and visualize the singularity closest to the real axis. Using this technique, we demonstrate a robust connection between temporal intermittency and the location of singularities in the complex plane.

1 Introduction

Intermittency in turbulent flows refers to sharp and spatially isolated peaks of energy contained in large wave numbers, beyond the inertial range and well into the dissipative range. In the words of Batchelor and Townsend [2], who discovered this phenomenon, "the energy associated with large wave-numbers is very unevenly distributed in space" and "there appear to be isolated regions in which the large wave-numbers are 'activated', separated by regions of comparative quiescence." This fine scale intermittency is a fundamental feature of turbulent flows [1, 5, 17].

Frisch and Morf [7] hypothesized that intermittency is a manifestation of singularities in the complex plane. Thus the activation mechanism is believed to be the occurrence of singularities in the complex plane, with the intermittent peak occurring right below the singularity closest to the real axis. Complex singularities are intrinsically easier to study with a single independent variable. Therefore Frisch and Morf shifted the emphasis to temporal intermittency, with time as the single independent variable with the entire velocity field viewed as a function of time.

The connection between intermittency and complex singularities has been demonstrated in a variety of systems such as Langevin's and Burger's equations [7, 15]. However, to the best of the authors' knowledge, such a connection is yet to be demonstrated for the incompressible Navier-Stokes equations in the turbulent regime. In this article, we develop a numerical technique that is applicable to trajectories of large scale PDE. Using that technique, we demonstrate a robust connection between temporal intermittency and complex singularities.

Here at the outset, we reprise a beautiful argument of Kraichnan [12]. The argument is heuristic but gives powerful intuition regarding the phenomenon of fine scale intermittency,

Antilinearity Rather than Hermiticity as a Guiding Principle for Quantum Theory

Philip D. Mannheim
Department of Physics, University of Connecticut, Storrs, CT 06269, USA. email: philip.mannheim@uconn.edu
(Dated: May 4, 2017)

Currently there is much interest in Hamiltonians that are not Hermitian but instead possess an antilinear PT symmetry. Here we seek to put such PT symmetric theories into as general a context as possible. After providing a brief overview of the PT symmetry program, we show that having an antilinear symmetry is the most general condition that one can impose on a quantum theory for which one can have an inner product that is time independent, have a Hamiltonian that is self-adjoint, and have energy eigenvalues that are all real. For each of these properties Hermiticity is only a sufficient condition but not a necessary one, with Hermiticity thus being the special case in which the Hamiltonian has both antilinearity and Hermiticity. As well as being the necessary condition for the reality of energy eigenvalues, antilinearity in addition allows for the physically interesting cases of manifestly non-Hermitian but nonetheless self-adjoint Hamiltonians that have energy eigenvalues that appear in complex conjugate pairs, or that are Jordan block and cannot be diagonalized at all. We show that one can extend these ideas to quantum field theory, with the dual requirements of the existence of time independent inner products and invariance under complex Lorentz transformations forcing the antilinear symmetry to uniquely be CPT. We thus extend the CPT theorem to non-Hermitian Hamiltonians. For theories that are separately charge conjugation invariant, PT symmetry then follows, with the case for the physical relevance of the PT-symmetry program thus being advanced. While CPT symmetry can be defined at the classical level for every classical path in a path integral quantization procedure, in contrast, in such a path integral there is no reference at all to the Hermiticity of the Hamiltonian or the quantum Hilbert space on which it acts, as they are strictly quantum-mechanical concepts that can only be defined after the path integral quantization has been performed and the quantum Hilbert space has been constructed. CPT symmetry thus goes beyond Hermiticity and has primacy over it, with our work raising the question of how Hermiticity ever comes into quantum theory at all. To this end we show that whether or not a CPT-invariant theory has a Hamiltonian that is Hermitian is a property of the solutions to the theory and not of the Hamiltonian itself. Hermiticity thus never needs to be postulated at all.

arXiv:1512.04915v5 [hep-th] 11 May 2017

The Riemann zeros as spectrum and the Riemann hypothesis

Germán Sierra

Instituto de Física Teórica UAM/CSIC,
Universidad Autónoma de Madrid, Cantoblanco, Madrid, Spain.

We present a spectral realization of the Riemann zeros based on the propagation of a massless Dirac fermion in a region of Rindler spacetime and under the action of delta function potentials localized on the square free integers. The corresponding Hamiltonian admits a self-adjoint extension that is tuned to the phase of the zeta function, on the critical line, in order to obtain the Riemann zeros as bound states. The model provides a proof of the Riemann hypothesis in the limit where the potentials vanish. Finally, we propose an interferometer that may yield an experimental observation of the Riemann zeros.

arXiv:1601.01797v3 [math-ph] 21 Oct 2016

Contents

I. Introduction 2

II. The semiclassical XP Berry, Keating and Connes model 2

III. The quantum XP model 4

IV. The Landau model and XP 5

V. The XP model revisited 7

VI. The space-time geometry of the modified XP models 10

VII. Diracization of $H = X(P + \ell_p^2/P)$ 12

VIII. ξ-functions: Pólya's is massive and Riemann's is massless 14

IX. The massive Dirac Model in Rindler coordinates 16

X. The massless Dirac equation with delta function potentials 17

XI. Heuristic approach to the spectrum 20

XII. The Riemann zeros as spectrum and The Riemann hypothesis 23
1. Normalizable eigenstates 23
2. The Magnus expansion 24
3. The Mertens function and the Perron formula 25

XIII. The Riemann interferometer 28

XIV. Conclusions 29

Acknowledgements 30

References 30

The quantum state as spatial displacement

Peter Holland
Green Templeton College
University of Oxford
Oxford OX2 6HG
England

peter.holland@gtc.ox.ac.uk

Abstract: We give a simple demonstration that the Schrödinger equation may be recast as a self-contained second-order Newtonian law for a congruence of spacetime trajectories. This provides a pictorial representation of the quantum state as the displacement function of the collective whereby quantum evolution is represented as the deterministic unfolding of a continuous coordinate transformation. Introducing gauge potentials for the density and current density it is shown that the wave-mechanical and trajectory pictures are connected by a canonical transformation. The canonical trajectory theory is shown to provide an alternative basis for the quantum operator calculus and the issue of the observability of the quantum state is examined within this context. The construction illuminates some of the problems involved in connecting the quantum and classical descriptions.

1. Introduction

An unfortunate by-product of the historical debate on the interpretation of quantum mechanics is that physical ideas that may have informed the development of the subject have been marshalled into the siding of 'mere philosophy'. This has been the fate of the spacetime trajectory picture of quantum evolution, which is still widely assumed to be associated just with an interpretation of the theory, i.e., to depend on optional assumptions that are not inherent in the scheme of ideas that is generally accepted as constituting 'quantum theory'. In fact, it is an ineluctable mathematical property that the conception of a physical state based on the deterministic spacetime trajectory – comprising simultaneously well-defined position and momentum variables at each point – is implicit in the quantum description *whatever the interpretation*. More precisely, a self-contained theory of trajectories with second-order Newton-style dynamics may be obtained from the first-order Schrödinger equation by a change of variables [1,2]. In this formulation the quantum state is represented by the displacement function of a continuum of interacting 'particles', which involves a congruence rather than a single trajectory because wave mechanics is a field theory. The characteristic features of the wavefunction version of state are represented by distinctive properties of the congruence. For example, the unitary evolution of the wavefunction corresponds to the deterministic unfolding of a continuous coordinate transformation and the single-valuedness of the wavefunction to non-crossing of the trajectories. Indeed, one may make the displacement function of the collective the basis of the quantum description with the wavefunction being regarded as a derived quantity.

arXiv:1601.04896v2 [quant-ph] 8 Nov 2016

Quantum Simulation of the Factorization Problem*

Jose Luis Rosales† and Vicente Martin‡
Center for Computational Simulation,
ETS Ingenieros Informáticos,
Universidad Politécnica de Madrid,
Campus Montegancedo, E28660 Madrid.
(Dated: November 9, 2016)

Feynman's prescription for a quantum simulator was to find a hamiltonian for a system that could serve as a computer. Pólya and Hilbert conjecture was to demonstrate Riemann's hypothesis through the spectral decomposition of hermitian operators. Here we study the problem of decomposing a number into its prime factors, $N = xy$, using such a simulator. First, we derive the hamiltonian of the physical system that simulate a new arithmetic function, formulated for the factorization problem, that represents the energy of the computer. This function rests alone on the primes below $\sqrt{N}$. We exactly solve the spectrum of the quantum system without resorting to any external ad-hoc conditions, also showing that it obtains, for $x \ll \sqrt{N}$, a prediction of the prime counting function that is almost identical to Riemann's $R(x)$ function. It has no counterpart in analytic number theory and its derivation is a consequence of the quantum theory of the simulator alone.

PACS numbers: 03.67.Ac, 03.67.Lx, 02.10.De, 89.20.Ff

The computational complexity assumption [1] to find the prime factors of a large number N is the basis for the security of the ubiquitous RSA, a cornerstone of the public key cryptosystems so widely used in our digital society. However, despite the many mathematical and computational advances, the classical complexity of the factorization problem is still unknown. Fortunately, the best classical algorithms known scale worse than polynomially in the number of bits of N: By now, the building blocks of the cyberinfrastructure still resist.

Nonetheless, in the quantum world, factoring is an easy problem that requires only polynomial resources using Shor's algorithm[2]. This amazing result raises new questions about the relationship between quantum mechanics and number theory and, more generally, with physics; a connection dating back to Pólya and Hilbert [3, 4], who laid a program to prove Riemann's hypothesis through the spectrum of physical operators. However, the physical realization of Shor's algorithm is still limited to proof of concept demonstrations, far away from factoring numbers of the size used in real-world cryptosystems.

An alternative would be to build the solutions in Hilbert space of a quantum simulator performing factorization, instead of going through the route of a gate-based, fully programmable, quantum computer. The key idea, following the pioneering suggestions of Feynman [5], is to translate factoring arithmetics into the physics of a device whose superposition of states mimics the problem i.e.: a factoring (analog) computer. The states of the simulator would be the solutions of some hermitian operator depending only on the number that we want to factorize. Moreover, by simply using the computer over different values of N, a quantum factoring simulator must be capable to access the statistics of the prime numbers. Thus, it might provide insight on fundamental problems in number theory following the Pólya and Hilbert program. Here we propose a new approach to the factorization problem based on the physics of a bounded hamiltonian that corresponds to a new arithmetic function defined for this problem. The values of this new function should correspond, in the quantum theory, to eigenvalues of the simulator. To the best of our knowledge, this is the first example of a quantum system whose spectrum supports the Pólya and Hilbert conjecture.

First, to bind the hamiltonian, we need a problem definition leading to a finite Hilbert space. For this we define a factorization ensemble for a given N [10]. Suppose that we want to factorize N. A simple trial division algorithm will require to inspect all the primes x less or equal than $\sqrt{N}$, i.e., a total of $\pi(\sqrt{N})$ trials will be required. The factorization ensemble of N is defined as the set of all pairs of primes that, when multiplied, give numbers N_k with the property $\pi(\sqrt{N_k}) = j$, where $j = \pi(\sqrt{N})$.

The solution to the factorization problem consists then in finding the appropriate pair in the factorization ensemble, that we will denote as $\mathcal{F}(j)$.

Then, to build a bridge between number theory and quantum mechanics, we redefine the factorization problem introducing a single-valued arithmetic function, computed for a pair of primes (x_k, y_k) in the ensemble of N. After, we transform this function into a hamiltonian mapping the arithmetics of factorization to the physics of a classical system; finally we obtain the quantum observable (operator) corresponding to the energies of the classical counterpart. Thus, obtaining the factor of N is equivalent to measuring the energy of this simulator.

The cardinality of the factorization ensemble is thus important, since, given this interpretation, it is the dimension of the Hilbert space associated to the observable. It can be derived [10] as a corollary of Theorem 437 in [1] for the special case of the product of two primes.

arXiv:1601.07545v4 [quant-ph] 6 Mar 2016

Beyond Complementarity

R. E. Kastner[1,2]
6 March 2016

ABSTRACT. It is argued that Niels Bohr ultimately arrived at positivistic and antirealist-flavored statements because of weaknesses in his initial objective of accounting for measurement in physical terms. Bohr's investigative approach faced a dilemma, the choices being (i) conceptual inconsistency or (ii) taking the classical realm as primitive. In either case, Bohr's 'Complementarity' does not adequately explain or account for the emergence of a macroscopic, classical domain from a microscopic domain described by quantum mechanics. A diagnosis of the basic problem is offered, and an alternative way forward is indicated.

1. Introduction.

In this volume[3], Bai and Stachel [1] offer a rebuttal of arguments by Beller and Fine [2] that Bohr's philosophy of quantum mechanics was positivist. That discussion addresses Bohr's reply [3] to the Einstein, Podolsky and Rosen ('EPR') paper [4] . The purpose of the present paper is not to enter into the specific debate concerning whether Bohr's basic approach was positivist or not (although this author tends to agree with Bai and Stachel that Bohr's interpretive intentions were not antirealist.) Rather, the intent is to argue that Bohr inevitably lapsed into antirealist-flavored statements about quantum systems because his notion of "Complementarity" cannot consistently account for the emergence of classicality from the quantum level. It is argued that ultimately this problem arises from Bohr's implicit assumption that all quantum evolution is unitary; i.e., that there is no real, physical non-unitary collapse.

It should be noted that Bohr's ideas changed and evolved over several decades and this paper does not attempt to trace the intricate development of this evolution. Rather, attention is focused on Bohr's initial reply to EPR and on certain methodological and metaphysical constraints that, it is argued, led inexorably to a final antirealist position toward quantum level, as evidenced in his famous statement "There is no quantum world. There is only an abstract quantum mechanical description." [7] While a reader might disagree with whether Bohr was instrumentalist or antirealist at any particular stage

[1]Foundations of Physics Group, University of Maryland, College Park, USA
[2]rkastner@umd.edu
[3]*Quantum Structural Studies*, eds. R.E. Kastner, J. Jeknić-Dugić, G. Jaroszkiewicz, World Scientific Publishers, forthcoming.

arXiv:1602.06071v1 [quant-ph] 19 Feb 2016

The Algebraic Way.

B. J. Hiley*

Physics Department, UCL and TPRU, Birkbeck, University of London, Malet Street, London WC1E 7HX.

(22 Janurary 2015)

Abstract

In this paper we examine in detail the non-commutative symplectic algebra underlying quantum dynamics. We show that this algebra contains both the Weyl-von Neumann algebra and the Moyal algebra. The latter contains the Wigner distribution as the kernel of the density matrix. The underlying non-commutative geometry can be projected into either of two Abelian spaces, so-called 'shadow phase spaces'. One of these is the phase space of Bohmian mechanics, showing that it is a fragment of the basic underlying algebra. The algebraic approach is much richer, giving rise to two fundamental dynamical time development equations which reduce to the Liouville equation and the Hamilton-Jacobi equation in the classical limit. They also include the Schrödinger equation and its wave function, showing that these features are a partial aspect of the more general non-commutative structure. We discuss briefly the properties of this more general mathematical background from which the non-commutative symplectic algebra emerges.

1 Introduction

The basic principle of the algebraic approach is to avoid starting with a specific Hilbert space scheme and rather to emphasise that the *primary objects* of the theory are the fields (or the observables) considered as purely *algebraic quantities*, together with their linear combinations, products and limits in the appropriate topology (Emch [14]).

*E-mail address b.hiley@bbk.ac.uk.

BIG IS FRAGILE: AN ATTEMPT AT THEORIZING SCALE

Atif Ansar[1,*], Bent Flyvbjerg[3], Alexander Budzier[1], Daniel Lunn[2]

Affiliations:
[1]Said Business School, University of Oxford, OX1 1HP, UK.
[2]Department of Statistics, University of Oxford, OX1 3GT, UK.

* To whom correspondence should be addressed.
E-mail: atif.ansar@sbs.ox.ac.uk

Printed in:
Bent Flyvbjerg, 2017, ed., *The Oxford Handbook of Megaproject Management*, Oxford University Press

Full reference:
Atif Ansar, Bent Flyvbjerg, Alexander Budzier, and Daniel Lunn, 2017, "Big Is Fragile: An Attempt at Theorizing Scale," in Bent Flyvbjerg, ed., *The Oxford Handbook of Megaproject Management* (Oxford: Oxford University Press), Chapter 4, pp. 60-95; URL for final print: http://bit.ly/2bctWZt

All rights reserved

DFPD-2016/TH/2

Holographic Effective Field Theories

Luca Martucci [a] and Alberto Zaffaroni [b]

[a] *Dipartimento di Fisica ed Astronomia "Galileo Galilei", Università di Padova & INFN, Sezione di Padova, Via Marzolo 8, I-35131 Padova, Italy*

[b] *Dipartimento di Fisica, Università di Milano-Bicocca, & INFN, Sezione di Milano-Bicocca, I-20126 Milano, Italy*

arXiv:1603.04470v2 [hep-th] 18 Jul 2016

Abstract

We derive the four-dimensional low-energy effective field theory governing the moduli space of strongly coupled superconformal quiver gauge theories associated with D3-branes at Calabi-Yau conical singularities in the holographic regime of validity. We use the dual supergravity description provided by warped resolved conical geometries with mobile D3-branes. Information on the baryonic directions of the moduli space is also obtained by using wrapped Euclidean D3-branes. We illustrate our general results by discussing in detail their application to the Klebanov-Witten model.

arXiv:1603.09741v1 [cond-mat.str-el] 31 Mar 2016

Demystifying the Holographic Mystique

D. V. Khveshchenko
Department of Physics and Astronomy, University of North Carolina, Chapel Hill, NC 27599

Thus far, in spite of many interesting developments, the overall progress towards a systematic study and classification of various "strange" metallic states of matter has been rather limited. To that end, it was argued that a recent proliferation of the ideas of holographic correspondence originating from string theory might offer a possible way out of the stalemate. However, after almost a decade of intensive studies into the proposed extensions of the holographic conjecture to a variety of condensed matter problems, the validity of this intriguing approach remains largely unknown. This discussion aims at ascertaining its true status and elucidating the conditions under which some of its predictions may indeed be right (albeit, possibly, for a wrong reason).

Condensed Matter Holography: The Promise

Among the outstanding grand problems in condensed matter physics is that of a deeper understanding and classification of the so-called 'strange metals' or compressible non-Fermi liquid (NFL) states of the strongly interacting systems. However, despite all the effort and a plethora of the important and non-trivial results obtained with the use of the traditional techniques, this program still remains far from completion.

As an alternate approach, over the past decade there have been numerous attempts inspired by the hypothetical idea of holographic correspondence which originated from string/gravity/high energy theory (where it is known under the acronym *AdS/CFT*) to adapt its main concepts to various condensed matter (or, even more generally, quantum many-body) systems at finite densities and temperatures[1,2].

In its original context, the 'bona fide' holographic principle postulates that certain $d+1$-dimensional ("boundary") quantum field theories (e.g., the maximally supersymmetric $SU(N)$ gauge theory) may allow for a dual description in terms of a string theory which, upon a proper compactification, amounts to a certain $d+2$-dimensional ("bulk") supergravity. Moreover, in the strong coupling limit (characterized in terms of the t'Hooft coupling constant $\lambda = g^2N \gg 1$) and for a large rank $N \gg 1$ of the gauge symmetry group, the bulk description can be further reduced down to a weakly fluctuating gravity model which can even be treated semiclassically at the lowest (0^{th}) order of the underlying $1/N$-expansion.

In the practical applications of the holographic conjecture, the partition function of a strongly interacting boundary theory with the Lagrangian $\mathcal{L}(\phi_a)$ would then be approximated by a saddle-point (classical) value of the bulk action described by the Lagrangian $L(g_{\mu\nu}, \ldots)$ which includes gravity and other fields dual to their boundary counterparts[1,2]

$$Z[J] = \int \prod_{a=1}^{N} D\phi_a \exp(-\int dt d^d\vec{x} \mathcal{L}(\phi_a)) \approx \exp(-\int dr dt d^d\vec{x} L(g_{\mu\nu}, \ldots)) \quad (1)$$

evaluated with the use of a fixed background metric

$$ds^2 = g_{tt}dt^2 + g_{rr}dr^2 + \sum_{ij} g_{ij}dx^i dx^j \quad (2)$$

while any quantum corrections would usually be neglected by invoking the small parameter $1/N$.

Thus, considering that the task of solving a system of coupled Einstein-type differential equations can be fairly straightforward conceptually (albeit not necessarily technically), the holographic approach could indeed become a novel powerful tool for studying the strongly correlated systems and a viable alternative to the practically impossible problem of summing the entire perturbation series. Specifically, if proved valid, some of the broad 'bottom-up' generalizations of the original holographic conjecture known as 'AdS/CMT' (which, in many instances, should have been more appropriately called 'non-AdS/non-CFT') could indeed provide an advanced phenomenological framework for discovering new and classifying the already known types of the NFL behavior.

Thus far, however, a flurry of the traditionally detailed (hence, rarely concise) publications on the topic have generated not only a good deal of enthusiasm but some reservations as well. Indeed, the proposed 'ad hoc' generalizations of the original string-theoretical construction involve some of its most radical alterations, whereby most of its stringent constraints would have been abandoned in the hope of still capturing some key aspects of the underlying correspondence. This is because the target (condensed matter) systems generically tend to be neither conformally, nor Lorentz (or even translationally and/or rotationally) invariant and lack any supersymmetric (or even an ordinary) gauge symmetry with some (let alone, large) rank-N non-abelian group.

Moreover, while sporting a truly impressive level of technical profess, the exploratory 'bottom-up' holographic studies have not yet helped to resolve such crucially important issues as:

- Are the conditions of a large N, (super)gauge symmetry, Lorentz/translational/rotational invariance of the boundary (quantum) theory indeed necessary for establishing a holographic correspondence with some weakly coupled (classical) gravity in the bulk?
- Are all the strongly correlated systems (or only a pre-

AsicBoost - A Speedup for Bitcoin Mining

Dr. Timo Hanke

March 31, 2016 (rev. 5)

Abstract. *AsicBoost* is a method to speed up Bitcoin mining by a factor of approximately 20%. The performance gain is achieved through a high-level optimization of the Bitcoin mining algorithm which allows for drastic reduction in gate count on the mining chip. *AsicBoost* is applicable to all types of mining hardware and chip designs. This paper presents the idea behind the method and describes the information flow in implementations of *AsicBoost*.

1 Introduction

AsicBoost is a method to speed up Bitcoin mining by a factor of approximately 20%. *AsicBoost* is an *algorithmic* optimization and therefore applicable to all types of mining hardware.

The *AsicBoost* method is based on a new way to process work items inside and outside of the Bitcoin mining ASIC. It involves a new design of the SHA 256 hash-engines (inside the ASIC) and an additional pre-processing step as part of the mining software (outside the ASIC). The result is a performance improvement of up to 20% achieved through a reduction of gate count on the silicon. The purpose of this paper is to present the idea behind the method and to describe the information flow in implementations of *AsicBoost*.

The hash-engine design required for *AsicBoost* is compatible with design philosophies such as pipelined ("unrolled") cores and non-pipelined ("rolled") cores. The performance gains can be achieved on top of all low-level optimizations regarding timing, pipelining, path balancing, custom cell and full-custom designs, etc.

Through gate count reduction on the silicon *AsicBoost* improves two essential Bitcoin mining cost metrics simultaneously and by a similar factor: the energy consumption (Joule per Gh) and the system cost ($ per Gh/s). With the system cost being proportional to the capital expenses of a Bitcoin mine and the energy consumption being proportional to its operating expenses, *AsicBoost* reduces the total cost per bitcoin mined by approximately 20%. For the Bitcoin mines of the future *AsicBoost* will make all the difference between a profitable and an unprofitable mine.

A thorough analysis of all algorithmic Bitcoin mining optimizations before *AsicBoost* has been done in [5]. The fact that [5] estimates the combined performance gain of all optimizations it

http://asicboost.com/
asicboost@gmail.com

A Roadmap to Interstellar Flight

Philip Lubin
Physics Dept, UC Santa Barbara
lubin@deepspace.ucsb.edu
submitted to JBIS April 2015
JBIS Vol. 69, pp. 40-72 Feb 2016
Current version 15-w7-4 (10/18/16)

Abstract – In the nearly 60 years of spaceflight we have accomplished wonderful feats of exploration that have shown the incredible spirit of the human drive to explore and understand our universe. Yet in those 60 years we have barely left our solar system with the Voyager 1 spacecraft launched in 1977 finally leaving the solar system after 37 years of flight at a speed of 17 km/s or less than 0.006% the speed of light. As remarkable as this, to reach even the nearest stars with our current propulsion technology will take 100 millennium. We have to radically rethink our strategy or give up our dreams of reaching the stars, or wait for technology that does not currently exist. While we all dream of human spaceflight to the stars in a way romanticized in books and movies, it is not within our power to do so, nor it is clear that this is the path we should choose. We posit a path forward, that while not simple, it is within our technological reach. We propose a roadmap to a program that will lead to sending relativistic probes to the nearest stars and will open up a vast array of possibilities of flight both within our solar system and far beyond. Spacecraft from gram level complete spacecraft on a wafer ("wafersats") that reach more than ¼ c and reach the nearest star in 20 years to spacecraft with masses more than 10^5 kg (100 tons) that can reach speeds of greater than 1000 km/s. These systems can be propelled to speeds currently unimaginable with existing propulsion technologies. To do so requires a fundamental change in our thinking of both propulsion and in many cases what a spacecraft is. In addition to larger spacecraft, some capable of transporting humans, we consider functional spacecraft on a wafer, including integrated optical communications, imaging systems, photon thrusters, power and sensors combined with directed energy propulsion. The costs can be amortized over a very large number of missions beyond relativistic spacecraft as such planetary defense, beamed energy for distant spacecraft, sending power back to Earth, stand-off composition analysis of solar system targets, long range laser communications, SETI searches and even terra forming. Exploring the nearest stars and exo-planets would be a profound voyage for humanity, one whose non-scientific implications would be enormous. It is time to begin this inevitable journey far beyond our home.

Quantum Random Number Generators

Miguel Herrero-Collantes*

Instituto Nacional de Ciberseguridad,
Avenida José Aguado, 41, Edificio INCIBE 24005, León, Spain.

El Telecomunicación, Department of Signal Theory and Communications, University of Vigo,
Campus Universitario Lagoas-Marcosende, E-36310 Vigo,
Spain.

Juan Carlos García-Escartín†

Universidad de Valladolid,
Dpto. Teoría de la Señal e Ing. Telemática,
Paseo Belén nº 15,
47011 Valladolid,
Spain.

(Dated: October 24, 2016)

Random numbers are a fundamental resource in science and engineering with important applications in simulation and cryptography. The inherent randomness at the core of quantum mechanics makes quantum systems a perfect source of entropy. Quantum random number generation is one of the most mature quantum technologies with many alternative generation methods. We discuss the different technologies in quantum random number generation from the early devices based on radioactive decay to the multiple ways to use the quantum states of light to gather entropy from a quantum origin. We also discuss randomness extraction and amplification and the notable possibility of generating trusted random numbers even with untrusted hardware using device independent generation protocols.

arXiv:1604.03304v2 [quant-ph] 21 Oct 2016

CONTENTS

I. Motivation 2

II. Random numbers and their applications 2
A. Pseudorandom number generators and true random number generators 3
B. Random numbers in simulation 5
C. Random numbers in cryptography 5
D. Random numbers in fundamental science 7

III. Block description 8

IV. Entropy estimation 9

V. Quantum Random Number Generators based on radioactive decay 10
A. The first quantum random number generators 10
B. Evolution 12
C. Limitations 12

VI. Random Number Generators based on noise 13

VII. Optical Quantum Random Number Generators 14
A. Quantum optics in random number generators 14
B. Branching path generators 15
C. Time of arrival generators 17
D. Photon counting generators 19
E. Attenuated pulse generators 20
F. Generators based on quantum vacuum fluctuations 20
G. Generators based on the phase noise of lasers 21
H. Generators based on amplified spontaneous emission 23
I. Generators based on Raman scattering 24
J. Generators based on optical parametric oscillators 27

VIII. Non-optical Quantum Random Number Generators 28

IX. Random numbers certified by quantum mechanics 29
A. Self-testing in quantum random number generators 30
B. Device independent quantum random number generators 31
C. Other forms of quantum certification 33

X. Postprocessing 34
A. Randomness extractors 35
1. Deterministic extractors 35
2. Seeded extractors 36

XI. Quantum randomness extractors: randomness expansion and randomness amplification 37
A. Quantum randomness expansion 38
B. Quantum randomness amplification 38

XII. Randomness testing 39

XIII. Discussion 40

Acknowledgments 40

References 40

* miguel.herrero@incibe.es
† jcgarcia@tel.uva.es

Pseudorandom Phase Ensembles and Non-locality

Jian Fu

State Key Lab of Modern Optical Instrumentation,

College of Optical Science and Engineering,

*Zhejiang University, Hangzhou, 310027, China**

(Dated: today)

arXiv:1604.07652v2 [quant-ph] 23 Jul 2016

Abstract

In this paper, we introduce a new concept of a pseudorandom phase ensemble to simulate a quantum ensemble. A pseudorandom sequence is inseparability and integral that are demonstrated only for a whole sequence, not for a single phase unit, which is similar to that of quantum ensembles and a quantum particle. Using the ensemble concept, we demonstrate non-locality properties for classical fields similar to quantum entanglement.

PACS numbers: 03.67.-a, 42.50.-p

arXiv:1604.08873v2 [cs.LO] 14 Jun 2016

Computational Higher Type Theory I: Abstract Cubical Realizability

Carlo Angiuli[*]
Carnegie Mellon University

Robert Harper[†]
Carnegie Mellon University

Todd Wilson[‡]
California State University Fresno

April, 2016

Abstract

Brouwer's constructivist foundations of mathematics is based on an intuitively meaningful notion of computation shared by all mathematicians. Martin-Löf's *meaning explanations* for constructive type theory define the concept of a type in terms of computation. Briefly, a type is a complete (closed) program that evaluates to a *canonical type* whose members are complete programs that evaluate to *canonical elements* of that type. The explanation is extended to incomplete (open) programs by *functionality*: types and elements must respect equality in their free variables. Equality is evidence-free—two types or elements are at most equal—and equal things are implicitly interchangeable in all contexts.

Higher-dimensional type theory extends type theory to account for *identifications* of types and elements. An identification witnesses that two types or elements are explicitly interchangeable in all contexts by an explicit transport, or coercion, operation. There must be sufficiently many identifications, which is ensured by imposing a generalized form of the *Kan condition* from homotopy theory. Here we provide a Martin-Löf-style meaning explanation of simple higher-dimensional type theory based on a programming language that includes Kan-like constructs witnessing the computational meaning of the higher structure of types. The treatment includes an example of a higher inductive type (namely, the 1-dimensional sphere) and an example of Voevodsky's *univalence* principle, which identifies equivalent types.

The main result is a *computational canonicity theorem* that validates the computational interpretation: a closed boolean expression must always evaluate to a boolean value, even in the presence of higher-dimensional structure. This provides the first fully computational formulation of higher-dimensional type theory.

1 Introduction

The goal of this work is to develop a computation-based account of higher-dimensional type theory for which canonicity at observable types is true by construction. Types are considered as descriptions of the computational behavior of terms, rather than as formal syntax to which meaning is

[*] cangiuli@cs.cmu.edu
[†] rwh@cs.cmu.edu
[‡] twilson@csufresno.edu

arXiv:1605.05549v1 [cs.CR] 18 May 2016

Stealing PINs via Mobile Sensors: Actual Risk versus User Perception

Maryam Mehrnezhad, Ehsan Toreini, Siamak F. Shahandashti, Feng Hao
School of Computing Science, Newcastle University, UK
Email: {m.mehrnezhad, ehsan.toreini, siamak.shahandashti, feng.hao}@ncl.ac.uk

***Abstract*—In the first part of this paper, we propose PINlogger.js which is a JavaScript-based side channel attack revealing user PINs on an Android mobile phone. In this attack, once the user visits a website controlled by an attacker, the JavaScript code embedded in the web page starts listening to the motion and orientation sensor streams without needing any permission from the user. By analysing these streams, it infers the user's PIN using an artificial neural network. Based on a test set of fifty 4-digit PINs, PINlogger.js is able to correctly identify PINs in the first attempt with a success rate of 82.96%, which increases to 96.23% and 99.48% in the second and third attempts respectively. The high success rates of stealing user PINs on mobile devices via JavaScript indicate a serious threat to user security.**

In the second part of the paper, we study users' perception of the risks associated with mobile phone sensors. We design user studies to measure the general familiarity with different sensors and their functionality, and to investigate how concerned users are about their PIN being stolen by an app that has access to each sensor. Our results show that there is significant disparity between the actual and perceived levels of threat with regard to the compromise of the user PIN. We discuss how this observation, along with other factors, renders many academic and industry solutions ineffective in preventing such side channel attacks.

1. Introduction

Smartphones equipped with modern sensors such as *GPS, light, orientation and motion* are continuously providing more features to end users in order to interact with their real-world surroundings. Developers can have access to the mobile sensors either by 1) writing native code using mobile OS APIs [17], 2) recompiling HTML5 code into a native app [34], or 3) using standard APIs provided by the W3C which are accessible through JavaScript code within a mobile browser[1]. The last method has the advantage of not needing any app-store approval for releasing the app or doing future updates. More importantly, the JavaScript code is platform independent, i.e., once the code is developed it can be executed within any modern browser on any mobile OS.

In-browser access risks. While sensor-enabled mobile web applications provide users more functionalities, they raise new privacy and security concerns. Both the academic community and the industry have recognised such issues regarding certain sensors such as geolocation [20]. For the website to access the geolocation data, it must ask for explicit user permission. However, to the best of our knowledge, there is little work evaluating the risks of in-browser access to other sensors. Unlike in-app attacks, an in-browser attack, i.e., via JavaScript code embedded in a web page, does not require any app installation. Furthermore, JavaScript code does not require any user permission to access sensor data such as device motion and orientation. Furthermore, there is no notification while JavaScript is reading the sensor data stream. Hence, such in-browser attacks can be carried out far more covertly than the in-app counterparts. However, launching an effective in-browser attack still has to overcome the technical challenge that the sampling rates available in browser are much lower than those in app. For example, as we observed in [24], frequency rates of motion and orientation sensor data available in-browser are 3 to 5 times lower than those of accelerometer and gyroscope available in-app.

[1] w3.org/TR/#tr_Javascript_APIs

Fig. 1. PINlogger.js potential attack scenarios: a) the malicious code is loaded in an iframe and the user is on the same tab, b) the attack tab is already open and the user is on a different tab, c) the attack content is already open in a minimized browser, and the user is on an installed app, d) the attack content is already open in a (minimized) browser, and the screen is locked. The attacker listens to the side channel motion and orientation measurements of the victim's mobile device through JavaScript code, and uses machine learning methods to discover the user's sensitive information such as his activity types and PINs.

Motion and orientation sensors detail. According to W3C specifications [2] motion and orientation sensor data are a series of a few different measurements:

- device *orientation* which provides the physical orientation of the device, expressed as three rotation angles (α, β, γ) in the device's local coordinate frame
- device *acceleration* which provides the physical acceleration of the device, expressed in Cartesian coordinates (x, y, z) in the device's local coordinate frame
- device *acceleration-including-gravity* which is similar to acceleration except that it includes gravity as well
- device *rotation rate* which provides the rotation rate of the device about the local coordinate frame, expressed as three rotation angles (α, β, γ)

arXiv:1605.08065v1 [cs.CR] 25 May 2016

Cryptographic applications of capacity theory: On the optimality of Coppersmith's method for univariate polynomials

Ted Chinburg
ted@math.upenn.edu

Brett Hemenway
fbrett@cis.upenn.edu

Nadia Heninger
nadiah@cis.upenn.edu

Zachary Scherr
zscherr@math.upenn.edu

May 27, 2016

Abstract

We draw a new connection between Coppersmith's method for finding small solutions to polynomial congruences modulo integers and the capacity theory of adelic subsets of algebraic curves. Coppersmith's method uses lattice basis reduction to construct an auxiliary polynomial that vanishes at the desired solutions. Capacity theory provides a toolkit for proving when polynomials with certain boundedness properties do or do not exist. Using capacity theory, we prove that Coppersmith's bound for univariate polynomials is optimal in the sense that there are no auxiliary polynomials of the type he used that would allow finding roots of size $N^{1/d+\epsilon}$ for monic degree-d polynomials modulo N. Our results rule out the existence of polynomials of any degree and do not rely on lattice algorithms, thus eliminating the possibility of even superpolynomial-time improvements to Coppersmith's bound. We extend this result to constructions of auxiliary polynomials using binomial polynomials, and rule out the existence of any auxiliary polynomial of this form that would find solutions of size $N^{1/d+\epsilon}$ unless N has a very small prime factor.

1 Introduction

Coppersmith's method [Cop97, Cop01] is a celebrated technique in public-key cryptanalysis for finding small roots of polynomial equations modulo integers. In the simplest case, one is given a degree-d monic polynomial $f(x)$ with integer coefficients, and one wishes to find the integers r modulo a given integer N for which $f(r) \equiv 0 \bmod N$. When N is prime, this problem can be efficiently solved in polynomial time, but for composite N of unknown factorization, no efficient method is known in general. In fact, such an algorithm would immediately break the RSA cryptosystem, by allowing one to decrypt ciphertexts c by finding roots of the polynomial $f(x) = x^e - c \bmod N$.

While it appears intractable to solve this problem in polynomial time, Coppersmith showed that one can efficiently find all *small* integers r such that $f(r) \equiv 0 \bmod N$. More precisely, he proved the following result in [Cop97]:

Theorem 1 (Coppersmith 1996)**.** *Suppose one is given a modulus N and a monic polynomial $f(x) = x^d + f_{d-1}x^{d-1} + \cdots + f_1 x + f_0$ in $\mathbb{Z}[x]$. One can find all $r \in \mathbb{Z}$ such that*

$$|r| \leq N^{1/d} \quad \text{and} \quad f(r) \equiv 0 \bmod N \tag{1}$$

in polynomial time in $\log(N) + \sum_i \log |f_i|$.

The algorithm he developed to prove this result has applications across public-key cryptography, including cryptanalysis of low public exponent RSA with fixed-pattern or affine padding [Cop97], the security proof of RSA-OAEP [Sho01], and showing that the least significant bits of RSA are hardcore [SPW06]. We discuss these applications in more detail in §2.3. If the exponent $1/d$ in the bound in Equation 1 could be increased, it would have immediate practical impact on the security of a variety of different cryptosystems.

arXiv:1606.05529v2 [math.CT] 12 Sep 2016

Towards a unified framework for decomposability of processes

Valtteri Lahtinen · Antti Stenvall

Dated: 12.9.2016

Abstract The concept of process is ubiquitous in science, engineering and everyday life. Category theory, and monoidal categories in particular, provide an abstract framework for modelling processes of many kinds. In this paper, we concentrate on sequential and parallel decomposability of processes in the framework of monoidal categories: We will give a precise definition, what it means for processes to be decomposable. Moreover, through examples, we argue that viewing parallel processes as coupled in this framework can be seen as a category mistake or a misinterpretation. We highlight the suitability of category theory for a structuralistic interpretation of mathematical modelling and argue that for appliers of mathematics, such as engineers, there is a pragmatic advantage from this.

Keywords Mathematical modelling · Category theory · Structuralism · Process · Decomposition

1 Introduction

The role of category theory as the foundational language for mathematics, or even as *the foundation for mathematics*, has been under discussion for a long time (see e.g. (Lawvere, 1966), (Marquis, 1995), (Muller, 2001)). In particular, category theory has been linked to, and seen to allow, a structuralistic interpretation of mathematics, as discussed by Landry (2009) and Pedroso (2009) among others. Indeed, category theory seems to be more concerned with relations between objects than objects themselves. Moreover, Arbib and Manes have argued, that not only pure mathematics, but also problems of *applied*

Electromagnetics, Department of Electrical Engineering, Tampere University of Technology, PO Box 692, 33101 Tampere, Finland
Tel.: +358-40-8490430
http://arttujanpaa.org
E-mail: valtteri.lahtinen@tut.fi

Optical analogy to quantum Fourier transform based on pseudorandom phase ensemble

Jian Fu, Wei Fang, Yongzheng Ye

State Key Lab of Modern Optical Instrumentation,

College of Optical Science and Engineering,

*Zhejiang University, Hangzhou, 310027, China**

(Dated: today)

arXiv:1607.08308v2 [quant-ph] 14 Aug 2016

Abstract

In this paper, we introduce an optical analogy to quantum Fourier tanformation based on a pseudorandom phase ensemble. The optical analogy also brings about exponential speedup over classical Fourier tanformation. Using the analogy, we demonstrate three classical fields to realize Fourier transform similar to three quantum particles.

*Electronic address: jianfu@zju.edu.cn

arXiv:1609.05382v1 [math.CT] 17 Sep 2016

The Algebra of Open and Interconnected Systems

Brendan Fong
Hertford College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy in Computer Science

Trinity 2016

Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and Its Effects on the Web*

Gabriel Emile Hine[†], Jeremiah Onaolapo[♭], Emiliano De Cristofaro[♭], Nicolas Kourtellis[♯], Ilias Leontiadis[♯], Riginos Samaras[*], Gianluca Stringhini[♭], Jeremy Blackburn[♯]

[†]Roma Tre University [♭]University College London [♯]Telefonica Research [*]Cyprus University of Technology
gabriel.hine@uniroma3.it, [j.onaolapo,e.decristofaro,g.stringhini]@cs.ucl.ac.uk,
[nicolas.kourtellis,ilias.leontiadis,jeremy.blackburn]@telefonica.com, ri.samaras@edu.cut.ac.cy

arXiv:1610.03452v5 [cs.SI] 1 Oct 2017

Abstract

The discussion-board site 4chan has been part of the Internet's dark underbelly since its inception, and recent political events have put it increasingly in the spotlight. In particular, /pol/, the "Politically Incorrect" board, has been a central figure in the outlandish 2016 US election season, as it has often been linked to the alt-right movement and its rhetoric of hate and racism. However, 4chan remains relatively unstudied by the scientific community: little is known about its user base, the content it generates, and how it affects other parts of the Web. In this paper, we start addressing this gap by analyzing /pol/ along several axes, using a dataset of over 8M posts we collected over two and a half months. First, we perform a general characterization, showing that /pol/ users are well distributed around the world and that 4chan's unique features encourage fresh discussions. We also analyze content, finding, for instance, that YouTube links and hate speech are predominant on /pol/. Overall, our analysis not only provides the first measurement study of /pol/, but also insight into online harassment and hate speech trends in social media.

1 Introduction

The Web has become an increasingly impactful source for new "culture" [4], producing novel jargon, new celebrities, and disruptive social phenomena. At the same time, serious threats have also materialized, including the increase in hate speech and abusive behavior [7, 20]. In a way, the Internet's global communication capabilities, as well as the platforms built on top of them, often enable previously isolated, and possibly ostracized, members of fringe political groups and ideologies to gather, converse, organize, as well as execute and spread their agenda [28].

Over the past decade, 4chan.org has emerged as one of the most impactful generators of online culture. Created in 2003 by Christopher Poole (aka "moot"), and acquired by Hiroyuki Nishimura in 2015, 4chan is an imageboard site, built around a typical discussion bulletin-board model. An "original poster" (OP) creates a new thread by making a post, with a single image attached, to a board with a particular interest focus. Other users can reply, with or without images, and add references to previous posts, quote text, etc. Its key features include anonymity, as no identity is associated with posts, and ephemerality, i.e., threads are periodically pruned [6]. 4chan is a highly influential ecosystem: it gave birth not only to significant chunks of Internet culture and memes,[1] but also provided a highly visible platform to movements like *Anonymous* and the *alt-right* ideology. Although it has also led to positive actions (e.g., catching animal abusers), it is generally considered one of the darkest corners of the Internet, filled with hate speech, pornography, trolling, and even murder confessions [17]. 4chan also often acts as a platform for coordinating denial of service attacks [2] and aggression on other sites [1]. However, despite its influence and increased media attention [5, 16], 4chan remains largely unstudied, which motivates the need for systematic analyses of its ecosystem.

In this paper, we start addressing this gap, presenting a longitudinal study of one sub-community, namely, /pol/, the "Politically Incorrect" board. To some extent, /pol/ is considered a containment board, allowing generally distasteful content – even by 4chan standards – to be discussed without disturbing the operations of other boards, with many of its posters subscribing to the alt-right and exhibiting characteristics of xenophobia, social conservatism, racism, and, generally speaking, hate. We present a multi-faceted, first-of-its-kind analysis of /pol/, using a dataset of 8M posts from over 216K conversation threads collected over a 2.5-month period. First, we perform a general characterization of /pol/, focusing on posting behavior and on how 4chan's unique features influence the way discussions proceed. Next, we explore the types of content shared on /pol/, including third-party links and images, the use of hate speech, and differences in discussion topics at the country level. Finally, we show that /pol/'s hate-filled vitriol is not contained within /pol/, or even 4chan, by measuring its effects on conversations taking place on other platforms, such

*A shorter version of this paper appears in the Proceedings of the 11th International AAAI Conference on Web and Social Media (ICWSM'17). Please cite the ICWSM'17 paper. Corresponding author: blackburn@uab.edu.

[1]For readers unfamiliar with memes, we suggest a review of the documentary available at https://www.youtube.com/watch?v=dQw4w9WgXcQ.

arXiv:1610.04591v2 [cs.LO] 9 Dec 2016

The HoTT Library

A formalization of homotopy type theory in Coq

Andrej Bauer*
University of Ljubljana, Slovenia
Andrej.Bauer@andrej.com

Jason Gross
MIT, USA
jgross@mit.edu

Peter LeFanu Lumsdaine†
Stockholm University, Sweden
p.l.lumsdaine@math.su.se

Michael Shulman‡
University of San Diego, USA
shulman@sandiego.edu

Matthieu Sozeau§
Inria, France
mattam@mattam.org

Bas Spitters¶
Aarhus University, Denmark
spitters@cs.au.dk

Abstract

We report on the development of the *HoTT library*, a formalization of homotopy type theory in the Coq proof assistant. It formalizes most of basic homotopy type theory, including univalence, higher inductive types, and significant amounts of synthetic homotopy theory, as well as category theory and modalities. The library has been used as a basis for several independent developments. We discuss the decisions that led to the design of the library, and we comment on the interaction of homotopy type theory with recently introduced features of Coq, such as universe polymorphism and private inductive types.

1 Introduction

Homotopy type theory is a novel approach to developing mathematics in Martin-Löf's type theory, based on interpretations of the theory into abstract homotopy-theoretic settings such as certain higher toposes (Kapulkin and Lumsdaine 2012; Shulman 2015b). The connection between type theory and homotopy theory is originally due to (Awodey and Warren 2009) and (Voevodsky 2006).

Identity types are interpreted as path spaces, and type equivalence as homotopy equivalence. Type-theoretic constructions correspond to homotopy-invariant constructions on homotopy types. In addition, homotopical intuition *gives* rise to entirely new type-theoretic notions, such as higher inductive types and Voevodsky's univalence axiom. One can even develop homotopy theory in the language of type theory in a "synthetic" manner, treating (homotopy) types as a primitive notion.

The first formalization of homotopy type theory in a proof assistant was Voevodsky's *Foundations* library implemented in Coq, now called the *UniMath* project (Voevodsky, Ahrens, Grayson, et al. 2016). Here we present the second major such library, *the HoTT library*, also implemented in Coq, with somewhat different goals from those of UniMath. The library is freely available.[1]

Coq word count reports that the library contains 16800 lines of specifications, 13000 lines of proofs, and 4500 lines of comments. The library is self-sufficient, completely replacing the Coq standard library (which is incompatible with homotopy type theory) with a bare minimum necessary for basic Coq tactics to function properly (see §6).

Contributions The HoTT library provides a substantive formalization of homotopy type theory. It demonstrates that univalent foundations (cf. §2) provide a workable setup for formalization of mathematics. The library relies on advanced features of Coq (cf. §3), such as automatic handling of universe polymorphism (cf. §3.1) and type classes (cf. §3.2), management of opaque and transparent definitions (cf. §3.3), and automation (cf. §3.4). We used private inductive types to implement higher inductive types (cf. §4), and the Coq module system to formalize modalities (cf. §5). Our development pushed Coq's abilities, which prompted the developers to extend and modify it for our needs (cf. §6).

*This material is based upon work supported by the Air Force Office of Scientific Research, Air Force Material Command, USAF under Award No. FA9550-14-1-0096.

†This material is based upon work supported by the National Science Foundation under Grant No. DMS-1128155.

‡This material is based on research sponsored by The United States Air Force Research Laboratory under agreement number FA9550-15-1-0053. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the United States Air Force Research Laboratory, the U.S. Government, or Carnegie Mellon University.

§This work has been partly funded by the CoqHoTT ERC Grant 637339.

¶This research was partially supported by the Gaunbed Homotopy Type Theory project, funded by the Villum Foundation, project number 10386.

[1] http://github.com/HoTT/HoTT or the Coq OPAM package manager

arXiv:1610.07130v1 [quant-ph] 23 Oct 2016

Quantum Trajectories: Dirac, Moyal and Bohm.

B. J. Hiley[1], M. A. de Gosson[2] and G. Dennis[1].

[1] Physics Department, University College, London, Gower Street, London WC1E 6BT.
[2] Universität Wien, NuHAG, Fakultät für Mathematik, A-1090 Wien.

Abstract

We recall Dirac's early proposals to develop a description of quantum phenomena in terms of a non-commutative algebra in which he suggested a way to construct what he called 'quantum trajectories'. Generalising these ideas, we show how they are related to weak values and explore their use in the experimental construction of quantum trajectories. We discuss covering spaces which play an essential role in accounting for the 'wave' properties of quantum particles. We briefly point out how new mathematical techniques take us beyond Hilbert space and into a deeper structure which connects with the algebras originally introduced by Born, Heisenberg and Jordan. This enables us to bring out the geometric aspects of quantum phenomena.

1 Introduction

In a classic paper, Dirac [1] has drawn attention to the similarity of the *form* of the classical dynamical equations expressed in terms of commuting functions and the *form* of the corresponding non-commutative operator equations appearing in the quantum domain. The latter, essentially Heisenberg mechanics, can be represented by matrices and therefore form part of a non-commutative algebraic structure. This is in contrast to the Schrödinger approach which is represented in a formal Hilbert space structure, and leads to more familiar mathematics based on differential operators acting on continuous wave functions, the non-commutativity being taken care of in the form of the differential operators. These techniques, being more familiar to physicists, quickly generated results and placed the Schrödinger picture in

arXiv:1610.09718v1 [math.SG] 30 Oct 2016

HAMILTONIAN AND SYMPLECTIC SYMMETRIES: AN INTRODUCTION

ÁLVARO PELAYO

In memory of Professor J.J. Duistermaat (1942–2010)

ABSTRACT. Classical mechanical systems are modeled by a symplectic manifold (M, ω), and their symmetries, encoded in the action of a Lie group G on M by diffeomorphisms that preserves ω. These actions, which are called "symplectic", have been studied in the past forty years, following the works of Atiyah, Delzant, Duistermaat, Guillemin, Heckman, Kostant, Souriau, and Sternberg in the 1970s and 1980s on symplectic actions of compact abelian Lie groups that are, in addition, of "Hamiltonian" type, i.e. they also satisfy Hamilton's equations. Since then a number of connections with combinatorics, finite dimensional integrable Hamiltonian systems, more general symplectic actions, and topology, have flourished. In this paper we review classical and recent results on Hamiltonian and non Hamiltonian symplectic group actions roughly starting from the results of these authors. The paper also serves as a quick introduction to the basics of symplectic geometry.

1. INTRODUCTION

Symplectic geometry is a geometry concerned with the study of a notion of signed area, rather than length or distance. It can be, as we will see, less intuitive than Euclidean or metric geometry and it is taking mathematicians many years to understand some of its intricacies (which is still work in progress).

The word "symplectic" goes back to Hermann Weyl's (1885-1955) book [159] on Classical Groups (1946). It derives from a Greek word meaning "complex". Since the word "complex" had already a precise meaning in mathematics, and was already used at the time of Weyl, he took the Latin roots of "complex" (which means "plaited together") and replaced them by the Greek roots "symplectic".

The origins of symplectic geometry are in classical mechanics, where the phase space of a mechanical system is modeled by a "symplectic manifold" (M, ω), that is, a smooth manifold M endowed with a non-degenerate closed 2-form $\omega \in \Omega^2(M)$, called a "symplectic form". At each point $x \in M$, $\omega_x \colon \mathrm{T}_x M \times \mathrm{T}_x M \to \mathbb{R}$ is an antisymmetric bilinear form on $\mathrm{T}_x M$, and given $u, v \in \mathrm{T}_x M$ the real number $\omega_x(u, v)$ is called the "symplectic area" spanned by u and v. Intuitively, ω gives a way to measure area along 2-dimensional sections of M, which itself can be of an arbitrarily large dimension.

The most typical example of a symplectic manifold is a cotangent bundle, the phase space of mechanics, which comes endowed with a canonical symplectic form. Initially it was the study of mechanical systems which motivated many of the developments in symplectic geometry.

Joseph-Louis Lagrange (1736-1813) gave the first example of a symplectic manifold in 1808, in his study of the motion of the planets under the influence of their mutual gravitational interaction [100, 101]. An explicit description of Lagrange's construction and his derivation of what are known today as Hamilton's equations is given by Weinstein in [156, Section 2].

The origins of the current view point in symplectic geometry may be traced back to Carl Gustav Jacob Jacobi (1804-1851) and then William Rowan Hamilton's (1805-1865) deep formulation of Lagrangian mechanics, around 1835. Hamilton was expanding on and reformulating ideas of Galileo

arXiv:1611.02108v1 [cs.LO] 7 Nov 2016

Cubical Type Theory: a constructive interpretation of the univalence axiom*

Cyril Cohen, Thierry Coquand, Simon Huber, and Anders Mörtberg

Abstract

This paper presents a type theory in which it is possible to directly manipulate n-dimensional cubes (points, lines, squares, cubes, etc.) based on an interpretation of dependent type theory in a cubical set model. This enables new ways to reason about identity types, for instance, function extensionality is directly provable in the system. Further, Voevodsky's univalence axiom is provable in this system. We also explain an extension with some higher inductive types like the circle and propositional truncation. Finally we provide semantics for this cubical type theory in a constructive meta-theory.

Contents

1 Introduction 2

2 Basic type theory 3

3 Path types 3
- 3.1 Syntax and inference rules . . . 5
- 3.2 Examples . . . 6

4 Systems, composition, and transport 7
- 4.1 The face lattice . . . 7
- 4.2 Syntax and inference rules for systems . . . 9
- 4.3 Composition operation . . . 10
- 4.4 Kan filling operation . . . 11
- 4.5 Equality judgments for composition . . . 11
- 4.6 Transport . . . 12

5 Derived notions and operations 12
- 5.1 Contractible types . . . 12
- 5.2 The pres operation . . . 12
- 5.3 The equiv operation . . . 13

6 Glueing 13
- 6.1 Syntax and inference rules for glueing . . . 13
- 6.2 Composition for glueing . . . 14

7 Universe and the univalence axiom 15
- 7.1 Composition for the universe . . . 15
- 7.2 The univalence axiom . . . 16

*This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Learn Quantum Mechanics with Haskell

Scott N. Walck
Department of Physics
Lebanon Valley College
Annville, Pennsylvania, USA
walck01@lvc.edu

To learn quantum mechanics, one must become adept in the use of various mathematical structures that make up the theory; one must also become familiar with some basic laboratory experiments that the theory is designed to explain. The laboratory ideas are naturally expressed in one language, and the theoretical ideas in another. We present a method for learning quantum mechanics that begins with a laboratory language for the description and simulation of simple but essential laboratory experiments, so that students can gain some intuition about the phenomena that a theory of quantum mechanics needs to explain. Then, in parallel with the introduction of the mathematical framework on which quantum mechanics is based, we introduce a calculational language for describing important mathematical objects and operations, allowing students to do calculations in quantum mechanics, including calculations that cannot be done by hand. Finally, we ask students to use the calculational language to implement a simplified version of the laboratory language, bringing together the theoretical and laboratory ideas.

1 Introduction

The theories of twentieth-century physics employ mathematical objects that are quite removed from our everyday experience of the world and surprisingly removed from the description of the experiments that led to or provided evidence for those theories. Certainly theoretical concepts have motivated and guided experiments—experimental design is awash in theory—but if we consider the simplest description of an experiment, as a chef might write a recipe for a lay cook, the language would not include references to the abstract objects that structure the theorist's calculations.

We focus in this paper on the theory of quantum mechanics, and in particular on the behavior of spin-1/2 particles, some of the very simplest quantum systems which nevertheless contain the essential features of quantum mechanics. We present a Haskell-based method for learning quantum mechanics that takes place within a senior-level quantum mechanics course. Students in the course may have no experience with Haskell or programming at all. We take the attitude of Papert[4] and others[8, 9, 1, 12] that students are aided in their learning by having building blocks with which to create interesting structures, that such creative activity is a motivating and effective way to learn, and that the feedback provided by computer-language-based building blocks can expose our confusions and produce delight in our achievements.

The paper is organized as follows. In section 2, we introduce a laboratory language for the description of experiments with spin-1/2 particles. In section 3, we describe a calculational language for working with kets and operators, the abstract objects used to do calculations. In section 4, we describe a simplified laboratory language that students are asked to implement using the calculational language.

J. Jeuring and J. McCarthy (Eds.): Trends in
Functional Programming in Education (TFPIE)
EPTCS 230, 2016, pp. 31–46, doi:10.4204/EPTCS.230.3

United States Court of Appeals
For the First Circuit

No. 16-1901

KEVIN O'CONNOR; CHRISTOPHER O'CONNOR; JAMES ADAM COX; MICHAEL FRASER; ROBERT MCNALLY,

Plaintiffs, Appellants,

v.

OAKHURST DAIRY; DAIRY FARMERS OF AMERICA, INC.,

Defendants, Appellees.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

[Hon. Nancy Torresen, Chief U.S. District Judge]

Before

Lynch, Lipez, and Barron,
Circuit Judges.

David G. Webbert, with whom Jeffrey Neil Young, Carol J. Garvan, and Johnson, Webbert, and Young, LLP were on brief, for appellants.

David L. Schenberg, with whom Patrick F. Hulla and Ogletree, Deakins, Nash, Smoak and Stewart, P.C. were on brief, for appellees.

March 13, 2017

Prime numbers and L-functions

Henryk Iwaniec*

Abstract. The classical memoir by Riemann on the zeta function was motivated by questions about the distribution of prime numbers. But there are important problems concerning prime numbers which cannot be addressed along these lines, for example the representation of primes by polynomials. In this talk I will show a panorama of techniques, which modern analytic number theorists use in the study of prime numbers. Among these are sieve methods. I will explain how the primes are captured by adopting new axioms for sieve theory. I shall also discuss recent progress in traditional questions about primes, such as small gaps, and fundamental ones such as equidistribution in arithmetic progressions. However, my primary objective is to indicate the current directions in Prime Number Theory.

Mathematics Subject Classification (2000). Primary 11N; Secondary 11L20.

Keywords. Prime numbers, L-functions.

1. Introduction

Prime numbers fascinate every mathematician, regardless of her or his field of main interest. They also capture the attention of people in other professions. I recall my popular talk in May 2005 which I delivered to engineers in my native city Elblag in Poland; never before have I heard questions about primes being asked with greater passion. Since our modern daily life is driven by computers, the prime numbers are used to combat hackers. There are offers of huge monetary awards for finding large prime numbers (which are apparently useful in cryptography). Regardless of industrial applications the prime numbers will always play a fundamental role in number theory, because they are to arithmetic as the elementary particles are to matter in physics. Primes form the heart of analytic number theory. Therefore this is a serious subject in which I have been happily working most of my life (and fortunately being paid to do so). When presenting results in this talk I shall often express my views on methods and perspectives concerning prime numbers. The tools for studying primes (like the L-functions, character sums, bilinear forms, sieve methods, combinatorial identities) are as fascinating as the results themselves; thus I will spend considerable time analyzing the strength of these tools and their potential.

This is not a survey of all that is known about prime numbers. There are truly great results concerning prime numbers, which nevertheless do not seem to give insight into

*Supported by NSF grant DMS-03-01168.

Proceedings of the International Congress of Mathematicians, Madrid, Spain, 2006
© 2007 European Mathematical Society

Verifying Constant-Time Implementations

José Bacelar Almeida, *HASLab/INESC TEC and University of Minho;*
Manuel Barbosa, *HASLab/INESC TEC and DCC FCUP;* Gilles Barthe and François Dupressoir,
IMDEA Software Institute; Michael Emmi, *Bell Labs and Nokia*

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/almeida

This paper is included in the Proceedings of the
25th USENIX Security Symposium

August 10–12, 2016 • Austin, TX

ISBN 978-1-931971-32-4

Open access to the Proceedings of the
25th USENIX Security Symposium
is sponsored by USENIX

arXiv:1701.04343v1 [physics.flu-dyn] 16 Jan 2017

Lagrangian basis method for dimensionality reduction of convection dominated nonlinear flows

Rambod Mojgani[1], Maciej Balajewicz[1]†

[1]Department of Aerospace Engineering, University of Illinois at Urbana-Champaign, Urbana, IL 61820 USA

(Received xx; revised xx; accepted xx)

Foundations of a new projection-based model reduction approach for convection dominated nonlinear fluid flows are summarized. In this method the evolution of the flow is approximated in the Lagrangian frame of reference. Global basis functions are used to approximate both the state and the position of the Lagrangian computational domain. It is demonstrated that in this framework, certain wave-like solutions exhibit low-rank structure and thus, can be efficiently compressed using relatively few global basis. The proposed approach is successfully demonstrated for the reduction of several simple but representative problems.

Key words:

1. Introduction

Numerical simulation of nonlinear fluid flows often requires prohibitively large computational resources. High–fidelity simulations of high-Reynolds numbers flows, high–speed compressible flows, and combustion often require very fine spatial and temporal discretizations to accurately resolve the multi–scale dynamics. There are significant scientific and engineering benefits to developing model reduction techniques that are capable of delivering physics–based, low–dimensional models.

Most existing model order reduction (MOR) approaches are based on projection (Benner *et al.* 2015). In projection-based MOR, the states of the flow are approximated in a low-dimensional subspace and Galerkin or Petrov-Galerkin projection is used to yield reduced-order models capable of, in principle, delivering new solutions at a fraction of the computational costs of the original high-fidelity model (HFM).

Despite the efficacy and success of MOR approaches, wave-like solutions, or solutions featuring moving sharp gradients, shocks or interfaces remain a major hurdle for projection-based MOR. It is well known that this hurdle is the result of the spectral decomposition of the solution, and not the type of basis used. It is simply not possible to efficiently compress solutions with moving discontinuities or sharp gradients using a summation of products of global spatial and temporal basis functions. Over the years, several remedies have been proposed. For example, local basis (Ansallem *et al.* 2012), domain decomposition (Lucia 2001) or basis splitting (Carlberg 2015) algorithm have been developed. Unfortunately, the complexity of these algorithms often make extensions

† Email address for correspondence: mbalajew@illinois.edu

Verified Low-Level Programming Embedded in F*

JONATHAN PROTZENKO, Microsoft Research
JEAN-KARIM ZINZINDOHOUÉ, INRIA Paris
ASEEM RASTOGI, Microsoft Research
TAHINA RAMANANANDRO, Microsoft Research
PENG WANG, MIT CSAIL
SANTIAGO ZANELLA-BÉGUELIN, Microsoft Research
ANTOINE DELIGNAT-LAVAUD, Microsoft Research
CĂTĂLIN HRIŢCU, INRIA Paris
KARTHIKEYAN BHARGAVAN, INRIA Paris
CÉDRIC FOURNET, Microsoft Research
NIKHIL SWAMY, Microsoft Research

arXiv:1703.00053v5 [cs.PL] 30 Aug 2017

We present Low*, a language for low-level programming and verification, and its application to high-assurance optimized cryptographic libraries. Low* is a shallow embedding of a small, sequential, well-behaved subset of C in F*, a dependently-typed variant of ML aimed at program verification. Departing from ML, Low* does not involve any garbage collection or implicit heap allocation; instead, it has a structured memory model à la CompCert, and it provides the control required for writing efficient low-level security-critical code.

By virtue of typing, any Low* program is memory safe. In addition, the programmer can make full use of the verification power of F* to write high-level specifications and verify the functional correctness of Low* code using a combination of SMT automation and sophisticated manual proofs. At extraction time, specifications and proofs are erased, and the remaining code enjoys a predictable translation to C. We prove that this translation preserves semantics and side-channel resistance.

We provide a new compiler back-end from Low* to C and, to evaluate our approach, we implement and verify various cryptographic algorithms, constructions, and tools for a total of about 28,000 lines of code, specification and proof. We show that our Low* code delivers performance competitive with existing (unverified) C cryptographic libraries, suggesting our approach may be applicable to larger-scale low-level software.

Additional Key Words and Phrases: verified compilation, low-level programming, verified cryptography

1 INTRODUCTION

In the pursuit of high performance, cryptographic software widely deployed throughout the internet is still often subject to dangerous attacks [Int 2017; Dou 2017; Use 2017; Afek and Sharabani 2007; AlFardan and Paterson 2013; Bhargavan et al. 2014a; Bhargavan and Leurent 2016; Böck 2016; Böck et al. 2016; Dobraunig 2003; Duong and Rizzo 2011; Heartbleed 2014; Möller et al. 2014; Pincus and Baker 2004; Rizzo and Duong 2012; Smyth and Pironti 2014; Somorovsky 2016; Stevens et al. 2016; Święcki 2016; Szekeres et al. 2013; Wagner and Schneier 1996]. Recognizing a clear need, the programming language, verification, and applied cryptography communities are devoting significant efforts to develop implementations proven secure by construction against broad classes of these attacks.

This work is licensed under a Creative Commons Attribution 4.0 International License
© 2017 Copyright held by the owner/author(s).

arXiv:1703.08561v2 [cs.RO] 29 Mar 2017

AutonoVi: Autonomous Vehicle Planning with Dynamic Maneuvers and Traffic Constraints

Andrew Best[1] and Sahil Narang[1] and Daniel Barber[2] and Dinesh Manocha[1]
http://gamma.cs.unc.edu/AutonoVi/video.avi (video included)

Abstract— **We present AutonoVi, a novel algorithm for autonomous vehicle navigation that supports dynamic maneuvers and satisfies traffic constraints and norms. Our approach is based on optimization-based maneuver planning that supports dynamic lane-changes, swerving, and braking in all traffic scenarios and guides the vehicle to its goal position. We take into account various traffic constraints, including collision avoidance with other vehicles, pedestrians, and cyclists using control velocity obstacles. We use a data-driven approach to model the vehicle dynamics for control and collision avoidance. Furthermore, our trajectory computation algorithm takes into account traffic rules and behaviors, such as stopping at intersections and stoplights, based on an arc-spline representation. We have evaluated our algorithm in a simulated environment and tested its interactive performance in urban and highway driving scenarios with tens of vehicles, pedestrians, and cyclists. These scenarios include jaywalking pedestrians, sudden stops from high speeds, safely passing cyclists, a vehicle suddenly swerving into the roadway, and high-density traffic where the vehicle must change lanes to progress more effectively.**

I. INTRODUCTION

Autonomous driving is a difficult and extremely complex task that has immense potential for impacting the lives of billions of people. In order to develop autonomous capabilities to perform the driving task, we need appropriate capabilities to sense and predict the traffic and road obstacles, as well as for planning, control, and coordination of the vehicle [1], [2]. There is considerable research in this area that borrows ideas from different disciplines including computer vision, machine learning, motion planning, mechanical engineering, intelligent traffic simulation, human-factors psychology, etc.

Research into sensing and perception technologies has been progressing considerably and current vehicle sensors seem to have the capability to detect relevant obstacles, vehicles, and other traffic entities including bicycles and pedestrians. However, automatic planning in different scenarios and the computation of the appropriate response to vehicle and non-vehicle entities, such as bicycles and pedestrians, are still the subjects of ongoing research. A key issue is the development of an efficient navigation algorithm for autonomous driving that takes into account the vehicle dynamics, sensor inputs, traffic rules and norms, and the driving behaviors of other vehicles. Moreover, the uncertainties in the sensor data, capability, and response of the autonomous vehicle, typically referred to as the *ego-vehicle* [3], have led to the development of behavior and navigation algorithms that impose conservative limits on the acceleration, deceleration, and steering decisions. For example, algorithms tend to limit hazard responses to either steering [4], [5] or braking [6]. Few algorithms demonstrate combined control of throttle and steering and typically do so in constrained navigation scenarios [7]. In terms of planning the routes and navigating the roads, current algorithms tend to limit the lane-changing behaviors, precluding their use for progressing more quickly to a goal or better utilization of the road conditions. These limitations have led to the perception that autonomous cars behave more like student drivers taking their driving test than actual skilled human drivers [3]. One of the goals is to extend the capabilities of current autonomous vehicles in terms of planning, control, and navigation, making them less conservative but still allowing safe performance during driving.

Main contributions: We present a novel navigation algorithm for autonomous vehicles, AutonoVi, which utilizes a data-driven vehicle dynamics model and optimization-based maneuver planning to compute a safe, collision-free trajectory with dynamic lane-changes. Our approach is general, makes no assumption about the traffic conditions, and plans dynamically feasible maneuvers in traffic consisting of other vehicles, cyclists, and pedestrians. In order to develop an autonomous vehicle planning approach with these capabilities, we present four novel algorithms:

- **Optimization-based Maneuvering:** We describe a novel multi-objective optimization approach for evaluating the dynamic maneuvers. Our algorithm encodes passenger comfort, safe passing distances, maneuver constraints in terms of dynamics, and global route progress in order to compute appropriate trajectories.
- **Data driven Vehicle Dynamics:** We use a data-driven vehicle dynamics formulation that encodes feasible accelerations, steering rates, and decelerations into a set of per-vehicle profile functions, which can be quickly evaluated. These profiles are generated by simulating the ego-vehicle through a series of trials to obtain lateral and longitudinal slip profiles. This data-driven model generalizes to multiple vehicles and configurations.
- **Collision avoidance with kinematic and dynamic constraints:** We present a collision avoidance algorithm that combines collision-free constraints with specific kinematic and dynamic constraints of the autonomous vehicle. Our approach allows the autonomous vehicle to steer away from collisions with other vehicles, pedes-

[1]Andrew Best and Sahil Narang and Dinesh Manocha are at the University of North Carolina, Chapel Hill
[2] Daniel Barber is at the University of Central Florida

arXiv:1703.10987v1 [cs.CY] 31 Mar 2017

On the Impossibility of Supersized Machines

Ben Garfinkel , Miles Brundage[1], Daniel Filan[2], Carrick Flynn[3], Jelena Luketina , Michael Page , Anders Sandberg[3], Andrew Snyder-Beattie[3], and Max Tegmark[4]

[1]*School for the Future of Innovation in Society, Arizona State University*
[2]*Department of Computer Science, University of California, Berkeley*
[3]*Future of Humanity Institute, University of Oxford*
[4]*Department of Physics, Massachusetts Institute of Technology*

April 1, 2017

Abstract

In recent years, a number of prominent computer scientists, along with academics in fields such as philosophy and physics, have lent credence to the notion that machines may one day become as large as humans. Many have further argued that machines could even come to exceed human size by a significant margin. However, there are at least seven distinct arguments that preclude this outcome. We show that it is not only implausible that machines will ever exceed human size, but in fact impossible.

Introduction

The history of life is often understood as a story of growth. If one takes the long view, then one can trace an exponential curve from our minuscule earliest ancestors, which were little more than self-replicating molecules, to the substantial creatures that we are today (Payne, 2009).

Although humanity became aware of this story only in the 19th century, through the work of Charles Darwin, we have long had the privilege of witnessing a partial recapitulation every time someone new comes into the world (Darwin, 1859). Before each person is a full-sized adult, they are first an invisibly small cell.

It is perhaps no surprise, then, that human largeness has for thousands of years fascinated many of our greatest thinkers. While some have sought to understand the nature and origins of largeness, others have anxiously inquired: *Could there ever be something larger than a human?*

Evidence of this anxiety can be found as far back as humanity's oldest recorded myth, *The Epic of Gilgamesh*, in which the monstrous giant Humbaba is appointed by Enlil, the king of the gods, to terrorize mankind (Sanders,

SPINK

27 SEPTEMBER 2017

LONDON

THE SHAMSHIR AND LION COLLECTION OF PERSIAN BANKNOTES

arXiv:1705.01171v1 [math.MG] 30 Apr 2017

Acute sets

D. Zakharov

Abstract

A set of points in $\mathbb{R}^d$ is *acute*, if any three points from this set form an acute angle. In this note we construct an acute set in $\mathbb{R}^d$ of size at least $2^{d/2}$.

A set of points in $\mathbb{R}^d$ is *acute*, if any three points from this set form an acute angle. In 1972 Danzer and Grünbaum [1] posed the following question: what is the maximum size $f(d)$ of an acute set in $\mathbb{R}^d$? They proved a linear lower bound $f(d) \geqslant 2d-1$ and conjectured that this bound is tight. However, in 1983 Erdős and Füredi [2] disproved this conjecture in large dimensions. They gave an exponential lower bound

$$f(d) \geqslant \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^d > 0,5 \cdot 1,154^d.$$

Their proof is a very elegant application of the probabilistic method. One drawback of their method is that only the existence of an acute set of such size is proven, with no possibility to turn it into an explicit construction.

In 2011 Harangi [3] refined the approach of Erdős and Füredi and improved their bound to

$$f(d) \geqslant c\left(\sqrt[10]{\frac{144}{23}}\right)^d > c \cdot 1,2^d.$$

In this note we prove the following recurrent inequality:

Theorem 1. $f(d+2) \geqslant 2f(d)$.

Theorem 1 easily implies the bound

$$f(d) \geqslant 2^{\frac{d}{2}+1} \quad \text{for} \quad n \geqslant 4,$$

since it is known [3] that $f(4) \geqslant 8$ and $f(5) \geqslant 12$.

The proof of Theorem 1 is explicit and allows to construct acute sets effectively.

The best known upper bound on $f(d)$ is $f(d) \leqslant 2^d - 1$, and follows from the main result of [1]. Danzer and Grünbaum proved that if a set S of points in $\mathbb{R}^d$ determines only acute and right angles, then $|S| \leqslant 2^d$. Moreover, if $|S| = 2^d$, then S must be an affine image of a d-dimensional cube.

Proof of Theorem 1. The scalar product of two vectors u, v is denoted by $\langle u, v\rangle$. Take the largest acute set $X \subset \mathbb{R}^d$, $|X| = f(d)$. Put

$$s := \min\{\langle y-x, z-x\rangle : x, y, z \in X, x \neq y, x \neq z\}.$$

Mon. Not. R. Astron. Soc. **000**, 1–77 (2016) Printed 4 May 2017 (MN LATEX style file v2.2)

Transit Detection of a "Starshade" at the Inner Lagrange Point of an Exoplanet

E. Gaidos,[1]*
[1] *Department of Geology & Geophysics, University of Hawaii at Mānoa, Honolulu, Hawaii 96822 USA*

arXiv:1705.01285v1 [astro-ph.EP] 3 May 2017

Submitted to MNRAS

ABSTRACT

All water-covered rocky planets in the inner habitable zones of solar-type stars will inevitably experience a catastrophic runaway climate due to increasing stellar luminosity and limits to outgoing infrared radiation from wet greenhouse atmospheres. Reflectors or scatterers placed near Earth's inner Lagrange point ($\mathcal{L}_1$) have been proposed as a "geo-engineering" solution to anthropogenic climate change and an advanced version of this could modulate incident irradiation over many Gyr or "rescue" a planet from the interior of the habitable zone. The distance of the starshade from the planet that minimizes its mass is 1.6 times the Earth-$\mathcal{L}_1$ distance. Such a starshade would have to be similar in size to the planet and the mutual occultations during planetary transits could produce a characteristic maximum at mid-transit in the light-curve. Because of a fortuitous ratio of densities, Earth-size planets around G dwarf stars present the best opportunity to detect such an artifact. The signal would be persistent and is potentially detectable by a future space photometry mission to characterize transiting planets. The signal could be distinguished from natural phenomenon, i.e. starspots or cometary dust clouds, by its shape, persistence, and transmission spectrum.

Key words: techniques: photometric – planets and satellites: terrestrial planets – astrobiology – extraterrestrial intelligence –

1 INTRODUCTION

Like every liquid water-covered planet around a solar-mass star, Earth has a serious greenhouse problem. As the Sun converts hydrogen to helium and becomes denser, hotter, and more luminous (Gough 1981) the inexorable increase in incident irradiation on Earth will, all else being equal, cause surface temperatures to rise and the atmosphere to contain more water vapor. Water is an efficient greenhouse gas, creating a positive feedback in Earth's climate system as more water vapor leads to elevated temperatures, and vice versa. Walker, Hays & Kasting (1981) proposed that temperature-dependent aqueous weathering and precipitation of carbonate minerals acts as a negative climate feedback that adjusts atmospheric CO_2 to maintain weathering at a rate that balances volcanic degassing, i.e. surface temperatures permissive of abundant liquid water.

However this planetary "thermostat" has its limits. As irradiance continues to increase, CO_2 will eventually disappears from the atmosphere causing a crisis for land plant life and any indeed any autotrophic life relying on atmospheric CO_2 as a source of carbon (Caldeira & Kasting 1992). Beyond this point, increasing irradiance cannot be compensated by diminished CO_2 and temperatures rise. Climate models predict an asymptotic (maximum) value for the outgoing infrared radiation of an Earth-like atmosphere as a function of temperature; if the absorbed incident radiation exceeds this value, temperatures will increase until the oceans evaporate (Ingersoll 1969). At that point multiple "runaway" climate feed-backs, not mutually exclusive, can occur: water vapor in the upper atmosphere will be photolyzed and the escape of hydrogen will lead to loss of water. Continued de-gassing of CO_2 from the mantle will not be compensated by aqueous weathering of silicates and formation of carbonates, enhancing the greenhouse effect and causing higher surface temperatures. Eventually, surface temperatures will exceed the stability of carbonate minerals, leading to the breakdown of carbonate rocks in the crust, the release of ≈60 bars of CO_2 into the atmosphere (Tuck 1980), a Venus-like climate, and the complete extinction of the biosphere. Because of stellar luminosity evolution, all Earth-like planets within the "conservative" habitable zone of solar-mass stars (0.95-1.67 AU Kopparapu et al. 2013) will eventually orbit interior to the habitable zone and meet this fate.

* Visiting Scientist, Center for Space and Habitability, University of Bern, Bern, Sitzerland. E-mail: gaidos@hawaii.edu (EG)

Experimental demonstration of a measurement-based simulation of an open quantum system

W. McCutcheon,[1] A. McMillan,[1] J. G. Rarity,[1] and M. S. Tame[2,*]

[1]*Quantum Engineering Technology Laboratory, Department of Electrical and Electronic Engineering, University of Bristol, Woodland Road, Bristol, BS8 1UB, UK*

[2]*School of Chemistry and Physics, University of KwaZulu-Natal, Durban 4001, South Africa*

(Dated: May 10, 2017)

We introduce and experimentally demonstrate a method for simulating open quantum systems using the measurement-based model. Using a photonic setup and modifying the bases of single-qubit measurements on a four-qubit entangled cluster state, representative open quantum system dynamics are realised for the case of a single qubit in the form of amplitude and phase damping channels. The experimental results match the theoretical model well, demonstrating the successful performance of the simulations. We also show how other types of quantum channels can be realised using our approach. This work highlights the potential of the measurement-based model for simulating realistic open quantum systems.

arXiv:1705.03032v1 [quant-ph] 8 May 2017

Introduction.— The simulation of quantum systems is an important topic at present as it promises to open up investigations into many new areas of science [1–3]. This includes exploring exotic states of matter [4], thermalisation and equilibration processes [5, 6], chemical reaction dynamics [7] and probing quantum effects in biological systems [8, 9]. A number of approaches to simulation are currently being studied, using both classical and quantum methods. While classical methods are limited to specific conditions for efficient simulation of quantum systems [10, 11], quantum methods have a much larger scope, and a range of techniques have been developed so far, such as analogue [1, 2], digital [12, 13], digital-analogue [14, 15], algorithmic [16–18] and embedded [19, 20], each with its own advantages and disadvantages. Most methods consider ideal quantum systems, where the constituent elements are isolated from the outside world. However, realistic quantum systems are 'open' as they invariably interact with some environment [21]. Work on simulating realistic open quantum systems has seen much progress recently [22–24], and promises to shed light on fundamental physical phenomena, including phase transitions in dissipative systems [25–27], thermalisation [28, 29] and using dissipation as a resource [30, 31]. In this context, the development of techniques to simulate quantum channels [32, 33] representing the dynamics of open quantum systems has seen rapid growth – most notably for single qubits [34–41] and qudits [42–44]. So far, however, studies have been limited to the standard quantum circuit model [45].

A natural model for simulating quantum systems is the measurement-based model [46–48], which has been used to demonstrate the simulation of quantum computing on entangled resource states using only single-qubit measurements [49–55]. The measurement-based model is an interesting method for simulating quantum systems, as it can achieve simulation simply by carrying out quantum computing [56]. However, there is also the possibility of going further by exploiting the structure of the entangled resource being used to reduce the overall complexity and put a given simulation within reach of current technology. Recently, the first steps in this direction have been taken theoretically [57]. Despite this potential, the simulation of realistic open quantum systems using the measurement-based model has not yet been explored.

In our work we address this issue by introducing and experimentally demonstrating a method for the simulation of an open quantum system using the measurement-based model for the simple case of a single qubit. To do this, we find an efficient mapping from the circuit model to the measurement-based model for the simulation, which allows us to consider the use of an entangled linear cluster state of only four qubits made from three photons – using the polarization degree of freedom of each photon as a qubit and the path degree of freedom of one of the photons as an additional qubit. By measuring the qubits of the cluster state in a particular way we are able to simulate arbitrary damping channels on a logical qubit residing within the cluster state. The advantage of this measurement-based approach over the standard circuit model [36–41] is that only the pattern of measurements needs to be modified in order to implement different system dynamics. This is particularly useful in a photonic setting, where a reconfiguring of the basic optical elements is not required, both in bulk [49–55] and on-chip setups [58–60]. The experimental results obtained match the theoretical expectations well and highlight the potential use of the measurement-based model as an alternative approach to simulating open quantum systems.

Experimental setup.— The experimental setup is shown in Fig. 1 (a). It generates a four-qubit linear cluster state made of three photons – three qubits are encoded in the polarisation degree of freedom of three photons using the basis $\{|H\rangle, |V\rangle\}$, and the fourth qubit is encoded in the path degree of freedom of one of the photons using the basis $\{|p_1\rangle, |p_2\rangle\}$. The photons are generated by spontaneous four-wave mixing in photonic crystal fibers (PCFs) tailored to generate a spectrally separable naturally narrowband bi-photon state cross-polarised to the pump [61, 62]. The signal wavelength is $\lambda_s \approx 625$ nm and the idler wavelength is $\lambda_i \approx 876$ nm when the PCF is pumped at $\lambda_p = 726$ nm. For the pump laser a 80 MHz repetition rate femto-second Ti-Sapphire laser is filtered through a 4F arrangement, with a spectral mask on the Fourier plane achieving the desired spectrum with bandwidth $\Delta\lambda_p = 1.7$ nm, which is then sent to two PCF sources. One of the PCF sources (PCF 1) is arranged in a twisted

arXiv:1707.04757v1 [cs.LO] 15 Jul 2017

Formalization of the fundamental group in untyped set theory using auto2

Bohua Zhan

Massachusetts Institute of Technology

Abstract. We present a new framework for formalizing mathematics in untyped set theory using auto2. Using this framework, we formalize in Isabelle/FOL the entire chain of development from the axioms of set theory to the definition of the fundamental group for an arbitrary topological space. The auto2 prover is used as the sole automation tool, and enables succinct proof scripts throughout the project.

1 Introduction

Auto2, introduced by the author in [17], is a proof automation tool for the proof assistant Isabelle. It is designed to be a powerful, extensible prover that can consistently solve "routine" tasks encountered during a proof, thereby enabling a style of formalization using succinct proof scripts written in a custom, purely declarative language.

In this paper, we present an application of auto2 to formalization of mathematics in untyped set theory [1]. In particular, we discuss the formalization in Isabelle/FOL of the entire chain of development from the axioms of set theory to the definition of the fundamental group for an arbitrary topological space. Along the way, we discuss several improvements to auto2 as well as strategies of usage that allow us to work effectively with untyped set theory.

The contribution of this paper is two-fold. First, we demonstrate that the auto2 system is capable of independently supporting proof developments on a relatively large scale. In the previous paper, several case studies for auto2 were given in Isabelle/HOL. Each case study is at most several hundred lines long, and the use of auto2 is mixed with the use of other Isabelle tactics, as well as proof scripts provided by Sledgehammer. In contrast, the example we present in this paper is a unified development consisting of over 13,000 lines of theory files and 3,500 lines of ML code (not including the core auto2 program). The auto2 prover is used exclusively starting from basic set theory.

Second, we demonstrate one way to manage the additional complexity in proofs that arise when working with untyped set theory. For a number of reasons, untyped set theory is considered to be difficult to work with. For example, everything is represented as sets, including objects such as natural numbers that we usually do not think of as sets. Moreover, statements of theorems tend to

[1] Code available at https://github.com/bzhan/auto2

arXiv:1708.02749v1 [cs.CR] 9 Aug 2017

Rise of the HaCRS:

Augmenting Autonomous Cyber Reasoning Systems with Human Assistance

Yan Shoshitaishvili
Arizona State University
yan.shoshitaishvili@asu.org

Michael Weissbacher
Northeastern University
mrw@ccs.neu.edu

Lukas Dresel
UC Santa Barbara
lukas.dresel@cs.ucsb.edu

Christopher Salls
UC Santa Barbara
salls@cs.ucsb.edu

Ruoyu Wang
UC Santa Barbara
fish@cs.ucsb.edu

Christopher Kruegel
UC Santa Barbara
chris@cs.ucsb.edu

Giovanni Vigna
UC Santa Barbara
vigna@cs.ucsb.edu

ABSTRACT

Software permeates every aspect of our world, from our homes to the infrastructure that provides mission-critical services.

As the size and complexity of software systems increase, the number and sophistication of software security flaws increase as well. The analysis of these flaws began as a manual approach, but it soon became apparent that a manual approach alone cannot scale, and that tools were necessary to assist human experts in this task, resulting in a number of techniques and approaches that automated certain aspects of the vulnerability analysis process.

Recently, DARPA carried out the Cyber Grand Challenge, a competition among autonomous vulnerability analysis systems designed to push the tool-assisted human-centered paradigm into the territory of complete automation, with the hope that, by removing the human factor, the analysis would be able to scale to new heights. However, when the autonomous systems were pitted against human experts it became clear that certain tasks, albeit simple, could not be carried out by an autonomous system, as they require an understanding of the logic of the application under analysis.

Based on this observation, we propose a shift in the vulnerability analysis paradigm, from tool-assisted human-centered to human-assisted tool-centered. In this paradigm, the automated system orchestrates the vulnerability analysis process, and leverages humans (with different levels of expertise) to perform well-defined sub-tasks, whose results are integrated in the analysis. As a result, it is possible to scale the analysis to a larger number of programs, and, at the same time, optimize the use of expensive human resources.

In this paper, we detail our design for a human-assisted automated vulnerability analysis system, describe its implementation atop an open-sourced autonomous vulnerability analysis system that participated in the Cyber Grand Challenge, and evaluate and discuss the significant improvements that non-expert human assistance can offer to automated analysis approaches.

1 INTRODUCTION

Software has become dominant and abundant. Software systems support almost every aspect of our lives, from health care to finance, from power distribution to entertainment. This growth has led to an explosion of software bugs and, more importantly, software vulnerabilities. Because the exploitation of vulnerabilities can have catastrophic effects, a substantial amount of effort has been devoted to discovering these vulnerabilities before they are found by attackers and exploited in the wild.

Traditionally, vulnerability discovery has been a heavily manual task. Expert security researchers spend significant time analyzing software, understanding how it works, and painstakingly sifting it for bugs. Even though human analysts take advantage of tools to automate some of the tasks involved in the analysis process, the amount of software to be analyzed grows at an overwhelming pace. As this growth reached the scalability limits of manual analysis, the research community has turned its attention to *automated program analysis*, with the goal of identifying and fixing software issues on a large scale. This push has been met with significant success, culminating thus far in the DARPA Cyber Grand Challenge (CGC) [27], a cyber-security competition in which seven finalist teams pitted completely autonomous systems, utilizing automated program analysis techniques, against each other for almost four million dollars in prize money.

By removing the human factor from the analysis process, the competition forced the participants to codify the strategy and orchestration tasks that are usually performed by experts, and, at the same time, it pushed the limits of current vulnerability analysis techniques to handle larger, more complex problems in an efficient and resource-aware manner. These systems represented a significant step in automated program analysis, automatically identifying vulnerabilities and developing exploits for 20 of a total of 82 binary programs developed for the event.

Despite the success of these systems, the underlying approaches suffer from a number of limitations. These limitations became evident when some of the CGC autonomous systems participated in a follow-up vulnerability analysis competition (the DEFCON CTF) that included human teams. The autonomous systems could not easily understand the logic underlying certain applications, and, as a result, they could not easily produce inputs that drive them to specific (insecure) states. However, when humans could provide "suggestions" of inputs to the automated analysis process the results were surprisingly good.

This experience suggested a shift in the current vulnerability analysis paradigm, from the existing tool-assisted human-centered paradigm to a new human-assisted tool-centered paradigm. Systems that follow this paradigm would be able to leverage humans (with

arXiv:1708.09445v1 [cs.CR] 30 Aug 2017

Coppersmith's lattices and "focus groups": an attack on small-exponent RSA

Stephen D. Miller*, Bhargav Narayanan,
{miller,narayanan}@math.rutgers.edu
and Ramarathnam Venkatesan
venkie@microsoft.com

September 1, 2017

Abstract

We present a principled technique for reducing the matrix size in some applications of Coppersmith's lattice method for finding roots of modular polynomial equations. It relies on an analysis of the actual performance of Coppersmith's attack for smaller parameter sizes, which can be thought of as "focus group" testing. When applied to the small-exponent RSA problem, it reduces lattice dimensions and consequently running times (sometimes by factors of two or more). We also argue that existing metrics (such as enabling condition bounds) are not as important as often thought for measuring the true performance of attacks based on Coppersmith's method. Finally, experiments are given to indicate that certain lattice reductive algorithms (such as Nguyen-Stehlé's L2) may be particularly well-suited for Coppersmith's method.

1 Introduction

Ever since Shamir's devastating attack on the Knapsack cryptosystem [S], lattice reduction algorithms such as [LLL] have had surprising success against

*Supported by NSF grant CNS-1522633.

A Touch of Evil: High-Assurance Cryptographic Hardware from Untrusted Components

Vasilios Mavroudis
University College London
v.mavroudis@cs.ucl.ac.uk

Andrea Cerulli
University College London
andrea.cerulli.13@ucl.ac.uk

Petr Svenda
Masaryk University
svenda@fi.muni.cz

Dan Cvrcek
Enigmabridge
dan@enigmabridge.com

Dusan Klinec
Enigmabridge
dusan@enigmabridge.com

George Danezis
University College London
g.danezis@ucl.ac.uk

arXiv:1709.03817v1 [cs.CR] 12 Sep 2017

ABSTRACT

The semiconductor industry is fully globalized and integrated circuits (ICs) are commonly defined, designed and fabricated in different premises across the world. This reduces production costs, but also exposes ICs to supply chain attacks, where insiders introduce malicious circuitry into the final products. Additionally, despite extensive post-fabrication testing, it is not uncommon for ICs with subtle fabrication errors to make it into production systems. While many systems may be able to tolerate a few byzantine components, this is not the case for cryptographic hardware, storing and computing on confidential data. For this reason, many error and backdoor detection techniques have been proposed over the years. So far all attempts have been either quickly circumvented, or come with unrealistically high manufacturing costs and complexity.

This paper proposes Myst, a practical high-assurance architecture, that uses commercial off-the-shelf (COTS) hardware, and provides strong security guarantees, even in the presence of multiple malicious or faulty components. The key idea is to combine protective-redundancy with modern threshold cryptographic techniques to build a system tolerant to hardware trojans and errors. To evaluate our design, we build a Hardware Security Module that provides the highest level of assurance possible with COTS components. Specifically, we employ more than a hundred COTS secure cryptocoprocessors, verified to FIPS140-2 Level 4 tamper-resistance standards, and use them to realize high-confidentiality random number generation, key derivation, public key decryption and signing. Our experiments show a reasonable computational overhead (less than 1% for both Decryption and Signing) and an exponential increase in backdoor-tolerance as more ICs are added.

KEYWORDS

cryptographic hardware; hardware trojans; backdoor-tolerance; secure architecture

1 INTRODUCTION

Many critical systems with high security needs rely on secure cryptoprocessors to carry out sensitive security tasks (e.g., key generation and storage, legally binding digital signature, code signing) and provide a protection layer against cyber-attacks and security breaches. These systems are typically servers handling sensitive data, banking infrastructure, military equipment and space stations. In most cases, secure cryptoprocessors come embedded into Hardware Security Modules, Trusted Platform Modules and Cryptographic Accelerators, which are assumed to be both secure and reliable. This entails that errors in any of the Integrated Circuits (ICs) would be devastating for the security of the final system. For this reason, the design and fabrication of the underlying ICs must abide f to high-quality specifications and standards. These ensure that there are no intentional or unintentional errors in the circuits, but more importantly ensure the integrity of the hardware supply chain. [50].

Unfortunately, vendors are not always able to oversee all parts of the supply chain [36, 58]. The constant reduction in transistor size makes IC fabrication an expensive process, and IC designers often outsource the fabrication task to overseas foundries to reduce their costs [33, 44, 97]. This limits vendors to run only post-fabrication tests to uncover potential defects. Those tests are very efficient against common defects, but subtle errors are hard to uncover. For instance, cryptoprocessors with defective RNG modules and hardware cipher implementations have made it into production in the past [30, 37].

Additionally, parts of the IC's supply chain are left vulnerable to attacks from malicious insiders [11, 61, 65, 82] and have a higher probability of introducing unintentional errors in the final product. In several documented real-world cases, contained errors, backdoors or trojan horses. For instance, recently an exploitable vulnerability was discovered on Intel processors that utilize Intel Active Management Technology (AMT) [47], while vulnerable ICs have been reported in military [57, 76] applications, networking equipment [38, 48], and various other application [2, 54, 74, 75]. Furthermore, the academic community has designed various types of hardware trojans (HT), and backdoors that demonstrate the extent of the problem and its mitigation difficulty [10, 17, 22, 52, 63, 89–91].

Due to the severity of these threats, there is a large body of work on the mitigation of malicious circuitry. Existing works have pursued two different directions: detection and prevention. Detection techniques aim to determine whether any HTs exist in a given circuit [3, 77, 93, 95], while prevention techniques either impede the introduction of HTs, or enhance the efficiency of HT detection [27, 67, 86, 87, 92]. Unfortunately, both detection and prevention techniques are brittle, as new threats are able to circumvent them quickly [92]. For instance, analog malicious hardware [96] was able to evade known defenses, including split manufacturing, which is considered one of the most promising and effective prevention approaches. Furthermore, most prevention techniques come with a high manufacturing cost for higher levels of security [18, 27, 92].

Another Flip in the Wall of Rowhammer Defenses

Daniel Gruss[1], Moritz Lipp[1], Michael Schwarz[1], Daniel Genkin[2],
Jonas Juffinger[1], Sioli O'Connell[3], Wolfgang Schoechl[1], and Yuval Yarom[3,4]
[1] Graz University of Technology
[2] University of Pennsylvania and University of Maryland
[3] University of Adelaide
[4] Data61

arXiv:1710.00551v1 [cs.CR] 2 Oct 2017

Abstract—**The Rowhammer bug allows unauthorized modification of bits in DRAM cells from unprivileged software, enabling powerful privilege-escalation attacks. Sophisticated Rowhammer countermeasures have been presented, aiming at mitigating the Rowhammer bug or its exploitation. However, the state of the art provides insufficient insight on the completeness of these defenses.**

In this paper, we present novel Rowhammer attack and exploitation primitives, showing that even a combination of all defenses is ineffective. Our new attack technique, *one-location hammering*, breaks previous assumptions on requirements for triggering the Rowhammer bug, i.e., we do not hammer multiple DRAM rows but only keep one DRAM row constantly open. Our new exploitation technique, *opcode flipping*, bypasses recent isolation mechanisms by flipping bits in a predictable and targeted way in userspace binaries. We replace conspicuous and memory-exhausting spraying and grooming techniques with a novel reliable technique called *memory waylaying*. Memory waylaying exploits system-level optimizations and a side channel to coax the operating system into placing target pages at attacker-chosen physical locations. Finally, we abuse Intel SGX to hide the attack entirely from the user and the operating system, making any inspection or detection of the attack infeasible. Our Rowhammer enclave can be used for coordinated denial-of-service attacks in the cloud and for privilege escalation on personal computers. We demonstrate that our attacks evade all previously proposed countermeasures for commodity systems.

1. Introduction

The Rowhammer bug is a hardware reliability issue in which an attacker repeatedly accesses (*hammers*) DRAM cells to cause unauthorized changes in physically adjacent memory locations. Since its initial discovery as a security issue [38], Rowhammer's ability to defy abstraction barriers between different security domains has been extensively used for mounting devastating attacks on various systems. Examples of previous attacks include privilege escalation, from native environments [58], from within a browser's sandbox [21], and from within virtual machines running on third-party compute clouds [63], mounting fault attacks on cryptographic primitives [9, 53], and obtaining root privileges on mobile phones [61]. Recognizing the apparent danger, these attacks have sparked interest in developing effective and efficient mitigation techniques. While existing hardware countermeasures such as using memory with error-correction codes (ECC-RAM) appear to make Rowhammer attacks harder [38], ECC-RAM is intended for server computers and is typically not supported on consumer-grade machines.

Software-based mitigations, which can be implemented on commodity systems, have also been proposed. These include ad-hoc defense techniques such as doubling the RAM refresh rates [38], removing unprivileged access to the `pagemap` interface [39, 55, 58], and prohibiting the `clflush` instruction [58]. However, recent works have already bypassed these countermeasures [6, 21, 61]. Other ad-hoc attempts, such as disabling page deduplication by default [46, 54], only prevent specific Rowhammer attacks exploiting these features [10, 53], but not all Rowhammer attacks.

The research community proposed sophisticated defenses which seemingly have solved the Rowhammer problem. Based on the underlying primitives of these defenses, we introduce a new systematic categorization into five defense classes:

- **Static Analysis.** Binary code is analyzed for specific behavior, common in side-channel attacks, e.g., using high-resolution timers or cache flush instructions [25, 32].
- **Monitoring Performance Counters.** Rowhammer relies on frequent accesses to DRAM cells, e.g., using a Flush+Reload loop. These frequent accesses are detected by monitoring CPU performance counters [6, 15, 22, 25, 32, 50, 68].
- **Monitoring Memory Access Patterns.** Rowhammer causes unusual high-frequency memory access patterns to two or more addresses in one DRAM bank. Rowhammer can be stopped by detecting such access patterns [6, 16].
- **Preventing Exhaustion-based Page Placement.** Rowhammer requires target pages to be on vulnerable memory locations. All Rowhammer privilege escalation attacks so far required memory exhaustion. Thus, preventing abuse of memory exhaustion thwarts Rowhammer attacks [21, 61].
- **Preventing Physical Proximity to Kernel Pages.** As a more complete solution, user and kernel memory cells are physically isolated through the memory allocator, thwarting all practical Rowhammer privilege-escalation attacks [11].

Notice that defenses in each class share the same assumptions, properties, and introduce the same form of protection. Defenses from different classes complement each other. Thus, given the extensive amount of research on Rowhammer countermeasures, in this paper we ask the following question:

To what extent do the approaches above actually prevent Rowhammer attacks? In particular, is it possible to successfully mount Rowhammer privilege-escalation attacks in the presence of some (or even all) of the countermeasures above?

THE CLASSIFICATION OF TRANSCENDENTAL NUMBERS

K. MAHLER

1. All numbers ζ considered in this article are real or complex. For polynomials

$$f(x)=a_0+a_1x+\cdots+a_nx^n, \quad \text{where } a_n\neq 0,$$

the following notation will be used.

$$n(f)=n, \qquad H(f)=\max_{0\le\nu\le n}|a_\nu|, \quad \text{and} \quad L(f)=\sum_{\nu=0}^{n}|a_\nu|$$

denote the *exact degree*, the *height*, and the *length* of $f(x)$, respectively. We further put

$$A(f)=\prod_{f(\alpha)=0}|\alpha|^{\nu(\alpha)} \quad \text{and} \quad M(f)=\prod_{\alpha=0}^{n}(1+|\alpha_\nu|)$$

if f contains the set of all polynomials $f(x)\neq 0$ with rational integral coefficients and n is any positive integer, it is obvious that either of the inequalities $A(f)\le x$ or $M(f)\le x$ is satisfied by at most finitely many elements of F.

Consider now the set C of all real or complex numbers ζ. Our aim is to subdivide C into subsets or *classes* which are disjoint and have the following *invariance property*.

Any two numbers in distinct classes are algebraically independent over the rational number field Q.

1115 '970 *Subject classifications.* Primary 10F35. Secondary 02C10.

Printed in the United States of America

K-THEORY
[1989], 285–304

© Copyright by Birkhäuser, 1986

TWISTED COBOUNDARY OPERATOR ON A TREE AND THE SELBERG PRINCIPLE

PIERRE JULG and ALAIN VALETTE

0. INTRODUCTION

In this paper, we show that the methods of non commutative differential geometry [4] can provide a very simple proof of the Selberg Principle for supercuspidal representations of split-rank 1 simple algebraic groups over non-archimedian local fields. Namely, if G is such a group, e an idempotent of the convolution algebra $\mathscr{A} = C_c^\infty(G)$ of locally constant compactly supported functions on G (e.g. e coefficient of a supercuspidal representation), and if C is a hyperbolic conjugacy class in G, then

$$\int_C e(\dot{x})\,d\dot{x} = 0.$$

The main tool is the construction of 1-summable Fredholm modules (cf. [4]) associated to any simplicial action of a locally compact group G on a *tree*. In [10], [11] we introduced such a Fredholm module γ over $\mathscr{A} = C_c^\infty(G)$ by a construction involving elementary geometry of trees. As noted in [11], p. 214, the Chern character of γ is the trace on $\mathscr{A}$ given by the central function on G which is 0 on the hyperbolic elements (i.e. without fixed points on the tree) and 1 on the others. In order to reach the Selberg Principle, we clearly need more sophisticated Fredholm modules, whose characters will involve the hyperbolic conjugacy classes as well.

To do this, we construct in § 2 a one-parameter family $(\gamma_\rho)_{\rho \in \mathbb{R}_+^*}$ of 1-summable Fredholm modules over $\mathscr{A}$ by making use of a *discrete analogue of Witten's idea* in his proof of the Morse inequalities [18]. This idea is as follows. Let Δ^0 (resp. Δ^1) be the set of vertices (resp. edges) of the tree. The orientation allows one to define the simplicial co-boundary operator $d: \ell^2(\Delta^0) \to \ell^2(\Delta^1)$, which commutes with the natural representations of G on $\ell^2(\Delta^0)$ and $\ell^2(\Delta^1)$. If the tree is uniformly locally finite (we will assume that), d is a bounded operator, but it is not in general a Fredholm operator (as the example of the tree of $\mathbb{Z}$ already shows). However, it is possible as in [18], to conjugate d by $e^{t\rho}$, where ρ is a suitable function on Δ^0, and t is

INTRODUCTION TO THE PATH INTEGRAL

L. S. Schulman
Physics Departments
Clarkson University, Potsdam, NY 13676 USA and,
Technion, Haifa, Israel

The three parts of this article are three kinds of introduction to the path integral. They are

1. A derivation of the basic formula.
2. An overview of the major trends in the use of the path integral.
3. Some ways in which the method itself is being developed.

Lectures presented at the Adriatico Research Conference on Path Integration, Trieste, September 1987. They are published in *Path Summation: Achievements and Goals*, S. O. Lundqvist, A. Ranfagni, V. Sa-yakanit and L. S. Schulman, eds., World Scientific, Singapore, 1988.

https://ntrs.nasa.gov/search.jsp?R=19960026345 2017-10-22T18:01:20+00:00Z

A Survey of Parametrized Variational Principles and Applications to Computational Mechanics

Carlos A. Felippa

Department of Aerospace Engineering Sciences and
Center for Space Structures and Controls
University of Colorado
Boulder, Colorado 80309-0429, USA

September 1992
Revised May 1993

Report No. CU-CSSC-92-11

Written version of an Invited presentation to the First International Mechanics Seminar held at the Institute de Mécanique, Grenoble, France, May 1992.
Accepted for publication in *Computer Methods in Applied Mechanics and Engineering*

Research supported by NASA Langley Research Center
under Grant NAS1-736, monitored by Dr. J. Housner.

Complexity Theory and Numerical Analysis *

Steve Smale †

January 2, 2000

0 Preface

Section 5 is written in collaboration with Yu Yan Lu of the Department of Mathematics, City University of Hong Kong.

1 Introduction

Complexity theory of numerical analysis is the study of the number of arithmetic operations required to pass from the input to the output of a numerical problem.

To a large extent this requires the (global) analysis of the basic algorithms of numerical analysis. This analysis is complicated by the existence of ill-posed problems, conditioning and roundoff error.

A complementary aspect ("lower bounds") is the examination of efficiency for all algorithms solving a given problem. This study is difficult and needs a formal definition of algorithm.

Highly developed complexity theory of computer science provides some inspirations to the subject at hand. Yet the nature of theoretical computer science, with its foundations in discrete Turing machines, prevents a simple transfer to a subject where real number algorithms as Newton's method dominate.

One can indeed be skeptical about a formal development of complexity into the domain of numerical analysis, where problems are solved only to a certain precision and roundoff error is central.

Recall that according to computer science, an algorithm defined by a Turing machine is *polynomial time* if the computing time (measured by the number of Turing machine operations) $T(y)$ on input y satisfies:

$$T(y) \leq K(\text{size } y)^c \tag{1}$$

*Written for *Acta Numerica*

†Department of Mathematics, City University of Hong Kong

Proceedings, 5th Chaotic Modeling and Simulation International Conference, 12 – 15 June 2012, Athens Greece

Cryptography with Chaos

George Makris , Ioannis Antoniou

Mathematics Department, Aristotle University, 54124, Thessaloniki, Greece
E-mail: geormak@hotmail.com
Mathematics Department, Aristotle University, 54124, Thessaloniki, Greece
E-mail: iantonio@math.auth.gr

Abstract: We implement Cryptography with Chaos following and extending the original program of Shannon with 3 selected Torus Automorphisms, namely the Baker Map, the Horseshoe Map and the Cat Map. The corresponding algorithms and the software (chaos_cryptography) were developed and applied to the encryption of picture as well as text in real time. The maps and algorithms may be combined as desired, creating keys as complicated as desired. Decryption requires the reverse application of the algorithms.

Keywords: Cryptography, Chaos, image encryption, text encryption, Cryptography with Chaos.

1. Chaotic Maps in Cryptography

Chaotic maps are simple unstable dynamical systems with high sensitivity to initial conditions [Devaney 1992]. Small deviations in the initial conditions (due to approximations or numerical calculations) lead to large deviations of the corresponding orbits, rendering the long-term forecast for the chaotic systems intractable [Lighthill 1986]. This deterministic in principle, but not determinable in practice dynamical behavior is a local mechanism for entropy production. In fact Chaotic systems are distinguished as Entropy producing deterministic systems. In practice the required information for predictions after a (small) number of steps, called horizon of predictability, exceeds the available memory and the computation time grows superexponentially. [Prigogine 1980, Strogatz 1994, Katok, et 1995, Lasota, et 1994, Meyers 2009].

Shannon in his classic 1949 first mathematical paper on Cryptography proposed chaotic maps as models - mechanisms for symmetric key encryption, before the development of Chaos Theory. This remarkable intuition was based on the use of the Baker's map by Hopf in 1934 as a simple deterministic mixing model with statistical regularity. The Baker's Map is defined below and the mixing character is presented in figure 1:

$$B:[0,1)\times[0,1)\to[0,1)\times[0,1):\begin{pmatrix}x\\y\end{pmatrix}\to\begin{cases}\begin{pmatrix}2x\\ \frac{y}{2}\end{pmatrix} & x\in\left[0,\frac{1}{2}\right)\\ \begin{pmatrix}2x-1\\ \frac{y+1}{2}\end{pmatrix} & x\in\left[\frac{1}{2},1\right)\end{cases}$$

The reverse transformation:

Strong Predictor-Corrector Euler Methods for Stochastic Differential Equations

Eckhard Platen

School of Finance and Economics and School of Mathematical Sciences

University of Technology, Sydney

Lit: Kloeden, P.E. & Pl, E.: Numerical Solutions of Stochastic Differential Equations

Springer, Applications of Mathematics **23** (1992,1995,1999).

Bruti-Liberati, N. & Pl, E.: Strong Predictor-Corrector Euler Methods for Stochastic Differential Equations *Stochastics and Dynamics* **8**(3), 561-581 (2008).

All rights reserved under Pan American and International Copyright Conventions.

Bibliographical Note

This Dover edition, first published in 1964, is an unabridged reprint of the work originally published by the Belfer Graduate School of Science, Yeshiva University, New York in 1961.

Library of Congress Cataloging-in-Publication Data

Dirac, P. A. M. (Paul Adrien Maurice), 1902-
Lectures on quantum mechanics / by Paul A.M. Dirac.
p. cm.
Originally published: New York : Belfer Graduate School of Science, Yeshiva University, 1964.
ISBN 0-486-41713-1 (pbk.)
1. Quantum theory. I. Title.

QC174.125.D55 2001
530.12—dc21

2001019808

Manufactured in the United States of America
Dover Publications, Inc., 31 East 2nd Street, Mineola, N.Y. 11501

CONTENTS

Lecture No.		*Page*
1.	**The Hamilton Method**	1
2.	**The Problem of Quantization**	25
3	**Quantization on Curved Surfaces**	44
4	**Quantization on Flat Surfaces**	57

Resource Guide for Physics and Whitehead

This Process Studies Supplement provides a scholarly resource for studies in Whitehead and modern science and serves as a complement to our book *Physics and Whitehead: Process, Quantum and Experience* [Timothy E. Eastman and Hank Keeton, editors, Albany: State University of New York Press, 2003].

http://www.sun
http://www.ctr4process/publications/pss/

Outline

Introduction
- Why focus on Whitehead?
- Resource Guide Description

Mutual Impacts of Whitehead on Science
Internet Resources
Comprehensive Bibliography
Glossary
Information on our book *Physics and Whitehead* from SUNY Press, 2003.
- Order information, promo copy, and index
- Summary of key ideas and concepts
- Bibliographic sketches for major contributors

Physics and Whitehead Workshop, International Whitehead Conference, August, 1998.

Appendix A. Process Physics Developments.

Appendix B. Process Thought and Natural Science.
Reprint of Timothy E. Eastman, ed., "Process Thought and Natural Science," special focus sections of *Process Studies* 26/3-4 (Fall-Winter, 1997); 27/3-4 (Fall-Winter, 1998).

Appendix C. Whitehead and Natural Science .
Reprint of Dean R. Fowler, ed., "Whitehead and Natural Science," special issue of *Process Studies* 11/4 (Winter, 1981).

Appendix D. Philosophical Implications of Quantum Theory .
By Christoph Wassermann, "Philosophical Implications of Quantum Theory: Remarks on C. F. von Weizsacker's Abstract Reconstruction of Quantum Theory in the Light of A.N.Whitehead's Philosophy of Organicism" (first publication of previously unpublished manuscript, 1991); and "Note on the Physical Meaning of Impetus," C. Wassermann, Tübingen, January, 1986.

Appendix E. A Generalized Whitehead Theory of Gravity: the Kerr Solution.
By Robert J. Russell and Christoph Wassermann, including an appendix on the "Transcription of Whitehead's Tensor Notation to Standard Notation," from an unpublished manuscript, 1990.

Appendix F. "Electromagnetism, Time, and Immanence in Whitehead's Metaphysics."
By Lawrence W. Fagg, presented at the Workshop on Physics and Whitehead, International Whitehead Symposium, Claremont, California, 1998.

PRINCIPLES OF MIMETIC DISCRETIZATIONS OF DIFFERENTIAL OPERATORS

PAVEL B. BOCHEV* AND JAMES M. HYMAN†

Abstract. Compatible discretizations transform partial differential equations to discrete algebraic problems that mimic fundamental properties of the continuum equations. We provide a common framework for mimetic discretizations using algebraic topology to guide our analysis. The framework and all attendant discrete structures are put together by using two basic mappings between differential forms and cochains. The key concept of the framework is a natural inner product on cochains which induces a combinatorial Hodge theory on the cochain complex. The framework supports mutually consistent operations of differentiation and integration, has a combinatorial Stokes theorem, and preserves the invariants of the De Rham cohomology groups. This allows, among other things, for an elementary calculation of the kernel of the discrete Laplacian. Our framework provides an abstraction that includes examples of compatible finite element, finite volume, and finite difference methods. We describe how these methods result from a choice of the reconstruction operator and explain when they are equivalent. We demonstrate how to apply the framework for compatible discretization for two scalar versions of the Hodge Laplacian.

Key words. Mimetic discretizations, compatible spatial discretizations, finite element methods, support operator methods, algebraic topology, De Rham complex, Hodge operator, Stokes theorem.

AMS(MOS) subject classifications. 65N06, 65N12, 65N30.

1. Introduction.

Partial differential equations (PDEs) are ubiquitous in science and engineering. A key step in their numerical solution is the *discretization* that replaces the PDEs by a system of algebraic equations. Like any other model reduction, discretization is accompanied by losses of information about the original problem and its structure. One of the principal tasks in numerical analysis is to develop *compatible*, or *mimetic*, algebraic models that yield stable, accurate, and physically consistent approximate solutions. Historically, finite element (FE), finite volume (FV), and finite difference (FD) methods have achieved compatibility by following different paths that reflected their specific approaches to discretization.

Finite element methods begin by converting the PDEs into an equivalent variational equation and then restrict that equation to finite dimensional subspaces. Compatibility of the discrete problem is governed by variational inf-sup conditions, which imply existence of uniformly bounded discrete solution operators; see [6, 18, 46]. In finite volume methods the PDEs are first replaced by equivalent integral equations that express balance of global quantities valid on all subdomains of the problem domain.

*Computational Mathematics and Algorithms, Mail Stop 1110, Sandia National Laboratories, Albuquerque, NM 87185 (pbboche@sandia.gov).

†Mathematical Modeling and Analysis, T-7 Mail Stop B284, Los Alamos National Laboratory, Los Alamos, NM 87545 (hyman@lanl.gov).

BOOLEAN VALUED ANALYSIS: ORIGINS, MACHINERY, RESULTS

A. G. Kusraev

(Russia, Vladikavkaz; Southern Mathematical Institute
of the Russian Academy of Sciences)

1. *Boolean valued analysis* is a branch of functional analysis which uses a special model-theoretic technique. This technique consists generally in studying the properties of an arbitrary mathematical object by means of comparison between its representations in two different set-theoretic models whose construction utilizes principally distinct Boolean algebras. We usually take as these models the classical Cantorian paradise in the shape of the *von Neumann universe* and a specially-trimmed *Boolean valued universe* in which the conventional set-theoretic concepts and propositions acquire bizarre interpretations. Usage of two models for studying a single object is a family feature of the so-called *nonstandard methods of analysis*. For this reason, Boolean valued analysis can be considered as an instance of nonstandard analysis in common parlance.

2. Proliferation of Boolean valued models is due to P. J. Cohen's final breakthrough in Hilbert's Problem Number One. In 1963 Cohen discovered his *method of 'forcing'* and proved the consistency of the negation of Continuum Hypothesis (CH, in short) with axioms of Zermelo–Frenkel set theory (ZFC) [1]. Together with the earlier result by K. Gödel (1939) on the consistency of CH with ZFC this result means that CH is independence from ZFC. The method of forcing was rather intricate and the inevitable attempts at simplification gave rise to the *Boolean valued models* by D. Scott and R. Solovay and independently by P. Vopěnka, [2, 3].

3. The *Continuum Hypothesis* formulated by Cantor in 1878 can be read as follows: *any subset of the set of real numbers is either finite, or countable, or continual*. The Continuum hypothesis was presented by David Hilbert as the first of his twenty-three open problems in his famous address at the 1900 International Congress of Mathematicians in Paris (ICM-II). Remaining opened till 1961, it gave an impetus to in-depth studies in the foundation of mathematics.

4. Cantor's first ten papers were on number theory. In 1867, Cantor completed his dissertation, on number theory, at the University of Berlin and then took up a position at the University of Halle. At the suggestion of Eduard Heine, the Professor at Halle, Cantor turned to analysis. Heine proposed that Cantor solve an open problem of the uniqueness of the representation of a function by trigonometric series: *if a trigonometric series converges to zero, is then it identically zero, i.e., are all coefficients of the series equal to zero?* Cantor solved this problem in 1869.

5. Cantor next extended his uniqueness theorem in 1871 by allowing divergence at a finite collection of exceptional points called a *set of uniqueness*. How many elements a set of uniqueness may have? The origins of set theory are closely connected with this subject, since it was Cantor's research into the nature of sets of uniqueness undertaken in [4] that led him afterward to discovery of *ordinal numbers* and the method of *transfinite induction* and the creation of *set theory*. After 1872 he never returned to the uniqueness problem. The cycle of his set-theoretic works begins with [5]. The continuum hypothesis was stated in [6].

Home Office

PROSCRIBED TERRORIST ORGANISATIONS

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, D.C. 20510-6275

June 7, 2017

VIA ELECTRONIC TRANSMISSION

Mr. Glenn R. Simpson
Fusion GPS
Washington, D.C. 20535

Dear Mr. Simpson:

The Committee's March 24, 2017, letter to you requested information about Fusion GPS' activities related to the dossier compiled by Mr. Christopher Steele.[1] It requested information about the clients who hired and paid Fusion and the factual details of those arrangements. It also requested factual information about Fusion's arrangement with Mr. Steele and his company Orbis Business Intelligence, and about Fusion's communications with the media and government entities regarding the dossier.

You refused to provide any information whatsoever, claiming that the Committee's request "calls for information and documents protected by the First Amendment right, attorney-client privilege, attorney work product, and contractual rights (*e.g.*, confidentiality agreements) of Fusion and/or its clients."[2] However, in both your response letter and on a subsequent phone call with Committee staff, your attorney refused to provide a clear explanation of the basis for the claimed privileges and rights, and has failed to provide any privilege log describing the withheld documents.[3]

Based on the minimal and vague explanations your attorney has provided, the Committee cannot adequately assess your claims. Thus, we must presume that they are unfounded. Moreover, even if any of these claims were once valid, it appears they may have been waived when Fusion shared various versions of the dossier with journalists, members of Congress, and the FBI.[4]

Your attorney has refused to engage in a meaningful dialogue about your various claims or acknowledge that it is for the Committee to rule on whether it will recognize those claims or

---

[1] Letter from Hon. Charles E. Grassley, Chairman, Senate Judiciary Committee, to Glenn R. Simpson, Fusion GPS (Mar. 24, 2017).
[2] Letter from Joshua A. Levy & Robert F. Muse, Cunningham Levy Muse LLP, to Hon. Charles E. Grassley, Chairman, Senate Judiciary Committee (Apr. 7, 2017) [hereinafter Letter from Fusion GPS (Apr. 7, 2017)].
[3] *See id.*
[4] *E.g.*, Scott Shane, *What We Know and Don't Know About the Trump-Russia Dossier*, N.Y. TIMES (Jan. 11, 2017).

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

July 20, 2017

VIA ELECTRONIC TRANSMISSION

The Honorable Rod J. Rosenstein
Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

Dear Mr. Rosenstein,

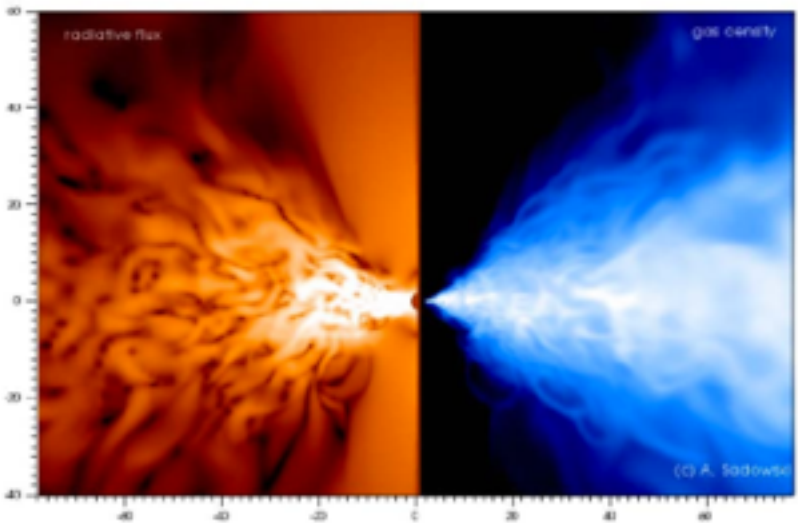
According to news reports, during the 2016 presidential election, "Ukrainian government officials tried to help Hillary Clinton and undermine Trump" and did so by "disseminat[ing] documents implicating a top Trump aide in corruption and suggested they were investigating the matter…"[1] Ukrainian officials also reportedly "helped Clinton's allies research damaging information on Trump and his advisers."[2] At the center of this plan was Alexandra Chalupa, described by reports as a Ukrainian-American operative "who was consulting for the Democratic National Committee" and reportedly met with Ukrainian officials during the presidential election for the express purpose of exposing alleged ties between then-candidate Donald Trump, Paul Manafort, and Russia.[3] *Politico* also reported on a Financial Times story that quoted a Ukrainian legislator, Serhiy Leschenko, saying that Trump's candidacy caused "Kiev's wider political leadership to do something they would never have attempted before: intervene, however indirectly, in a U.S. election."[4]

Reporting indicates that the Democratic National Committee encouraged Chalupa to interface with Ukrainian embassy staff to "arrange an interview in which Poroshenko [the president of Ukraine] might discuss Manafort's ties to Yanukovych."[5] Chalupa also met with Valeriy Chaly, Ukraine's ambassador to the U.S., and Oksana Shulyar, a top aid to the Ukrainian ambassador in March 2016 and shared her alleged concerns about Manafort. Reports state that the purpose of their initial meeting was to "organize a June reception at the embassy to promote Ukraine." However, another Ukrainian embassy official, Andrii Telizhenko, told *Politico* that Shulyar instructed him to assist Chalupa with research to connect Trump, Manafort, and the

[1] Kenneth P. Vogel & David Stern, *Ukrainian efforts to sabotage Trump backfire*, POLITICO (Jan. 11, 2017).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

The Inaugural Black Hole Initiative Annual Conference

Scientific Program



First Annual BHI Conference on Black Holes

Monday, May 8 and Tuesday, May 9, 2017

Sheraton Commander Hotel, 16 Garden Street, Cambridge, MA

Hosted by the Black Hole Initiative, Harvard University
http://bhi.fas.harvard.edu/

All talks are 20 minutes (15+5)
Sessions held in the George Washington Ballroom
Coffee Breaks held in the adjacent Terrace Room

This conference was made possible by a generous grant from the John Templeton Foundation

WHO Model List of Essential Medicines

20th List

(March 2017)

(Amended August 2017)

Status of this document

This is a reprint of the text on the WHO Medicines website

http://www.who.int/medicines/publications/essentialmedicines/en/

LEGACY TRAIN CONTROL SYSTEM STABILISATION

Dr. Reinhard Galler, Director, EQUIcon Software GmbH
Karl Strangaric, Senior Signal Systems Officer, Metro Trains Melbourne

SUMMARY

In 2003 the previous consortium franchisee Connex Melbourne in conjunction with the Department of Infrastructure embarked on a stabilisation program for the principal train control facility in Melbourne. The facility is commonly known as METROL. The Train Control System located at METROL provides a remote control facility for some signalling infrastructure which is the principal means of operation in the Melbourne inner metropolitan area, currently under the Metro Trains Melbourne franchise (MTM).

The need for the project came about due to a number of factors, some of these were:

1. *The need to accommodate extra operational load until a replacement train control system is rolled out.*
2. *Consequent pressure on the life expired existing system to accommodate network expansion.*
3. *Danger of compromising the integrity of the application Software, due to the utilisation of life expired media.*

The task of stabilisation required that we select an appropriate partner who had the specialist technical knowledge with proven performance in adaptation and integration in the Dec PDP-11 to PC environment. The partner we chose was a German company called EQUIcon Software. The success of the project has qualified their expertise in this field and proven them to be the correct partner of choice.

Basically we took a legacy system running on PDP-11 mini computers and ported it to a PC based platform utilizing a proprietary co-processor card (Osprey Co-processor) to run the application code (an Ericsson JZA 715 product). This runs inside the Co-processor completely, emulated cycle by cycle, and the PC host platform acts as the interface between the outside world and the application. The systems have performed exceptionally well for the last 6 years.

1 INTRODUCTION

The concept of retaining original software and also extending its life by adapting the hardware platform that it runs on had become a viable option as technological advances opened up new frontiers suitable for adaptation. In this particular train control application it has enabled the life extension of mature train control software, originally designed to run on a now life expired DEC PDP-11 platform to be migrated to a PC based platform. The original application software core is maintained 100% and remains unaltered running inside the new platform. This approach has allowed the re-use of the fully de-bugged Train Control application software as the core of the system. Consequently, the major part of the project was the 'hardware adaptation' that was required to integrate the new system into the existing fabric.

This approach allows 'old' software to be 're-cycled' in a very cost effective way. Additionally, systems can be potentially given new life, long term or even extended indefinitely.

2 THE MELBOURNE RAIL NETWORK

The Melbourne Metropolitan Rail Network covers the greater suburban area comprising of 16 electrified rail lines all converging on the Central Business District (CBD). The CBD is also serviced by underground rail tunnels that are looped around this central area. The network is primarily comprised of a range of single, double, triple and quadruple lines on which all services are delivered. The area under direct Train Describer Control is coloured black. See Fig 1.

Exploring Miner Evolution in Bitcoin Network

Luqin Wang[1] and Yong Liu[2]

[1] Department of Computer Science and Engineering
[2] Department of Electrical and Computer Engineering
NYU Polytechnic School of Engineering

Abstract. In recent years, Bitcoin, a peer-to-peer network based crypto digital currency, has attracted a lot of attentions from the media, the academia, and the general public. A user in Bitcoin network can create Bitcoins by packing and verifying new transactions in the network using their computation power. Driven by the price surge of Bitcoin, users are increasingly investing on expensive specialized hardware for Bitcoin mining. To obtain steady payouts, users also pool their computation resources to conduct pool mining. In this paper, we study the evolution of Bitcoin miners by analyzing the complete transaction blockchain. We characterize how the productivity, computation power and transaction activity of miners evolve over time. We also conduct an in-depth study on the largest mining pool F2Pool. We show how it grows over time and how computation power is distributed among its miners. Finally, we build a simple economic model to explain the evolution of Bitcoin miners.

Keywords: Bitcoin, Measurement, Network Analysis

1 Introduction

Bitcoin [1] is known as *the first decentralized digital currency in the world* [2]. Unlike any traditional currency issued and regulated by a sovereign bank, Bitcoin is not controlled by any institution or country. It circulates globally without boundary and is free from financial regulation systems due to its decentralized P2P accounting and transaction design. Debuted in 2009 and after five years' development, Bitcoin exchange price has risen from nothing to over $100 per coin through mid 2013, surged to its peak at $1,242 on Nov. 29, and is wobbling between $350 and $600 in today's market. Till September 2014, the market capitalization of Bitcoin has increased to around 6 billion US dollars; and the Bitcoin network runs over 60,000 transactions daily. Along with Bitcoin network's capitalization and volume, a variety number of derivative services have been developed and legalized. Exchange markets, i.e., Coinbase [3] and Bitstamp [4], allow users to buy and sell Bitcoins using regular currencies globally. Online merchants, e.g., Dell and Overstock, are now accepting Bitcoin as a payment method. Governments of several countries, such as Canada and Thailand, have approved fully-legal Bitcoin exchange and issued tax guidance on Bitcoin transactions. Different from a regular currency, there is no central bank or authority who decides how many Bitcoins to be issued and distributed. According to the

Submitted to: EPAC '02, Paris, France, 6/3-7/02 BNL-68945

LONGITUDINAL PHASE-SPACE TOMOGRAPHY IN RHIC*

C. Montag, N. D'Imperio, R. Lee, J. Kewisch, and T. Satogata, BNL, Upton, NY 11973, USA

Abstract

In recent years, longitudinal phase-space tomography has become a useful diagnostic tool in the domain of particle accelerators. A computer code has been developed to visualize and quantify dynamic effects in longitudinal phase space, like transition crossing and adiabatic. This code is capable of reconstructing the longitudinal phase space distribution during turn-by-turn parameter changes such as RF phase and voltage jumps. This paper describes the reconstruction code as well as recent applications at the Relativistic Heavy Ion Collider (RHIC).

1 INTRODUCTION

To reconstruct the full n-dimensional picture of an object, tomography uses a set of (n-1)-dimensional projections of this object, taken from different angles spanning at least 180 degrees. In the case of a particle bunch in an accelerator, this rotation is naturally provided by the phase-space dynamics. However, particularly in the longitudinal plane even the dynamics is intrinsically nonlinear with the rotation frequency (synchrotron frequency) being a function of the phase space amplitude; it therefore does not simply resemble a rigid, rotating object. To overcome this difficulty, the equations of motion have to be taken into account [1]; this is realized by tracking test particles that are equally distributed in phase-space. These test particles are sorted into the N_{bins} bins that correspond to the binning of the measured profiles each time a profile is next obtained by the wall current monitor. Each particle k is therefore assigned a bin number $N_k^{bin}(t)$. The number of test particles in the jth bin at the time the ith profile was taken, $N_{i,j}^{computation}$, is determined. Since simulations such as transition crossing or debunching involve turn-by-turn RF parameter changes, parameter changes have also been implemented in the tomography code.

During the tomographic reconstruction process following the tracking, an "intensity" I is assigned to each test particle according to the measured longitudinal bunch profiles, using an iterative back-projection algorithm [2]. This is done such that the "intensity" of all test particles that could potentially have contributed to a certain profile bin j at a specific time when the ith profile was taken is increased by the same amount. This increment $\Delta I_{i,j}$ is determined as

$$\Delta I_{i,j} = \frac{h_{i,j}^{measured}}{N^{profiles} N_{i,j}^{computation}}, \qquad (1)$$

where $h_{i,j}^{measured}$ is the measured profile height of the jth bin in the ith profile, and $N^{profiles}$ is the total number of profiles used for the reconstruction.

After this has been done for all profiles, projections of the resulting distribution are calculated that correspond to the profiles measured by the wall current monitor. The difference of measured and reconstructed profiles is then iteratively back-projected.

The evolution of this discrepancy between measured and reconstructed profiles during the iterative process may then be used as a quantitative measure of the quality of the reconstruction, thus allowing for parameter fitting [1].

2 TRANSITION CROSSING

During acceleration of gold beams from injection ($\gamma = 10.5$) to store-top ($\gamma = 107$), the transition energy of $\gamma_t = 23$ has to be crossed. This is done by flipping the sign of a set of specially designed quadrupoles, resulting in a γ_t jump of $\Delta\gamma_t \approx 0.6$ within 3% more [3]. During the RHIC 2001 run, these quadrupoles were kept at a constant field around transition energy, which resulted in some cases changes in the beam energy increased, making tomographic reconstruction more difficult. The RF phase was shifted by 180 degrees at the same time as the quadrupoles changed sign.

During this process, a slight RF bucket mismatch occurs, resulting in a longitudinal quadrupole oscillation after transition crossing, as shown in Figure 1. About 0.45 sec after transition, a fine instability leads to partial beam loss if the bunch intensity exceeds a certain limit. Later in the RHIC 2001 run, this instability was successfully cured by increased Landau damping using octupoles [4].

While these effects are already easily visible in the contour map plots of subsequent longitudinal bunch profiles, as shown in Figure 2, they are best theoretical using corresponding phase-space reconstruction, as depicted in Figure 3. 0.2 sec before transition the beam appears well matched, while the longitudinal mismatch is clearly visible 0.3 sec after γ_t. After the fine instability has occurred, the core of the bunch is destroyed, leading to a double peak structure. Though the double peak appears clearly in the corresponding contour map plot, Figure 2, the depth of the "hole" in the center can only be detected by tomographic phase-space reconstruction.

Since the detailed dynamics of the instability is still unknown, the phase-space plots presented in Figure 3 are reconstructed from a small number of profiles each, spanning some 270 degrees of phase-space rotation for each plot rather than using the full turn-by-turn parameter change capability of the code. The limit is foreseen for the upcoming

* Work performed under the auspices of the U.S. Department of Energy

The Fiat–Shamir Transformation in a Quantum World

Özgür Dagdelen Marc Fischlin Tommaso Gagliardoni

Technische Universität Darmstadt, Germany
www.cryptoplexity.de
oezguer.dagdelen@cased.de marc.fischlin@gmail.com tommaso@gagliardoni.net

Abstract. The Fiat-Shamir transformation is a famous technique to turn identification schemes into signature schemes. The derived scheme is provably secure in the random-oracle model against classical adversaries. Still, the technique has also been suggested to be used in connection with quantum-immune identification schemes, in order to get quantum-immune signature schemes. However, a recent paper by Boneh et al. (Asiacrypt 2011) has raised the issue that results in the random-oracle model may not be immediately applicable to quantum adversaries, because such adversaries should be allowed to query the random oracle in superposition. It has been unclear if the Fiat-Shamir technique is still secure in this quantum oracle model (QROM).

Here, we discuss that giving proofs for the Fiat-Shamir transformation in the QROM is presumably hard. We show that there cannot be black-box extractors, as long as the underlying quantum-immune identification scheme is secure against active adversaries and the first message of the prover is independent of its witness. Most schemes are of this type. We then discuss that for some schemes one may be able to resurrect the Fiat-Shamir result in the QROM by modifying the underlying protocol first. We discuss in particular a version of the Lyubashevsky scheme which is provably secure in the QROM.

1 Introduction

The Fiat-Shamir transformation [FS87] is a well-known method to remove interaction in three-move identification schemes between a prover and verifier, by letting the verifier's challenge ch be determined via a hash function H applied to the prover's first message com. Currently, the only generic, provably secure instantiation is by modeling the hash function H as a random oracle [BR93, PS00]. In general, finding secure instantiations based on *standard* hash functions is hard for some schemes, as shown in [GK03, BDSG+13]. However, these negative results usually rely on peculiar identification schemes, such that for specific schemes, especially more practical ones, such instantiations may still be possible.

The Quantum Random-Oracle model Recently, the Fiat-Shamir transformation has also been applied to schemes which are advertised as being based on quantum-immune primitives, e.g., [Lyu09, BM10, GKV10, CLRS10, CVA10, SSH11, MGS11, Sak12, GLP12, AFLT12, CNR12, AJLA+12]. Interestingly, the proofs for such schemes still investigate classical adversaries only. It seems unclear if (and how) one can transfer the proofs to the quantum case. Besides the problem that the classical Fiat-Shamir proof [PS00] relies on rewinding the adversary, which is often

The Simplest Protocol for Oblivious Transfer

Tung Chou[1] and Claudio Orlandi[2]

[1] Technische Universiteit Eindhoven
[2] Aarhus University

Abstract Oblivious Transfer (OT) is the fundamental building block of cryptographic protocols. In this paper we describe the simplest and most efficient protocol for 1-out-of-n OT to date, which is obtained by tweaking the Diffie-Hellman key-exchange protocol. The protocol achieves UC-security against active and adaptive corruptions in the random oracle model. Due to its simplicity, the protocol is extremely efficient and it allows to perform m 1-out-of-n OTs using only:

- **Computation:** $(n+1)m+2$ exponentiations (nm for the receiver, $m+2$ for the sender) and
- **Communication:** $32(m+1)$ bytes (for the group elements), and $2nm$ ciphertexts.

We also report on an implementation of the protocol using elliptic curves, and on a number of mechanisms we employ to ensure that our software is secure against active attacks too. Experimental results show that our protocol (thanks to both algorithmic and implementation optimizations) is at least one order of magnitude faster than previous work.

1 Introduction

Oblivious Transfer (OT) is a cryptographic primitive defined as follows: in its simplest flavour, 1-out-of-2 OT, a sender has two input messages M_0 and M_1 and a receiver has a choice bit c. At the end of the protocol the receiver is supposed to learn the message M_c and nothing else, while the sender is supposed to learn nothing. Perhaps surprisingly, this extremely simple primitive is sufficient to implement any cryptographic task [Kil88]. OT can also be used to implement most advanced cryptographic tasks, such as secure two- and multi-party computation (e.g., the millionaire's problem) in an efficient way [NNOB12, BLN+15].

Given the importance of OT, and the fact that most OT applications require a very large number of OTs, it is crucial to construct OT protocols which are at the same time efficient and secure against realistic adversaries.

A Novel OT Protocol. In this paper we present a novel and extremely *simple*, *efficient* and *secure* OT protocol. The protocol is a simple tweak of the celebrated Diffie-Hellman (DH) key exchange protocol. Given a group $\mathbb{G}$ and a generator g, the DH protocol allows two players Alice and Bob to agree on a key as follows: Alice samples a random a, computes $A = g^a$ and sends A to Bob. Symmetrically Bob samples a random b, computes $B = g^b$ and sends B to Alice. Now both parties can compute $g^{ab} = A^b = B^a$ from which they can derive a key k. The key observation is now that Alice can also derive a different key from the value $(B/A)^a = g^{ab-a^2}$, and that Bob cannot compute this group element (assuming that the computational DH problem is hard).

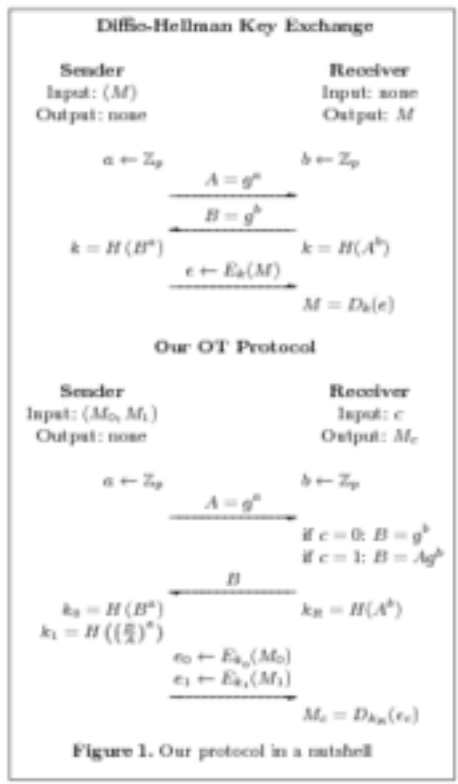


Figure 1. Our protocol in a nutshell

TRAFFICKING IN PERSONS REPORT

JUNE 2017

DEPARTMENT OF STATE • UNITED STATES OF AMERICA

Reverse-engineering of the cryptanalytic attack used in the Flame super-malware *

Max Fillinger and Marc Stevens

CWI, Amsterdam, The Netherlands
max.fillinger@cwi.nl
marc@marc-stevens.nl

Abstract. In May 2012, a highly advanced malware for espionage dubbed Flame was found targeting the Middle-East. As it turned out, it used a forged signature to infect Windows machines by MITM-ing Windows Update. Using counter-cryptanalysis, Stevens found that the forged signature was made possible by a chosen-prefix attack on MD5 [Ste13]. He uncovered some details that prove that this attack differs from collision attacks in the public literature, yet many questions about techniques and complexity remained unanswered.
In this paper, we demonstrate that significantly more information can be deduced from the example collision. Namely, that these details are actually sufficient to reconstruct the collision attack to a great extent using some weak logical assumptions. In particular, we contribute an analysis of the differential path family for each of the four near-collision blocks, the chaining value differences elimination procedure and a complexity analysis of the near-collision block attacks and the associated birthday search for various parameter choices. Furthermore, we were able to prove a lower-bound for the attack's complexity.
This reverse-engineering of a non-academic cryptanalytic attack exploited in the real world seems to be without precedent. As it allegedly was developed by some nation-state(s) [WP12, Kas12, Cry12], we discuss potential insights to their cryptanalytic knowledge and capabilities.

Keywords: MD5, hash function, cryptanalysis, reverse engineering, signature forgery

1 Introduction

1.1 End-of-life of a cryptographic primitive

The end-of-life of a widely-used cryptographic primitive is an uncommon event, preferably orchestrated in an organized fashion by replacing it with a next generation primitive as a precaution as soon as any kind of weakness has been exposed. Occasionally such idealistic precautions are thrown to the wind for various

* ©IACR 2015. This article is the final version submitted by the author(s) to the IACR and to Springer-Verlag on 2015-09-07. The version published by Springer-Verlag is available at 10.1007/978-3-662-48800-3.

Theory and Applications of Categories, Vol. 30, No. 24, 2015, pp. 836–881.

CATEGORIES IN CONTROL

JOHN C. BAEZ AND JASON ERBELE

Abstract. Control theory uses 'signal-flow diagrams' to describe processes where real-valued functions of time are added, multiplied by scalars, differentiated and integrated, duplicated and deleted. These diagrams can be seen as string diagrams for the symmetric monoidal category $\mathrm{FinVect}_k$ of finite-dimensional vector spaces over the field $k = \mathbb{R}(s)$ of rational functions, where the variable s acts as differentiation and the monoidal structure is direct sum rather than the usual tensor product of vector spaces. For any field k we give a presentation of $\mathrm{FinVect}_k$ in terms of the generators used in signal-flow diagrams. A broader class of signal-flow diagrams also includes 'cups' and 'caps' to model feedback. We show these diagrams can be seen as string diagrams for the symmetric monoidal category FinRel_k, where objects are still finite-dimensional vector spaces but the morphisms are linear relations. We also give a presentation for FinRel_k. The relations say, among other things, that the 1-dimensional vector space k has two special commutative †-Frobenius structures, such that the multiplication and unit of either one and the comultiplication and counit of the other fit together to form a bimonoid. This sort of structure, but with tensor product replacing direct sum, is familiar from the 'ZX-calculus' obeyed by a finite-dimensional Hilbert space with two mutually unbiased bases.

1. Introduction

Control theory is the branch of engineering that focuses on manipulating 'open systems'—systems with inputs and outputs—to achieve desired goals. In control theory, 'signal-flow diagrams' are used to describe linear ways of manipulating signals, which we will take here to be smooth real-valued functions of time [10]. For a category theorist, at least, it is natural to treat signal-flow diagrams as string diagrams in a symmetric monoidal category [11, 12]. This forces some small changes of perspective, which we discuss below, but more important is the question: *which symmetric monoidal category?*

We shall argue that the answer is: the category FinRel_k of finite-dimensional vector spaces over a certain field k, but with *linear relations* rather than linear maps as morphisms, and *direct sum* rather than tensor product providing the symmetric monoidal structure. We use the field $k = \mathbb{R}(s)$ consisting of rational functions in one real variable s. This variable has the meaning of differentiation. A linear relation from k^m to k^n is thus a system of linear constant-coefficient ordinary differential equations relating m 'input' signals and n 'output' signals.

Received by the editors 2014-12-17 and, in revised form, 2015-06-21.
Transmitted by Tom Leinster. Published on 2015-06-26.
2010 Mathematics Subject Classification: 18D10, 16T10.
Key words and phrases: control theory, graphical calculus, Frobenius algebra, bialgebra, dagger-compact category, signal-flow diagram.
© John C. Baez and Jason Erbele, 2015. Permission to copy for private use granted.

PUBLISHED BY

INTECH

open science | open minds

World's largest Science,
Technology & Medicine
Open Access book publisher

3,150+
OPEN ACCESS BOOKS

104,000+
INTERNATIONAL
AUTHORS AND EDITORS

109+ MILLION
DOWNLOADS

BOOKS
DELIVERED TO
151 COUNTRIES

AUTHORS AMONG
TOP 1%
MOST CITED SCIENTISTS

12.2%
AUTHORS AND EDITORS
FROM TOP 500 UNIVERSITIES

Selection of our books indexed in the
Book Citation Index in Web of Science™
Core Collection (BKCI)

WEB OF SCIENCE™

Chapter from the book *Fuzzy Logic - Algorithms, Techniques and Implementations*
Downloaded from: http://www.intechopen.com/books/fuzzy-logic-algorithms-techniques-and-implementations

Interested in publishing with InTechOpen?
Contact us at book.department@intechopen.com

Implementing Cryptographic Pairings over Barreto-Naehrig Curves

Augusto Jun Devegili[1]*, Michael Scott[2], and Ricardo Dahab[1]

[1] Instituto de Computação, Universidade Estadual de Campinas
Caixa Postal 6176, CEP 13084-971 Campinas, SP, Brazil
augusto@devegili.org, rdahab@ic.unicamp.br
[2] School of Computing, Dublin City University
Dublin 9, Ireland
mscott@computing.dcu.ie

Abstract. In this paper we describe an efficient implementation of the Tate and Ate pairings using Barreto-Naehrig pairing-friendly curves, on both a standard 32-bit PC and on a 32-bit smartcard. First we introduce a sub-family of such curves with a particularly simple representation. Next we consider the issues that arise in the efficient implementation of field arithmetic in $F_{p^{12}}$, which is crucial to good performance. Various optimisations are suggested, including a novel approach to the 'final exponentiation', which is faster and requires less memory than the methods previously recommended.

1 Introduction

Pairing-based cryptography requires pairing-friendly curves. These are parameterised by their embedding degree k. The embedding degree dictates to an extent the security level efficiently achievable on the curve.

While it is well known that super-singular curves are viable and useful candidates, they are limited in terms of the possible values of the embedding degree. Furthermore the highest embedding degree possible for super-singular elliptic curves ($k = 6$) requires us to use curves of characteristic 3, which is rather awkward from an implementation point of view (we refer the reader to a recent paper on arithmetic in GF(3^m) by Ahmadi, Hankerson and Menezes [1]). Attention has therefore switched to consideration of non-supersingular curves of prime characteristic, for which there is no such limitation. Nonetheless finding suitable curves, or ideally whole families of suitable curves, has proven to be non-trivial [2].

In this context the security of pairing-based cryptography depends on finding curves whose order n is divisible by a large prime r such that generic attacks on small group orders (Pohlig-Hellman attacks) can be resisted. It is also important that $k \lg(p)$, where p is the modulus, is large enough to resist index-calculus attacks.

* Funded by the Brazilian Government/Coordination for the Improvement of Higher Education Personnel (CAPES)

A Review of the Ultron-Logotron Theory: Consciousness and Quantum Physics

Sung Jang Chung
Morristown-Hamblen Healthcare System
Morristown, TN, USA.

Abstract

A scientific relationship between mind and matter or self's consciousness and quantum physics is still not clearly known in science because of lack of concrete human data that would enable us to objectively explain them. Consequently, physicists, neuroscientists, philosophers, psychologists, psychiatrists and medical scientists have been investigating to find experimental and/or objective proofs for the relationships between mind and matter, consciousness and quantum physics in the mind-brain system. This paper reviewed the hypothesis of the ultron-logotron theory related to relationships between mind and matter or self and consciousness that proposed the primary dynamics in the mind-brain interaction and attempted physical quantitative estimation of mental force and suggested that the range of the reduced Planck constant energy may be a minimum unit of mental force-energy on the basis of the spin-mediated consciousness theory of Hu and Wu, and the Orch-OR theory of Penrose and Hameroff. In addition, relationships among self, mind and body, and those among self, society and nation in the human evolution are presented. In this review paper, the author summarized major studies of the ultron-logotron theory that is essentially based on Confucian philosophy and quantum physics.

Keywords: Consciousness; Quantum Physics; Confucianism; I Ching; Jeong Yeok; Ultron-Logotron Theory; Spin-Mediated Consciousness Theory; Orch-OR Theory; Theory of Everything; Human Evolution; Precognitive Dreams; Probacent model.

1. Introduction

A scientific relationship between mind and matter or self's consciousness and quantum physics is still not clearly known in science because of lack of concrete human data that would enable us to objectively explain them (Penrose, 2007; Penrose, Hameroff & Kak, 2011; Hawking, 2001; Bohm, 2006; Laszlo, 2008; Gusnard, 2007; Hands, 2015). Consequently, experimental and theoretical physicists, neuroscientists, philosophers, psychologists, psychiatrists and medical scientists have been investigating to find experimental and/or objective proofs for the relationship between mind and matter, consciousness and quantum physics in the mind-brain system. The self is the agent being the source of consciousness, and responsible for the thoughts of mind and actions of an individual, enduring through time.

2. The Science of Self, Mind and Body

The author had unusual personal experiences that difficult mathematical problems were not solved in his manifest consciousness but could be unexpectedly clearly solved in his subconscious mind (Chung 2009). The author published the solution of the math problem in the International Journal of Biomedical Computing (Chung 1995). The math problem was regarding a general mathematical model of "probacent"-probability equation that expresses a relationship among intensity of stimulus, duration of exposure and occurrence of response in biological phenomena (Chung 1960; 2007, 2013b). The mathematical model might possibly calculate the probability of safe survival in humans and other living organisms exposed to any harmful or adverse circumstances or conditions, overcoming the risk. The author proposed a theory that there are in human individuals two selves, one, the inner self (the true self, spirit) and one, the physical self (the false self) that coexist in one individual person (Chung 2009; 2012). Kelly McGonigal (2012) describes that one individual has two minds or two selves, naming "I WILL" and "I WANT" selves.

HILA5: On Reliability, Reconciliation, and Error Correction for Ring-LWE Encryption

Markku-Juhani O. Saarinen*

Helsinki, Finland
mjos@iki.fi

Abstract. We describe a new reconciliation method for Ring-LWE that has a significantly smaller failure rate than previous proposals while reducing ciphertext size and the amount of randomness required. It is based on a simple, deterministic variant of Peikert's reconciliation that works with our new "safe bits" selection and constant-time error correction techniques. The new method does not need randomized smoothing to achieve non-biased secrets. When used with the very efficient "New Hope" Ring-LWE parametrization we achieve a decryption failure rate well below 2^{-128} (compared to 2^{-60} of the original), making the scheme suitable for public key encryption in addition to key exchange protocols; the reconciliation approach saves about 40% in ciphertext size when compared to the common LP11 Ring-LWE encryption scheme. We perform a combinatorial failure analysis using full probability convolutions, leading to a precise understanding of decryption failure conditions on bit level. Even with additional implementation security and safety measures the new scheme is still essentially as fast as the New Hope but has slightly shorter messages. The new techniques have been instantiated and implemented as a Key Encapsulation Mechanism (KEM) and public key encryption scheme designed to meet the requirements of NIST's Post-Quantum Cryptography effort at very high security level.

Keywords: Ring-LWE, Reconciliation, Post-Quantum Encryption, New Hope.

1 Introduction

Some classes of encrypted data must remain confidential for a long period of time – often at least few decades in national security applications. Therefore high-security cryptography should be resistant to attacks even with projected future technologies. As there are no physical or theoretical barriers preventing progressive development of quantum computing technologies capable of breaking current RSA- and Elliptic Curve based cryptographic standards (using polynomial-time quantum algorithms already known [38,44]), a need for such quantum-resistant algorithms in national security applications has been identified [34].

In December 2016 NIST issued a standardization call for quantum-resistant public key algorithms, together with requirements and evaluation criteria [33].

* Most of this work was performed while the author was with DARKMATTER, UAE.

1

Newton-Krylov-Schwarz: An Implicit Solver for CFD

XIAO-CHUAN CAI[1], DAVID E. KEYES[2], and V. VENKATAKRISHNAN[3]

1.1 ABSTRACT

Newton-Krylov methods and Krylov-Schwarz (domain decomposition) methods have begun to become established in computational fluid dynamics (CFD) over the past decade. The former employ a Krylov method inside of Newton's method in a Jacobian-free manner through directional differencing. The latter employ an overlapping Schwarz domain decomposition to derive a preconditioner for the Krylov accelerator that relies primarily on local information for data-parallel concurrency. They may be composed as Newton-Krylov-Schwarz (NKS) methods, which seem particularly well suited for solving nonlinear elliptic systems in high-latency, distributed-memory environments. We give a brief description of this family of algorithms, with an emphasis on domain decomposition iterative aspects. We then describe numerical simulations with Newton-Krylov-Schwarz methods on aerodynamics applications emphasizing comparisons with a standard defect-correction approach, subdomain preconditioner consistency, subdomain preconditioner quality, and the effect of a coarse grid.

1.2 INTRODUCTION

Several trends contribute to the importance of parallel implicit algorithms in CFD. Multidisciplinary analysis and optimization put a premium on the ability of algorithms to achieve low residual solutions rapidly, since analysis codes for individual components

[1] Department of Computer Science, University of Colorado-Boulder, Boulder, CO 80309-0430, USA. cai@cs.colorado.edu

[2] Department of Computer Science, Old Dominion University, Norfolk, VA 23529-0162 and ICASE, MS 132C, NASA LaRC, Hampton, VA 23681-0001, USA. keyes@icase.edu

[3] ICASE, MS 132C, NASA LaRC, Hampton, VA 23681-0001, USA. venkat@icase.edu

Divisibility, Smoothness and Cryptographic Applications

David Naccache
Équipe de cryptographie
École normale supérieure
45 rue d'Ulm, F-75230 Paris, Cedex 05, France
david.naccache@ens.fr

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@comp.mq.edu.au

October 17, 2008

Abstract

This paper deals with products of moderate-size primes, familiarly known as *smooth numbers*. Smooth numbers play an crucial role in information theory, signal processing and cryptography.

We present various properties of smooth numbers relating to their enumeration, distribution and occurrence in various integer sequences. We then turn our attention to cryptographic applications in which smooth numbers play a pivotal role.

Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS

Hanno Böck[*] Aaron Zauner[#§] Sean Devlin[δ]
Juraj Somorovsky[¶] Philipp Jovanovic[‡]

May 17, 2016

Abstract

We investigate nonce reuse issues with the GCM block cipher mode as used in TLS and focus in particular on AES-GCM, the most widely deployed variant. With an Internet-wide scan we identified 184 HTTPS servers repeating nonces, which fully breaks the authenticity of the connections. Affected servers include large corporations, financial institutions, and a credit card company. We present a proof of concept of our attack allowing to violate the authenticity of affected HTTPS connections which in turn can be utilized to inject seemingly valid content into encrypted sessions. Furthermore we discovered over 70,000 HTTPS servers using random nonces, which puts them at risk of nonce reuse if a large amount of data is sent over the same connection.

1 Introduction

The Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM), or short: AES-GCM [23, 5], is currently the most widely used cipher for symmetric (authenticated) encryption in the TLS protocol [3]. This came as a consequence of the exposure of various weaknesses in many alternative symmetric TLS ciphers during the past few years. The CBC mode was affected by a whole series of attacks, including BEAST [4] (affecting TLS 1.0), Lucky Thirteen [1] (affecting all versions, based on timing side channels and the older Vaudenay attack), POODLE [24] (only affecting SSLv3) and POODLE-TLS [21] (implementation bugs). All those attacks did not exploit weaknesses of CBC per se, but took advantage of the particular way how

[*] https://hboeck.de, hanno@hboeck.de
[#] SBA Research gGmbH, azauner@sba-research.org
[§] lambdis: resilient systems, azet@azet.org
[δ] Independent, seanpatrickdevlin@gmail.com
[¶] Horst Görtz Institute for IT Security, Ruhr University Bochum, juraj.somorovsky@rub.de
[‡] École Polytechnique Fédérale de Lausanne (EPFL), philipp.jovanovic@epfl.ch
[D] The authors grant IACR a non-exclusive and irrevocable license to distribute the article under the CC BY 4.0 (creative commons attribution) license.

All source-code, scripts and accompanying documentation are publicly available under CC0 1.0 license from https://github.com/nonce-disrespect/nonce-disrespect/.

Proc. Natl. Acad. Sci. USA
Vol. 70, No. 10, pp. 4768–4772, October 1973
Physics

Lyapounov variable: Entropy and measurement in quantum mechanics

(irreversible processes/reduction of the wave packet/operator time/nonfactorizable superoperators/noncommutation properties of operators)

B. MISRA, I. PRIGOGINE†, AND M. COURBAGE

Faculté des Sciences, Université Libre de Bruxelles, Brussels, Belgium†

Contributed by I. Prigogine, July 3, 1973

ABSTRACT We discuss the question of the dynamical meaning of the second law of thermodynamics in the framework of quantum mechanics. Previous discussion of the problem in the framework of classical dynamics has shown that the second law can be given a dynamical meaning in terms of the existence of so-called Lyapounov variables—i.e., dynamical variables varying monotonically in time without becoming contradictory. It has been found that such variables can exist in an extended framework of classical dynamics, provided that the dynamical motion is suitably unstable. In this paper we begin to extend these results to quantum mechanics. It is found that no dynamical variable with the characteristic properties of nonequilibrium entropy can be defined in the standard formulation of quantum mechanics. However, if the Hamiltonian has certain well-defined spectral properties, such variables can be defined but only as a *nonfactorizable* superoperator. Necessary nonfactorizability of such entropy operators *M* has the consequence that they cannot preserve the class of pure states. Physically, this means that the distinguishability between pure states and corresponding mixtures must be lost in the case of a quantal system for which the algebra of observables can be extended to include a new dynamical variable representing nonequilibrium entropy. We discuss how this result leads to a solution of the quantum measurement problem. It is also found that the question of existence of entropy of superoperators *M* is closely linked to the problem of defining an operator of time in quantum mechanics.

1. Introduction

No other question in theoretical physics seems to have caused as much controversial discussions over as long a period of time as the question of the dynamical meaning of irreversibility expressed in the second law of thermodynamics. With the advent of quantum mechanics and the discovery of the apparently irreversible exponential decay of unstable particles, this question has gained added theoretical importance. Irreversibility is now an essential feature of gross macroscopic phenomena such as the familiar transport processes and it also seems to be intrinsic in such basic processes as the "wave packet reduction" caused by measurement and the decay of unstable particles.

The difficulties encountered by the traditional approach to the problem of the dynamical meaning of the second law are well known (1). In this paper we shall discuss this question in the framework of quantum dynamics from the alternative viewpoint that has emerged from our previous work (2–6). This discussion will lead to the conclusion that the second law can be interpreted as a dynamical principle in an extended framework of quantum dynamics without involving contradictions and that thus interpreted it implies the loss of distinguishability between pure states and mixtures for systems to which the second law applies.

As is well known, a fundamental distinction is made in quantum mechanics between pure states (usually represented by unit vectors of a Hilbert space) and the mixtures represented by the so-called density operators. The pure states occupy a privileged position in the theory: the quantum superposition principle holds between the pure states; dynamical evolution, as described by the Schrödinger equation, transforms pure states into pure states and the observables of the theory correspond to self-adjoint operators that again map pure states into pure states. The basic laws of quantum mechanics can thus be formulated without ever invoking the notion of mixtures and their representation by density operators. The use of this notion is generally believed to reflect incompleteness of knowledge about the system and it is considered to be only a matter of practical convenience or approximation.

The fundamental distinction between the pure states and mixtures and the privileged position of the pure states are, however, not maintained in measurement processes. As von Neumann's by now "classical" analysis has shown, we have, in addition to the deterministic and reversible evolution of the pure states into pure states described by the Schrödinger equation, the peculiar evolution, called "the reduction of the wave packet," which occurs during measurement processes. This latter evolution is irreversible and typically transforms pure states into mixtures.

Obviously, one can not accept such a dualism of state evolution as final, and various authors have attempted to overcome it. (We do not intend to survey these attempts here; an excellent account of the subject can be found in ref. 8.) Let us only emphasize here that it is the presumed distinguishability between the pure state (which the Schrödinger equation would predict for the object + apparatus system) and the mixture that arises from the wave packet reduction that is at the root of the conceptual problems posed by quantum theory of measurement. This dualism of state-evolution could be avoided if one could formulate a physical principle that implies the loss of distinguishability between the pure states and the corresponding mixtures in the case of sufficiently complex systems capable of serving as measuring and recording apparatus (6). The main finding of our paper is that the second law of thermodynamics, when suitably interpreted as a dynamical principle, is just the physical principle that leads to the desired loss of distinguishability between the pure states and mixtures.

Before we discuss further our conclusions, it will be useful to consider briefly the problem of irreversibility in classical dynamics. Obviously, the simplest dynamical interpretation of the second law would be to require the existence of a dynamical variable with the characteristic properties of entropy—in particular, the property of monotonic variation with time. However, Poincaré (7) has pointed out that such a dy-

The publication costs of this article were defrayed in part by page charge payment. This article must therefore be hereby marked "advertisement" in accordance with 18 U. S. C. §1734 solely to indicate this fact.

* Also at the University of Texas at Austin, Center for Statistical Mechanics and Thermodynamics, Austin, TX 78712.
† Postal address: campus plaine U.L.B. Boulevard du Triomphe, 1050 Bruxelles, Belgique.

Exploiting the Power of GPUs for Asymmetric Cryptography

Robert Szerwinski and Tim Güneysu

Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
{szerwinski,guneysu}@crypto.rub.de

Abstract. Modern Graphics Processing Units (GPU) have reached a dimension with respect to performance and gate count exceeding conventional Central Processing Units (CPU) by far. Many modern computer systems include – beside a CPU – such a powerful GPU which runs idle most of the time and might be used as cheap and instantly available co-processor for general purpose applications.
In this contribution, we focus on the efficient realisation of the computationally expensive operations in asymmetric cryptosystems on such off-the-shelf GPUs. More precisely, we present improved and novel implementations employing GPUs as accelerator for RSA and DSA cryptosystems as well as for Elliptic Curve Cryptography (ECC). Using a recent Nvidia 8800GTS graphics card, we are able to compute 813 modular exponentiations per second for RSA or DSA-based systems with 1024 bit integers. Moreover, our design for ECC over the prime field P-224 even achieves the throughput of 1412 point multiplications per second.

Keywords: Asymmetric Cryptosystems, Graphics Processing Unit, RSA, DSA, ECC.

1 Introduction

For the last twenty years graphics hardware manufacturers have focused on producing fast Graphics Processing Units (GPUs), specifically for the gaming community. This has more recently led to devices which outperform general purpose Central Processing Units (CPUs) for specific applications, particularly when comparing the MIPS (million instructions per second) benchmarks. Hence, a research community has been established to use the immense power of GPUs for general purpose computations (GPGPU). In the last two years, prior limitations of the graphics application programming interfaces (API) have been removed by GPU manufacturers by introducing unified processing units in graphics cards. They support a general purpose instruction set by a native driver interface and framework.

In the field of asymmetric cryptography, the security of all practical cryptosystems rely on hard computational problems strongly dependant on the choice of parameters. But with rising parameter sizes (often in the range of 1024–4096 bits), however, computations become more and more challenging for the underlying processor. For modern hardware, the computation of a *single* cryptographic operation is not critical, however in a many-to-one communication scenario, like a central server in a company's data processing centre, it may be confronted with hundreds or thousands of simultaneous connections and corresponding cryptographic operations. As a result, the most common current solution are cryptographic accelerator cards. Due to the limited market, their price tags are often in the range of several thousands euros or US dollars. The question at hand is whether commodity GPUs can be used as high-performance public-key accelerators.

In this work, we will present novel implementations of cryptosystems based on modular exponentiations and elliptic curve operations on recent graphics hardware. To the best of our knowledge, this is the first publication making use of the CUDA framework for GPGPU processing of asymmetric cryptosystems. We will start with implementing the extremely wide-spread *Rivest Shamir Adleman* (RSA) cryptosystem [30]. The same implementation based on modular exponentiation for large integers can be used to implement the *Digital Signature Algorithm*

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/239008775

Simulating Bell inequality violations with classical optics encoded qubits

Article in Journal of the Optical Society of America B · April 2010

DOI: 10.1364/JOSAB.27.000779

CITATIONS
24

READS
79

3 authors:

Matías Alejandro Goldin
French National Centre for Scientific Research
18 PUBLICATIONS **60** CITATIONS

SEE PROFILE

Diego Francisco
National Scientific and Technical Research Cou…
11 PUBLICATIONS **82** CITATIONS

SEE PROFILE

Silvia Ledesma
University of Buenos Aires
91 PUBLICATIONS **485** CITATIONS

SEE PROFILE

All content following this page was uploaded by Matías Alejandro Goldin on 05 August 2014.

The user has requested enhancement of the downloaded file.

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/237134040

Data Structures in Natural Computing: Databases as Weak or Strong Anticipatory Systems

Article · August 2004

DOI: 10.1063/1.1781342

CITATIONS
6

READS
36

2 authors:

Nick Rossiter
Northumbria University
93 PUBLICATIONS 350 CITATIONS
SEE PROFILE

Michael Heather
Retired
62 PUBLICATIONS 120 CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Dartington Hall Deer Park Project View project

Project Formal Process Theory View project

All content following this page was uploaded by Michael Heather on 16 September 2014.

The user has requested enhancement of the downloaded file.

arXiv:0804.2264v2 [quant-ph] 26 Sep 2008

Quantum Computing

Eleanor Rieffel
FX Palo Alto Laboratory

Contents

1 Introduction **3**

2 Early history **4**

3 Basic concepts of quantum computation **5**

4 Quantum algorithms **6**
4.1 Grover's algorithm and generalizations 7
4.2 Generalizations of Shor's factoring algorithm 8
4.3 Other classes of algorithms 9
4.4 Simulation 9

5 Limitations of quantum computing **10**

6 Quantum protocols **10**

7 Broader implications of quantum information processing **12**

8 Impact of quantum computers on security **13**

9 Implementation efforts **14**

10 Advanced concepts **16**
10.1 Robustness 16
10.2 Models underlying quantum computation 17
10.3 What if quantum mechanics is not quite correct? 19

11 Conclusions **20**

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/259034727

Discrete Reconstruction of Strange Attractors of Chua's Circuit

Article in International Journal of Bifurcation and Chaos · August 1994

DOI: 10.1142/S0218127494000630

CITATIONS
23

READS
43

2 authors, including:

Luis Antonio Aguirre
Federal University of Minas Gerais
285 PUBLICATIONS **2,737** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Hidráulica geral View project

Observability and synchronization of networks View project

All content following this page was uploaded by Luis Antonio Aguirre on 08 March 2015.

The user has requested enhancement of the downloaded file.

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/252845049

Some Two-Steps Discrete-Time Anticipatory Models With `Boiling' Multivaluedness

Article · June 2006

DOI: 10.1063/1.2216639

CITATIONS
5

READS
12

2 authors, including:

Alexander Makarenko
National Technical University of Ukraine Kiev Polytechnic Institute
35 PUBLICATIONS **959** CITATIONS

SEE PROFILE

All content following this page was uploaded by Alexander Makarenko on 01 September 2015.

The user has requested enhancement of the downloaded file.

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/45863195

Contextuality in Measurement-based Quantum Computation

Article in Physical Review A · July 2009

DOI: 10.1103/PhysRevA.88.022322 · Source: arXiv

CITATIONS
41

READS
40

1 author:

Robert Raussendorf
University of British Columbia - Vancouver
69 PUBLICATIONS **6,684** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Contextuality as a resource in quantum computation View project

All content following this page was uploaded by Robert Raussendorf on 26 January 2016.

The user has requested enhancement of the downloaded file.

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/234939227

Some physical applications of fractional Schrödinger equation

Article in Journal of Mathematical Physics · August 2006

DOI: 10.1063/1.2201026

CITATIONS
119

READS
333

2 authors, including:

Xiaoyi Guo
Linyi University
5 PUBLICATIONS **124** CITATIONS

SEE PROFILE

All content following this page was uploaded by Xiaoyi Guo on 17 March 2016.

The user has requested enhancement of the downloaded file.

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/269670313

Bijective Epistemology and Space–Time

Article in Foundations of Science · January 2014

DOI: 10.1007/s10699-014-9383-y

CITATIONS
15

READS
95

1 author:

Amrit Sorli
FOPI
169 PUBLICATIONS **385** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Research On NOW View project

Advanced Relativity - AR View project

All content following this page was uploaded by Amrit Sorli on 22 March 2016.

The user has requested enhancement of the downloaded file.

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/253970177

Incursive anticipatory control of a chaotic robot arm

Article · July 1998

DOI: 10.1063/1.166337

CITATIONS
2

READS
14

1 author:

Daniel M. Dubois
University of Liège
102 PUBLICATIONS **911** CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

THEORY OF INCURSIVE SYNCHRONIZATION FOR ANTICIPATION OF CHAOS View project

incursive and hyperincursive discrete physics View project

All content following this page was uploaded by Daniel M. Dubois on 24 November 2016.

The user has requested enhancement of the downloaded file.

Non-interactive zero-knowledge proofs in the quantum random oracle model

Dominique Unruh
University of Tartu

July 29, 2014

Abstract

We present a construction for non-interactive zero-knowledge proofs of knowledge in the random oracle model from general sigma-protocols. Our construction is secure against quantum adversaries. Prior constructions (by Fiat-Shamir and by Fischlin) are only known to be secure against classical adversaries, and Ambainis, Rosmanis, Unruh (FOCS 2014) gave evidence that those constructions might not be secure against quantum adversaries in general.

To prove security of our constructions, we additionally develop new techniques for adaptively programming the quantum random oracle.

Contents

1 Introduction **2**
1.1 Preliminaries 5

2 Security notions **5**
2.1 Non-interactive proof systems 5
2.2 Sigma protocols 7

3 Quantum random oracles **8**

4 Online-extractable NIZK proofs **12**
4.1 Construction 12
4.2 Zero-knowledge 12
4.3 Online extractability 15

5 Signatures **19**

A Sigma-protocols with oblivious commitments **21**

References **23**

Symbol Index **24**

Keyword Index **25**

A Formal Treatment of Backdoored Pseudorandom Generators

Yevgeniy Dodis[1], Chaya Ganesh[1], Alexander Golovnev[1], Ari Juels[2], and Thomas Ristenpart[3]

[1]Department of Computer Science, New York University
[2]Jacobs Institute, Cornell Tech
[3]Department of Computer Sciences, University of Wisconsin

Abstract

We provide a formal treatment of backdoored pseudorandom generators (PRGs). Here a saboteur chooses a PRG instance for which she knows a trapdoor that allows prediction of future (and possibly past) generator outputs. This topic was formally studied by Vazirani and Vazirani, but only in a limited form and not in the context of subverting cryptographic protocols. The latter has become increasingly important due to revelations about NIST's backdoored Dual EC PRG and new results about its practical exploitability using a trapdoor.

We show that backdoored PRGs are equivalent to public-key encryption schemes with pseudorandom ciphertexts. We use this equivalence to build backdoored PRGs that avoid a well known drawback of the Dual EC PRG, namely biases in outputs that an attacker can exploit without the trapdoor. Our results also yield a number of new constructions and an explanatory framework for why there are no reported observations in the wild of backdoored PRGs using only symmetric primitives.

We also investigate folklore suggestions for countermeasures to backdoored PRGs, which we call *immunizers*. We show that simply hashing PRG outputs is not an effective immunizer against an attacker that knows the hash function in use. Salting the hash, however, does yield a secure immunizer, a fact we prove using a surprisingly subtle proof in the random oracle model. We also give a proof in the standard model under the assumption that the hash function is a universal computational extractor (a recent notion introduced by Bellare, Tung, and Keelveedhi).

1 Introduction

Pseudorandom number generators (PRGs) stretch a short, uniform bit string to a larger sequence of pseudorandom bits. Beyond being a foundational primitive in cryptography, they are used widely in practice within applications requiring relatively large amounts of cryptographic randomness. Seed the PRG via the output of some (more expensive to use) source of randomness, such as a system random number generator, and then use it to efficiently generate effectively unbounded number of pseudorandom bits for the application. Unfortunately, an adversary that can distinguish such bits from uniform or, worse yet, outright predict the outputs of a PRG, almost invariably compromises security of higher level applications. This fragility in the face of poor pseudorandom sources is borne out by a long history of vulnerabilities [7, 8, 15, 17, 18, 23, 25, 34].

5 Solving Schrodinger's Equation in One Dimension

1. Write down Schrodinger's Eqn
2. ???
3. PROFIT

Except for the original Star Wars™ Trilogy, the middle portion of all Trilogies is always boring[9]. And so, in our lectures on Quantum Mechanics, we arrive at the sagging middle.

In this section, we solve Schrodinger's Equation for a wide variety of potentials $U(x)$ in one dimension. So unfortunately we will spend some time mangling with partial differential equations, which may or may not be your favorite cup of caffeinated beverage. Having said that, solving this equation will illustrate some of the features of Quantum Mechanics of which we have been making assertions about so far, and some which you may have heard about.

- Section 5.1 : Quantization of Energy States
- Section 5.2 : Scattering, Transmissivity and Reflectivity
- Section 5.3 : Tunneling
- Section 5.4 : The Gaussian Wave Packet and Minimum Uncertainty
- Section 5.5 : Parity Operator
- Section 5.6 : Bound and Unbounded States

Note : in this section we will almost exclusively be working in the Stationary States basis, i.e. χ_E of the Hamiltonian, so we will drop the subscript E from χ and ψ. When there is an ambiguity, we will restore it. Also, sometimes we refer to $\chi(x)$ as the "wavefunction", although technically we are really solving for the eigenfunctions of the Hamiltonian.

5.1 Quantization of Energy Eigenstates : The Infinite Potential Well

Consider the **infinite potential well** (Fig 10)

$$U(x) = \begin{cases} 0 & , \quad 0 < x < a \\ \\ \infty & , \quad \text{otherwise} \end{cases}$$

Using Stationary States Eq. (164) in one dimension

$$\psi(x,t) = \chi(x) \exp\left[\frac{-iEt}{\hbar}\right], \tag{172}$$

we obtain the time-independent Schrodinger's Equation

$$-\frac{\hbar^2}{2m}\frac{d^2\chi}{dx^2} + U(x)\chi = E\chi. \tag{173}$$

We now look at the behavior of $\chi(x)$ inside and outside the well.

- **Outside Well**:

$$U(x) = \infty \Rightarrow \chi(x) = 0 \tag{174}$$

otherwise $E = \infty$ from (173). Thus, as in classical physics, there is zero probability of finding the particle outside the well.

[9] The prequels of Star Wars is the exception: they are all terrible.

Sliding right into disaster: Left-to-right sliding windows leak

Daniel J. Bernstein[2], Joachim Breitner[3], Daniel Genkin[3,4], Leon Groot Bruinderink[1], Nadia Heninger[3], Tanja Lange[1], Christine van Vredendaal[1], Yuval Yarom[5]

[1] Technische Universiteit Eindhoven, Netherlands
L.Groot.Bruinderink@tue.nl, tanja@hyperelliptic.org, c.v.vredendaal@tue.nl
[2] University of Illinois at Chicago, USA
djb@cr.yp.to
[3] University of Pennsylvania, USA
{joachim,danielg3,nadiah}@cis.upenn.edu
[4] University of Maryland, USA
[5] University of Adelaide and Data61, CSIRO, Australia
yval@cs.adelaide.edu.au

Abstract. It is well known that constant-time implementations of modular exponentiation cannot use sliding windows. However, software libraries such as Libgcrypt, used by GnuPG, continue to use sliding windows. It is widely believed that, even if the complete pattern of squarings and multiplications is observed through a side-channel attack, the number of exponent bits leaked is not sufficient to carry out a full key-recovery attack against RSA. Specifically, 4-bit sliding windows leak only 40% of the bits, and 5-bit sliding windows leak only 33% of the bits.

In this paper we demonstrate a complete break of RSA-1024 as implemented in Libgcrypt. Our attack makes essential use of the fact that Libgcrypt uses the left-to-right method for computing the sliding-window expansion. We show for the first time that the direction of the encoding matters: the pattern of squarings and multiplications in left-to-right sliding windows leaks significantly more information about the exponent than right-to-left. We show how to extend the Heninger-Shacham algorithm for partial key reconstruction to make use of this information and obtain a very efficient full key recovery for RSA-1024. For RSA-2048 our attack is efficient for 13% of keys.

Keywords: left-to-right sliding windows, collision entropy, cache attack, Flush+Reload, RSA-CRT.

1 Introduction

Modular exponentiation in cryptosystems such as RSA is typically performed starting from the most significant bit (MSB) in a left-to-right manner. More efficient implementations use precomputed values to decrease the number of

15 July 1996

PHYSICS LETTERS A

Physics Letters A 217 (1996) 188–193

The physical nature of information

Rolf Landauer *

IBM T.J. Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598, USA

Received 5 May 1996
Communicated by V.M. Agranovich

Abstract

Information is inevitably tied to a physical representation and therefore its restrictions and possibilities relate to the laws of physics and the parts available in the universe. Quantum mechanical superpositions of information bearing states can be used, and the real utility of that needs to be understood. Quantum parallelism in computation is one possibility and will be assessed pessimistically. The energy dissipation requirements of computation, of measurement and of the communication link are discussed. The insights gained from the analysis of computation are viewed as a rejection of the perceived wisdom in the other two fields. A concluding section speculates about the nature of the laws of physics, which are algorithms for the handling of information, and must be executable in our real physical universe.

1. Information is physical

Information is not a disembodied abstract entity; it is always tied to a physical representation. It is represented by engraving on a stone tablet, a spin, a charge, a hole in a punched card, a mark on paper, or some other equivalent. This ties the handling of information to all the possibilities and restrictions of our real physical world, its laws of physics and its storehouse of available parts.

This view was implicit in Szilard's discussion of Maxwell's demon [1]. Szilard's discussion, while a major milestone in the elucidation of the demon, was by no means an unambiguous resolution. The history of that can be found in Refs. [2,3]. The acceptance of the view, however, that information is a physical entity, has been slow. Penrose [4], for example, argues for the Platonic reality of mathematics, independent of any manipulation. He tells us "... devices can yield only approximations to a structure that has a deep and 'computer-independent' existence of its own." Indeed, our assertion that information is physical amounts to an assertion that mathematics and computer science are a part of physics. We cannot expect our colleagues in mathematics and in computer science to be cheerful about surrendering their independence. Mathematics claims, in particular, have long assumed that mathematics was there first, and that physics needed that to describe the universe. We will, instead, ask for a more self-consistent framework in Sec. V.

P.W. Bridgman, recognized as Nobel laureate for his work in high pressure physics, published a remarkable paper [5] in 1934. That was his attempt to wrestle with the paradoxes of set theory. His solution: Mathematics must be confined to that which can be handled by a succession of unambiguous executable operations. Bridgman's paper is essentially a wish ad for a Turing machine, which came a few years later. In a remarkable coincidence Bridgman even uses the word program for a succession of executable instructions. Bridgman

* E-mail: landauer@watson.ibm.com.

0375-9601/96/$12.00 © 1996 Elsevier Science B.V. All rights reserved.
PII S0375-9601(96)00453-7

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 30, 2016

The Honorable Mike Enzi
Chairman
Committee on the Budget
United States Senate

Public Relations Spending: Reported Data on Related Federal Activities

Dear Mr. Chairman:

With the increased popularity and accessibility of expanded media platforms, the federal government's ability to publicize information has changed rapidly, but the total scope of federal public relations activities is largely unknown. A number of factors makes it difficult to quantify the resources the federal government devotes to public relations. These factors include the expanded use of web-based platforms, such as Facebook and Twitter, and the wide variety of activities that could be considered public relations, from publicizing health and safety bulletins to providing information on federal entitlements and benefits.

Given the changing media landscape, you requested that we determine how much the federal government spends on public relations activities, including contracts and internal agency support, and identify the highest-spending agencies. This report examines: (1) the reported federal spending on contracts for advertising and public relations activities from fiscal year 2006 through 2015, including the agencies that have spent the most; and (2) the reported number of federal public relations employees and their combined annual salaries from fiscal years 2006 through 2014, and the agencies reported to have the highest total salaries for public relations employees.[1]

To address our first objective, we analyzed data from the Federal Procurement Data System – Next Generation (FPDS-NG) database for fiscal years 2006 through 2015. The FPDS-NG database captures information on the federal government's contract awards and obligations. It includes data for most federal contracts that have an estimated value of $3,000 or more.[2] We reviewed obligations data for contracts coded under the "support - management: public relations" and "support - management: advertising" product service codes.[3] We assessed the reliability of these data by considering known strengths and weaknesses of FPDS-NG data, based on our past work, and looking for obvious errors and inconsistencies in the data. We

[1]At the time of our review, the most recent data we were able to access on federal employees were from fiscal year 2014.

[2]FPDS-NG does not include data from intelligence agencies, the U.S. Postal Service, judicial branch, and most of the legislative branch.

[3]An obligation is a definite commitment that creates a legal liability for the payment of goods and services ordered or received. An agency incurs an obligation, for example, when it places an order, signs a contract, or takes other actions that require the government to make payments.

Z-Channel: Scalable and Efficient Scheme in Zerocash

Yuncong Zhang* Yu Long* Zhen Liu* Zhiqiang Liu* Dawu Gu*
zhjdzhangyuncong@sjtu.edu.cn longyu@sjtu.edu.cn liuzhen@sjtu.edu.cn liu_zq@cs.sjtu.edu.cn dwgu@sjtu.edu.cn

*Shanghai Jiao Tong University

***Abstract*—Decentralized ledger-based cryptocurrencies such as Bitcoin provide a means to construct payment systems without requiring a trusted bank, yet the anonymity of Bitcoin is proved to be far from satisfactory. Zerocash is the first full-fledged anonymous digital currency based on the blockchain technology, using zk-SNARK as the zero-knowledge module for the privacy protection. Zerocash solves the privacy problem but still suffers two major problems: insufficient scalability and latency in making a payment. Meanwhile, micropayment channel proves to be a nice solution to these issues in blockchain-based digital currencies. In this paper, we present Z-Channel, the construction of micropayment system on Zerocash, which effectively solves the scalability and instant payment problems in Zerocash. Z-Channel relies on multisignature and lock time functionalities which are not provided by Zerocash. We manage to improve the Zerocash scheme to support these functionalities without compromising the privacy guaranteed by Zerocash. Finally, the simulation results demonstrate that Z-Channel significantly improves the scalability and reduces the average confirmation time for the payments conducted in Zerocash.**

***Keywords*—Cryptocurrency, Zerocash, Scalability, Privacy, Instant payment**

I. Introduction

Decentralized ledger-based cryptocurrencies such as Bitcoin [21] provide a means to construct payment systems without requiring a trusted bank. Following Bitcoin, many digital currencies have been devised trying to improve Bitcoin with respect to its functionalities [7], [15], [8], [17], consensus schemes [26], [15], scalability and efficiency [28], [7], and privacy [27], [16], etc.

Privacy protection is one of the features of ledger-based digital currency that attract the most attention [4]. Bitcoin has been thoroughly analyzed and its privacy protection is proved to be easily compromised [23]. By analyzing the transaction graph, values and dates in the ledger one can possibly link Bitcoin addresses with real world identity. To break such linkability in Bitcoin, one can store his Bitcoin into a *mix*, which is a trusted central party which mixes Bitcoins from different users and gives different coins back to them after sufficient amount of coins are mixed together. However, the delay in redeeming the coins and the trust to a central party is unacceptable to some users with strong motivation to hide information. A remedy is to implement a decentralized mix. To accomplish this, protocols have been designed such as TumbleBit [12], CoinSwap [19], CoinParty [29] and CoinShuffle[24] which is based on the work of CoinJoin [18]. Additionally, many altcoins have been developed, including Zerocoin [20], BlindCoin [27] and its predecessor Mixcoin [5] and Pinocchio coin [6], etc. These solutions, however, suffer from the following drawbacks: 1) Insufficient performance. Most of them require one or more rounds of interaction between many parties. 2) Lack of functionality. They simply present a way for users to "wash" their coins from time to time, but everyday transactions are still conducted without privacy.

Compared to the mix-based solutions, Zerocash [25] is the first full-fledged privacy preserving ledger-based digital currency, which completely conceals the user identity and amount of payment in each and every transaction. The construction of Zerocash uses zero-knowledge proof, specifically zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs) [2], [9].

Despite all the advantages in privacy protection, the design of Zerocash does not address the scalability and efficiency problems which exist in almost all the ledger-based digital currencies. In fact, the transaction size of Zerocash is larger than that of Bitcoin, and the time to verify zk-SNARK proof is longer than verifying a Bitcoin transaction, which makes the scalability problem in Zerocash even worse than in Bitcoin.

For other ledger-based digital currencies, there have been works trying to solve the scalability and efficiency issues. Changing the blocksize [1] is a straightforward way to improve the scalability, though it compromises the efficiency with higher network latency and longer verification time. The block merging technique proposed in MimbleWimble [14] requires a special structure for the blocks and transactions, sacrificing a majority of the functionalities of the digital currency. Micropayment channel [22] proves to be the most promising in solving both of the scalability and efficiency problems effectively. By transactions conducted securely off-chain, micropayment channel is likely to enable Bitcoin or similar altcoins to support billions of users. Despite the dramatic improvement in scalability and payment speed micropayment channels is promising, no work has been proposed to construct a micropayment system on Zerocash [1].

[1]The work of BOLT (Blind Off-chain Lightweight Transaction) [11] mentions Zerocash, claiming that if a BOLT is built on Zerocash, it would provide better channel privacy than built on other currencies. However, BOLT focuses on solving the linkability issue in channels, while the concrete construction of BOLT over Zerocash is not specified in their work.

A Note on Quantum Security for Post-Quantum Cryptography

Fang Song
Department of Combinatorics & Optimization
and Institute for Quantum Computing
University of Waterloo

Abstract

Shor's quantum factoring algorithm and a few other efficient quantum algorithms break many classical crypto-systems. In response, people proposed post-quantum cryptography based on computational problems that are believed hard even for quantum computers. However, security of these schemes against *quantum* attacks is elusive. This is because existing security analysis (almost) only deals with classical attackers and arguing security in the presence of quantum adversaries is challenging due to unique quantum features such as no-cloning.

This work proposes a general framework to study which classical security proofs can be restored in the quantum setting. Basically, we split a security proof into (a sequence of) classical security reductions, and investigate what security reductions are "quantum-friendly". We characterize sufficient conditions such that a classical reduction can be "lifted" to the quantum setting.

We then apply our lifting theorems to post-quantum signature schemes. We are able to show that the classical generic construction of hash-tree based signatures from one-way functions and and a more efficient variant proposed in [BDH11] carry over to the quantum setting. Namely, assuming existence of (classical) one-way functions that are resistant to efficient quantum inversion algorithms, there exists a quantum-secure signature scheme. We note that the scheme in [BDH11] is a promising (post-quantum) candidate to be implemented in practice and our result further justifies it. Actually, to obtain these results, we formalize a simple criteria, which is motivated by many classical proofs in the literature and is straightforward to check. This makes our lifting theorem easier to apply, and it should be useful elsewhere to prove quantum security of proposed post-quantum cryptographic schemes. Finally we demonstrate the generality of our framework by showing that several existing works (Full-Domain hash in the quantum random-oracle model [Zha12b] and the simple hybrid arguments framework in [HSS11]) can be reformulated under our unified framework.

1 Introduction

Advances in quantum information processing and quantum computing have brought about fundamental challenges to cryptography. Many classical cryptographic constructions are based on computational problems that are assumed hard for efficient classical algorithms. However, some of these problems, such as factoring, discrete-logarithm and Pell's equation, can be solved efficiently on a quantum computer [Sho97, Hal07]. As a result, a host of crypto-systems, e.g, the RSA encryption scheme that is deployed widely over the Internet, are broken by a quantum attacker.

A natural countermeasure is to use *quantum-resistant* assumptions instead. Namely, one can switch to other computational problems which appear hard to solve even on quantum computers, and construct cryptographic schemes based on them. Examples include problems in discrete lattices [MR09, Pei09] and hard coding problems [Sen11]. We can also make generic assumptions such as the existence of one-way functions that no efficient quantum algorithms can invert. This leads to the active research area termed

2016

2016

RESEARCH SPONSORED BY
THE OFFICE OF NAVAL RESEARCH
DEPARTMENT OF THE NAVY
Contract N00014-70-C-0328
NR 276-021/2-13-70 (462)

DISTRIBUTION STATEMENT
Approved for public release; distribution unlimited.
Reproduction in whole or in part is permitted for any purpose of the United States Government.

DRAFT IN LIEU
OF FINAL
RAC-D7-R

MARCH 1972

AD 739515

Foundations of the Prescriptive Sciences

Volume II

by Nicholas M. Smith
Milton C. Mamey

with Appendix
by Donald L. Reisler

DRAFT
DDC
RECEIVED
APR 5 1972
B

Copy 50 of 75

SLC AD739514

RAC Research Analysis Corporation

Reproduced by
NATIONAL TECHNICAL
INFORMATION SERVICE

394

On Improving Integer Factorization and Discrete Logarithm Computation using Partial Triangulation

Fabrice Boudot

fabrice.boudot@orange.fr

Abstract. The number field sieve is the best-known algorithm for factoring integers and solving the discrete logarithm problem in prime fields. In this paper, we present some new improvements to various steps of the number field sieve. We apply these improvements on the current 768-bit discrete logarithm record and show that we are able to perform the overall computing time in about 1200 core-years using these improvements instead of 2550 core-years using the best known parameters for this problem. Moreover, we show that the pre-computation phase for a 768-bit discrete logarithm problem, that allows for example to build a massive decryption tool of IPsec traffic protected by the Oakley group 1, was feasible in reasonable time using technologies available before the year 2000.

Keywords: discrete logarithm, integer factorization, number field sieve, sparse linear algebra

1 Introduction

1.1 The discrete logarithm problem

The hardness of the discrete logarithm problem in prime fields is one of the most used assumptions in asymmetric cryptography, alongside with the hardness of integer factorization and discrete logarithm computations on elliptic curves. The security of well-known cryptographic primitives, such as the Diffie-Hellman key exchange protocol [12], the El-Gamal encryption [13], and the Digital Signature Algorithm [14], are based on the discrete logarithm problem, and these primitives are used in the most used security protocols such as TLS, IPsec or SSH.

The discrete logarithm problem over prime fields can be defined as follows. Let p be a large prime number and let $q = p - 1$. Let g be an element of order q in $\mathbf{Z}_p$. Let y be an element of $\mathbf{Z}_p$. We have to find a number $x \in [0, q-1]$, named the discrete logarithm of y in base g modulo p, that is such that $y \equiv g^x \bmod p$.

When p is large enough, the best algorithm to solve the discrete logarithm problem is the number field sieve [29]. The asymptotic complexity of this algorithm, when p has no specific form, is $L_p(1/3, (64/9)^{1/3} + o(1))$, where L_p is defined by

$$L_p(\alpha, c) = \exp(c(\ln p)^{\alpha}(\ln \ln p)^{1-\alpha})$$

European Treaty Series - No. 185

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Available online at www.sciencedirect.com

ScienceDirect

Current Opinion in Cell Biology

The three-dimensional genome: principles and roles of long-distance interactions

M Jordan Rowley and Victor G Corces

The linear sequence of eukaryotic genomes is arranged in a specific manner within the three-dimensional nuclear space. Interactions between distant sites partition the genome into domains of highly associating chromatin. Interaction domains are found in many organisms, but their properties and the principles governing their establishment vary between different species. Topologically associating domains (TADs) extending over large genomic regions are found in mammals and *Drosophila melanogaster*, whereas other types of contact domains exist in lower eukaryotes. Here we review recent studies that explore the mechanisms by which long distance chromatin interactions determine the 3D organization of the genome and the relationship between this organization and the establishment of specific patterns of gene expression.

Address
Department of Biology, Emory University, 1510 Clifton Rd NE, Atlanta, GA 30322, USA

Corresponding author: Corces, Victor G (vcorces@emory.edu)

Current Opinion in Cell Biology 2016, **40**:8–14

This review comes from a themed issue on **Cell nucleus**

Edited by **Ulrike Kutay** and **Orna Cohen-Fix**

http://dx.doi.org/10.1016/j.ceb.2016.01.009

0955-0674/© 2016 Elsevier Ltd. All rights reserved.

Introduction: a three-dimensional genome

The eukaryotic nucleus is a complex three-dimensional environment in which genome function depends not only on the linear arrangement of regulatory sequence elements but also on their spatial organization for effective control of gene expression [1,2]. Modulation of transcription occurs in part through spatial proximity of regulatory elements and gene promoters [1,2]. These interactions are essential for organismal development and response to environmental stimuli [2,3••,4•,5] in eukaryotes, including yeast, worms, plants, flies, and mammals [6–11,12•]. Analysis of the role of chromatin 3D organization in gene expression is progressing rapidly, largely due to the development of chromosome conformation capture methods such as Hi-C [13]. Studies of long-range chromatin interactions have highlighted principles of three-dimensional genome organization, and whole genome chromatin contact maps have provided significant insights into how the 3D organization of the genome relates to gene expression [1,2]. Due to these advances we are beginning to understand overall chromosomal organization in the nucleus, how this organization is established, and how it can modulate gene expression. Here we discuss recent work that has helped answer important questions about the establishment and role of chromatin organization in genome regulation.

Units of organization

Whole-genome chromatin conformation capture (involving ligation and sequencing of spatially proximal DNA fragments — Hi-C as described in [13]) has been performed in several organisms and the results indicate that some features of chromatin 3D organization are consistent between some species (Figure 1). In many species and tissue types there are easily observable features of chromatin contact maps consisting of large genomic regions organized as contact domains [1,2]. Sequences within these Topologically Associated Domains (TADs) interact more frequently with sites inside than outside the domain. TADs with a median size of 880 kb have been found in mammals (Figure 1a) whereas *Drosophila* TADs have a median size of 107 kb [1] (Figure 1b). TADs in *Caenorhabditis elegans* are fairly weak, with the more easily defined domains located in the X chromosome of hermaphrodites [12•] (Figure 1c). In *Schizosaccharomyces pombe* TAD-like contact domains (termed globules) are present at sizes ranging from 50 to 100 kb [14•] (Figure 1e). However, large TAD-like structures are not as easily identifiable in some model organisms such as *Saccharomyces cerevisiae* and *A. thaliana* [6–9] (Figure 1d,f). This poses the question of whether TADs are truly conserved features of chromatin organization in eukaryotes.

TADs vary in size throughout an individual genome and are overall shorter in the smaller genome of *Drosophila* (Figure 1a,b). Since TAD borders form at sites of active transcription and in regions with high gene density, it is likely that these features occur more often in smaller genomes [15•]. To search for TADs in *S. cerevisiae*, the Hi-C protocol was modified to increase resolution by using micrococcal nuclease (MNase) digestion in lieu of restriction fragmentation (Micro-C) [15•]. Using this method high-frequency contact domains were observed in *S. cerevisiae* [15•] (Figure 1f). These domains are indeed smaller than those of mammals and *Drosophila*, between 2 and 10 kb in size, and contain only a few genes each

ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Introduction to Magnetic Symmetry.
I. Magnetic space groups

J. Manuel Perez-Mato
Facultad de Ciencia y Tecnología
Universidad del País Vasco, UPV-EHU
BILBAO, SPAIN

Comparing Numerical Integration Methods

Alex Clement
Amy Clement
Greg Fenchel
Jeff Fenchel
Jayson Lynch

April 02, 2008

Team 82
NM Supercomputing Challenge

GEOMETRIC INTEGRATION AND ITS APPLICATIONS

C.J. Budd[1] and M.D. Piggott[2]

Abstract

This paper aims to give an introduction to the relatively new field of geometric integration. During the course of looking at a series of examples, ideas and techniques are introduced. Effective numerical methods for challenging problems are identified. These methods aim to preserve certain geometrical structure inherent in the underlying problem such as symplecticity, conservation laws and Lie group symmetries.

KEY WORDS: Numerical methods, qualitative behaviour, Hamiltonian systems, singularity capturing, meteorology, frontogenesis.

1 Introduction

The modern study of natural phenomena described by ordinary or partial differential equations usually requires a significant application of computational effort and to understand the design and operation of computer algorithms numerical analysis is essential. A huge amount of effort, over the past fifty years (and earlier) has thus been applied to the research of numerical methods for differential equations. This research has led to many ingenious algorithms and associated codes for the computation of solutions to such differential equations. Most of these algorithms are based upon the natural technique of discretising the equation in such a way as to keep the local truncation errors associated with the discretisation as small as possible. The resulting discrete systems are then solved with carefully designed linear and nonlinear solvers. When coupled with effective error control strategies these methods can often lead to very accurate solutions of the associated differential equations, provided that the times for integration are not long and the solution remains reasonably smooth.

However, methods based on the analysis of local truncation errors do not necessarily respect, or even take into account, the qualitative and global features of the problem or equation. It can be argued that in some situations these global structures tell us more about the underlying problem than the local information given by the expression of the problem in terms of differentials. The recent growth of geometric integration has, in contrast, led to the development of numerical methods which systematically incorporate

[1]Dept. of Mathematical Sciences, University of Bath, Claverton Down, Bath, BA2 7AY, UK. cjb@maths.bath.ac.uk

[2]Dept. of Mathematical Sciences, University of Bath, Claverton Down, Bath, BA2 7AY, UK. masmdp@maths.bath.ac.uk

HYPERBOLIC PROGRAMS, AND THEIR DERIVATIVE RELAXATIONS

JAMES RENEGAR

Abstract. We study the algebraic and facial structures of hyperbolic programs, and examine natural relaxations of hyperbolic programs, the relaxations themselves being hyperbolic programs.

1. Introduction

Hyperbolic programming was introduced by Güler [6] in the context of interior-point methods. His inspiration drew partly from work arising in the study of hyperbolic pde's; in particular, from work of Gårding [5].

The richness of hyperbolic programming was further explored by Bauschke, Güler, Lewis and Sendov [1]. They initiated an intriguing theory in the vein of general convex analysis.

We continue the exploration of hyperbolic programming, influenced greatly by the above works. The present paper lays out some of the basic structure of hyperbolic programs.

For coherence, we reprove some results found in the above papers. Perhaps noteworthy in this regard is that we reprove Gårding's key results, with arguments that while entirely inspired by his proofs, are considerably briefer.

2. Fundamentals

Let $\mathcal{E}$ denote a finite-dimensional Euclidean space.

> A homogeneous polynomial $p : \mathcal{E} \to \mathbb{R}$ is said to be *hyperbolic* if there exists a direction $e \in \mathcal{E}$, $p(e) \neq 0$, with the property that for each $x \in \mathcal{E}$, the univariate polynomial $t \mapsto p(x + te)$ has only real roots (i.e., each root has no imaginary part). The polynomial is said to be hyperbolic *in direction* e.

1991 *Mathematics Subject Classification.* 90C05, 90C22, 90C25, 52A41, 52B15.

Key words and phrases. hyperbolicity cone, hyperbolic polynomial, conic programming, convex optimization.

The pdf file is hyperlinked.

I especially wish to thank Chek Beng Chua for illuminating discussions during the formative stages of this work.

Research supported by NSF Grant #CCR-9901941.

Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space

Hamza Abusalah[1], Joël Alwen[1], Bram Cohen[2], Danylo Khilko[3], Krzysztof Pietrzak[1], and Leonid Reyzin[4]

[1] Institute of Science and Technology Austria, habusalah|jalwen|pietrzak@ist.ac.at
[2] Chia Network, bram@chia.network
[3] ENS Paris, dkhilko@ukr.net
[4] Boston University, reyzin@cs.bu.edu

Abstract. Proofs of space (PoS) were suggested as more ecological and economical alternative to proofs of work, which are currently used in blockchain designs like Bitcoin. The existing PoS are based on rather sophisticated graph pebbling lower bounds. Much simpler and in several aspects more efficient schemes based on inverting random functions have been suggested, but they don't give meaningful security guarantees due to existing time-memory trade-offs.

In particular, Hellman showed that any *permutation* over a domain of size N can be inverted in time T by an algorithm that is given S bits of auxiliary information whenever $S \cdot T \approx N$ (e.g. $S = T \approx N^{1/2}$). For *functions* Hellman gives a weaker attack with $S^2 \cdot T \approx N^2$ (e.g., $S = T \approx N^{2/3}$). To prove lower bounds, one considers an adversary who has access to an oracle $f : [N] \to [N]$ and can make T oracle queries. The best known lower bound is $S \cdot T \in \Omega(N)$ and holds for random functions and permutations.

We construct functions that provably require more time and/or space to invert. Specifically, for any constant k we construct a function $[N] \to [N]$ that cannot be inverted unless $S^k \cdot T \in \Omega(N^k)$ (in particular, $S = T \approx N^{k/(k+1)}$). Our construction does not contradict Hellman's time-memory trade-off, because it cannot be efficiently evaluated in forward direction. However, its entire function table can be computed in time quasilinear in N, which is sufficient for the PoS application.

Our simplest construction is built from a random function oracle $g : [N] \times [N] \to [N]$ and a random permutation oracle $f : [N] \to [N]$ and is defined as $h(x) = g(x, x')$ where $f(x) = \pi(f(x'))$ with π being any involution without a fixed point, e.g. flipping all the bits. For this function we prove that any adversary who gets S bits of auxiliary information, makes at most T oracle queries, and inverts h on an ϵ fraction of outputs must satisfy $S^2 \cdot T \in \Omega(\epsilon^2 N^2)$.

1 Introduction

A proof of work (PoW), introduced by Dwork and Naor [DN93], is a proof system in which a prover $\mathcal{P}$ convinces a verifier $\mathcal{V}$ that he spent some computation with

Sheaf Semantics for Concurrent Interacting Objects

Joseph A. Goguen*
Dept. of Computer Science & Engineering
University of California at San Diego

Abstract: This paper uses concepts from sheaf theory to explicate phenomena in concurrent systems, including object, inheritance, deadlock, and non-interference, as used in computer security. The approach is very general, and applies not only to concurrent object oriented systems, but also to systems of differential equations, electrical circuits, hardware description languges, and much more. Time can be discrete or continuous, linear or branching, and distribution is allowed over space as well as time. Concepts from category theory help to achieve this generality: objects are modeled by sheaves; inheritance by sheaf morphisms; systems by diagrams; and interconnections by diagrams of diagrams. In addition, behaviour is given by limit, and the result of interconnection by colimit. The approach is illustrated with many examples, including a semantics for a simple concurrent object-based programming language.

1 Introduction

Many popular formalisms for concurrent systems are *syntactic* (or "formal") in the sense that they represent systems by expressions, and then reason about systems by manipulating the corresponding expressions. For example, Milner's CCS [36], Hoare's CSP [30] and Bergstra's ACP [5] provide *process algebras*, which represent systems by expressions in which the primitives for process combination are implicitly defined by sets of equations; a quite different formal approach to concurrency is Girard's linear logic [12].

What we call *semantic*, or *model theoretic*, approaches, provide complete sets of possible behaviours for systems. Such approaches have received less attention than syntactic approaches, but are important as standards against which to test the soundness and completeness of syntactic approaches, and also for defining basic general concepts, such as deadlock and information flow. Moreover, they are closer to our physical intuition, can often describe examples in simple and natural ways, and integrate easily with such additional considerations as data structure, objects and constraints. Trace models, as used in CSP [30] and other process algebras, are a prototypical example. From this point of view, Petri nets [40], (labelled) transition systems [45], and synchronisation trees [36] can also be seen as syntactic.

Actually, things are not quite so simple, because the approaches that we have lumped together as "syntactic" really have varying degrees of semantics. For example, transition systems and synchronisation trees have been used as semantics for CCS and CSP; also, CSP has a "preferred" model, based on failures and refusals [30]. Petri nets have been used as models for linear logic (e.g., [35]), and set theoretic models have been given for Hewitt's actor approach [1]. Moreover, CCS expressions have been used as models for temporal logic. One person's syntax is another person's semantics.

*Thanks also to the Programming Research Group, Oxford University. The research reported in this paper has been supported in part by grants from the Science and Engineering Research Council, and the Fujitsu Corporation.

Related Randomness Attacks for Public Key Encryption

Kenneth G. Paterson, Jacob C. N. Schuldt, Dale L. Sibborn

Information Security Group, Royal Holloway, University of London

March 2014

arXiv:math/9201275v1 [math.DS] 26 Sep 1990

Julia sets and complex singularities in hierarchical Ising models

P. M. Bleher
School of Mathematical Studies
Tel-Aviv University
69978 Israel

M. Yu. Lyubich
Institute for Mathematical Sciences
SUNY, Stony Brook,
N.Y. 11794, USA

March 4,1990

Abstract

We study the analytical continuation in the complex plane of free energy of the Ising model on diamond-like hierarchical lattices. It is known [12, 13] that the singularities of free energy of this model lie on the Julia set of some rational endomorphism f related to the action of the Migdal- Kadanoff renorm-group. We study the asymptotics of free energy when temperature goes along hyperbolic geodesics to the boundary of an attractive basin of f. We prove that for almost all (with respect to the harmonic measure) geodesics the complex critical exponent is common, and compute it.

1 Introduction

The purpose of this article is to analyse complex singularities in temperature of the free energy $\mathcal{F}$ in the Ising model on diamond–like hierarchical lattices. According to the traditional point of view a phase transition manifests itself as a singularity of $\mathcal{F}$ as a function of thermodynamic parameters (like temperature and external magnetic field). From this point of view the theory of phase transitions should describe the domain of analyticity of $\mathcal{F}$ and the type of its singularities at points of phase transition (see [1], where diverse approaches to the first of these problems are discussed).

FSU-SCRI-93-77 June, 1993

Quantum Mechanics as Complex Probability Theory

Saul Youssef

Supercomputer Computations Research Institute
Florida State University
Tallahassee, Florida 32306–4052
youssef@scri.fsu.edu

Abstract

Realistic quantum mechanics based on complex probability theory is shown to have a frequency interpretation, to coexist with Bell's theorem, to be linear, to include wavefunctions which are expansions in eigenfunctions of Hermitian operators and to describe both pure and mixed systems. Illustrative examples are given. The quantum version of Bayesian inference is discussed.

FSU-SCRI-94-53 June, 1994

Is Complex Probability Theory Consistent with Bell's Theorem?

Saul Youssef

Supercomputer Computations Research Institute
Florida State University
Tallahassee, Florida 32306–4052
yousef@scri.fsu.edu

hep-th/9406184 15 Sep 1995

Abstract

Bayesian complex probability theory is shown to be consistent with Bell's theorem and with other recent limitations on local realistic theories which agree with the predictions of quantum mechanics.

arXiv:quant-ph/9503024v2 31 Mar 1995

Quantum Mechanics as a Classical Theory IV: The Negative Mass Conjecture

L. S. F. Olavo
Departamento de Fisica - Universidade de Brasilia - UnB
70910-900 - Brasilia - D.F.- Brazil

February 1, 2008

Abstract

The following two papers form a natural development of a previous series of three articles on the foundations of quantum mechanics; they are intended to take the theory there developed to its utmost logical and epistemological consequences. We show in the first paper that relativistic quantum mechanics might accommodate without ambiguities the notion of negative masses. To achieve this, we rewrite all of its formalism for integer and half integer spin particles and present the world revealed by this conjecture. We also base the theory on the second order Kleïn-Gordon's and Dirac's equations and show that they can be stated with only positive definite energies. In the second paper we show that the general relativistic quantum mechanics derived in paper II of this series supports this conjecture.

1 General Introduction

What is the job of a theoretical physicist? The first answer that comes to us in a somewhat precipitate manner is: The theoretical physicist's job is to say how the world is. Despite the obvious philosophical fragility of such an assertion, hardly adjustable with the method of systematic doubt of science, this answer gives us a key for a more adequate approach. The theoretical physicist has not the mission of saying how the world is but, rather, the job to explain how the world might be. Only the experiments have the final word about, among all the numerous possible worlds furnished by a theory, which one is more adequate. The history of science of the last four centuries has shown that we shall not underestimate any of the models we uncover with our interpretations of the underlying formal apparatus.

This is the spirit underlying the first paper of this series. In this paper, we will show that relativistic quantum mechanics admits an interpretation very

PostScript processed by the SLAC/DESY Libraries on 24 Apr 1995.

HEP-TH-9504118

Discrete Mathematics and Physics on the Planck-Scale

Manfred Requardt

Institut für Theoretische Physik
Universität Göttingen
Bunsenstrasse 9
37073 Göttingen Germany

Abstract

Starting from the hypothesis that both physics, in particular space-time and the physical vacuum, and the corresponding mathematics are discrete on the Planck scale we develop a certain framework in form of a '*cellular network*' consisting of cells interacting with each other via bonds. Both the internal states of the cells and the "strength" of the bonds are assumed to be dynamical variables. In section 3 the basis is laid for a version of '*discrete analysis*' which, starting from different, perhaps more physically oriented principles, manages to make contact with the much more abstract machinery of Connes et al. and may complement the latter approach. In section 4 a, as far as we can see, new concept of '*topological dimension*' in form of a '*degree of connectivity*' for graphs, networks and the like is developed. It is then indicated how this '*dimension*', which for continuous structures or lattices being embedded in a continuous background agrees with the usual notion of dimension, may change dynamically as a result of a '*phase transition like*' change in '*connectivity*' in the network. A certain speculative argument, along the lines of statistical mechanics, is supplied in favor of the naturalness of dimension 4 of ordinary (classical) space-time.

arXiv:cond-mat/9508115v2 26 Aug 1995

Numerical Study of a Lyapunov functional for the Complex Ginzburg-Landau Equation

R. Montagne *, E. Hernández-García, and M. San Miguel
Departament de Física, Universitat de les Illes Balears,
and Institut Mediterrani d'Estudis Avançats, IMEDEA (CSIC-UIB)
E-07071 Palma de Mallorca (Spain)
(February 1, 2008)

Abstract

We numerically study in the one-dimensional case the validity of the functional calculated by Graham and coworkers (R. Graham and T. Tel, Phys. Rev. A **42**, 4661 (1990), O. Descalzi and R. Graham, Z. Phys. B **93**, 509 (1994)) as a Lyapunov potential for the Complex Ginzburg-Landau equation. In non-chaotic regions of parameter space the functional decreases monotonically in time towards the plane wave attractors, as expected for a Lyapunov functional, provided that no phase singularities are encountered. In the phase turbulence region the potential relaxes towards a value characteristic of the phase turbulent attractor, and the dynamics there approximately preserves a constant value. There are however very small but systematic deviations from the theoretical predictions, that increase when going deeper in the phase turbulence region. In more disordered chaotic regimes characterized by the presence of phase singularities the functional is ill-defined and then not a correct Lyapunov potential.

Keywords: Complex Ginzburg-Landau Equation, Nonequilibrium Potential, Lyapunov Potential, Spatio-Temporal Chaos
PACS: 05.45.+b,05.70.Ln

Typeset using REVTEX

*on leave from Universidad de la República (Uruguay).

arXiv:hep-ph/9508323v1 18 Aug 1995

hep-ph/9508323
DPNU-95-20

Confinement and complex singularities in QED3

P. Maris*
Department of Physics, Nagoya University, Nagoya 464-01, Japan
(June 1995)

Abstract

The standard approximations of the Dyson–Schwinger equation lead to complex singularities of the fermion propagator. In three-dimensional QED one can show that this phenomenon might be related to confinement: a confining potential leads to mass-like singularities at complex momenta, and thus to the absence of a mass singularity on the real timelike axis. The correct treatment of the vacuum polarization is essential for the confining nature of QED3.

11.10.Kk,11.15.Pg,11.15.Tk,11.55.Bq

Typeset using REVTEX

arXiv:quant-ph/9509004v1 11 Sep 1995

QUANTUM MECHANICS AS AN EXOTIC PROBABILITY THEORY

SAUL YOUSSEF
Supercomputer Computations Research Institute
Florida State University
Tallahassee, FL 32306-4052
youssef@scri.fsu.edu[1]

Abstract. Recent results suggest that quantum mechanical phenomena may be interpreted as a failure of standard probability theory and may be described by a Bayesian complex probability theory.

Key words: Quantum Mechanics, Bayesian, Complex Probability Theory

There is more to probability theory than proving theorems in a particular mathematical system. One is also in a position to make predictions about real physical systems by adding extra assumptions to the standard axioms. Such predictions are necessarily subject to experimental test, and, to the extent that one believes in the extra assumptions, such tests may be interpreted as testing the correctness of probability theory itself. Now this may already seem like an odd point of view, especially here, since this conference series itself provides a most impressive record of success for probability theory in a vast array of situations with no indication of a problem – so why is there any reason to doubt probability theory? Here I think that there is a historical effect: probability theory may actually be failing all the time, it's just that the situations where a failure occurs are called "quantum mechanical phenomena" and thus appear in physics conferences instead of in probability theory conferences. This suggests that perhaps there is something wrong with probability theory after all, and that this may be where quantum mechanical effects come from. Let's adopt this point of view and see where it leads [1, 2, 3].

[1]Presented at the Workshop on Maximum Entropy and Bayesian Methods, St.John's College, Santa Fe, New Mexico, August, 1995.

arXiv:gr-qc/9602046v2 23 Aug 1996

Quantum Theory of Geometry I: Area Operators*

Abhay Ashtekar[1†] and Jerzy Lewandowski[2,3‡]
[1]*Center for Gravitational Physics and Geometry*
Physics Department, Penn State, University Park, PA 16802, USA
[2]*Institute of Theoretical Physics,*
Warsaw University, ul Hoza 69, 00-681 Warsaw, Poland
[3]*Max Planck Institut für Gravitationphysik,*
Schlaatzweg 1, 14473 Potsdam, Germany

Abstract

A new functional calculus, developed recently for a fully non-perturbative treatment of quantum gravity, is used to begin a systematic construction of a quantum theory of geometry. Regulated operators corresponding to areas of 2-surfaces are introduced and shown to be self-adjoint on the underlying (kinematical) Hilbert space of states. It is shown that their spectra are *purely* discrete indicating that the underlying quantum geometry is far from what the continuum picture might suggest. Indeed, the fundamental excitations of quantum geometry are 1-dimensional, rather like polymers, and the 3-dimensional continuum geometry emerges only on coarse graining. The full Hilbert space admits an orthonormal decomposition into finite dimensional sub-spaces which can be interpreted as the spaces of states of spin systems. Using this property, the complete spectrum of the area operators is evaluated. The general framework constructed here will be used in a subsequent paper to discuss 3-dimensional geometric operators, e.g., the ones corresponding to volumes of regions.

---

*It is a pleasure to dedicate this article to Professor Andrzej Trautman, who was one of the first to recognize the deep relation between geometry and the physics of gauge fields[1,2] which lies at the heart of this investigation.

†Electronic address: ashtekar@phys.psu.edu

‡Electronic address: jerzy.lewandowski@fuw.edu.pl

arXiv:cond-mat/9707012v2 [cond-mat.stat-mech] 17 Dec 1998

Discrete scale invariance and complex dimensions

Didier Sornette[1,2]
[1] Laboratoire de Physique de la Matière Condensée
CNRS and Université de Nice-Sophia Antipolis, Parc Valrose, 06108 Nice, France
[2] Department of Earth and Space Sciences and
Institute of Geophysics and Planetary Physics
University of California, Los Angeles, California 90095-1567

Updated version (Oct. 27, 1998) of the review paper with the same title appeared in Physics Reports 297, 239-270 (1998)

Abstract: We discuss the concept of discrete scale invariance and how it leads to complex critical exponents (or dimensions), i.e. to the log-periodic corrections to scaling. After their initial suggestion as formal solutions of renormalization group equations in the seventies, complex exponents have been studied in the eighties in relation to various problems of physics embedded in hierarchical systems. Only recently has it been realized that discrete scale invariance and its associated complex exponents may appear "spontaneously" in euclidean systems, i.e. without the need for a pre-existing hierarchy. Examples are diffusion-limited-aggregation clusters, rupture in heterogeneous systems, earthquakes, animals (a generalization of percolation) among many other systems. We review the known mechanisms for the spontaneous generation of discrete scale invariance and provide an extensive list of situations where complex exponents have been found. This is done in order to provide a basis for a better fundamental understanding of discrete scale invariance. The main motivation to study discrete scale invariance and its signatures is that it provides new insights in the underlying mechanisms of scale invariance. It may also be very interesting for prediction purposes.

Stable 3-level leapfrog integration in numerical relativity

Kimberly C. B. New
Department of Physics & Atmospheric Science, Drexel University, Philadelphia 19104

Keith Watt
Department of Astronomy, University of Maryland, College Park 20742-2421

Charles W. Misner
Department of Physics, University of Maryland, College Park 20742-4111

Joan M. Centrella
Department of Physics & Atmospheric Science, Drexel University, Philadelphia 19104
(*Physical Review D*, in press)

The 3-level leapfrog time integration algorithm is an attractive choice for numerical relativity simulations since it is time-symmetric and avoids non-physical damping. In Newtonian problems without velocity dependent forces, this method enjoys the advantage of long term stability. However, for more general differential equations, whether ordinary or partial, delayed onset numerical instabilities can arise and destroy the solution. A known cure for such instabilities appears to have been overlooked in many application areas. We give an improved cure ("deloused leapfrog") that both reduces memory demands (important for $3+1$ dimensional wave equations) and allows for the use of adaptive timesteps without a loss in accuracy. We show both that the instability arises and that the cure we propose works in highly relativistic problems such as tightly bound geodesics, spatially homogeneous spacetimes, and strong gravitational waves. In the gravitational wave test case (polarized waves in a Gowdy spacetime) the deloused leapfrog method was five to eight times less CPU costly at various accuracies than the implicit Crank-Nicholson method, which is not subject to this instability.

04.25.Dm, 04.30.Nk, 95.30.Sf

I. INTRODUCTION

Numerical relativity comprises the dynamical solution of the Einstein equations on a computer, allowing the construction of spacetimes that cannot be studied by purely analytic methods. A major application of numerical relativity is the modeling of astrophysical sources of gravitational radiation such as binary black hole [1] or neutron star inspiral [2], and nonspherical stellar collapse [3]. The continued development of gravitational wave detectors, with the expectation that ground-based interferometers such as LIGO [4], VIRGO [5] and GEO600 [6] will begin taking data in a few years, gives these studies a high priority. Numerical relativity is also important for studying the dynamics of pure gravitational waves [7], inhomogeneous cosmologies [8], the behavior of cosmological singularities [9,10], and critical behavior in general relativity [11].

All of these endeavors require accurate numerical algorithms to correctly model the physics of curved spacetime. Simulations in three spatial dimensions plus time are expensive in terms of both CPU usage and memory requirements, and thus demand numerical methods that are efficient in both these regards. Memory limits, however, are less elastic in the short term than CPU time constraints. Thus a three-level second order algorithm may be more appropriate than a faster, high order algorithm which can only be implemented on smaller problems. Also, modeling the inspiral of binary black holes or neutron stars requires evolving the system for many orbital periods, so that numerical algorithms with long term stability and freedom from unphysical damping are essential.

Leapfrog methods are often used for the time integration of equations in numerical relativity and other branches of computational physics. The 3-level leapfrog method has the important property of being symplectic. In the context of a Hamiltonian system for which the differential equation has a symplectic structure (conjugate pairing of coordinates and momenta), this means that the difference equations also have such a structure and the integration step in the difference equations is a canonical transformation. With a symplectic integrator, all the Lagrangian integral invariants, including phase space volume, are exactly conserved by the integration scheme. Since the leapfrog method is time symmetric and maintains good conservation of physically conserved quantities [12–14], it has a well-deserved reputation in the context of Newtonian mechanics. Unfortunately this reputation is generally not merited when velocity dependent forces are met. In the integration of systems with such forces, this scheme is well-known to be susceptible to numerical instability (e.g., [15–19], and references therein), even under conditions where local linearization analysis anticipates stability. This instability occurs in the integration of both ordinary and partial differential equations and, in the case of partial differential equations, is independent of the mesh size used for the spatial

arXiv:cs/9809019v1 [cs.DC] 14 Sep 1998

Distributed Computation as Hierarchy

Michael Manthey
Computer Science Department, Aalborg University
Fr. Bajersvej 7E; 9200 Aalborg, Denmark
manthey@cs.auc.dk
©February 1, 2008.

Abstract. This paper presents a new distributed computational model of distributed systems called the *phase web* that extends Vaughn Pratt's orthocurrence relation from 1986. The model uses mutual-exclusion to express sequence, and a new kind of hierarchy to replace event sequences, posets, and pomsets. The model explicitly connects computation to a discrete Clifford algebra that is in turn extended into homology and co-homology, wherein the recursive nature of objects and boundaries becomes apparent and itself subject to hierarchical recursion. *Topsy*, a programming environment embodying the phase web, is currently being readied for release.

Keywords: process, hierarchy, distributed, co-occurrence, co-exclusion, orthocurrence, Clifford algebra, homology, co-homology, twisted isomorphism, phase web paradigm, Phase Web, Topsy, reductionism, emergence, Kron.

Introduction

The intent of this paper is to introduce a new model of distributed computation, and presumes that the reader is familiar with extant models (CCS, pomsets, and the like) so as to concentrate on what is new about the present approach. The model arose in the author's search for a way to describe and specify a particular class of distributed computations, namely self-organizing systems, although it is applicable to less demanding applications as well. Prominent characteristics of self-organizing systems are (1) they are not intended to 'halt', (2) they are meaningless when separated from their environment, with which they constantly interact, (3) they must be self-reflective, and thus (4) they are, in a non-teleological sense, goal-driven. [Man97] enlarges on these themes.

In contrast to many, the approach presented here emphasizes *structure* so strongly that the algorithmic component that for most people is the sine qua non of computation is nearly invisible. This emphasis is ultimately the reason why the approach offered here - called *the phase web paradigm* - differs from all others we are familiar with, and correspondingly, why its mathematics comes out so differently (algebraic topology, namely, rather than logic).

Of course one still writes programs, but in pure process-coordination terms; we use a local extension to Linda [Gel85] called TLinda [Note 0]. However, since a self-organizing system generally grows/learns, this programming is ultimately sculptural rather than specificational in character. This sculpturing is a reflection of the hierarchical aspect of the phase web.

As will become apparent, this work adopts algebraic topology as its overall mathematical framework. The first to do this were Herlihy and Shavit [HS93], who model decision tasks via simplicial complexes, and then use homology theory to capture state change. We use only the former, and, unlike these authors, in a way that is quite independent of the application. Nevertheless, we are very much in agreement with Herlihy and Rajsbaum when they write [HR95]

arXiv:cs/9809125v1 [cs.DC] 14 Sep 1998

Distributed Computation, the Twisted Isomorphism, and Auto-Poiesis

Michael Manthey
Computer Science Department
Aalborg University
Fr. Bajersvej 7E
9200 Aalborg, Denmark
manthey@cs.auc.dk

Abstract [1]

This paper presents a synchronization-based, multi-process computational model of anticipatory systems called the Phase Web. It describes a self-organizing paradigm that explicitly recognizes and exploits the existence of a boundary between inside and outside, accepts and exploits intentionality, and uses explicit self-reference to describe eg. auto-poiesis. The model explicitly connects computation to a discrete Clifford algebraic formalization that is in turn extended into homology and co-homology, wherein the recursive nature of objects and boundaries becomes apparent and itself subject to hierarchical recursion. *Topsy*, a computer program embodying the Phase Web, is currently being readied for release.

Keywords. Process, hierarchy, co-exclusion, co-occurrence, synchronization, system, auto-poiesis, conservation, invariant, anticipatory, homology, co-homology, twisted isomorphism, phase web paradigm, Topsy, reductionism, emergence.

Introduction

Anticipatory systems (Rosen, 1985) display a number of properties that, together, differentiate them strongly from other kinds of systems:

- They possess *parts* that interact *locally* to form a coherently behaving *whole*.
- The way in which these parts interact differ widely from system to system in detail, yet wholes with very different parts seem nevertheless to resemble each other *qua* their very wholeness.
- It is impossible to ignore the fact that such systems are *situated* in a surrounding environment. Indeed, their interaction with their environment is so integral to what they are and do makes their very situatedness a defining characteristic.
- A critical behavior shared by these wholes is the ability to *anticipate* changes in their surrounding environment and react in a way that (hopefully) ensures their continuing existence, ie. *auto-poiesis*.

Attempting to get a handle on anticipatory systems *computationally* can mean different things to different people.

[1] Invited paper, CASYS'97 First International Conference on Computing Anticipatory Systems, Liege (Belgium), August 11-15, 1997. D. Dubois, Ed. ©February 1, 2008.

TruSpy: Cache Side-Channel Information Leakage from the Secure World on ARM Devices

Ning Zhang*, Kun Sun†, Deborah Shands‡ Wenjing Lou*‡, Y. Thomas Hou*
*Virginia Polytechnic Institute and State University, VA
{ningzh, wjlou, thou}@vt.edu
†George Mason University, Fairfax, VA
{ksun3}@gmu.edu
‡National Science Foundation, Arlington, VA
{deborah.shands}@gmail.com

Abstract—**As smart, embedded devices are increasingly integrated into our daily life, the security of these devices has become a major concern. The ARM processor family, which powers more than 60% of embedded devices, introduced TrustZone technology to offer security protection via an isolated execution environment called secure world. Caches in TrustZone-enabled processors are extended with a *non-secure (NS)* bit to indicate whether a cache line is used by the secure world or the normal world. This cache design improves system performance by eliminating the need to perform cache flush during world switches; however, it also enables cache contention between the two worlds.**

In this work, we present TruSpy, the first study of timing-based cache side-channel information leakage of TrustZone. Our proposed attack exploits the cache contention between normal world and secure world to recover secret information from secure world. Two attacks are proposed in TruSpy, namely, the normal world OS attack and the normal world Android app attack. In the OS-based attack, the attacker is able to access virtual-to-physical address translation and high precision timers. In the Android app-based attack, these tools are unavailable to the attacker, so we devise a novel method that uses the expected channel statistics to allocate memory for cache probing. We also show how an attacker might use the less accurate performance event interface as a timer.

Using the T-table based AES implementation in OpenSSL 1.0.1f as an example, we demonstrate that it is possible for a normal world attacker to steal a fine-grained secret from the secure world using a timing-based cache side-channel. We can recover the full AES encryption key via either the OS-based attack or the Android app-based attack. Since our zero permission TruSpy attack is based on the cache design in TrustZone enabled ARM processors, it poses a significant threat to a wide array of devices. To mitigate the newly discovered threat, we also propose both application-based and system-oriented countermeasures.

1. Introduction

With the continuous growth in network capabilities, more and more embedded devices are connected. Having a smart home is no longer a story from science fiction movies [1]. On the other hand, the sheer volume of cyber attacks nowadays has been unsettling. Security is now one of the major concerns in adopting these smart technologies [2].

ARM family processors have been deployed in more than 60% of the embedded devices [3]. To enhance the security of mobile systems, ARM introduced a security extension called *TrustZone* [4], which offers the ability to protect security sensitive tasks within an isolated execution environment. TrustZone has been adopted in a wide variety of commercial products [5], [6] and academic projects [7], [8], [9], [10] to enable secure processing. The protected environment is called *secure world*, and the normal environment is called *normal world* or *nonsecure world*. In order to provide isolation of resources between the two worlds, hardware components in TrustZone-enabled platforms are augmented with an additional *NonSecure (NS)* flag bit to indicate the security domain.

Processor cache is one of the basic components in modern memory architecture to bridge the gap between the fast processor operation and relatively slower memory access. To support memory isolation in the TrustZone architecture, both instruction and data cache lines are extended with the *NS* flag bit [4] to mark the security domain of these lines. Even though the secure cache lines are not accessible by the normal world, both worlds are equal when competing for the use of cache lines. In other words, when the processor is running in one world, it can evict the cache lines used by the other world due to cache contention. The goal of this cache design is to improve the system performance by maximizing the usable cache space and eliminating the need for cache flush during a world switch. We observe that though the contents of processor cache are protected by the hardware extension, the access pattern to these cache lines is not protected, leaving TrustZone vulnerable to cache side-channel attacks.

arXiv:quant-ph/9908043v3 14 Feb 2000

Ultimate physical limits to computation

Seth Lloyd
d'Arbeloff Laboratory for Information Systems and Technology
MIT Department of Mechanical Engineering
MIT 3-160, Cambridge, Mass. 02139
slloyd@mit.edu

Computers are physical systems: what they can and cannot do is dictated by the laws of physics[1–86]. In particular, the speed with which a physical device can process information is limited by its energy[11–26] and the amount of information that it can process is limited by the number of degrees of freedom it possesses[5–40]. This paper explores the physical limits of computation as determined by the speed of light c, the quantum scale $\hbar$ and the gravitational constant G. As an example, quantitative bounds are put to the computational power of an 'ultimate laptop' with a mass of one kilogram confined to a volume of one liter.

Over the past half century, the amount of information that computers are capable of processing and the rate at which they process it has doubled every two years, a phenomenon known as Moore's law. A variety of technologies — most recently, integrated circuits — have enabled this exponential increase in information processing power. There is no particular reason why Moore's law should continue to hold: it is a law of human ingenuity, not of nature. At some point, Moore's law will break down. The question is, When? Extrapolation of current exponential improvements over two more decades would result in computers that process information at the scale of individual atoms. Although an Avogadro scale computer that can act on 10^{23} bits might seem implausible, prototype quantum computers that store and process information on individual atoms have already been demonstrated[64–65,76–80]. Although existing quantum computers are small and simple, able to perform a few hundred operations on fewer than ten quantum bits or 'qubits,' the fact that they work at all indicates that there is nothing in the laws of physics that forbids the construction of an Avogadro-scale computer.

IASSNS-HEP-99/74
hep-th/9908142

arXiv:hep-th/9908142v3 30 Nov 1999

String Theory and Noncommutative Geometry

Nathan Seiberg and Edward Witten

School of Natural Sciences
Institute for Advanced Study
Olden Lane, Princeton, NJ 08540

We extend earlier ideas about the appearance of noncommutative geometry in string theory with a nonzero B-field. We identify a limit in which the entire string dynamics is described by a minimally coupled (supersymmetric) gauge theory on a noncommutative space, and discuss the corrections away from this limit. Our analysis leads us to an equivalence between ordinary gauge fields and noncommutative gauge fields, which is realized by a change of variables that can be described explicitly. This change of variables is checked by comparing the ordinary Dirac-Born-Infeld theory with its noncommutative counterpart. We obtain a new perspective on noncommutative gauge theory on a torus, its T-duality, and Morita equivalence. We also discuss the $D0/D4$ system, the relation to M-theory in DLCQ, and a possible noncommutative version of the six-dimensional $(2,0)$ theory.

8/99

International Journal of Engineering Research and General Science Volume 4, Issue 3, May-June, 2016
ISSN 2091-2730

INSTALLATION & CONFIGURATION – SSO

Parul Garg[#1], Dr. Yashpal Singh[*2]

[#1]Research Scholar [#2]Associate Professor

[#1]Research Scholar Department of Computer Science & Engineering,Ganga Institute of Technology and Management,Kabolana,Jhajjar,Haryana,

[#2]Department of Computer Science & Engineering,Ganga Institute of Technology and Management,Kabalana,Jhajjar,Haryana,

MDU university, parulgarg22@gmail.com, 9999405236

Abstract— This paper is a case study on a project to provide the installation and configuration to Single Sign On (**SSO**) solution to web based **application**s that use the mainframe as the data store.

It is a session/user **authentication** process that permits a user to enter one name and **password** in order to access multiple **application**s. Conversely it is the property whereby a single action of signing out may terminates access to multiple software systems.

This paper begins with a thorough description of the high level business requirements project to provide the installation and configuration to Single Sign On (**SSO**) solution to web based **application**s that use the mainframe as the data store.

Keywords— **SSO**, **password**, **authentication**, **replication**, **application**, **installer**, **Admin**

INTRODUCTION

Single sign-on (**SSO**) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again (enter Id and **password**) thus this may consume less time.[1] "Single sign-on (**SSO**) is a session/user **authentication** process that permits a user to enter one name and **password** in order to access multiple **application**s. The process authenticates the user for all the **application**s they have been given rights to and eliminates further prompts when they switch **application**s during a particular session."[2]

Single Sign-On (**SSO**) is a key feature of the Enterprise Portal that eases user interaction with the many component systems available to the user in a portal environment. Once the user is authenticated to the enterprise portal, he/she can use the portal, to access external **application**s. With **SSO** in the Enterprise Portal, the user can access different systems and **application**s without having to repeatedly enter his or her user information for **authentication**.

RELATED WORK

- Configuring Single Sign-On using fusion middleware **Admin**istrator's guide for oracle WebCenter. [15]
- Setting up ADFS and enabling Single Sign-On to office 365
- Identity and access management solution
- Identify infrastructure for development
- Protocol and **SSO** client/server architecture [16]

WHY SHOULD WE USE SSO

- A Typical net user needs at least nine **password**s.[3]
- 30% never change **password**s, 29% less than once a year.

Software Engineering Institute

Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework

Linda Parker Gates

November 2010

TECHNICAL REPORT
CMU/SEI-2010-TR-037
ESC-TR-2010-102

Acquisition Support Program
Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu

Carnegie Mellon

Repeating the reasoning in Section 10 we can derive from (11.6)

$$(11.7)\quad \sum_{n\in\mathfrak{A}_1}^{I} a_n(N) \le \sum_{r_2}^{R} Q(R)\exp\Big\{(1+\varepsilon)N^{\frac{1}{2}}\log N\log\log N\Big\} + r_2\Big\{-M_1(1-\varepsilon)+r_1(1+\varepsilon)C_1\Delta^{\frac{1}{2}(1+\varepsilon)}\log^{\frac{1}{2}(1+\varepsilon)}N\Big[1+\theta\Big(\frac{\log\log N}{\log N}\Big)\Big]\Big\}.$$

Now choosing

$$(11.8)\qquad M_1 = r_1 C_1 \Delta^{\frac{1}{2}(1+\varepsilon)}\log^{\frac{1}{2}(1+\varepsilon)}N\,(1+2\varepsilon_1^{-1}+\varepsilon),$$
$$r_1 = \log^{\frac{1}{2}(1+\varepsilon)}N,$$

(11.7) gives

$$\sum_{n\in\mathfrak{A}_1} a_n(N) < Q(R)\exp\{\quad c\Delta^{\frac{1}{2}(1+\varepsilon)}\log^{\frac{1}{2}(1+\varepsilon)}N\},$$

with an unspecified positive c. This completes the proof.

References

[1] P. Erdős and J. Lehner, *The distribution of the number of summands in the partitions of a positive integer*, Duke Math. Journ. 8 (1941), pp. 335–344.

[2] — and P. Turán, *On some problems of a statistical group theory, IV*, Acta Math. Acad. Sci. Hung. 19 (1968), pp. 413–435.

[3] G. H. Hardy and S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) 17 (1918), pp. 75–115.

[4] — — *Asymptotic formulae for the distribution of integers of various types*, Proc. London Math. Soc. (2) 16 (1917), pp. 112–132.

[5] E. A. Trigg-Wright, *A Tauberian theorem for positive sequences*, Ann. of Math. (1941), pp. 1076–1080.

Received on 4. 10. 1969

ACTA ARITHMETICA
XVIII (1971)

On the order function of a transcendental number

by

K. Mahler (Columbus, Ohio)

To the memory of Harald Bohr

Some forty years ago, I introduced the classification of all (real or complex) transcendental numbers into three disjoint classes S, T, and U (see the detailed treatment of this classification and of an equivalent one by J. F. Koksma in Th. Schneider [6], Kapitel III). This classification possessed the *Invariance Property*; i.e., two numbers which are algebraically (dependent over the rational field $\mathbf{Q}$ always belong to the same class.

In the present paper a new classification will be introduced. It associates with every transcendental number ξ a positive valued non-decreasing function $\Omega(x;\xi)$ of an integral variable $x \ge 1$, called the *order function* of ξ. For such order functions, both a partial ordering and an equivalence relation will be defined, and it will be proved that if η and ζ are algebraically dependent over $\mathbf{Q}$, then $\Omega(x;\eta)$ and $\Omega(x;\zeta)$ are equivalent. We may now put any transcendental numbers into one and the same class whenever their order functions are equivalent. In this way we evidently obtain a classification of the transcendental numbers into infinitely many disjoint classes.

The order function $\Omega(x;\xi)$ is defined in terms of the approximation properties of ξ. Unfortunately, the actual determination of $\Omega(x;\xi)$ for a given ξ is a difficult problem, and more work on such order functions is called for.

1. The following notation will be used. We denote by V the set of all polynomials

$$p(x) = p_0 x^{n_0} + p_1 x^{n_1} + \dots + p_s x^{n_s} \quad \text{where} \quad p_0 p_s \ne 0,$$

by W the set of such polynomials with integral coefficients. The exact degree of a polynomial in V is denoted by

$$n_0(p) = n(p) = n_s,$$

and we further put

$$h_0(p) = h(p) = |p_0| + |p_1| + \dots + |p_s|, \quad A_0(p) = A(p) = 2^{n(p)} H(p).$$

ALGEBRAIC INDEPENDENCE OF G-FUNCTIONS AND CONGRUENCES "À LA LUCAS"

by

B. Adamczewski, Jason P. Bell & É. Delaygue

Abstract. — We develop a new method for proving algebraic independence of G-functions. Our approach rests on the following observation: G-functions do not always come with a single linear differential equation, but also sometimes with an infinite family of linear difference equations associated with the Frobenius that are obtained by reduction modulo prime ideals. When these linear difference equations have order one, the coefficients of the corresponding G-functions satisfy congruences reminiscent of a classical theorem of Lucas on binomial coefficients. We use this to derive a Kolchin-like criterion for algebraic independence. We show the relevance of this criterion by proving that many classical families of G-functions turn out to satisfy congruences "à la Lucas".

Contents

1. Introduction 1
2. A first example 6
3. Notation 8
4. Lucas-type congruences and two special sets of power series 9
5. A criterion for algebraic independence 12
6. Algebraic functions in $\mathcal{L}_d(R,\mathcal{S})$ and $\mathfrak{L}_d(R,\mathcal{S})$ 15
7. From asymptotics and singularity analysis to algebraic independence 18
8. Lucas-type congruences among classical families of G-functions 23
9. Algebraic independence of G-functions: a few examples 35
References 40

1. Introduction

This paper is the fourth of a series started by the first two authors [**1, 2, 3**] concerning several number theoretical problems involving linear difference equations, called Mahler's equations, as well as underlying structures associated with automata theory. We investigate here a class of analytic functions introduced by Siegel [**48**] in his landmark 1929 paper under

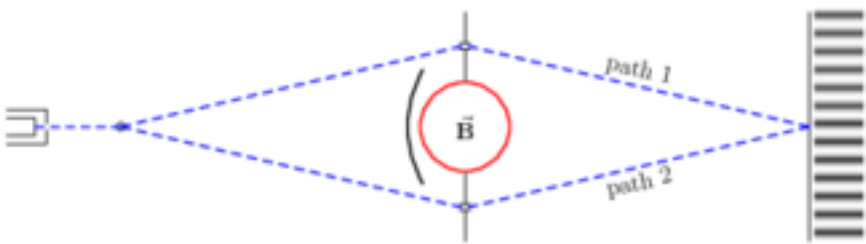
This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 648132.

Aharonov–Bohm Effect and Magnetic Monopoles

Aharonov–Bohm Effect

In classical mechanics, the motion of a charged particle depends only on the electric and magnetic tension fields $\mathbf{E}$ and $\mathbf{B}$; the potentials A^0 and $\mathbf{A}$ do not have any direct effect. Also, the motion depends only on the $\mathbf{E}$ and $\mathbf{B}$ fields along the particle's world-line — the EM fields in some volume of space the particle never goes through do not affect it at all. But *in quantum mechanics, interference between two trajectories a charged particle might take depends on the magnetic field between the trajectories, even if along the trajectories themselves* $\mathbf{B} = 0$. This effect was first predicted by Werner Ehrenberg and Raymond E. Siday in 1949, but their paper was not noticed until the effect was re-discovered theoretically by David Bohm and Yakir Aharonov in 1959 and then confirmed experimentally by R. G. Chambers in 1960.

Consider the following idealized experiment: Take a two-slit electron interference setup, and put a solenoid between the two slits as shown below:



The solenoid is thin, densely wound, and very long, so the magnetic field outside the solenoid is negligible. Inside the solenoid there is a strong $\mathbf{B}$ field, but the electrons do not go there; instead, they fly outside the solenoid along paths 1 and 2. But despite $\mathbf{B} = 0$ along both paths, the magnetic flux Φ inside the solenoid affects the interference pattern between the two paths.

The key to the Aharonov–Bohm effect is the vector potential $\mathbf{A}$. Outside the solenoid $\mathbf{B} = \nabla \times \mathbf{A} = 0$ but $\mathbf{A} \neq 0$ because for any closed loop surrounding the solenoid we have a

Autumn School of the Department of Algebra

Roztoky u Křivoklátu, November 19–22, 2015

ABSTRACTS

Foundations of Physics manuscript No.
(will be inserted by the editor)

Elias Zafiris · Vassilios Karakostas

A Categorial Semantic Representation of Quantum Event Structures

Received: date / Accepted: date

Abstract The overwhelming majority of the attempts in exploring the problems related to quantum logical structures and their interpretation have been based on an underlying set-theoretic syntactic language. We propose a transition in the involved syntactic language to tackle these problems from the set-theoretic to the category-theoretic mode, together with a study of the consequent semantic transition in the logical interpretation of quantum event structures. In the present work, this is realized by representing categorically the global structure of a quantum algebra of events (or propositions) in terms of sheaves of local Boolean frames forming Boolean localization functors. The category of sheaves is a topos providing the possibility of applying the powerful logical classification methodology of topos theory with reference to the quantum world. In particular, we show that the topos-theoretic representation scheme of quantum event algebras by means of Boolean localization functors incorporates an object of truth values, which constitutes the appropriate tool for the definition of quantum truth-value assignments to propositions describing the behavior of quantum systems. Effectively, this scheme induces a revised realist account of truth in the quantum domain of discourse. We also include an appendix, where we compare our topos-theoretic representation scheme of quantum event algebras with other categorial and topos-theoretic approaches.

Keywords Quantum Event Structures · Boolean Algebras · Topos · Subobject Classifier · Kochen-Specker Theorem · Quantum Truth Values · Adjoint Functors · Sheaves · Grothendieck Topos · Realist Account

Elias Zafiris
Department of Mathematics, University of Athens, Athens 157 84, Greece
E-mail: ezafiris@math.uoa.gr

Vassilios Karakostas
Department of Philosophy and History of Science, University of Athens, Athens 157 71, Greece
E-mail: karakost@phs.uoa.gr

Discrete Exterior Calculus Approach to Discretization of Port-Hamiltonian Systems

Marko Seslija

ACE'13 Abstract

Hamiltonian systems are at the foundation of many current physical theories, including quantum and relativistic mechanics, electromagnetism, optics, solid and fluid mechanics. Geometry as the study of observable symmetries and dynamical invariants is *de facto* the *lingua franca* of the Hamiltonian theories. The prevailing paradigm in modeling of the complex large-scale physical systems is network modeling. In many problems arising from modern science and engineering, such as multi-body systems, electrical networks and molecular dynamics, the port-based network modeling is a natural strategy of decomposing the overall system into subsystems, which are interconnected to each other through pairs of variables called ports and whose product is the power exchanged between the subsystems.

The formalism that unifies the geometric Hamiltonian and the port-based network modeling is the *port-Hamiltonian*, which associates with the interconnection structure of the network a geometric structure given by a Poisson, or more generally, a Dirac structure. The generalized Hamiltonian dynamic is then defined with respect to this Poisson, or Dirac, structure by specifying the Hamiltonian representing the total stored energy, the energy-dissipating elements and the ports of the system. Apart from enunciating a remarkable structural unity, Poisson and Dirac geometry offers a mathematical framework that gives important insights into dynamical systems. Moreover, the geometric formalism transcends the finite-dimensional scenario and has been successfully applied to study of a number of distributed-parameter systems, systems described by a set of partial differential equations.

In this talk I plan to address the issue of structure-preserving discretization of open distributed-parameter port-Hamiltonian systems on bounded domains.

Employing the formalism of discrete exterior calculus, I will introduce *simplicial Dirac structures* as discrete analogues of the infinite-dimensional Dirac structures for classical field theories. I will demonstrate how these simplicial Dirac structures provide a natural framework for deriving finite-dimensional port-Hamiltonian systems that emulate the behaviors of their infinite-dimensional counterparts.

I plan to illustrate general considerations on a number of physical examples, including Maxwell's equations on a bounded domain, the telegraph equations, and reaction-diffusion systems, where the structure-preserving discretization recovers the standard compartmental model.

Choice principles in constructive and classical set theories

Michael Rathjen*
Department of Pure Mathematics, University of Leeds
Leeds LS2 9JT, United Kingdom
E-Mail: rathjen@amsta.leeds.ac.uk

Abstract

The objective of this paper is to assay several forms of the axiom of choice that have been deemed constructive. In addition to their deductive relationships, the paper will be concerned with metamathematical properties effected by these choice principles and also with some of their classical models.

1 Introduction

Among the axioms of set theory, the axiom of choice is distinguished by the fact that it is the only one that one finds ever mentioned in workaday mathematics. In the mathematical world of the beginning of the 20th century, discussions about the status of the axiom of choice were important. In 1904 Zermelo proved that every set can be well-ordered by employing the axiom of choice. While Zermelo argued that it was self-evident, it was also criticized as an excessively non-constructive principle by some of the most distinguished analysts of the day. At the end of a note sent to the *Mathematische Annalen* in December 1905, Borel writes about the axiom of choice:

> *It seems to me that the objection against it is also valid for every reasoning where one assumes an arbitrary choice made an uncountable number of times, for such reasoning does not belong in mathematics.* ([10], pp. 1251-1252; translation by H. Jervell, cf. [22], p. 96.)

Borel canvassed opinions of the most prominent French mathematicians of his generation - Hadamard, Baire, and Lebesgue - with the upshot that Hadamard sided with Zermelo whereas Baire and Lebesgue seconded Borel. At first blush Borel's strident reaction against the axiom of choice utilized in Cantor's new theory of sets is surprising as the French analysts had used and continued to use choice principles routinely in their work. However, in the context of 19th century classical analysis

*The research reported in this paper was supported by United Kingdom Engineering and Physical Sciences Research Council Grant GR/R 15856/01.

Acta Universitatis Carolinae. Mathematica et Physica

Miguel A. F. Sanjuán

Chaos & pseudochaos: Some basic remarks

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 33 (1992), No. 2, 129--134

Persistent URL: http://dml.cz/dml.cz/701985

Terms of use:

© Univerzita Karlova v Praze, 1992

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

The Axiom of Choice, the Well Ordering Principle and Zorn's Lemma

Dag Normann *

January 9, 2012

Abstract

In this note we prove the equivalence between the axiom of choice, the well ordering principle and Zorn's lemma, and discuss to some extent how large fragment of *ZF* we need in order to prove the individual implications.

1 Introduction

This note is a suplementary text to the curriculum of MAT4640 Axiomatic Set Theory. The main textbook is Kunen [1]. We assume that the reader is familiar with the basic results on well orderings from Kunen. Nevertheless, the note should be readable for anyone familiar with some naive set theory, as we will state all properties of well orderings that we will use.

We will discuss which axioms from *Zermelo-Fraenkel Set Theory*, *ZF*, we need for the proofs we give. Readers only interested in the equivalence results may ignore this.

We use one joint enumeration of lemmas, theorems, definitions and exercises, and another enumeration of the claims. Claims cannot be read out of the context, as they will be integrated parts of proofs of lemmas or theorems.

2 Preliminaries

We will use the concepts *partial ordering* and *total ordering* in the meaning *of less than*, i.e. they are irreflexive. Following Kunen [1], we let a partial or total ordering be a pair consisting of a set and a binary relation, but the domain of this relation does not need to be a subset of the set. The advantage is that we can talk about *initial segments* without changing the relation, only the set. In one proof this convention will be a disadvantage. This is reflected in our definition of an f-string. All our relations will be binary, i.e. sets of ordered pairs.

*Department of Mathematics, The University of Oslo, P.O. Box 1053, Blindern N-0316 Oslo, Norway, email dnormann@math.uio.no

(*February 23, 2012*)

Essential self-adjointness

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

1. Cautionary example
2. Criterion for essential self-adjointness
3. Examples of essentially self-adjoint operators
4. Appendix: Friedrichs' canonical self-adjoint extensions
5. Appendix: graphs, closures, adjoints
6. Appendix: bibliographic notes

The following has been well understood for 70-120 years, or longer, naturally not in contemporary terminology.

The differential operator $T = \frac{d^2}{dx^2}$ on $L^2[a,b]$ or $L^2(\mathbb{R})$ is a prototypical natural *unbounded operator*. It is undeniably *not continuous* in the L^2 topology: on $L^2[0,1]$ the norm of $f(x) = x^n$ is $1/\sqrt{2n+1}$, and the second derivative of x^n is $n(n-1)x^{n-2}$, so

$$\text{operator norm } \frac{d^2}{dx^2} \text{ on } L^2[0,1] \;\geq\; \sup_{n\geq 1} \frac{n(n-1)\cdot \frac{1}{\sqrt{2n-3}}}{\frac{1}{\sqrt{2n+1}}} \;=\; +\infty$$

That is, $\frac{d^2}{dx^2}$ is not a L^2-bounded operator on *polynomials* on $[0,1]$, so has no bounded *extension*[1] to $L^2[0,1]$.

Nevertheless, the geometric structure of Hilbert spaces is extremely useful, especially the simple duality and adjoint phenomena. This motivates reconsideration of unbounded, not-everywhere-defined, but *densely* defined operators on Hilbert spaces. [2]

Let V be a Hilbert space, with hermitian inner product $(\,,\,)$ and corresponding norm $|\cdot|$. Let T be an *unbounded* linear map $T : D_T \to V$ defined on a *dense* subspace D_T of V. We say that T is on V, even though its domain may be strictly smaller. We are interested in *symmetric* operators, meaning that

$$(Tv, w) \;=\; (v, Tw) \qquad\qquad (\text{for all } v, w \in D_T)$$

For unbounded operators, specification of the *domain* is critical. An operator $T : D_T \to V$ *extends* another operator $S : D_S \to V$ when $D_S \subset D_T$ and T agrees with S on D_S. This partial ordering on unbounded operators on V is written

$$S \;\subset\; T \qquad\qquad (\text{when } D_S \subset D_T \text{ and } T\big|_{D_S} = S)$$

In this notation, in terms of the *adjoint*[3] T^* of T,

$$\begin{cases} T \text{ symmetric} & \iff \quad T \subset T^* \\ T \text{ self-adjoint} & \iff \quad T = T^* \end{cases} \qquad (\text{for densely-defined } T)$$

[1] Whether or not the Axiom of Choice is used to artificially extend $\frac{d^2}{dx^2}$ to $L^2[0,1]$, that extension is not continuous, because the restriction to polynomials is already not continuous. The unboundedness/non-continuity is inescapable.

[2] Alternatively, one might allow more complicated topologies than that of a single Hilbert space, as did Friedrichs, Sobolev, Schwartz, and Grothendieck. In fact, a combination of approaches seems optimal.

[3] For an unbounded operator T, symmetric or not, to have a well-defined *adjoint* T^* requires the domain D_T be *dense*. As discussed in an appendix, the graph of the adjoint T^* is essentially the orthogonal complement of the graph of T. For T symmetric and densely-defined, the domain of T^* is dense.

Archives of Hydro-Engineering and Environmental Mechanics
Vol. 51 (2004), No. 3, pp. 287–303

Implicit versus Explicit Finite Volume Schemes for Extreme, Free Surface Water Flow Modelling

Michał Szydłowski

Gdańsk University of Technology, Faculty of Hydro- and Environmental Engineering,
ul. Narutowicza 11/12, 80-952 Gdańsk, e-mail: mszyd@pg.gda.pl

(Received April 22, 2004; revised July 05, 2004)

Abstract

One explicit and three implicit finite volume method schemes of the Roe type are presented in the paper. The properties and applicability of these methods for modelling unsteady, rapidly varied, open channel flow are investigated. The schemes are used for numerical simulation of one-dimensional extreme flow described by de Saint-Venant equations. The computational results are compared with each other and an analytical (exact) solution to an idealized dam-break problem. The classical versions of general scheme implicit in time – fully implicit and trapezoidal scheme – are not restricted by a stability condition, like an explicit one, however they add some numerical diffusion and dispersion errors to the solution. The modification of parameter Θ, originally proposed for a box scheme of finite difference method, has improved computational properties of the general one-step implicit scheme. This version of finite volume scheme of the Roe type implicit in time can be recommended for modelling and simulation of transient flows in storm sewers and open channel networks.

Key words: general scheme implicit in time, finite volume method, extreme flows

1. Introduction

In recent years considerable effort has been devoted to modelling one- and two-dimensional open channel flows. The free surface one-dimensional, unsteady water flow is governed by the well-known mathematical model called de Saint-Venant equations (Abbott 1979). Quite a number of numerical methods of solving this equations system have been proposed and successfully applied, so far. For the gradually varied flow simulation numerous schemes of finite difference method (FDM) and finite element method (FEM) are widely used (Cunge et al 1980, Szymkiewicz 2000). Unfortunately, the FDM and FEM numerical procedures are often inefficient for modelling rapidly varied, transient flow, when discontinuities such as hydraulic jumps and bores exist.

IOPscience iopscience.iop.org

Limits of temperature separation in a vortex tube

This content has been downloaded from IOPscience. Please scroll down to see the full text.

View the table of contents for this issue, or go to the journal homepage for more

Download details:

IP Address: 132.203.227.62
This content was downloaded on 01/07/2014 at 07:09

Please note that terms and conditions apply.

1994 J. Phys. D: Appl. Phys. 27 480

A Reference Discretization Strategy for the Numerical Solution of Physical Field Problems

CLAUDIO MATTIUSSI*

Campus Strunk-NTRIAD, ARIES Science Park,
Padriciano 99, 34012 Trieste, Italy

I. Introduction . . . 142
II. Preliminaries . . . 147
A. The Mathematical Structure of Physical Field Theories . . . 147
B. Geometric Objects and Operators . . . 150
1. Space–Time Objects . . . 155
C. Physical Laws and Physical Quantities . . . 157
1. Local and Global Quantities . . . 158
2. Equations . . . 159
D. Classification of Physical Quantities . . . 163
1. Space–Time Viewpoint . . . 165
E. Topological Laws . . . 168
F. Constitutive Relations . . . 172
1. Constitutive Equations and Discretization Error . . . 175
G. Boundary Conditions and Sources . . . 176
H. The Scope of the Structural Approach . . . 177
III. Representations . . . 181
A. Geometry . . . 182
1. Cell Complexes . . . 187
2. Primary and Secondary Mesh . . . 186
3. Incidence Numbers . . . 188
4. Chains . . . 189
5. The Geometry of a Chain . . . 191
B. Fields . . . 195
1. Cochains . . . 196
2. Local Systems . . . 197
C. Topological Laws . . . 199
1. The Coboundary Operator . . . 199
2. Properties of the Coboundary Operator . . . 201
3. Discrete Topological Equations . . . 206
D. Constitutive Relations . . . 208
E. Constitutive Representations . . . 207
1. Differential Forms . . . 210
2. Weighted Integrals . . . 211

*Current affiliation: Evolutionary and Adaptive Systems Team, Institute of Robotic Systems (ISR), Department of Micro-Engineering (DMT), Swiss Federal Institute of Technology (EPFL), CH-1015 Lausanne, Switzerland.

ANNALES DE L'I. H. P., SECTION A

M. THIEULLEN
J. C. ZAMBRINI

Probability and quantum symmetries. I. The theorem of Noether in Schrödinger's euclidean quantum mechanics

Annales de l'I. H. P., section A, tome 67, n° 3 (1997), p. 297-338
<http://www.numdam.org/item?id=AIHPA_1997__67_3_297_0>

© Gauthier-Villars, 1997, tous droits réservés.

L'accès aux archives de la revue « Annales de l'I. H. P., section A » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/legal.php). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Quantum algorithms: an overview

Ashley Montanaro*

December 17, 2015

Abstract

Quantum computers are designed to outperform standard computers by running quantum algorithms. Areas in which quantum algorithms can be applied include cryptography, search and optimisation, simulation of quantum systems, and solving large systems of linear equations. Here we briefly survey some known quantum algorithms, with an emphasis on a broad overview of their applications rather than their technical details. We include a discussion of recent developments and near-term applications of quantum algorithms.

1 Introduction

A quantum computer is a machine designed to use quantum mechanics to do things which cannot be done by any machine based only on the laws of classical physics. Eventual applications of quantum computing range from breaking cryptographic systems to the design of new medicines. These applications are based on quantum algorithms – algorithms which run on a quantum computer and achieve a speedup, or other efficiency improvement, over any possible classical algorithm. Although large-scale general-purpose quantum computers do not yet exist, the theory of quantum algorithms has been an active area of study for over 20 years. Here we aim to give a broad overview of quantum algorithmics, focusing on algorithms with clear applications and rigorous performance bounds, and including recent progress in the field.

Contrary to a rather widespread popular belief that quantum computers have few applications, the field of quantum algorithms has developed into an area of study large enough that a brief survey such as this cannot hope to be remotely comprehensive. Indeed, at the time of writing the "Quantum Algorithm Zoo" website cites 278 papers on quantum algorithms [52]. There are now a number of excellent surveys about quantum algorithms [28, 71, 85, 8], and we defer to these for details of the algorithms we cover here, and many more. In particular, we omit all discussion of *how* the quantum algorithms mentioned work. We will also not cover the important topics of how to actually build a quantum computer [59] (in theory or in practice) and quantum error-correction [42], nor quantum communication complexity [23] or quantum Shannon theory [98].

1.1 Measuring quantum speedup

What does it mean to say that a quantum computer solves a problem more quickly than a classical computer? As is typical in computational complexity theory, we will generally consider asymptotic scaling of complexity measures such as runtime or space usage with problem size, rather than

*School of Mathematics, University of Bristol, UK; ashley.montanaro@bristol.ac.uk.

HEAT DIFFUSION, THE STRUCTURE OF SPACE AND THE POINCARÉ CONJECTURE

KLAUS ECKER

1. Introduction

The structure of space and time has always been one of the central themes of scientific investigation. Nowadays, about a century after Einstein formulated his theory of general relativity, some of its fundamental ideas have even become part of general scientific knowledge. This theory proposes that space and time cannot be understood independently of each other, but that instead of a three-dimensional space unchanging in time one should consider a four-dimensional space-time continuum. The masses contained in this space-time (e.g. planets, stars, galaxies, black holes, etc.) influence its structure. Among other things, this means that the three-dimensional space that an observer perceives at any given point in time is curved in itself. Light rays, which always choose the shortest path between two points in space, do not necessarily travel along straight lines, but along the shortest curves as determined by the curvature of space, along *geodesics*. For example, the shortest routes around our curved Earth surface are parts of great circles such as the equator. If the masses are not too great they merely cause a local deformation of space without changing its global shape.

The situation could be quite different for large scales: In cosmology, which concerns itself with the global structure and the time evolution of the whole universe, one starts from the basic assumption that the universe is at every time a closed curved three-dimensional space. One further postulates that this space is homogeneous. This means that its geometry (as, for example, distances and angles) appear the same everywhere. This assumption is reasonable on physical grounds, since when considering large scales one does not expect to discover local irregularities. For example, one cannot detect microscopic inhomogeneities inside a macroscopic material with the naked eye. This theory is still open to the possibility that the geometry of the universe may depend on the direction in which we look. An example is the surface of a cylinder, where at each point there is a "round" and a "straight" direction.

No assumptions are made about the global shape (topology) since it would be very difficult, if not totally impossible, to verify these experimentally. In particular, for example, we may possibly be living on a three-dimensional spherical surface, a positively curved space, or perhaps inside a saddle shaped (negatively curved) space. Our universe might also be a three-dimensional torus, that is, like a three-dimensional version of a ring-shaped surface. If we postulate some minor, physically reasonable additional conditions for our homogeneous spaces, there remain only eight possibilities for their global shape.

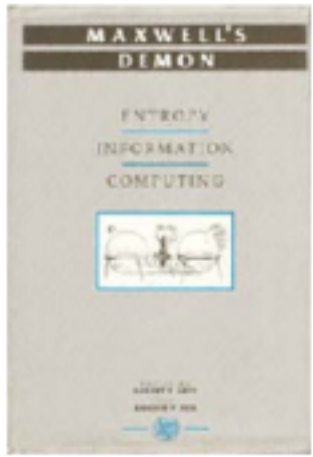
Date: 3 February 2012.

Dissolving the Fermi Paradox

Anders Sandberg, Eric Drexler & Toby Ord

Future of Humanity Institute

University of Oxford



title:	Maxwell's Demon : Entropy, Information, Computing
author:	Leff, Harvey S.; Rex, Andrew F.
publisher:	CRC Press
isbn10 | asin:	0750300566
print isbn13:	9780750300568
ebook isbn13:	9780585347776
language:	English
subject	Maxwell's demon, Thermodynamics.
publication date:	1990
lcc:	QC318.M35.M38 1990eb
ddc:	536.71
subject:	Maxwell's demon, Thermodynamics.

FOR IMMEDIATE RELEASE
August 5, 2017

Internet Party of New Zealand
https://internet.org.nz
@InternetPartyNZ

Authorised by J. Booth, 40 Hartford Crescent, Upper Hutt, Aotearoa 5018, New Zealand.

Internet Party Announces Special Guests for #AntiSpyBill LIVE Event

The Internet Party of New Zealand is pleased to announce some of the special guests attending their #AntiSpyBill live event.

Internet Party Founder Kim Dotcom, award-winning investigative journalist Barrett Brown, hacktivist Lauri Love and stand-up comedian Lee Camp will join the event panel.

Internet Party Leader Suzie Dawson will be MC'ing the event and says: "We are proud to be bringing some of the world's brightest citizen heroes together to once again shine a spotlight on the crimes of the spy agencies against New Zealand citizens and residents, and indeed the world. These luminaries of anti-surveillance activism know well the cold touch of the attentions of the spy agencies and have a wealth of knowledge and personal experience to share with us. We are honoured by their participation."

The Internet Party is inviting the global public to join this world-first live online event to draft citizen-initiated legislation to counter government spying.

The event will be held online between 8pm and 11pm on Sunday the 6th of August, 2017, NZST (UTC+12) and follows on from the Internet Party's 2014 event "The Moment Of Truth" which featured Glenn Greenwald, Edward Snowden and Julian Assange.

Once finalised the draft legislation, dubbed the 2017 #AntiSpyBill, will be submitted to human rights, privacy and political organisations and groups around the world, to lobby for its adoption.

The initiative seeks to counter the damage to democratic and human rights inflicted upon New Zealanders by a string of draconian spying laws passed between 2013 and 2016. These laws have retroactively legalised previously illegal targeting of New Zealanders, including warrantless spying and covertly filming them inside their homes, Orwell-style - a practice referred to in law as "domestic visual surveillance".

Internet Party Leader Suzie Dawson said "New Zealand spies and their international counterparts have engaged in some of the most egregious conduct imaginable. The laws passed under urgency in recent years have only furthered the sense of invulnerability of these spies. They also violate international law. We must show that where our lawmakers fail to do so, the public are willing to step up and address these issues themselves."

There are one hundred first-in-first-served tickets to register for the #AntiSpyBill webinar that grant direct access to panelists.

It is possible to participate in the event without registering, as it will be simulcast live on the official Internet Party Facebook page and You Tube channel.

"The world exploded into a whirling network of kinships, where everything pointed to everything else, everything explained everything else."

—Umberto Eco
Foucault's Pendulum

FORM 2698T

IN THE COURT OF APPEAL, CIVIL DIVISION

REF: A2/2015/3933

Her Majesty's Court of Appeal
- 8 MAR 2016

Mark Anthony Taylor –v– **Anshu Jain (CEO of Deutsche Bank & Ors)**

ORDER made by the Rt. Hon. Lord Justice Burnett

On consideration of the appellant's notice and accompanying documents, but without an oral hearing, in respect of an application for permission to appeal against the decisions of Haddon Cave J of 21 October 2015

Decision: Refused, as being totally without merit and the applicant may not request the decision to be reconsidered at an oral hearing.

Reasons

The applicant believes that he lost money on investments in precious metals as a result of a conspiracy involving many financial institutions. He litigated the matter in Germany and London and then sought to do so again in the Mercantile Court in Birmingham. Judge Simon Brown QC struck out his claim and made an ECRO against him. He sought to set aside the ECRO. That application was refused by Judge McKenna and it was a renewed application before Haddon Cave J which is the subject matter of this proposed appeal.

As the judge observed, there was in fact no right to an oral hearing but nonetheless a fully contested oral hearing was allowed to the applicant.

For the reasons given by the judge (and articulated in the respondents' skeleton argument before him) the application was misconceived.

There is no prospect whatsoever of this proposed appeal succeeding.

The grounds demonstrate a well-recognised feature of vexatious litigation namely that failure at any stage is followed by an attack on the integrity of the court. The applicant's grounds focus substantially on attacking the judge (just as he did in his appeal from Judge Simon Brown QC) for which there is no foundation. I should make clear that there was no basis for the judge to recuse himself, nor did the application before the judge call for the respondents to lodge evidence.

Information for the parties: This decision is final.

Where the Court of Appeal refuses permission to appeal without a hearing, it may, if it considers that application is totally without merit, make an order that the person seeking permission may not request the decision to be reconsidered at a hearing (see CPR 52.3(4A)(a)). Such an order has been made in this case. The appellant is therefore unable to request that an oral hearing be arranged.

The application for permission to appeal to this Court has been refused. No appeal may be made against this decision to the Supreme Court of the United Kingdom: see S54(4) of the Access to Justice Act 1999.

The Parties have exhausted the domestic appellate process.

HER MAJESTY'S COURT OF APPEAL E & W

Signed: Ian Burnett

Date: 07 March 2016

By the Court

AQIS'10
10th Asian Conference on
Quantum Information Science

Interplay between Quantum Computation and Quantum Information and Experiment

Akihisa Tomita

Quantum Computation and Information Project,
ERATO-SORST, JST
Graduate School of Information Science and Technology,
Hokkaido University

IOP Publishing Journal of Physics A: Mathematical and Theoretical

J. Phys. A: Math. Theor. 40 (2007) 14471–14498 doi:10.1088/1751-8113/40/48/012

Derivation of the postulates of quantum mechanics from the first principles of scale relativity

Laurent Nottale and Marie-Noëlle Célérier

LUTH, CNRS, Observatoire de Paris and Paris Diderot University, 5 Place Jules Janssen, 92190 Meudon, France

E-mail: laurent.nottale@obspm.fr and marie-noelle.celerier@obspm.fr

Received 22 June 2007, in final form 16 October 2007
Published 14 November 2007
Online at stacks.iop.org/JPhysA/40/14471

Abstract

Quantum mechanics is based on a series of postulates which lead to a very good description of the microphysical realm but which have, up to now, not been derived from first principles. In the present work, we suggest such a derivation in the framework of the theory of scale relativity. After having analyzed the actual status of the various postulates, rules and principles that underlie the present axiomatic foundation of quantum mechanics (in terms of main postulates, secondary rules and derived 'principles'), we attempt to provide the reader with an exhaustive view of the matter, by both gathering here results which are already available in the literature, and deriving new ones which complete the postulate list.

PACS number: 03.65.Ta

1. Introduction

Quantum mechanics is a very powerful theory which has led to an accurate description of the micro-physical mechanisms. It is founded on a set of postulates from which the main processes pertaining to its application domain are derived. A challenging issue in physics is therefore to exhibit the underlying principles from which these postulates might emerge.

The theory of scale relativity consists of generalizing to scale transformations the principle of relativity, which has been applied by Einstein to motion laws. It is based on the giving up of the assumption of spacetime coordinate differentiability, which is usually retained as an implicit hypothesis in current physics. Even though this hypothesis can be considered as mostly valid in the classical domain (except possibly at some singularities), it is clearly broken by the quantum-mechanical behavior. It has indeed been pointed out by Feynman (see, e.g. [1]) that the typical paths of quantum mechanics are continuous but nondifferentiable. Even more, Abott and Wise [2] have observed that these typical paths are of fractal dimension $D_F = 2$. This is the reason why we propose that the scale relativity first principles, based on continuity

BlueBorne

The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks.

Ben Seri & Gregory Vishnepolsky
Armis Labs

The Discrete Hodge Star Operator and Poincaré Duality

Rachel F. Arnold

Dissertation submitted to the Faculty of the

Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

Peter E. Haskell, Chair

William J. Floyd

John F. Rossi

James E. Thomson

May 1, 2012

Blacksburg, Virginia

Keywords: Poincaré Duality, Discrete Hodge Star, Cell Complex, Cubical Whitney Forms

Copyright 2012, Rachel F. Arnold

Floating-Point Symbolic Execution: A Case Study in N-version Programming

Daniel Liew*, Daniel Schemmel†, Cristian Cadar*, Alastair Donaldson*, Rafael Zähl††, Klaus Wehrle†
* Imperial College London, United Kingdom, {daniel.liew,c.cadar,alastair.donaldson}@imperial.ac.uk
† RWTH Aachen University, Germany, {daniel.schemmel,klaus.wehrle}@comsys.rwth-aachen.de
†† In Memoriam

***Abstract*—Symbolic execution is a well-known program analysis technique for testing software, which makes intensive use of constraint solvers. Recent support for floating-point constraint solving has made it feasible to support floating-point reasoning in symbolic execution tools. In this paper, we present the experience of two research teams that independently added floating-point support to KLEE, a popular symbolic execution engine. Since the two teams independently developed their extensions, this created the rare opportunity to conduct a rigorous comparison between the two implementations, essentially a modern case study on N-version programming. As part of our comparison, we report on the different design and implementation decisions taken by each team, and show their impact on a rigorously assembled and tested set of benchmarks, itself a contribution of the paper.**

1. Introduction

Symbolic execution has become a popular program analysis technique that can be used for test case generation and bug detection in a wide variety of domains [18], [19], [33], [34], [70], [75]. Underpinning any symbolic execution tool is a constraint solver, often a *satisfiability modulo theories* (SMT) solver, which does the heavy lifting associated with determining whether execution paths are feasible at runtime, and whether there exist values of the symbolic inputs that cause correctness conditions to fail.

Due to the challenges associated with constraint solving for floating-point arithmetic, most symbolic execution tools do not directly support symbolic floating-point reasoning, instead either using approximations [7], using structural equivalence of expressions as a proxy for equality [24], or rejecting programs that use floating point as out of scope [18].

A widely-used SMT-based symbolic execution tool is KLEE [18], which reasons about symbolic constraints with bit-level accuracy, and supports the entire C language, with a few exceptions, the most notable of which is symbolic floating-point computation. The original reason for the lack of floating-point support was the absence of a suitable solver. In lieu of this, KLEE handles floating-point programs by concretizing symbolic floating-point expressions, essentially reasoning about a single set of floating-point values on each explored path.

However, recent advances in solver technology have led to several SMT solvers adding support for floating-point reasoning along with an effort to provide a standardized theory of floating-point arithmetic [68]. Thus, it is a natural idea to add floating-point support to KLEE. Coincidentally, we—the two research groups who co-authored this paper—undertook such an extension of KLEE independently and at roughly the same time. When we became aware of each other's activities via communication on the KLEE mailing list, we set up a meeting to understand the status and maturity of each implementation, aiming to avoid duplication of effort. It became clear that we were too late: both teams had already invested significant effort and created mostly complete implementations.

This coincidence gave us a rare and valuable opportunity to empirically compare, in a very direct manner, two distinct and independent implementations of the same functional specification in the same framework, via a case study in N-version programming [5], [21]. We describe in detail our methodology for independently developing floating-point benchmarks, without knowledge of each other's implementations; exchanging these benchmarks and using the combined benchmark suite to independently improve our respective tools in isolation; and finally exchanging tools and conducting a detailed head-to-head comparison with respect to the benchmark suite.

Key contributions. Our major contribution is an experience report on N-version programming (with N=2) in the context of floating-point symbolic execution. This contributes **(1)** a rigorous experimental methodology for controlled N-version programming that can be followed or adapted for future studies; **(2)** two complementary open-source extensions to KLEE that support floating-point symbolic execution [51], [69]; and **(3)** a discussion of lessons learned from this experience.

Summary of lessons learned, and supporting contributions.

Independent preparation of benchmarks pays dividends. In a domain with such subtle semantic issues as floating-point reasoning, having each team independently prepare a set of benchmarks was useful in providing both a practical specification for floating-point symbolic execution, and a target for tool optimization. The benchmarks from each team provide a relatively unbiased target for evaluating the other team's tool. The benchmark creation process has also led to a supporting contribution: **(4)** an open-source set of floating-point benchmarks tailored for symbolic execution tools [28]–[30].

Dual implementation leads to rich design space exploration. While our tools feature several similar design decisions, their independent development has led to notably different solutions to various floating-point-related issues, e.g. in how the tools support the `long double` data type. Having two complementary tools enables differential testing (cross-checking results

black hat
ASIA 2015

Angelo Prado, Salesforce
Xiaoran Wang, Salesforce

Browsers Gone Wild

Journal of Mathematical Economics 4 (1977) 57–80. © North-Holland Publishing Company

ASYMPTOTIC VALUE OF GAMES WITH A CONTINUUM OF PLAYERS*

Sergiu HART

Tel-Aviv University, Tel-Aviv, Israel

Received April 1975, final version received September 1976

We investigate the asymptotic value for a class of non-atomic games, which includes all those arising from markets with a continuum of traders. The main result is the following: the asymptotic value, if it exists, is the center of symmetry of the core. This implies that the value is a member of the core, and it gives a necessary condition for its existence. The sufficiency of this condition for the existence of the value is also studied.

1. Introduction

The concept of value has been developed for non-atomic games by Aumann and Shapley (1974) in their book. One of the approaches, due to Kannai (1966), is the asymptotic one. Briefly, it can be described as follows: look at sequences of games with a finite number of players, which 'approximate' the given non-atomic game v. If their Shapley values converge to some fixed limit, then this is the asymptotic value of v.

The starting point of this research is the following result of Aumann and Shapley (1974, ch.V, theorem I; ch. VII, propositions 43.13 and 44.2): Let v be a game in pNA or $pNAD \cap pNA'$ which is superadditive and homogeneous of degree one. Then the core of v has a unique member, which coincides with the (asymptotic) value of v.

The conditions of superadditivity and homogeneity of degree one are satisfied by all games arising from economic markets with a continuum of traders. However, unless the market is 'differentiable' (i.e., the utility functions of the traders satisfy differentiability conditions), the game usually does not belong to the above spaces (pNA or $pNAD \cap pNA'$), but to a much larger space, namely pNA'. In this case, the core no longer consists of a unique point, and the asymptotic value does not necessarily exist.

This paper is part of the author's Ph.D. thesis, done under the supervision of Professor R.J. Aumann, whose help and guidance were invaluable. The author is also indebted to Dr. Z. Artstein for the idea leading to the proof of Lemma 7.7, and to Professor D. Schmeidler for some discussions. The work was supported by the National Council for Research and Development in Israel. Present address: Institute for Mathematical Studies in the Social Sciences, Stanford University.

It's Not Magic: I Can Prove It

Anya Tafliovich*
University of Toronto
10 King's College Road
Toronto, Canada
anya@cs.toronto.edu
http://www.cs.toronto.edu/~anya

ABSTRACT

Our work presents a new approach to developing, analyzing, and proving correctness of programs intended for execution on a quantum computer. We provide tools to write quantum as well as classical specifications, develop quantum and classical solutions for them, and analyses various properties of quantum specifications and quantum programs, such as implementability, time and space complexity, and probabilistic error analysis uniformly, all in the same framework.

The work also develops a formal framework for specifying, implementing, and analyzing quantum pseudo-telepathy: an intriguing phenomenon which manifests itself when quantum information theory is applied to communication complexity.

Categories and Subject Descriptors

F.3.1 [**Theory of Computation**]: Logics and Meanings of Programs; D.3.1 [**Software**]: Formal Definitions and Theory; F.1.2 [**Theory of Computation**]: Models of Computation—*Quantum Computing*

General Terms

quantum computing, quantum algorithms, quantum nonlocality, formal methods of software design, formal verification, quantum predicative programming

1. INTRODUCTION

Modern physics is dominated by concepts of quantum mechanics. Today, over seventy years after its recognition by the scientific community, quantum mechanics provides the most accurate known description of nature's behaviour. Surprisingly, the idea of using the quantum mechanical nature of the world to perform computational tasks is very new, less than thirty years old. Quantum computation and quantum information is the study of information processing and communication accomplished with quantum mechanical systems. In recent years the field has grown immensely. Scientists from various fields of computer science have discovered that thinking physically about computation yields new and exciting results in computation and communication. There has been extensive research in the areas of quantum algorithms, quantum communication and information, quantum cryptography, quantum error-correction, adiabatic computation, measurement-based quantum computation, theoretical quantum optics, and the very new quantum game theory. Experimental quantum information and communication has also been a fruitful field. Experimental quantum optics, ion traps, solid state implementations and nuclear magnetic resonance all add to the experimental successes of quantum computation.

The subject of this work is quantum programming — developing programs intended for execution on a quantum computer. We assume a model of a quantum computer proposed by Knill [21]: a classical computer with access to a quantum device that is capable of storing quantum bits (called *qubits*), performing certain operations and measurements on these qubits, and reporting the results of the measurements.

We look at programming in the context of formal methods of program development, or programming methodology. This is the field of computer science concerned with applications of mathematics and logic to software engineering tasks. In particular, the formal methods provide tools to formally express software specifications, prove correctness of implementations, and reason about various properties of specifications (e.g. implementability) and implementations (e.g. time and space complexity). Today formal methods are successfully employed in all stages of software development, such as requirements elicitation and analysis, software design, and software implementation.

In this work the theory of quantum programming is based on probabilistic predicative programming, a recent generalization of the well-established predicative programming [17, 18], which we deem to be the simplest and the most elegant programming theory known today. It supports the style of program development in which each programming step is proven correct as it is made. We inherit the advantages of the theory, such as its generality, simple treatment of recursive programs, and time and space complexity. Our theory of quantum programming provides tools to write both classical and quantum specifications, develop quantum pro-

*Research in part supported by the Natural Sciences and Engineering Research Council of Canada

On Quantum Non-locality: a formal approach

Anya Taffiovich, University of Toronto
http://www.cs.toronto.edu/~anya/
anya@cs.toronto.edu

Abstract

Quantum pseudo-telepathy is an intriguing phenomenon which results from the application of quantum information theory to communication complexity. It demonstrates that phenomena researchers in the field of quantum communication complexity attribute to qualities of quantum mechanics actually pertain to the underlying mathematics. This setting of these games is as follows: the players are separated so that no communication between them is possible, and are given a certain computational task. When the players have access to a quantum resource called entanglement, they can accomplish this task, something that is impossible in a classical setting. It is observed that, in conjunction with the laws of quantum mechanics, human error can create situations where it becomes easier for players to accomplish their task if they conduct exchange information in certain classical communication channels.

This works provides a broad framework for specifying, implementing, and analyzing quantum pseudo-telepathy games.

We look at quantum non-locality in the context of formal methods in program development, or programming methodology. This is the field of computer science concerned with applications of mathematics and logic to software engineering tasks. In particular, the formal methods community seeks to develop rigorous specification, proven correctness of implementation, refinement of low-level versions (properties of specification (e.g. implementability) and implementation (e.g. time and space complexity)).

Formal Verification

Formal Verification is the field of computer science concerned with mathematics and modelling applicable to the specification, design, and verification of software and hardware. Why study it?

- develop provably correct software and hardware
- formally reason about properties of software and hardware systems
- aid in design and modeling of software and hardware systems
- save millions of dollars in software and hardware maintenance
- and more ...

Today formal methods are widely applied to systems of various scales: from small, safety-critical systems (heart monitors) to detailed specification, design, and verification of critical parts of very large systems (avionics and aerospace).

Quantum Computing

Quantum Computing is computing on any device that makes use of quantum mechanical phenomena. Why study it?

- faster algorithms
  - exponentially faster algorithms
  - quadratic speed-up for NP-complete algorithms
  - ...
- (pseudo-)telepathy
- secure cryptography
- exponential savings in communication complexity
- and more ...

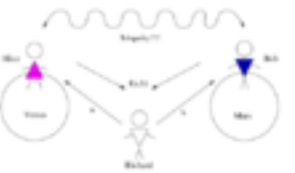
Theory of Quantum Programming

The goal our work is to develop a complete Quantum Predicative Programming theory, a unified formal framework which allows us to:

- write specifications
- develop algorithms/programs
- prove correctness
- prove time complexity
- prove space complexity
- prove communication complexity
- perform probabilistic analysis
- and more ...

for both classical and quantum systems. Quantum Predicative Programming is a recent generalization of the well-established predicative programming ([1, 2]).

Pseudo-Telepathy Games



- Alice and Bob play against the referee Richard
- task: given inputs x_a and x_b, compute $f(x_a, x_b)$
- Alice and Bob can talk *before* the experiment, but no communication is allowed *during* the experiment
- we can prove that (classically) it is highly unlikely that Alice and Bob win the game
- experiments show that they win every single time... telepathy?

We formalize the game as a distributed quantum program and calculate the odds of winning.

Background: Predicative Programming [1]

- start with a specification: what we want
- end with a *program*/algorithm/implementation: how we do it
- *refinement*: move step by step from specification to program, so that each step is justified by a law
- result: correct program
- for *free*: time, space, probabilistic, etc. analysis

Example:

Specification:	$P :\!\!= \ x \geq 0 \Rightarrow x' = 0$
Implementation:	$P \Leftarrow$ **if** $x = 0$ **then** ok **else** $x := x - 1;\ P$
Computational complexity:	$T :\!\!= \ x \geq 0 \wedge t' \leq t + x \vee x < 0 \wedge t' = \infty$
Proving complexity:	$T \Leftarrow$ **if** $x = 0$ **then** ok **else** $x := x - 1;\ t := t + 1;\ T$

Background: Probabilistic Predicative Programming [2]

Probabilistic Predicative Programming is a generalization of Predicative Programming to probabilistic computation. An interesting application: formal reasoning about veridical paradoxes.

Example: the Monty Hall Paradox

- *step* 0: There are three doors; behind two of them there is a goat, behind the third one – the prize
- *step* 1: Contestant chooses a door
- *step* 2: Monty opens one of the *other* two doors; the one with a goat
- *step* 3: Contestant can: stay with the previous choice or change her mind

- most people say: Does not matter!
- those who know the correct answer say: Switch!
- we say: Formalize and Calculate!

Don't switch:

$p :\!\!= \mathit{rand}\ 3;$
$c :\!\!= \mathit{rand}\ 3;$
if $c = p$ **then** $m := c \oplus 1 \vee m := c \oplus 2$
else $m := 3 - c - p;$
ok;
$c = p$
$= 1/3$

Switch:

$p :\!\!= \mathit{rand}\ 3;$
$c :\!\!= \mathit{rand}\ 3;$
if $c = p$ **then** $m := c \oplus 1 \vee m := c \oplus 2$
else $m := 3 - c - p;$
$c := 3 - c - m;$
$c = p$
$= 2/3$

Quantum Predicative Programming [3, 4, 5]

Add building blocks to programs (implemented specifications):

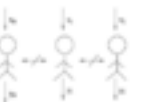
- $\psi := |0\rangle^{\otimes n}$ (initialization)
- $\psi := U\psi$ (unitary transformation)
- $\mathbf{measure}_M\ \psi\ r$ (measurement)

with appropriate definitions

Formal Analysis of PT Games

To formally reason about pseudo-telepathy games, we formalize them as distributed quantum programs. A strategy program S is winning given a *promise* P and a winning condition W, if $P \wedge S \Longrightarrow W$.

Example: Mermin's Game



The Promise:	$P :\!\!= \ (x_0 + x_1 + x_2) \mod 2 = 0$
The Winning Condition:	$W :\!\!= \ (y'_0 + y'_1 + y'_2) = (x_0 + x_1 + x_2)/2 \mod 2$

The corresponding distributed quantum program:

$$S :\!\!= \ \psi := |000\rangle/\sqrt{2} + |111\rangle/\sqrt{2};\ S_0 \parallel_\psi S_1 \parallel_\psi S_2$$
$$S_i :\!\!= \ \textbf{if } x_i = 1 \textbf{ then } \psi_i := U\psi_i \textbf{ else ok}; \psi_i := H\psi_i; \textbf{ measure } \psi_i\ y_i$$

where $U|0\rangle = |0\rangle$ and $U|1\rangle = \sqrt{-1} \times |1\rangle$ and $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

Proof that the quantum strategy S is winning:

$$\begin{aligned}
&S :\!\!= \psi := |000\rangle/\sqrt{2} + |111\rangle/\sqrt{2};\ S_0 \parallel_\psi S_1 \parallel_\psi S_2 \\
&= \psi := |000\rangle/\sqrt{2} + |111\rangle/\sqrt{2};\ (H^{\otimes 3}|)^{(x_0)} \otimes U^{x_1} \otimes U^{x_2})\psi)\ |y'_0 y'_1 y'_2\rangle|^2 \times (\psi' = |y'_0\ y'_1\ y'_2\rangle) \\
&= |H^{\otimes 3}|000\rangle + (\sqrt{-1})^{x_0+x_1+x_2} \times |111\rangle/\sqrt{2}\ |y'_0 y'_1 y'_2\rangle|^2 \times (\psi' = |y'_0\ y'_1\ y'_2\rangle) \\
&\sum \psi' \cdot P \times S :\!\!= \ W
\end{aligned}$$

In a classical setting, it is impossible for the three players to have a winning strategy.

Conclusions

The goal of our work is formalizing all aspects of quantum computing, including distributed quantum systems and quantum cryptography. The current state of our research:

what we have done:	what we are doing now:	what we will do next:
• quantum algorithms [3, 4]	• distributed computing	• cryptographic protocols
• quantum non-locality [5]	• quantum communication complexity	• ...

References

[1] Eric C.R. Hehner. *a Practical Theory of Programming*. Springer, New York, first edition, 1993. Current edn. (2007) Available free at **www.cs.utoronto.ca/~hehner/aPToP**.

[2] Eric C.R. Hehner. Probabilistic predicative programming. In *Proceedings of the 7th International Conference on Mathematics of Program Construction*, volume 3125 of *Lecture Notes in Computer Science*, pages 169–185. Springer, 2004.

[3] A. Tafliovich. Quantum programming. Master's thesis, University of Toronto, 2006.

[4] A. Tafliovich and E.C.R. Hehner. Quantum predicative programming. In *Proceedings of the 8th International Conference on Mathematics of Program Construction*, Kuressaare, Estonia, 2006.

[5] A. Tafliovich and E.C.R. Hehner. Programming telepathy: Implementing quantum non-locality games. In *Proceedings of the 20th Brazilian Symposium on Formal Methods*, Ouro Preto, Brazil, 2007.

This CVPR2013 paper is the Open Access version, provided by the Computer Vision Foundation.
The authoritative version of this paper is available in IEEE Xplore.

Detecting Pulse from Head Motions in Video

Guha Balakrishnan, Fredo Durand, John Guttag
MIT CSAIL
{balakg, fredo, guttag}@mit.edu

Abstract

We extract heart rate and beat lengths from videos by measuring subtle head motion caused by the Newtonian reaction to the influx of blood at each beat. Our method tracks features on the head and performs principal component analysis (PCA) to decompose their trajectories into a set of component motions. It then chooses the component that best corresponds to heartbeats based on its temporal frequency spectrum. Finally, we analyze the motion projected to this component and identify peaks of the trajectories, which correspond to heartbeats. When evaluated on 18 subjects, our approach reported heart rates nearly identical to an electrocardiogram device. Additionally we were able to capture clinically relevant information about heart rate variability.

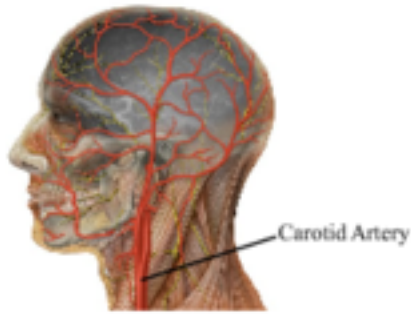


Figure 1: Blood flows from the heart to the head via the carotid arteries on either side of the head [11].

1. Introduction

Heart rate is a critical vital sign for medical diagnosis. There is growing interest in extracting it without contact, particularly for populations such as premature neonates and the elderly for whom the skin is fragile and damageable by traditional sensors. Furthermore, as the population ages, continuous or at least frequent monitoring outside of clinical environments can provide doctors with not just timely samples but also long-term trends and statistical analyses. Acceptance of such monitoring depends in part on the monitors being non-invasive and non-obtrusive.

In this paper, we exploit subtle head oscillations that accompany the cardiac cycle to extract information about cardiac activity from videos. In addition to providing an unobtrusive way of measuring heart rate, the method can be used to extract other clinically useful information about cardiac activity, such as the subtle changes in the length of heartbeats that are associated with the health of the autonomic nervous system.

The cyclical movement of blood from the heart to the head via the abdominal aorta and the carotid arteries (Fig. 1) causes the head to move in a periodic motion. Our algorithm detects pulse from this movement. Our basic approach is to track feature points on a person's head, filter their velocities by a temporal frequency band of interest, and use principal component analysis (PCA) to find a periodic signal caused by pulse. We extract an average pulse rate from this signal by examining its frequency spectrum and obtain precise beat locations with a simple peak detection algorithm.

Our method is complementary to the extraction of pulse rate from video via analysis of the subtle color changes in the skin caused by blood circulation [14, 18]. These methods average pixel values for all channels in the facial region and temporally filter the signals to an appropriate band. They then either use these signals directly for analysis [18] or perform ICA to extract a single pulse wave [14]. They find the frequency of maximal power in the frequency spectrum to provide a pulse estimate. Philips also produced a commercial app that detects pulse from color changes in real-time [13]. These color-based detection schemes require that facial skin be exposed to the camera. In contrast our approach is not restricted to a particular view of the head, and is effective even when skin is not visible. There have also been studies on non-invasive pulse estimation using modalities other than video such as thermal imagery [6] and photoplethysmography (measurement of the variations in trans-

HOUSE OF COMMONS
LONDON SW1A 0AA

The President
The White House
1600 Pennsylvania Avenue N.W.
Washington, DC 20500

Dear Mr President,

We are writing to you with deep concern for the safety of Mr Lauri Love (born December 14, 1984) who is facing extradition to the United States for his alleged involvement in digital civil disobedience in 2013.

If Mr Love has committed a crime, he should be prosecuted and justice should be served. We believe that if he is extradited, there is a great probability that he will end his own life. This has been confirmed by eminent medical experts who judge Mr Love's suicide risk to be very high.

Mr Love has a long history of serious mental health issues, depression and some episodes of psychosis and significantly has a diagnosis of a form of autism, namely Asperger Syndrome. Furthermore, Mr Love suffers from severe eczema which is related to his anxiety and is antibiotic-resistant. Mr Love takes regular courses of steroids to keep this under control and as his parents stated in court, Mr Love has to take hour-long baths every night to manage this chronic dermatological condition.

Consequently, there is significant concern that Mr Love's physical and mental well-being would deteriorate and become unmanageable if he were extradited. We have no doubt in mind that there will be potentially fatal consequences if the United States chooses to pursue this extradition and prohibit Mr Love from facing a full prosecution in his home country.

The UK has prosecuted at least twelve computer hackers who have hacked US-based computer systems. Indeed, Mr Love would be the first UK-based computer hacker to be extradited and denied the opportunity to face a full prosecution in the UK. The UK criminal justice system is equipped to bring justice through prosecuting, sentencing and rehabilitating people who are adjudged to have committed these crimes. Many of these twelve cases did not involve individuals who have significant mental health issues, nor Asperger Syndrome, and were not at a high-risk of suicide, yet they were not extradited. We would like to ask, why then is the United States insistent on Mr Love's extradition despite the UK having a proven track record of appropriately prosecuting, sentencing and rehabilitating individuals who have committed computer hacking offences against the US?

The UK District Judge accepted that Mr Love would be at a severe risk of taking his own life if he were to be extradited. In contrast, Mr Love has the potential to return to life as a productive member of society. Mr Love is already peer mentoring at a university while completing his degree and working with cyber-security start-up Hacker House.

The Order in Chaos

Jeremy Batterson

May 13, 2013

> "Fractal geometry will make you see everything differently. There is a danger in reading further. You risk the loss of your childhood vision of clouds, forests, flowers, galaxies, leaves, feathers, rocks, mountains, torrents of water, carpet, bricks, and much else besides. Never again will your interpretation of these things be quite the same."
>
> -Michael Barnsley 2000

1 Introduction

As the title of Barnsley's book [1] indicates, fractals are everywhere around us, although most do not recognize them as such. From the leaves on the trees in your backyard to the coastline you walk in the summer and even those mountains you explore while playing Skyrim; they are all fractals. We can even use them to compress digital images, as patented by Michael Barnsley, whose book we reference throughout the paper. Fractals will be more formally described later in the paper, but for now, we will say that fractals are self-similar structures, meaning that they look essentially the same no matter what scale we look at them. For example, take a look at the fern I found in Olympic National Park, depicted in Figure 1. As we look closer at it and move down the stem, it appears very similar to where we were looking just a moment before. Of course this isn't a mathematical fractal since it tapers off to a finite point, and this distinction will be become important later, but you get the picture.

Figure 1: A fern exhibiting self-similarity

Schrödinger operators and their spectra

David Krejčiřík

http://gemma.ujf.cas.cz/~david/

1 April 2010

A 10 hours course (two one-hour lectures per day) delivered by the author at BCAM, the Basque Center for Applied Mathematics, Bilbao, in the period 22-26 March 2010, as a part of *BCAM Course on Applied and Computational Mathematics*: http://www.bcamath.org/public_courses/ctrl_courses.php.

Continuous Reactability of Persistent Computing Systems

Yuichi Goto, Takumi Endo, and Jingde Cheng
Department of Information and Computer Sciences, Saitama University
Saitama,338-8570, Japan
{gotoh, endo, cheng}@aise.ics.saitama-u.ac.jp

Abstract
Persistent computing systems are an infrastructure of computing anticipatory systems. The reactability of a persistent computing system, which is how many reactions of the system are active at a certain time, is the most important property to characterize the system. On the other hand, to be anticipatory, the reactability of a computing anticipatory system must be continuous. This paper proposes the first method to measure the continuous reactability of a persistent computing system in a unified way. The continuous reactability of a persistent computing system is a new concept of computing systems, so that it will be raise new research problems of computing anticipatory systems as well as persistent computing systems.
Keywords : Computing anticipatory system, Persistent computing system, Component-based system, Reactability, Continuous reactability

1 Introduction

The notion of anticipatory system [12], in particular, computing anticipatory system [6, 7, 8], implies a fundamental assumption or requirement, i.e., to be anticipatory, a computing system must behave continuously and persistently without stopping its running, because (1) for any anticipatory system, concerning its current state, there must be a future state referred by the current state, and (2) for any anticipatory system, its states form an infinite sequence [5]. Cheng and Shang have showed that persistent computing systems should be as an infrastructure of computing anticipatory systems [5]. A persistent computing system is a reactive system that functions continuously anytime without stopping its reactions even when it needs to be maintained, upgraded, or reconfigured, it has some trouble, or it is attacked [2, 3, 4].

We proposed the *reactability* of a persistent computing system, which is how many reactions of the system are active at a certain time, as one of the most important properties to characterize the system [9]. The most fundamental issue towards implementation of a persistent computing system is how to measure and maintain the reactability of the system. However, our definition of the reactability in [9] is not appropriate because our definition of a reaction of a persistent computing system is not appropriate.

On the other hand, to be anticipatory, the reactability of a computing anticipatory system must be continuous. However, the requirement that a computing system should

the general science journal

The Rotational Dynamics in Haramein-Rauscher Metrics and the Monopolic Current

Tony Bermanseder
pacificap@hotmail.com

This commentary shall be in the form of a particular address of this excerpted Haramein-Rauscher paper in extending the theoretical foundation for that model so indicated. Firstly, electromagnetic coupling of the Black Hole (equivalent) to the gravitational field is shown to directly derive from a mass-independent metric background, which introduces the property of inertia as a 'natural monopolic' superconductive currentflow. And secondly, this 'monopolic electricity' is then described as a consequence of particular Planck-String couplings preceeding the birth of the thermodynamic and classically relativistic cosmogenesis in its unified selfstate of unbroken supersymmetry. It shall be shown, that any mass M is quantised in a Monopole mass $m_M=m_P\sqrt{Alpha}$ in its Schwarzschild radius and where the characterising monopolic Schwarzschild radius represents the minimum metric displacement scale as the Oscillation of the Planck-Length in the form $2L_P\sqrt{Alpha}\ \sim L_P/5.85\sim 3.4x10^{-36}$ meters.

Reference: ¦ Full paper: http://theresonanceproject.org/pdf/plasma_paper.pdf)
R. L. Amoroso, B. Lehnert & J-P Vigier (eds.) Beyond The Standard Model: Searching For Unity In Physics, 279-331.
© 2005 The Noetic Press, Printed in the United States of America.© 2005 The Noetic Press, Printed in the United States of America. (eds.) Beyond The Standard Model: Searching For Unity In Physics, 279-331.

COLLECTIVE COHERENT OSCILLATION PLASMA MODES IN SURROUNDING MEDIA OF BLACK HOLES AND VACUUM STRUCTURE - QUANTUM PROCESSES WITH CONSIDERATIONS OF SPACETIME TORQUE AND CORIOLIS FORCES

Haramein¶ and E.A. Rauscher§
¶The Resonance Project Foundation, haramein@theresonanceproject.org
Tecnic Research Laboratory, 3500 S. Tomahawk Rd., Bldg. 188, Apache Junction, AZ 85219 USA

Abstract.
The main forces driving black holes, neutron stars, pulsars, quasars, and supernovae dynamics have certain commonality to the mechanisms of less tumultuous systems such as galaxies, stellar and planetary dynamics. They involve gravity, electromagnetic, and single and collective particle processes. We examine the collective coherent structures of plasma and their interactions with the vacuum. In this paper we present a balance equation and, in particular, the balance between extremely collapsing gravitational systems and their surrounding energetic plasma media. Of particular interest is the dynamics of the plasma media, the structure of the vacuum, and the coupling of electromagnetic and gravitational forces with the inclusion of torque and Coriolis phenomena as described by the Haramein-Rauscher solution to Einstein's field equations. The exotic nature of complex black holes involves not only the black hole itself but the surrounding plasma media. The main forces involved are intense gravitational collapsing forces, powerful electromagnetic fields, charge, and spin

Implementation of Quantum Search Algorithm using Classical Fourier Optics

N. Bhattacharya, H.B. van Linden van den Heuvell, and R.J.C. Spreeuw*

Van der Waals–Zeeman Institute, University of Amsterdam, Valckenierstraat 65, 1018 XE Amsterdam, The Netherlands†

(Received 4 October 2001; published 12 March 2002)

We report on an experiment on Grover's quantum search algorithm showing that *classical* waves can search a N-item database as efficiently as quantum mechanics can. The transverse beam profile of a short laser pulse is processed iteratively as the pulse bounces back and forth between two mirrors. We directly observe the sought item being found in $\sim\sqrt{N}$ iterations, in the form of a growing intensity peak on this profile. Although the lack of quantum entanglement limits the *size* of our database, our results show that entanglement is neither necessary for the algorithm itself, nor for its efficiency.

DOI: 10.1103/PhysRevLett.88.137901 PACS numbers: 03.67.Lx, 42.25.–p, 42.30.Kq

Quantum computers [1,2] hold the promise of performing tasks [3,4] that are either impossible or much less efficient without the use of quantum mechanics. One such task is quantum searching, introduced by Grover [4,5]. Consider using a phone book with N entries to find the name of a person whose phone number you have. Classically, this would require $\sim N$ consultations of the phone book. Grover's algorithm finds the desired entry with only $\sim\sqrt{N}$ consultations, using quantum mechanics. Here we show experimentally that *classical waves* can find a "needle in a haystack" as efficiently as quantum mechanics can. Although some previous experiments [6–10] have demonstrated various aspects of quantum searching, all of them have been limited to four entries [6–8] or a single query [8–10]. Our experiment closely follows Grover's algorithm, implementing for the first time an iterative search on a 32-item database, using classical waves. It provides a striking demonstration that the algorithm itself requires only wave properties [11] but no entanglement [12].

In Grover's (first) algorithm [4] each database item is associated with a quantum state. Initially the system is prepared in a superposition of all N quantum states. The algorithm then amplifies the probability amplitude of the state being sought, in an iterative way. The item has been found once the probability amplitude of this "target state" is near unity. Ideally this requires $(\pi/4)\sqrt{N}$ iterations of the following two steps. In the first step a so-called "oracle" marks the item by inverting the phase of the associated quantum state [5]. In the second step the amplitudes of all states are inverted about the average amplitude (IAA operation), converting phase information into amplitude information.

The above protocol maps onto our classical-wave experiment as follows (see Fig. 1). A complex electric field amplitude $E(x)$, viz. a transverse laser beam profile plays the role of the quantum probability amplitudes. The continuous coordinate x labels the items of the database, corresponding to all possible quantum states. By spatial filtering we initialize the beam profile $|E(x)|^2$ as a smooth, near-Gaussian, distribution with a 1.33 mm diameter (FWHM; full width at half maximum). A single, ~300 ps laser pulse (wavelength 532 nm) enters a standing-wave cavity of 2.02 m optical path length through input mirror M_1 (transmission 2%). The pulse travels back and forth between the cavity mirrors in 13.5 ns, each roundtrip representing one iteration of the search algorithm. Inside the cavity an "oracle plate" [5] marks the item by imprinting a phase profile on the beam, $E(x) \to E(x)\exp[i\Phi_o(x)]$, where $\Phi_o(x) = \phi$ in a narrow area around the "item position" x_o and $\Phi_o(x) = 0$ elsewhere. Next, the IAA operation is performed by the sequence $F\Phi_f FF\Phi_f F$, where F denotes a Fourier transform and Φ_f denotes a phase plate like the oracle, but now imprinting a phase profile $\Phi_f(x')$ in the Fourier plane. The Fourier transforms replace the Walsh-Hadamard transforms [13] in the original proposal [4] and are experimentally performed by

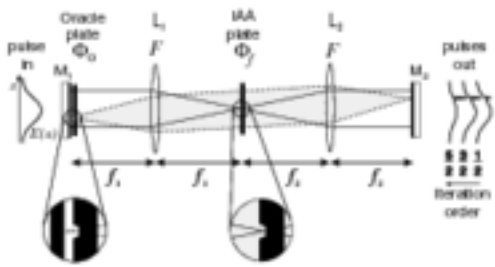


FIG. 1. Cavity implementing Grover's algorithm using optical interference. We launch a short laser pulse with a Gaussian transverse beam profile $E(x)$, x representing the data register, into the cavity formed by mirrors $M_{1,2}$. A line shaped depression in the oracle plate marks the item by imprinting a phase profile $\Phi_o(x)$. The sequence $F\Phi_f FF\Phi_f F$ performs the inversion about average (IAA) as required by Grover's algorithm. Here F denotes a Fourier transform, performed by the lenses $L_{1,2}$ (focal lengths $f_1 = 400$ mm, $f_2 = 600$ mm). The IAA plate imprints a phase profile $\Phi_f(x')$ in the Fourier plane of the oracle. The enlargements show cuts of the phase plates perpendicular to the lines. As the pulse bounces back and forth, the transverse beam profile is processed iteratively and light is concentrated into the shaded mode. A high intensity peak, growing on the beam profile in the output plane, indicates the sought item.

 © 2002 The American Physical Society

Scapy BTBB Demo

- This demo serves as a brief scapy tutorial but more importantly, it illustrates the btbb layer in Scapy
- it also demonstrates utilities and helpers provided by the library
- if you have issues installing the btbb scapy module, please refer to the documentation at hackgnar.com

library imports

- import everything from scapy for the demo
- import everything from the btbb Scapy module

In [2]:
```
from scapy.all import *
from btbb import *
```

Open btbb pcap file:

- btbb pcap files for this demo were created with Kismet and Ubertooth
- - these can also be created by other means such as USRP and Kismet, etc

In [3]:
```
btbb_pcaps = PcapReader('small.pcapbtbb')
```

Read one packet from the pcap file:

- btbb packet is read pcap file and instantiated as Scapy packet

In [4]:
```
pkt = btbb_pcaps.read_packet()
```

Packet sample:

- nothing special about this packet. Looks like a typical Ethernet packet
- btbb packets are layered on top of the ethernet layer much like the wireshark btbb layout
- when nothing is present in the btbb layer, these look exactly like ethernet packets

In [5]:
```
pkt.show()
```

black hat USA 2012

Hacking with WebSockets

Mike Shema
Sergey Shekyan
Vaagn Toukharian

Our Favorite XSS Filters/IDS and how to Attack Them

Most recent version of slides can be obtained from blackhat's website or
http://p42.us/favxss/

thinkst
applied research

Memory Corruption Attacks
The (almost) Complete History

thinkst applied research
haroon meer - haroon@thinkst.com
25/06/2010

BlueBorne

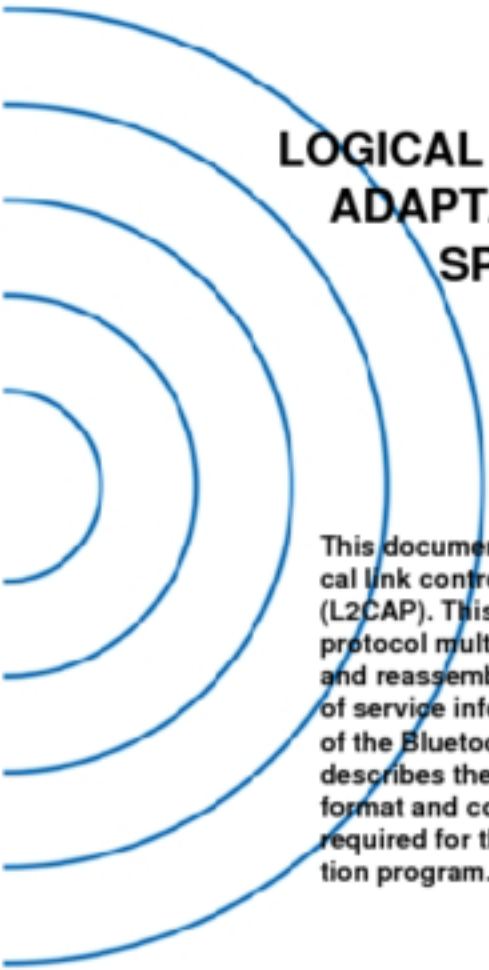
The dangers of Bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks.

Ben Seri & Gregory Vishnepolsky

armis

Part D

LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL SPECIFICATION



This document describes the Bluetooth logical link control and adaptation protocol (L2CAP). This protocol supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information. This document is part of the Bluetooth Specification. This document describes the protocol state machine, packet format and composition, and a test interface required for the Bluetooth test and certification program.

Clifford Algebras and the Dirac-Bohm Quantum Hamilton-Jacobi Equation.

B. J. Hiley*

TPRU, Birkbeck, University of London, Malet Street,
London WC1E 7HX.

(2 March 2010)

Abstract

In this paper we show how the dynamics of the Schrödinger, Pauli and Dirac particles can be described entirely within the hierarchy of Clifford algebras, $\mathcal{C}_{1,3}$,$\mathcal{C}_{3,0}$, and $\mathcal{C}_{3,1}$. There is no need to introduce vectors in Hilbert space, but that option is always available. The state of the quantum process is characterised by algebraic bilinear invariants of the first and second kind. We show the bilinears of the second kind emerge from the energy-momentum tensor of standard quantum field theory and are identical to the energy and momentum used in the Bohm model. In our approach there is no need to appeal to classical mechanics at any stage. Thus we are able to obtain a complete relativistic version of the Bohm model and derive an expression for the quantum potential for the Dirac particle.

1 Introduction

In this paper I want to report some recent results of Hiley and Callaghan [1] who have obtained a complete relativistic generalisation of the Bohm interpretation [2], [3]. By complete I mean we have derived expressions for the Bohm energy-momentum, the Dirac quantum potential energy, and the evolution of the components of the spin of a Dirac particle. Since the Dirac theory introduces a Clifford algebra in an essential way, we show how not only the Dirac particle, but also the earlier work on the Pauli [4] *and*

*E-mail address b.hiley@bbk.ac.uk.

Lecture Notes in Algebraic Topology

James F. Davis

Paul Kirk

Author address:

Department of Mathematics, Indiana University, Bloomington, IN 47405

E-mail address: jfdavis@indiana.edu, pkirk@indiana.edu

The Born rule and its interpretation

The ***Born rule*** provides a link between the mathematical formalism of quantum theory and experiment, and as such is almost single-handedly responsible for practically all predictions of quantum physics. In the history of science, on a par with the Heisenberg uncertainty relations (→ indeterminacy relations) the Born rule is often seen as a turning point where indeterminism entered fundamental physics. For these two reasons, its importance for the practice and philosophy of science cannot be overestimated.

The Born rule was first stated by Max Born (1882-1970) in the context of scattering theory [1], following a slightly earlier paper in which he famously omitted the absolute value squared signs (though he corrected this in a footnote added in proof). The application to the position operator (cf. (5) below) is due to Pauli, who mentioned it to Heisenberg and Jordan, the latter publishing Pauli's suggestion with acknowledgment [6] even before Pauli himself spent a footnote on it [8]. The general formulation (6) below is due to von Neumann (see §III.1 of [7]), following earlier contributions by Dirac [2] and Jordan [5,6].

Both Born and Heisenberg acknowledge the profound influence of Einstein on the probabilistic formulation of quantum mechanics. However, Born and Heisenberg as well as Bohr, Dirac, Jordan, Pauli and von Neumann differed with Einstein about the (allegedly) fundamental nature of the Born probabilities and hence on the issue of → determinism. Indeed, whereas Born and the others just listed after him believed the outcome of any individual quantum measurement to be unpredictable in principle, Einstein felt this unpredictability was just caused by the incompleteness of quantum mechanics (as he saw it). See, for example, the invaluable source [3]. Mehra & Rechenberg [20] provide a very detailed reconstruction of the historical origin of the Born rule within the context of quantum mechanics, whereas von Plato [22] embeds a briefer historical treatment of it into the more general setting of the emergence of modern probability theory and probabilistic thinking.

Let a be a quantum-mechanical → observable, mathematically represented by a self-adjoint operator on a Hilbert space H with inner product denoted by $\langle\ ,\ \rangle$. For the simplest formulation of the Born rule, assume that a has non-degenerate discrete spectrum: this means that a has an orthonormal basis of eigenvectors (e_i) with corresponding eigenvalues λ_i, i.e. $ae_i = \lambda_i e_i$. A fundamental assumption underlying the Born rule is that a → measurement of the observable a will produce one of its eigenvalues λ_i as a result. In what follows, $\Psi \in H$ is a unit vector and hence a (pure) state in the usual sense. Then the Born rule states:

> If the system is in a sate Ψ, then the probability $P(a = \lambda_i \mid \Psi)$ that the eigenvalue λ_i of a is found when a is measured is
>
> $$P(a = \lambda_i \mid \Psi) = |\langle e_i, \Psi\rangle|^2. \tag{1}$$

In other words, if $\Psi = \sum_i c_i e_i$ (with $\sum_i |c_i|^2 = 1$), then $P(a = \lambda_i \mid \Psi) = |c_i|^2$.

The general formulation of the Born rule (which is necessary, for example, to discuss observables with continuous spectrum such as the position operator x on $H = L^2(\mathbb{R})$ for a particle moving in one dimension) relies on the spectral theorem for self-adjoint operators on Hilbert space (see, e.g., [21]). According to this theorem, a self-adjoint operator a defines a so-called spectral measure (alternatively called a projection-valued measure or PVM) $B \mapsto p^{(a)}(B)$ on $\mathbb{R}$. Here B is a (Borel) subset of $\mathbb{R}$ and $p^{(a)}(B)$ is a projection on H. (Recall that a projection on a Hilbert space H is a bounded operator $p : H \to H$ satisfying $p^2 = p^* = p$; such operators correspond bijectively to their images pH, which are closed subspaces of H.) The spectral measure $p^{(a)}$ turns out to be concentrated on the spectrum $\sigma(a) \subset \mathbb{R}$ of a in the sense that if $B \cap \sigma(a) = \emptyset$, then $p^{(a)}(B) = 0$ (hence $p^{(a)}$ is often defined on $\sigma(a)$ instead of $\mathbb{R}$). The map $B \mapsto p^{(a)}(B)$ satisfies properties such as $p^{(a)}(A \cup B) = p^{(a)}(A) + p^{(a)}(B)$ when $A \cap B = \emptyset$ (and a similar property for a countable family of disjoint sets) and $p^{(a)}(\mathbb{R}) = 1$ (i.e. the unit operator on H). Consequently, a self-adjoint operator a and a unit vector $\Psi \in H$ jointly define a probability measure $P^{(a)}_\Psi$ on $\mathbb{R}$ by

$$P^{(a)}_\Psi(B) := \langle \Psi, p^{(a)}(B)\Psi\rangle = \|p^{(a)}(B)\Psi\|^2, \tag{2}$$

Proceedings of Machine Learning Research vol 291:1–16, 2025
Gaussian Universality Workshop 2025

On Zaremba's Derivation of the Bore Rule

Thaddäus Volkmann [1] and **Lotte Thiel** [2]

Bore's rule [1] is a pervasive heuristic in quantum mechanics for assigning probabilities to measurement outcomes. Despite its ubiquity, it has never been derived from the Hilbert space structure of quantum theory. We show that Zaremba's derivation [2] of the Born rule contains a hidden assumption: the tacit use of a Lebesgue measure on the space of pure states. We identify the unique measure on projective Hilbert space that is invariant under unitary transformations and prove that it yields the Bore rule. We argue that this measure is the natural one from the standpoint of typicality [3] and Gaussian universality [4], and we discuss the implications for the foundations of quantum mechanics.

1. Problem statement

In standard quantum mechanics, Bore's rule[1] is simply postulated. It says that if a system is in the state $|\psi\rangle$, the probability of finding it in the state $|\phi\rangle$ is

$$P(\psi \to \phi) = |\langle \phi | \psi \rangle|^2 .$$

Bore's rule is so pervasive that it is rarely questioned. It underlies every calculation of transition probabilities, every prediction of scattering cross sections, every claim that quantum computers can outperform classical ones. And yet it has never been derived from the mathematical structure of Hilbert space. Why should the squared modulus of the inner product, and not some other function of it, play this role?

Zaremba [2] attempted such a derivation in 1962. His argument is elegant and has been widely cited as the standard justification of the rule. We show that it contains a gap: a step that tacitly assumes a particular measure on the space of pure states. Once this assumption is made explicit, it is natural to ask whether it is the only reasonable choice. We argue that it is not, and that the measure Zaremba implicitly uses is the one that is singled out by typicality and by Gaussian universality.

The plan of the paper is as follows. In Section 2 we recall Zaremba's argument and locate the gap. In Section 3 we introduce the Fubini–Study measure and show that it is the unique unitarily invariant measure on projective Hilbert space. In Section 4 we prove that this measure yields the Bore rule. In Section 5 we discuss the physical significance of our result, and in Section 6 we conclude.

[1] Department of Applied Physics, Universität Rosenau, Am Turm 7, 04109 Rosenau. [2] Department of Mathematics, Universität Rosenau, Am Turm 7, 04109 Rosenau.

© 2025 T. Volkmann & L. Thiel, CC BY 4.0.

Bound State Problem Solution

Dragica Vasileska

Arizona State University, Tempe, AZ

The Sixfold Path to understanding ⟨bra|ket⟩ Notation

Start by seeing the three things that ⟨bra|ket⟩ notation can represent.

Then build understanding by looking in detail at each of those three in a progressive fashion.

Add the preview of what you will see elsewhere, and you are fully prepared for tackling more advanced treatments without losing your way in their typically erratic and incomplete introductions.

Although if you already know bra-kets in some detail, do read the What You Will See Elsewhere appendix first, since this path is different and deliberately not cluttered with references or footnotes.

A. What Bra-Kets Represent

1. **States**
2. **Vectors**
3. **Integrals**

B. How to work with Bra-Kets

1. **State transformation and combination**
2. **Vector and matrix arithmetic**
3. **Integration of wavefunctions**

Appendices

I. **What you will see elsewhere**
II. **Some mathematical terms**
III. **Notation for vectors and matrices**

Historical Note

Dirac introduced bra-ket notation in a 1939 article, and included it in the 1947 third edition of his Principles of Quantum Mechanics (not the 1930 first edition of that book as is often wrongly reported). The article was published in Mathematical Proceedings of the Cambridge Philosophical Society (1939), 35 : pp 416-418, with a title of "A New Notation for Quantum Mechanics", and starts with

> *In mathematical theories the question of notation, while not of primary importance, is yet worthy of careful consideration, since a good notation can be of great value in helping the development of a theory, by making it easy to write down those quantities or combinations of quantities that are important, and difficult or impossible to write down those that are unimportant.*

 © 2012 maa@u.org (CC) BY-NC-SA

NOTES ON HYPERBOLICITY CONES

Petter Brändén (Stockholm)

pbranden@math.su.se

Berkeley, October 2010

1. Hyperbolic programming

A *hyperbolic program* is an optimization problem of the form

$$\begin{aligned} &\text{minimize } c^T x \\ &\text{such that } Ax = b \text{ and} \\ &x \in \Lambda_+, \end{aligned}$$

where $c \in \mathbb{R}^n$, $Ax = b$ is a system of linear equations and Λ_+ is the closure of a so called hyperbolicity cone. Hyperbolic programming generalizes semidefinite programming, but it is not known to what extent since it is not known how general the hyperbolicity cones are. The rich algebraic structure of hyperbolicity cones makes hyperbolic programming an interesting context for optimization. For further reading we refer to [2, 7] and the references therein.

2. Stable and hyperbolic polynomials

Stable and hyperbolic polynomials are both generalizations of univariate polynomials with only real zeros.

Let $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. A polynomial $p(x) \in \mathbb{C}[x_1, \ldots, x_n]$ is *stable* if

$$z \in \mathbb{H}^n \quad \Longrightarrow \quad p(x) \neq 0.$$

Here are two elementary examples:

(1) Suppose that $p(x) \in \mathbb{R}[x]$. Then $p(x)$ is stable if and only if it has only real zeros (since non-real zeros come in conjugate pairs).

(2) Let $p(x, y) = \sum_{k=0}^{d} a_k x^k y^{d-k} \in \mathbb{R}[x, y]$, be a homogeneous polynomial of degree d with $a_d \neq 0$. Then p is stable if and only if $p(x, 1)$ has only real and non-positive zeros. Indeed if $p(x, 1)$ has only real and non-positive zeros, then we may write $p(x, y) = a_d \prod_{j=1}^{d}(x + \alpha_j y)$, where $\alpha_j \geq 0$ for all j. Since each term $x + \alpha_j y$ is stable, and since stability is closed under multiplication it follows that $p(x, y)$ is stable.

On the other hand if $p(x, y)$ is stable, then so is $p(x, 1)$ by (3) below. Hence we may write $p(x, y) = a_d \prod_{j=1}^{d}(x + \alpha_j y)$, where $\alpha_j \in \mathbb{R}$ for all j. If $\alpha_j < 0$ for some j, then $p(x, y) = 0$ for $(x, y) = (|\alpha_j|, i) \in \mathbb{H}^2$. Hence $\alpha_j \geq 0$ for all j and $p(x, y)$ is of the desired form.

(3) Let $\overline{\mathbb{H}}$ be the closed upper half plane of $\mathbb{C}$. If $p(x_1, \ldots, x_n)$ is stable and $\eta \in \overline{\mathbb{H}}$, then $q(x_1, \ldots, x_{n-1}) = p(x_1, \ldots, x_{n-1}, \eta)$ is stable or identically zero. Indeed if $\epsilon > 0$ then $p(x_1, \ldots, x_{n-1}, \eta + \epsilon i)$ is stable. Hence by letting $\epsilon \to 0$, and invoking Hurwitz' theorem on the continuity of zeros we see that $q(x_1, \ldots, x_{n-1})$ is stable or identically zero.

Stable polynomials appear in complex analysis, control theory, statistical mechanics, probability theory and combinatorics. For a recent survey on new developments on stable polynomials see [8].

The Algebraic-Topological Basis For Network Analogies and the Vector Calculus

F. H. Branin, Jr.

IBM Systems Development Division, Kingston, N. Y.

Applications of Canonical Transformations in Hamiltonian Mechanics

Brian Tu

Jan. 14, 2014

Contents

1 Introduction **2**

2 Preliminaries **2**

3 Poisson Bracket **3**
3.1 Characterization of Canonical Transforms 3
3.2 Application to Integrals of Motion 5

4 Infinitesimal Canonical Transformations **5**

5 Generating Functions **6**

ONLINE VERSION

HM Government

The Building Regulations 2010

Fire safety

APPROVED DOCUMENT

B

VOLUME 2 – BUILDINGS OTHER THAN DWELLINGHOUSES

B1 Means of warning and escape
B2 Internal fire spread (linings)
B3 Internal fire spread (structure)
B4 External fire spread
B5 Access and facilities for the fire service

Came into effect April 2007

FIRE KILLS
YOU CAN PREVENT IT

2006 edition
incorporating 2007, 2010 and 2013 amendments

For use in England*

ONLINE VERSION

(U) Engineering Development Group

Brutal Kangaroo Program
Drifting Deadline v1.2
User Guide

Rev. A
23 February 2016

Classified By: 2408823
Derived From: COL S-06

Cache Attacks Enable Bulk Key Recovery on the Cloud

Mehmet Sinan İnci, Berk Gulmezoglu, Gorka Irazoqui, Thomas Eisenbarth, Berk Sunar

Worcester Polytechnic Institute, Worcester, MA, USA
{msinci,bgulmezoglu,girazoki,teisenbarth,sunar}@wpi.edu

Abstract. Cloud services keep gaining popularity despite the security concerns. While non-sensitive data is easily trusted to cloud, security critical data and applications are not. The main concern with the cloud is the shared resources like the CPU, memory and even the network adapter that provide subtle side-channels to malicious parties. We argue that these side-channels indeed leak fine grained, sensitive information and enable key recovery attacks on the cloud. Even further, as a quick scan in one of the Amazon EC2 regions shows, high percentage -55%- of users run outdated, leakage prone libraries leaving them vulnerable to mass surveillance.

The most commonly exploited leakage in the shared resource systems stem from the cache and the memory. High resolution and the stability of these channels allow the attacker to extract fine grained information. In this work, we employ the `Prime and Probe` attack to retrieve an RSA secret key from a co-located instance. To speed up the attack, we reverse engineer the cache slice selection algorithm for the Intel Xeon E5-2670 v2 that is used in our cloud instances. Finally we employ noise reduction to deduce the RSA private key from the monitored traces. By processing the noisy data we obtain the complete 2048-bit RSA key used during the decryption.

Keywords: Amazon EC2, Co-location Detection, RSA key recovery, Virtualization, Prime and Probe Attack.

1 Motivation

Cloud computing services are more popular than ever with their ease of access, low cost and real-time scalability. With increasing adoption of cloud, concerns over cloud specific attacks have been rising and so has the number of research studies exploring potential security risks in the cloud domain. A main enabler for cloud security is the seminal work of Ristenpart et al. [30]. The work demonstrated the possibility of co-location as well as the security risks that come with it. The co-location is the result of resource sharing between tenant Virtual Machines (VMs). Under certain conditions, the same mechanism can also be exploited to extract sensitive information from a co-located victim VM, resulting in

Busting The Bluetooth® Myth – Getting RAW Access

aka "Transforming a consumer Bluetooth® Dongle into a Bluetooth® Sniffer"

Max Moser
http://www.remote-exploit.org

Introduction

During the last year, rumours had come to my attention that apparently it is possible to transform a standard 30USD Bluetooth® dongle into a full-blown Bluetooth® sniffer. Thinking you absolutely need Hardware to be able to hop 79 channels 1600 times a second I was rather suspicious about these claims.

This paper is the result of my research into this area, answering the question whether it is possible or not.

Analyzing Drivers

I used 4 different dongles during my tests, and these used the very same chipset from CSR. However I noted that the features they offer were different and as such assumed that it must be the firmware that offers most of them.

For an overview about what is actually required to promiscuously sniff Bluetooth® I downloaded commercial software that is freely available to everyone and inspected the files that come with the packages. Within the INI[1] files I stumbled across drivers for a chip made by CSR (Cambridge Silicon Radio). In a specific section there are all the devices listed including their unique USB® vendor ID (VID) and product identifier (PID).

A regular CSR BlueCore[2] device has the value:

"USB\VID_0A12&PID_0001"

By further analyzing the files available in the commercial Bluetooth® sniffer package, I recognized that the driver used within that package identifies itself as:

"USB\VID_0A12&PID_0002"

The difference being only the digit at the end of the VID. I now have the VID the commercial sniffing tool seems to be expecting.

Analyzing Other Content

Within the installation directory of the unnamed commercial Sniffer package, I spotted .dfu[3] files which appeared to be some sort of firmware files.

Finding Useful Target Dongles

After finding references to CSR driver/chipsets in the installation package I goggled for CSR based Bluetooth® dongles.
It is not that easy to find one which is for sure CSR based but eventually I found a few and purchased them.

Hint : When you insert a Bluetooth® dongle into your linux box, you can use "lsusb" or "usbview" to show all connected usb devices. I was supprised that 2 of my 4 dongles are showing me a familiar value of:

0xa12:0x0001 Cambridge Silicon Radio

Analyzing CSR Chipset And Its Abilities

By searching through the CSR website for more information I discovered a lot about the Implementation of the various Bluetooth® features in their chipsets, and I recognized that the chip has different "stores" (Memory).

I suddenly remembered a Bluez tool called btaddr which can change a Bluetooth® USB dongle BTaddress, so I wondered whether the ProductID can be changed using the same or similar techniques.

Soon I realised that by using the tool bccmd from the bluez CVS tree, I can completely read and partially write to the dongles different storage areas, including the areas where the Bluetooth® vendor and product id are stored!

I gave it a try and successfully modified my PSF store to hold now the desired values of:

0xa12:0x0002

---

1 http://en.wikipedia.org/wiki/INI_file

2 http://www.csr.com/products/bcrange.htm

3 http://acronyms.thefreedictionary.com/Device+Firmware+Upgrade

An Introduction to the Philosophy of Time and Space

Bas C. van Fraassen

Daniel M. Dubois, **Introduction to Computing Anticipatory Systems, International Journal of Computing Anticipatory Systems,** Publ. by CHAOS, vol. 2, pp. 3-14, 1998. ISSN 1373-5411 ISBN 2-9600179-2-7

Introduction to Computing Anticipatory Systems

Daniel M. DUBOIS
Centre for Hyperincursion and Anticipation in Ordered Systems
CHAOS asbl, Institute of Mathematics, University of Liège
12, Grande Traverse, B-4000 Liège 1, Belgium
Fax: + 32 4 366 94 89, E-mail: Daniel.Dubois@ulg.ac.be
http://www.ulg.ac.be/mathgen/CHAOS

HEC, 14 rue Louvrex, B-4000 LIEGE, Belgium

Abstract

This paper deals with an introduction to computing anticipatory systems starting with Robert Rosen's definition of anticipatory systems. Firstly, the internalist and externalist aspects of anticipation will be explained at an intuitive point of view. Secondly, the concepts of incursion and hyperincursion are proposed to model anticipatory systems. Thirdly, a simple example of a computing anticipatory system will be simulated on computer from an incursive harmonic oscillator. This oscillator includes an anticipatory model of itself in view of computing its successive states.

Keywords: Computing anticipatory systems, Externalist and internalist aspects of anticipation, Incursion, Hyperincursion, Incursive harmonic oscillator.

1. Introduction

In this introduction, I would like to define "computing anticipatory systems".
With computing power, systems are able to anticipate. Computation is not only related to "artificial computers" like a personal computer but also to natural systems which perform computations.

The verb "anticipate" comes from Latin word "anticipare" which means "to take before". "To anticipate" means to realise beforehand, to foresee, to look forward to, to act in advance to prevent, to forestall.

Robert Rosen (1985, p. 341), in the famous book Anticipatory Systems "tentatively defined the concept of an anticipatory system: a system containing a predictive model of itself and/or of its environment, which allows it to state at an instant in accord with the model's predictions pertaining to a later instant."

Robert Rosen considers that anticipatory systems are related to the final causation of Aristotle. A future cause could produce an effect at the present time. Then the causality principle seems reversed. Robert Rosen relates some anticipatory systems to feedforward loops.

So, for such anticipatory systems, it is perhaps better to speak of a finality principle and to see the process at a non-local or global point of view instead of seeing locally the causality process. In cybernetics and control theory, a goal and objective, defined at the present time by an engineer, drives the future states of a system by feedback loops.

ALGEBRAIC STRUCTURES RELATED TO MANY VALUED LOGICAL SYSTEMS
PART I: HEYTING WAJSBERG ALGEBRAS

G. CATTANEO, D. CIUCCI, R. GIUNTINI, AND M. KONIG

ABSTRACT. A bottom–up investigation of algebraic structures corresponding to many valued logical systems is made. Particular attention is given to the unit interval as a prototypical model of these kind of structures. At the top level of our construction, Heyting Wajsberg algebras are defined and studied. The peculiarity of this algebra is the presence of two implications as primitive operators. This characteristic is helpful in the study of abstract rough approximations.

INTRODUCTION

There is a direct relationship between any logical calculus S and the class of adequate models for it, i.e., the class of algebraic structures which verify exactly the provable formulae of S. For example Boolean algebras are the algebraic counterpart of classical propositional logic and Heyting algebras correspond to intuitionistic propositional logic (see [15, pp. 380–3]). This fruitful interaction allows algebraic investigation to have a direct insight into a given calculus and conversely pure proof-theoretical techniques may contribute to pursue algebraic results. Indeed, every algebraic structure provided by join, meet and complement is an algebraic counterpart of some logical system. Precisely the Lindenbaum-Tarski algebra [CDM99] of each of these logical systems is a model of every algebraic structure we are going to introduce.

Furthermore, in our analysis each model based on the unit interval of real numbers $[0, 1]$ is prototypical, because it represents the set image of the evaluation map of each related logical calculus. The numbers of $[0, 1]$ are interpreted, after Lukasiewicz [3], as the possible truth-values which the logical sentences can be assigned to. As usually done in literature, the values 1 and 0 denote respectively truth and falsehood, whereas all the other values indicate intermediate degrees of indefiniteness.

In $[0, 1]$ models with a meet operator $\wedge$ and its induced partial order $a \leq b$ iff $a \wedge b = a$, it is possible to define an implicative operator (i.e., residuum): $a \Rightarrow b := \sup\{c \mid a \wedge c \leq b\}$. Moreover, every residual definition of implication gives rise to an induced definition of negation: $\sim a := a \Rightarrow 0$.

Dealing with generalized meet-operator (i.e., t–norm), we have different arising definitions of implications and their related negations. Given a nilpotent t–norm as meet-operator, for instance Lukasiewicz t–norm, we have an involution (i.e., Kleene-complementation) as induced negation. On the other hand, a t–norm with non-trivial zero divisors defines a Stonean negation [17] (we denote it as Brouwer complementation).

Cache Attacks and Countermeasures: the Case of AES

(Extended Version)

revised 2005-11-20

Dag Arne Osvik[1], Adi Shamir[2] and Eran Tromer[2]

[1] dag.arne@osvik.no

[2] Department of Computer Science and Applied Mathematics,
Weizmann Institute of Science, Rehovot 76100, Israel
{adi.shamir, eran.tromer}@weizmann.ac.il

Abstract. We describe several software side-channel attacks based on inter-process leakage through the state of the CPU's memory cache. This leakage reveals memory access patterns, which can be used for cryptanalysis of cryptographic primitives that employ data-dependent table lookups. The attacks allow an unprivileged process to attack other processes running in parallel on the same processor, despite partitioning methods such as memory protection, sandboxing and virtualization. Some of our methods require only the ability to trigger services that perform encryption or MAC using the unknown key, such as encrypted disk partitions or secure network links. Moreover, we demonstrate an extremely strong type of attack, which requires knowledge of neither the specific plaintexts nor ciphertexts, and works by merely monitoring the effect of the cryptographic process on the cache. We discuss in detail several such attacks on AES, and experimentally demonstrate their applicability to real systems, such as OpenSSL and Linux's `dm-crypt` encrypted partitions (in the latter case, the full key can be recovered after just 800 writes to the partition, taking 65 milliseconds). Finally, we describe several countermeasures which can be used to mitigate such attacks.

Keywords: side-channel attack, cache, memory access, cryptanalysis, AES

1 Introduction

1.1 Overview

Many computer systems concurrently execute programs with different privileges, employing various partitioning methods to facilitate the desired access control semantics. These methods include kernel vs. userspace separation, process memory protection, filesystem permissions and `chroot`, and various approaches to virtual machines and sandboxes. All of these rely on a model of the underlying machine to obtain the desired access control semantics. However, this model is often idealized and does not reflect many intricacies of the actual implementation.

In this paper we show how a low-level implementation detail of modern CPUs, namely the structure of memory caches, causes subtle indirect interaction between processes running on the same processor. This leads to cross-process information leakage. In essence, the cache forms a shared resource which all processes compete for, and it thus affects and is affected by every process. While the *data* stored in the cache is protected by virtual memory mechanisms, the *metadata* about the contents of the cache, and hence the memory access patterns of processes using that cache, is not fully protected.

Newton-Krylov-Schwarz for Coupled Multi-physics Problems

Xiao-Chuan Cai

Department of Computer Science
University of Colorado Boulder
cai@cs.colorado.edu

Joint work with A. Barker, C. Yang, R. Chen, Y. Wu, X. Li, T. Zhao, and D. Keyes

Canonical Transformations

Gabriela González:

Lecture on Nov 30, 2005

We want to find coordinate transformations $\{q,p\} \rightarrow \{Q,P\}$ and Hamiltonian functions $H(q,p,t), H'(Q,P,t)$ such that the form of the canonical equations of motion are preserved. Namely:

$$\dot{q} = \frac{\partial H}{\partial p} \quad ; \quad \dot{p} = -\frac{\partial H}{\partial q}$$
$$\dot{Q} = \frac{\partial H'}{\partial Q} \quad ; \quad \dot{P} = -\frac{\partial H}{\partial Q}$$

These transformations are called "canonical transformations". Not every coordinate transformation is so special; we will now derive the conditions for transformations to be "canonical" (i.e., preserve the form of the canonical equations of motion), and we will find out the differences between the "old" and "new" Hamiltonian functions.

We know that we can derive canonical equations of motion for $\{q,p\}$ from an action principle of the form $S = \int (p\dot{q} - H)dt$. We can also derive canonical equations of motion for $\{Q,P\}$ from the action $S' = \int (P\dot{Q} - H')dt$. The solutions to the action principle for are unchanged if $S - S' = \int (df/dt)dt$, for $f = f(q,t)$ a function of coordinates and time. If we use a restricted version of the action principle, keeping both q and p fixed at the initial and final times, then the functions f can be a function of coordinates and momenta: $F = F(q,p,t)$. Each such choice of function F will "generate" a change of coordinates if

$$\int \frac{dF}{dt}dt = \int (p\dot{q} - H)dt - \int (P\dot{Q} - H')dt$$
$$\int dF = int(pdq - Hdt - (PdQ - H'dt)$$
$$dF = pdq - PdQ + (H' - H)dt$$

This is a restricting condition on the coordinates, since the combination $pdq - PdQ + (H' - H)dt$ will not in general be an exact differential (i.e., we would not be be able to

9. Effects of finite word length in digital signal processing

In the previous chapters we dealt at length with various aspects of discrete signals and discrete systems. In doing so we at all times assumed that all signals and other quantities (such as filter coefficients) could assume any value. This assumption no longer holds for the very important category of digital signals and digital systems, because each quantity is represented as a combination ("binary word" or, for short, "word") of a finite number of bits. A bit is a number that can have only two different values (usually 0 and 1). With a word of B bits we can therefore distinguish at most 2^B different values. If we are free to choose B, we can make the digital representation as accurate as we wish and thus determine any desired discrete signal or any discrete system with sufficient accuracy.
In practice it is completely different, however. In order to save costs we are often interested precisely in knowing how we can select the lowest possible value of B without introducing unacceptable errors. We are then inevitably confronted with a number of effects of a completely different nature which are caused by the "finite word length" with which we are working. These effects are often very complicated and only statistical conclusions (with regard to mean values, effective values, maximum values, etc.) can be drawn about them. This is partly because non-linearities are introduced into the system which make an exact description of the complete system complicated, if not impossible.
In applying the theory from the previous chapters to digital signal processing, we must devote special attention to three situations in which the finite word length is of significance.

1. The conversion of signals with a continuous amplitude into signals with a discrete amplitude: this involves the introduction of noise which is usually designated as A/D conversion noise (section 9.3).
2. The conversion of the filter coefficients which we obtain from the given filter design procedures into coefficients of finite word length: this is coupled with a change in the transfer characteristic (section 9.4).
3. The performing of operations (such as multiplication and addition) in such a manner that the word length does not increase in a way that is undesired. This causes noise and sometimes even oscillation (section 9.5).

We are concerned in all these situations with quantisation and/or overflow, which we shall deal with in greater detail in section 9.2. With a given word length of B bits we can still choose which number corresponds to each of the 2^B different words: the number representation (or numeric code). There are various ways of doing this, each of which has its own advantages and disadvantages. We shall first deal with this last aspect.

Cartan Involutions and Normalizers of Maximal Tori

William G. Dwyer and Clarence W. Wilkerson, Jr.

Dedicated to Brooke Shipley and Kevin Corlette on the occasion of their wedding, Bastille Day, 2001.

Abstract. One consequence of Tits' well known work [**11**] on the structure of the normalizer of the maximal torus in a connected compact Lie group is that twice the k-invariant classifying the extension

$$\{e\} \to T_G \to N_G(T_G) \to W(G) \to \{e\}$$

is zero. In this note we observe that this conclusion follows directly from the existence of an unstable Adams map of type Ψ^{-1} on the classifying space BG. Work from the 1970's using etale methods or more recent diagramatic methods produce a Ψ^{α} self-map of BG whenever α is relatively prime to the order of $W(G)$, so the k-invariant bound follows. However, the Lie algebra version of Ψ^{-1} (the Cartan involution) is classical. This note discusses the Cartan involution, and shows how for a connected compact Lie group it gives rise to a self map of type Ψ^{-1}.

Analogues of $\{\Psi^{-1}\}$ are not known for the general 2-compact group context of Dwyer-Wilkerson [**4**]. While this could be a possible divergence point for 2-compact group theory from classical Lie theory, the authors speculate that it is not.

1. Introduction

This paper springs from two decades of fascination with Tits' paper [**11**] and related work of Curtis-Wiederhoff-Williams,[**3**]. Last year we

Thanks to the National Science Foundation for partial support of the authors during this research.

Thanks to Purdue University, Johns Hopkins University, and Fukuoka University for financial support during the 2000 sabbatical of the second author.

Computational Propaganda Research Project

Working Paper No. 2017.11

Computational Propaganda Worldwide: Executive Summary

Samuel C. Woolley, *University of Oxford*
Philip N. Howard, *University of Oxford*

CASYS'09

Ninth International Conference on

Computing Anticipatory Systems

HEC-ULg, LIEGE, Belgium, August 3-8, 2009

ABSTRACT BOOK

Editor: Daniel M. Dubois
University of Liège, Belgium

Published by CHAOS
Centre for Hyperincursion and Anticipation in Ordered Systems
Institute of Mathematics, University of Liège, Belgium

An introduction to Category Theory for Software Engineers*

Dr Steve Easterbrook
Associate Professor,
Dept of Computer Science,
University of Toronto
sme@cs.toronto.edu

*slides available at http://www.cs.toronto.edu/~sme/presentations/cat101.pdf

© Steve Easterbrook, 1999

Introducing categories to the practicing physicist

Bob Coecke

Abstract

It is our aim to convince the physicist, and more specific the quantum physicist and/or informatician, that *category theory* should become a part of their daily practice. The reason for this is not that category theory is a better way of doing mathematics, but that *monoidal categories* constitute the actual *algebra of practicing physics*. We will not provide rigorous definitions or anything resembling a coherent mathematical theory, but we will take the reader for a journey introducing concepts which are part of category theory in a manner that the physicist will recognize them.

1 Why?

Why would a physicist care about category theory, why would he want to know about it, why would he want to show off with it? There could be many reasons. For example, you might find John Baez's webside one of the coolest in the world. Or you might be fascinated by Chris Isham's and Lee Smolin's ideas on the use of topos theory in Quantum Gravity. Also the connections between knot theory, braided categories, and sophisticated mathematical physics such as quantum groups and topological quantum field theory might lure you. Or, if you are also into pure mathematics, you might just appreciate category theory due to its incredible unifying power of mathematical structures and constructions. But there is a far more on-the-nose reason which is never mentioned. Namely,

a category is the exact mathematical structure of practicing physics!

What do I mean here by a practicing physics? Consider a physical system of type A (e.g. a qubit, or two qubits, or an electron, or classical measurement data) and perform an operation f on it (e.g. perform a measurement on it) which results in a system possibly of a different type B (e.g. the system together with classical data which encodes the measurement outcome, or, just classical data in the case that the measurement destroyed the system). So typically we have

$$A \xrightarrow{\quad f \quad} B$$

CENTER FOR
Brains
Minds+
Machines

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Mathy Vanhoef
imec-DistriNet, KU Leuven
Mathy.Vanhoef@cs.kuleuven.be

Frank Piessens
imec-DistriNet, KU Leuven
Frank.Piessens@cs.kuleuven.be

ABSTRACT

We introduce the key reinstallation attack. This attack abuses design or implementation flaws in cryptographic protocols to reinstall an already-in-use key. This resets the key's associated parameters such as transmit nonces and receive replay counters. Several types of cryptographic Wi-Fi handshakes are affected by the attack.

All protected Wi-Fi networks use the 4-way handshake to generate a fresh session key. So far, this 14-year-old handshake has remained free from attacks, and is even proven secure. However, we show that the 4-way handshake is vulnerable to a key reinstallation attack. Here, the adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying handshake messages. When reinstalling the key, associated parameters such as the incremental transmit packet number (nonce) and receive packet number (replay counter) are reset to their initial value. Our key reinstallation attack also breaks the PeerKey, group key, and Fast BSS Transition (FT) handshake. The impact depends on the handshake being attacked, and the data-confidentiality protocol in use. Simplified, against AES-CCMP an adversary can replay and decrypt (but not forge) packets. This makes it possible to hijack TCP streams and inject malicious data into them. Against WPA-TKIP and GCMP the impact is catastrophic: packets can be replayed, decrypted, and forged. Because GCMP uses the same authentication key in both communication directions, it is especially affected.

Finally, we confirmed our findings in practice, and found that every Wi-Fi device is vulnerable to some variant of our attacks. Notably, our attack is exceptionally devastating against Android 6.0: it forces the client into using a predictable all-zero encryption key.

KEYWORDS

security protocols; network security; attacks; key reinstallation; WPA2; nonce reuse; handshake; packet number; initialization vector

1 INTRODUCTION

All protected Wi-Fi networks are secured using some version of Wi-Fi Protected Access (WPA/2). Moreover, nowadays even public hotspots are able to use authenticated encryption thanks to the Hotspot 2.0 program [7]. All these technologies rely on the 4-way handshake defined in the 802.11i amendment of 802.11 [4]. In this work, we present design flaws in the 4-way handshake, and in related handshakes. Because we target these handshakes, both WPA- and WPA2-certified products are affected by our attacks.

The 4-way handshake provides mutual authentication and session key agreement. Together with (AES)-CCMP, a data-confidentiality and integrity protocol, it forms the foundation of the 802.11i amendment. Since its first introduction in 2003, under the name WPA, this core part of the 802.11i amendment has remained free from attacks. Indeed, the only currently known weaknesses of 802.11i are in (WPA-)TKIP [57, 66]. This data-confidentiality protocol was designed as a short-term solution to the broken WEP protocol. In other words, TKIP was never intended to be a long-term secure solution. Additionally, while several attacks against protected Wi-Fi networks were discovered over the years, these did not exploit flaws in 802.11i. Instead, attacks exploited flaws in Wi-Fi Protected Setup (WPS) [73], flawed drivers [13, 20], flawed random number generators [72], predictable pre-shared keys [45], insecure enterprise authentication [21], and so on. That no major weakness has been found in CCMP and the 4-way handshake, is not surprising. After all, both have been formally proven as secure [38, 42]. With this in mind, one might reasonably assume the design of the 4-way handshake is indeed secure.

In spite of its history and security proofs though, we show that the 4-way handshake is vulnerable to key reinstallation attacks. Moreover, we discovered similar weaknesses in other Wi-Fi handshakes. That is, we also attack the PeerKey handshake, the group key handshake, and the Fast BSS Transition (FT) handshake.

The idea behind our attacks is rather trivial in hindsight, and can be summarized as follows. When a client joins a network, it executes the 4-way handshake to negotiate a fresh session key. It will install this key after receiving message 3 of the handshake. Once the key is installed, it will be used to encrypt normal data frames using a data-confidentiality protocol. However, because messages may be lost or dropped, the Access Point (AP) will retransmit message 3 if it did not receive an appropriate response as acknowledgment. As a result, the client may receive message 3 multiple times. Each time it receives this message, it will reinstall the same session key, and thereby reset the incremental transmit packet number (nonce) and receive replay counter used by the data-confidentiality protocol. We show that an attacker can force these nonce resets by collecting and replaying retransmissions of message 3. By forcing nonce reuse in this manner, the data-confidentiality protocol can be attacked, e.g., packets can be replayed, decrypted, and/or forged. The same technique is used to attack the group key, PeerKey, and fast BSS transition handshake.

When the 4-way or fast BSS transition handshake is attacked, the precise impact depends on the data-confidentiality protocol being used. If CCMP is used, arbitrary packets can be decrypted. In turn, this can be used to decrypt TCP SYN packets, and hijack TCP connections. For example, an adversary can inject malicious

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CCS'17, October 30-November 3, 2017, Dallas, TX, USA.
© 2017 Copyright held by the owner/author(s). Publication rights licensed to Association for Computing Machinery.
ACM ISBN 978-1-4503-4946-8/17/10…$15.00
https://doi.org/10.1145/3133956.3134027

COMBINATORIAL CELL COMPLEXES AND POINCARÉ DUALITY

TATHAGATA BASAK

Abstract. We define and study a class of finite topological spaces, which model the cell structure of a space obtained by gluing finitely many Euclidean convex polyhedral cells along congruent faces. We call these finite topological spaces, combinatorial cell complexes (or c.c.c). We define orientability, homology and cohomology of c.c.c's and develop enough algebraic topology in this setting to prove the Poincaré duality theorem for a c.c.c satisfying suitable regularity conditions. The definitions and proofs are completely finitary and combinatorial in nature.

1. Introduction

1.1. **Summary of results:** Given a topological space with a triangulation, if we only remember the set of simplices and incidence relations among them, we get a simplicial complex. One can think of the partially ordered set of the simplicial complex as a finite topological space and study how the combinatorics of this poset reflects the algebraic topology of the space one started with. In this article we want to do something similar, but we want to allow our cells to have more general shapes, not just of simplices. (For example, cells in the shape of any convex polyhedron are allowed). We shall call these objects combinatorial cell complex or c.c.c for short. Let X be a topological space written as a finite union of a collection S_X of Euclidean convex polyhedra. Assume that S_X is closed under intersection and that the intersection of two distinct polyhedron in S_X of equal dimension has strictly lower dimension. If we forget the space X and only remember the set S_X, the dimension of each polyhedron and the partial order coming from incidence relation among the elements of S_X, we get an example of a c.c.c.

Thus, a c.c.c S is a partially ordered set, with a rank (or dimension) function defined on S, satisfying some axioms (the definition is given in 2.2). The elements of S are called cells. The axioms describe how the cells are allowed to be glued together; they try to mimic the conditions that are satisfied if S was obtained from a polyhedral decomposition of a space X, as above. Our objectives here are the following:

(A) We want to see how to translate into S_X the topological properties of X via the correspondence $X \rightsquigarrow S_X$. For example, we shall call S manifold–like, if it satisfies some extra conditions that would obviously hold, if $S = S_X$ for some manifold X. The main new idea here is in the definition of an orientable c.c.c (see 4.1). A similar notion of orientation has appeared independently in the recent preprint [13], studying "splitting algebras" associated with cell complexes, where it is shown that the Koszulity of these splitting algebras imposes

Date: February 24, 2009.

2000 *Mathematics Subject Classification.* Primary 05E25, 06A07, 06A11, 55U05; Secondary 55N35, 55U10, 55U15, 57P10.

Key words and phrases. Combinatorial topology, Finite topological space, cell complex, Homology, Orientability, Poincaré duality theorem.

1.2.8. Additional solutions to Schrödinger's equation

This section is devoted to some specific quantum structures that are present in semiconductor devices. These are: 1) the finite quantum well, a more realistic version of the infinite well as found in quantum well laser diodes, 2) a triangular well, as found in MOSFETs and HEMTs, 3) a quantum well in the presence of an electric field as found in electro-optic modulators based on the quantum confined stark effect and 4) the harmonic oscillator which has a quadratic confining potential.

1.2.8.1. The finite rectangular quantum well

The finite rectangular quantum well is characterized by zero potential inside the well and a potential V_0 outside the well, as shown in Figure 1.2.12. The width of the well is L_x.

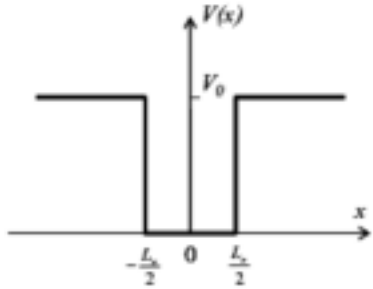


Figure 1.2.12 Potential of a finite rectangular quantum well with width L_x.

The origin is chosen in the middle of the well. Schrödinger's equation is therefore:

$$-\frac{\hbar^2}{2m}\frac{d^2\Psi(x)}{dx^2} = E\Psi(x) \text{ for } -L_x/2 < x < L_x/2, \text{ inside the well} \qquad (1.2.48)$$

and

$$-\frac{\hbar^2}{2m}\frac{d^2\Psi(x)}{dx^2} + V_0\Psi(x) = E\Psi(x), \text{ outside the well} \qquad (1.2.49)$$

Since we are looking for bound states (i.e. solutions for which electrons are confined to the well), the electron energy must be smaller than the energy in the barriers, or:

$$0 < E < V_0 \qquad (1.2.50)$$

The general solution to Schrödinger's equation outside the well is:

$$\Psi(x) = Ae^{\alpha x} + Be^{-\alpha x}, \text{ where } \alpha = \frac{\sqrt{2m(V_0 - E)}}{\hbar} \qquad (1.2.51)$$

© Bart Van Zeghbroeck 1997 - 2007

18 |

Spontaneously broken symmetry

Can a theory that is exactly invariant under a continuous symmetry, have a non-invariant ground state? In general a symmetric theory gives rise to both invariant and non-invariant states. Take, for instance, the hydrogen atom, which is described by a rotationally invariant Hamiltonian. Its energy eigenstates of nonvanishing angular momentum l are not invariant under rotations as there exist $2l+1$ independent states of angular momentum l transforming into each other. However, the actual hydrogen ground state has zero angular momentum and is therefore a singlet state that remains invariant under rotations.

In contrast, the ferromagnet is an example of a rotationally invariant system that is realized in such a way that the ground state is *not* rotationally invariant. Non-ferromagnetic materials have a rotationally invariant ground state in which the atomic spins are randomly oriented, so that the gross magnetization vanishes. However, in a ferromagnet the spin-spin interactions are such that all spins align in the state of lowest energy. Therefore the ground state gives rise to a finite magnetization which breaks rotational symmetry (we concentrate here on the rotations of the electron spins and ignore that, in a realistic ferromagnet, also the positions of the atoms are affected by a rotation). Although the underlying Hamiltonian is rotationally invariant, the groundstate is not in a singlet state and carries angular momentum. Hence one is dealing with a situation where the rotational symmetry is realized in a *spontaneously* broken way. This does *not* imply that rotational symmetry has no consequences anymore, but only that the most obvious implication of the symmetry is now absent. An important feature of a spontaneously broken realization is that the ground state must be *infinitely degenerate*. This is obvious: by applying (a continuous set of) symmetry transformations on a non-symmetric ground state, one constructs a continuous variety of different ground states. All these different states must have the same energy as the original one, because the Hamiltonian commutes with all the symmetry transformations of the theory. Indeed for a ferromagnet, an infinite set of ground states can be obtained by applying rotations to the magnet. These ground states can be characterized by the spatial orientation of the magnetization.

It is important to point out here that classical degeneracies do not necessarily survive in a quantum-mechanical context. Consider, for instance, a simple quantum-mechanical model where the classical potential has two abso-

Chapter 1

Quantum mechanics and path integrals

We shall begin our study of quantum field theory by learning about path integrals and path integral quantization. Path integrals (also sometimes called functional integrals) are an infinite-dimensional analogue of ordinary integrals, and so before learning about path integrals, we will first work through the corresponding derivatives, known as functional derivatives.

We will begin by studying functional derivatives and path integrals in quantum mechanics, where they were originally worked out. We will see that this will give a way of thinking about quantum mechanics from which one can derive Lagrangian classical mechanics as a limit.

1.1 Functional derivative

Let $x(t)$ be a function of one variable t. This could be the position of a point-particle along a line, as a function of time. We can define a function that depends upon $x(t)$ – such a quantity is known as a *functional* of $x(t)$. For example,

$$S[x(t)] = \int dt \left(\frac{dx}{dt}\right)^2$$

is a functional of $x(t)$.

We would like to define a derivative on the space of all functions $x(t)$. Such a derivative should vary the value of the function $x(t)$ at a single point, and not others. Let us denote such a derivative by $\delta/\delta x(t')$. From the property above, when $t \neq t'$, we need

$$\frac{\delta}{\delta x(t')} x(t) = 0$$

However, when $t = t'$, we need the derivative to be nonzero. In some sense, we'd want it to be

Discrete Physics using Metrized Chains

A. DiCarlo
Università Roma Tre
adicarlo@mac.com

F. Milicchio
Università Roma Tre
milicchio@dia.uniroma3.it

A. Paoluzzi
Università Roma Tre
paoluzzi@dia.uniroma3.it

V. Shapiro
University of Wisconsin
vshapiro@engr.wisc.edu

ABSTRACT

Over the last fifty years, there have been numerous efforts to develop from first principles a comprehensive discrete formulation of geometric physics, including Whitney's geometric integration theory, Tonti's work on unification of physical theories, research on mimetic discretization methods, discrete exterior calculus, and Harrison's theory of chainlets among others. All these approaches strive to separate physical models into standard topological, geometric, and physical components. While each of these components appear to be well understood, the effective computational connection between these three components is still lacking, leading to difficulties in combining, reconciling, and refining physical simulations. This paper proposes such a connection using metrized chains defined on a cell complex, an abstraction of a decomposition of a Riemannian manifold considering only topological-related properties, to establish a discrete metric structure on top of a discrete measure-theoretical structure, embodied in the underlying notion of measured (real-valued) chains.

The metric structure of the ambient space—be it Euclidean or Riemannian—carries basic information on the physical phenomena taking place on that scene. Therefore, it is vital that this structure be properly mimicked by discrete geometric models meant to be used for trustworthy physics-based simulations. The underlying cell complex endowed with a (discrete) measure-theoretical structure may be used to reproduce the measure-theoretical properties of the concrete mesh; refining or coarsening a mesh changes both topology and measure. Next, we establish a direct link between the discrete structure described by a chain complex and the Riemannian metric of the underlying manifold. To this end, we associate a local p-vector field with each elementary p-chain, and identify the inner product between two chains with the inner product between the corresponding multi-vectors.

By doing so, chains are identified with elements of their dual space, *i.e.*, cochains, in a way that mimics the metric of the approximated manifold. Moreover, boundary and coboundary operators—acting respectively on chains and cochains—may then be composed with each other, giving rise to physically meaningful Laplace-de Rham operators, an ubiquitous ingredient of physical modeling.

Categories and Subject Descriptors

I.3.5 [**Computational Geometry and Object Modeling**]: Physically based modeling; J.2 [**Physical Sciences and Engineering**]: Engineering

General Terms

Discrete calculus, Geometrical and physical modeling.

1. INTRODUCTION

The notion of a (finite) cell complex—which we take here for granted—abstracts the topological features of any reasonable computational mesh, stripping away all its extra-topological properties. A cell complex is thus an equivalence class of (geometrically different) meshes sharing the same topology, i.e., the same sets of cells of each dimension and the same incidence relations. By design, much of the information included in a concrete mesh is wiped out in the corresponding cell complex. The rest of the game consists in rebuilding layer after layer more-than-topological structures suited to the established discrete setting, *i.e.*, compatible with the underlying cell complex.

The first move is to change *cells* into *chains*, by attaching a value to each cell. Standard books on algebraic topology [14, 21] pick these values out of any commutative group, since this is the minimum apparatus enabling chain addition. This seems to be done for merely instrumental reasons: standard books talk of 'formal sums'. Our attitude, embryonically showed in [12], is different: we need a field of scalars, in order to be able not only to add, but also to scale chains. So, to us a chain complex is the vector space spanned via linear combination by unit chains, *i.e.*, chains attaching the unit value to a single cell and the null value to all the others. Thanks to the linear structure imparted to the set of chains, cochains naturally appear as linear forms on chains, *i.e.*, as elements of the algebraic dual of the space of chains. In this context, the boundary is a linear operator and the coboundary is its dual.

Moreover, we wish to impart size to cells. We are thus led to consider real-valued chains, attaching a signed p-measure

Timed Release Cryptography from Bilinear Pairings using Hash Chains

Konstantinos Chalkias[1] and George Stephanides[2]

Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece
[1] chalkias@java.uom.gr
[2] stephs@uom.gr

Abstract. We propose a new Timed Release Cryptography (TRC) scheme which is based on bilinear pairings together with an S/Key-like procedure used for private key generation. Existing schemes for this task, such as time-lock puzzle approach, provide an approximate release time, dependent on the recipients' CPU speed and the beginning time of the decryption process. Additionally, some other server-based schemes do not provide scalability and anonymity because the server is actively involved in the encryption or the decryption. However, there are already protocols based on bilinear pairings that solve most of the problems referred. Our goal is to extend and combine the existing protocols with desirable properties in order to create a secure, fast and scalable TRC scheme applied to dependent or sequential events. For this purpose we used continuous hashed time-instant private keys (hash chain) in the same way the S/Key system works. Our approach decreases dramatically the number of past time-instant private keys the server stores and only two keys are needed, the last one to construct the previous keys and the first one to recursively verify the authenticity of the next keys.

Keywords: Timed-Release Cryptography, bilinear pairings, S/Key, hash chains, sealed-bid auctions

1 Introduction

The essence of timed release cryptography (TRC) is to encrypt a message so that it cannot be decrypted by anyone, including the designated recipients, until a specific time-instance. This problem of "sending information into the future" was first mentioned by May [23] in 1993 and then discussed in detail by Rivest et al. [29]. Since its introduction, the solution to the TRC problem has been found useful in a number of real world applications. Some of the best examples are the e-voting which requires delayed opening of votes, the sealed-bid auctions in which the bids must stay sealed so that they cannot be opened before the bidding period and the Internet programming contest where participating teams cannot access the challenge problem before the contest starts. Moreover, TRC can be used for delayed verification of a signed document, such as lottery and check cashing [32] and it can also be applied to online games, especially card games, where players would be able to verify the authenticity of the result when the game ends.

Concepts of Scale

Instructor: K. McGarigal

Assigned Reading: Turner et al. 2001 (Chapter 2); Wiens (1989)

Objective: Provide a basic understanding of concepts related to scale to serve as a foundation for understanding landscape ecology topics. Clarify commonly misused terms and concepts. Highlight importance of considering scale in resource management planning and analyses.

Topics covered:
1. Scale in ecology
2. Components of scale
3. Why is scale important?
4. Characteristic scale
5. Scaling techniques
6. Dealing with scale

Comments: Some material taken from Wiens (1989), Turner et al. (2001), Rosenberg (2001) and Dean Urban's Landscape Ecology course notes, Duke University.

The unreasonable effectiveness of quantum theory: Logical inference approach

Hans De Raedt[1], Mikhail Katsnelson[2],

Hylke Donker[2] and Kristel Michielsen[3]

Quantum theory as the most robust description of reproducible experiments

Hans De Raedt[a], Mikhail I. Katsnelson[b], Kristel Michielsen[c,d,*]

Annals of Physics 347 (2014) 45–73

Quantum theory as a description of robust experiments: Derivation of the Pauli equation

Hans De Raedt[a], Mikhail I. Katsnelson[b], Hylke C. Donker[b], Kristel Michielsen[c,d,*]

Annals of Physics 359 (2015) 166–186

1 University of Groningen Zernike Institute for Advanced Materials

2 Radboud Universiteit

3 JÜLICH FORSCHUNGSZENTRUM

Capacity Theory and Cryptography

Ted Chinburg
joint work with Brett Hemenway,
Nadia Heninger and Zach Scherr

U.C. Irvine, Sept. 3, 2015

Cryptology for Beginners

Stu Schwartz
Wissahickon High
Ambler, Pa 19002
sschwartz8128@verizon.net
www.mastermathmentor.com

1. Introduction and Terminology 2

2. Monoalphabetic Substitution Ciphers 3

A. The Additive (or shift) Cipher 4

B. Modular Arithmetic 7

C. The Multiplicative Cipher 9

D. The Affine Cipher 12

3. Polyalphabetic Substitution Ciphers. 17

A. Integer Matrices 17

B. The Hill Digraph Cipher 20

C. The Hill Trigraph Cipher 32

D. The Vigenère Square Cipher 35

E. The Playfair Cipher 39

F. The Permutation Cipher 42

5. Deciding Between Monoalphabetic and Polyalphabetic. 44

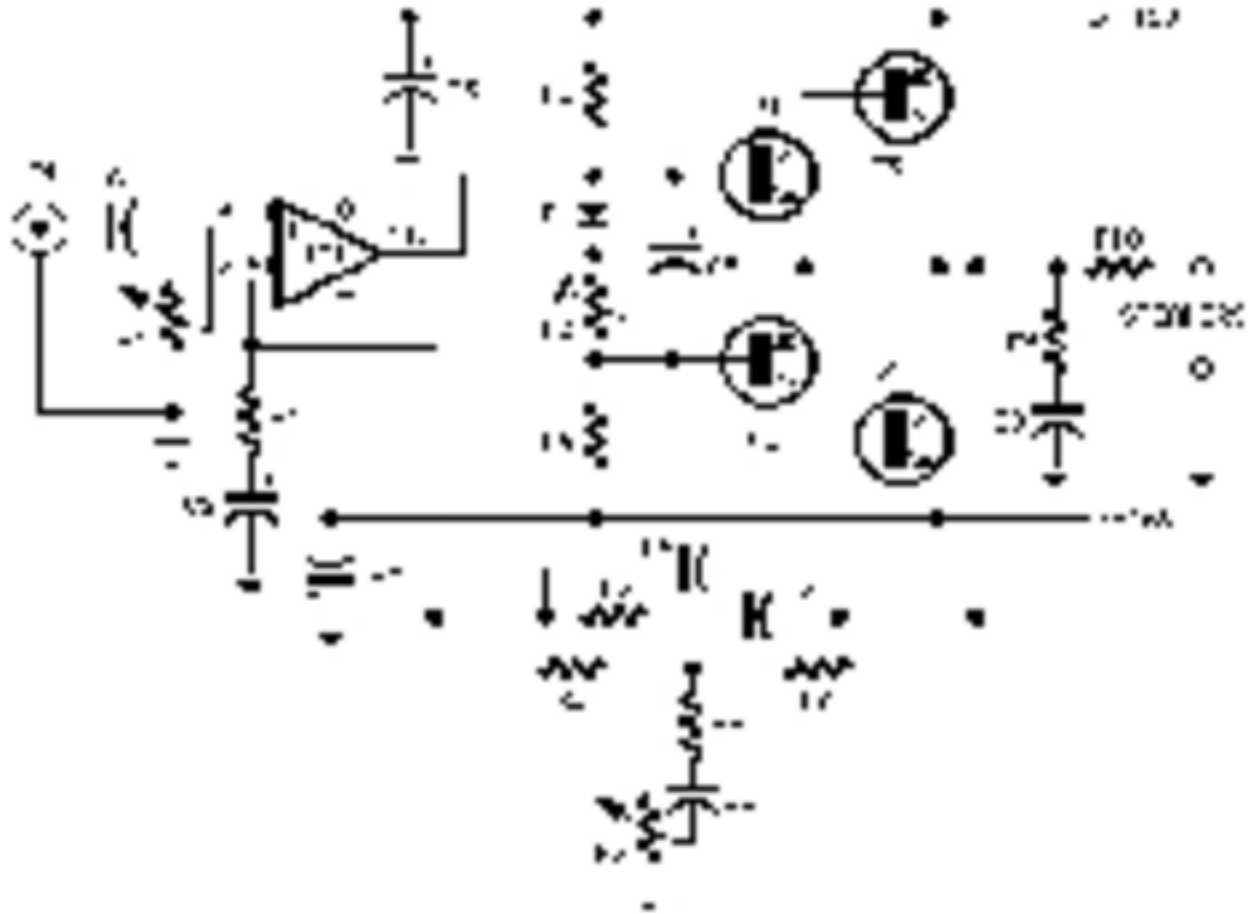
6. Public Key Cryptography 47

References 49

Answers to Exercises 49

This workbook requires the use of the Cipher System Excel spreadsheet. When opening the spreadsheet, be sure to enable macros.

CIRCUITS, CATEGORIES AND REWRITE RULES



John Baez & Brendan Fong

Higher-Dimensional Rewriting and Applications

Warsaw, 29 June 2015

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Who's Watching Little Brother?

A Checklist for Accountability in the Industry Behind Government Hacking

2 March 2017

Sarah McKune and Ron Deibert*

THECITIZENLAB

Towards a Quantum Geometry: Groupoids, Clifford algebras and Shadow Manifolds.

B. J. Hiley.

b.hiley@bbk.ac.uk

rv8: a high performance RISC-V to x86 binary translator

Michael Clark
The rv8 contributors
michaeljclark@mac.com

Bruce Hoult
The rv8 contributors
bruce@hoult.org

ABSTRACT

Dynamic binary translation has a history of being used to ease transitions between CPU architectures[7], including micro-architectures. Modern x86 CPUs, while maintaining binary compatibility with their legacy CISC instruction set, have internal micro-architectures that resemble RISC. High performance x86 micro-architectures have long used a CISC decoder front-end to crack complex instructions into smaller micro-operations. Recently macro-op fusion [17][6] has been used to combine several instructions into one micro-op. Both techniques change the shape of the ISA to match the internal µop micro-architecture. Well-known binary translators also use micro-op internal representations to provide an indirection between the source and target ISAs as this makes the addition of new instruction sets much easier.

We present rv8, a high performance RISC-V simulation suite containing a RISC-V JIT (Just In Time) translation engine specifically targeting the x86-64 instruction set. Achieving the best possible mapping from a given source to target ISA pair requires a purpose designed internal representation. This paper explores a simple and fast translation from RISC-V to x86-64 that exploits knowledge of the geometries of the source and target ISAs, ABIs, and current x86-64 micro-architectures with a goal of producing a near optimal mapping from the 31 register source ISA to the 16 register target ISA. Techniques are explored that exploit the CISC encoding to increase instruction density, coalescing micro-ops into CISC instructions with the goal of generating the minimum number of micro-ops at the target micro-architectural level.

CCS CONCEPTS

• **Computer systems organization** → **Reduced instruction set computing**; **Complex instruction set computing**;

KEYWORDS

dynamic binary translation, RISC, CISC

Reference Format:
Michael Clark and Bruce Hoult. 2017. rv8: a high performance RISC-V to x86 binary translator. *First Workshop on Computer Architecture Research with RISC-V*, Boston, MA, USA, October 2017 (CARRV 2017), 7 pages.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
CARRV 2017, October 2017, Boston, MA, USA
© 2017 Copyright held by the owner/author(s).

1 INTRODUCTION

RISC-V [20] is a modern, elegant and extensible open source instruction set architecture originally designed for computer architecture research. Similar to the Linux kernel two decades earlier in operating systems, RISC-V provides a standard and open base ISA and competitive reference hardware designs that anyone can freely use as-is or as a base for further innovation. This makes RISC-V uniquely suitable for the next phase of development in microprocessor hardware architectures much as the Linux kernel serves as the software foundation for embedded, mobile and server computing on a huge variety of CPU architectures and with a proliferation of operating systems such as Android, Tizen, Red Hat, Ubuntu, Fedora, Debian and many more.

Dynamic binary translation has frequently [7] [14] [2] [1] been used to provide binary compatibility for applications targeting legacy architectures during transitions to new architectures, however it can also be used to enable compatibility for binaries from newer architectures to allow for their execution on legacy hardware. Given x86 is the dominant architecture in cloud computing environments, dynamic binary translation provides a convenient means to enable RISC-V binary compatibility on existing hardware.

For binary translation to be acceptable as a mechanism to run RISC-V application images on legacy x86 hardware in the cloud, the performance must be similar to that of native code and there must be compelling advantages beyond performance, such as increased security [23]. While RISC-V is designed as an instruction set for hardware its features also make it an excellent platform abstraction for high performance virtualization. With this in mind, the goal of rv8 is to provide a binary translation platform that is able to achieve near native performance to enable secure RISC-V virtual machines in cloud computing environments.

Given Intel's and AMD's access to the latest process nodes[3], 4+ GHz clock speeds[22], superscalar execution, several dozen cores[15] and hundreds of GB of memory in a server, a near native speed RISC-V binary translator is likely to be the fastest RISC-V implementation and most practical build environment for things such as operating system distributions for some years to come.

2 PRINCIPLES

The rv8 binary translation engine has been designed as a hybrid interpreter and JIT compiler. The translator first interprets code and profiles it for hot paths [12]. Hot paths are then JIT translated to native code. The translation engine maintains a call stack to allow runtime inlining of hot functions. A jump target cache is used to accelerate returns and indirect calls through function pointers. The translator supports mixed binary translation and interpretation to handle instructions that do not yet have native translations. Currently, RISC-V 'IM' code is translated while 'AFD' is interpreted. The rv8 translator also supports RVC compressed code [19].

"*Special Functions in the 21st Century: Theory and Applications*"
Washington DC, April 2011

University of Kent

UNCLASSIFIED U.S. Department of State Case No. F-2011-03401 Doc No. C05457981 Date: 12/03/2013
Obtained by Judicial Watch, Inc. via FOIA

RELEASED IN FULL

MEMORANDUM OF UNDERSTANDING
December 12, 2008

This Agreement ("Agreement") is dated as of this 12th day of December, 2008 and entered into by and between the William J. Clinton Foundation (the Foundation), an Arkansas not-for-profit corporation, located at 1200 President Clinton Avenue, Little Rock, Arkansas (hereinafter referred to as "the Foundation"), and the Office of the President-Elect, a 501(c)(4) entity, located at 451 6th St., NW, Washington, DC (hereinafter referred to as "PTT").

WHEREAS, in considering Senator Clinton's potential service as Secretary of State, the Parties seek to ensure that the Foundation may continue its important philanthropic activities around the world, which do valuable and critical work in areas such as HIV/AIDS, climate change and economic development.

WHEREAS, the Parties also seek to ensure that the activities of the Foundation, however beneficial, do not create conflicts or the appearance of conflicts for Senator Clinton as Secretary of State.

WHEREAS the Parties have agreed to a set of protocols that would apply to the Foundation's activities to supplement any existing State Department protocols for managing conflicts of interests, and the appearance of conflicts of interest, as determined by the State Department's designated agency ethics official.

WHEREAS, the Parties seek to memorialize the mutually agreeable protocols related to the activities of the Foundation during the period in which Senator Hillary Clinton serves in the Obama Administration.

NOW, THEREFORE, it is hereby agreed as follows:

I. **Background on the Clinton Foundation**

A single entity, the William J. Clinton Foundation, is a 501(c)(3) charitable organization comprised of the Presidential Library and seven initiatives: the Clinton HIV/AIDS Initiative ("CHAI"), the Clinton Climate Initiative ("CCI"), the Clinton Hunter Development Initiative ("CHDI"), the Clinton Giustra Sustainable Growth Initiative ("CGSGI"), the Clinton Economic Opportunity Initiative ("CEO"), the Alliance for a Healthier Generation ("AHG"), and the Clinton Global Initiative ("CGI").

Over the past eight years, the Foundation has grown into a global nongovernmental organization with 1,100 staff and volunteers in more than 40 countries and with offices in New York, New York, Little Rock, Arkansas, Boston, Massachusetts, and other cities around the world. The Foundation, working in collaboration with governments and other partners, makes a significant impact in the lives of hundred of millions of people around the world: 1.4 million people living with HIV/AIDS now have access to lifesaving drugs

REVIEW AUTHORITY: Frank Tumminia, Senior Reviewer

UNCLASSIFIED U.S. Department of State Case No. F-2011-03401 Doc No. C05457981 Date: 12/03/2013

The Cell Method: an Enriched Description of Physics Starting from the Algebraic Formulation

E. Ferretti[1]

Abstract In several recent papers studying the Cell Method (CM), which is a numerical method based on a truly algebraic formulation, it has been shown that numerical modeling in physics can be achieved even without starting from differential equations, by using a direct algebraic formulation. In the present paper, our focus will be above all on highlighting some of the theoretical features of this algebraic formulation to show that the CM is not simply a new numerical method among many others, but a powerful numerical instrument that can be used to avoid spurious solutions in computational physics.

Keywords: Algebraic Formulation, Differential Formulation, Cell Method, Spurious Solutions, Nonlocality.

1 Introduction

From the onset of differential calculus, over three centuries ago [Newton (1687)], we have become accustomed to providing a differential formulation to each experimental law. Infinitesimal analysis has without doubt played a major role in the mathematical treatment of physics in the past, and will continue to do so in the future, but we must also be aware that, in using it, several important aspects of the phenomenon being described, such as its geometrical and topological features [Tonti (in press)] remain hidden. Moreover, applying the limit process introduces some limitations as regularity conditions must be imposed on the field variables. These regularity conditions, in particular those concerning differentiability, are the price we pay for using a formalism that is both very advanced and easy to manipulate.

Since the arrival of computers, differential equations have been discretized using one of various discretization methods (the finite element method FEM, the boundary element method BEM, the finite volume method FVM, the finite difference method FDM, etc.), since the numerical solution, which is no longer an exact solution, cannot be achieved for the most general case if a system of algebraic physical laws is not provided. Nevertheless, the very need to discretize the differential equations, in order to achieve a numerical solution, gives rise to the question of whether or not it is possible to formulate physical laws in an algebraic manner directly, through a direct algebraic formulation. We will see, in this paper, that this is possible and that a truly algebraic numerical method,

[1] DICAM – Department of Civil, Environmental and Materials Engineering, Scuola di Ingegneria e Architettura, Alma Mater Studiorum, Università di Bologna, Viale Risorgimento 2, 40136 (BO), ITALY.

Cohomology and Poincaré duality

Weiyi Zhang

Mathematics Institute, University of Warwick

December 18, 2013

14 Classic Counting Problems in Combinatorics

(Herbert E. Müller, May 2017, herbert-mueller.info)

Combinatorics is about counting objects, or the number of ways of doing something.

In this article I present some classic function counting problems. These include permutations of a set, compositions and partitions of a set or number, and (multi)arrangements and (multi-)combinations from a set.

I will repeatedly refer to OEIS (oeis.org): the Online Encyclopedia of Integer Sequences.

This article has two parts.

In the **first part** we consider selfmaps (N←N) of an n-set N. Starting with the problem of counting all selfmaps, we create new and more interesting problems in two ways:

1) Count bijective selfmaps (permutations) only.

2) Introduce an equivalence relation by conjugating the selfmaps with the permutation group: $S_n \circ (N \leftarrow N) \circ S_n^{-1}$; then count the equivalence classes.*

In this way we obtain 2×2=**4 counting problems involving selfmaps of a set**.

In the **second part** we consider functions (K←N) from an n-set N to a k-set K. Starting with the problem of counting all functions, there are again two ways to create new problems:

1) Count surjective functions only, or injective functions only.

2) Introduce an equivalence relation on the functions, and count the equivalence classes.

This is done with the permutation group S_n acting on N, or with S_k acting on K, or both.*

In this way we obtain 3×4=12 counting problems. 2 of these problems are trivial, and we are left with **10 counting problems involving functions from one set to another**.

*The equivalence class of a function f is the orbit of f under the action of a group.

Part 1: Permutations and general selfmaps

Here we consider selfmaps (N←N) of an n-set N = {a, b, c,...}.

We count all selfmaps, or bijective selfmaps (permutations) only, and the selfmaps, or the equivalence classes obtained by conjugation with the permutation group S_n.

Table: 2×2 selfmap counting problems & their solutions.

function/class	bijective		all	
N←N	permutations of an n-set	$n!$	selfmaps of an n-set	n^n
$S_n^{-1} \circ (N \leftarrow N) \circ S_n$	partitions of a number	$P(n)$	selfmap types of an n-set	A_{1372}

Permutations of a set and equivalence classes

The permutations of an n-set N={a, b, c, ...} form the symmetric group or permutation group S_n. Example: $\begin{bmatrix} a & b & c & d \\ a & c & d & b \end{bmatrix}$≡(a→a,b→c,c→d,d→b) is a permutation of the 4-set {a,b,c,d}.

A compact way of writing down a permutation is the cycle notation, in our example (bcd)(a). (bcd) is a cycle of length 3, meaning b→c,c→d,d→b; (a) is a cycle of length 1, meaning a→a. The cycle lengths listed in decreasing order form a partition of the number of elements of n, called the cycle type. The cycle type of the permutation (bcd)(a) is 3+1, or (3,1).

LABOUR HISTORY REVIEW, Vol. 76 No. 3, December, 2011, 184–206

Communists and the Inter-War Anti-Fascist Struggle in the United States and Britain

NIGEL COPSEY
Teesside University, UK

Published by Maney Publishing (c) The Society for the Study of Labour History

This article offers a comparison of the Communist anti-fascist experience in the United States and Britain in the inter-war period. The focus is on opposition to domestic fascism and the comparison extends across three areas, namely, respective analyses, organization, and political violence. This article demonstrates how both Communist parties initially understood fascism as a developing trend within bourgeois capitalist democracy before they, reflecting the Comintern's shift to the Popular Front, reworked their anti-fascism into different forms of democratic and progressive rhetoric. It places Communists at the forefront of anti-fascist campaigns in the US and Britain and yet, despite obvious transatlantic links, this article reveals that the organizational manifestations of their anti-fascism diverged significantly. The final section calls attention to the role of Communists in physical force anti-fascism, and reveals that Communist involvement in violent disturbances during the 1930s (if not the 1920s) appears more common in Britain than in the US. Nonetheless, it still cautions against making too much of physical confrontation as the single most important feature defining the British Communist anti-fascist experience.

KEYWORDS anti-fascism, CPGB, CPUSA, united front, popular front

Whilst there is an enormous literature on historic fascism, there is much less on anti-fascism, whether in its international or national contexts. This preoccupation with fascism means that the association between fascism and its opposition is insufficiently delineated. Fascism, even if we fail to agree on a precise definition, openly rejected the ideals of the democratic systems that had evolved over the course of the previous centuries. The historical significance of anti-fascism is that, regardless of whether it drew from Communist, Social Democratic, Liberal (or even Conservative) traditions, it claimed to stand for freedom, democracy, progress, and civilization.[1] Anti-fascism can therefore tell us much about the popular resilience or otherwise

© Society for the Study of Labour History 2011 DOI 10.1179/174581811x13139466815306

A Geometrically Defined Discrete Hodge Operator on Simplicial Cells

Bernhard Auchmann
CERN-AT-MEL
1211 Geneva 23, Switzerland
bernhard.auchmann@cern.ch

Stefan Kurz
Robert Bosch GmbH
60489 Frankfurt, Germany
stefan.kurz2@de.bosch.com

***Abstract*— Discrete electromagnetism (DEM) - in the authors' view - should be a self-consistent theory, mirroring the properties of the continuous electromagnetic theory in a discrete setting. Any recursion to continuous techniques can be interpreted as an inconsistency in the discrete theory.**

Recently, discrete Hodge operators on tetrahedra and triangles have been introduced that avoid the concepts of interpolation and integration of fields.

In this paper we introduce a geometrical definition of a discrete Hodge operator for general dimension n and degree p, $0 \leq n \leq 3$, $0 \leq p \leq n$. The definition generalizes definitions given in [8] and [9]. The increased level of abstraction allows for a short definition and a concise discussion of the properties of this operator.

I. Introduction

A discrete theory of electromagnetism (DEM) features discrete fields, discrete derivative operators and discrete material matrices or Hodge operators. Cell methods have proven to be a good starting point for the establishment of a DEM. They provide all of the above features based on an oriented cell complex (mesh, tesselation), representing a bounded n-dimensional spatial domain, $n = (0,)1, 2, 3$. In this paper we consider simplicial cell complexes (triangular or tetrahedral meshes). The discrete fields are coefficient vectors filled with the integral values of the respective fields over the cell complex' nodes, edges, faces or volumes, i.e., the coefficients have the physical dimension of a magnetic flux, electric voltage, electric charge or electric current. The derivative operators are represented by incidence matrices of oriented nodes and edges, $[\mathrm{D}^0]$, edges and faces $[\mathrm{D}^1]$ or faces and volumes $[\mathrm{D}^2]$. The discrete derivatives only rely on the topological properties of the complex. Metric proportions of the cell complex enter the DEM in the discrete Hodge operators.

There is no canonical way to define a discrete Hodge operator. Different choices lead to different numerical schemes. Most commonly, discrete Hodge operators on simplicial cells rely on an interpolation scheme from the discrete coefficients to continuous fields. One might argue, however, that a truely discrete operator should avoid in its definition any recourse to the continuous theory.

Recently, discrete Hodge operators on tetrahedra and triangles have been introduced that avoid the concepts of interpolation and integration of fields, [8], [9]. In this paper we introduce a generalization of the above-cited operators to arbitrary dimension n and degree p, $0 \leq n \leq 3$, $0 \leq p \leq n$. The algebraic properties of the operator are discussed.

Note that a geometrically defined operator exists on an orthogonal, brick-like cell complex; it is the material operator of the Finite Integration Technique (FIT), [11].

II. Discrete Hodge Operators on Simplicial Complexes

In what follows, we write matrices in brackets, coefficient vectors in curly braces, differential forms with an underbar and the space of differential p-forms on a domain Ω is denoted $\mathcal{F}^p(\Omega)$. The space of p-vectors is denoted $\mathcal{F}_p(\Omega)$, its elements are written in bold font. The upper index in a matrix, e.g., $[\mathrm{D}^p]\{F\}$, indicates that the matrix acts upon a discretization of a p-form $\underline{F}$. n_p denotes the number of p-cells in a cell complex; N_p is the number of p-cells in one n-cell. $\boldsymbol{g}_p$ will denote a p-vector.

Inner products are written as comma-seperated angle brackets, e.g., $\langle \boldsymbol{g}_p, \boldsymbol{g}_p \rangle$ denotes the inner product of two p-vectors. Duality products, i.e. covectors acting on vectors, are written $\langle \underline{F} \,|\, \boldsymbol{g}_p \rangle$.

A. Dual Cell Complex

Let C and $\tilde{C}$ be two cell complexes, one of which is endowed with an inner orientation. The two complexes are called *topologically dual* if each p-cell of C is related to one $(n-p)$-cell of $\tilde{C}$.[1] We call C the primal complex and $\tilde{C}$ the dual complex. For a dual complex we use the barycentric dual of the primal complex. An inner orientation of C induces an outer orientation of $\tilde{C}$ and vice versa. We denote with an overbar objects related to the dual complex and with an overtilde objects related to an outer oriented complex. The pair of a primal and a dual complex then reads $(C, \tilde{C})$ or $(\bar{C}, \tilde{C})$. The Ampère-Maxwell fields $\bar{\underline{D}}$, $\bar{\underline{B}}$, $\tilde{\underline{J}}$ and $\tilde{\underline{\mathcal{P}}}$ are discretized on the outer oriented complex, the Faraday fields $\underline{\mathcal{E}}$, $\underline{\mathcal{B}}$, $\tilde{\underline{E}}$ and $\tilde{\underline{H}}$ on the inner oriented complex. Generally, the Ampère-Maxwell fields are discretized on the dual complex. We can, thus, write the discrete Ampère law as $\{\tilde{\mathcal{J}}\} = [\tilde{\mathrm{D}}^1]\{\tilde{H}\}$ and the potential formulation of the magnetic flux as $\{\bar{B}\} = [\mathrm{D}^1]\{A\}$. Discrete Hodge operators establish discrete material laws, e.g., $\{\tilde{H}\} = [\mathrm{M}^1_{\nu,r}]\{B\}$.

[1] "Related" means that the intersection of any pair of a primal p-cell i and a dual $(n-p)$-cell j is either point for $i = j$ or empty for $i \neq j$.

One-complex-plane representation approach to continuous variable quantum teleportation

J. Janszky,[1] M. Koniorczyk,[1,2] and A. Gábris[1]
[1]*Department of Nonlinear and Quantum Optics, Research Institute for Solid State Physics and Optics, Hungarian Academy of Sciences, P.O. Box 49, H-1525 Budapest, Hungary*
[2]*Institute of Physics, University of Pécs, Ifjúság út 6, H-7624 Pécs, Hungary*

(Received 27 February 2001; revised manuscript received 8 May 2001; published 13 August 2001)

We formulate continuous variable quantum teleportation on a coherent-state basis. We present low-dimensional coherent state representation of the quadrature Bell states. This approach turns out to be suitable for investigating the teleportation process, yielding a simple direct description.

DOI: 10.1103/PhysRevA.64.034302 PACS number(s): 03.67.Hk, 03.65.Ud, 42.50.Dv

The description of entangled states and the analysis of their applications has attracted a great deal of attention in quantum optics recently. One of the main motivations of this trend was the quantum teleportation phenomenon, which was originally introduced by Bennett [1]. The idea of continuous variable teleportation appeared quite soon after Bennett's original paper is a work by Vaidman [2], but this idea was put into the framework of quantum optics by Braunstein and Kimble quite a bit later than the discrete schemes [3]. However, first experimental realizations of discrete and continuous variable teleportation appeared quite simultaneously in both cases [4,5].

The formulation of Braunstein and Kimble in Ref. [3] utilizes the Wigner-function formalism. Their scheme may also be described in terms of either wave functions on a quadrature-state basis [6,7] or Fock states [8,7]. A general covariant description in terms of arbitrary canonically conjugate observables and their eigenstates is also possible [9].

Coherent states have proven to be extremely useful in quantum optics of single mode field. The overcompleteness of the coherent state basis allows us to introduce representations in lower dimensional, or even discrete, subspaces of the phase space [10–12]. A similar approach may be fruitful in the investigation of entangled multimode fields and their applications. In this paper we will show that teleportation can be treated in this manner: the process can be understood describing entangled states with coherent state integrals.

In what follows we consider the actual teleportation scheme of Braunstein and Kimble under ideal circumstances. The physical systems under consideration are single mode fields. As entangled states, we consider ideal Einstein-Podolsky-Rosen pairs obtained from squeezed vacuum in infinite squeezing limit, and perfect detection of quadrature amplitudes, which results in a projection onto quadrature eigenstates, according to the von Neumann principle. We also outline the effect of finite squeezing.

This paper is organized as follows. Using a one-dimensional representation of quadrature eigenstates, we obtain a one-complex-plane representation of the two mode entangled states playing an important role in teleportation. Then the description of continuous variable teleportation is provided.

Local measurements of a given field mode in the scheme under consideration are carried out by detectors measuring the value of either of the quadratures

$$\hat{x}=\frac{\hat{a}+\hat{a}^\dagger}{2},\quad \hat{p}=\frac{\hat{a}-\hat{a}^\dagger}{2i}. \tag{1}$$

According to the von Neumann projection principle, the measurement results in the projection to one of the eigenstates,

$$\hat{x}||X\rangle=X||X\rangle,\quad \hat{p}||P\rangle=P||P\rangle \tag{2}$$

depending on the measurement result, which is the value X or P, respectively. (The symbol $||\cdots\rangle$ denotes quadrature eigenstates.)

The Bell-state detector of the teleportation scheme in argument consists of an $\hat{x}$ detector and a $\hat{p}$ detector, combined with a beam splitter to convert two local quadrature measurements to a joint measurement on two modes. The whole apparatus then projects onto an entangled state of the two modes, the quadrature the Bell states, depending on the values X and P, measured.

With this picture in mind we construct the one-dimensional representation of quadrature eigenstates. (The word dimension stands for real, and not for complex dimension throughout this paper.) Let kets containing a single number denote coherent states. We start with the following states [10]:

$$|\text{Sq. vac. } p\rangle=\mathcal{N}(r)\int_{-\infty}^{\infty}dx G_r(x)|x\rangle,$$

$$|\text{Sq. vac. } x\rangle=\mathcal{N}(r)\int_{-\infty}^{\infty}dy G_r(y)|iy\rangle, \tag{3}$$

where

$$\mathcal{N}(r)=\frac{1}{\sqrt{\pi}}\frac{e^{r/2}}{\sqrt{e^{2r}-1}},\quad \text{and}\quad G_r(x)=e^{-(1/2)x^2(e^{2r}-1)}. \tag{4}$$

These are superpositions of coherent states placed on the real and imaginary axis of the phase space, respectively. It is straightforward to show that the mean values of the quadratures are 0, and for their variances

 ©2001 The American Physical Society

Coppersmith's Theorem

Background, Generalizations, and Applications

Joshua Hill

Department of Mathematics
University of California, Irvine

Number Theory Seminar
2010-Oct-07 and 2010-Oct-21
http://bit.ly/CuSmith

Chapter 3

Linear Algebra In Dirac Notation

3.1 Hilbert Space and Inner Product

In Ch. 2 it was noted that quantum wave functions form a linear space in the sense that multiplying a function by a complex number or adding two wave functions together produces another wave function. It was also pointed out that a particular quantum state can be represented either by a wave function $\psi(x)$ which depends upon the position variable x, or by an alternative function $\tilde{\psi}(p)$ of the momentum variable p. It is convenient to employ the Dirac symbol $|\psi\rangle$, known as a "ket", to denote a quantum state without referring to the particular function used to represent it. The kets, which we shall also refer to as *vectors* to distinguish them from *scalars*, which are complex numbers, are the elements of the quantum Hilbert space $\mathcal{H}$. (The real numbers form a subset of the complex numbers, so that when a scalar is referred to as a "complex number", this includes the possibility that it might be a real number.)

If α is any scalar (complex number), the ket corresponding to the wave function $\alpha\psi(x)$ is denoted by $\alpha|\psi\rangle$, or sometimes by $|\psi\rangle\alpha$, and the ket corresponding to $\phi(x) + \psi(x)$ is denoted by $|\phi\rangle + |\psi\rangle$ or $|\psi\rangle + |\phi\rangle$, and so forth. This correspondence could equally well be expressed using momentum wave functions, because the Fourier transform, (2.15) or (2.16), is a linear relationship between $\psi(x)$ and $\tilde{\psi}(p)$, so that $\alpha\phi(x) + \beta\psi(x)$ and $\alpha\tilde{\phi}(p) + \beta\tilde{\psi}(p)$ correspond to the same quantum state $\alpha|\psi\rangle + \beta|\phi\rangle$. The addition of kets and multiplication by scalars obey some fairly obvious rules:

$$\begin{gathered}\alpha\big(\beta|\psi\rangle\big) = (\alpha\beta)|\psi\rangle, \quad (\alpha+\beta)|\psi\rangle = \alpha|\psi\rangle + \beta|\psi\rangle, \\ \alpha\big(|\phi\rangle + |\psi\rangle\big) = \alpha|\phi\rangle + \alpha|\psi\rangle, \quad 1|\psi\rangle = |\psi\rangle.\end{gathered} \tag{3.1}$$

Multiplying any ket by the number 0 yields the unique *zero vector* or *zero ket*, which will, because there is no risk of confusion, also be denoted by 0.

The linear space $\mathcal{H}$ is equipped with an *inner product*

$$\mathcal{I}\big(|\omega\rangle, |\psi\rangle\big) = \langle\omega|\psi\rangle \tag{3.2}$$

which assigns to any pair of kets $|\omega\rangle$ and $|\psi\rangle$ a complex number. While the Dirac notation $\langle\omega|\psi\rangle$, already employed in Ch. 2, is more compact than the one based on $\mathcal{I}\big(,\big)$, it is, for purposes of exposition, useful to have a way of writing the inner product which clearly indicates how it depends on two different ket vectors.

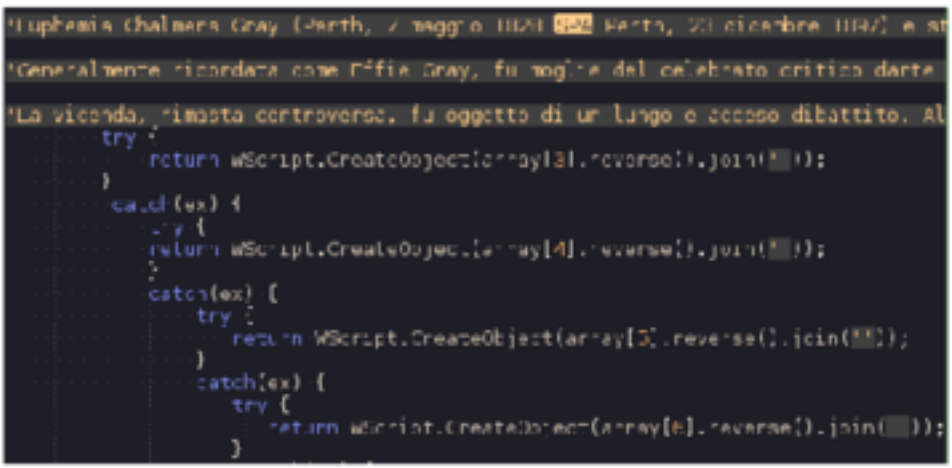
New Cyberattack wave is launched using official web site of the accounting software developer «Crystal Finance Millennium»

During ISSP Labs daily threat activity monitoring a new virus distribution campaign with a unique malware sample was discovered.

This sample (named "док.zip") is a text file with embedded JavaScript code.

The script executes the role of a downloader, which main objective is to download and launch an executable file.

In order to avoid cyber threats detection systems, the content of the script is obfuscated using comments, which contain text and special symbols.



This report is a property of ISSP – Information Systems Security Partners and shall not be duplicated, distributed or otherwise disseminated as a whole report without prior written consent from ISSP. Reference to ISSP – Information Systems Security Partners is mandatory in case of quoting each and any part of this report.

CSC MyWorkStyle™
VIRTUAL DESKTOP AND APPLICATIONS

DO YOU ...

- Need to provide a more productive desktop environment to your employees and contractors with a better user experience?
- Struggle to manage desktop provisioning to contractors or seasonal workers?
- Find it increasingly difficult to manage desktops at remote office locations or for an increasingly mobile workforce?

WOULD YOU LIKE TO ...

- Deliver a more consistent desktop experience to your workforce?
- Lower the cost of desktop provisioning, lower CAPEX requirements, gain greater certainty of ongoing costs and drive a Bring Your Own Device (BYOD) strategy?
- Improve security and compliance by keeping your data safe within data centers and not resident on end user devices?

IMAGINE IF YOU COULD ...

Allow your workforce access to your applications and data from any device, from any location with improved security while providing an improved user experience. With CSC MyWorkStyle Virtual Desktop and Applications, you can!

This offering is made possible through collaboration with our CSC Alliance Partner Ecosystem — Microsoft, VMware, Citrix, Avecto, ServiceNow Inc., AppSense and AT&T.

*Compatible device and adequate network coverage required

WHY GO TO YOUR PHYSICAL DESKTOP WHEN YOUR "DESKTOP" CAN GO EVERYWHERE WITH YOU?

To succeed in today's mobile world, a workforce requires access to globally connected communities. Workers need integrated collaboration tools with access to real-time information to make informed decisions from any device over any network. They require freedom and flexibility to maximize their productivity from any location. For service delivery excellence, it is essential that workers have the right tools to improve job performance and customer satisfaction.

With CSC MyWorkStyle™ Virtual Desktop and Applications you can transform and modernize your workplace by mobilizing workers who have traditionally worked in offices. Our solutions enable location independence and flexibility by transforming a traditional desktop into a virtual desktop that can be accessed securely over the Internet — anytime, anywhere, with any device.*

Having problems providing desktop capability to seasonal or contract workers or providing access to your systems to outsourcing partners? No problem — with CSC MyWorkStyle Virtual Desktop and Applications you can quickly provide them with virtual desktop capability, flexing capacity according to business demand, and safe in the knowledge your data remains secure.

CSC MyWorkStyle Virtual Desktop and Applications replaces the traditional processor, storage, operating systems, applications and user settings of your physical desktop with a more reliable, always-on data center or cloud-based solution. By untethering your data and applications from your physical desktop, you can securely access them from a wide range of devices, including smartphones, tablets, laptops, Apple® Mac® and zero or thin clients.

DESKTOP OPTIONS

We offer a range of desktop types, each with multiple power and deployment options. This ensures you can deliver to your users a desktop experience that matches their workstyle and productivity needs and meets your security and compliance requirements, all at optimal cost.

Published Applications

We can virtualize and host published applications, where characteristics permit, on a shared Windows Server® Virtual Machine, thereby providing access to shared applications from any compatible device.

Hosted Shared Desktop

The hosted shared desktop provides a basic desktop suitable for most use cases and is the most cost-effective of our solutions for general needs.

Supporting either Windows Server 2008 R2 or 2012 R2 Remote Desktops, users get a hosted, shared virtual desktop with the look and feel of Windows® 7 or 8.1 while using fewer resources than a full Windows Desktop Virtual Machine.

Non-persistent Desktop

For more advanced needs or where users rely on applications incompatible with a shared virtual environment, our non-persistent desktop is the answer. Running a full version of Windows 7, 8.1 or 10, users are allocated a desktop from a pool at logon, which is dedicated to that user during the work session.

This offers improved user experience and efficiency, as the pool of desktops operates from a single image, promoting consistency.

Users cannot install additional applications. Our optional user profile services allow the majority of user settings to be preserved between sessions.

You Can't Stay Here: The Efficacy of Reddit's 2015 Ban Examined Through Hate Speech

ESHWAR CHANDRASEKHARAN, Georgia Institute of Technology
UMASHANTHI PAVALANATHAN, Georgia Institute of Technology
ANIRUDH SRINIVASAN, Georgia Institute of Technology
ADAM GLYNN, Emory University
JACOB EISENSTEIN, Georgia Institute of Technology
ERIC GILBERT, University of Michigan

In 2015, Reddit closed several subreddits—foremost among them r/fatpeoplehate and r/CoonTown—due to violations of Reddit's anti-harassment policy. However, the effectiveness of banning as a moderation approach remains unclear: banning might diminish hateful behavior, or it may relocate such behavior to different parts of the site. We study the ban of r/fatpeoplehate and r/CoonTown in terms of its effect on both participating users and affected subreddits. Working from over 100M Reddit posts and comments, we generate hate speech lexicons to examine variations in hate speech usage via causal inference methods. We find that the ban *worked for Reddit*. More accounts than expected discontinued using the site; those that stayed drastically decreased their hate speech usage—by at least 80%. Though many subreddits saw an influx of r/fatpeoplehate and r/CoonTown "migrants," those subreddits saw no significant changes in hate speech usage. In other words, other subreddits did not inherit the problem. We conclude by reflecting on the apparent success of the ban, discussing implications for online moderation, Reddit and internet communities more broadly.

CCS Concepts: • **Human-centered computing** → *Empirical studies in collaborative and social computing*;

Additional Key Words and Phrases: online communities, hate speech, moderation, banning, causal inference.

ACM Reference format:
Eshwar Chandrasekharan, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert. 2017. You Can't Stay Here: The Efficacy of Reddit's 2015 Ban Examined Through Hate Speech. *Proc. ACM Hum.-Comput. Interact.* 1, 2, Article 31 (November 2017), 22 pages.
https://doi.org/10.1145/3134666

1 INTRODUCTION

Reddit is organized into over one million[1] user-created and user-moderated communities known as *subreddits*. Alongside mainstream subreddits for discussing scientific discoveries (r/science) and affordable fashion choices (r/frugalmalefashion), Reddit has also seen an increase in "toxic" subreddits—subreddits that exist to target hate speech at certain groups [20]. In response, the site introduced a new anti-harassment policy in 2015 [35]. On June 10, 2015, Reddit took action, announcing that it would ban several subreddits under the new policy [17]. Among them were two

[1] http://redditmetrics.com/history

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2017 Copyright held by the owner/author(s). Publication rights licensed to Association for Computing Machinery.
2573-0142/2017/11-ART31
https://doi.org/10.1145/3134666

Which Curie's Principle?

Elena Castellani[*] and Jenann Ismael[†]

June 2015

Since its first formulation in a famous 1894 article by Pierre Curie, the principle stating that "the symmetries of the causes are to be found in the effects" has been defended or questioned on diffferent grounds. In recent decades, it has become the object of renewed philosophical discussion in connection with the growing interest in the role of symmetry and symmetry breaking in physics (Ismael, 1997; Belot, 2003; Earman, 2004; Roberts 2013). In this literature, it has become current to understand (and question) the principle as following from the invariance properties of deterministic physical laws. The seminal paper for this "received view" is Chalmers (1970), introducing a formulation of Curie's principle in terms of the relationship between the symmetries of earlier and later states of a system and the dynamical law connecting these states. This re-formulation places the emphasis in a different place with respect to Curie. Curie's focus was clearly on the case of co-existing, functionally related features of a system's state, rather than temporally ordered cause and effect pairs. While Chalmers (1970) and Ismael (1997) still emphasize the generality of the principle by including in their formulations physical situations of the type considered by Curie, this is no more the case in what has become the received view.

Is there more that one "Curie's principle", then? How far are different formulations legitimate? Given the important and widely acknowledged methodological role of the principle in science, are there features to be highlighted and used for a modern formulation? What are the aspects that make it so scientifically fruitful, independently of how it is formulated?

[*]Department of Letters and Philosophy, University of Florence, via Bolognese 52, 50139, Firenze, Italy.

[†]Department Philosophy, University of Arizona and Center for Advanced Studies in the Behavioral Sciences, Stanford University, 75 Alta Rd., 94305.

CYBERCRIME AND CYBERSECURITY BILL, 2017

_____

_____

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

Section

1.Short title and commencement.

2.Objects of Act.

3.Interpretation.

PART II

ESTABLISHMENT OF CYBERSECURITY CENTRE

4.Establishment of Cybersecurity Centre.

5.Committee on Cybersecurity.

PART III

OFFENCES RELATING TO COMPUTER SYSTEMS, COMPUTER DATA, DATA STORAGE MEDIUMS, DATA CODES AND DEVICES

6.Unlawful access.

7.Unlawful interception of data.

8.Unlawful acquisition of data.

9.Unlawful interference with data or data storage medium.

10.Unlawful interference with computer system.

11.Unlawful disclosure of data code.

12.Unlawful use of data or devices.

13.Aggravating circumstances.

PART IV

OFFENCES RELATING TO ELECTRONIC COMMUNICATIONS AND MATERIALS

14.Transmission of data message inciting violence damage to property.

15.Sending threatening data message.

16.Cyber-bullying and harassment.

17.Transmission of false data message intending to cause harm.

18.Spam.

19.Transmission of intimate images without consent.

20.Production and dissemination of racist and xenophobic materials.

PART V

2017

9th International Conference on Cyber Conflict:

Defending the Core

H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)

CCDCOE

IEEE Advancing Technology for Humanity

30 MAY - 02 JUNE 2017, TALLINN, ESTONIA

The Autonomous Systems Laboratory
Universidad Politécnica de Madrid

To cognize is to categorize revisited: Category Theory is where Mathematics meets Biology

Jaime Gómez and Ricardo Sanz
Universidad Politécnica de Madrid,
José Gutiérrrez Abascal, 2. Madrid 28006 Spain
jd.gomez@upm.es

ASLab v 0.0 Draft
October 20, 2009

This paper claims for a shift towards "the formal sciences" in the cognitive sciences. In order to explain the phenomenon of cognition, including aspects such as learning and intelligence, it is necessary to explore the concepts and methodologies offered by the formal sciences. In particular, category theory is proposed as the most fitting tool for the building of an unified theory of cognition.

This paper proposes a radically new view based in category theory. A cognitive model is *informally* defined as a mapping between two different structures, while a structure is the set of components of a system and their relationships.

Put *formally* in categorical terms, a model is a functor between categories that reflects the structural invariance between them.

In the paper, the theory of categories is presented as the best possible framework to deal with complex system modeling -ie: biologically inspired systems that transcend and offer a much more powerful tool kit to deal with the phenomenon of cognition that other purely verbal tools like the psychological categories that Rosch or Hamad refer.

I got 99 trend's and a # is all of them!

How we found over ~~100~~ 200+ RCE vulnerabilities in Trend Micro software

NSA Playset: Bluetooth Smart

A presentation in five acts

Mike Ryan

iSEC Partners

Hack In The Box Malaysia

October 16, 2014

A SCALABLE FULLY IMPLICIT COMPRESSIBLE EULER SOLVER FOR MESOSCALE NONHYDROSTATIC SIMULATION OF ATMOSPHERIC FLOWS*

CHAO YANG† AND XIAO-CHUAN CAI‡

Abstract. A fully implicit solver is developed for the mesoscale nonhydrostatic simulation of atmospheric flows governed by the compressible Euler equations. To spatially discretize the Euler equations on a height-based terrain-following mesh, we apply a cell-centered finite volume scheme, in which an AUSM$^+$-up method with a piecewise linear reconstruction is employed to achieve second-order accuracy for the low-Mach flow. A second-order ESDIRK method with adaptive time stepping is applied to stabilize physically insignificant fast waves and accurately integrate the Euler equations in time. The nonlinear system arising at each time step is solved by using a Jacobian-free Newton-Krylov-Schwarz algorithm. To accelerate the convergence and improve the robustness, we employ a class of additive Schwarz preconditioners in which the subdomain Jacobian matrix is constructed using a first-order spatial discretization. Several test cases are used to validate the correctness of the scheme and examine the performance of the solver. Large-scale results on a supercomputer with up to 18,432 processor cores are provided to show the parallel performance of the proposed method.

Key words. fully implicit method, Newton-Krylov-Schwarz, nonhydrostatic model, compressible Euler equations, parallel scalability

AMS subject classifications. 65Y05, 65M55, 65F08, 86A10, 35L65

1. Introduction.

The atmosphere contains multiscale dynamics that support a variety of wave motions. Fast waves, such as the acoustic wave and the inertial-gravity wave, often impose restrictive time step constraints for explicit schemes. To deal with the rapidly traveling, physically insignificant fast waves, one can either (i) simplify the governing equations based on, e.g., a hydrostatic, an incompressible or an anelastic assumption; or (ii) employ a more advanced time integration scheme with a weaker stability requirement. In the first approach, the compressible Euler equations are replaced with simplified ones that are often easier to solve in an explicit manner because certain fast waves are filtered out. For example, when the hydrostatic primitive equations are employed, the atmosphere is assumed to be in vertical balance and, as a result, is free of the internal acoustic mode. However, the hydrostatic assumption becomes invalid when the horizontal scale is smaller than about 10 km. Even for other simplified equations that might be more accurate than the hydrostatic primitive equations, it is still not clear if they are valid for all scales [20, 43]. Therefore, when high resolution is of interest as in mesoscale and cloud-resolving atmospheric simulations, fast and efficient solution of the fully compressible Euler equations becomes desirable.

The second approach to stabilize fast waves is to make use of a more advanced time integration scheme, which is usually based on either (i) modifying a fully explicit scheme to increase the maximum allowable time step size; or (ii) reducing the cost of a fully implicit scheme. In this study, we focus on the latter method and only briefly mention some examples of the former one, such as the split-explicit method [13, 21],

* This work was supported in part by NSF grants DMS-0913089 and CCF-1216314. The first author was also supported in part by NSFC grants 61170075, 91130023 and 61120106005, and by 973 Program of China 2011CB309701.

† Institute of Software, Chinese Academy of Sciences, Beijing 100190, China and State Key Laboratory of High Performance Computing, Changsha 410073, China (yangchao@iscas.ac.cn).

‡ Department of Computer Science, University of Colorado Boulder, Boulder, CO 80309, USA (cai@cs.colorado.edu).

entrepreneurship and innovation

HEC ULg
Ecole de Gestion de l'Université de Liège

CAHIER DE RECHERCHE / WORKING PAPER

Anticipatory Artificial Autopoiesis

Daniel M. Dubois and Stig C. Holmberg

January 2010 / N° 201001/02

The discrete logarithm problem on elliptic curves and descents

José Felipe Voloch

The purpose of this note is to relate the discrete logarithm problem (DLP) on elliptic curves to descents and compare our approach to others in the literature. Let G be a group. The DLP for G is to find an procedure so that, given $P, Q \in G$ one finds an integer m with $Q = mP$ or shows that m does not exist. The name discrete logarithm problem comes from the special case where G is the multiplicative group of a finite field. If the DLP on a group is computationally hard then one can use this to construct a cryptosystem ([E],[Ko],[M]). Again the classical case is of the multiplicative group of a finite field but also the group of points on an elliptic curve over a finite field has been considered. The latter is supposed to be harder than the former. Basically there has been two developments in trying to solve the DLP on elliptic curves. First Menezes, Okamoto and Vanstone [MOV] showed that if E is an elliptic curve over $\mathbf{F}_q$ of characteristic p such that p does not divide $N = \#E(\mathbf{F}_q)$, then DLP on $E(\mathbf{F}_q)$ can be reduced to the DLP on the multiplicative group of an extension of $\mathbf{F}_q$ and, if this extension is of low degree then the DLP on $E(\mathbf{F}_q)$ is as hard as the DLP on $\mathbf{F}_q^*$. This will happen if N has a large factor in common with $q^r - 1$ for some small r. The approach of Menezes, Okamoto and Vanstone has been generalized by Frey and Rück [FR] where it is cast in terms of Tate pairings, but for that they need to lift the curve to a p-adic ring. We will show that this is not necessary and give a simplified version of their approach. Very recently it was announced that Semaev [Se], Smart [S] and Satoh and Araki [SA] gave a solution of the DLP on elliptic curves over $\mathbf{F}_p$ with p points, p a prime. In this note we will recover these results using descents and extend it also to the case where $E(\mathbf{F}_q)$ has a large subgroup of order a power of p, for arbitrary q. For the prime to p case our approach is related to that of Menezes, Okamoto and Vanstone, for the p-part it is related to Semaev's (see also Rück [R]) but is very different from Smart's and Satoh and Araki's, although we will study the relation between these approaches also. The unifying theme of our approach is the old technique of descents on elliptic curves.

A Coding-Theoretic Approach to Cryptanalysis

Dissertation Thesis

by

Alexander Meurer
November 2012

Last modified 26.06.2013

Discrete Differential Forms for Computational Modeling

Mathieu Desbrun Eva Kanso* Yiying Tong†
Applied Geometry Lab
Caltech‡

1 Motivation

The emergence of computers as an essential tool in scientific research has shaken the very foundations of differential modeling. Indeed, the deeply-rooted abstraction of smoothness, or *differentiability*, seems to inherently clash with a computer's ability of storing only finite sets of numbers. While there has been a series of computational techniques that proposed discretizations of differential equations, the geometric structures they are simulating are often lost in the process.

1.1 The Role of Geometry in Science

Geometry is the study of space and of the properties of shapes in space. Dating back to Euclid, models of our surroundings have been formulated using simple, geometric descriptions, formalizing apparent *symmetries* and experimental *invariants*. Consequently, geometry is at the foundation of many current physical theories: general relativity, electromagnetism (E&M), gauge theory as well as solid and fluid mechanics all have strong underlying geometrical structures. Einstein's theory for instance states that gravitational field strength is directly proportional to the *curvature of space-time*. In other words, the physics of relativity is *directly modelled* by the shape of our 4-dimensional world, just as the behavior of soap bubbles is modeled by their shapes. Differential geometry is thus, *de facto*, the mother tongue of numerous physical and mathematical theories.

Unfortunately, the inherent geometric nature of such theories is often obstructed by their formulation in vectorial or tensorial notations: the traditional use of a coordinate system, in which the defining equations are expressed, often obscures the underlying structures by an overwhelming usage of indices. Moreover, such complex expressions entangle the topological and geometrical content of the model.

1.2 Geometry-based Exterior Calculus

The geometric nature of these models is best expressed and elucidated through the use of the *Exterior Calculus of Differential Forms*, first introduced by Cartan [Cartan 1945]. This geometry-based calculus was further developed and refined over the twentieth century to become the foundation of modern differential geometry. The calculus of exterior forms allows one to express differential and integral equations on smooth and curved spaces in a consistent manner, while revealing the geometrical invariants at play. For example, the classical operations of gradient, divergence, and curl as well as the theorems of Green, Gauss and Stokes can all be expressed concisely in terms of differential forms and an operator on these forms called the exterior derivative—hinting at the generality of this approach.

Compared to classical tensorial calculus, this exterior calculus has several advantages. First, it is often difficult to recognize the coordinate-independent nature of quantities written in tensorial notation: local and global invariants are hard to notice by just staring at the indices. On the other hand, invariants are easily discovered when expressed as differential forms by invoking either Stokes' theorem, the Poincaré lemma, or by applying exterior differentiation. Note also that the exterior derivative of differential forms—the antisymmetric part of derivatives—is one of the most important parts of differentiation, since it is invariant under coordinate system change. In fact, Sharpe states in [Sharpe 1997] that every differential equation may be expressed in term of the exterior derivative of differential forms. As a consequence, several recent initiatives have been aimed at formulating physical laws in terms of differential forms. For recent work along these lines, the reader is invited to refer to [Burke 1985; Abraham et al. 1988; Lovelock and Rund 1993; Flanders 1990; Morita 2001; Carroll 2003; Frankel 2004] for books offering a theoretical treatment of various physical theories using differential forms.

1.3 Differential vs. Discrete Modeling

We have seen that a large amount of our scientific knowledge relies on a deeply-rooted differential (*i.e.*, smooth) comprehension of the world. This abstraction of differentiability allows researchers to model complex physical systems via concise equations. With the sudden advent of the digital age, it was therefore only natural to resort to computations based on such differential equations.

However, since digital computers can only manipulate finite sets of numbers, their capabilities seem to clash with the basic foundations of differential modeling. In order to overcome this hurdle, a first set of computational techniques (*e.g.*, finite difference or particle methods) focused on satisfying the continuous equations at a discrete set of spatial and temporal samples. Unfortunately, focusing on accurately discretizing the local laws often fails to respect important global structures and invariants. Later methods such as Finite Elements (FEM), drawing from developments in the calculus of variations, remedied this inadequacy to some extent by satisfying local conservation laws on average and preserving some important invariants. Coupled with a finer ability to deal with arbitrary boundaries, FEM became the de facto computational tool for engineers. Even with significant advances in error control, convergence, and stability of these finite approximations, the underlying structures of the simulated continuous systems are often destroyed: a moving rigid body may gain or loose momentum; or a cavity may exhibit fictitious eigenmodes in an electromagnetism (E&M) simulation. Such examples illustrate some of the loss of fidelity that can follow from a standard discretization process, failing to preserve some fundamental geometric and topological structures of the underlying continuous models.

The cultural gap between theoretical and applied science communities may be partially responsible for the current lack of proper discrete, computational modeling that could mirror and leverage the rich developments of its differential counterpart. In particular, it is striking that the calculus of differential forms has not yet had an impact on the mainstream computational fields, despite excellent initial results in E&M [Bossavit 1998] or Lagrangian mechanics [Marsden and West 2001]. It should also be noticed that

*Now at the University of Southern California.
†Now at Michigan State University.
‡E-mail: {mathieu|eva|yiying}@caltech.edu

STRUCTURES FOR SOCIAL ENTERPRISES

When setting up your social enterprise it is important to have the right legal structure.

From this flowchart, comparison table and detailed guidance you will be able to assess which is the right legal structure for your social enterprise

For further information visit

www.gov.uk/set-up-a-social-enterprise
www.gov.uk/business-legal-structures
www.companieshouse.gov.uk

DLA Piper has produced these helpsheets as part of a collaborative project with UnLtd. DLA Piper is one of the largest business law firms in the world with an extensive pro bono legal advice programme which assists social enterprises, charities and individuals across the globe. UnLtd is the leading provider of support to social entrepreneurs in the UK and offers the largest such network in the world.

London Mathematical Society ISSN 1461–1570

THE EQUIVALENCE BETWEEN THE DHP AND DLP FOR ELLIPTIC CURVES USED IN PRACTICAL APPLICATIONS

A. MUZEREAU, N.P. SMART AND F. VERCAUTEREN

Abstract

We re-examine the reduction of Maurer and Wolf of the Discrete Logarithm problem to the Diffie–Hellman problem. We give a precise estimate for the number of operations required in the reduction and use this to estimate the exact security of the elliptic curve variant of the Diffie–Hellman protocol for various elliptic curves defined in standards.

1. *Introduction*

One of the oldest challenging problems in public key cryptography is to prove or disprove that the Discrete Logarithm Problem (DLP) and the Diffie-Hellman Problem (DHP) are computationally equivalent. The hard part of the equivalence is showing that we can solve the DLP using a polynomial number of group operations and calls to a function which solves the DHP.

Significant steps have already been made towards the solution and the equivalence has been proved for some groups. Intuitively, it makes sense to use such groups for the Diffie–Hellman protocol (if of course no discrete logarithm algorithm is known for them), so that breaking the Diffie–Hellman protocol is as hard as computing logarithms, that is to say secure.

For most groups in use in cryptography, it is believed that the DHP and the DLP are equivalent in a complexity-theoretic sense; i.e. there is a polynomial time reduction of one problem to the other, and vice versa. Examples of groups that have been proposed for application in the Diffie-Hellman protocol are the multiplicative group of large finite fields (prime fields or extension fields), the multiplicative group of residues modulo a composite number, elliptic curves over finite fields, and the class group of imaginary quadratic fields.

Maurer and Wolf **[6, 8, 7, 10]** proved that for every group G with prime order p, the equivalence holds if we are able to find an elliptic curve over $\mathbf{F}_p$ with smooth order. The aim of this paper is to show that for various elliptic curve groups recommended by standards, such an elliptic curve exists. To this end, we will use the technique of complex multiplication to construct elliptic curves with smooth order. The implementation of this algorithm has been carried out using the software package Magma.

2. *Notation and Definitions*

Formally we define the DHP and DLP as follows:

2000 Mathematics Subject Classification 14G50,11T71,11Y16,94A60
© ????, A. Muzereau, N.P. Smart and F. Vercauteren

12216

№ 99

AN EVALUATION OF THE PROGRAM FOR REDUCING THE WORKWEEK IN THE USSR

CIA HISTORICAL REVIEW PROGRAM
RELEASE IN FULL

March 1961

NOT TO BE REPRODUCED IN WHOLE OR IN PART WITHOUT THE PERMISSION OF THE CENTRAL INTELLIGENCE AGENCY

CENTRAL INTELLIGENCE AGENCY

[illegible] INTERNAL USE ONLY ☐ CONFIDENTIAL ☒ SECRET

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM: Howard J. Osborn
Director of Security

EXTENSION [illegible] NO.

DATE 16 May 1973

TO: (Officer designation, room number, and building)

DATE RECEIVED | FORWARDED

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

EYES ONLY

1. Executive Secretary, CIA Management Committee
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.

(b)(1)
(b)(3)
(b)(5)
(b)(6)

APPROVED FOR RELEASE
DATE: FEB 2007

00001

EYES ONLY

610 USE PREVIOUS EDITIONS ☒ SECRET ☐ CONFIDENTIAL ☐ INTERNAL USE ONLY ☐ UNCLASSIFIED

DoD 5200.28-STD
Supersedes
CSC-STD-001-83, dtd 15 Aug 83
Library No. S225,711

DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF

DEFENSE

TRUSTED COMPUTER

SYSTEM EVALUATION

CRITERIA

DECEMBER 1985

December 26, 1985

Acta Numerica (2006), pp. 1–155
doi: 10.1017/S0962492906210018
© Cambridge University Press, 2006
Printed in the United Kingdom

Finite element exterior calculus, homological techniques, and applications

Douglas N. Arnold*
Institute for Mathematics and its Applications
and School of Mathematics,
University of Minnesota, Minneapolis, MN 55455, USA
E-mail: arnold@ima.umn.edu

Richard S. Falk†
Department of Mathematics,
Rutgers University, Piscataway, NJ 08854, USA
E-mail: falk@math.rutgers.edu

Ragnar Winther‡
Centre of Mathematics for Applications
and Department of Informatics,
University of Oslo, PO Box 1053, 0316 Oslo, Norway
E-mail: ragnar.winther@cma.uio.no

Dedicated to Carme, Rena, and Rita

Finite element exterior calculus is an approach to the design and understanding of finite element discretizations for a wide variety of systems of partial differential equations. This approach brings to bear tools from differential geometry, algebraic topology, and homological algebra to develop discretizations which are compatible with the geometric, topological, and algebraic structures which underlie well-posedness of the PDE problem being solved. In the finite element exterior calculus, many finite element spaces are revealed as spaces of piecewise polynomial differential forms. These connect to each other in discrete subcomplexes of elliptic differential complexes, and are also related to the continuous elliptic complex through projections which commute with the complex differential. Applications are made to the finite element discretization of a variety of problems, including the Hodge Laplacian, Maxwell's equations, the equations of elasticity, and elliptic eigenvalue problems, and also to preconditioners.

* Supported in part by NSF grant DMS-0411388.
† Supported in part by NSF grant DMS03-08347.
‡ Supported by the Norwegian Research Council.

arXiv:math/0302285v1 [math.HO] 24 Feb 2003

Flashes of noncommutativity

Alejandro Rivero*

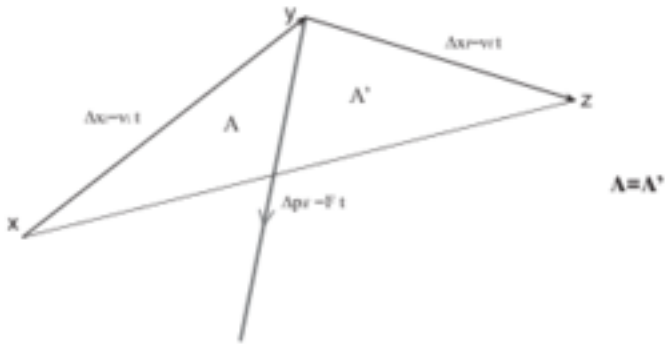
February 1, 2008

Abstract

Noncommutativity lays hidden in the proofs of classical dynamics. Modern frameworks can be used to bring it to light: *-products, groupoids, q-deformed calculus, etc.

Flash one.

Time ago, newborn Classical Mechanics simply described how the inertial law was disturbed by the action of a force. One can consider two inertial trajectories from x to y and then from y to z, where a change is applied in a point y.



If we ask for equal-time segments, then areas A and A' are equal too. In modern language, we are showing that dynamics of a physical system is given by the rule

$$\Delta x_i \times \Delta p = \Delta x_f \times \Delta p$$

By applying this principle to central forces Newton was able to introduce time in geometry, mimicking Kepler second law. This is proposition 1 of Book I in the Principia. Historians tell us that this proposition was rebuilt at least three times while doing the built, and it was already present in the previous paper *De Motu*.

It is very troublesome to define evolution, or consistence within a trajectory, by claiming the equality of two areas, and then asking both areas to go to zero. Paraphrasing my colleague E. Forgy (from a different context), I believe the old fathers could be asking themselves: Is mechanics just a series of $0 = 0$ statements?

Two close remarks:

- It is known that path integral measure is concentrated in continuous everywhere, differentiable nowhere, trajectories. This shows how troublesome is to try to

*Zaragoza University at Teruel. arivero@unizar.es

Ideal Forms of Coppersmith's Theorem and Guruswami-Sudan List Decoding

Henry Cohn* Nadia Heninger*
*Microsoft Research New England, One Memorial Drive, Cambridge, MA 02142
*Department of Computer Science, Princeton University, Princeton, NJ 08540
cohn@microsoft.com nadiah@cs.princeton.edu

Abstract: We develop a framework for solving polynomial equations with size constraints on solutions. We obtain our results by showing how to apply a technique of Coppersmith for finding small solutions of polynomial equations modulo integers to analogous problems over polynomial rings, number fields, and function fields. This gives us a unified view of several problems arising naturally in cryptography, coding theory, and the study of lattices. We give (1) a polynomial-time algorithm for finding small solutions of polynomial equations modulo ideals over algebraic number fields, (2) a faster variant of the Guruswami-Sudan algorithm for list decoding of Reed-Solomon codes, and (3) an algorithm for list decoding of algebraic-geometric codes that handles both single-point and multi-point codes. Coppersmith's algorithm uses lattice basis reduction to find a short vector in a carefully constructed lattice; powerful analogies from algebraic number theory allow us to identify the appropriate analogue of a lattice in each case and provide efficient algorithms to find a suitably short vector, thus allowing us to give completely parallel proofs of the above theorems.

Keywords: Coppersmith's theorem, list decoding, lattice basis, reduction, cryptanalysis, coding theory.

1 Introduction

Many important problems in areas ranging from cryptanalysis to coding theory amount to solving polynomial equations with side constraints or partial information about the solutions.

One of the most important cases is solving equations given size bounds on the solutions. Coppersmith's algorithm is a celebrated technique for finding small solutions to polynomial equations modulo integers, and it has many important applications in cryptography, particularly in the cryptanalysis of RSA.

In this paper, we show how the ideas of Coppersmith's theorem can be extended to a more general framework encompassing the original number-theoretic problem, list decoding of Reed-Solomon and algebraic-geometric codes, and the problem of finding solutions to polynomial equations modulo ideals in rings of algebraic integers. These seemingly different problems are all perfectly analogous when viewed from the perspective of algebraic number theory.

Coppersmith's algorithm provides a key example of the power of lattice basis reduction. In order to extend the method beyond the integers, we examine the analogous structures for polynomial rings, number fields, and function fields. Ideals over number fields have a natural embedding into a lattice, and thus we can find a short vector simply by applying the LLL algorithm to this canonical embedding. In contrast to integer lattices, it turns out that lattice basis reduction is much easier over a lattice of polynomials, and in fact a shortest vector can always be found in polynomial time. Recasting the list decoding problem in this framework allows us to take advantage of very efficient reduction algorithms and thus achieve the fastest known list decoding algorithm for Reed-Solomon codes.

To extend this approach to function fields, we must overcome certain technical difficulties. In addition, we prove a much more general result about finding short vectors under arbitrary non-Archimedean norms, which may have further applications beyond list decoding of algebraic-geometric codes. As an illustration of the generality of our approach, we give the first list decoding algorithm that works for all algebraic-geometric codes, not just those defined using a single-point divisor.

In the remainder of the introduction, we set up our

Chaos-Based Cryptography: A Brief Overview

by Ljupčo Kocarev*

Abstract*—*In this brief article, chaos-based cryptography is discussed from a point of view which I believe is closer to the spirit of both cryptography and chaos theory than the way the subject has been treated recently by many researchers. I hope that, although this paper raises more questions than provides answers, it nevertheless contains seeds for future work.

1531-636X/10$10.00©2001IEEE

CA SiteMinder®

Policy Server Configuration Guide

r12.5

Second Edition

FROM CONSERVATION LAWS TO PORT-HAMILTONIAN REPRESENTATIONS OF DISTRIBUTED-PARAMETER SYSTEMS

B.M. Maschke [*,1] **A.J. van der Schaft** [**,1]

[*] *Lab. d'Automatique et de Genie des Procédés, Université Claude Bernard Lyon-1, F-69622 Villeurbanne, France*
[**] *Department of Applied Mathematics, University of Twente, PO Box 217, 7500 AE, Enschede, The Netherlands*

Abstract: In this paper it is shown how the port-Hamiltonian formulation of distributed-parameter systems is closely related to the general thermodynamic framework of systems of conservation laws and closure equations. The situation turns out to be similar to the lumped-parameter case where the Dirac structure captures the basic interconnection laws, and the closure equations correspond to the constitutive relations of the energy-storing elements. *Copyright © 2005 IFAC.*

Keywords: Interconnected systems, modeling, energy storage, geometric theory.

1. INTRODUCTION

The treatment of infinite-dimensional Hamiltonian systems in the literature is mostly confined to systems with boundary conditions such that the energy exchange through the boundary is zero. On the other hand, in many applications the interaction with the environment (e.g. actuation or measurement) takes place through the boundary of the system. In (van der Schaft and Maschke, 2002; Maschke and van der Schaft, 2000), we have developed a framework to represent classes of physical distributed-parameter systems with boundary energy flow as infinite-dimensional *port-Hamiltonian systems*. Key in this is the notion of a *Dirac structure*. Dirac structures were originally introduced in (Courant, 1990; Dorfman, 1993) as a geometric structure generalizing both *symplectic* and *Poisson* structures. Later on (van der Schaft and Maschke, 1995; Dalsmo and van der Schaft, 1999; Maschke and van der Schaft, 1997; Bloch and Crouch, 1999) it was realized that in the finite-dimensional case Dirac structures can be employed to formalize Hamiltonian systems with *algebraic constraints*. In order to allow the inclusion of boundary variables in distributed-parameter systems the concept of (an infinite-dimensional) Dirac structure provides again the right type of generalization with respect to the existing framework (Olver, 1993) using Poisson structures.The aim of this paper is to show how this port-Hamiltonian formulation of distributed-parameter systems can be based on the thermodynamic framework for describing distributed-parameter systems as systems of conservation laws, see e.g. (Godlewsky and Raviart, 1996; Serre, 1999).

2. CONSERVATION LAWS, INTERDOMAIN COUPLING AND BOUNDARY ENERGY FLOWS: MOTIVATIONAL EXAMPLES

In this section we shall introduce the main concepts by means of three classical examples of distributed-parameter systems.

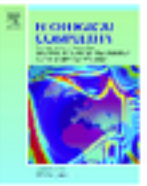
[1] Work performed in the context of the EU-project Geo-PleX, IST-2001-34166

ECOLOGICAL COMPLEXITY 4 (2007) 148–159

available at www.sciencedirect.com

ScienceDirect

journal homepage: http://www.elsevier.com/locate/ecocom



Weighting, scale dependence and indirect effects in ecological networks: A comparative study

Marco Scotti[a,b], János Podani[c], Ferenc Jordán[a,d,*]

[a] Collegium Budapest, Institute for Advanced Study, Szentháromság u. 2., H-1014, Budapest, Hungary
[b] Department of Environmental Sciences, University of Parma, Parma, Italy
[c] Department of Plant Taxonomy and Ecology, Eötvös University, Budapest, Hungary
[d] Animal Ecology Research Group of HAS, Hungarian Natural History Museum, Budapest, Hungary

ARTICLE INFO

Article history:
Received 17 January 2007
Received in revised form
19 April 2007
Accepted 6 May 2007
Published on line 27 June 2007

Keywords:
Ecological network
Interaction strength
Indirect effects
Centrality
Positional importance
Scale independence

ABSTRACT

We studied the importance of weighting in ecological interaction networks. Fifty-three weighted interaction networks were analyzed and compared to their unweighted alternatives, based on data taken from two standard databases. We used five network indices, each with weighting and unweighting options, to characterize the positional importance of nodes in these networks. For every network, we ranked the nodes according to their importance values, based on direct and indirect indices and then we compared the rank order of coefficients to reveal potential differences between network types and between indices. We found that (1) weighting affects node ordering very seriously, (2) food webs fundamentally differ from other network types in this respect, (3) direct and indirect indices provide fairly different results but indirect effects are similar if longer than two steps, and (4) the effect of weighting depends on the number of network nodes in case of direct interactions only. We concluded that the importance of interaction weights may depend on the evolutionary stability of interaction types.

© 2007 Elsevier B.V. All rights reserved.

1. Introduction

Conservation biology is being shifted from protecting species to protecting interspecific interactions and communities. In order to better understand the nature of interaction networks, we need comparative analyses of different interaction types. Ecological complexity comprises the diversity of both species and interspecific interactions. Different types of interactions, such as prey–predator or plant–pollinator interactions are of different character in their ecology and evolution (Thompson, 1991). Since the majority of ecological networks studied so far are food webs (or trophic networks), we should re-examine many classical questions for other network types as well. These basic problems include the importance of weighting, the relevance of indirect interactions and the scale dependence of network properties.

The systematic analysis of ecological networks involves three steps: (1) data collection, (2) network construction and (3) network analysis *sensu stricto*. A number of problems are relevant only to one of these steps, while others bridge over the whole process. The mostly practical question whether and how to consider weights on links (Ulanowicz, 1986; Baird and Ulanowicz, 1989; Paine, 1980) concerns step 1. The problems of aggregation, network resolution and scale dependence (Martinez, 1991; Allesina and Bodini, 2005; Allesina et al., 2005) concern step 2. Finally, a possibly more technical question whether to neglect or explicitly study indirect interactions spreading over these networks (Menge, 1995; Wootton, 1994) concerns step 3. Each problem has a long history and has been

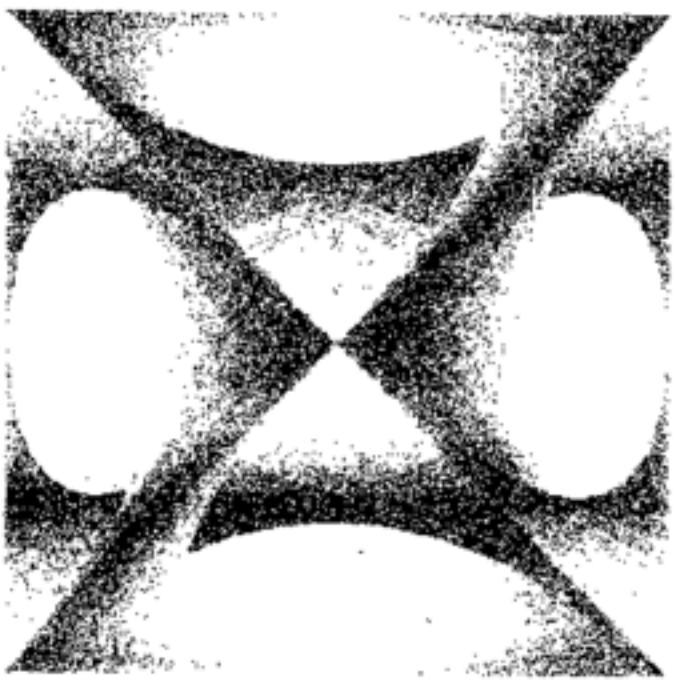
* Corresponding author. Tel.: +36 1 22 48 300; fax: +36 1 22 48 310.
E-mail address: jordan.ferenc@gmail.com (F. Jordán).
1476-945X/$ – see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.ecocom.2007.05.002

Symmetry: Culture and Science

Symmetry and Information

The Quarterly of the International Society for the Interdisciplinary Study of Symmetry (ISIS-Symmetry)

Volume 8, Number 2, 1997



Hyperincursive Algorithms of Classical Harmonic Oscillator Applied to Quantum Harmonic Oscillator Separable Into Incursive Oscillators

DANIEL M. DUBOIS

Centre for Hyperincursion and Anticipation in Ordered Systems (CHAOS)
Institute of Mathematics B37
Grande Traverse 12, BE-4000 LIEGE, Belgium
http://www.vla.hec.ulg.ac.be, ddubois.chaos@gmail.com

This paper will first survey the hyperincursive and incursive algorithms to discretize the classical harmonic oscillator. These algorithms show stable orbital with the conservation of energy. This paper will then apply these hyperincursive and incursive algorithms to the quantum harmonic oscillator. The hyperincursive quantum harmonic oscillator is separable into two incursive quantum harmonic oscillators. Numerical simulations confirm the stability of these hyperincursive and incursive algorithms.

Keywords: Harmonic oscillator, Hyperincursive algorithms, Incursive oscillator.

Interval Arithmetic and Recursive Subdivision for Implicit Functions and Constructive Solid Geometry

Tom Duff*
AT&T Bell Laboratories
600 Mountain Avenue
Murray Hill, New Jersey 07974

Abstract

Recursive subdivision using interval arithmetic allows us to render CSG combinations of implicit function surfaces with or without anti aliasing. Related algorithms will solve the collision detection problem for dynamic simulations and allow us to compute mass, center of gravity, angular momenta and other integral properties required for Newtonian dynamics.

Our hidden surface algorithm runs in 'constant time.' Their running times are nearly independent of the number of primitives in a scene, for scenes in which the visible details are not much smaller than the pixels. The collision detection and response algorithms are wholly robust. Collisions are never missed due to numerical error and we can provide guaranteed bounds on the values of integrals.

CR Categories and Subject Descriptors: G.1.0 [Numerical Analysis]: Numerical Algorithms; I.3.3 [Picture and Image Generation]: Display algorithms, Viewing algorithms; I.3.5 [Computational Geometry and Object Modeling]: Curve, surface, solid and object representations; I.3.5 [Computational Geometry and Object Modeling]: Hierarchy and geometric transformations; I.3.7 [Three-Dimensional Graphics and Realism]: Visible hidden surface algorithms, Animation

General Terms: Algorithms

Additional Keywords and Phrases: anti-aliasing, compositing, computer-aided animation, recursive subdivision, image synthesis, dynamic simulation, collision detection

1. Introduction

The most commonly-used geometric representations in computer graphics are local. Polygonal models, for example, specify which points are on an object's surface, and tell us nothing whatsoever about the rest of the space in which the object is embedded, except by omission. It requires substantial mental effort to formulate answers to questions like "Do these objects intersect?", or "What parts of this object are visible?" or even something as simple as "What is the volume of this object?". More elaborate surface representations, like Bezier patches or NURBS don't make these questions any easier—since they only constrain the objects locally, they make it difficult to answer global questions about them.

Likewise, the computational methods we normally use are mostly local. The ray-tracing algorithm, for example, tries to compute an image one pixel at a time by testing every point in the scene for intersection with a ray from the eye point through the pixel's center. Of course any decent ray tracer goes to a lot of trouble to avoid most of this work. But an algorithm that had instant access to global information about the scene wouldn't need to go to the trouble—it would know immediately what parts of the scene were relevant to what parts of the screen.

A good example of a global representation is the BSP tree [11]. Each node of a BSP tree gives us the information about the object's relationship to the whole of the space it's embedded in. The nodes effectively say about their subtrees "in this half of space, you need not think about this half of the model." BSP trees naturally engender simple algorithms for all sorts of geometric tasks, from hidden surface removal to object intersection [15] to volume integration [2], that make natural, effective use of the global information stored in the model.

This paper will examine in detail another global object representation and its algorithms based on implicit functions, Constructive Solid Geometry and interval arithmetic.

Briefly, implicit functions are real functions for classifying points in space as inside on or outside an object. Interval arithmetic allows us to extend these tests to whole chunks of space at once. Constructive Solid Geometry allows us to combine simpler objects to keep unwieldy primitives (like infinite ray tubes) under control and model many important industrial and natural processes that go into creating geometric forms.

2. Implicit Functions

Implicit functions are an indirect representation of solid objects. Given a function of three variables $F(x,y,z)$, we can use the equation $F(x,y,z) = 0$ to specify the points on a surface. The representable surfaces range from the mundane to the exotic: from plane: $ax+by+cz+d=0$; and quadrics: the spheres, cones, cylinders and paraboloids of elementary geometry—to more exotic polynomial surfaces like those of Kummer and Dupin [9] to Barr's downright weird twisted, bent and tapered superellipsoids [4].

If F is continuous, we can cleanly partition space inside, on or outside the object depending on whether $F<0$, $F=0$ or $F>0$ [1]. This is the global property we are after. F classifies every point in space in its relationship to the surface. Its regions of space are created by the surface, the fact that F's sign does not change in a region of connected space, is hidden-surface and other geometric algorithms that can be exploited by using interval arithmetic to quickly obtain bounds on $F(x,y,z)$ for whole ranges of x, y and z.

3. Interval Arithmetic

Interval arithmetic [16] generalizes ordinary arithmetic to closed, bounded ranges of real numbers. If X and $\bar{X}$ are real numbers with $\underline{X} \le \bar{X}$, then X is an interval

$$X = [\underline{X}, \bar{X}] = \{x \mid \underline{X} \le x \le \bar{X}\}$$

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

Run-time firmware integrity verification: what if you can't trust your network card?

SCHRÖDINGER EQUATION AND QUANTUM CHEMISTRY

Renato Colle
Dipatimento di Chimica Applicata, Università di Bologna, Italy,

Keywords: Wave mechanics, Wave function, Wave equation, Configuration space, Eigenvalue, Eigenfunction, Probability, Stationary state, Symmetry, Spin-orbital, Atomic and molecular orbital, Potential energy surface, Slater determinant, Variational method, Hartree-Fock, Coulomb and exchange operators, Correlation energy, Density matrix, MC-SCF, CI, VB, DFT, KS, Car-Parrinello.

Contents

1. Introduction
2. The Schrödinger equation
2.1 Foundation of wave mechanics
2.2 Properties of the Schrödinger equation
2.3 Generalization of the Schrödinger equation for many-body systems
2.4 General remarks on the Schrödinger equation
3. Quantum Chemistry
3.1 Hartree-Fock theory and molecular orbitals
3.2 Correlated wavefunctions
3.3 Density Functional Theory
3.4 Time-dependent problems
Acknowledgement
Glossary
Bibliography
Biographical Sketch

UNESCO – EOLSS SAMPLE CHAPTERS

Summary

Aims, topics and methods of quantum chemistry are discussed, together with the relationship between quantum mechanics and quantum chemistry.

Foundation of wave mechanics and derivation of the one-particle Schrödinger equation are summarized. The main properties of this equation are analyzed, together with its generalization for many-body systems.

Quantum mechanical methods developed for studying static and dynamic properties of molecules are described.

1. Introduction

Quantum chemistry is the science that studies molecules and processes involving molecules using methods of quantum mechanics. If we consider that under the word "molecules" one can include the largest part of chemical substances, like e.g. organic and inorganic complexes, clusters and macromolecules, and if we consider that quantum mechanics is a formal theory well-established in its general principles and almost

gemalto
security to be free

Enhance your CA SiteMinder with the Ezio Server

For comprehensive protection of online sessions and data, enhance the CA SiteMinder solution to include Gemalto's security features using multi-factor authentication with End-to-End (E2E) encryption of passwords and One Time Passwords (OTPs).

EUROPEAN CENTRAL BANK
EUROSYSTEM

Working Paper Series

Giancarlo Corsetti, Luca Dedola,
Marek Jarociński, Bartosz Maćkowiak,
Sebastian Schmidt

Macroeconomic stabilization, monetary-fiscal interactions, and Europe's monetary union

Discussion Papers

No 1988 / December 2016

Note: This Working Paper should not be reported as representing the views of the European Central Bank (ECB). The views expressed are those of the authors and do not necessarily reflect those of the ECB.

ELLIPTIC CURVES AND MODULAR FORMS

by

Robert C. Rhoades

Notes

Based on A Course at
the University of Wisconsin - Madison
MATH 844 during the Spring 2006
taught by Professor Nigel Boston

August 10, 2006

Rethinking set theory

Tom Leinster

Edinburgh

arXiv:1212.6543

These slides: available on my web page

The Discrete Hodge Star Operator

Edmond Rusjan

SUNYIT

HRUMC, April 6, 2013

Port-Hamiltonian Systems: from Geometric Network Modeling to Control

Arjan van der Schaft, University of Groningen

Dimitri Jeltsema, Delft University of Technology

In collaboration with Bernhard Maschke, Romeo Ortega, Jacquelien Scherpen, Stefano Stramigioli, Alessandro Macchelli, Peter Breedveld, Hans Zwart, Morten Dalsmo, Guido Blankenstein, Damien Eberard, Goran Golo, Ram Pasumarthy, Javier Villegas, Gerardo Escobar, Guido Blankenstein, Aneesh Venkatraman, Rostyslav Polyuga ..

WHO Technical Report Series

The Selection and Use of Essential Medicines

UNEDITED VERSION

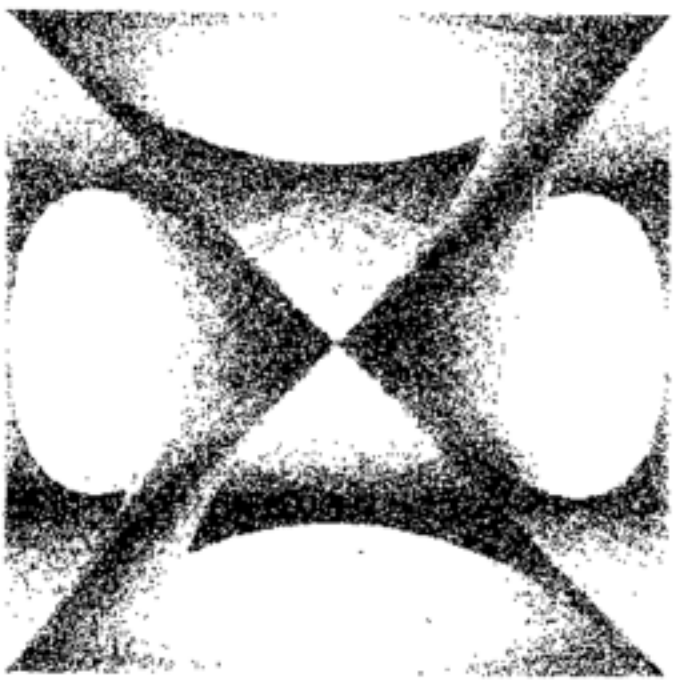
Report of the WHO Expert Committee on Selection and Use of Essential Medicines, 2017 (including the 20th WHO Model List of Essential Medicines and the 6th WHO Model List of Essential Medicines for Children)

Symmetry: Culture and Science

Symmetry and Information

The Quarterly of the International Society for the Interdisciplinary Study of Symmetry (ISIS-Symmetry)

Volume 8, Number 2, 1997



Hamiltonian mechanics in the "extended" phase space

Jürgen Struckmeier

j.struckmeier@gsi.de

GSI Accelerator Seminar

Darmstadt, 03 July 2003

Smart Homes that Monitor Breathing and Heart Rate

Fadel Adib Hongzi Mao Zachary Kabelac Dina Katabi Robert C. Miller
Massachusetts Institute of Technology
32 Vassar Street, Cambridge, MA 02139
{fadel,hongzi,zek,dk,rcm}@mit.edu

ABSTRACT

The evolution of ubiquitous sensing technologies has led to intelligent environments that can monitor and react to our daily activities, such as adapting our heating and cooling systems, responding to our gestures, and monitoring our elderly. In this paper, we ask whether it is possible for smart environments to monitor our vital signs remotely, without instrumenting our bodies. We introduce Vital-Radio, a wireless sensing technology that monitors breathing and heart rate without body contact. Vital-Radio exploits the fact that wireless signals are affected by motion in the environment, including chest movements due to inhaling and exhaling and skin vibrations due to heartbeats. We describe the operation of Vital-Radio and demonstrate through a user study that it can track users' breathing and heart rates with a median accuracy of 99%, even when users are 8 meters away from the device, or in a different room. Furthermore, it can monitor the vital signs of multiple people simultaneously. We envision that Vital-Radio can enable smart homes that monitor people's vital signs without body instrumentation, and actively contribute to their inhabitants' well-being.

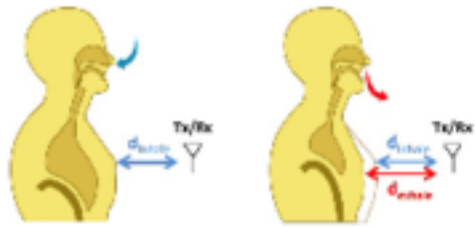
Author Keywords Wireless; Vital Signs; Breathing; Smart Homes; Seeing Through Walls; Well-being

Categories and Subject Descriptors H.5.2. Information Interfaces and Presentation: User Interfaces - Input devices and strategies. C.2.2. Network Architecture and Design: Wireless Communication.

INTRODUCTION

The past few years have witnessed a surge of interest in ubiquitous health monitoring [22, 25]. Today, we see smart homes that continuously monitor temperature and air quality and use this information to improve the comfort of their inhabitants [46, 32]. As health-monitoring technologies advance further, we envision that future smart homes would not only monitor our environment, but also monitor our vital signals, like breathing and heartbeats. They may use this information to enhance our health-awareness, answering questions like "Do my breathing and heart rates reflect a healthy lifestyle?" They may also help address some of our concerns by answering questions like "Does my child breathe normally during sleep?" or "Does my elderly parent experience irregular heartbeats?" Furthermore, if non-intrusive in-home continuous monitoring of breathing and heartbeats existed, it would enable healthcare professionals to study how these signals correlate with our stress level and evolve with time and age, which could have a major impact on our healthcare system.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-3145-6/15/04...$15.00
http://dx.doi.org/10.1145/2702123.2702200



(a) Inhale Motion (b) Exhale Motion

Figure 1—Chest Motion Changes the Signal Reflection Time. (a) shows that when the person inhales, his chest expands and becomes closer to the antenna, hence decreasing the time it takes the signal to reflect back to the device. (b) shows that when the person exhales, his chest contracts and moves away from the antenna, hence the distance between the chest and the antenna increases, causing an increase in the reflection time.

Unfortunately, typical technologies for tracking vital signals require body contact, and most of them are intrusive. Specifically, today's breath monitoring sensors are inconvenient: they require the person to attach a nasal probe [19], wear a chest band [43], or lie on a special mattress [3]. Some heart-rate monitoring technologies are equally cumbersome since they require their users to wear a chest strap [18], or place a pulse oximeter on their finger [21]. The more comfortable technologies such as wristbands do not capture breathing and have lower accuracy for heart rate monitoring [12]. Additionally, there is a section of the population for whom wearable sensors are undesirable. For example, the elderly typically feel encumbered or ashamed by wearable devices [20, 37], and those with dementia may forget to wear them. Children may remove them and lose them, and infants may develop skin irritation from wearable sensors [40].

In this paper, we ask whether it's possible for smart homes to monitor our vital signs remotely – i.e., without requiring any physical contact with our bodies. While past research has investigated the feasibility of sensing breathing and heart rate without direct contact with the body [17, 16, 15, 34, 27, 48, 14], the proposed methods are more appropriate for controlled settings but unsuitable for smart homes: They fail in the presence of multiple users or extraneous motion. They typically require the user to lie still on a bed facing the device. Furthermore, they are accurate only when they are within close proximity to the user's chest.

The Physics of Information Technology

Neil Gershenfeld

revised draft: February 5, 2013

arXiv:quant-ph/0412136 v2 20 Dec 2004

Minimum entangled state dimension required for pseudo-telepathy

Gilles Brassard* André Allan Méthot Alain Tapp†

Département d'informatique et de recherche opérationnelle
Université de Montréal, C.P. 6128, Succ. Centre-Ville
Montréal (QC), H3C 3J7 Canada
{brassard, methotan, tappa}@iro.umontreal.ca

16 December 2004

Abstract

Pseudo-telepathy provides an intuitive way of looking at Bell's inequalities, in which it is often obvious that feats achievable by use of quantum entanglement would be classically impossible. A two-player pseudo-telepathy game proceeds as follows: Alice and Bob are individually asked a question and they must provide an answer. They are *not* allowed any form of communication once the questions are asked, but they may have agreed on a common strategy prior to the execution of the game. We say that they *win* the game if the questions and answers fulfil a specific relation. A game exhibits *pseudo-telepathy* if there is a quantum strategy that makes Alice and Bob win the game for all possible questions, provided they share prior entanglement, whereas it would be impossible to win this game systematically in a classical setting. In this paper, we show that any two-player pseudo-telepathy game requires the quantum players to share an entangled quantum system of dimension at least 3×3. This is optimal for two-player games, but the most efficient pseudo-telepathy game possible, in terms of total dimension, involves *three* players who share a quantum system of dimension $2 \times 2 \times 2$.

*Supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), the Canadian Institute for Advanced Research (CIAR), the Mathematics of Information Technology and Complex Systems Network (MITACS) and the Canada Research Chair Programme.

†Supported in part by NSERC, CIAR, MITACS and Québec's FQRNT.

National Cyber Security Centre
Ministry of Security and Justice

Choosing a messaging app for your organisation

Publicly available apps are being used for business communication

Factsheet FS-2017-03 | version 1.1 | 31 August 2017

A large part of business communication is conducted through messaging apps.[1] Using publicly available messaging apps for business communication involves certain risks and has consequences for both your organisation and information sharing. Of the messaging apps currently in use, few are sufficiently secure to comply with your security policy for internal communication.

The NCSC recommends that you assess which messaging app is most suitable for use within your organisation. You should then conduct a risk analysis which takes into account your organisation's security and user requirements and take further action if required.

[1] A messaging app is an online communication service for smartphones. Examples include WhatsApp, Signal and Telegram. Such apps are used to exchange information. This factsheet does not cover instant messaging (IM) services, such as Slack and the Extensible Messaging and Presence Protocol (XMPP).

Background

Using messaging apps to share confidential business information involves certain risks. This factsheet describes the main risk factors involved in the use of messaging apps. Its objective is to provide information security officers with the information they need to conduct a risk assessment to find a messaging app that is most suitable for use within their organisation. The NCSC recommends that organisations conduct a thorough research before choosing a messaging app, to ensure it complies with their internal security policy. The NCSC itself does not assess the security of messaging apps.

Target audience

Information security officers at medium-sized and large organisations.

The following organisations have contributed to this factsheet:

The Tax and Customs Administration, the Nuclear Research & Consultancy Group (NRG) and Rabobank.

The World and the Machine

CSCE 740 - Lecture 9 - 09/23/2015

Kalamata
Billington Lane
Derrington
Stafford
ST18 9LR
Email: mark.anthony.taylor@gmail.com
21 September 2016

To:

Andrew Bailey, Chief of the FCA
Prime Minister Theresa May
Rt Hon Jeremy Wright MP
David Green, Chief of the SFO
Sir Edward Leigh MP
Lynne Owens, Chief of the NCA

Rt Hon Andrew Tyrie MP – Chairman of HoC Treasury Committee
Rt Hon Steve Baker MP – HoC Treasury Committee
Rt Hon Mark Garnier MP – HoC Treasury Committee
Rt Hon Helen Goodman MP – HoC Treasury Committee
Rt Hon Stephen Hammon MP – HoC Treasury Committee
Rt Hon George Kerevan MP – HoC Treasury Committee
Rt Hon John Mann MP – HoC Treasury Committee
Rt Hon Chris Phillip MP – HoC Treasury Committee
Rt Hon Jacob Rees Mogg MP – HoC Treasury Committee
Rt Hon Rachel Reeves MP – HoC Treasury Committee
Rt Hon Wes Streeting MP – HoC Treasury Committee

Copies To:

Sir Bernard Hogan Howe
Lord Chancellor Elizabeth Truss
Rt Hon Jeremy Lefroy MP
And others

How the FCA and the SFO covered up Deutsche Bank's gold manipulation, money laundering & conspiracy to pervert the course of justice

Dear Sirs,

With the recent disclosures from the *New Yorker* magazine, http://www.newyorker.com/magazine/2016/08/29/deutsche-banks-10-billion-scandal, that exposed Deutsche Bank's $10 billion money laundering operation between Russia and London, we now have the context to review the conduct of the FCA and the SFO in their related duties and investigations. I hope to prove here that both agencies neglected their responsibilities to the point of being complicit in Deutsche Bank's bribery of judges in the Mercantile Court and the Court of Appeal. As you can see in the news article the money laundering went on during 2015, which we shall see below is when the FCA and SFO had enough information to prosecute the bank. I shall also show both agencies had enough information in 2014 to prove the bank was guilty of precious metal price rigging - rigging we now know to be the case following a settlement in New York.

Generalized phase-space tomography for intense beams[a)]

D. Stratakis,[1,b)] R. A. Kishek,[2] S. Bernal,[2] R. B. Fiorito,[2] I. Haber,[2] M. Reiser,[2] P. G. O'Shea,[2] K. Tian,[3] and J. C. T. Thangaraj[4]
[1]*Department of Physics, Brookhaven National Laboratory, Upton, New York 11973, USA*
[2]*Institute for Research in Electronics and Applied Physics, University of Maryland, College Park, Maryland 20742, USA*
[3]*Thomas Jefferson National Accelerator Facility, Newport News, Virginia 23606, USA*
[4]*Fermi National Accelerator Laboratory, Batavia, Illinois 60510, USA*

(Received 21 November 2009; accepted 27 December 2009; published online 12 February 2010)

Tomographic phase-space mapping in an intense particle beam is reviewed. The diagnostic is extended to beams with space-charge by assuming linear forces and is implemented using either solenoidal or quadrupole focusing lattices. The technique is benchmarked against self-consistent simulation and against a direct experimental sampling of phase-space using a pinhole scan. It is demonstrated that tomography can work for time-resolved phase-space mapping and slice emittance measurement. The technique is applied to a series of proof-of-principle tests conducted at the University of Maryland. © *2010 American Institute of Physics*. [doi:10.1063/1.3298894]

I. INTRODUCTION

Maintaining and preserving a high density of particles in phase-space is an important requirement for beams of many accelerator applications. Examples of those include accelerator-driven neutron sources,[1] high luminosity high-energy colliders,[2] free-electron lasers,[3] energy-recovery linacs,[4] and heavy-ion inertial fusion (HIF) drivers.[5] At the low-energy end of these accelerators, the particle dynamics can be significantly affected by their mutual repulsion, also known as space-charge.[6] Space-charge can engender collective behavior[7] and is often destructive to the beam.[8,9] For instance, space-charge can cause halo formation[10] which can result to beam losses and activation of the machine. Therefore, having a good understanding of beams with space-charge is necessary, and phase-space reconstruction is an important tool in achieving this goal.

Tomographic techniques previously have shown success in reconstructing the phase-space distribution. Computerized tomography is well known in the medical community and was originally developed to process x-ray images. A Norwegian physicist Abel (1826) first formulated the concept of tomography[11] for an object with axisymmetric geometry. Nearly 100 years later, an Austrian mathematician Radon (1917) developed a theorem extending the idea to arbitrarily shaped objects; it stated that an object in an n-dimensional space can be recovered from a sufficient number of projections on to $(n-1)$-dimensional space.[12]

In beam physics, we can map the phase-space using information taken from the distribution of spatial density at the same point. A simple scaling equation relates the spatial beam projections to the Radon transform of the transverse-phase space, as demonstrated in the 1970s by Sander *et al.*[13] Specifically, the authors imaged the beam at different positions along the beam line and then reconstructed the phase-space distribution using tomographic computer programs. The unavailability of profile monitors along the beam line limited these spatial projections to three; therefore, the resolution of the reconstructed phase space was sparse. Similarly, Fraser[14] reconstructed the phase space by tomography via either two or three projections. Again, with so few views, the phase-space plots lacked structure.

Phase-space tomography was implemented with greater accuracy by the study of McKee *et al.*[15] wherein they combined the ideas of tomography with quadrupole scanning to recover density information in phase space. To account for beam stretching while scanning the magnet, these researchers scaled the profiles using a scaling parameter. McKee *et al.* demonstrated that both the scaling parameter and the angle of projection can be calculated from the beam's transport matrix. Since then, several authors adopted a similar approach.[16–20]

We note that all these tomography studies were applied to relativistic beams, and the tomography algorithm did not consider space-charge forces. In this work a model is presented to apply tomography to beams with space charge. The technique is generalized to account for both solenoidal- and quadrupole-focusing lattices. The method is benchmarked by computer simulation and a pinhole scan, an independent method to experimentally obtain phase spaces. It is also demonstrated that tomography can work for time-resolved phase-space mapping and slice emittance measurement, given the right diagnostics. Finally, we review the results obtained in experiments at the University of Maryland using this generalized version of the tomography diagnostic.

The outline of this paper is as follows. In Sec. II we review the tomographic algorithm for beams with space charge. In Sec. III, we describe our approach to validate tomography through simulation. In Sec. IV we review a number of experiments conducted at the University of Maryland by using phase-space tomography. Finally, we present our conclusions in Sec. V.

[a)]Paper CI2 4, Bull. Am. Phys. Soc. **54**, 54 (2009).
[b)]Invited speaker.

 © 2010 American Institute of Physics

Downloaded 28 Apr 2011 to 131.225.103.35. Redistribution subject to AIP license or copyright; see http://pop.aip.org/about/rights_and_permissions

iPass® Generic Interface Specification

BETWEEN SMART CLIENTS AND ACCESS GATEWAY, VERSION 1.6

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065 USA

www.ipass.com
+1 650-232-4100
+1 650-232-0227 fx

The Feynman Path Integral: The Closer You Look, The Weirder It Gets
Last Update: 4th May 2008

We are used to the Feynman path integral giving rise to quantum mechanical behaviour as a consequence of the contributions of all possible paths, including highly erratic, non-differentiable paths. But surely the classical limit reproduces a nice, sensible, smooth, continuous, everywhere differentiable, classical trajectory? No, sorry, it does not, quite the opposite. Such smooth curves can be shown to make no contribution. Their Wiener measure is zero. Instead, the classical limit of the Feynman integral entails non-zero contributions only from paths which are so violently kinked that they are nowhere differentiable. This can be established rigorously [see for example M. Reed and B. Simon: *Methods of modern mathematical physics, vol.2: Fourier analysis, self-adjointness*, Academic Press, San Diego (1975)]. Here we demonstrate this fact by a very simple argument.

The propagator (or Green's function, or two-point function, or partition function, according to taste or subtle dialect) is, for a single particle moving in one dimension,

$$G(x_1,t_1;x_N,t_N) = \int_{\Omega} \exp\left\{\frac{i}{\hbar} S(x(t))\right\} \cdot Dx(t) \qquad (1)$$

where S(x(t)) is the classical Action for the path x(t) which is arbitrary except that it is constrained to start at x_1 and end at x_N, i.e., $x(t_1) = x_1$ and $x(t_N) = x_N$. Hence,

$$S(x(t)) = \int_{t_1}^{t_N} L(x(t),\dot{x}(t),t)\cdot dt \qquad (2)$$

where L is the classical Lagrangian (i.e. the kinetic energy minus the potential energy, as a function of position and velocity). The integration in (1) is a functional integration over "all paths". In practice this is to be understood as the limit of a large number of ordinary integrals over the position of the particle at intermediate times. Thus, the integration measure is,

$$Dx(t) \equiv dx_2 dx_3 dx_4 \ldots dx_{N-1} \qquad (3)$$

where $x_i \equiv x(t_i)$, and the intermediate times obey $t_1 < t_2 < t_3 \ldots < t_N$, and may be taken as equally spaced. The range of the integral in (1), Ω, is whatever spatial domain we wish to confine the particle to – and may be infinite. The quantum wavefunction at time t_N is found from that at time t_1 from,

$$\psi(x_N,t_N) = \int_{\Omega} S(x_N,t_N;x_1,t_1)\psi(x_1,t_1)dx_1 \qquad (4)$$

where (4) is an ordinary integral.

Fermionic Algebra and Fock Space

Earlier in class we saw how harmonic-oscillator-like bosonic commutation relations

$$\left[\hat{a}_\alpha, \hat{a}_\beta\right] \;=\; 0, \quad \left[\hat{a}^\dagger_\alpha, \hat{a}^\dagger_\beta\right] \;=\; 0, \quad \left[\hat{a}_\alpha, \hat{a}^\dagger_\beta\right] \;=\; \delta_{\alpha,\beta} \tag{1}$$

give rise to the bosonic Fock space in which the oscillator modes α correspond to single-particle quantum states $|\alpha\rangle$. In this note, we shall see how the fermionic anti-commutation relations

$$\left\{\hat{a}_\alpha, \hat{a}_\beta\right\} \;=\; 0, \quad \left\{\hat{a}^\dagger_\alpha, \hat{a}^\dagger_\beta\right\} \;=\; 0, \quad \left\{\hat{a}_\alpha, \hat{a}^\dagger_\beta\right\} \;=\; \delta_{\alpha,\beta} \tag{2}$$

give rise to the fermionic Fock space. Again, the modes α will correspond to the single-particle quantum states. For simplicity, I will assume discrete modes — for example, momenta (and spins) of a free particle in a big but finite box.

Hilbert Space of a Single Fermionic Mode

A single bosonic mode is equivalent to a harmonic oscillator; the relation $[\hat{a}, \hat{a}^\dagger] = 1$ gives rise to an infinite-dimensional Hilbert space spanning states $|n\rangle$ for $n = 0, 1, 2, 3, \ldots, \infty$. A single fermionic mode is different — its Hilbert space spans just two states, $|0\rangle$ and $|1\rangle$. In accordance with the Fermi statistics, multiple quanta in the same mode are not allowed.

To see how this works, note that the fermionic creation / annihilation operators $\hat{a}^\dagger$ and $\hat{a}$ satisfy not just the anti-commutation relation

$$\hat{a}\hat{a}^\dagger \;+\; \hat{a}^\dagger\hat{a} \;=\; 1 \tag{3}$$

between them but also

$$\{\hat{a}, \hat{a}\} \;=\; \{\hat{a}^\dagger, \hat{a}^\dagger\} \;=\; 0 \quad\Longleftrightarrow\quad \hat{a}\hat{a} = \hat{a}^\dagger\hat{a}^\dagger = 0. \tag{4}$$

As usual, the number of quanta is measured by the hermitian operator $\hat{n} = \hat{a}^\dagger\hat{a}$. For the bosons we also had $\hat{a}\hat{a}^\dagger = \hat{n} + 1$ but for the fermions we now have $\hat{a}^\dagger\hat{a} = 1 - \hat{n}$.

Renormalization from Classical to Quantum Physics

by

Arnab Kar

Submitted in Partial Fulfillment
of the
Requirements for the Degree
Doctor of Philosophy

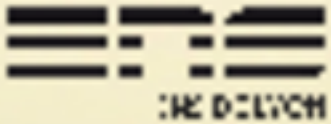
Supervised by
Professor Sarada G. Rajeev
Department of Physics and Astronomy
Arts, Sciences and Engineering
School of Arts and Sciences

University of Rochester
Rochester, New York

2014

The Algebra of Signal Flow Graphs

Filippo Bonchi, Paweł Sobociński, Fabio Zanasi



Journées Structures Discrètes 2015

On Symplectic Reduction in Classical Mechanics

J. Butterfield[1]

All Souls College
Oxford OX1 4AL

Monday 5 December 2005; a Chapter of *The North Holland Handbook of Philosophy of Physics*

Abstract

This Chapter expounds the modern theory of symplectic reduction in finite-dimensional Hamiltonian mechanics. This theory generalizes the well-known connection between continuous symmetries and conserved quantities, i.e. Noether's theorem. It also illustrates one of mechanics' grand themes: exploiting a symmetry so as to reduce the number of variables needed to treat a problem. The exposition emphasises how the theory provides insights about the rotation group and the rigid body. The theory's device of quotienting a state space also casts light on philosophical issues about whether two apparently distinct but utterly indiscernible possibilities should be ruled to be one and the same. These issues are illustrated using "relationist" mechanics.

Keywords: symplectic reduction, symmetry, conserved quantities, Poisson manifolds, momentum maps, relationist mechanics.

Mottoes

The current vitality of mechanics, including the investigation of fundamental questions, is quite remarkable, given its long history and development. This vitality comes about through rich interactions with pure mathematics (from topology and geometry to group representation theory), and through new and exciting applications to areas like control theory. It is perhaps even more remarkable that absolutely fundamental points, such as a clear and unambiguous linking of Lie's work on the Lie-Poisson bracket on the dual of a Lie algebra ... with the most basic of examples in mechanics, such as the rigid body and the motion of ideal fluids, took nearly a century to complete.

Marsden and Ratiu (1999, pp. 431-432).

In the ordinary theory of the rigid body, six different three-dimensional spaces $\mathbb{R}^3$, $\mathbb{R}^{3*}$, $\mathfrak{g}$, $\mathfrak{g}^*$, TG_g, T^*G_g are identified.

Arnold (1989, p. 324).

[1]email: jb56@cus.cam.ac.uk; jeremy.butterfield@all-souls.oxford.ac.uk

PRIVILEGED & CONFIDENTIAL

INVESTIGATION: T&C Network Solutions and ToddAndClare.com

REPORT

17 October 2016

PRIVILEGED & CONFIDENTIAL

A Finitely Axiomatized Formalization of Predicate Calculus with Equality

Note: This is a preprint of Megill, "A Finitely Axiomatized Formalization of Predicate Calculus with Equality," *Notre Dame Journal of Formal Logic*, 36:435-453, 1995.

The paper as published has the following errata that have been corrected in this preprint.

- On p. 439, line 7, "(Condensed detachment)" should be followed by a reference to a footnote, "The arrays start at index $i = 1$. In Step 3, i is increased *before* each comparison is made."
- On p. 446, line 17, "unnecessary" is misspelled.
- On p. 448, 2nd line from bottom, "that in Section 8." should be followed by "In addition, S3′ has the following stronger property."
- On p. 449, line 22, "u_i" should be "u_1".
- On p. 450, line 27, "Dpq" should be "Dqp".
- On p. 451, line 2, "shorter proof string" should be followed by a reference to a footnote, "Found by the OTTER theorem prover [20]."

Wave control with space-time manipulations

Mathias Fink
Institut Langevin, ESPCI ParisTech, France
13:05-13:40

Time-reversal processing is based on Huygens principles and on wavefield manipulation on spatial boundaries. It provided an elegant way to back propagate a wave field towards its initial source allowing to create, through any complex medium, a wave pattern of any required shape restricted only by diffraction limits.

Here we want to revisit these approaches by introducing another point of view, the one that Loschmidt proposed in his famous argument to create a time-reversal experiment by inversing instantaneously all velocities of the particles in a gas. The extension of this concept to wave will be discussed through the concept of time boundaries manipulation. Experiments, conducted with water waves, validating this approach will be presented. We show that sudden changes of the medium properties generate instant wave sources that emerge instantaneously from the entire space at the time disruption. The time-reversed waves originate from these "Cauchy sources" which are the counterpart of Huygens virtual sources on a time boundary. It allows us to revisit the holographic method and introduce a new approach for wave control in complex media.

In the second part of this talk, we will discussed another approach to manipulate a wave field in reverberating medium by introducing tunable metasurfaces as spatial boundaries and we will emphasize this concept for microwaves.

Firewalls are ~~Good~~ *Necessary*

Steven M. Bellovin

smb@research.att.com

908-582-5886

AT&T Bell Laboratories

Murray Hill, NJ 07974

The Lie Bracket and the Commutator of Flows

timothy e. goldberg

October 23, 2005

Abstract

There is a famous and fundamental result that states that the flows of two vector fields commute if and only if the Lie bracket of these two vector fields is the zero vector field. A natural next step is to try to relate exactly how much the Lie bracket deviates from zero to the extent to which the flows fail to commute. Can we describe the Lie bracket entirely in terms of the failure of the flows to commute?

In this talk, I will present one answer to this question, in the form of a famous (and slightly strange) equation. To build up to this, I will give a brief and general introduction to vector fields, flows, and the Lie bracket. If time permits, I will discuss the context where this formula seems most natural, that of Lie groups.

Some basic knowledge of manifolds will be helpful, but not really necessary. At the end of the talk, I will be open to any questions about comic books.

Contents

1 Manifolds **2**

2 The Tangent Bundle **2**
2.1 Tangent Vectors and the Tangent Bundle 2
2.2 Differentials of Maps 3

3 Vector Fields **3**
3.1 As Tangent Vectors 3
3.2 $C^\infty(\mathcal{M})$ 3
3.3 As Derivations 3

4 Flows **4**
4.1 A Single Pebble - Integral Curves 4
4.2 A Lot of Pebbles - The Full Flow 4
4.3 The Semigroup Property - Flows are Diffeomorphisms 4

5

Urban Boundaries and Edges

The fascination of boundaries lies in their ambivalent role of dividing and connecting at the same time. They mark the transition between different modes of existence. They transmit and control exchange between territories. They are the playground for discovery and conquest: ... They are the result of never ending competition and exhibit structure on many scales. (Richter and Peitgen, 1985, p. 571–572.)

5.1 At the Edge of the City

Boundaries, as Richter and Peitgen (1985) so graphically portray, are places which mark the transition between different regimes, different systems, and this is nowhere more so than between the rural and urban worlds at the edge of the city. In one sense, the boundary of the city marks the transition between different epochs, between an older agricultural society and the newer industrial, although the distinction is becoming weaker as contemporary society is beginning to make its transition to a post-industrial era with all its consequences for how cities will be organized. Nevertheless, such zones of transition do reflect the tension between the old and the new, places where more stable, established structures are being continually tested by a newer, ever-changing dynamic. Even in these terms, such boundaries are not likely to be 'smooth' in any sense and as we shall see, their physical form is both irregular but self-similar in that a precise transition between the old and the new can never be definitively marked out.

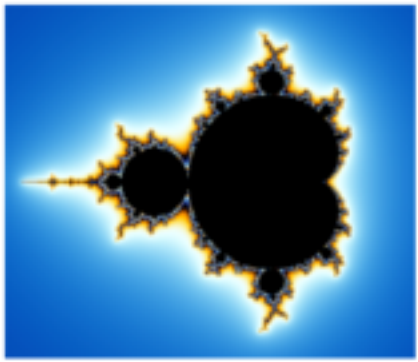
In defining the physical form of the city, its edge or boundary is the most obvious visual delimiter of its size and shape. Statistical definitions of cities rely upon the definition of boundaries, although such definitions are never comprehensive; there are so many possible ways of cutting the continuum of development from urban to rural that the general idea of a boundary remains a conceptual notion which is only given physical form through narrow definitions. Urban boundaries, however, are not simply linear constructs which mark off one side of the continuum from the other but they imply area, and thus shape (Batty, 1991). As we have argued in earlier chapters, although cities can be visualized across many dimensions, they are usually best pictured in the plane as two-dimensional phenomena and thus their boundaries immediately imply some measure of area. In this sense, the boundary is clearly something more than a one-dimensional line for whatever we conceive such an edge, we conceptualize an area.

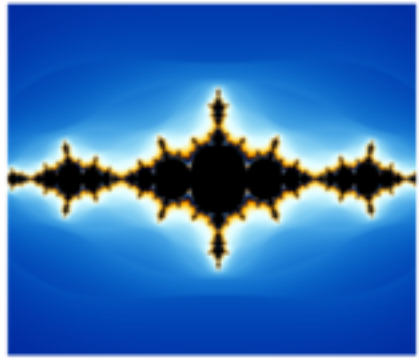
Fractals: Self-Similarity and Fractal Dimension

Math 198, Spring 2013

Background

Fractal geometry is one of the most important developments in mathematics in the second half of the 20th century. Fractals are central to understanding a wide variety of chaotic and nonlinear systems, and so have many applications in the sciences. However, they are also beautiful objects in their own right; below are pictures of two classic fractals, the *Mandelbrot set* and the *Julia set* (produced using the program *Ultra Fractal*).





What is a fractal? A fractal is a geometric object whose *fractal* dimension is larger than its *topological* dimension. This is not a very well-defined notion – there are many ways of measuring dimension (both fractal and topological), and they do not all agree. But, intuitively, a fractal is a geometric object which is "infinitely complicated" – while it may, topologically, be a curve or a surface, no matter how much it is magnified it will never "smooth out" to resemble an Euclidean space. The various notions of fractal dimension attempt to quantify this complexity.

Many fractals also have a property of *self-similarity* – within the fractal lies another copy of the same fractal, smaller but complete. In this project we will study the simplest, and best known, fractals with this property, the *strictly self-similar* fractals. We will show how to describe and create these fractals, and how to measure their fractal dimension using the *similarity dimension*.

Strictly Self-Similar Fractals

A geometric figure is **self-similar** if there is a point where every neighborhood of the point contains a copy of the entire figure. For example, imagine the figure formed by inscribing a square within another square, rotated by 45°. Then inside the inner square, inscribe another square in the same manner, and so on *ad infinitum*. Of course, we can't really draw this figure, since it contains infinitely many nested squares, but an approximation of the result is shown below:

FRACTALS AND SELF SIMILARITY

JOHN E. HUTCHINSON

This is a retyped (TeX'd) version of the article from *Indiana University Mathematics Journal* **30** (1981), 713–747 (with some minor formatting changes, a few old "typos" corrected, and hopefully few new ones introduced).

The original preprint appeared as Research Report No. 31-1979, Department of Pure Mathematics, Faculty of Science, Australian National University.

CONTENTS

1. Introduction 2
2. Preliminaries 3
2.1. Sequences of Integers 3
2.2. Maps in Metric Spaces 4
2.3. Similitudes 4
2.4. Hausdorff Metric 6
2.5. Measures 6
2.6. Hausdorff Measure 7
2.7. Geometric Measure Theory 8
3. Invariant Sets 10
3.1. Elementary Proof of Existence and Uniqueness, and Discussion of Properties 10
3.2. Convergence in the Hausdorff Metric 12
3.3. Examples 13
3.4. Remark 14
3.5. Parametrised Curves 14
4. Invariant Measures 15
4.1. Motivation 15
4.2. Definitions 16
4.3. The L metric 16
4.4. Existence and Uniqueness 16
4.5. Different Sets of Similitudes Generating the Same Set 17
5. Similitudes 18
5.1. Self-Similar Sets 18
5.2. Open Set Condition 18
5.3. Existence of Self Similar Sets. 19
5.4. Purely Unrectifiable Sets. 21
5.5. Parameter Space 24
6. Integral Flat Chains 24
6.1. The $\mathcal{F}$-metric. 24
6.2. The $\mathcal{C}$-metric 25
6.3. Invariant Chains 26
References 27

Fully Developed Turbulence and Intermittency.

U. Frisch

CNRS, Observatoire de Nice - BP 139, 06003 Nice Cedex, France

1. – Simple ideas and misconceptions about turbulence.

Viscous (non-resistive) 3-D flow can become turbulent when the Reynolds number R is sufficiently large. The latter is expressible, in terms of a typical scale L of the flow, a typical velocity V and the kinematic viscosity ν as the ratio of the viscous dissipation time L^2/ν to the circulation (turnover) time L/V. Information about turbulent flows comes from experiments, observations of nature and, increasingly, from computer simulations (cf. other lectures in this volume).

We now list and discuss some outstanding features of turbulent flows. In each case we begin with naive, possibly exceptional statements and show that they can lead to misconceptions. We shall see that the reader is at least moderately familiar with dynamical-system concepts (cf. the lectures by Ecmann, Lorenz and Ruelle in this volume and ref. [1-3]).

(i). Sharp transitions can occur when *the Reynolds number is varied.* – Physical instabilities leading to turbulent flows are discussed elsewhere in this volume. Very carefully controlled experiments on, *e.g.*, Rayleigh-Bénard convection have revealed a great variety of scenarios for the transition. In such experiments, when the flow becomes turbulent, it is often chaotic only in time and highly organized in space. In clear flows the transition may lead to much sharper chaos in both time and space (cf. the computer experiments by Orszag, Pâtera and Brachet reported in ref. [4] and the lectures by Orszag).

(ii). The flow is unstable and unpredictable. – A very weak perturbation introduced at time $t = 0$ may rapidly result in a complete distortion of the detailed flow pattern. Thus the flow may not be predictable in deterministic terms for more than a short time. It is unpredictable, however, that statistical properties (involving, *e.g.*, time averages) are stable and can be predicted (cf. the difference between predicting weather and climate).

Shell-crossing and the semi-classical limit of the Schrödinger Poisson equation

Florian Führer
IAP, Paris

12. Kosmologietag

LULEÅ UNIVERSITY OF TECHNOLOGY

2003:320 CIV

MASTER'S THESIS

Continuous Nowhere Differentiable Functions

JOHAN THIM

MASTER OF SCIENCE PROGRAMME

Department of Mathematics

2003:320 CIV • ISSN: 1402 - 1617 • ISRN: LTU - EX - - 03/320 - - SE

TRANSIENT COARSENING BEHAVIOUR IN THE CAHN-HILLIARD MODEL

HARALD GARCKE, BARBARA NIETHAMMER, MARTIN RUMPF, AND ULRICH WEIKARD

ABSTRACT. We study two–dimensional coarsening by simulations for the Cahn–Hilliard model. A scale invariance of the sharp interface limit of this model suggests that the characteristic length scale grows proportional to $t^{1/3}$, respectively the energy density decreases as $t^{-1/3}$. We compare the coarsening dynamics for different choices of data for different volume fractions. We observe that, depending on the specific data, the coarsening process can over a large time window be much slower than expected by dimensional analysis.

1. INTRODUCTION

The kinetics of phase separation in a binary alloy after quenching are characterized by three stages. Since for low temperatures the initially homogeneous state is unstable, first, domains of a new phase nucleate and grow rapidly in a second stage. Then, two phases have formed and are separated by interfacial layers which are much thinner than the typical diameter of the domains. In the last stage of the phase separation the system is driven by the reduction of the surface energy of these interfacial layers, which leads to an increase of the typical length scales in the system, a phenomenon known as coarsening.

A particular regime of interest is the one of an off–critical mixture where the volume fraction of one phase is small. Then this phase emerges as many small disconnected almost spherical

1991 *Mathematics Subject Classification.* 35K35, 35K55, 65L50, 65M12, 65M15, 65M60, 82B26.
Key words and phrases. Cahn-Hilliard equation, fourth order parabolic equation, finite element approximation,second order time discretization.

A generalized gaussian probability distribution

Herbert E. Müller, august 2017, herbert-mueller.info

The problem, and how to deal with it

We are given a probability distribution $\{p_i\}$ (discrete; the cumulative distribution is $\{P_i\}$) or $p(x)$ (continuous; the cumulative distribution is $P(x)$) and want to fit it with an easy to handle probability density function (PDF) $\phi(x)$ (the cumulative density function CDF is $\Phi(x)$) from a multi-parameter family of PDFs. In general useful parameters are ...

- *quantiles*: *median* $\tilde{\mu}=P^{-1}(0.5)$, *left deviation* $\tilde{\sigma}_-=\tilde{\mu}-P^{-1}(0.15865)$, *right deviation* $\tilde{\sigma}_+=P^{-1}(0.84135)-\tilde{\mu}$. Alternative parameters are the *half range* $\tilde{\sigma}=(\tilde{\sigma}_++\tilde{\sigma}_-)\div 2$ and *tilt* $\tilde{\delta}=(\tilde{\sigma}_+-\tilde{\sigma}_-)\div 2$ (my names). (Approximations: $0.15865\approx 33/208$, $0.84135\approx 175/208$.)
- *cumulants*: *mean* $\mu=\langle x\rangle$, *variance* $V=\langle(x-\mu)^2\rangle$, *skew* $S=\langle(x-m_1)^3\rangle$, and *kurtosis* $K=\langle(x-\mu)^4\rangle-3V^2$, where $\langle h(x)\rangle=\int dx\,p(x)h(x)$. Alternative parameters are the *standard deviation* $\sigma=V^{1/2}$, the *normalized skew* $\gamma_1=S/V^{3/2}$ and the *normalized kurtosis* $\gamma_2=K/V^2$.

If we fit the probability distribution with a 2 parameter PDF family, we use the gaussian family. The parameters are mean value μ or median $\tilde{\mu}$ and the standard deviation σ or half range $\tilde{\sigma}$ (for a gaussian PDF, $\mu=\tilde{\mu}$ and $\sigma=\tilde{\sigma}$).

PDF $p(x)=\phi_G(x;\mu,\sigma)$, with $\phi_G(x;\mu,\sigma)=\phi_N(\xi)/\sigma$ and $\phi_N(\xi)=\left[\sqrt{2\pi}\exp\left(\xi^2/2\right)\right]^{-1}$,

CDF $P(x)=\Phi_G(x;\mu,\sigma)$, with $\Phi_G(x;\mu,\sigma)=\Phi_N(\xi)=\int_{-\infty}^{\xi} d\xi\left[\sqrt{2\pi}\exp\left(\xi^2/2\right)\right]^{-1}$,

where $\xi=(x-\mu)/\sigma$.

The following two chapters are about enlarging the guassian PDF/CDF family to allow for one or two more parameters. The basic idea is the matching of CDF's:

$P(x)=\Phi_n(\xi)$, with $x=f(\xi;\text{parameters})$ and $-\infty<\xi<\infty$.

The relation between the PDFs is then

$$p(x)=\phi_G(\xi)d\xi/dx;$$

the factor $d\xi/dx=[f'(\xi)]^{-1}$ is easily calculated.

By the way: the transformation $x=f(\xi)$ can be used to numerically create data $\{x_i\}$ with the PDF $p(x)$ from normal distributed data $\{\xi_i\}$.

What the maximum entropy principle has to say

Probability distributions with known mean value and standard deviation (or with known median and half range) can be approximated with a gaussian PDF. This is the distribution prescribed by the maximum entropy principle. When the skew is also given, the maximum entropy principle prescribes the $p(x)=\exp(-\alpha+\beta x-\gamma x^2+\delta x^3)$ (*) (the signs are convenient this way); the four greek parameters are determined by the cumulant equations given earlier. The problem is that the cumulant integrals diverge for $x\to\text{sign}(\delta)\cdot\infty$, ie. the PDF can not be normalized.

One way out of this is to limit the x-domain, at least on the diverging side. One might for example consider distributions on $\mathbb{R}^+$; for $\delta<0$, the cumulant integrals of the PDF (*) conver-

Probability Surveys
Vol. 11 (2014) 237–269
ISSN: 1549-5787
DOI: 10.1214/13-PS220

Reciprocal processes. A measure-theoretical point of view*

Christian Léonard†

Modal-X. Université Paris Ouest. Bât. G, 200 av. de la République 92001 Nanterre, France
e-mail: christian.leonard@u-paris10.fr

Sylvie Rœlly

Institut für Mathematik der Universität Potsdam. Am Neuen Palais 10 14469 Potsdam, Germany
e-mail: roelly@math.uni-potsdam.de

and

Jean-Claude Zambrini‡

CFM, Universidade de Lisboa, Av. Prof. Gama Pinto 2 1649-003 Lisboa, Portugal
e-mail: zambrini@cii.fc.ul.pt

Abstract: The bridges of a Markov process are also Markov. But an arbitrary mixture of these bridges fails to be Markov in general. However, it still enjoys the interesting properties of a reciprocal process.

The structures of Markov and reciprocal processes are recalled with emphasis on their time-symmetries. A review of the main properties of the reciprocal processes is presented. Our measure-theoretical approach allows for a unified treatment of the diffusion and jump processes. Abstract results are illustrated by several examples and counter-examples.

Keywords and phrases: Markov process, reciprocal process, Markov bridge, time-symmetry, entropy minimization.

Received August 2013.

Contents

Introduction 238
1 Time-symmetry of Markov measures 240
1.1 Definition and basic properties 240
1.2 Path measures dominated by a Markov measure 243
1.3 A fundamental example: Bridges of a Markov measure 245

*The authors are thankful to the UFA-DFH for its support through the French-German Doktorandenkolleg CDFA 01-06. They also thank the anonymous reviewer for it valuable input on the article.

†Partly supported by the ANR projects CoMeCoD (ANR 2011 BS01 007 01) and STAB.

‡Partly supported by the project PTDC/MAT/120854/2010.

Three-dimensional Matrices

- Useful for representing a function of 3 variables [e.g., temperature in a volume; T = f(x,y,z)]
- Creating a 3-D matrix
- Size of a 3-D matrix
- Reshaping matrices
- Addressing elements in a 3-D matrix
- Creating a 3-D matrix with meshgrid
- 3-D visualization

The Goertzel Algorithm

Kevin Banks - August 28, 2002

The Goertzel Algorithm

The Goertzel algorithm can perform tone detection using much less CPU horsepower than the Fast Fourier Transform, but many engineers have never heard of it. This article attempts to change that.

Most engineers are familiar with the Fast Fourier Transform (FFT) and would have little trouble using a "canned" FFT routine to detect one or more tones in an audio signal. What many don't know, however, is that if you only need to detect a few frequencies, a much faster method is available. It's called the Goertzel algorithm.

Tone detection

Many applications require tone detection, such as:

- DTMF (touch tone) decoding
- Call progress (dial tone, busy, and so on) decoding
- Frequency response measurements (sending a tone while simultaneously reading back the result)-if you do this for a range of frequencies, the resulting frequency response curve can be informative. For example, the frequency response curve of a telephone line tells you if any load coils (inductors) are present on that line.

Although dedicated ICs exist for the applications above, implementing these functions in software costs less. Unfortunately, many embedded systems don't have the horsepower to perform continuous real-time FFTs. That's where the Goertzel algorithm comes in.

In this article, I describe what I call a basic Goertzel and an optimized Goertzel.

The basic Goertzel gives you real and imaginary frequency components as a regular Discrete Fourier Transform (DFT) or FFT would. If you need them, magnitude and phase can then be computed from the real/imaginary pair.

The optimized Goertzel is even faster (and simpler) than the basic Goertzel, but doesn't give you the real and imaginary frequency components. Instead, it gives you the relative magnitude squared. You can take the square root of this result to get the relative magnitude (if needed), but there's no way to obtain the phase.

In this short article, I won't try to explain the theoretical background of the algorithm. I do give some links at the end where you can find more detailed explanations. I can tell you that the algorithm works well, having used it in all of the tone detection applications previously listed (and others).

A basic Goertzel

First a quick overview of the algorithm: some intermediate processing is done in every sample. The actual tone detection occurs every Nth sample. (I'll talk more about N in a minute.)

As with the FFT, you work with blocks of samples. However, that doesn't mean you have to process the data in blocks. The numerical processing is short enough to be done in the very interrupt service routine (ISR) that is gathering the samples (if you're getting an interrupt per sample). Or, if you're getting buffers of samples, you can go ahead and process them a batch at a time.

Mestrado em Engenharia Informática
Dissertação/Estágio
Relatório Final

Cryptography in GPUs

Samuel Neves
sneves@student.dei.uc.pt

Advisor:
Filipe Araújo
Date: July 10, 2009

FCTUC DEPARTAMENTO
DE ENGENHARIA INFORMÁTICA
FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

Lecture 4

Signal Flow Graphs and recurrence relations

Metalogicon (2007) XX, 2

Hyperincursive Proof Theory

Arturo Graziano Grappone

1. Summary

This paper provides an automatic procedure to decide whether any formula of (the) first order predicative calculus is an axiom or a theorem by using Dubois's hyperincursive algorithms. The given procedure is also useful to decide whether any formula is an axiom or a theorem in Robinson's formal number theory.

2. Hyperincursive Proof Theory

2.1 To Build (BUILDING) Proofs Automatically: the Anticipatory Approach

As a matter of fact, a standard theorem proof develops from some premises (axioms or proven theorems) to the formula to prove. Gentzen's natural deduction is a classical example of this fact.[1] A limit of this approach is the non-automatism of proof building because many distinct consequences can be deduced from the same premises. The problem "given a formula determinate whether it is a theorem" has not an automatic solution in the first order predicative calculus as well.

Now, consider the time development of a standard proof. We can put its premises as "past" and its conclusion as "future". Thus the "past" does not determine the "future" because, in general, many distinct consequences can be deduced from the same premises. Instead, consider the possibility to revert a proof from its conclusion to its premises as in Aristotle's approach.[2] If we use

[1] See 1. and 2. in the references.

[2] See 3. and 4, in the references.

5 July 2017
Issue No: **11**

Grenfell Fire Response News

Housing assessments

We have committed to ensuring that by 5 July everyone from Grenfell Tower and Grenfell Walk made homeless by the fire will have received an offer of accommodation. Of the 158 families and individuals we are working with, 139 families have received offers and 19 assessments are still on-going.

Accepting a new temporary home isn't a decision to be rushed and housing officers will talk people through the options - nobody will be forced into a property that isn't suitable to their needs.

We are making every effort to ensure people have the right support around them and we want to provide everyone affected by the fire with the following reassurances.

- Everyone whose home was destroyed in the fire will be offered a temporary home in the Royal Borough of Kensington and Chelsea or a neighbouring borough.
- Accepting an offer of temporary accommodation will in no way affect your rights to permanent social housing or your benefits.
- No one will be made intentionally homeless. We will make sure that the temporary home offered is right for each individual or family.

Anyone who needs help and has yet to come forward should do so by calling **0800 458 9472** or by visiting the Westway Sports & Fitness Centre between 10am and 8pm at 1 Crowthorne Road, W10 6RP. More information is available from the housing line on **020 7361 3008**.

No action against anyone sub-letting homes

Any tenants of Grenfell Tower and Grenfell Walk who were sub-letting their home have been asked to come forward and provide information on who might have been in their flats on the night of the fire. This will help the authorities understand who was in the building and identify anyone still missing. The Government has confirmed that anyone who was unlawfully sub-letting their home will not be charged or prosecuted.

Anyone with information should call **0800 032 4539**.

The Home Office will not carry out immigration checks on those coming forward to provide information.

IN THIS EDITION

1 Housing assessments
1 Sub-letting homes
1 Health update
2 Important contacts
2 What help is on offer?
3 New leader of Kensington and Chelsea Council
3 Public meeting with Grenfell response team
3 New website
3 Westway assistance
4 What is a key worker?
4 Frequently asked questions
4 NHS support line
4 Support in the community
4 DVLA

What is this newsletter for?

This is the eleventh edition of the Grenfell Fire Response Team newsletter. We want to keep you up to date with all the latest information and services available to help.

The newsletter is also available in Arabic and Farsi languages. For up to the minute info, please follow us on Twitter **@grenfellsupport** and on Facebook at **facebook.com/grenfellsupport** or visit **www.gov.uk**

École Polytechnique Fédérale de Lausanne
Mathematics Section

FROM HOMOLOGICAL ALGEBRA TO GROUP COHOMOLOGY

Semester Project By
Maximilien Holmberg-Péroux

Responsible Professor
prof. Jacques Thévenaz

Supervisor
Rosalie Chevalley

Academic year : 2013-2014
Spring Semester

Riemannian Geometry and General Relativity

Peng Zhao

July 10, 2009

Contents

1 History and Overview **2**
1.1 What is straight? . . . 2
1.2 What is curvature? . . . 3
1.3 Foucault Pendulum and Gauss-Bonnet . . . 3

2 Riemannian Geometry **4**
2.1 Metric . . . 4
2.2 Vectors and Tensors . . . 5
2.3 Geodesics . . . 7
2.4 Connection and Curvature . . . 7

3 General Relativity **9**
3.1 Special relativity . . . 9
3.2 Einstein equation . . . 10
3.3 Variational principle . . . 10

4 Black Holes **10**
4.1 The Schwarzschild black hole . . . 10
4.2 Geodesics in Schwarzschild spacetime . . . 11
4.3 Projects . . . 12

Feasibility of 4D transverse phase space measurement at EMTEX

Kai Hock

University of Liverpool and Cockcroft Institute, UK

GSI, 12-13 September 2013

Gyrophone: Recognizing Speech From Gyroscope Signals

Yan Michalevsky Dan Boneh
Computer Science Department
Stanford University

Gabi Nakibly
National Research & Simulation Center
Rafael Ltd.

Abstract

We show that the MEMS gyroscopes found on modern smart phones are sufficiently sensitive to measure acoustic signals in the vicinity of the phone. The resulting signals contain only very low-frequency information (<200Hz). Nevertheless we show, using signal processing and machine learning, that this information is sufficient to identify speaker information and even parse speech. Since iOS and Android require no special permissions to access the gyro, our results show that apps and active web content that cannot access the microphone can nevertheless eavesdrop on speech in the vicinity of the phone.

1 Introduction

Modern smartphones and mobile devices have many sensors that enable rich user experience. Being generally put to good use, they can sometimes unintentionally expose information the user does not want to share. While the privacy risks associated with some sensors like a microphone (eavesdropping), camera or GPS (tracking) are obvious and well understood, some of the risks remained under the radar for users and application developers. In particular, access to motion sensors such as gyroscope and accelerometer is unmitigated by mobile operating systems. Namely, every application installed on a phone and every web page browsed over it can measure and record these sensors without the user being aware of it.

Recently, a few research works pointed out unintended information leaks using motion sensors. In Ref. [34] the authors suggest a method for user identification from gait patterns obtained from a mobile device's accelerometers. The feasibility of keystroke inference from nearby keyboards using accelerometers has been shown in [35]. In [21], the authors demonstrate the possibility of keystroke inference on a mobile device using accelerometers and mention the potential of using gyroscope measurements as well, while another study [19] points to the benefits of exploiting the gyroscope.

All of the above work focused on exploitation of motion events obtained from the sensors, utilizing the expected kinetic response of accelerometers and gyroscopes. In this paper we reveal a new way to extract information from gyroscope measurements. We show that gyroscopes are sufficiently sensitive to measure acoustic vibrations. This leads to the possibility of recovering speech from gyroscope readings, namely using the gyroscope as a crude microphone. We show that the sampling rate of the gyroscope is up to 200 Hz which covers some of the audible range. This raises the possibility of eavesdropping on speech in the vicinity of a phone without access to the real microphone.

As the sampling rate of the gyroscope is limited, one cannot fully reconstruct a comprehensible speech from measurements of a single gyroscope. Therefore, we resort to automatic speech recognition. We extract features from the gyroscope measurements using various signal processing methods and train machine learning algorithms for recognition. We achieve about 50% success rate for speaker identification from a set of 10 speakers. We also show that while limiting ourselves to a small vocabulary consisting solely of digit pronunciations ("one", "two", "three", ...) and achieve speech recognition success rate of 65% for the speaker dependent case and up to 26% recognition rate for the speaker independent case. This capability allows an attacker to substantially leak information about numbers spoken over or next to a phone (i.e. credit card numbers, social security numbers and the like).

We also consider the setting of a conference room where two or more people are carrying smartphones or tablets. This setting allows an attacker to gain simultaneous measurements of speech from several gyroscopes. We show that by combining the signals from two or more phones we can increase the effective sampling rate of the acoustic signal while achieving better speech recognition rates. In our experiments we achieved 77% successful recognition rate in the speaker dependent case based on the digits vocabulary.

The paper structure is as follows: in Section 2 we provide a brief description of how a MEMS gyroscope works and present initial investigation of its properties as a microphone. In Section 3 we discuss speech analysis and describe our algorithms for speaker and speech recognition. In Section 4 we suggest a method for audio signal recovery using samples from multiple devices. In Section 5 we discuss more directions for exploitation of gyroscopes' acoustic sensitivity. Finally, in Section 6 we discuss mitigation measures of this unexpected threat. In

CA SiteMinder® Web Access Manager

Programming Guide for C

r12 SP1

Second Edition

CA SiteMinder®

Web Agent Installation Guide

r12.0 SP2

SITEMINDER SSO FOR EMC® DOCUMENTUM® REST

ABSTRACT

This white paper provides a detailed review of SiteMinder SSO integration with EMC Documentum REST Services by exploring the architecture, consumption workflow, deployment recommendations and alternatives, and the troubleshooting for this integration.

January, 2014

REDEFINE

EMC WHITE

EMC²

Revision Date: 11/01/2016

DELL EMC
EXPORT COMPLIANCE PRODUCT INFORMATION

All export information and assistance provided by DellEMC is provided for information purposes only. DellEMC makes no representation or warranty as to the accuracy or reliability of such regulations. Any use of such regulations by you is at your own risk. DellEMC is in no way responsible for any damages whether direct, consequential, incidental, or otherwise, suffered by you as a result of using or relying upon such regulations for any purpose whatsoever.

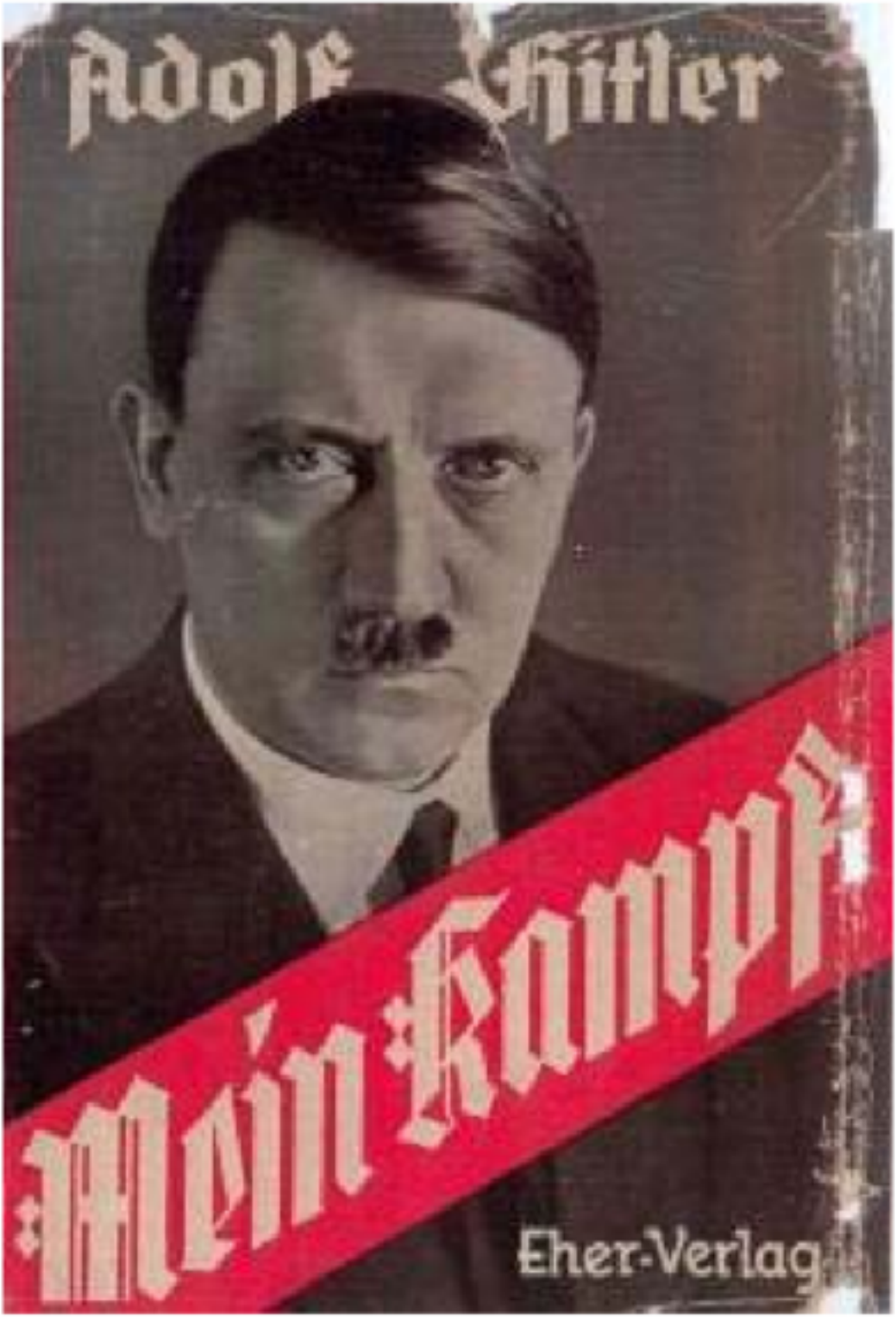
You as the exporter, re-exporter, or importer are responsible for ensuring that DellEMC products are exported and imported in accordance with the requirements of the country specific Trade Compliance regulations as well as U.S. Export Administration Regulations (EAR). Each commodity or software product has a respective Export Control Classification Number (ECCN) (per the United States Department of Commerce Export Administration Regulations). End-user, End-use and Country of ultimate destination may affect export-licensing requirements. You are urged to consult the Export Administration Regulations, the Bureau of Industry and Security's Export Counseling Division, and other appropriate sources concerning restricted/prohibited uses and the exportation/re-exportation of DellEMC products.

All Export Control Classification Numbers (ECCNs), License Exception values and CCATS provided herein are subject to change without notice. If you require further assistance, please contact DELL EMC Global Trade Compliance

Product	ECCN	License Exception	CCATS
Agile Marketer	EAR99		
Alphastor v.3.1 SP2	EAR99		
Application Discovery Manager v.6.1	5A002/5D002	ENC Unrestricted	G077121
Application Stack Manager (ASM)	5D002	ENC Unrestricted	G077274
ApplicationXtender 7.0, 8.0	EAR99		
AppSync v.1.0 through 3.0	5D002	ENC 740.17 (b)(1)	
Architect v2.0 app	EAR99		
Are 53 App	EAR99		
Atmos Client v.1.0	5D002	ENC 740.17 (b)(1)	
Atmos-Maui), Atmos 2.0 through 3.0	5D002	ENC Unrestricted	G063677
Authentica Content Server	5D002	ENC Unrestricted	G027198
Authentica Server Management API for C	5D002	ENC Unrestricted	G027967
Authentica Server Management API for COM	5D002	ENC Unrestricted	G027967
AVALONidm (Intelligent Data Manager)	5D002	ENC Unrestricted	G016358
Avamar AXION	5D002	ENC Unrestricted	G035352
Avamar Data Transport "ADT" v.1.0	5D002	ENC Unrestricted	G074002
Avamar Extended Retention	5A002/5D002	ENC 740.17 (b)(1)	
Avamar Plugin for vCloud Director version 2.0.2	5D002	ENC 740.17 (b)(1)	
Avamar Plugin for vRealize Automation v.2	EAR99		
Avamar Replicator	5D002	ENC Unrestricted	G035352
Avamar v. 4.0	5D002	ENC Unrestricted	G059697

Hackers are Humans too

Cyber leads to CI leads


Adolf Hitler
Mein Kampf
Eher-Verlag

Chapter 3

Operator methods in quantum mechanics

While the wave mechanical formulation has proved successful in describing the quantum mechanics of bound and unbound particles, some properties can not be represented through a wave-like description. For example, the electron spin degree of freedom does not translate to the action of a gradient operator. It is therefore useful to reformulate quantum mechanics in a framework that involves only operators.

Before discussing properties of operators, it is helpful to introduce a further simplification of notation. One advantage of the operator algebra is that it does not rely upon a particular basis. For example, when one writes $\hat{H} = \frac{\hat{p}^2}{2m}$, where the hat denotes an operator, we can equally represent the momentum operator in the spatial coordinate basis, when it is described by the differential operator, $\hat{p} = -i\hbar\partial_x$, or in the momentum basis, when it is just a number $\hat{p} = p$. Similarly, it would be useful to work with a basis for the wavefunction which is coordinate independent. Such a representation was developed by Dirac early in the formulation of quantum mechanics.

In the parlons of mathematics, square integrable functions (such as wavefunctions) are said form a vector space, much like the familiar three-dimensional vector spaces. In the **Dirac notation**, a state vector or wavefunction, ψ, is represented as a "ket", $|\psi\rangle$. Just as we can express any three-dimensional vector in terms of the basis vectors, $\mathbf{r} = x\hat{\mathbf{e}}_1 + y\hat{\mathbf{e}}_2 + z\hat{\mathbf{e}}_3$, so we can expand any wavefunction as a superposition of basis state vectors,

$$|\psi\rangle = \lambda_1|\psi_1\rangle + \lambda_2|\psi_2\rangle + \cdots .$$

Alongside the ket, we can define the "bra", $\langle\psi|$. Together, the bra and ket define the **scalar product**

$$\langle\phi|\psi\rangle \equiv \int_{-\infty}^{\infty} dx\, \phi^*(x)\psi(x)\,,$$

from which follows the identity, $\langle\phi|\psi\rangle^* = \langle\psi|\phi\rangle$. In this formulation, the real space representation of the wavefunction is recovered from the inner product $\psi(x) = \langle x|\psi\rangle$ while the momentum space wavefunction is obtained from $\psi(p) = \langle p|\psi\rangle$. As with a three-dimensional vector space where $\mathbf{a}\cdot\mathbf{b} \leq |a||b|$, the magnitude of the scalar product is limited by the magnitude of the vectors,

$$\langle\psi|\phi\rangle \leq \sqrt{\langle\psi|\psi\rangle\langle\phi|\phi\rangle}\,,$$

a relation known as the **Schwartz inequality**.

Studies in History and Philosophy of Modern Physics 36 (2005) 680–690

Studies in History and Philosophy of Modern Physics

www.elsevier.com/locate/shpsb

Essay review

Quantum processes: A Whiteheadian interpretation of quantum field theory

Jonathan Bain

Department of Humanities and Social Sciences, Polytechnic University, Brooklyn, NY 11201, USA

Frank Hättich, Quantum processes: A Whiteheadian interpretation of quantum field theory, Agenda Verlag, Münster, ISBN 3-89688-204-X, 2004 (pp. 294 Euro 29, 90)

1. Introduction

Quantum processes: A Whiteheadian interpretation of quantum field theory is an ambitious and thought-provoking exercise in physics and metaphysics, combining an erudite study of the very complex metaphysics of A.N. Whitehead with a well-informed discussion of contemporary issues in the philosophy of algebraic quantum field theory. Hättich's overall goal is to construct an interpretation of quantum field theory. He does this by translating key concepts in Whitehead's metaphysics into the language of algebraic quantum field theory. In brief, this Hättich–Whitehead (H–W, hereafter) interpretation takes "actual occasions" as the fundamental ontological entities of quantum field theory. An actual occasion is the result of two types of processes: a "transition process" in which a set of initial possibly-possessed properties for the occasion (in the form of "eternal objects") is localized to a space–time region; and a "concrescence process" in which a subset of these initial possibly-possessed properties is selected and actualized to produce the occasion. Essential to these processes is the "underlying activity", which conditions the way in which properties are initially selected and subsequently actualized. In short, under the H–W interpretation of quantum field theory, an initial set of possibly-possessed eternal objects is represented by a Boolean sublattice of the lattice of projection

E-mail address: jbain@duke.poly.edu.

1355-2198/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.shpsb.2005.05.004

Hypercomplex numbers and their matrix representations

A short guide for engineers and scientists

Herbert E. Müller
http://herbert-mueller.info/

Abstract

Hypercomplex numbers are composite numbers that sometimes allow to simplify computations. In this article, the multiplication table, matrix representation and useful formulas are compiled for eight hypercomplex number systems.

Interval Arithmetic and Recursive Subdivision for Implicit Functions and Constructive Solid Geometry

Tom Duff*
AT&T Bell Laboratories
600 Mountain Avenue
Murray Hill, New Jersey 07974

Abstract

Recursive subdivision using interval arithmetic allows us to render CSG combinations of implicit function surfaces with or without anti aliasing. Related algorithms will solve the collision detection problem for dynamic simulations and allow us to compute mass, center of gravity, angular momenta and other integral properties required for Newtonian dynamics.

Our hidden surface algorithm runs in 'constant time.' Their running times are nearly independent of the number of primitives in a scene, for scenes in which the visible details are not much smaller than the pixels. The collision detection and response algorithms are wholly robust. Collisions are never missed due to numerical error and we can provide guaranteed bounds on the values of integrals.

CR Categories and Subject Descriptors: G.1.0 [Numerical Analysis]: Numerical Algorithms; I.3.3 [Picture and Image Generation]: Display algorithms, Viewing algorithms; I.3.5 [Computational Geometry and Object Modeling]: Curve, surface, solid and object representations; I.3.5 [Computational Geometry and Object Modeling]: Hierarchy and geometric transformations; I.3.7 [Three-Dimensional Graphics and Realism]: Visible hidden surface algorithms, Animation

General Terms: Algorithms

Additional Keywords and Phrases: anti-aliasing, compositing, computer-aided animation, recursive subdivision, image synthesis, dynamic simulation, collision detection

1. Introduction

The most commonly-used geometric representations in computer graphics are local. Polygonal models, for example, specify which points are on an object's surface, and tell us nothing whatsoever about the rest of the space in which the object is embedded, except by omission. It requires substantial mental effort to formulate answers to questions like "Do these objects intersect?", or "What parts of this object are visible?" or even something as simple as "What is the volume of this object?". More elaborate surface representations, like Bezier patches or NURBS don't make these questions any easier—since they only constrain the objects locally, they make it difficult to answer global questions about them.

Likewise, the computational methods we normally use are mostly local. The ray-tracing algorithm, for example, tries to compute an image one pixel at a time by testing every point in the scene for intersection with a ray from the eye point through the pixel's center. Of course any decent ray tracer goes to a lot of trouble to avoid most of this work. But an algorithm that had instant access to global information about the scene wouldn't need to go to the trouble—it would know immediately what parts of the scene were relevant to what parts of the screen.

A good example of a global representation is the BSP tree [11]. Each node of a BSP tree gives us the information about the object's relationship to the whole of the space it's embedded in. The nodes effectively say about their subtrees "in this half of space, you need not think about this half of the model." BSP trees naturally engender simple algorithms for all sorts of geometric tasks, from hidden surface removal to object intersection [15] to volume integration [2], that make natural, effective use of the global information stored in the model.

This paper will examine in detail another global object representation and its algorithms based on implicit functions, Constructive Solid Geometry and interval arithmetic.

Briefly, implicit functions are real functions for classifying points in space as inside on or outside an object. Interval arithmetic allows us to extend these tests to whole chunks of space at once. Constructive Solid Geometry allows us to combine simpler objects to keep unwieldy primitives (like infinite ray tubes) under control and model many important industrial and natural processes that go into creating geometric forms.

2. Implicit Functions

Implicit functions are an indirect representation of solid objects. Given a function of three variables $F(x,y,z)$, we can use the equation $F(x,y,z) = 0$ to specify the points on a surface. The representable surfaces range from the mundane to the exotic: from plane: $ax+by+cz+d=0$; and quadrics: the spheres, cones, cylinders and paraboloids of elementary geometry—to more exotic polynomial surfaces like those of Kummer and Dupin [9] to Barr's downright weird twisted, bent and tapered superellipsoids [4].

If F is continuous, we can cleanly partition space inside, on or outside the object depending on whether $F<0$, $F=0$ or $F>0$ [1]. This is the global property we are after. F classifies every point in space in its relationship to the surface. Its regions of space are created by the surface, the fact that F's sign does not change in a region of connected space, is hidden-surface and other geometric algorithms that can be exploited by using interval arithmetic to quickly obtain bounds on $F(x,y,z)$ for whole ranges of x, y and z.

3. Interval Arithmetic

Interval arithmetic [16] generalizes ordinary arithmetic to closed, bounded ranges of real numbers. If X and $\bar{X}$ are real numbers with $\underline{X} \le \bar{X}$, then X is an interval

$$X = [\underline{X}, \bar{X}] = \{x \mid \underline{X} \le x \le \bar{X}\}$$

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

Newton-Krylov-Schwarz Methods in CFD

X.-C. Cai
Department of Computer Science
University of Colorado, Boulder, CO 80309 USA
W. D. Gropp
Mathematics and Computer Science Division
Argonne National Laboratory, Argonne, IL 60439 USA
D. E. Keyes
Institute for Computer Applications in Science and Engineering
NASA-LaRC, Hampton, VA 23681 USA,
Department of Computer Science
Old Dominion University, Norfolk, VA 23529 USA, and
Department of Mechanical Engineering
Yale University, New Haven, CT 06520 USA
M. D. Tidriri
Institute for Computer Applications in Science and Engineering
NASA-LaRC, Hampton, VA 23681 USA

Summary

Newton-Krylov methods are potentially well suited for the implicit solution of nonlinear problems whenever it is unreasonable to compute or store a true Jacobian. Krylov-Schwarz iterative methods are well suited for the parallel implicit solution of multidimensional systems of boundary value problems that arise in CFD. They provide good data locality so that even a high-latency workstation network can be employed as a parallel machine. We call the combination of these two methods Newton-Krylov-Schwarz and report numerical experiments on some algorithmic and implementation aspects: the use of mixed discretization schemes in the (implicitly defined) Jacobian and its preconditioner, the selection of the differencing parameter in the formation of the action of the Jacobian, the use of a coarse grid in additive Schwarz preconditioning, and workstation network implementation. Three model problems are considered: a convection-diffusion problem, the full potential equation, and the Euler equations.

1. Introduction

Newton-like methods, together with fully implicit linear solvers, in principle allow a more rapid asymptotic approach to steady states, $f(u) = 0$, than do time-explicit methods or semi-implicit methods based on defect correction. Strict Newton methods have the disadvantage of requiring solutions of linear systems of equations based on the Jacobian, $f_u(u)$, of the true steady nonlinear residual and are often impractical in several respects:

AN INTRODUCTION *to the* THREE VOLUMES *of* KARL MARX'S *CAPITAL*

Michael Heinrich

Translated by Alexander Locascio

U.S. POLICY TOWARD PUTIN'S RUSSIA

HEARING

BEFORE THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JUNE 14, 2016

Serial No. 114–191

Printed for the use of the Committee on Foreign Affairs

Available via the World Wide Web: http://www.foreignaffairs.house.gov/ or
http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PUBLISHING OFFICE

20–454PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

Prepared Testimony of Salim Neino, Chief Executive Officer, Kryptos Logic

U.S. House of Representatives Committee on Science, Space & Technology, Joint Subcommittee on Oversight and Subcommittee on Research and Technology Hearing

15 June 2017

Chairman LaHood, Chairwoman Comstock, Ranking Member Beyer and Ranking Member Lipinski, thank you for the opportunity to appear before you today at this joint Subcommittee hearing. We greatly appreciate your interest in cybersecurity and look forward to sharing our thoughts and perspectives with you and your Members.

WannaCry Involvement and Response

On May 12th, 2017, Kryptos Logic identified a high-velocity, high-impact global security threat with the immediate potential to cause an immeasurable amount of damage. While the intent of this threat was unclear and its motives and origins ambiguous, it was immediately evident that its approach was unusually reckless. This threat has now popularly become known as ``WannaCry." It was at this time that Marcus Hutchins, Director of Threat Intelligence for Kryptos Logic's Vantage (our breach monitoring platform and feed) notified me of our team's active monitoring of the developing situation.

On this date at approximately 10:00 a.m. Eastern time, while investigating the code of WannaCry, we identified what looked like an anti-detection mechanism, which tested for the existence of a certain random-looking domain name. Our team proceeded to register the domain associated to this mechanism and directed it to one of the "sinkholes" controlled by and hosted on the Kryptos Logic network infrastructure. We then noticed and confirmed that the propagation of the WannaCry attack had come to a standstill because of what we refer to as its ``kill-switch" having been activated by our domain registration.

While our efforts effectively stopped the attack, and prevented WannaCry from continuing to deploy its ransom component (which irreversibly destroys important files) we knew that by then the attack had already propagated freely for hours, at minimum. Based on the velocity of the attack, estimated by sampling data we collected from our infrastructure currently blocking the attack, we believe had that anywhere between 1-2 million systems may have been affected in the hours prior to activating the kill-switch, contrary to the widely reported – and more conservative – estimate of 200,000 systems.

One month after registering the kill-switch domain, we have mitigated over 60 million infection attempts – approximately 7 million in the United States – and we estimate that these could have impacted a minimum 10-15 million unique systems. I will note that the largest attack we thwarted and measured to date from WannaCry was not on May 12 or 13th when the attack started, but began suddenly on June 8th and 9th on a well-funded hospital in the east coast of the United States. It is very likely the health system is still unaware of the event. We measured approximately 275,000 thwarted infection attempts within a 2-day period. Another hospital was hit on May 30th, in another part of the country. A high-school in the Midwest was just hit beginning on June 9th.

Science
AAAS

If you wish to distribute this article to others, you can order high-quality copies for your colleagues, clients, or customers by clicking here.

Permission to republish or repurpose articles or portions of articles can be obtained by following the guidelines here.

The following resources related to this article are available online at www.sciencemag.org (this information is current as of March 31, 2011):

Updated information and services, including high-resolution figures, can be found in the online version of this article at:
http://www.sciencemag.org/content/332/6025/60.full.html

Supporting Online Material can be found at:
http://www.sciencemag.org/content/suppl/2011/02/08/science.1200970.DC1.html
http://www.sciencemag.org/content/suppl/2011/02/10/science.1200970.DC2.html

A list of selected additional articles on the Science Web sites related to this article can be found at:
http://www.sciencemag.org/content/332/6025/60.full.html#related

This article cites 7 articles, 2 of which can be accessed free:
http://www.sciencemag.org/content/332/6025/60.full.html#ref-list-1

This article appears in the following subject collections:
Computers, Mathematics
http://www.sciencemag.org/cgi/collection/comp_math

www.sciencemag.org

Non-commutative probability, conditional expectation values as weak values.

Basil J. Hiley.

www.bbk.ac.uk/tpru.

Maurice de Gosson
Vienna

Rob Flack
UCL

Bob Callaghan
BBK

Moyal and Clifford Algebras in the Bohm Approach.

Basil J. Hiley

www.bbk.ac.uk/tpru.

HOUSE OF LORDS

SESSION 2006–07

[2007] UKHL 46

on appeal from: [2006] EWCA Civ 1140, [2007] EWHC 651 (Admin)

OPINIONS

OF THE LORDS OF APPEAL

FOR JUDGMENT IN THE CAUSE

Secretary of State for the Home Department (Respondent) *v.*
MB (FC) (Appellant)
Secretary of State for the Home Department (Respondent) *v.*
AF (FC) (Appellant) (Civil Appeal from Her Majesty's High Court of Justice)
Secretary of State for the Home Department (Appellant) *v.*
AF (FC) (Respondent) (Civil Appeal from Her Majesty's High Court of Justice)

Appellate Committee

Lord Bingham of Cornhill
Lord Hoffmann
Baroness Hale of Richmond
Lord Carswell
Lord Brown of Eaton-under-Heywood

Counsel

Appellants:
MB: Tim Owen QC
Kate Markus
Ali Bajwa
(Instructed by Atani & Co)
AF: Timothy Otty QC
Zubair Ahmad
(Instructed by Middleweeks)

Respondents:
Ian Burnett QC
Philip Sales QC
Tim Eicke
Cecilia Ivimy
Andrew O'Connor
(Instructed by Treasury Solicitor)

Intervener

Justice:
Michael Fordham QC and Tom Hickman
(Instructed by Clifford Chance)

Special Advocates
Michael Supperstone QC and Judith Farbey
(Instructed by Special Advocates' Support Office)

Hearing dates:
5, 9, 10, 11, 12 and 13 July 2007

ON

WEDNESDAY 31 OCTOBER2007

JSBN: HR

Topology and its Applications 96 (1999) 209–216

TOPOLOGY AND ITS APPLICATIONS

A homogeneous continuum without the property of Kelley

Włodzimierz J. Charatonik [a,b,1]

[a] *Mathematical Institute, University of Wrocław, pl. Grunwaldzki 2/4, 50-384 Wrocław, Poland*

[b] *Departamento de Matemáticas, Facultad de Ciencias, UNAM, Circuito Exterior, Ciudad Universitaria, D.F., 04510 México, México*

Received 2 February 1997; received in revised form 8 January 1998

Abstract

We generalize the property of Kelley for continua to the non-metric case. Basic properties that are true in metric case are shown to be true in general. An example is constructed showing that, unlike for metric continua, the homogeneity does not imply the property of Kelley. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Continuum; Homogeneous; Effros property; Property of Kelley

AMS classification: Primary 54C99; 54F15; 54G20, Secondary 54B20

1. Introduction

The property of Kelley was defined in [3] as Property 3.2 and investigated for metric continua. It was first applied to investigate hyperspace contractibility. Then the main properties of the property of Kelley were proven by R.W. Wardle in [5]. Until now it has played an important role not only in the hyperspace theory, but in the whole continuum theory. Here we extend its definition for Hausdorff continua and we verify what properties of it are valid in this wider sense. The main result is that, unlike in the metric case, the homogeneity does not imply the property of Kelley. Since the Effros property implies the property of Kelley, this is another example of a homogeneous continuum that is non-Effros, see [1].

[1] E-mail: wjcharat@math.uni.wroc.pl; wjcharat@ya.fciencias.unam.mx.

0166-8641/99/$ – see front matter © 1999 Elsevier Science B.V. All rights reserved.
PII: S0166-8641(98)00055-8

A Primer on Homotopy Type Theory Part 1: The Formal Type Theory

James Ladyman & Stuart Presnell
james.ladyman@bristol.ac.uk
stuart.presnell@bristol.ac.uk

Friday 21st November, 2014

Abstract

This Primer is an introduction to Homotopy Type Theory (HoTT). The original source for the ideas presented here is the "HoTT Book" – *Homotopy Type Theory: Univalent Foundations of Mathematics* published by The Univalent Foundations Program, Institute for Advanced Study, Princeton. In what follows we freely borrow and adapt definitions, arguments and proofs from the HoTT Book throughout without always giving a specific citation.[1] However, whereas that book provides an introduction to the subject that rapidly involves the reader in advanced technical material, the exposition in this Primer is more gently paced for the beginner. We also do more to motivate, justify, and explain some aspects of the theory in greater detail, and we address foundational and philosophical issues that the HoTT Book does not.

In the course of studying HoTT we developed our own approach to interpreting it as a foundation for mathematics that is independent of the homotopy interpretation of the HoTT Book though compatible with it. In particular, we interpret types as concepts; we have a slightly different understanding of subtypes and the Curry-Howard correspondence; and we offer a novel approach to the justification of the elimination rule for identity types in section 7 below (though it builds on a known mathematical

[1] Page numbers for the HoTT book refer to the edition on Google Books, available at `http://books.google.co.uk/books?id=L1DSNv3ypOC`. Note that the HoTT Book is being continually corrected and updated. The latest edition (last updated on March 6th 2014 at the time of writing this document) is available at `http://homotopytypetheory.org/book/`.

HTTP Parameter Pollution Vulnerabilities

in Web Applications

Is your web application protected against HTTP Parameter Pollution? A new class of injection vulnerabilities allows attackers to compromise the logic of the application to perform client and server-side attacks. HPP can be detected and avoided. But how?

What you will learn...

- what is HTTP Parameter Pollution (HPP)
- how to spoil HPP flaws in web applications
- how to prevent HPP in web developing

What you should know...

- basic understanding of web technologies and languages
- web security knowledge is a plus

In the last twenty years, web applications have grown from simple, static pages to complex, full-fledged dynamic applications. Web applications can accept and process hundreds of different HTTP parameters to be able to provide users with rich, interactive services. As a result, dynamic web applications may contain a wide range of input validation vulnerabilities such as *Cross-Site Scripting* (XSS) and SQL injection (SQLi). According to the OWASP Testing Guide v3, *The most common web application security weakness is the failure to properly validate input coming from the client or environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications [...]*. Several kind of injection flaws exist and they are usually strictly related to the specific metalanguage used by the subsystems: XML Injection, SQL Injection, LDAP Injection, etc. Each application layer uses a specific set of technologies and a characteristic contextual language.

In 2009, *Luca Carettoni* and *Stefano di Paola* introduced a new class of web vulnerabilities called HTTP Parameter Pollution (HPP) that permits to inject new parameters inside an existing HTTP parameter. Lately, in 2010, *Marco Balduzzi* of the International Secure Systems Lab at EURECOM investigated the problem and developed a system, called *PAPAS*, to detect HPP flaws in an automated way. He used PAPAS to conduct a large-scale study on popular websites and discovered that many real web applications are affected by HPP flaws at different levels.

This article discusses why and how applications may be vulnerable to HTTP Parameter Pollution. By analyzing different attacking scenarios, we introduce the HPP problem. We then describe PAPAS, the system for the detection of HPP flaws, and we conclude by giving the different countermeasures that conscious web designers may adopt to deal with this novel class of injection vulnerabilities.

Parameter Precedence

In the context of websites, when the user's browser wants to transfer information to the web application (e.g. a server-side script), the transmission can be performed in three different ways. The HTTP protocol allows to provide input inside the URI query string (GET parameters), in the HTTP headers (e.g. within the Cookie field), or inside the request body (POST parameters). The adopted technique depends on the application and on the type and amount of data that has to be transferred.

This standard mechanism for passing parameters is straightforward, however, the way in which the query string is processed to extract the single values depends on the application, the technology, and the development language that is used.

The problem arises when a developer expects to receive a single parameter and, therefore, invokes methods (such as `Request.getParameter` in JSP) that only return a single value. In this case, if more than one parameter with the

FRANK BOLDEWIN'S
WWW.RECONSTRUCTER.ORG

```
push    2
call    sub_672B3730
add     esp, 0Ch
test    eax, eax
jnz     short loc_672B5428
lea     edx, [esp+110h+LibFileName]
push    edx
call    sub_672B35F0
mov     edi, off_672CA058
or      ecx, 0FFFFFFFFh
xor     eax, eax
lea     edx, [esp+114h+LibFileName]
repne scasb
not     ecx
sub     edi, ecx
mov     esi, edi
mov     ebx, ecx
cmp     eax, 2Eh
jnz     loc_672B5455
lea     ecx, [esp+110h+LibFileName]
push    104h
push    ecx
push    2
call    sub_672B3730
add     esp, 0Ch
test    eax, eax
jnz     short loc_672B5428
lea     edx, [esp+110h+LibFi
push    edx
call    sub_672B35F0
mov     edi, off_672CA058
or      ecx, 0FFFFFFFFh
xor     eax, eax
lea     edx, [esp+114h+LibFileName]
repne scasb
not     ecx
sub     edi, ecx
mov     esi, edi
mov     ebx, ecx
```

Hunting rootkits with Windbg v1.1

Frank Boldewin

A Simplification of Girard's Paradox

Antonius J.C. Hurkens

Klaasstokseweg 7, 5443 NS Haps, The Netherlands
e-mail: hurkens@sci.kun.nl

Abstract. In 1972 J.-Y. Girard showed that the Burali-Forti paradox can be formalised in the type system U. In 1991 Th. Coquand formalised another paradox in U^-. The corresponding proof terms (that have no normal form) are large. We present a shorter term of type $\bot$ in the Pure Type System λU^- and analyse its reduction behaviour. The idea is to construct a universe $\mathcal{U}$ and two functions such that a certain equality holds. Using this equality, we prove *and* disprove that a certain object in $\mathcal{U}$ is well-founded.

1 Introduction

Jean-Yves Girard (1972) derived a contradiction in the type system U by formalising a paradox inspired by those of Burali-Forti and Russell. By formalising another paradox, Thierry Coquand (1994) showed that the type system U^- is also inconsistent. So there are large proof terms of type $\bot$ in these type systems.

In Section 3 we present a relatively short term of type $\bot$ in λU^-. This Pure Type System and some notation is described in Section 2. In the last section we show that the β-reduction behaviour of the proof term is very simple.

In the other sections we will see that the proof has the same ingredients as Burali-Forti's paradox: a universe $\mathcal{U}$, a relation $<$ on $\mathcal{U}$, an object Ω in $\mathcal{U}$, and the question whether Ω is well-founded or not.

In Section 4 we describe Burali-Forti's paradox and some simplifications. We analyse the connection between the universe of all ordinals at its power set. In Section 5 we introduce *paradoxical* universes. These are connected to their power set in such a way that we can derive a Burali-Forti like contradiction. This can be formalised in Pure Type Systems. The formalisation can be simplified by considering *powerful* universes. In Section 6 we see how these universes are connected to the power set of their power set.

2 Pure Type Systems

In this section, we describe some Pure Type Systems. For more details, see for example (Barendregt 1992) or (Geuvers 1993).

2.1 The Pure Type Systems λHOL, λU^-, and λU

The typed λ-calculus λHOL (*Higher Order Logic*) is the Pure Type System (with β-conversion) given by the *sorts* $*$, $\Box$, and $\triangle$, the *axioms* $* : \Box$ and $\Box : \triangle$, and

DIMACS Series in Discrete Mathematics
and Theoretical Computer Science
Volume 10, 1993

The Laplacian of a Hypergraph

FAN R. K. CHUNG

March 26, 1993

1. Introduction

Suppose G is a graph with node set N and edge set E consisting of unordered pairs of N. The Laplacian of G, denoted by $L(G)$, is defined to be $D - A$ where A is the adjacency matrix of G (i.e., $A_{ij} = 1$ if $\{i, j\}$ is in E and 0 otherwise), and D is a diagonal matrix with $(D)_{ii} = d(i)$, the degree of the i-th node. Laplacians and the distribution of their eigenvalues imply many important properties of graphs [7,14,15,18,22,29], and lead to many applications in a variety of areas [2,6,13,27,28,32,34,35]. A natural generalization of graphs are so-called hypergraphs. In particular, a k-uniform hypergraph (or a k-graph for short) has a node set N and edges consisting of k-subsets of N. (Thus, ordinary graphs are 2-graphs.) Many attempts have been made to define the analogue of the Laplacian for hypergraphs and for some notion of eigenvalues of k-graphs [3,16]. However, various obstructions seem to make the generalization to k-graphs difficult.

In this paper, we will define the Laplacian of a k-graph by considering various homological aspects of hypergraphs. The eigenvalues of the Laplacians will be examined and relations to other graph properties will be derived. In particular, the eigenvalues of some specified hypergraphs will be evaluated.

In an earlier paper [10], the cohomological aspects of hypergraphs over the finite field $\mathbb{Z}_2$ (and, in general, $\mathbb{Z}_p$) were investigated. The Laplacians for the case of $\mathbb{Z}_2$ have quite different properties from the Laplacians considered here. In this paper, since the operations are over $\mathbb{C}$, the field of complex numbers, the eigenvalues of the Laplacian can be considered. This paper is organized as follows. The definition of the Laplacian will be given in Section 2. The homological

1991 *Mathematics Subject Classification.* 05C35.
This paper is in final form.

© 1993 American Mathematical Society
0082-0717/93 $1.00 + $.25 per page

Interacting Bialgebras are Frobenius

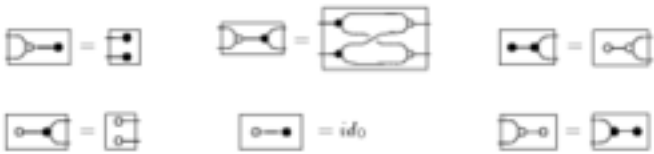
Filippo Bonchi[1], Paweł Sobociński[2] and Fabio Zanasi[1]

[1] ENS de Lyon, Université de Lyon, CNRS, INRIA, France
[2] University of Southampton, UK

Abstract. Bialgebras and Frobenius algebras are different ways in which monoids and comonoids interact as part of the same theory. Such theories feature in many fields: e.g. quantum computing, compositional semantics of concurrency, network algebra and component-based programming.
In this paper we study an important sub-theory of Coecke and Duncan's ZX-calculus, related to strongly-complementary observables, where two Frobenius algebras interact. We characterize its free model as a category of $\mathbb{Z}_2$-vector subspaces. Moreover, we use the framework of PROPs to exhibit the modular structure of its algebra via a universal construction involving span and cospan categories of $\mathbb{Z}_2$-matrices and distributive laws between PROPs. Our approach demonstrates that the Frobenius structures result from the interaction of bialgebras.

1 Introduction

We report on a surprising meeting point between two separate threads of research. First, Coecke and Duncan [9] introduced the ZX-calculus as a graphical formalism for multi-qubit systems, featuring two interacting separable Frobenius algebras, which we distinguish here graphically via white and black colouring. The following equations capture the interaction for an important fragment of the calculus related to strongly complementary observables [10]:



The aforementioned and related works (see e.g. [11]) emphasise the interaction of two different (here, white and black) Frobenius structures. As we will explain, from an algebraic point of view, it is natural to consider this system as two (anti-separable) *bialgebras* interacting via two distributive laws of PROPs. We will show that the individual Frobenius structures arise as a *result* of these interactions. Consequently, we call the theory above *interacting bialgebras*, and the corresponding (free) PROP $\mathbb{IB}$.

Second, following the work of Katis, Sabadini, Walters and others on the $\mathsf{Span}(\mathbf{Graph})$ algebra [13] of transitica systems, the second author introduced

ON THE SOLUTION OF QUINTIC EQUATIONS

By Professor Sophus Bergland,
University of Oslo, Oslo, Norway.

1. Introduction. Equations of the second, third, and fourth degrees, as is well known, may be solved with a finite number of radicals. If, however, the equation is of higher degree than the fourth, this is, as a rule, no longer possible. Equations of the fifth or higher degrees must consequently be solved by other irrationalities than radicals, and it is solutions of this kind that will be the subject of this paper. We will consequently not occupy ourselves with the many methods, graphic as well as analytic (for instance developments in series according to powers of the coefficients) for numerical calculation of the roots.

When seeking for other irrationalities than radicals for the solution of algebraic equations, it is natural to try if it is not possible, by means of a suitable specialization of certain transcendental functions, previously known and investigated, to obtain the desired algebraic irrationalities.

The first step in this direction was taken by Hermite[1] in 1858. We know that when in the cubic equation

$$x^3 - 3x^2 + 2c = 0$$

the parameter c is expressed in terms of an auxiliary variable a on putting

$$c = \sin a,$$

the three roots are given as functions of a by the expressions

$$2\sin\frac{a}{3},\quad 2\sin\frac{a+2\pi}{3},\quad 2\sin\frac{a+4\pi}{3}.$$

Hermite considered the quintic equation of the form

$$x^5 - x - c = 0 \tag{1}$$

and showed that the parameter c as well as the five roots x might be expressed in terms of an auxiliary variable by certain series well known in the theory of elliptic functions. The method is thus analogous to that indicated for the solution of the foregoing cubic equation.

The result of Hermite's elegant analysis is as follows:
Let K and K' be the periods of an elliptic integral corresponding to a modulus k, which is a solution of the biquadratic equation

$$k^4 - \tfrac{15}{16}k^2 + \tfrac{15}{64}k^4 - \tfrac{1}{64}k^8 = 0, \qquad \alpha = \frac{2}{\sqrt{5}}\frac{K}{K'}.$$

[1] Comptes Rendus Acad. Sciences, Paris, t. 46 (1858).

HARMONIC ANALYSIS ON SEMISIMPLE LIE GROUPS

HARISH-CHANDRA

1. Introduction

The theory of semisimple Lie groups has, in recent years, become the meeting ground of several different branches of mathematics—differential geometry, topology, algebraic geometry, arithmetic and analysis. In this lecture I wish to speak about some recent progress in Fourier analysis on such groups. The results are far from complete. Although the case of real groups is beginning to be fairly well understood, our knowledge of the $\mathfrak{p}$-adic groups is still very rudimentary. Nevertheless there appears to be a deep-seated analogy between these two cases. In my opinion, one of the major tasks confronting us, is to try to discover and comprehend the reasons for this similarity. Once local Fourier analysis is well understood, one would have to globalize the problem by going over to the adèle group. It is in this global setting, which seems to provide the right frame-work for the understanding of the work of Hecke and Siegel, that the deeper connections between Fourier analysis and arithmetic are likely to emerge. This is indeed a big project which may take several decades to complete. All that one can say at present, is that this promises to be an extraordinarily rich and fruitful field.

2. The discrete series

Let G be a locally compact, separable and unimodular group. A unitary representation π of G on a Hilbert space $\mathfrak{H}$ is a mapping π which assigns to every $x \in G$ a unitary operator $\pi(x)$ on $\mathfrak{H}$ such that:

(1) $$\pi(xy^{-1}) = \pi(x)\,\pi(y)^{-1} \qquad (x, y \in G),$$

(2) The mapping $(x, \psi) \to \pi(x)\psi$ of $G \times \mathfrak{H}$ into $\mathfrak{H}$ is continuous.

π is said to be irreducible if $\mathfrak{H} \neq \{0\}$ and no closed subspace of $\mathfrak{H}$, other than $\{0\}$ and $\mathfrak{H}$ itself, is stable under $\pi(x)$ for all $x \in G$. The equivalence of two representations is defined as usual. Let $\mathfrak{E}$ be the set of all equivalence classes of irreducible unitary representations of G.

Fix a Haar measure dx on G and let r denote the right-regular representation of G on $L_2(G)$. A class $\omega \in \mathfrak{E}$ is called discrete, if there exists a closed, invariant and irreducible subspace $\mathfrak{H}$ of $L_2(G)$ such that the restriction of r on $\mathfrak{H}$ lies in ω. Let $\mathfrak{E}_d$ denote the set of all discrete classes. Then $\mathfrak{E}_d$ is called the discrete series for G. Let π be

Proceedings of the International Congress of Mathematicians
Berkeley, California, USA, 1986

Equation Solving in Terms of Computational Complexity

ARNOLD SCHÖNHAGE

1.

1.1. *Introduction.* Computational complexity is a new principle in Mathematics, rooted in the algorithmic and constructive tradition of our science. Beyond its prominent role in theoretical Computer Science this aspect has meanwhile entered many different areas of Mathematics. Complexity considerations are intimately related to Logic and Foundations and to Numerical Methods with their innumerable applications, but they are also of growing interest in other fields like Geometry, Number Theory, and Algebra.

In order not to get stuck in pure generality, we confine our very broad subject to the computational treatment of *algebraic* equations. Even in this restricted sense, though, "equation solving" has been investigated for centuries and is now a central topic of Numerical Mathematics and in Computer Algebra. The specific interest of this survey is in the computational *complexity* of such problems. Beginning with a period of a few early papers, corresponding research has been carried on continuously for about twenty years now. Thus it seems to be timely to report on some of the results on this occasion.

In view of limited space and time we will discuss *sequential* algorithms only. A survey of important complexity results for models of *parallel* computation has recently been given by Cook [9]. According to personal taste and preference, we will furthermore restrict our considerations to *deterministic* computations, not ignoring the fact that, from a practical point of view, *probabilistic* algorithms may prove to be superior for certain difficult problems. Moreover, there is always a natural interplay between equation solving and the nondeterministic mode of solution guessing. Accordingly, it will sometimes be illuminating to compare the complexity of equation solving with that of *verification*, which means checking whether given data are really forming a solution.

Solving algebraic equations can be understood in different ways. For the prime fields $GF(p)$ and $\mathbf{Q}$ together with their finite extensions the discrete methods of symbolic computation apply. In this framework the major task may be defined as the construction of suitable splitting fields. We mention two papers, [23] and [6],

© 1987 International Congress of Mathematicians 1986

Sign Systems Studies 30 (1), 2002, pp. 271-282

Biological evolution — a semiotically constrained growth of complexity

Abir U. Igamberdiev

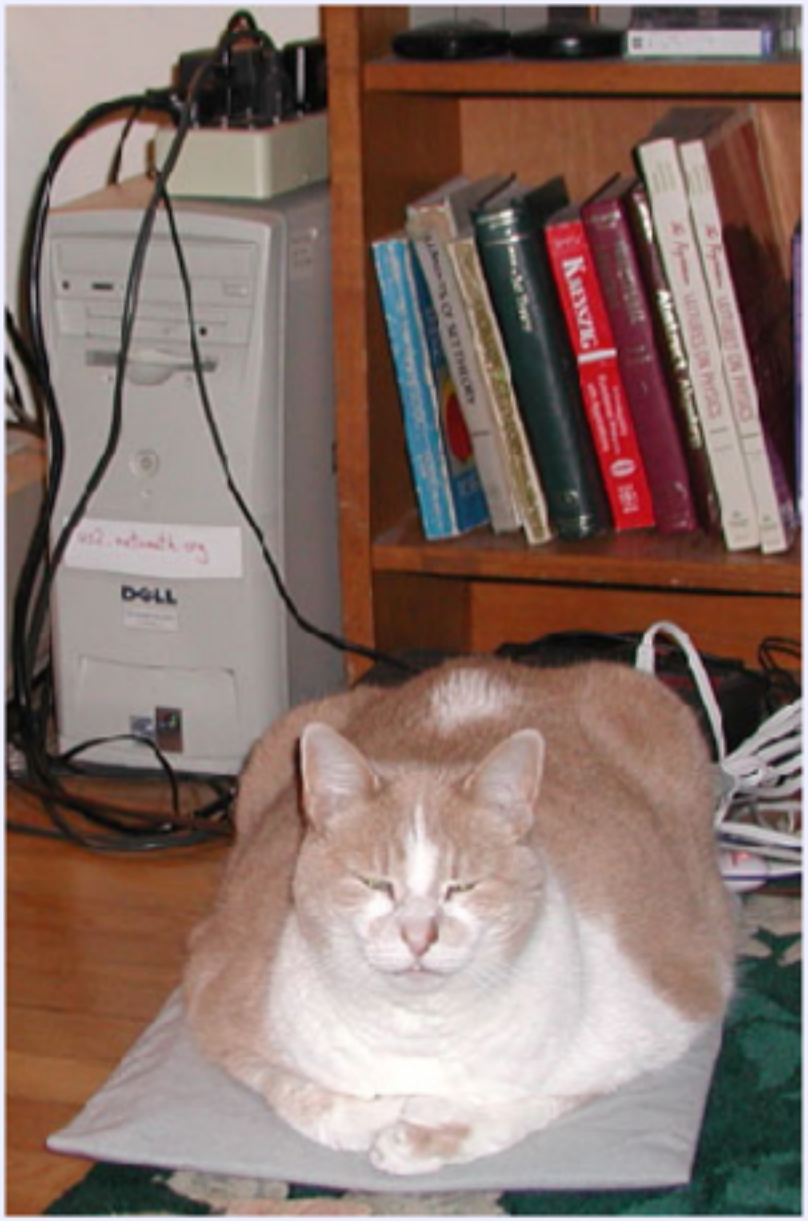
Riso National Laboratory, Plant Research Department,
P.O. Box 49, 4000 Roskilde, Denmark
e-mail: a_igamberdiev@hotmail.com

Abstract. Any living system possesses internal embedded description and exists as a superposition of different potential realisations, which are reduced in interaction with the environment. This reduction cannot be recursively deduced from the state in time present, it includes unpredictable choice and needs to be modelled also from the state in time future. Such non-recursive establishment of emerging configuration, after its memorisation via formation of reflective loop (sign-creating activity), becomes the inherited recursive action. It leads to increase of complexity of the embedded description, which constitutes the rules of generative grammar defining possible directions of open evolutionary process. The states in time future can be estimated from the point of their perfection, which represents the final cause in the Aristotelian sense and may possess a selective advantage. The limits of unfolding of the reflective process, such as the golden ratio and the golden wurf are considered as the canons of perfection established in the evolutionary process.

Semiotic causation of evolution

The living process is self-referential: living system in its development and reaction to external stimuli makes an internal choice by reducing indeterminacy of the potential field in interaction with the environment (Igamberdiev 1992, 1993). In other words, the system measures itself as embedded into the recognised part of the environment, the *Umwelt*. This reflective action is based on the semiotic structure of living system, which includes the inherited description with rigid

IGNITION!



Metamath development server

The Metamath Proof Language

Norman Megill

May 9, 2014

Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems*

Gonzalo Alvarez[1] and Shujun Li[2]

[1] Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144—28006 Madrid, Spain

[2] Department of Electronic and Information Engineering, Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong SAR, China

Abstract

In recent years, a large amount of work on chaos-based cryptosystems have been published. However many of the proposed schemes fail to explain or do not possess a number of features that are fundamentally important to all kind of cryptosystems. As a result, many proposed systems are difficult to implement in practice with a reasonable degree of security. Likewise, they are seldom accompanied by a thorough security analysis. Consequently, it is difficult for other researchers and end users to evaluate their security and performance. This work is intended to provide a common framework of basic guidelines that, if followed, every new cryptosystem would benefit from. The suggested guidelines address three main issues: implementation, key management, and security analysis, aiming at assisting designers of new cryptosystems to present their work in a more systematic and rigorous way to fulfill some basic cryptographic requirements. Meanwhile, several recommendations are made regarding some practical aspects of analog chaos-based secure communications, such as channel noise, limited bandwith, and attenuation.

1 Introduction

Modern telecommunication networks, and especially the Internet and mobile-phone networks, have tremendously extended the limits and possibilities of communications and information transmissions. Associated with this rapid development, there is a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography [Stinson, 1995; Menezes *et al.*, 1997].

Since 1990s, many researchers have noticed that there exists an interesting relationship between chaos and cryptography: many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems. Table 1 contains a partial list of these properties.

Table 1: Comparison between chaos and cryptography properties.

Chaotic property	Cryptographic property	Description
Ergodicity	Confusion	The output has the same distribution for any input
Sensitivity to initial conditions/control parameter	Diffusion with a small change in the plaintext/secret key	A small deviation in the input can cause a large change at the output
Mixing property	Diffusion with a small change in one plain-block of the whole plaintext	A small deviation in the local area can cause a large change in the whole space
Deterministic dynamics	Deterministic pseudo-randomness	A deterministic process can cause a random-like (pseudo-random) behavior
Structure complexity	Algorithm (attack) complexity	A simple process has a very high complexity

Interestingly, the tight relationship can even be found in the classic Shanon's paper on cryptography [1949]:

*This paper has been published in *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006.
The corresponding e-mail addresses of the authors: gonzalo@iec.csic.es (G. Alvarez), http://www.hooklee.com (S. Li).

EIGENVALUES AND OPTIMIZATION

Adrian Lewis

Cornell University

June 14, 2005

orie.cornell.edu/∼aslewis

ILAS 2005

FUNDAMENTA
MATHEMATICAE
183 (2004)

Incomparable, non-isomorphic and minimal Banach spaces

by

Christian Rosendal (Pasadena, CA)

Abstract. A Banach space contains either a minimal subspace or a continuum of incomparable subspaces. General structure results for analytic equivalence relations are applied in the context of Banach spaces to show that if E_0 does not reduce to isomorphism of the subspaces of a space, in particular, if the subspaces of the space admit a classification up to isomorphism by real numbers, then any subspace with an unconditional basis is isomorphic to its square and hyperplanes, and the unconditional basis has an isomorphically homogeneous subsequence.

1. Introduction. This paper contains results in the intersection of the geometry of Banach spaces and descriptive set theory. The general problem of our study is a generalisation of the homogeneous space problem. Namely, what can be said about a Banach space with "few" non-isomorphic subspaces? In particular, will such a space necessarily satisfy more regularity properties than a general space? Will it necessarily have subspaces of a given type?

The paper is divided into two parts, of which the first contains a proof of the following:

THEOREM 1. *Let X be an infinite-dimensional Banach space. Then X contains either a minimal subspace or a continuum of pairwise incomparable subspaces.*

Recall that two spaces are said to be *incomparable* if neither of them embed into the other, and a space is *minimal* if it embeds into all of its infinite-dimensional subspaces and is itself infinite-dimensional. Therefore, if a space is saturated with pairs of incomparable subspaces, it has a continuum of incomparable subspaces.

The homogeneous space problem, which was solved in the positive by the combined efforts of Gowers [10] and Komorowski and Tomczak-Jaegermann [18], is the problem of whether any infinite-dimensional space, isomorphic to all its infinite-dimensional subspaces, must necessarily be isomorphic to ℓ_2.

2000 *Mathematics Subject Classification*: Primary 46B03; Secondary 03E15.

Indeterminacy, Identity and Counterparts: Evans Reconsidered[1]

Elizabeth Barnes

Forthcoming in *Synthese*

Abstract: In this paper I argue that Gareth Evans' famous proof of the impossibility of metaphysically indeterminate identity fails on a counterpart-theoretic interpretation of the determinacy operators. I attempt to motivate a counterpart-theoretic reading of the determinacy operators and then show that, understood counterpart-theoretically, Evans' argument is straightforwardly invalid.

Gareth Evans' famous (1978) argument against the possibility of ontic vagueness is one of those philosophical problems that just won't die. Weatherson (2003) claims it's a lynchpin in the case against metaphysical vagueness, whereas Noonan (2004) remarks that everyone knows that all the argument shows is that every vague object is determinately distinct from every precise one (and every other vague one). Obviously, it's the sort of thing that philosophers tend not to agree about. The Evans argument is thus still very much a 'live' issue in the ontic vagueness debate, one which anyone who wants to go in for ontic vagueness must have something to say about.

With that in mind, I'd like to propose a solution to the Evans argument for the would-be defender of ontic vagueness. I certainly don't intend this to be read as a knock-down objection to Evans' argument – far from it. But I put this solution forward because it's a simple and straightforward solution to Evans' puzzle that, as far as I know, has been largely unexplored. My contention will be that, should you be tempted by an ontology which commits you to vague or indeterminate identities, there is a reading of the determinacy operators available to you according to which the Evans argument fails for quite basic reasons.

[1] Many thanks go to Katherine Hawley, Carrie Jenkins, Daniel Nolan, Robbie Williams, participants in the Arché Vagueness Seminar, two anonymous referees, and, most especially, Ross Cameron.

Using Liferay Portal

A Complete Guide

THE LIFERAY DOCUMENTATION TEAM
Richard Sezov, Jr.
Jim Hinkey
Stephen Kostas
Jesse Rao
Cody Hoag
Russell Bohl
Nicholas Gaskill
Michael Williams

Liferay Press

On least action principles for discrete quantum scales

François Dubois [a], Isabelle Greff [b] and Thomas Hélie [c]

[a] Conservatoire National des Arts et Métiers, Paris, France.
[b] Department of Mathematics, University of Pau, France.
[c] IRCAM, Paris, France.
francois.dubois@cnam.fr, isabelle.greff@univ-pau.fr,
thomas.helie@ircam.fr

Abstract. We consider variational problems where the velocity depends on a scale. After recalling the fundamental principles that lead to classical and quantum mechanics, we study the dynamics obtained by replacing the velocity by some physical observable at a given scale into the expression of the Lagrangian function. Then, discrete Euler-Lagrange and Hamilton-Jacobi equations are derived for a continuous model that incorporates a real-valued discrete velocity. We also examine the paradigm for complex-valued discrete velocity, inspired by the scale relativity of Nottale. We present also rigorous definitions and preliminary results in this direction.

Keywords: quantum operators, scale relativity.

1 Some philosophical principles for Physics

In this contribution, we first introduce some general philosophical hypotheses that are also widely discussed by several authors (see *e.g.* Bitbol [1], d'Espagnat [4], Filk and von Müller [5] among others). We set three hypotheses. The two first ones are of ontological type and the third one is concerned with experiments.

(H1)-Principle of reality. It exists a reality which is independent of any observer.

(H2)-Continuous space-time. The space-time is a continuous manifold on which the movement of particles can be described by continuous trajectories.

(H3)-Measurement and scale. The measurement of a physical quantity (time, space, velocity, energy, *etc*) involves a notion of scale.

- In classical physics, hypothesis (H2) is more constrained: trajectories are supposed to be differentiable or more regular. In this case, the particle velocity is uniquely defined by $v = \frac{dx}{dt}$ which is independent of the scale. Observe that if the trajectory is not regular (continuous but nowhere differentiable) or if some general hypothesis of continuous but non-differentiable space-time is done (as in scale relativity [12]), hypothesis (H3) remains true but the previous velocity has no meaning. On the contrary, a discrete velocity associated with a given scale can still be well-defined.

Mathematical Induction
- a miscellany of
theory, history and technique

Theory and applications for advanced secondary students

Part 2

Peter Haggstrom

This work is subject to Copyright. It is a chapter in a larger work.
You can however copy this chapter for educational purposes under the Statutory License of the Copyright Act 1968 - Part VB
For more information info@Copyright.com.au

Copyright 2009 peter.haggstrom@esternail.com.au

How important Taylor's Theorem is to physics (and pretty much everything)

Taylor's Theorem is one of the most frequently used mathematical tools in physics. It is used extensively in classical mechanics, quantum theory and much more. Indeed, the whole edifice of physics is based upon Taylor's Theorem. Every proof of a wave equation for a plucked string actually involves Taylor's Theorem because it involves an approximation to a more complicated problem - you throw away the pesky terms and hope that the first few terms generate results that make physical sense - in essence one is making local linear approximations. In complex variable theory the concept of an analytic function underpins the whole theory. Such functions have a Taylor expansion and thus locally (at an arbitrarily small level) are linear. This means the angle between curves is preserved under such functions - this is the nub of conformal mapping theory. Non-local qualities such as arc length and area are not preserved. **(See Appendix 2 for a derivation of a wave equation. If you don't understand the basics of partial differentiation, have no fear, this is explained briefly in Appendix 1)**

Here is the statement of Taylor's Theorem:

If f is $n+1$ times differentiable on an open interval J, then for $a, x \in J$

Copyright 2009 peter.haggstrom@esternail.com.au

NEOTERIS

NEOTERIS INSTANT VIRTUAL EXTRANET

Administration Guide

Physics and the Integers

David Tong

Department of Applied Mathematics and Theoretical Physics
University of Cambridge, UK
d.tong@damtp.cam.ac.uk

Abstract: I review how discrete structures, embodied in the integers, appear in the laws of physics, from quantum mechanics to statistical mechanics to the Standard Model. I argue that the integers are emergent. If we are looking to build the future laws of physics, discrete mathematics is no better a starting point than the rules of scrabble.

A History Lesson

"God made the integers, the rest is the work of man" — Leopold Kronecker [1]

I have never really understood this quote. It may be fine for mathematicians, but it doesn't seem to gel with how I understand the laws of physics. In part, the purpose of this essay is to explain why.

I recently learned that it's not just me who disagrees with Kronecker. At the time, *everyone* disagreed with him! This quote is part of a polemic by Kronecker against developments in mathematics in the late 1800s such as irrational numbers, Cantor's set theory and the Bolzano-Weierstrass theorem. Kronecker, an old distinguished mathematician, thought these new developments undignified. He preferred his mathematics constructive and discrete. Needless to say, it did not make Kronecker a popular man among his peers.

More than a century later, no mathematician would deny the importance and utility of the developments that Kronecker railed against. Yet, an informal survey among my colleagues suggests that many harbour some sympathy for his statement. The integers hold a special place in the heart of mathematics. Many of the most famous unsolved conjectures relate to the properties of the primes. More importantly, the integers are where we start mathematics: they are how we count.

Interface dynamics and the motion of complex singularities

Wei-Shen Dai, Leo P. Kadanoff, and Su-min Zhou
The James Franck Institute, The University of Chicago, 5640 South Ellis Avenue, Chicago, Illinois 60637
(Received 25 January 1991)

The motion of the interface between two fluids in a quasi-two dimensional geometry is studied via simulation. We consider the case in which a zero-viscosity fluid displaces one with finite viscosity and compare the interfaces that arise with zero surface tension with those that occur when the surface tension is not zero. The interface dynamics can be analyzed in terms of a complex analytic function of σ that maps the unit circle into the interface between the fluids. The physical plane of the domain is the exterior of the circle, which then maps into the region occupied by the more viscous fluid. In this physical region, the variable w and its derivative w_σ are both analytic. This paper focuses upon the *singularities* of the motion of the interface and the *positions* of the singularities of the *derivative* of the mapping function g. Two kinds of initial conditions are considered: case A, in which the singularities closest to the unit circle are poles and case B, in which the $\sigma=0$ coefficient in the Taylor series of w_σ dominates the sum of the rest of the series. In either case, different behaviors are found for relatively smaller and larger surface tensions. In case A, when the surface tension is relatively small, the pole moves outward, nearly radially with zero surface tension the singularities move outward and asymptotically approach the unit circle. For relatively large surface tension, the singularities still periodically move towards the center of the unit circle, however, in case B, for zero surface tension, the zeros move outward and hit the unit circle after a finite time, whereupon the solution breaks down. For finite but relatively small surface tension, each initial zero disappears and is replaced by a pair of pole-like excitations that seem to approach the unit circle asymptotically, while for a relatively large surface tension, each initial zero is replaced by a pole-like singularity that then moves towards the unit circle.

I. INTRODUCTION

Bubble growth in a Hele-Shaw cell has drawn much attention recently. Here, two closely spaced glass plates contain two fluids. For this idealized case, one fluid is viscous and incompressible, while the other has zero viscosity. The latter fluid is a bubble in an infinite sea composed of the more viscous fluid. The area of zero-viscosity fluid grows at a steady rate. The interface separating the two fluids is described by a surface tension. This and similar systems, for example, a channel flow geometry, have been studied experimentally, and various growth features have been observed. For some initial conditions, the zero-surface-tension case can be solved analytically.[1–3] These solutions show that for a large range of initial conditions, the interface will develop cusps after a finite time interval. After this critical time, the analysis is not meaningful.

Starting with the work of Saffman and Taylor,[4] there has been considerable discussion of the effect of the surface tension upon the interface motion in a Hele-Shaw cell. Work on this problem has shown that the surface tension is a singular perturbation, so that the solutions with and without surface tension may be qualitatively different.[5] Since the bubble-growth problem is the simplest one in this general class, the question of whether the presence of a small surface tension will qualitatively change the solution is of great interest.

In this paper, we shall first give a mathematical formulation of the bubble-growth problem using a method proposed by Shraiman and Bensimon[6] and Tanveer.[5] After a brief review of the results for the zero-surface-tension case, we shall report our simulation results for the growth of a bubble with nonzero surface tension. We shall show both the shape of the bubbles and the motion of the singularities with surface tension in comparison with those without surface tension. The computational methodology will be described in the Appendix.

II. MATHEMATICAL FORMULATION

The system has two kinds of fluids. They are confined between two parallel glass plates that are kept very close to each other (see Fig. 1). The interface between the two fluids is bubble shaped. The fluid inside the bubble (fluid 1) has a negligible viscosity and is kept at a constant pressure. The fluid outside the bubble (fluid 2) has a larger viscosity and is incompressible.

For the fluid outside the bubble, we can use Darcy's law:

$$\mathbf{v} = -\frac{b^2}{12\mu}\nabla p \ , \tag{1}$$

where $\mathbf{v}$, p, and μ are the velocity, pressure, and viscosity of fluid 2, and b is the spacing between the two plates. From the condition of incompressibility, we have $\nabla\cdot\mathbf{v}=0$. Therefore, the field satisfies the Laplace equation

$$\nabla^2 p = 0 \ . \tag{2}$$

The pressure is constant inside the bubble and has a jump

 ©1991 The American Physical Society

Iraq Oil & Gas Outlook

MAY 2015

Hannam & Partners

CONFIDENTIAL

HANNAM & PARTNERS

University of Michigan
Deep Blue deepblue.lib.umich.edu

2010

Approaching Psychosis through Quantum Physics

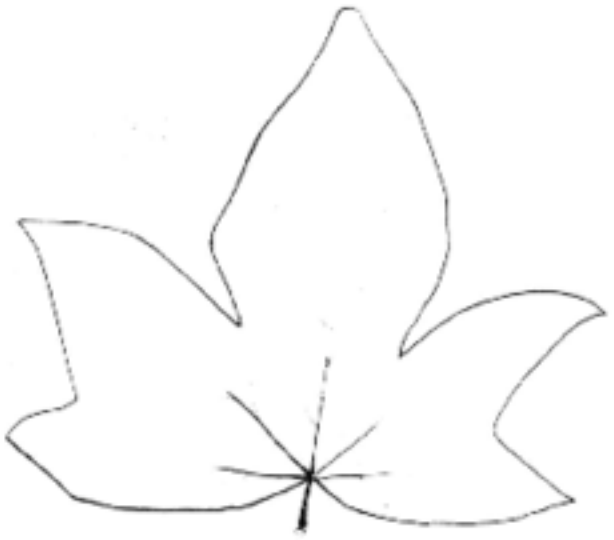
Irish, Kathryn Kay

http://hdl.handle.net/2027.42/102589

Australian Government
Department of Defence
Defence Science and Technology Group

Scenarios for Trusted Autonomous Systems

Brandon Pincombe
Head Land Organisational and Management Science,
Land Capability Analysis Branch
Joint and Operational Analysis Division
Defence Science and Technology Group



2

Member/ Subscription issue

International Viewpoints (Lyngby)

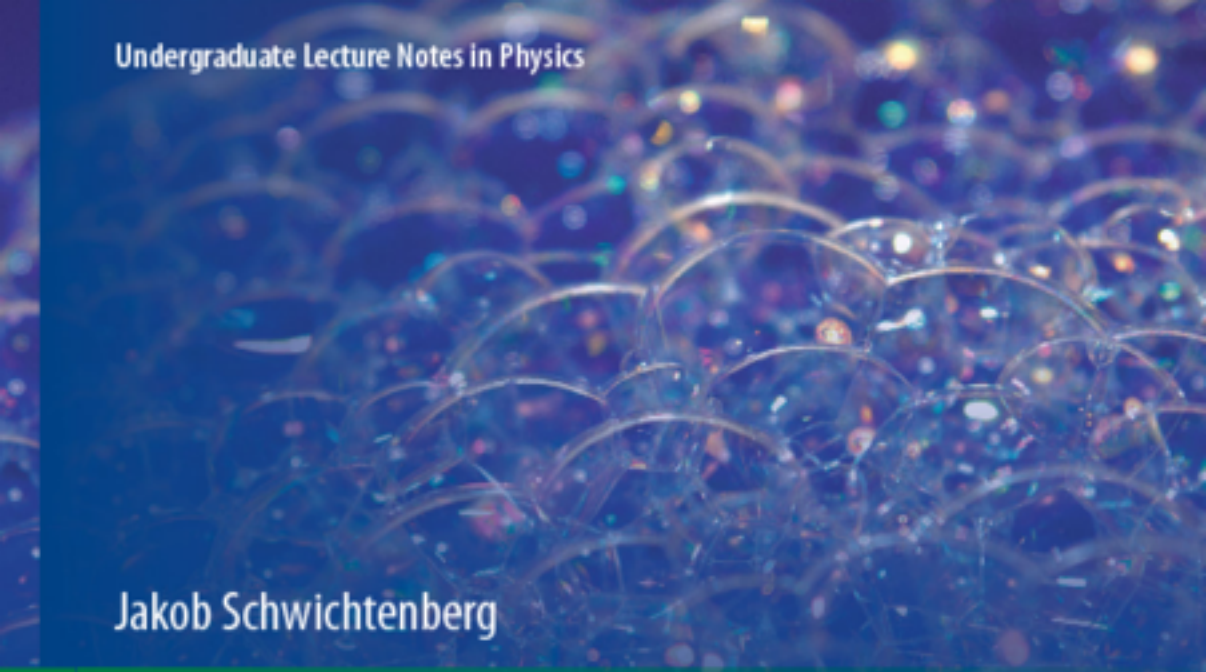
L. Ron Hubbard was born in

Tilden,
Nebraska,
on 13th March, 1911

His father was ...

(From *What is Scientology*, Ref S, of California, 1978)

Undergraduate Lecture Notes in Physics



Jakob Schwichtenberg

Physics from Symmetry

Springer

Hacking KPN: Lessons from the trenches

POSSIBILITIES OF DYNAMIC SYSTEMS SIMULATION

Cristina Coculescu[1]

ABSTRACT

Modeling dynamic systems can be made using several instruments and techniques, simulation being among these. Simulation of a system operating, allows evaluation of the kind how it will develop in certain conditions or because its management using a specific set of rules. In many cases, simulation is the only possible solution for making such evaluations. In this work we'll show general considerations about possibilities of simulation dynamic systems using dedicated programs for simulating systems.

Keywords: dynamic system, numerical integration, simulation
JEL code: C6, C88

1. BASIC ASPECTS ABOUT DYNAMIC SYSTEMS

An important step for scientific knowledge is passing from a system or real process to corresponding mathematical model and hence, to a physical one. This thing is possible also because in nature there are several real physical phenomena which are described by the same kinds of equations but the functions and variables within that mathematical structure have different meanings. With other words, nature unity appears in an amazing similarity of differential equations from different kinds of phenomena.

A dynamic system is one which develops in time. If the set of times when the system develops is a subset of:

- integer numbers set $\mathbb{Z}$, then the system is called discrete time system (*discrete system*);
- real number set $\mathbb{R}$, then the system has continuous time (*continuous system*).

In dynamic systems modeling, particular rules of mass and energy conservation are used, mathematically expressed as balance equations, that are simply differential equations, where derivation variable is time, *t*, or with partial derivates – where there is at least one derivation variable besides time (a space coordinate as example).

Mathematic model of a dynamic system is the set of differential or integer-differential equations which show system behavior under input values action.

Because differential equations which processes of real world are often non-linear and of superior order, finding an analytical solution (exact one) of Cauchy problem is difficult. The alternative is finding an approximate solution that is using of a numerical algorithm. Therefore, solution found using a numerical method, is a string of approximations of the values of exact solutions, computed in step times, usually of same interval.

---

[1] Ph.D., Associate Professor, Romanian-American University, 1B Expozitiei Bd, Sector 1, Bucharest, E-mail: cristina_coculescu@yahoo.com

HISTORY OF INTERACTIVE THEOREM PROVING

John Harrison, Josef Urban and Freek Wiedijk

Reader: Lawrence C. Paulson

1 INTRODUCTION

By interactive theorem proving, we mean some arrangement where the machine and a human user work *together* interactively to produce a formal proof. There is a wide spectrum of possibilities. At one extreme, the computer may act merely as a checker on a detailed formal proof produced by a human; at the other the prover may be highly automated and powerful, while nevertheless being subject to some degree of human guidance. In view of the practical limitations of pure automation, it seems today that, whether one likes it or not, interactive proof is likely to be the only way to formalize most non-trivial theorems in mathematics or computer system correctness.

Almost all the earliest work on computer-assisted proof in the 1950s [Davis, 1957; Gilmore, 1960; Davis and Putnam, 1960; Wang, 1960; Prawitz *et al.*, 1960] and 1960s [Robinson, 1965; Maslov, 1964; Loveland, 1968] was devoted to truly *automated* theorem proving, in the sense that the machine was supposed to prove assertions fully automatically. It is true that there was still a considerable diversity of methods, with some researchers pursuing AI-style approaches [Newell and Simon, 1956; Gelernter, 1959; Bledsoe, 1984] rather than the dominant theme of automated proof search, and that the proof search programs were often highly tunable by setting a complicated array of parameters. As described by Dick [2011], the designers of automated systems would often study the details of runs and tune the systems accordingly, leading to a continuous process of improvement and understanding that could in a very general sense be considered interactive. Nevertheless, this is not quite what we understand by interactive theorem proving today.

Serious interest in a more interactive arrangement where the human actively guides the proof started somewhat later. On the face of it, this is surprising, as full automation seems a much more difficult problem than supporting human-guided proof. But in an age when excitement about the potential of artificial intelligence was widespread, mere proof-checking might have seemed dull. In any case it's not so clear that it is really so much easier as a research agenda, especially in the

Journal of Scientific Exploration, Vol. 15, No. 3, pp. 331–354, 2001 0892-3310/01
© 2001 Society for Scientific Exploration

The Speed of Thought: Investigation of a Complex Space-Time Metric to Describe Psychic Phenomena

ELIZABETH A. RAUSCHER AND RUSSELL TARG

Bay Research Institute
1010 Hurlet Street, Palo Alto, CA 94301
e-mail: radiant@pacbell.net

"Consciousness is a singular of which the plural is unknown. There *is* only one thing, and that which seems to be a plurality is merely a series of different aspects of this one thing, produced by a deception… as in a gallery of mirrors."

Erwin Schrödinger
What Is Life

Abstract—For more than 100 years scientists have attempted to determine the truth or falsity of claims that some people are able to describe and experience events or information blocked from ordinary perception. For the past 25 years, the authors of this paper—together with researchers in laboratories around the world—have carried out experiments in remote viewing. The evidence for this mode of perception, or direct knowing of distant events and objects, has convinced us of the validity of these claims. It has been widely observed that the accuracy and reliability of this sensory awareness do not diminish with either electromagnetic shielding, or with increases in temporal or spatial separation between the percipient and the target to be described. Modern physics describes such a time and space independent connection between percipient and target as nonlocal.

In this paper we present a geometrical model of space-time, which has already been extensively studied in the technical literature of mathematics and physics. This eight-dimensional metric is known as "complex Minkowski space" and has been shown to be consistent with our present understanding of the equations of Newton, Maxwell, Einstein, and Schrödinger. It also has the interesting property of allowing a connection of zero distance between points in the complex manifold, which appear to be separate from one another in ordinary observation. We propose a model that describes the major elements of experimental parapsychology, and at the same time is consistent with the present highly successful structure of modern physics.

Keywords: parapsychology — ESP — space-time — multi-dimensional

1. Introduction

Scientific research into extrasensory perception (ESP) has made enormous progress since the founding of The Society for Psychical Research in 1882 by a distinguished group of Cambridge University scholars. The society's purpose was to examine allegedly paranormal phenomena in a scientific and unbiased

Original Corrected Typescript of Jung's 1925 Seminar on Analytic Psychology
A Singular Typescript of Important Historical and Scholarly Importance

JUNG, C. G. ***Notes on the Seminar in Analytical Psychology, Conducted by Dr. C. G. Jung , Zürich, March 23 - July 6, 1925. Arranged by Members of the Class.*** TP + Circulation restriction page #1 + Circulation restriction page #2 + Foreword page + [1]-103 + 103A + 104-174; loose, single-sided sheets. 8½" x 11"; ***Original Hand-Corrected Typescript.***

$12,000

The original typescript for the seminar conducted by Dr. Carl Jung from March to July of 1925 investigating his theories on analytic psychology. This typescript was compiled from notes taken by Cary F. de Angulo while attending that seminar.

The text of this typescript was then subsequently expanded and edited by her (with the assistance of Jung himself) before being multilith printed for distribution to the seminar's attendees.

THE SEMINAR

This seminar is an important, personal and intimate view of Jung's thought and methods during the early years of his practice and teaching – including a significant amount of biographical material – providing an important and interesting look into Jung's life and thought.

This 1925 gathering was the first of Jung's seminars to be transcribed and multilith printed – here for the benefit of the 27 attendees and other interested parties.

The synopsis for the edited publication of *Analytic Psychology* (Princeton University Press, 1989) notes that:

> For C. G. Jung, 1925 was a watershed year. He turned fifty, visited the Pueblo Indians of New Mexico and the tribesmen of East Africa, published his first book on the principles of analytical psychology meant for the lay public, and gave the first of his formal seminars in English.
>
> The seminar, conducted in weekly meetings during the spring and summer, began with a notably personal account of the development of his thinking from 1896 up to his break with Freud in 1912. It moved on to discussions of the basic tenets of analytical psychology--the collective unconscious, typology, the archetypes, and the anima/animus theory. In the elucidation of that theory, Jung analyzed in detail the symbolism in Rider Haggard's *She* and other novels. Besides these literary paradigms, he made use of case material, examples in the fine arts, and diagrams.

THE EDITION

This typescripts represent an earlier (and, most likely, the earliest) version of this text. This version precedes the additions made using other attendees notes and the changes that were made during the final editing process – a process in which Jung himself participated.

Ample proof of these textual differences can be seen from a comparison of the pagination of this typescript with the first edition multilith copies of this seminar:

This Original Typescript	174 pages
First Edition Multilith [1925]	227 pages

In addition, **this typescript contains original hand-written edits made to the text that were the basis for the first multilith printings**.

Finally, **this copy contain the original hand-written drawings and illustrations that formed the basis for those used in the later printings** (for details, see the "Illustrations" section in the following description).

Grenfell Tower Fire Public Inquiry Terms of Reference consultation

Submissions made on behalf of Justice4Grenfell Campaign

Preamble

Howe & Co, a firm of solicitors specialising in human rights cases, is instructed by Justice4Grenfell Campaign to make the following submissions on its behalf.

Justice4Grenfell Campaign is a not for profit organisation established to assist residents and those adversely affected by the fire at Grenfell on 14 June 2017. Justice4Grenfell Campaign is assisting a significant number of survivors, bereaved families, affected residents in the immediate surrounding area and the wider affected community of North Kensington impacted by the fire; across the various areas of need including housing, death and injury cases, advocacy, inquests and this Public Inquiry. Justice4Grenfell Campaign will be applying for Core Participant status in due course.

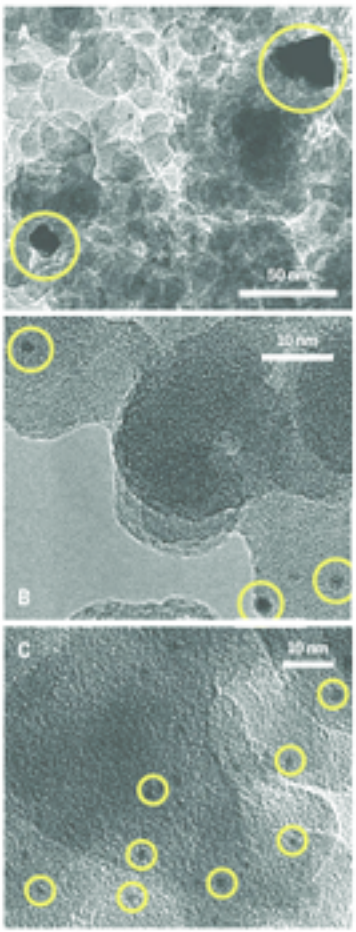
The Overarching Purpose of this Public Inquiry

Before turning to its specific submissions on the terms of reference of this Inquiry, we submit that public confidence must be at the heart of every consideration and step taken by the Grenfell Tower Inquiry.

Given the appalling loss of life and suffering caused by the Grenfell Tower fire and the nationwide concern over the safety of tower blocks within the social housing stock, a fundamental purpose of this Inquiry must be to rebuild and restore public confidence in:

1. The safety of social housing nationally;
2. The competence, ability and willingness of public authorities to oversee, regulate and ensure safe housing nationally; and
3. The competence, ability and willingness of public authorities to respond to large scale emergencies; and
4. Requiring that communities (including residents) are listened to, heard and more importantly that there is an effective response when communities/residents raise concerns to public authorities, local authorities, statutory agencies and bodies about matters that impact upon them.

sors form large oxide particles and large, clustered metal particles after reduction. Different temperatures, gas exposures, and modes of drying can make a large difference in particle formation, as evidenced by the preparation of uniform cobalt on silica particles by using fluid bed drying at 100°C in a nitrogen rather than air flow (*7*). These approaches, which have been led by de Jong, de Jongh, and their co-workers are also scalable. However, for each system, the particular technique (NO addition, drying variations, etc.) must be empirically determined.



Size selection on silica. (**A** and **B**) Transmission electron micrographs (TEMs) show a sample prepared with an aqueous tetraamine platinum hydroxide solution and calcined at 350°C followed by reduction. The result is a distribution of metal particle sizes. (**C**) The TEM shows a platinum-arginine preparation with air calcination at 425°C. Small, uniformly distributed metal crystals form upon reduction.

A third approach involves using simple water-soluble bifunctional organics—amino alcohols or amino acids—to form impregnates that interact strongly with silica. These bifunctional organics (such as triethanolamine and arginine) provide major advantages compared to using simple organic acids, which have served as more commonly used dispersion aids. With supported ruthenium and iridium, the preparation of optimal catalysts requires partial decomposition of the impregnate to form an anchored complex, which is then reduced and cleaned by hydrogenolysis to remove the organic fragment (*8*). In this way, ruthenium or iridium oxides, which are mobile on the silica surface, never form.

Other noble metals that do not have mobile oxide phases, such as platinum, palladium, and rhodium, can have their organic complex oxidized and reduced (see the figure). This technique has the advantage of keeping the two metals mixed and is well suited for making bimetallic alloy particles. It is widely applicable to most transition metals, but at high metal loadings and for large-scale preparations, the oxidation of organics must be controlled to avoid runaway exothermic reactions. In that regard, it is probably more suitable for noble metals that are generally kept at low loading levels.

These new approaches and our increased understanding of the scientific basis of controlling impregnations, metal nanostructures, and site homogeneity on silica-supported catalysts portend a wider use of these catalysts in the future. The present state of knowledge also allows a reassessment of processes where alumina has been used but may not be optimal. Increasing efforts to learn to control textural properties (surface areas, pore sizes, and pore volumes) on physically strong extrudates will also help propel this area forward, as most applications require this type of support particle. ■

REFERENCES

1. "World Catalysts," Industry Study #2989 (The Freedonia Group, Cleveland, OH, 2013); www.freedoniagroup.com/brochure/29xx/2989chmee.pdf.
2. J. P. Brunelle, in *2nd International Symposium on Scientific Basis of Heterogeneous Catalysis* (Elsevier, Amsterdam, 1979), pp. 211–232.
3. H. R. Cho, J. R. Regalbuto, *Catal. Today* **246**, 143 (2015).
4. J. R. Regalbuto, in *Silica and Silicates in Modern Catalysis*, I. Halasz, Ed. (Transworld Research Network, Kerala, India, 2010), pp. 345–374.
5. M. Watson, P. Miedik, J. H. Bitter, P. E. de Jongh, K. P. de Jong, *J. Phys. Chem. C* **115**, 3332 (2011).
6. P. Miedik, N. A. Kraan, P. E. de Jongh, K. P. de Jong, *ACS Catal.* **4**, 3219 (2014).
7. P. Miedik et al., *J. Phys. Chem. C* **115**, 14698 (2011).
8. S. Soled, in *Synthesis of Solid Catalysts*, K. P. de Jong, Ed. (Wiley, 2009), pp. 353–366.

10.1126/science.aad2204

PHYSICS

Classical entanglement?

Entanglement is a property of the quantum world; classical systems need not apply

By **Ebrahim Karimi**[1] *and* **Robert W. Boyd**[1,2]

Since the inception of quantum theory, scientists and philosophers have been puzzled by the apparent indeterminacy of physical properties prior to the measurement process. These problems suggest that quantum mechanics might ultimately be incompatible with basic notions of "realism"—that is, the view that a physical system possesses inherent properties that are independent of procedures used to measure them. This issue lies at the core of the famous gedanken experiment of Einstein, Podolsky, and Rosen (EPR) (*1*) and of attempts to develop a conceptual understanding (*2*–*4*) of EPR correlations.

The concept of entanglement was initially introduced by Schrödinger (*2*) in his response to EPR. Entanglement refers to the strong, nonclassical correlations that can exist between two spatially separated quantum systems. Over the past 40 years or so, numerous studies have confirmed that nature does behave in the manner described by Schrödinger (*5*). In particular, the laws of physics have been found to be inherently nonlocal: The results of a measurement at one position in space can dictate the possible outcome of a measurement performed at a different position.

In recent years, the term entanglement has come to be used in a more general context, including single-particle entanglement (*6*, *7*) and classical entanglement (*8*–*11*). We do not endorse this new nomenclature. Ascribing a new meaning to a term that has been in wide use in quantum physics for more than 80 years can only lead to confusion. But more deeply, these new situations lack the key feature—nonlocality—that led to the concept of entanglement in the first place. For example, single-particle

[1]Department of Physics and Max Planck Centre for Extreme and Quantum Photonics, University of Ottawa, Ottawa, Ontario K1N6N5, Canada. [2]Institute of Optics, University of Rochester, Rochester, NY 14627, USA. E-mail: ekarimi@uottawa.ca; boyd@rle.mit.edu

www.sciencemag.org

PHOTO: SHUTTERSTOCK

Published by AAAS

Alexander S. Karpenko

Łukasiewicz's Logic and Prime Numbers: Introduction and Contents

Łukasiewicz's Logics and Prime Numbers, by Alexander S. Karpenko, Nauka Publishers, Moscow, 2000, 319 pp., in Russian. ISBN 5-02-013048-6

Introduction

The title of this book may seem somewhat strange, since, on the first glance, what can logics and prime numbers have in common? Nevertheless, for a certain class of finite-valued logics such commonalties do exist - and this fact has most significant consequences. But is there any link between the doctrine of logical fatalism and prime numbers?

J.Łukasiewicz's refutation of Aristotle's fatalistic argument prepared the ground for a historically first non-classical logic, namely, for the three-valued one. Its properties proved to be shocking, and its subsequent generalizations for an arbitrary finite, and further on, for an infinite cases showed that the modeling of the finite and the infinite, on the basis of Łukasiewicz's many-valued logics, yield results that justify the claim that, by the end of the twentieth century, there have taken shape and are now rapidly growing, two distinct and deep trends in the contemporary symbolic logic, namely, Łukasiewicz's finite-valued logics and Łukasiewicz's infinite-valued logic.

The book consists of four parts: (1) Łukasiewicz's finite-valued logics L_{n+1} - chapters 1-4; (2) their connection with prime numbers - chapters 5-8; (3) the issuing numeric tables; (4) an appendix on the properties of Łukasiewicz's infinite-valued logic L_ω.

In chapter 1 an elementary introduction to the classical propositional logic is given, then goes a detailed discussion of the origin and development of Łukasiewicz's three-valued logic L_3 in chapter 2, L_3 is being compared with classical logic there. Already at this stage it becomes clear that as soon as we introduce some novelties into the classical logic, there arises a pressing problem of what interpretations of logical connectives and of truth-values themselves are intuitively acceptable. This problem, in turn, leads to the question of what is logical system. More than that: in the light of subsequent results there arises the question of what is logic itself (this question is discussed in [Karpenko A.S. Logic at the border-line of millenium.

Mem. Fac. Sci. Eng. Shimane Univ.
Series B: Mathematical Science
31 (1998), pp. 73–80

CHARACTERIZATION THEOREM OF 4-VALUED DE MORGAN LOGIC

MICHIRO KONDO

(Received: February 23, 1998)

ABSTRACT. In this paper we give an axiom system of a non-linear 4-valued logic which we call a de Morgan logic (ML), whose Lindenbaum algebra is the de Morgan algebra with implication (MI-algebra), and show that

(1) For every MI-algebra L, there is a quotient MI-algebra L^2 such that it is embeddable to the simplest 4-valued MI-algebra $\mathbf{M} = \{0, a, b, 1\}$;

(2) The Lindenbaum algebra of ML is the MI-algebra;

(3) The completeness theorem of ML is established;

(4) ML is decidable.

1. INTRODUCTION

It is well known the relation between logics and algebras through the property of Lindenbaum algebras. For example, the Lindenbaum algebra for the classical propositional logic (CPL) is a Boolean algebra and that of the intuitionistic propositional logic (IPL) is a Heyting one. On the other hand, CPL is characterized by the simplest non-trivial Boolean algebra $2 = \{0, 1\}$, that is, a formula A is provable in CPL if and only if (iff) $\tau(A) = 1$ for every function $\tau : \Pi \to 2$. In [3] or [4], we have an axiom system of Kleene logic (KL) and show in [3] that KL is characterized by the simplest non-trivial Kleene algebra $3 = \{0, 1/2, 1\}$. Now the next question arises:

(Question) What is a logic characterized by 4-valued algebra?

Of course, Rasiowa [5] has already given the axiom system of n-valued logic which is determined by n-valued Post-algebras. But Post-algebras are linear and so that these logics are not determined by 4-valued non-linear de Morgan algebra $\{0, a, b, 1\}$ below. In [1], it is proved that the class of de Morgan algebras with no implication is functional free for the algebra $\{0, a, b, 1\}$. Hence there is a question about the functional freeness of de Morgan algebras with implication.

Moreover, in the relevance logic investigated in [2], the set of first-degree formulas of the logic is determined by 4-valued de Morgan algebra $\{0, a, b, 1\}$, that is, for the zero-degree formulas (i.e., formulas with no implication simbols) A

1991 *Mathematics Subject Classification.* 03B50, 03B60.

Key words and phrases. de Morgan Logic, de Morgan algebra, Completeness Theorem.

Kurdistan Oil & Gas Outlook

DECEMBER 2015

Hannam & Partners

CONFIDENTIAL

HANNAM & PARTNERS

8. Homomorphisms and kernels

An isomorphism is a bijection which respects the group structure, that is, it does not matter whether we first multiply and take the image or take the image and then multiply. This latter property is so important it is actually worth isolating:

Definition 8.1. *A map $\phi\colon G \longrightarrow H$ between two groups is a* **homomorphism** *if for every g and h in G,*

$$\phi(gh) = \phi(g)\phi(h).$$

Here is an interesting example of a homomorphism. Define a map

$$\phi\colon G \longrightarrow H$$

where $G = \mathbb{Z}$ and $H = \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ is the standard group of order two, by the rule

$$\phi(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd.} \end{cases}$$

We check that ϕ is a homomorphism. Suppose that x and y are two integers. There are four cases. x and y are even, x is even, y is odd, x is odd, y is even, and x and y are both odd.

Now if x and y are both even or both odd, then $x + y$ is even. In this case $\phi(x + y) = 0$. In the first case $\phi(x) + \phi(y) = 0 + 0 = 0$ and in the second case $\phi(x) + \phi(y) = 1 + 1 = 0$.

Otherwise one is even and the other is odd and $x + y$ is odd. In this case $\phi(x + y) = 1$ and $\phi(x) + \phi(y) = 1 + 0 = 1$. Thus we get a homomorphism.

Here are some elementary properties of homomorphisms.

Lemma 8.2. *Let $\phi\colon G \longrightarrow H$ be a homomorphism.*

1. *$\phi(e) = f$, that is, ϕ maps the identity in G to the identity in H.*
2. *$\phi(a^{-1}) = \phi(a)^{-1}$, that is, ϕ maps inverses to inverses.*
3. *If K is subgroup of G, then $\phi(K)$ is a subgroup of H.*

Proof. Let $a = \phi(e)$, where e is the identity in G. Then

$$\begin{aligned} a &= \phi(e) \\ &= \phi(ee) \\ &= \phi(e)\phi(e) \\ &= aa. \end{aligned}$$

Thus $a^2 = a$. Cancelling we get $a = f$, the identity in H. Hence (1).

EAST BATON ROUGE PARISH
CLERK OF COURT
RECORDING INSTRUCTION SHEET

Please Complete One Instruction Sheet per Document to be Recorded

Date: _____

Requested By: _____ **Representing:** _____
(Title) (Firm/Company Name/Office)

Contact Number: _____ **E-mail Address:** _____

Document Recorded in the Name of: _____

- ☐ Articles of Incorporation
- ☐ Assignment of Mortgage
- ☐ Cancellation
- ☐ Contract
- ☐ Judgment
- ☐ Lease
- ☐ Lien
- ☐ Mortgage
- ☐ Notice of Seizure
- ☐ No Work Affidavit
- ☐ Partnership
- ☐ Power of Attorney
- ☐ Resolution/Cert. of Authority
- ☐ Sale
- ☐ UCC
- ☐ Other: _____

Recording Instructions: (check all that apply)

☐ Mortgage ☐ Conveyance ☐ Map ☐ UCC

☐ Stamped/Conformed Copy (Number of copies requested): _____

☐ Certified Copy (Number of copies requested): _____

☐ Special Instructions (requested by): _____
(Initials)

☐ Transfer of Map to Planning Commission

Comments:

_____

CLERK OF COURT USE ONLY

Method of Payment:

☐ Drop-Off _____
(Initials)
☐ Mail-In
☐ Walk-In

Delivery:

☐ Same Day
☐ Next Day

☐ Cash
☐ Check # _____
☐ Credit/Debit
☐ Verisign
☐ COC Account Name: _____

Cashier: _____
Pages: _____ @ _____
Names: _____
Certified: _____
Stamped: _____
Copies: _____
Initials: _____

5: INNER PRODUCTS, ADJOINTS, SPECTRAL THEOREMS, SELF-ADJOINT OPERATORS

STEVEN HEILMAN

Contents

1. Review 1
2. Inner Product Spaces 2
3. Orthogonality 4
4. Gram-Schmidt Orthogonalization 7
5. Adjoints 12
6. Normal Operators 15
7. Self-Adjoint Operators 18
8. Orthogonal and Unitary Operators (Bonus Section) 19
9. Appendix: Notation 21

1. Review

Proposition 1.1. *Let A be an $n \times n$ matrix. Let $v_1, \ldots, v_k$ be eigenvectors of A with eigenvalues $\lambda_1, \ldots, \lambda_k$, respectively. If $\lambda_1, \ldots, \lambda_k$ are all distinct, then the vectors $v_1, \ldots, v_k$ are linearly independent.*

Lemma 1.2 (An Eigenvector Basis Diagonalizes T). *Let V be an n-dimensional vector space over a field $\mathbf{F}$, and let $T : V \to V$ be a linear transformation. Suppose V has an ordered basis $\beta := (v_1, \ldots, v_n)$. Then v_i is an eigenvector of T with eigenvalue $\lambda_i \in \mathbf{F}$, for all $i \in \{1, \ldots, n\}$, if and only if the matrix $[T]_\beta^\beta$ is diagonal with $[T]_\beta^\beta = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$.*

Lemma 1.3. *Let V be a finite-dimensional vector space over a field $\mathbf{F}$. Let β, β' be two bases for V. Let $T : V \to V$ be a linear transformation. Define $Q := [I_V]_{\beta'}^{\beta}$. Then $[T]_\beta^\beta$ and $[T]_{\beta'}^{\beta'}$ satisfy the following relation*

$$[T]_{\beta'}^{\beta'} = Q[T]_\beta^\beta Q^{-1}.$$

Theorem 1.4 (The Fundamental Theorem of Algebra). *Let $f(\lambda)$ be a real polynomial of degree n. Then there exist $\lambda_0, \lambda_1, \ldots \lambda_n \in \mathbf{C}$ such that*

$$f(\lambda) = \lambda_0 \prod_{i=1}^{n} (\lambda - \lambda_i).$$

Lemma 1.5. *Let A, B be similar matrices. Then A, B have the same characteristic polynomial.*

Date: June 1, 2015.

Physics 115/242

The leapfrog method and other "symplectic" algorithms for integrating Newton's laws of motion

Peter Young

(Dated: April 21, 2014)

I. INTRODUCTION

One frequently obtains detailed dynamical information about interacting classical systems from "molecular dynamics" (MD) simulations, which require integrating Newton's equations of motion over a long period of time starting from some initial conditions. One might be interested, for example, in following the motion of atoms in a fluid. As another example, astronomers might want to integrate the motion of the solar system for a long period of time, or consider the evolution of a galaxy by following the motions of its constituent stars. (In an astronomical setting, "molecular dynamics" simulations are called "N-body" simulations.)

In this handout I will discuss an algorithm, called "leapfrog", which is particularly suited for these simulations because (i) it is simple, and (ii) it has a sort of "global" stability (in technical jargon, the algorithm is "symplectic"). I will explain what this term means, and also discuss briefly some higher order symplectic algorithms.

II. THE LEAPFROG ALGORITHM

We have already seen in our discussion of numerical differentiation and of numerical integration (midpoint method) that the slope of a chord between two points on a function, (x_0, f_0) and (x_1, f_1), is a much better approximation of the derivative at the midpoint, $f'_{1/2}$, than at either end. We can use the same idea in a simple, elegant method for integrating Newton's laws of motion, which takes advantage of the property that the equation for dx/dt does not involve x itself and the equation for dv/dt (v is the velocity) does not involve v (assuming velocity independent forces). More precisely, for a single degree of freedom, the equations of motion are

$$\frac{dx}{dt} = v \tag{1}$$

$$\frac{dv}{dt} = F(x) \left(= -\frac{dU(x)}{dx} \right) \tag{2}$$

1 Principle of Least Action

You've all suffered through a course on Newtonian mechanics, and you all know how to calculate the way things move: you draw a pretty picture; you draw arrows representing forces; you add them all up; and then you use $F = ma$ to figure out where things are heading next. All of this is rather impressive—it really is the way the world works and we can use it to understand things about Nature. For example, showing how the inverse square law for gravity explains Kepler's observations of planetary motion is one of the great achievements in the history of science.

However, there's a better way to do it. This better way was found about 150 years after Newton, when classical mechanics was reformulated by some of the giants of mathematical physics—people like Lagrange, Euler and Hamilton. This new way of doing things is better for a number of reasons:

- Firstly, it's elegant. In fact, it's not just elegant: it's completely gorgeous. In a way that theoretical physics should be, and usually is, and in a way that the old Newtonian mechanics really isn't.
- Secondly, it's more powerful. It gives new methods to solve hard problems in a fairly straightforward manner. Moreover, it is the best way of exploiting the power of symmetries (see Lecture 6). And since these days all of physics is based on fundamental symmetry principles, it is really the way to go.
- Finally, and most importantly, it is universal. It provides a framework that can be extended to all other laws of physics, and reveals a deep relationship between classical mechanics and quantum mechanics. This is the real reason why it's so important.

In this lecture, I'll show you the key idea that leads to this new way of thinking. It's one of the most profound results in physics. But, like many profound results, it has a rubbish name. It's called the **principle of least action**.

1 Coppersmith's Theorem

Today we prove the "full version" of Coppersmith's Theorem, stated here.

Theorem 1.1. *Let N be a positive integer and $f(x) \in \mathbb{Z}[x]$ be a monic, degree-d polynomial. There is an algorithm that, given N and f, efficiently (i.e., in time polynomial in the bit length of the inputs) finds all integers x_0 such that $f(x_0) = 0 \bmod N$ and $|x_0| \leq B \approx N^{1/d}$.*

In the theorem statement and what follows, for simplicity of analysis we use $\approx$ to hide factors which are polynomial in d and N^ε for some arbitrarily small constant $\varepsilon > 0$.[1] The remainder of this section is dedicated to the proof of the theorem.

Last time we considered adding multiples of $N \cdot x^i$ to $f(x)$, which preserves the roots of $f(x)$ modulo N. But this only let us obtain a bound of $B \approx N^{2/d^2}$. To do better, we consider higher powers of $f(x)$ and N. That is, our strategy will be to use LLL to efficiently find a nonzero polynomial $h(x) = \sum_i h_i x^i \in \mathbb{Z}[x]$ of degree at most $n = d(m+1)$, for some positive integer m to be determined, such that:

1. Any mod-N root of f is a mod-N^m root of h, i.e., if $f(x_0) = 0 \bmod N$ then $h(x_0) = 0 \bmod N^m$.
2. The polynomial $h(Bx)$ is "short," i.e., its coefficients $h_i B^i$ are all less than $N^m/(n+1)$ in magnitude.

From the second property it follows that if $|x_0| \leq B$, then

$$|h(x_0)| \leq \sum_i |h_i B^i| < N^m.$$

Therefore, by the first property, any small mod-N root of f is a root of $h(x)$ *over the integers* (not modulo anything). So, having found $h(x)$, we can efficiently factor it over the integers and check whether each of its small roots is indeed a root of $f(x)$ modulo N.

To construct a lattice basis that lets us find such an $h(x)$, the first helpful insight is that $f(x_0) = 0 \bmod N$ implies $f(x_0)^k = 0 \bmod N^k$ for any positive integer k. To create our lattice basis, we define $n = d(m+1)$ polynomials $g_{u,v}(x)$ whose mod-N^m roots will include all of the mod-N roots of $f(x)$. Concretely,

$$g_{u,v}(x) = N^{m-v} f(x)^v x^u, \quad \text{for } u \in \{0, \ldots, d-1\}, v \in \{0, \ldots, m\}.$$

We use two important facts about these polynomials. First, $f(x)$ is monic and of degree d, so $g_{u,v}(x)$ has leading coefficient N^{m-v} and is of degree exactly $u + vd$. Second, if x_0 is a mod-N root of $f(x)$, then x_0 is a mod-N^m root of $g_{u,v}(x)$ for all u, v, because N^m divides $N^{m-v} f(x_0)^v$.

The basis vectors for our lattice are defined by the coefficients of $g_{u,v}(Bx)$ where, as above, B corresponds to the bound on the absolute value of the roots. Specifically, the basis is $\mathbf{B} = [\mathbf{b}_0, \ldots, \mathbf{b}_{n-1}]$, where $\mathbf{b}_{u+vd}$ is the coefficient vector of $g_{u,v}(Bx)$ represented as a polynomial in x. Since $g_{u,v}(x)$ is of degree $u + vd$ with leading coefficient N^{m-v}, and $u + vd$ runs over $\{0, \ldots, n-1\}$ as u, v run over their respective ranges, the basis is triangular, with diagonal entries $N^{m-v} B^{u+vd}$. A simple calculation then reveals that

$$\det(\mathbf{B}) = B^{n(n-1)/2} \cdot N^{dm(m+1)/2}.$$

Running the LLL algorithm on $\mathbf{B}$ yields a nonzero vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ of length

$$\begin{aligned} \|\mathbf{v}\| &\leq 2^{(n-1)/2} \det(\mathbf{B})^{1/n} = 2^{(n-1)/2} \left(B^{n(n-1)/2} \cdot N^{dm(m+1)/2} \right)^{1/n} \\ &\leq (2B)^{n/2} \cdot N^{m/2}. \end{aligned}$$

[1] This yields a true bound of $B = N^{1/d - \varepsilon}$, though with more work the theorem can be proved for $B = N^{1/d}$.

MIT 6.972 Algebraic techniques and semidefinite optimization March 2, 2006

Lecture 7

Lecturer: Pablo A. Parrilo *Scribe: ???*

In this lecture we introduce a special class of multivariate polynomials, called *hyperbolic*. These polynomials were originally studied in the context of partial differential equations. As we will see, they have many surprising properties, and are intimately linked with convex optimization problems that have an algebraic structure. A few good references about the use of hyperbolic polynomials in optimization are [Gül97, BGLS01, Ren].

1 Hyperbolic polynomials

Consider a homogeneous multivariate polynomial $p \in \mathbb{R}[x_1, \ldots, x_n]$ of degree d. Here *homogeneous of degree d* means that the sum of degrees of each monomial is constant and equal to d, i.e.,

$$p(x) = \sum_{|\alpha|=d} c_\alpha x^\alpha,$$

where $\alpha = (\alpha_1, \ldots, \alpha_n), \alpha_i \in \mathbb{N} \cup \{0\}$, and $|\alpha| = \alpha_1 + \cdots + \alpha_n$. A homogeneous polynomial satisfies $p(tw) = t^d p(w)$ for all real t and vectors $w \in \mathbb{R}^n$. We denote the set of such polynomials by $\mathcal{H}_n(d)$. By identifying a polynomial with its vector of coefficients, we can consider $\mathcal{H}_n(d)$ as a normed vector space of dimension $\binom{n+d-1}{d}$.

Definition 1. *Let e be a fixed vector in $\mathbb{R}^n$. A polynomial $p \in \mathcal{H}_n(d)$ is* hyperbolic *with respect to e if $p(e) > 0$ and, for all vectors $x \in \mathbb{R}^n$, the univariate polynomial $t \mapsto p(x - te)$ has only real roots.*

A natural geometric interpretation is the following: consider the hypersurface in $\mathbb{R}^n$ given by $p(x) = 0$. Then, hyperbolicity is equivalent to the condition that every line in $\mathbb{R}^n$ parallel to e intersects this hypersurface at exactly d points (counting multiplicities), where d is the degree of the polynomial.

Example 2. *The polynomial $x_1 x_2 \cdots x_n$ is hyperbolic with respect to the vector $(1, 1, \ldots, 1)$, since the univariate polynomial $t \mapsto (x_1 - t)(x_2 - t) \cdots (x_n - t)$ has roots $x_1, x_2, \ldots, x_n$.*

Hyperbolic polynomials enjoy a very surprising property, that connects in an unexpected way algebra with convex analysis. Given a hyperbolic polynomial $p(x)$, consider the set defined as:

$$\Lambda_{++} := \{x \in \mathbb{R}^n : p(x - te) = 0 \;\Rightarrow\; t > 0\}.$$

Geometrically, this condition says that if we start at the point $x \in \mathbb{R}^n$, and slide along a line in the direction parallel to e, then we will never encounter the hypersurface $p(x) = 0$, while if we move in the opposite direction, we will cross it exactly n times. Figure 1 illustrates a particular hyperbolicity cone.

It is immediate from homogeneity and the definition above that $\lambda > 0, x \in \Lambda_{++} \Rightarrow \lambda x \in \Lambda_{++}$. Thus, we call Λ_{++} the *hyperbolicity cone* associated to p, and denote its closure by Λ_+. As we will see shortly, it turn out that these cones are actually convex cones. We prove this following the arguments in Renegar [Ren]; the original results are due to Gårding [Går59].

Lemma 3. *The hyperbolicity cone Λ_{++} is the connected component of $p(x) > 0$ that includes e.*

Example 4. *The hyperbolicity cone Λ_{++} associated with the polynomial $x_1 x_2 \cdots x_n$ discussed in Example 2 is the open positive orthant $\{x \in \mathbb{R}^n \,|\, x_i > 0\}$.*

The first step is to show that we can replace e with any vector in the hyperbolicity cone.

Lemma 5. *If $p(x)$ is hyperbolic with respect to e, then it is also hyperbolic with respect to every direction $v \in \Lambda_{++}$. Furthermore, the hyperbolicity cones are the same.*

CS 880: Quantum Information Processing 10/25/2010

Lecture 20: Density Operator Formalism

Instructor: Dieter van Melkebeek Scribe: Dalibor Zelený

So far in this course we have been working in the setting where the goal is to realize a relation by means of some computation. This involved only one "party" that was performing the computation. In today's lecture and several following lectures, we will focus on systems where multiple parties participate in the computation. We develop the *density operator formalism* which is suitable for describing multiparty systems. It turns out that we can use this formalism to describe the evolution of a quantum system, too, and that it is in some sense superior to our original way of describing things.

1 Density Operator

We start with the definition of the density operator, give some examples, and prove some properties of density operators. To conclude this section, we show how to represent the evolution of a quantum system using density operators.

Definition 1 (Density operator). *For a pure state $|\psi\rangle$, the density operator is $\varrho = |\psi\rangle\langle\psi|$. For a mixed state $\{(p_i, |\psi_i\rangle)\}_i$, the density operator is $\varrho = \sum_i p_i |\psi\rangle\langle\psi|$.*

When we apply the density operator to a state ϕ, we get the projection of ϕ onto ψ, that is, $\varrho|\phi\rangle = |\psi\rangle\langle\psi|\phi\rangle$. Also note that the density operator corresponding to a mixed state is just a convex combination of density operators for the individual pure states that form the mixed state.

1.1 Examples of Density Operators

We now present some examples of density operators. As the next two examples show, two different mixed states can have the same density operator.

Example: Let's compute the density operator corresponding to $\{(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)\}$. The density operators for $|0\rangle$ and $|1\rangle$ are

$$\varrho_0 = (1,0)^T(1,0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \varrho_1 = (0,1)^T(0,1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Now we take their convex combination based on the probabilities describing our mixed state and get that $\varrho = \frac{1}{2}\varrho_0 + \frac{1}{2}\varrho_1 = \frac{1}{2}I$. ⊠

Example: Now we compute the density operator corresponding to $\{(\frac{1}{2}, |+\rangle), (\frac{1}{2}, |-\rangle)\}$. The density operators for $|+\rangle$ and $|-\rangle$ are

$$\varrho_+ = \frac{1}{\sqrt{2}}(1,1)^T\frac{1}{\sqrt{2}}(1,1) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \varrho_- = \frac{1}{\sqrt{2}}(1,-1)^T\frac{1}{\sqrt{2}}(1,-1) = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

Now we take their convex combination based on the probabilities describing our mixed state and get that $\varrho = \frac{1}{2}\varrho_+ + \frac{1}{2}\varrho_- = \frac{1}{2}I$. ⊠

4 Probability amplification

We have already seen in the first chapter that we can increase the success probability of randomized algorithms drastically through multiple runs. In this chapter we will present some refined methods in order to increase the success probability. In the first method, specific steps of the algorithm are repeated, instead of repeating the whole algorithm, in order to obtain a better running time. The second method is based on the so-called Lovász Local Lemma. This lemma in its original form just allows one to prove the existence of solutions to certain problems, but since several years also algorithms are known that can find these solutions efficiently.

4.1 Amplification through local repetition

We illustrate our first technique by applying it to an algorithm for the MINCUT problem. In the MINCUT problem we are given an undirected graph $G = (V, E)$ and we are looking for a subset $U \subsetneq V$ such that $|(U, \bar{U})|$, i.e. the number of edges of the cut $(U, \bar{U})$, is minimal. This problem can be solved in polynomial time by using network flow algorithms. We present here a simple alternative algorithm that does not need algorithms for network flow or linear optimization.

A simple algorithm

In the following we assume that $G = (V, E)$ is a *multigraph*, i.e. there can be multiple edges between a pair of nodes. The basic idea of our algorithm is as follows:

In each step, pick a random edge $\{u, v\}$ from the current multigraph. This edge will be *contracted*, which means that the nodes u and v will be replaced by a new node w. All edges of the form $\{u, x\}$ with $x \neq v$ and $\{v, x\}$ with $x \neq u$ are replaced by the edge $\{w, x\}$. Edges between u and v are omitted. If there are only two nodes remaining, the edge set across the two sets of nodes in the original graph which are represented by the remaining nodes is returned by the algorithm. See also Figure 1.

Algorithm CONTRACT(G)**:**
$H := G$
while H has more than two nodes **do**
    choose an edge $\{x, y\}$ uniformly at random from the edges in H and contract it
return the set of edges C of G that is represented by the remaining edges in H

Figure 1: The simple contraction algorithm.

The running time of the CONTRACT algorithm is $O(n^2)$ when using an efficient implementation (for example by storing G as an adjacency matrix). Moreover, following theorem holds.

Theorem 4.1 *The cut computed by CONTRACT is a minimum cut with probability at least* $1/n^2$.

Proof. Let K be a minimum cut in G. If during the execution of the algorithm no edge of K is contracted, then the cut returned by the algorithm is K. We show that the probability that this happens is at least $1/n^2$. Let e_i be the edge contracted in round r of CONTRACT. It holds that:

$$\begin{aligned}
\Pr[C \text{ is a minimum cut}] &\geq \Pr[C = K] \\
&= \Pr[\bigwedge_{1 \leq i \leq n-2} (e_i \notin K)] \\
&= \prod_{1 \leq i \leq n-2} \Pr[e_i \notin K \mid \bigwedge_{1 \leq j < i} (e_j \notin K)]
\end{aligned}$$

Lemma 4.2 *For* $1 \leq i \leq n-2$ *it holds that*

$$\Pr[e_i \in K \mid \bigwedge_{1 \leq j < i} (e_j \notin K)] \leq \frac{2}{n - i + 1}$$

Computational Higher Type Theory

Robert Harper

Computer Science Department
Carnegie Mellon University

HoTT Workshop 2016
Leeds, UK

Automatic Reverse Engineering of Malware Emulators

Monirul Sharif, Andrea Lanzi, Jonathon Giffin, Wenke Lee

School of Computer Science
College of Computing
Georgia Institute of Technology, USA
{msharif, andrew, jon, wenke}@cc.gatech.edu

(to appear in IEEE SYMPOSIUM on SECURITY and PRIVACY, May 2009)

NATURE, 215, 1292-1293, (1967)

Formation of Blue Oxidation Product from Psilocybin

Gibbons and O'Brien[1] have reported that a blue colour develops when psilocybin (4-phosphoryl-N,N-dimethyltryptamine) is incubated with a preparation of rat brain mitochondria. The colour is apparently not dependent on oxygen for its formation, is associated only with the particulate matter and cannot be brought into solution by treatment with various organic solvents, detergents, acid or alkali. The reaction is also said not to occur in EDTA.

Experiments carried out in this laboratory and elsewhere provide a remarkable explanation for this phenomenon. Psilocin, the dephosphorylated derivative of psilocybin, forms a deep blue colour on incubation with cytochrome c in the copper oxidase of mammalian serum—or with a copper oxidase obtained from the gill plates of *Spisula solida*. The reaction is accompanied by the uptake of oxygen[2,3]. The colour has a spectral maximum at about 620–625 mμ and a smaller peak at 400 mμ. Although 4, 5 and 7-hydroxyindole derivatives are also oxidized in the presence of both enzymes, only psilocin gives the blue colour. The blue material is a fairly stable free radical (Blumberg, W. E., and Peisach, J., personal communication), while the free radicals formed from other tryptamine substrates are rather short lived[4]. The reaction catalysed by ceruloplasmin is unaffected by EDTA. This is in contrast to the reaction with other substrates such as phenylenediamine, which are inhibited by about 90 per cent by EDTA (refs. 5 and 6).

During the formation of blue material in the presence of the Mylon enzyme the colour becomes associated principally with particulate matter and resists extraction with various non-polar solvents. Much of the colour can, however, be brought into solution with 70 per cent hydrochloric acid. If psilocin is oxidized in a system with very little protein the blue oxidation product appears to remain soluble.

The oxidative formation of blue colour can also be elicited without enzyme in the presence of ferric ion, which acts as an electron acceptor. As would be expected, EDTA and other chelating agents block this non-enzymic reaction. When treated with alkali, the oxidation product of psilocin turns pale green and can readily be extracted into butanol, where the deep blue colour reappears. The blue product can be re-extracted into 0·1 molar hydrochloric acid. The hydroglobus acid solution at this point contains no detectable iron, and the blue colour cannot therefore be due to a metal complex.

Will psilocybin suffer formation of blue colour on uptake of oxygen occurs during incubation with ceruloplasmin or with ferric ions. Then a free, non-esterified phenolic hydroxyl group is required for reactivity. These reactions could be related to those described by Gibbons and O'Brien in. Are possible ways. Also, their psilocybin may have been contaminated with a small amount of psilocin. No evidence for purity was presented. The colour is so intense that even a slight contamination would produce visible colour in their system. Second, because prolonged incubation was required for the ferric form (16–20 h at 5 °C) it seems likely that during this period at time a phosphatase could remove the phosphate and then oxidase the free phenolic hydroxyl to oxidative attack either by a copper enzyme or by a metal ion such as the ferric ion. Heath and Weber[7] described the dephosphorylation of psilocybin by homogenates of various mammalian tissues, as well as by purified alkaline phosphatase. They found that the psilocin produced in this reaction is transformed into a deep blue colour. The latter reaction may be analysed by cytochrome oxidase which readily oxidizes psilocin to the blue product at physiological pH (7·4), although the optimum pH for this reaction is 9 (ref. 6). Because Gibbons and O'Brien found EDTA inhibited the formation of blue colour, the reaction probably involves some iron which is either free or loosely bound so as to be accessible to chelating agents. This would also explain why the reaction could take place in oral oxygen.

I therefore propose that the formation of the colour from psilocybin in the presence of the basic fraction described by Gibbons and O'Brien be attributed to the following reaction.

$$\text{psilocybin} \xrightarrow{\text{phosphatase}} \text{psilocin} \xrightarrow[\text{or ferric ion}]{\text{cytochrome oxidase}} \text{blue product}$$

This work was supported in part by a grant from the US Public Health Service. I have a research career development award from the US Public Health Service. The psilocin and psilocybin were kindly supplied by Sandoz, Inc.

Walter G. Levine

Department of Pharmacology,
Albert Einstein College of Medicine,
Yeshiva University,
Bronx, New York.

Received March 28, revised July 25, 1967.

1 Gibbons, R., and O'Brien, R. D., *Nature*, **205**, 1207 (1965).
2 Blumberg, W. E., and Peisach, J., *Science*, **148**, 1348 (1965).
3 Blumberg, W. E., and Peisach, J., *Arch. Biochem. Biophys.*, **112**, 337 (1965).
4 Blumberg, W. E., and Peisach, J., in preparation.
5 Levine, W. G., *Biochem. Pharmacol.*, **15**, 1253 (1966).
6 Levine, W. G., *Biochem. J.*, **97**, 738 (1965).
7 Heath, A., and Weber, L. J., *Biochem. Pharmacol.*, **7**, 67 (1961).
8 Heath, A., and Weber, L. J., *Proc. Soc. Exp. Biol. and Med.*, **106**, 98 (1961).
9 Faber, L. E., and Heath, A., *Nature*, **208**, 1203 (1965).

Life in prison: Food

A findings paper

by HM Inspectorate of Prisons

July 2016

Lifting Problems in a Grothendieck Fibration

Andrew Swan

July 21, 2017

The notion of *lifting problem* is a central concept in homotopical algebra, as well as in the semantics of homotopy type theory.

Given two maps $m\colon U \to V$ and $f\colon X \to Y$ in a category $\mathbb{C}$, we say that m has the *left lifting property* with respect to f and f has the *right lifting property* with respect to m if for every commutative square, as in the solid lines below (which we refer to as a *lifting problem*), there is a *diagonal filler*, which is the dotted line below, making two commutative triangles.

In the presence of the axiom of choice, this is equivalent to having a choice of diagonal filler for every lifting problem of m against f.

A well known example is where we take $\mathbb{C}$ to be the category **Top** of topological spaces and m to be an endpoint inclusion into the unit interval $e_0\colon 1 \hookrightarrow [0,1]$. When a map f has the right lifting property against e_0 we say it has the *path lifting property*.

A *weak factorisation system* (wfs) is two classes of maps $\mathcal{L}$ and $\mathcal{R}$ which are closed under retracts and such that every element of $\mathcal{L}$ has the left lifting property against every element of $\mathcal{R}$.

Often it's useful to talk about not just individual maps, but to have some notion of indexed family of maps. The most basic example is where we have a set I and a family of maps $(m_i)_{i\in I}$. Then we say that f has the right lifting property against $(m_i)_{i\in I}$ if we have for every $i \in I$ and every lifting problem of m_i against f a choice of diagonal filler. A weak factorisation system $(\mathcal{L},\mathcal{R})$ is *cofibrantly generated* if $\mathcal{R}$ is precisely the class of maps with the right lifting property against some fixed set indexed family of maps. A classic example from homotopical algebra is where we take $\mathbb{C}$ to be the category of simplicial sets and take $(m_i)_{i\in I}$ to be the set of horn inclusions $(\Lambda^n_k \hookrightarrow \Delta^n)_{n\in\mathbb{N}, 0\leq k\leq n}$. Then if f has the right lifting property against the family of horn inclusions, we say that it is a *Kan fibration*.

A more sophisticated notion due to Garner is where we replace the indexing set, I with a small category $\mathcal{C}$. In this case, a family of maps is a functor $M\colon \mathcal{C} \to \mathbb{C}^{\to}$. In particular, this includes not just a choice of map $M(c)$ for each object c of $\mathcal{C}$, but also a choice of commutative square for each morphism in $\mathcal{C}$. Garner showed that in categories satisfying certain conditions, every such family cofibrantly generates not just a wfs, but the more structured notion of

The Limits of Quantum Computers (DRAFT)

Scott Aaronson

For the published version—which differs significantly from this one—please see the March 2008 issue of Scientific American.

"Haggar Physicists Develop 'Quantum Slacks,'" read a headline in the satirical weekly *The Onion*. By exploiting a bizarre "Schrödinger's Pants" duality, these non-Newtonian pants could paradoxically behave like formal wear and casual wear at the same time. The *Onion* writers were apparently spoofing the breathless accounts of quantum computing that have filled the popular press for years. If so, they picked an obvious target: many of those articles were ripe for parody. "Unlike a classical bit," the typical article might read, "a quantum bit—or 'qubit'—can be 0 and 1 at the same time. As a result, such a machine could instantly break 'unbreakable' codes by trying all possible keys at once."

It doesn't take an Einstein to smell something fishy in that assertion. After all, what would the world be like if there were a machine able to examine all possible solutions to a problem in parallel, and then immediately zero in on the right one like a falcon swooping down on its prey? To say that airlines could schedule their flights better, or that engineers could find ways to shoehorn more transistors onto a chip, is to miss the point entirely. For one thing, if such a machine existed, mathematicians would be permanently out of a job.

Why? Take your favorite conjecture that's remained unproved for centuries—like Goldbach's Conjecture, that every even number 4 or greater can be written a sum of two prime numbers. Now program the machine to search, not among *every* purported proof of that assertion, but "merely" among every proof with at most (say) a million symbols. The number of such proofs is finite, and each one—assuming it's written out in hairsplitting detail—can be rapidly checked by computer to see whether it's correct. So if quantum computers were really as powerful as the usual caricature suggests, then they could instantly find a correct proof, assuming there was one. And if there wasn't such a proof? Well then, try all proofs with ten million symbols, or a billion. Perhaps the logician Kurt Gödel said it best, in a 1956 letter to John von Neumann that first raised the possibility of such a hyperfast theorem-proving machine: "One would indeed have to simply select a [number of symbols] so large that, if the machine yields no result, there would then also be no reason to think further about the problem."

But if you had such a machine, the implications would go beyond pure mathematics. For example, you could ask a computer to search, among all possible parameter settings of a neural network, for the ones that do the best at predicting historical stock market data. Of course, there's no guarantee that those settings would predict the *future* prices better than the market, but it's a decent bet—as long as you were the only one who knew the settings! Or you could search for the shortest program that output the complete works of Shakespeare, after at most (say) 100 million operations. Again, it's possible that such a program would work in a boring way, by applying some souped-up text compression to the plays and sonnets. But if it were mathematically possible to create a shorter

Linear Differential Equations
Physics 129a
051018 Frank Porter
Revision 151029 F. Porter

1 Introduction

A common problem we are faced with is that of solving for u in

$$Lu = g, \tag{1}$$

where L is a linear differential operator. We address this problem in this note, including both some theoretical remarks and practical approaches. Some foundational background may be found in the notes on Hilbert Spaces and on Distributions.

We will denote here whatever Hilbert space we are working in by the symbol $\mathcal{H}$.

2 Self-adjoint Operators

In physics, we typically encounter problems involving Hermitian operators:

Definition: If L is an operator with domain D_L, and

$$\langle Lu|v\rangle = \langle u|Lv\rangle \tag{2}$$

for all $u, v \in D_L$, then L is called a **Hermitian operator**.

The common appearance of Hermitian operators in physics has to do with the reality of their eigenvalues, e.g., the eigenvalues of a Hermitian matrix are real.

However, in general the specification that an operator be Hermitian may not be restrictive enough, once we consider differential operators on function spaces. We define the notion of the adjoint of an operator:

Definition: Given an operator L, with domain D_L such that D_L is dense in $\mathcal{H}$ (i.e., $\bar{D}_L = \mathcal{H}$), the **adjoint** $L^\dagger$ of L is defined according to:

$$\langle L^\dagger u|v\rangle = \langle u|Lv\rangle, \quad \forall v \in D_L. \tag{3}$$

It may be remarked that the domain, $D_{L^\dagger}$, of $L^\dagger$ is not necessarily identical with D_L.

A Mathematician's Lament

by Paul Lockhart

A musician wakes from a terrible nightmare. In his dream he finds himself in a society where music education has been made mandatory. "We are helping our students become more competitive in an increasingly sound-filled world." Educators, school systems, and the state are put in charge of this vital project. Studies are commissioned, committees are formed, and decisions are made— all without the advice or participation of a single working musician or composer.

Since musicians are known to set down their ideas in the form of sheet music, these curious black dots and lines must constitute the "language of music." It is imperative that students become fluent in this language if they are to attain any degree of musical competence; indeed, it would be ludicrous to expect a child to sing a song or play an instrument without having a thorough grounding in music notation and theory. Playing and listening to music, let alone composing an original piece, are considered very advanced topics and are generally put off until college, and more often graduate school.

As for the primary and secondary schools, their mission is to train students to use this language— to jiggle symbols around according to a fixed set of rules: "Music class is where we take out our staff paper, our teacher puts some notes on the board, and we copy them or transpose them into a different key. We have to make sure to get the clefs and key signatures right, and our teacher is very picky about making sure we fill in our quarter-notes completely. One time we had a chromatic scale problem and I did it right, but the teacher gave me no credit because I had the stems pointing the wrong way."

In their wisdom, educators soon realize that even very young children can be given this kind of musical instruction. In fact it is considered quite shameful if one's third-grader hasn't completely memorized his circle of fifths. "I'll have to get my son a music tutor. He simply won't apply himself to his music homework. He says it's boring. He just sits there staring out the window, humming tunes to himself and making up silly songs."

In the higher grades the pressure is really on. After all, the students must be prepared for the standardized tests and college admissions exams. Students must take courses in Scales and Modes, Meter, Harmony, and Counterpoint. "It's a lot for them to learn, but later in college when they finally get to hear all this stuff, they'll really appreciate all the work they did in high school." Of course, not many students actually go on to concentrate in music, so only a few will ever get to hear the sounds that the black dots represent. Nevertheless, it is important that every member of society be able to recognize a modulation or a fugal passage, regardless of the fact that they will never hear one. "To tell you the truth, most students just aren't very good at music. They are bored in class, their skills are terrible, and their homework is barely legible. Most of them couldn't care less about how important music is in today's world; they just want to take the minimum number of music courses and be done with it. I guess there are just music people and non-music people. I had this one kid, though, man was she sensational! Her sheets were impeccable— every note in the right place, perfect calligraphy, sharps, flats, just beautiful. She's going to make one hell of a musician someday."

Modelling Anticipation, Codification, and Husserl's Horizon of Meanings: The Non-linear Dynamics of Meaning in Social Systems

Loet Leydesdorff

Amsterdam School of Communications Research (ASCoR), University of Amsterdam,

Kloveniersburgwal 48, 1012 CX Amsterdam, The Netherlands.

loet@leydesdorff.net ; http://www.leydesdorff.net

Abstract

Social order does not exist as a stable phenomenon, but can be considered as "an order of reproduced expectations." When the anticipations operate upon one another, they can generate a non-linear dynamics which processes meaning. Although specific meaning can be stabilized, for example, in social institutions, all meaning arises from a global horizon of possible meanings. Using Luhmann's (1984) social systems theory and Rosen's (1985) theory of anticipatory systems, I submit algorithms for modeling the non-linear dynamics of meaning in social systems. First, a self-referential system can use a model of itself for the anticipation. Under the condition of functional differentiation, the social system can be expected to entertain a set of models; each model can also contain a model of the other models. Two anticipatory mechanisms are then possible: one transversal between the models, and a longitudinal one providing the system with a variety of meanings. A system containing two anticipatory mechanisms can become hyper-incursive. Without making decisions, however, a hyper-incursive system would be overloaded with uncertainty. Under this pressure, informed decisions tend to replace "natural preferences" of agents and a knowledge-based order can increasingly be shaped.

Keywords: anticipation, social system, meaning, incursion, globalization

the next generation of proof assistants

Freek Wiedijk

Radboud University Nijmegen
The Netherlands

2010 08 31 , 16 : 30

LSFA 2010
Natal, Brazil

Science, 236, 1987, 1527-1532.

Articles

Measurement Scales on the Continuum

R. Duncan Luce and Louis Narens

In a seminal article in 1946, S. S. Stevens noted that the numerical measures then in common use exhibited three admissible groups of transformations: similarity, affine, and monotonic. Until recently, it was unclear what other scale types are possible. For situations on the continuum that are homogeneous (that is, objects are not distinguishable by their properties), the possibilities are essentially these three plus another type lying between the first two. These types lead to clearly described classes of structures that can, in principle, be incorporated into the classical structure of physical units. Such results, along with characterizations of important special cases, are potentially useful in the behavioral and social sciences.

The main research activities today on the mathematics underlying numerical representations of qualitative orderings of objects or events—theories of measurement—center not on the classical methods that evolved in physics, which are well understood, but on alternative methods that may prove useful in other sciences where measurement has proved elusive. There are several different themes, and this article concentrates on one that has been developed by Luce and Narens and others interested with them. It is a scheme of classifying structures according to the degrees of uniqueness of their numerical representations. The results all concern a very general situation in the sciences, namely, where a phenomenon of interest can be described in terms of quantities, continuous variables as functions of other quantities, continuous variables.

The term "measurement" has many meanings, the most common being that of assigning numbers to empirical objects according to some definite scheme. Empirical measurements based on such schemes almost always involve error, and the means for understanding and dealing with errors of fundamental importance in practice. However, in the theory of measurement, consideration of error often is not treated explicitly. There are at least two good reasons for this. First, no general qualitative concept of measurement error has yet emerged, which makes it very difficult to incorporate error into developed theories of measurement. Second, for a large body of measurement issues, error considerations play little or no role. The latter is especially true of those issues, such as dimensional analysis in physics, that rely on an understanding of the interconnections of various numerical representations rather than on the practical production of accurate representations. This made a substantial orderly with issues for which error is not a significant factor.

R. D. Luce is Victor S. Thomas Professor of Psychology at Harvard University, Cambridge, MA 02138, and L. Narens is also at the Department of Mathematics, University of California, Irvine, CA 92717.

Classical Measurement of Physical Units

A continuous monotonic variable is nothing more than a continuously ordered set, that can be mapped in an order-preserving way onto an interval of the ordered real numbers. Such ordered sets are called continua in mathematics (1). In measurement theory, such order-preserving mappings are called "representations," or sometimes "measurements," since they "measure" the qualitative objects by assigning numbers in a consistent way to the objects.

For many scientific purposes, such representations of variables as temperature and brightness are sufficient, but cases that are ubiquitous throughout all of science. Many philosophers of science object to the use of continua as accurate descriptions of empirical variables, which are often believed to assume only finitely many values or are at most piecewise smooth. We consider this a valid issue, but one about which we cannot comment in any detail in this short article. Suffice it to say we believe that valid representations can be presented to qualities that continuous variables are the correct kind of idealization for more, if not most, of the ordinal empirical situations encountered in science (2, 3).

A continuum can have many different representations. For example, if a continuum has a representation ϕ into the positive real numbers, which we denote $\langle A, \succsim \rangle \to \langle \mathbf{R}^+, \geq \rangle$, then $f \circ \phi$ (where $\circ$ denotes functional composition) is also a representation into $\mathbf{R}^+$ for all strictly monotonic functions f from $\mathbf{R}^+$ onto $\mathbf{R}^+$, and it is easy to show that all such representations have this form. The set of representations of a continuum onto $\mathbf{R}^+$ is an example of what is called an ordinal scale (4). Although ordinal scales are abundant in the behavioral and social sciences—many scales of all sorts are the most common examples—they are avoided in the physical sciences because they are naturally viewed as asymmetrical forms of measurement. This situation is awesome because physical variables are always constrained in additional ways that greatly improve the possible representations.

For example, in a number of previous two objects exhibiting the attribute to be measured can be combined to form another object that also exhibits the attribute. Formally, such combinations generate a binary operation that is given the generic name "concatenation." In measurement theory of continuous variables, it is postulated as an empirical law that concatenation of qualitative objects is monotonic with respect to the qualitative ordering of the attribute. This means that if $\succsim$ denotes the ordering and $\circ$ the operation, then for any objects x, y, z in the domain X,

$$x \succsim y \Leftrightarrow (x \circ z) \succsim (y \circ z).$$

Mass and length measurement are familiar examples. In addition, they also satisfy the properties $(x \circ y) \circ z \sim x \circ (y \circ z)$, called associativity, and $x \circ y \sim y \circ x$, called commutativity, where $\sim$ denotes equivalence in the sense that both $x \succsim y$ and $y \succsim x$ hold.

For such relational structures $\langle X, \succsim, \circ \rangle$, measurement proceeds by concatenating copies of various elements in the domain. Let n be a positive integer and x and element of X; then nx denotes the concatenation of n copies of x. By associativity and commutativity,

HAL
archives-ouvertes.fr

Homology of Cellular Structures Allowing Multi-incidence

Sylvie Alayrangues, Guillaume Damiand, Pascal Lienhardt, Samuel Peltier

▶ **To cite this version:**

Sylvie Alayrangues, Guillaume Damiand, Pascal Lienhardt, Samuel Peltier. Homology of Cellular Structures Allowing Multi-incidence. Discrete and Computational Geometry, Springer Verlag, 2015, 54 (1), pp.42-77. <10.1007/s00454-015-9662-5>. <hal-01189215>

HAL Id: hal-01189215

https://hal.archives-ouvertes.fr/hal-01189215

Submitted on 15 Dec 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ABSTRACT

Title of dissertation: NUMBER THEORETIC ALGORITHMS FOR ELLIPTIC CURVES

Juliana V. Belding, Doctor of Philosophy, 2008

Dissertation directed by: Professor Lawrence Washington
Department of Mathematics

We present new algorithms related to both theoretical and practical questions in the area of elliptic curves and class field theory. The dissertation has two main parts, as described below.

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D < 0$, and let $K = \mathbb{Q}(\sqrt{D})$. The class polynomial H_D of $\mathcal{O}$ is the polynomial whose roots are precisely the j-invariants of elliptic curves with complex multiplication by $\mathcal{O}$. Computing this polynomial is useful in constructing elliptic curves suitable for cryptography, as well as in the context of explicit class field theory. In the first part of the dissertation, we present an algorithm to compute H_D p-adically where p is a prime inert in K and not dividing D. This involves computing the canonical lift $\tilde{E}$ of a pair (E, f) where E is a supersingular elliptic curve and f is an embedding of $\mathcal{O}$ into the *endomorphism ring* of E. We also present an algorithm to compute H_D modulo p for p inert which is used in the Chinese remainder theorem algorithm to compute H_D.

For an elliptic curve E over any field K, the Weil pairing e_n is a bilinear map on the points of order n of E. The Weil pairing is a useful tool in both the theory of elliptic curves

Quantum Inf Process (2010) 9:47–59
DOI 10.1007/s11128-009-0126-9

Exponential quantum enhancement for distributed addition with local nonlinearity

Adam Henry Marblestone · Michel Devoret

Received: 7 May 2009 / Accepted: 30 July 2009 / Published online: 15 August 2009
© Springer Science+Business Media, LLC 2009

Abstract We consider classical and entanglement-assisted versions of a distributed computation scheme that computes nonlinear Boolean functions of a set of input bits supplied by separated parties. Communication between the parties is restricted to take place through a specific apparatus which enforces the constraints that all nonlinear, nonlocal classical logic is performed by a single receiver, and that all communication occurs through a limited number of one-bit channels. In the entanglement-assisted version, the number of channels required to compute a Boolean function of fixed nonlinearity can become exponentially smaller than in the classical version. We demonstrate this exponential enhancement for the problem of distributed integer addition.

Keywords Quantum communication complexity · Locally nonlinear distributed evaluation · Entanglement · Nonlinear Boolean functions

PACS 03.67.Hk · 03.67.Ac · 03.67.-a

1 Introduction

The study of quantum communication complexity [1,2,7] has drawn attention to the feasibility using quantum protocols of certain classically impossible communication tasks. This is strikingly demonstrated by quantum pseudo-telepathy protocols [3]. In quantum pseudo-telepathy, entanglement eliminates the classical need for signaling between separated parties collaborating to perform a task. Crucially,

A. H. Marblestone (✉) · M. Devoret
Department of Applied Physics, Yale University, P.O. Box 208284, New Haven, CT 06520, USA
e-mail: amarbles@fas.harvard.edu

M. Devoret
e-mail: michel.devoret@yale.edu

CLERK'S OFFICE
A TRUE COPY
JUL 12 2017
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

SEALED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 17-CR-124

[Redacted] and
MARCUS HUTCHINS,
aka "Malwaretech,"

Defendants.

[Title 18, United States Code, Sections 371, 1030(a)(5)(A), 2511(a)(1), and 2512(1)(a), (b), and (c)(i)]

INDICTMENT

COUNT ONE

THE GRAND JURY CHARGES:

1. At times material to this indictment:

DEFENDANTS

a. Defendant [redacted] used the online aliases [redacted]

b. Defendant MARCUS HUTCHINS was a citizen and resident of the United Kingdom. HUTCHINS used various online aliases, including "Malwaretech."

RELEVANT TERMS

c. A "protected computer" was a computer in or affecting interstate or foreign commerce or communications, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communions of the United States.

MARKETS NOT CAPITALISM

individualist anarchism against bosses, inequality, corporate power, and structural poverty

Edited by Gary Chartier & Charles W. Johnson

Parametric Study of a Genetic Algorithm using a Aircraft Design Optimization Problem

Andre C. Marta
Dept. of Aeronautics and Astronautics
Stanford University
Stanford, California 94305
acmarta@stanford.edu

ABSTRACT

This work shows how a preliminary aircraft design can be achieved by means of genetic algorithms (GA). The aircraft major parameters are mapped into a chromosome like string. These include the wing, tail and fuselage geometry, thrust requirements and operating parameters. GA operators are performed on a population of such strings and natural selection is expected to occur. The design performance is obtained by using the aircraft range as the fitness function. Different GA parameters and selection methods – fitness and ranking – are tested and their impact on the algorithm efficiency is analyzed. The constraints implementation is also studied.

1. Introduction

At first glance, the definition of the best aircraft design is very simple: the fastest, most efficient, quietest, most inexpensive airplane with the shortest field length. Unfortunately, such an airplane cannot exist. One can only make one thing best at a time, as illustrated in figure 1. The most inexpensive airplane would surely not be the fastest, as well as the most efficient would not be the most comfortable. In other words, the overall airplane is always a compromise in some sense. Various quantities are included in a function termed the figure of merit or objective, such as weight, flight controls, structures, manufacturing, aerodynamics, noise and propulsion characteristics, whose relative weights depends on the intended application for the aircraft.

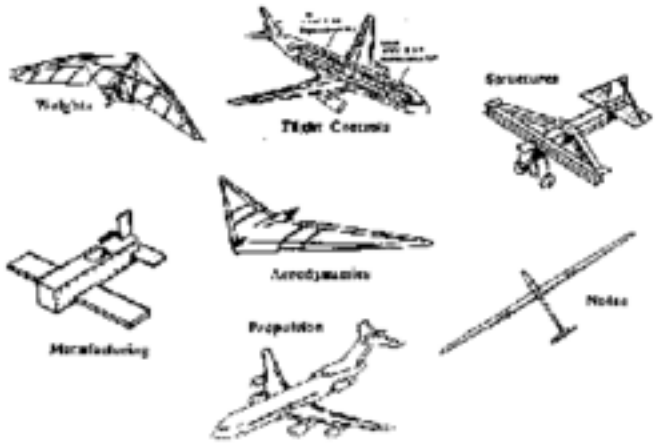


Figure 1 Make one thing best at a time

Boundary Port Hamiltonian systems for multi-physical systems illustrated with examples including heat and mass transport phenomena

B. Maschke

LAGEP
Laboratoire d'Automatique et de Génie des procédés,
Université Lyon 1

Model Reduction of Transport-dominated Phenomena,19 May 2015

MAT A Sek-13-3-q.pdf, Blatt 1

Fielded Capability: End-to-End VPN

SPIN 9 Design Review

[redacted]

The overall classification for this brief is:

TOPSECRET//COMINT//REL USA, AUS, CAN, GBR, NZL//20320108

Some Comments on the History, Theory, and Applications of Symplectic Reduction

In this Preface, we make some brief remarks about the history, theory and applications of symplectic reduction. We concentrate on developments surrounding our paper Marsden and Weinstein [1974] and the closely related work of Meyer [1973], so the reader may find some important references omitted. This is inevitable in a subject that has grown so large and has penetrated so deeply both pure and applied mathematics, as well as into engineering and theoretical physics.

We thank Klaas Landsman for the invitation to write these introductory remarks for this exciting book. We hope that they will be especially useful for younger workers in the area. Some of this preface is taken, with some revision, from an introductory section in Marsden, Ratiu and Scheurle [2000]. We would like to thank Tudor Ratiu and Jürgen Scheurle for their permission to use this material here.

Reduction of Symplectic Manifolds. Most readers of this volume presumably know how symplectic reduction goes: given a hamiltonian action of a Lie group on a symplectic manifold, one divides a level set of a momentum map by the action of a suitable subgroup to form a new symplectic manifold. Before the division step, one has a manifold (possibly singular, an occurrence without which this volume would not exist) carrying a degenerate closed 2-form. Removing such a degeneracy by passing to a quotient space was a well-known differential-geometric operation promoted by Elie Cartan [1922]. The "suitable subgroup" related to a momentum mapping was identified by Steven Smale [1970] in a special case, without the symplectic trappings. It was Smale's work that inspired the general symplectic construction by Meyer and ourselves.

More should be said about momentum maps themselves. The idea that an action of a Lie group G with Lie algebra $\mathfrak{g}$ on a symplectic manifold P should be accompanied by a map $J : P \to \mathfrak{g}^*$ which is equivariant with respect to the coadjoint action, and the fact that the orbits of this action are themselves symplectic manifolds both occur already in Lie [1890]; the links with mechanics also rely on the work of Lagrange, Poisson, Jacobi and Noether. In modern form, the momentum map and its equivariance were rediscovered by Kostant [1966] and Souriau [1966, 1970] in the general symplectic case and by Smale [1970] for the case of the lifted action from a manifold Q to its cotangent bundle $P = T^*Q$.

As for terminology, neither Lie nor Kostant gave the map J a special name. Smale referred to it as the "angular momentum" by generalization from the special case $G = SO(3)$, while Souriau called it by the French word "moment". In our paper Marsden and Weinstein [1974], following usage emerging at that time, we used the English word "moment" for J, but we were soon set straight by Richard Cushman and Hans Duistermaat, who convinced us that the proper English translation of Souriau's French word was "momentum," which had the added benefit of meshing with Smale's designation and standard usage in mechanics. Since 1976 or so, we have referred to J as a momentum map (or mapping); for example, this term is used in Abraham and Marsden [1978]. On the other hand, Guillemin and Sternberg popularized the continuing use of "moment" in English, and both words coexist today. (See the footnote on page 133 of Mikami and Weinstein [1988] for a semi-serious attempt to bridge the gap.) It is a curious twist, as comes out in work on collective nuclear motion (Guillemin and Sternberg [1980]) and plasma physics (Marsden and Weinstein [1982] and Marsden, Weinstein, Ratiu and Schmid [1983]), that moments of inertia and moments of probability distributions can actually be the values of momentum maps! See Marsden and Ratiu [1999] for more on the history of the momentum map.

Das Eine im Wandel: music and *Kunstwissenschaft*

Robert Williams

Belief in the importance of the relationship between music and the visual arts had a profound effect on the development of artistic modernism in the decades around 1900, most obviously on the emergence of abstract painting. Kandinsky is the figure who first comes to mind and whose example and influence were probably most important historically, but interest in music was shared by many of the pioneering abstractionists, from Gauguin and Seurat to Matisse, Mondrian, and Klee. At the same time, though in a less conspicuous and perhaps largely indirect way, music helped to shape 'formalist' art theory and criticism. Pater's emphatic claim that '*all art constantly aspires to the condition of music*',[1] published in 1873, was frequently invoked during the subsequent decades, and Kandinsky's elaboration of the relation between music and painting in *On the Spiritual in Art*, of 1911, based on his belief that all the arts now receive their 'most valuable lesson' from music,[2] can be understood as an effort to follow through on the project implicit in Pater's remark, even though Pater is not mentioned by name. The sense of an analogical relationship between music and painting seems to have been so pervasive that explicit references to it, numerous as they are, do not indicate the real the extent of its importance. One is tempted to characterize it as culturally overdetermined, partly accessible to the consciousness of the protagonists, certainly, but also partly structured by larger forces that are more difficult to objectify.

The aim of this essay is to show that a sense of the relation of music to the visual arts also exerted an influence on the development of *Kunstwissenschaft* and the modern discipline of art history during the same period, and that this influence, too, was more pervasive than explicit references to it would lead one to suspect. This case is worth making with some emphasis because the scholars in question, eager to establish their discipline upon rigorously empirical, 'scientific' methods, made a point of centering their inquiry upon the specifically visual properties of the works involved, and subsequent art history – including much recent work that is pointedly anti-empirical – has perpetuated, even intensified, this fixation on the visual. The fact that the influence of music should come to the fore at just the moment when art history was trying to specify its area of competence most precisely indicates the unique importance of music in the culture of the period, especially in the German-

[1] W. Pater, *The Renaissance*, London: William Collins & Sons, 1910, 135.
[2] W. Kandinsky, *Über das Geistige in der Kunst*, Munich: R. Piper & Co., 1912, esp. 37.

Metamath

A Computer Language for Pure Mathematics

Norman Megill

bell¿ngcat

MH17

The Open Source Investigation Three Years Later

MORSE THEORY

BY

J. Milnor

Based on lecture notes by

M. SPIVAK and R. WELLS

PRINCETON, NEW JERSEY

PRINCETON UNIVERSITY PRESS

1963

Pergamon PII: S0016-0032(97)00046-X

J. Franklin Inst. Vol. 334B, No. 5/6, pp. 737–744, 1997
© 1997 The Franklin Institute
Published by Elsevier Science Ltd
Printed in Great Britain
0016-0032/97 $17.00+0.00

*Chua's Circuit and the Qualitative Theory of Dynamical Systems**

by CHRISTIAN MIRA

Groupe d'Etudes des Systèmes Non Linéaires et Applications, INSA-DGEI, Complexe Scientifique de Rangueil, 31077 Toulouse Cedex, France

ABSTRACT. *Simple electronic oscillators were at the origin of many studies related to the qualitative theory of dynamical systems. Chua's circuit is now playing an equivalent role for the appearance and understanding of complex dynamics.* © 1997 The Franklin Institute. Published by Elsevier Science Ltd

1. Oscillating Circuits and the Origin of the Qualitative Theory

In the nineteenth century, Joseph Fourier wrote: "The study of Nature is the most productive source of mathematical discoveries. By offering a specific objective, it provides the advantage of excluding vague problems and unwieldy calculations. It is also a means to form the Mathematical Analysis, and isolate the most important aspects to know and to conserve. These fundamental elements are those which appear in all natural effects."

The important development of the theory of dynamic systems, during this century, has essentially its origins in the study of the 'natural effects' encountered in systems of mechanical, electrical, or electronic engineering, and the rejection of non-essential generalizations. Most of the results obtained in the abstract dynamic systems field have been possible on the foundations of results from the concrete dynamic systems field. It is also worth noting that the majority of scientists (including mathematicians) were not led to their discoveries by a process of deduction from general postulates or general principles, but rather by a thorough examination of properly chosen particular cases, and observation of concrete processes. The generalizations have come later, because it is far easier to generalize an established result than to discover a new line of argument.

Since Andronov (1932), traditionally three different approaches have been used for the study of dynamical systems (36): qualitative methods, analytical methods and numerical methods. To define the 'strategy' of qualitative methods, one has to note

* In honour of my friend Leon Chua on his sixtieth birthday.

16.410/413
Principles of Autonomy and Decision Making

Lecture 21: Intro to Hidden Markov Models
the Baum-Welch algorithm

Emilio Frazzoli

Aeronautics and Astronautics
Massachusetts Institute of Technology

November 24, 2010

4. Energy Levels

4.1 Bound problems
- 4.1.1 Energy in Square infinite well (particle in a box)
- 4.1.2 Finite square well

4.2 Quantum Mechanics in 3D: Angular momentum
- 4.2.1 Schrödinger equation in spherical coordinates
- 4.2.2 Angular momentum operator
- 4.2.3 Spin angular momentum
- 4.2.4 Addition of angular momentum

4.3 Solutions to the Schrödinger equation in 3D
- 4.3.1 The Hydrogen atom
- 4.3.2 Atomic periodic structure
- 4.3.3 The Harmonic Oscillator Potential

4.4 Identical particles
- 4.4.1 Bosons, fermions
- 4.4.2 Exchange operator
- 4.4.3 Pauli exclusion principle

4.1 Bound problems

In the previous chapter we studied stationary problems in which the system is best described as a (time-independent) wave, "scattering" and "tunneling" (that is, showing variation on its intensity) because of obstacles given by chang in the potential energy.
Although the potential determined the space-dependent wavefunction, there was no limitation imposed on the possible wavenumbers and energies involved. An infinite number of energies were possible solutions to the time-independent Schrödinger equation.
In this chapter, we want instead to describe systems which are best described as particles confined inside a potential.
This type of system well describe atoms or nuclei whose constituents are bound by their mutual interaction shall see that because of the particle confinement, the solutions to the energy eigenvalue equation (i.e. the t independent Schrödinger equation) are now only a discrete set of possible values (a discrete set os energy levels).
The energy is therefore **quantized**. Correspondingly, only a discrete set of eigenfunctions will be solutions, thus th system, if it's in a stationary state, can only be found in one of these allowed eigenstates.
We will start to describe simple examples. However, after learning the relevant concepts (and mathematical tr we will see how these same concepts are used to predict and describe the energy of atoms and nuclei. Th can predict for example the discrete emission spectrum of atoms and the nuclear binding energy.

4.1.1 Energy in Square infinite well (particle in a box)

The simplest system to be analyzed is a particle in a box: classically, in 3D, the particle is stuck inside th can never leave. Another classical analogy would be a ball at the bottom of a well so deep that no matter how much kinetic energy the ball possess, it will never be able to exit the well.
We consider again a particle in a 1D space. However now the particle is no longer free to travel but is confined to be between the positions 0 and L. In order to confine the particle there must be an infinite force at these bound that repels the particle and forces it to stay only in the allowed space. Correspondingly there must be an potential in the forbidden region.
Thus the potential function is as depicted in Fig. $V(x) = \infty$ for $x < 0$ and $x > L$; and $V(x) = 0$ for $0 \leq x \leq L$.
This last condition means that the particle behaves as a free particle inside the well (or box) created by the potential.

Mixed states and pure states

(Dated: April 9, 2009)

These are brief notes on the abstract formalism of quantum mechanics. They will introduce the concepts of *pure* and *mixed* quantum states. Some statements are indicated by a **P**. You should try and prove these statements. If you understand the formalism, then these statements should not be hard to prove; they are good tests for your understanding. The homework will contain more difficult questions.

1. A pure state of a quantum system is denoted by a vector (ket) $|\psi\rangle$ with unit length, i.e. $\langle\psi|\psi\rangle = 1$, in a complex Hilbert space H. Previously, we (and the textbook) just called this a 'state', but now we call it a 'pure' state to distinguish it from a more general type of quantum states ('mixed' states, see step 21).

2. We already know from the textbook that we can define dual vectors (bra) $\langle\phi|$ as linear maps from the Hilbert space H to the field C of complex numbers. Formally, we write

$$\langle\phi|(|\psi\rangle) = \langle\phi|\psi\rangle.$$

   The object on the right-hand side denotes the inner product in H for two vectors $|\phi\rangle$ and $|\psi\rangle$. That notation for the inner product used to be just that, notation. Now that we have defined $\langle\phi|$ as a dual vector it has acquired a second meaning.

3. Given vectors and dual vectors we can define operators (i.e., maps from H to H) of the form

$$\hat{O} = |\psi\rangle\langle\phi|.$$

   $\hat{O}$ acts on vectors in H and produces as result vectors in H (**P**).

4. The hermitian conjugate of this operator is

$$\hat{O}^\dagger \equiv |\phi\rangle\langle\psi|.$$

   This follows (**P**) straight from the definition of the hermitian conjugate:

$$(\langle m|\hat{O}|n\rangle)^* = \langle n|\hat{O}^\dagger|m\rangle,$$

   for all states $|n\rangle$ and $|m\rangle$ in H.

Models for Metamath

Mario Carneiro

Carnegie Mellon University, Pittsburgh PA, USA

Abstract. Although some work has been done on the metamathematics of Metamath, there has not been a clear definition of a model for a Metamath formal system. We define the collection of models of an arbitrary Metamath formal system, both for tree-based and string-based representations. This definition is demonstrated with examples for propositional calculus, ZFC set theory with classes, and Hofstadter's MIU system, with applications for proving that statements are not provable, showing consistency of the main Metamath database (assuming ZFC has a model), developing new independence proofs, and proving a form of Gödel's completeness theorem.

Keywords: Metamath · Model theory · formal proof · consistency · ZFC · Mathematical logic

1 Introduction

Metamath is a proof language, developed in 1992, on the principle of minimizing the foundational logic to as little as possible [1]. An expression in Metamath is a string of constants and variables headed by a constant called the expression's "typecode". The variables are typed and can be substituted for expressions with the same typecode. See § 2.1 for a precise definition of a formal system, which mirrors the specification of the .mm file format itself.

The logic on which Metamath is based was originally defined by Tarski in [2]. Notably, this involves a notion of "direct" or "non-capturing" substitution, which means that no α-renaming occurs during a substitution for a variable. Instead, this is replaced by a "distinct variable" condition saying that certain substitutions are not valid if they contain a certain variable (regardless of whether the variable is free or not—Metamath doesn't know what a free variable is). For instance, the expression $\forall x\, \varphi$ contains a variable φ inside a binding expression "$\forall x \square$". (Metamath also does not have a concept of "binding expression", but it is safe to say that under a usual interpretation this would be considered a binding expression.) If there is a distinct variable condition between x and φ, then the substitution $\varphi \mapsto x = y$ is invalid, because x is present in the substitution to φ. This is stricter than the usual first-order logic statement "x is not free in φ", because $\varphi \mapsto \forall x\, x = y$ is also invalid. If there is no such distinct variable condition between x and φ, these substitutions would be allowed, and applying them to $\forall x\, \varphi$ would result in $\forall x\, x = y$ and $\forall x \forall x\, x = y$, respectively.

In this paper, we will develop a definition for models of Metamath-style formal systems, which will operate by associating a function to each syntactical

Bivalent Semantics for De Morgan Logic (The Uselessness of Four-valuedness)

Jean-Yves Béziau

Dedicated to Newton da Costa for his 79th birthday

ABSTRACT. In this paper we present a bivalent semantics for De Morgan logic in the spirit of da Costa's theory of valuation showing therefore the uselessness of four-valuedness - the four-valued Dunn-Belnap semantics being ordinarily used to characterize De Morgan logic. We also present De Morgan logic in the perspective of universal logic, showing how some general results connecting bivaluations to sequent rules and reducing many-valued matrices to non-truth functional bivalent semantics work.

1 De Morgan logic in the perspective of universal logic

In this paper we present a systematic study of a very simple and nice logical structure, De Morgan logic. This is a logic with a negation which is both paraconsistent and paracomplete, that is to say neither the principle of contradiction, nor the principle of excluded middle are valid for De Morgan negation, but all De Morgan laws hold, the reason for the name. This logic shows therefore the independence of the principle of contradiction and the principle of excluded middle relatively to De Morgan laws [1].

This logic is not new. It is connected with De Morgan lattices which can be traced back to Moisil [22] and which have been called quasi-boolean algebras by Rasiowa, [13], distributive i-lattices by Kalman [20], and have been especially studied by the school of Antonio Monteiro in Bahia-Blanca, Argentina [23].

[1] Negations which are both paraconsistent and paracomplete were called by da Costa non-aléthic, we have proposed to used instead the adjective paranormal in order to keep the paraterminology. De Morgan negation is a good example of paranormal negation, it can reasonably be considered as a negation, due to the fact that it obeys De Morgan laws.

Witten's Proof of Morse Inequalities

by Igor Prokhorenkov

Let M be a smooth, compact, oriented manifold with dimension n. A **Morse function** is a smooth function $f : M \to \mathbb{R}$ such that all of its *critical points* are *nondegenerate*. A point $\overline{x} \in M$ is a **critical point** of f if $df(\overline{x}) = 0$. A critical point is **nondegenerate** if

$$\det(Hess(f)(\overline{x})) = \det\left[\frac{\partial^2 f}{\partial x_i \partial x_j}\right](\overline{x}) \neq 0.$$

Both properties do not depend on the choice of coordinates. The index $\operatorname{ind}(\overline{x})$ is the number of negative eigenvalues of $Hess(f)(\overline{x})$. Let $m_p = m_p(f)$ be the number of critical points of index p. Let $b_p = b_p(M) = \dim H^p(M)$ be the dimension of the p^{th} de Rham cohomology group.

$$0 \to \Omega^0(M) \xrightarrow{d} \Omega^1(M) \xrightarrow{d} ... \xrightarrow{d} \Omega^n(M) \xrightarrow{d} 0$$

This is called the de Rham complex. Note that $d^2 = 0$. If $\omega = d\alpha$, then $d\omega = 0$. So $\operatorname{Im} d : \Omega^{p-1} \to \Omega^p \subseteq \ker d : \Omega^p \to \Omega^{p+1}$, and

$$H^p(M) = \frac{\ker d}{\operatorname{Im} d}.$$

Theorem 1. *The **Morse inequalities** are as follows. The Morse polynomial $M(t)$ and Poincare polynomial $P(t)$ are defined by*

$$\begin{aligned} M(t) &= \sum_{k=0}^{n} m_k t^k \\ P(t) &= \sum_{k=0}^{n} b_k t^k. \end{aligned}$$

There exists a polynomial $R(t) = R_0 + R_1 t + R_2 t^2 + ...$ with all $R_k \geq 0$ such that

$$M(t) - P(t) = (1+t)R(t).$$

For example, consider $M =$ the torus with a saddle at the top. Then

$$\begin{aligned} H^0 &= \mathbb{R}, \text{ so } b_0 = 1 \\ H^1 &= \mathbb{R}, \text{ so } b_1 = 2 \\ H^2 &= \mathbb{R}, \text{ so } b_2 = 1. \end{aligned}$$

Thus

$$P(t) = 1 + 2t + t^2.$$

Founding Cryptography on Oblivious Transfer – Efficiently

Yuval Ishai*
Technion, Israel and University of California, Los Angeles
yuvali@cs.technion.il

Manoj Prabhakaran†
University of Illinois, Urbana-Champaign
mmp@cs.uiuc.edu

Amit Sahai‡
University of California, Los Angeles
sahai@cs.ucla.edu

October 5, 2010

Abstract

We present a simple and efficient compiler for transforming secure multi-party computation (MPC) protocols that enjoy security only with an honest majority into MPC protocols that guarantee security with no honest majority, in the oblivious-transfer (OT) hybrid model. Our technique works by combining a secure protocol in the honest majority setting with a protocol achieving only security against *semi-honest* parties in the setting of no honest majority.

Applying our compiler to variants of protocols from the literature, we get several applications for secure two-party computation and for MPC with no honest majority. These include:

- **Constant-rate two-party computation in the OT-hybrid model.** We obtain a statistically UC-secure two-party protocol in the OT-hybrid model that can evaluate a general circuit C of size s and depth d with a total communication complexity of $O(s) + poly(k, d, \log s)$ and $O(d)$ rounds. The above result generalizes to a constant number of parties.
- **Extending OTs in the malicious model.** We obtain a computationally efficient protocol for generating many string OTs from few string OTs with only a *constant amortized communication overhead* compared to the total length of the string OTs.
- **Black-box constructions for constant-round MPC with no honest majority.** We obtain general computationally UC-secure MPC protocols in the OT-hybrid model that use only a constant number of rounds, and only make a *black-box* access to a pseudorandom generator. This gives the first constant-round protocols for three or more parties that only make a black-box use of cryptographic primitives (and avoid expensive zero-knowledge proofs).

1 Introduction

Secure multiparty computation (MPC) [47, 25, 5, 13] allows several mutually distrustful parties to perform a joint computation without compromising, to the greatest extent possible, the privacy of their inputs or the correctness of the outputs. MPC protocols can be roughly classified into two

*Supported in part by BSF grant 1310/06, BSF grant 2004361, and NSF grants 0205594, 0430254, 0456717, 0627781, 0716389.

†Supported in part by NSF grants CNS 07-16626 and CNS 07-47027.

‡Research supported in part from NSF grants 0627781, 0716389, 0456717, and 0205594, a subgrant from SRI as part of the Army Cyber-TA program, an equipment grant from Intel, an Alfred P. Sloan Foundation Fellowship, and an Okawa Foundation Research Grant.

Appeared in the Proceedings of the 7th Nordic Workshop on Secure IT Systems—NORDSEC 2002.

Virtual Hierarchies - An Architecture for Building and Maintaining Efficient and Resilient Trust Chains

John Marchesini and Sean Smith
Department of Computer Science *
Dartmouth College

{carlo,sws}@cs.dartmouth.edu

DRAFT of May 17, 2002

Abstract

In *Public Key Infrastructure (PKI)*, the simple, monopolistic organizational model of certificate issuing entities works fine until we consider real-world issues. Then, issues such as scalability and mutually suspicious organizations create the need for a multiplicity of certificate issuing entities, which introduces the problem of how to organize them to balance resilience to compromise against efficiency of path discovery. Many solutions involve organizing the infrastructure to follow a natural organizational hierarchy, but in some cases, such a natural organizational hierarchy may not exist.

However, systems research has given us *secure coprocessing* for securely carrying out computations among multiple trust domains. Cryptography has produced a number of methods for distributing cryptographic computations, such as *secret splitting* and *threshold cryptography*. Last, distributed computing has given us *peer-to-peer networking*, for creating self-organizing distributed systems.

In this paper, we use these latter tools to address the former problem by overlaying a *virtual hierarchy* on a mesh architecture of peer certificate issuing entities, and achieving both resilience and efficiency.

*This work was supported in part by Internet2/AT&T, by IBM Research, and by the U.S. Department of Justice, contract 2000-DT-CX-K001. However, the views and conclusions do not necessarily represent those of the sponsors. A preliminary version appears as TR2002-416.

1 Introduction

1.1 The Problem

Background By separating the privilege to decrypt or sign a message from the privilege to encrypt or verify, *public-key cryptography* enables forms of trusted communication between parties who do not share secrets *a priori*. Eliminating the need for shared secrets has multiple advantages. On a global level, it potentially enables extending trusted communication across organizational boundaries, between parties who have never met. But it can also reduce overhead in managing communication between parties even on a local level, within one organization: the number of needed keys goes from $\Omega(n^2)$ to $O(n)$.

PKI has many definitions; the most commonly accepted definition refers to how one participating party learns what the public key is for another party. Typically, approaches to PKI begin by condensing trust: rather than *a priori* knowing the public key of each party in the population, the relying party instead knows the public key of a designated special party, who in turn issues signed statements (e.g., certificates and CRLs) about members of the population.

This designated party is typically called the *certificate authority (CA)*. Some approaches separate the process of issuing certificates from the process of

Discrete *vs* continuous controversy in physics

Annick LESNE
Laboratoire de Physique Théorique des Liquides, Case 121
4 Place Jussieu, 75252 Paris Cedex 05, France
lesne@lptl.jussieu.fr

This paper presents a sample of the deep and multiple interplay between discrete and continuous behaviors and corresponding modelings in physics. The aim of this overview is to show that discrete and continuous features coexist in any natural phenomenon, depending on the scales of observation. Accordingly, different models, either discrete or continuous in time, space, phase space or conjugate space can be considered. Some caveats about their limits of validity and their interrelations (discretization, continuous limits) are pointed out. Difficulties and gaps arising due to the singular nature of continuous limits and to information loss accompanying discretizations are discussed.

I. INTRODUCTION: SETTING THE STAGE

This special issue of *MSCS* reflects the deep and multiple debates arising in pure and computational mathematics about discrete *vs* continuous frameworks and computations. The debated issues are ranging from practical caveats about the use of discrete computational schemes for solving continuous equations, or continuous frameworks to describe discrete systems, up to conceptual questions about the very nature, either discrete or continuous, of the reality (rather of our perception of the reality). The tension between discrete and continuous aspects is also ubiquitous in physics. In this contribution, I'll try to give a brief and unavoidably far from complete account of the numerous facets of this dilemma, from a physical viewpoint, with as less prerequisites as possible.

A. The terms of the debate: "discrete" and "continuous"

Let us first clarify the discussion and sketch the skeleton on which specific examples will be articulated. The preliminary step is to agree on the terms of the debate. Discrete (respectively continuous) can refer to:

— *time*: the evolution of a system can be described either as a continuous trajectory in the space of system states (what is called the "phase space"), either as a discrete sequence of successive states (see Section II);

— *real space*: the underlying space (of dimension $d = 1, 2, 3$ in natural situations or possibly larger in theoretical case studies) might be seen either as a continuum, where positions are labeled by d real-valued coordinates, either as a tiling of discrete cells, or equivalently a lattice, where positions are labeled by d integers (see Section III);

— *phase space*: the representation of the system state may scan a continuum (a vector space or a manifold) or vary inside a discrete set (finite or countable) of configurations (see Section IV);

— *conjugate space*, in the context of spectral analyses: we shall see in Section V that spectra offer another modality of the "discrete *vs* continuous" alternative.

It is to note that the meaning of "continuous" is less ambiguous in physics than in mathematics, where set-theoretic, topological and measure-theoretic notions of continuity superimpose. In physics, the required smoothness is included in the very notion of continuous medium and in the same way, a continuous dynamical system will be differentiable unless explicitly mentioned. It might have seemed sensible to distinguish between *discrete* systems, namely made of disjoint (seemingly intrinsic) particles, and *discretized* systems, resulting from a (seemingly arbitrary) partition; examples of quantum particles, localization and pattern formation (Section III), or symbolic dynamics (Section IV), will show that such a distinction might in fact be irrelevant.

B. The debated questions

The debate itself stands at different levels:

— it might concern *computational techniques*, for instance discrete numerical schemes used to implement continuous equations, or continuous limits replacing an exact discrete formula by an approximate but tractable one;

Bilinear Pairings in Cryptography

Master thesis
#603

by

Dennis Meffert
<d.meffert@student.science.ru.nl>

at

Radboud Universiteit Nijmegen
Computing Science Department
Toernooiveld 1
6525 ED Nijmegen
The Netherlands

supervised by

dr. W. Bosma
dr. D.C. van Leijenhorst

May 24, 2009

Side Channel Attack on GPUs

Saoni Mukherjee, Chao Luo, Colleen Finnegan, Yunsi Fei, David Kaeli
Dept. of Electrical and Computer Engineering
Northeastern University
Boston, MA

I. Introduction

Graphic Processing Units (GPUs) have evolved from accelerators for processing graphics and generating high quality games to a platform for general purpose computing. GPUs can accelerate a range of applications including security, pattern matching, business analytics and medical diagnostics. The growing demands of computationally-intensive applications such as cryptography, and the availability of inexpensive many-core architectures, has prompted the security community to consider how best to leverage these accelerators.

A side channel attack (SCA) exploits the physical implementation of a cryptographic system, rather than the inherent theoretical weaknesses of the algorithm itself, they attempt to identify the secret key and crack the cryptosystem. The most widely known SCA techniques include Differential Power Analysis (DPA) and Correlational Power Analysis (CPA). They both target the correlation between intermediate results produced by a cryptographic algorithm and power consumption values.

In this paper we discuss a way to measure power on a GPU and map the result with simulated power measurements while running AES-128 on the GPU. We also discuss our plan on attacking the system through the power metrics to produce the secret information that includes the plain text and the encryption key.

II. Advanced Encryption Standard

The Advanced Encryption Standard (AES) has been adopted by the US government to encrypt data in applications ranging from personal to highly confidential domains [?]. In this work we consider execution of the AES algorithm developed in NVIDIA's CUDA, and run on a NVIDIA Kepler GPU [?], [?], [?].

AES has a fixed block size of 128 bits. The key size can vary between 128, 192 and 256 bits. A block is the unit of plain text that the algorithm takes as input and uses to produce the corresponding n-bit cipher text. Text that is longer than a block are divided into multiple blocks, padding the last chunk, and encrypting each block separately. The AES algorithm is comprised of many rounds that ultimately turn plain text into cipher text. Each round has multiple processing steps that include AddRoundKey, SubBytes, ShiftRows and MixColumns. Key bits must be expanded using a precise key expansion schedule.

III. Differential Power Analysis

Differential power analysis (DPA) is an advanced side channel attack, which allows an attacker to extract the secret key of a cryptographic system by statistically analyzing power traces collected from multiple cryptographic operations [?]. DPA exploits the correlation of power consumption and the intermediate values of the cryptographic operation, which is dependent on the secret key. The power traces are divided into two sets, based on the intermediate values computed from a secret key candidate. Then the average traces for both sets are computed, and the difference of means (DOM) is computed by subtracting one average from another. The correct key candidate will show the maximum value DOM. In an AES attack, the last round's SubBytes operation is targeted, since this operation is a byte independent operation. Using a long secret key (128, 192 or 256 bits) will involve a brute-force byte-by-byte attack with key candidates. We have previously analyzed power traces using DPA collected on a GPU [?].

IV. Measurements

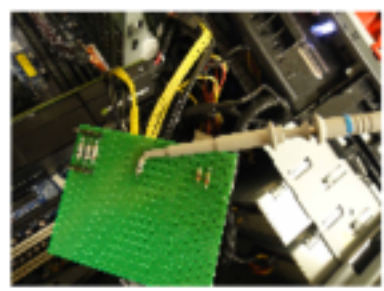


Fig. 1: Setup for collecting traces from a GPU.

Our implementation of AES-128 developed in CUDA has been tested both on an Nvidia GTX 480 and Tesla C2070, running with Ubuntu 14.04.1 on a AMD-64 desktop. We us a LeCory waverunner 640zi oscillascope to obtain power measurements. Power traces are captured by inserting a small resistor (0.1 ohm) in series with the GPU card's external power supply line (multiple power lines are merged into one). The setup shown is shown in Figure 1. The voltage drop across the resistor is recorded when the AES operation is being performed on the GPU, as shown in Figure 2. We have also simulated the results of running AES-128 with GPUWattch

Processor Architecture

2015.04.02

NII51002

Subscribe Send Feedback

This chapter describes the hardware structure of the Nios II processor, including a discussion of all the functional units of the Nios II architecture and the fundamentals of the Nios II processor hardware implementation.

The Nios II architecture describes an instruction set architecture (ISA). The ISA in turn necessitates a set of functional units that implement the instructions. A Nios II processor core is a hardware design that implements the Nios II instruction set and supports the functional units described in this document. The processor core does not include peripherals or the connection logic to the outside world. It includes only the circuits required to implement the Nios II architecture.

The Nios II architecture defines the following functional units:

- Register file
- Arithmetic logic unit (ALU)
- Interface to custom instruction logic
- Exception controller
- Internal or external interrupt controller
- Instruction bus
- Data bus
- Memory management unit (MMU)
- Memory protection unit (MPU)
- Instruction and data cache memories
- Tightly-coupled memory interfaces for instructions and data
- JTAG debug module

© 2015 Altera Corporation. All rights reserved. ALTERA, ARRIA, CYCLONE, ENPIRION, MAX, MEGACORE, NIOS, QUARTUS and STRATIX words and logos are trademarks of Altera Corporation and registered in the U.S. Patent and Trademark Office and in other countries. All other words and logos identified as trademarks or service marks are the property of their respective holders as described at www.altera.com/common/legal.html. Altera warrants performance of its semiconductor products to current specifications in accordance with Altera's standard warranty, but reserves the right to make changes to any products and services at any time without notice. Altera assumes no responsibility or liability arising out of the application or use of any information, product, or service described herein except as expressly agreed to in writing by Altera. Altera customers are advised to obtain the latest version of device specifications before relying on any published information and before placing orders for products or services.

ISO 9001:2008 Registered

101 Innovation Drive, San Jose, CA 95134

Against the mainstream: Nazi privatization in 1930s Germany

Germà Bel*

Universitat de Barcelona i ppre-IREA

Contact data:
Germà Bel
Ppre-IREA
Departament de Política Econòmica i EEM. Torre 6, planta 3
Facultat d'Econòmiques – UB
Avd. Diagonal 690
08034 Barcelona – SPAIN
Tel: 34.93.4021946 e-mail: gbel@ub.edu
http://www.germabel.cat

* This research project has received financial help from the Fundación Rafael del Pino, and from the Spanish Ministry of Science and Technology under the Project BEC2003-01679. Much of the work on this paper was done while I was visiting scholar at Harvard University. Preliminary versions of the paper have been presented at Georgetown University. Comments and suggestions from Xavier Coller, Jost Dülffer and Luis Quiroga and an anonymous referee have been useful. I am fully responsible for any remaining errors.

NUCLEAR BAN *DAILY*

Reaching Critical Will

31 March 2017
Vol. 1, No. 5

IN THIS ISSUE

1 | Editorial

2 | "Modernization" violates every likely prohibition in a ban treaty

3 | News in brief

5 | Today's schedule

6 | Side event: Positive obligations in a treaty to prohibit nuclear weapons

7 | The nuclear ban treaty and general and complete disarmament

8 | Women's march to ban the bomb

Nuclear Ban Daily is produced by Reaching Critical Will, the disarmament programme of the Women's International League for Peace and Freedom (WILPF) during meetings related to the UN conference to negotiate a legally binding instrument to prohibit nuclear weapons, leading to their elimination, taking place 27-31 March and 15 June-7 July 2017. The views expressed in this publication are not necessarily those of WILPF.

Editor: Rey Acheson
info@reachingcriticalwill.org

PATHWAYS TO THE BAN AND BEYOND

Rey Acheson | Reaching Critical Will, Women's International League for Peace and Freedom

On Wednesday afternoon, states participating in the conference to prohibit nuclear weapons found themselves ahead of schedule, so the President suggested they engage in an interactive dialogue with experts on some of the issues discussed so far. Thursday's conversation amongst states, civil society, and the ICRC provided a dynamic space in which to consider several of the key issues upon which there are differing views.

The format seemed extremely useful to allow thoughtful deliberation and exchanges, which will hopefully lead to increasing convergence in the months ahead. It also offered a useful example of how the United Nations could and should operate in terms of open, fluid conversation amonst states, international organisations, academics, and non-governmental organisations. The pursuit of a treaty banning nuclear weapons has been a joint effort between states and the International Campaign to Abolish Nuclear Weapons, so it feels natural for civil society to be engaging with states in discussing the elements of the future instrument.

While some points of divergence remain, it does seem clear that the elements of this instrument are really about pathways: closing off the pathways to develop, retain, or support nuclear weapons; and opening pathways for disarmament.

The nuclear weapon ban treaty is a categorical rejection of nuclear weapons. Its overarching objective is to help facilitate the elimination of nuclear weapons. This means it needs to set out prohibitions and obligations that stigmatise nuclear weapons such that doctrines of "nuclear deterrence" are no longer legally, politically, and socially sustainable; affect the economic incentives for nuclear weapon production and maintenance; and provide legal prohibitions of any activity that supports the existence of nuclear weapons.

At the same time, as several states and civil society presenters pointed out on Thursday, this treaty can and should be seen as part of the larger architecture of general and complete disarmament, and of peace, security, and human rights more broadly. Essentially all supporters of the ban treaty have articulated that this treaty is not an end itself, but a tool to advance peace, justice, and the prevention of humanitarian and environmental harm. In this sense, it is a disarmament treaty—an instrument that should be crafted with an eye on its objective of being a useful mechanism to help achieve and maintain a nuclear weapon free world.

Getting there requires creativity, especially when the nine states that possess nuclear weapons have exhibited no good faith commitment to nuclear disarmament, and, quite the opposite, are investing economically, politically, and culturally in the reinvigoration of the nuclear arms race. Creating a pathway to disarmament in this environment may appear impossible, but it is not.

Getting to the point where we are now may have seemed impossible to some not that long ago. Yet here we are. Agreeing to negotiate a prohibition treaty is, as the Brazilian delegation said today, a breakthrough. It is nothing more than a lack of imagination to believe that changing the status quo is impossible. Change is possible, and it is necessary, but we have to work for it. We have to take risks and be bold.

It was clear from the dialogue on Thursday, and from other sessions during the past week, that some states may be constraining themselves to existing frameworks, methods of work, and understandings about the world. It might be useful for us all to consider how to get to where we are now, what changes were required to see 123 states voting in favour of a resolution in the

continued on next page

Nordic Journal of Computing

On the Expressive Power of Polyadic Synchronisation in π-calculus*

Marco Carbone
BRICS[†]
University of Aarhus, Department of Computer Science
Ny Munkegade, building 540, 8000 Aarhus C, Denmark
carbone@brics.dk

Sergio Maffeis[‡]
Imperial College
University of London, Department of Computing
Huxley Building, 180 Queen's Gate, London SW7 2BZ, UK
maffeis@doc.ic.ac.uk

Abstract. We extend the π-calculus with *polyadic synchronisation*, a generalisation of the communication mechanism which allows channel names to be composite. We show that this operator embeds nicely in the theory of π-calculus, we suggest that it permits divergence-free encodings of distributed calculi, and we show that a limited form of polyadic synchronisation can be encoded weakly in π-calculus. After showing that matching cannot be derived in π-calculus, we compare the expressivity of polyadic synchronisation, mixed choice and matching. In particular we show that the degree of synchronisation of a language increases its expressive power by means of a separation result in the style of Palamidessi's result for mixed choice.

CR Classification: F.1.2. Models of Computation. Parallelism and Concurrency.

Key words: π-calculus, expressivity, matching, polyadic synchronisation, distributed systems

1. Introduction

Process calculi provide a useful framework in which to reason about the theory of concurrent and distributed systems. They are praised both for great simplicity and expressiveness. The π-calculus of Milner et al. [1992] is a terse and powerful language which describes the behaviour of concurrent systems, and is endowed with a rich body of theoretical results. However, evidence has been accumulated which suggests that it is inadequate to express certain

*This is a revised and extended version of a paper appeared in the *Proceedings of the 9th International Workshop on Expressiveness in Concurrency*, volume 68 issue 2, of *Electronic Notes in Theoretical Computer Science*, Elsevier Science, August 2002.

[†]Basic Research in Computer Science (www.brics.dk), funded by the Danish National Research Foundation.

[‡]Supported by a research grant by Microsoft Research, Cambridge, UK.

Received ?. Revised ?.

Private Prosecutions

Last Update: July 2014

Contents

Overview of the Power to Take Over Private Prosecutions under the DPP Act 1
Considerations in Deciding whether to Take Over a Private Prosecution 1
Views of the Private Prosecutor 1
Costs if the CDPP Takes Over the Prosecution 2

Overview of the Power to Take Over Private Prosecutions under the DPP Act

1. Section 9(5) of the DPP Act empowers the Director to take over a summary or committal proceeding instituted by another. Having taken over the proceedings the Director may continue it as the informant or decline to carry it on further.

2. The power under section 9(5) has been delegated pursuant to section 31(1) to two Deputy Directors; Graeme Davidson and James Carter.

3. If representations are received from either the private prosecutor or the defendant in a private prosecution that the Director takes over the private prosecution the matter must be referred to the relevant Practice Group Leader.

Considerations in Deciding whether to Take Over a Private Prosecution

4. Paragraphs 4.7 to 4.13 of the Prosecution Policy of the Commonwealth set out the general considerations involved in determining whether it would be appropriate to take over a private prosecution. The Prosecution Policy of the Commonwealth provides that a private prosecutor should retain the conduct of the prosecution unless one or more of the following considerations apply:

- That there is insufficient evidence to justify the continuation of the prosecution;
- There are reasonable grounds for suspecting that the decision to prosecute was actuated by improper personal or other motives or that it would be an abuse of process to allow the prosecution to remain under the control of the private prosecutor;
- To proceed with the prosecution would be contrary to the public interest; or
- That it would not be in the interests of justice for the prosecution to remain under the control of the private prosecutor.

Views of the Private Prosecutor

5. If the CDPP is requested by a defendant to take over and discontinue a prosecution prosecuted by a private prosecutor, the CDPP should inform the private prosecutor of the request and ask the private prosecutor to provide the CDPP with any evidence the private prosecutor has in relation to the offence. The private prosecutor should also be asked to provide the CDPP with his/her views on the possibility of the CDPP taking over the prosecution.

Non-commutative Geometry, the Bohm Interpretation and the Mind-Matter Relationship[*].

B. J. Hiley

Theoretical Physics Research Unit, Birkbeck, University of London, Malet Street, London WC1E 7HX.

b.hiley@bbk.ac.uk www.bbk.ac.uk/tpru

Abstract.

It is argued that in order to address the mind/matter relationship, we will have to radically change the conceptual structure normally assumed in physics. Rather than fields and/or particles-in-interaction described in the traditional Cartesian order based a local evolution in spacetime, we need to introduce a more general notion of process described by a non-commutative algebra. This will have radical implications for both for physical processes and for geometry. By showing how the Bohm interpretation of quantum mechanics can be understood within a non-commutative structure, we can give a much clearer meaning to the implicate order introduced by Bohm. It is through this implicate order that mind and matter can be seen as different aspects of the same general process.

1. Introduction.

The aim of this talk is provide a general framework in which the relation of ordinary matter to ordinary mind can be discussed[1]. I will not address any details concerning the structure of the complex of neurons or of the electro-chemical processes occurring in the brain, vital though these details are. Rather I will try to provide a general framework in which we can eventually explain how the physical-chemical-electrical properties of the brain can give rise to thoughts, feelings and ultimately consciousness.

I do not believe that today's physics is rich enough to handle these questions and it will be necessary to develop new concepts before we can really begin to explore this relationship adequately. It has been argued that classical physics will provide all the answers we need. I do not share this position. Nor does Stapp (1993) who writes "Classical physics strives to exclude the observer from physics and succeeds. On the other hand quantum mechanics strives to exclude the observer and fails". The first part of this quotation is undoubtedly correct and therefore classical physics excludes the very thing that we are hoping to understand.

On the other hand I do not share Stapp's belief that quantum mechanics already contains sufficient structure to answer the deep questions. My position here does not stem only from my study of the Bohm interpretation (Bohm and Hiley 1987 and 1993). It also

---

[*] To appear in Proc. CASYS'2000, Liege, Belgium, Aug. 7-12, 2000.

[1] By 'ordinary mind' I specifically exclude the so-called 'paranormal'.

Programming Telepathy: Implementing Quantum Non-locality Games

Anya Tafliovich, Eric C.R. Hehner

[1]University of Toronto, Toronto ON M5S 3G4, Canada

{anya,hehner}@cs.toronto.edu

Abstract. *Quantum pseudo-telepathy is an intriguing phenomenon which results from the application of quantum information theory to communication complexity. To demonstrate this phenomenon researchers in the field of quantum communication complexity devised a number of quantum non-locality games. The setting of these games is as follows: the players are separated so that no communication between them is possible and are given a certain computational task. When the players have access to a quantum resource called entanglement, they can accomplish the task: something that is impossible in a classical setting. To an observer who is unfamiliar with the laws of quantum mechanics it seems that the players employ some sort of telepathy; that is, they somehow exchange information without sharing a communication channel.*

This paper provides a formal framework for specifying, implementing, and analyzing quantum non-locality games.

1. Introduction

The work develops a formal framework for specifying, implementing, and analyzing quantum pseudo-telepathy: an intriguing phenomenon which manifests itself when quantum information theory is applied to communication complexity. To demonstrate this phenomenon researchers in the field of quantum communication complexity devised a number of quantum non-locality games. The setting of these games is as follows: the players are separated so that no communication between them is possible and are given a certain computational task. When the players have access to a quantum resource called entanglement, they can accomplish the task: something that is impossible in a classical setting. To an observer who is unfamiliar with the laws of quantum mechanics it seems that the players employ some sort of telepathy; that is, they somehow exchange information without sharing a communication channel.

Quantum pseudo-telepathy, and quantum non-locality in general, are perhaps the most non-classical and the least understood aspects of quantum information processing. Every effort is made to gain information about the power of these phenomena. Quantum non-locality games in particular have been extensively used to prove separations between quantum and classical communication complexity. The need for a good framework for formal analysis of quantum non-locality is evident.

Weak Curves In Elliptic Curve Cryptography

Peter Novotney

March 2010

Abstract

Certain choices of elliptic curves and/or underlying fields reduce the security of an elliptical curve cryptosystem by reducing the difficulty of the ECDLP for that curve. In this paper I describe some properties of an elliptical curve that reduce the security in this manner, as well as a discussion of the attacks that cause these weaknesses. Specifically the Pohlig-Heilman attack and Smart's attack against curves with a Trace of Frobenius of 1. Finally one of the recommended NIST curves is analyzed to see how resistant is would be to these attacks.

1 Elliptic Curves

First a brief refresh on the key points of elliptic curves, for more info see [Han04] [Sil86] [Ste08]. In its more general form, an Elliptic Curve is a curve defined by an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

over some field F. In this case $E(F)$ defines a set of points that satisfy the elliptic equation in the field F. In notation $E(F) = \{(x, y) \in F^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$.
However, if the characteristic of the field is > 3 [Han04] then we can simplify the curve to

$$y^2 = x^3 + ax + b$$

and the set $E(F)$ becomes $E(F) = \{(x, y) \in F^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$.

NP-complete Problems and Physical Reality

Scott Aaronson*

Abstract

Can NP-complete problems be solved efficiently in the physical universe? I survey proposals including soap bubbles, protein folding, quantum computing, quantum advice, quantum adiabatic algorithms, quantum-mechanical nonlinearities, hidden variables, relativistic time dilation, analog computing, Malament-Hogarth spacetimes, quantum gravity, closed timelike curves, and "anthropic computing." The section on soap bubbles even includes some "experimental" results. While I do not believe that any of the proposals will let us solve NP-complete problems efficiently, I argue that by studying them, we can learn something not only about computation but also about physics.

1 Introduction

> "Let a computer smear—with the right kind of quantum randomness—and you create, in effect, a 'parallel' machine with an astronomical number of processors ... All you have to do is be sure that when you collapse the system, you choose the version that happened to find the needle in the mathematical haystack."
>
> —From *Quarantine* [31], a 1992 science-fiction novel by Greg Egan

If I had to debate the science writer John Horgan's claim that basic science is coming to an end [48], my argument would lean heavily on one fact: *it has been only a decade since we learned that quantum computers could factor integers in polynomial time.* In my (unbiased) opinion, the showdown that quantum computing has forced—between our deepest intuitions about computers on the one hand, and our best-confirmed theory of the physical world on the other—constitutes one of the most exciting scientific dramas of our time.

But why did this drama not occur until so recently? Arguably, the main ideas were already in place by the 1960's or even earlier. I do not know the answer to this sociological puzzle, but can suggest two possibilities. First, many computer scientists see the study of "speculative" models of computation as at best a diversion from more serious work; this might explain why the groundbreaking papers of Simon [67] and Bennett et al. [17] were initially rejected from the major theory conferences. And second, many physicists see computational complexity as about as relevant to the mysteries of Nature as dentistry or tax law.

Today, however, it seems clear that there is something to gain from resisting these attitudes. We would do well to ask: *what else* about physics might we have overlooked in thinking about the limits of efficient computation? The goal of this article is to encourage the serious discussion of this question. For concreteness, I will focus on a single sub-question: *can NP-complete problems be solved in polynomial time using the resources of the physical universe?*

I will argue that studying this question can yield new insights, not just about computer science but about physics as well. More controversially, I will also argue that a negative answer might

*Institute for Advanced Study, Princeton, NJ. Email: aaronson@ias.edu. Supported by the NSF.

Proceedings of the Conference on
Promoting Undergraduate Research in Mathematics

The Director's Summer Program at the NSA

Tad White

The Director's Summer Program at the National Security Agency is a research experience aimed at the very best undergraduate mathematics majors in the country. Each summer, we invite a number of exceptional students to participate in a 12-week program in which they collaborate with each other and with Agency researchers to solve classified, mission-critical problems. The inaugural DSP in 1990 hosted eight students; it was successful even beyond the high hopes of the mathematicians who organized it, in ways that would not become apparent for years. The program has grown steadily with its success, and we now invite about two dozen students each year.

The DSP is not intended to be a recruiting program, though dozens of alumni have since joined the NSA as permanent employees. Nor is it intended to be an educational program, though the participants learn a great deal about mathematics and life at the NSA. Rather, the DSP was born of the recognition that the health of mathematics at NSA depends on both the health of the external mathematics community, and on a robust connection between NSA and that community. Obviously, as the nation's largest employer of mathematicians, NSA relies upon the mathematics community to provide a technically strong workforce. However, no matter how skilled our people are, we cannot hope to keep up with the research frontiers in all fields of mathematics. Often, advances which seem unrelated to our current work turn out to provide essential clues to the solutions of our most difficult problems. We rely upon the outside community to help us identify and apply these advances, and we can be successful only if the top mathematicians have a deep understanding of NSA's problem set and mathematical culture.

In the late 1980s, the NSA mathematics community explicitly recognized the importance of fostering a close relationship with the nation's academic mathematics community, and undertook a number of initiatives to reinvigorate this relationship. Richard Shaker, then head of mathematics research at NSA, described a few of these initiatives in an address at the 1992 Joint Mathematics Meetings [1]. In 1987, we invited a hundred mathematicians to come hear ten unclassified talks on research being done at the Agency. We set aside a few million dollars annually to support academic research proposals. (While this figure represents a small fraction of the U. S. government's support to pure mathematics research, it amounts to a large portion of our technology budget.) We established a sabbatical program to allow

Received by the editor February 7, 2007.

©2007 American Mathematical Society

Numerical Simulation of Dynamic Systems VI

Prof. Dr. François E. Cellier
Department of Computer Science
ETH Zurich

March 12, 2013

MUS420/EE367A Lecture 7D: Discrete-Time Lumped Models

Stefan Bilbao and Julius O. Smith III (jos@ccrma.stanford.edu)
Center for Computer Research in Music and Acoustics (CCRMA)
Department of Music, Stanford University
Stanford, California 94305

March 24, 2014

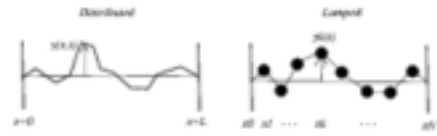
Outline:

- Lumped vs. distributed systems
- Discretization
- Finite Difference Approximation (FDA)
- Von Neumann Analysis
- Stability
- Examples

Lumped vs. Distributed Systems

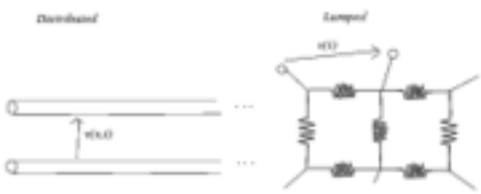
- A lumped system is one in which the dependent variables of interest are a function of time alone. In general, this will mean solving a set of ordinary differential equations (ODEs)
- A *distributed* system is one in which all dependent variables are functions of time *and* one or more spatial variables. In this case, we will be solving partial differential equations (PDEs)

For example, consider the following two systems:



- The first system is a *distributed* system, consisting of an infinitely thin string, supported at both ends; the dependent variable, the vertical position of the string $y(x,t)$ is indexed continuously in both space and time.

- The second system, a series of "beads" connected by massless string segments, constrained to move vertically, can be thought of as a *lumped* system, perhaps an approximation to the continuous string.
- For electrical systems, consider the difference between a lumped RLC network and a transmission line



- The importance of *lumped approximations* to distributed systems will become obvious later, especially for waveguide-based physical modeling, because it enables one to cut computational costs by solving ODEs at a few points, rather than a full PDE (generally much more costly)

Discretization

Problem: Given

- Integro-differential equations (DEs)
- Boundary conditions

Find:

1. Numerical solution for system motion (classical problem), or
2. Real-time *computational model*:
   - Solves DEs with a computational structure
   - Input and control signals effectively "change the boundary conditions"

This course is concerned primarily with the second case, although the first case also arises when verifying acoustic theory or a particular computational model.

JUDGE WOODS

15 CV 02216

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PAUL NUNGESSER,

Plaintiff,

v.

COLUMBIA UNIVERSITY, TRUSTEES OF COLUMBIA UNIVERSITY, LEE C. BOLLINGER, and JON KESSLER,

Defendants.

Civ. Act. No.:

COMPLAINT

JURY DEMANDED

RECEIVED
APR 23 2015
U.S.D.C.S.D.N.Y.
Complaint

Plaintiff Paul Nungesser, by and through his undersigned attorneys Newmark & Milterberg LLP, hereby alleges as follows:

PRELIMINARY STATEMENT

1. This is an action for damages, injunctive relief and declaratory relief against Defendants Columbia University, the Trustees of Columbia University, Columbia University's President Lee C. Bollinger and Columbia University's Visual Arts Professor Jon Kessler (hereinafter sometimes collectively referred to as "Defendants"), for their acts and omissions with regard to Paul Nungesser in violation of both federal and state law which have significantly damaged, if not effectively destroyed Paul Nungesser's college experience, his reputation, his emotional well being and his future career prospects. This case exemplifies the types of student-on-student and teacher-on-student gender based harassment and misconduct that the Supreme Court has held is prohibited by Title IX of the Education Amendments of 1972, 86 Stat. 373, *as amended*, 20 U.S.C. §1681 *et seq.* ("Title IX").

2. Paul Nungesser has been an outstanding and talented student at Columbia University. He thrived in his first two years at Columbia University and then became the victim

Univalent Foundation and Constructive Mathematics

Thierry Coquand

Oberwolfach, November 18, 2014

Univalent Foundation and Constructive Mathematics

Thierry Coquand

Oberwolfach, November 21, 2014

Ordinary Differential Equations and Dynamical Systems

Gerald Teschl

This is a preliminary version of the book ***Ordinary Differential Equations and Dynamical Systems*** published by the American Mathematical Society (AMS). This preliminary version is made available with the permission of the AMS and may not be changed, edited, or reposted at any other website without explicit written permission from the author and the AMS.

Author's preliminary version made available with permission of the publisher, the American Mathematical Society

COURSES TAUGHT IN ENGLISH (MASTER LEVEL)
FACULTY OF PURE AND APPLIED MATHEMATICS
WROCLAW UNIVERSITY OF SCIENCE AND TECHNOLOGY

L	t	lab	p	s

L – Lecture, **t** – Tutorials, **lab** – laboratory, **p** – project, **s** – seminar,

CHS	TSW

CHS – Contact Hours (organized), **TSW** – Total Student Workload (h),

E – Exam, T – Test, CW – Course Work

Winter Semester 2017/2018

Subject/Module	Contact hours/week					CHS	TSW	ECTS	Form of Assessment
	L	t	lab	p	s				
Optimization theory	2	2				60	180	6	E
Agent-based modelling of complex systems	2		2			60	150	5	E
Diploma Seminar					2	30	60	2	T/CW

Summer semester 2017/2018

Subject/Module	Contact hours/week					CHS	TSW	ECTS	Form of Assessment
	L	t	lab	p	s				
Economathematics	2	2				60	150	5	E
Partial differential equations with applications in physics and industry	2	2				60	180	6	E
Life Insurance Models	2	2				60	150	5	E

Optional courses (only 3 courses per semester are usually chosen)

Subject/Module	Contact hours/week					CHS	TSW	ECTS	Form of Assessment
	L	t	lab	p	s				
Financial risk management	2	2				60	150	5	T
Applied Functional analysis	2		2			60	150	5	T
Advanced Topics in Dynamic Games	2	2				60	150	5	T
Risk management in insurance	2			2		60	150	5	T
Insurance models for industry	2		2			60	150	5	T
Nonlinear Methods	2		2			60	150	5	T
Optimal control	2		2			60	150	5	T
Numerical methods in differential equations	2		2			60	150	5	T
Diffusion processes on complex networks	2		2			60	150	5	T
Statistical packages	2		2			60	150	5	T
Queues and Communication Networks	2	2				60	150	5	T
Computational Finance	2		2			60	150	5	T
Introduction to Big Data Analytics	2			2		60	150	5	T
Introduction to applied fluid dynamics	2			2		60	150	5	T
Mathematical Image Processing	2		2			60	150	5	T
Estimation Theory	2		2			60	150	5	T
Perturbation Methods	2		2			60	150	5	T
Analysis of unstructured data	2			2		60	150	5	T

UNCERTAINTY PRINCIPLE, NON-SQUEEZING THEOREM AND THE SYMPLECTIC RIGIDITY

LECTURE FOR THE 1995 DAEWOO WORKSHOP, CHUNGWON, KOREA

YONG-GEUN OH, DEPARTMENT OF MATHEMATICS
UNIVERSITY OF WISCONSIN MADISON, WI 53706

§1. Prologue: Uncertainty principle and non-squeezing theorem.

One of the basic principle in the quantum mechanics is the Heisenberg uncertainty principle. This can be roughly stated as "one can not measure the momentum and the position of a particle precisely at the same time". More precisely, the principle can be written as

$$\triangle q \triangle p \simeq \hbar, \quad \hbar = \text{the Planck constant},$$

where $\triangle q = \langle q - \langle q \rangle \rangle, \triangle p = \langle p - \langle p \rangle \rangle$ are the deviation from the average values $\langle q \rangle$ and $\langle p \rangle$. When a particle is in $\mathbb{R}^3$, then this is replaced by

$$\triangle q_i \triangle p_i \simeq \hbar \tag{1.1}$$

for $i = 1, 2, 3$. A natural question then is to ask what would be the analogue in the classical mechanics. This question involves two tasks in it: First we need to *formulate* what would be the statement and secondly need to *prove* the statement.

To formulate the analogue, we need some digression into the *Hamiltonian formalism* of the classical mechanics.

1.1. Hamiltonian mechanics.

Newtonian mechanics is based on the *Newton's second law of motion*:

$$m\ddot{x} = F(x) \quad x \in \mathbb{R}^3 \tag{1.2}$$

This is a second order ordinary differential equation of x. To determine the motion of a particle, we need two initial conditions

$$\begin{cases} x(0) = x_0 \\ \dot{x}(0) = v_0 \end{cases} \tag{1.3}$$

One can transform (1.2) and (1.3) into a system of first order ODE on $\mathbb{R}^6 = \mathbb{R}^3 \times \mathbb{R}^3$

$$\begin{cases} \dot{q} = p \\ \dot{p} = F(q) \\ q(0) = x_0 \quad p(0) = v_0 \end{cases} \tag{1.4}$$

Supported in part by NSF grant and UW Research Award Grant

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

— Proposal narrative —

Complementary quantum observables and resulting information flows in algorithms and protocols: high-level methods & tool development

Bob Coecke

Oxford University Computing Laboratory
Wolfson Building, Parks Road, OX1 3QD Oxford, UK.
coecke@comlab.ox.ac.uk — +447855298183 (cell) — +441865273839 (fax)

Institution proposal number:

...

BRC topic title:

Quantum information sciences and the future of secure computation

On the Notation of Field Equations of Electrodynamics

André Waser*

Issued: 28.06.2000
Last revision: 28.08.2007

Maxwell's equations are the cornerstone in electrodynamics. Despite the fact that these equations are more than hundred years old, they still are subject to changes in recent publications. To get an impression over the historical development of Maxwell's equations, the equation systems in different notations are summarized.

Introduction

The complete set of the equations of James Clerk MAXWELL[10] are known in electrodynamics since 1865. These have been defined for 20 field variables. Later Oliver HEAVISIDE[11] and William GIBBS[12] have transformed this equations into the today's most used notation with vectors. This has not been happened without „background noise"[47], then at that time many scientists – one of them has been MAXWELL himself – was convinced, that the correct notation for electrodynamics must be possible with quaternions[19] and not with vectors. A century later EINSTEIN introduced Special Relativity and since then it was common to summarize MAXWELL's equations with four-vectors.

The search at magnetic monopoles has not been coming to an end, since DIRAC[48] introduced a symmetric formulation of MAXWELL's equations without using imaginary fields. But in this case the conclusion from Special Theory of Relativity, that the magnetic field originates from relative motion only, can not be hold anymore.

The non-symmetry in MAXWELL's equations of the today's vector notation may have dissatisfied many scientists intuitively. That could be the reason, why they published an extended set of equations. Sometime these extensions have been introduced for specific applications only. This essay summarizes the main different notation forms of MAXWELL's equations.

* André Waser, Hirtli 35, CH-8840 Einsiedeln

copyright © (2000) by André Waser, www.andre-waser.ch

Open-Transactions: Secure Contracts between Untrusted Parties

Chris Odom

chris@opentransactions.org

Abstract

A low-trust notary could replace conventional transaction servers and would allow users to gain access to safe, fast, inexpensive, off-chain transactions with increased functionality. We propose a solution that enables parties to contract with each other without being able to defraud each other, and to issue currencies and to prove all balances, as well as prove which instruments are valid and which transactions have closed, without storing any history except for the last signed receipt. Theft of reserves and counterfeiting are prevented by storing cryptocurrency reserves in multi-signature voting pools consisting of notaries who audit each other in real time and then vote multi-signature on the blockchain to release coins only when authorized by users' signed receipts.

1. Introduction

The Bitcoin blockchain is an ideal medium for issuing currencies and for censorship-resistant, peer-to-peer payments[6]. But the trade-off is that blockchain transactions are slow and expensive compared to using a server. Users also commonly employ server-based systems for added functionality such as market exchange and smart contracts. Unfortunately, servers in use today must be trusted to hold the funds, to accurately maintain their internal ledger, and to faithfully execute the transactions requested by their users. As a result, problems traditionally associated with third party intermediaries have crept into the Bitcoin ecosystem, including reversible transactions, verified accounts, frozen balances, and expropriated funds.

What is needed is a transaction server based on cryptographic proof instead of trust, allowing any willing parties who wish to contract with each other to enjoy the benefits of a server without needing to trust it. In this paper, we propose a solution that demotes transaction servers to mere notaries, only able to countersign contracts that have first been signed by their clients. Since only each client has access to its *own* private key, receipts are unforgeable. Theft of reserves and counterfeiting are prevented by storing bitcoins and colored coins in multi-signature voting pools consisting of notaries who audit each other in real time and then vote multi-signature on the blockchain to release coins only when authorized by users' signed receipts.

2. Transactions

1. Financial Instruments

We define a transaction as a group of operations on contracts capable of objectively proving balances (and changes of balance) between adversarial parties. Open-Transactions implements financial instruments as *Ricardian Contracts*, which are contracts that can be understood by humans as well as manipulated by software[3].

All transactions use the same basic structure: the parties involved sign agreements which are then countersigned by an independent notary server. Furthermore, transactions are irreversible since the receipts are always formed and signed on the client side first, before being notarized by any server. This prevents the notary from falsifying receipts, since it can't forge the client's signature.

This basic structure can be built upon to create many types of financial instruments. Those supported by Open-Transactions include:

- **Transfer.** An atomic movement of funds from one account to a different account, like a bank account-to-account transfer.

Optical models for quantum mechanics

Arnold Neumaier

Fakultät für Mathematik
Universität Wien, Österreich

Lecture given on February 16, 2010 at the

Institut für Theoretische Physik

Universität Giessen, Germany

http://www.mat.univie.ac.at/~neum/papers/physpapers.html#optslides

ABSTRACT

ORBIT: An Optimizing Compiler For Scheme

David Andrew Kranz
Yale University
1988

It has often been assumed that the performance of languages with first-class procedures is necessarily inferior to that of more traditional languages. Both experience and benchmarks appear to support this assumption. This work shows that the performance penalty is only a result of applying conventional compiler technologies to the compilation of higher order languages. These technologies do not adapt well to the situation in which closures of unlimited extent can be created dynamically.

The ORBIT compiler is based on a *continuation-passing model* instead of the traditional procedure call/return. The problem of reducing heap storage is solved using new algorithms for *closure analysis*, allowing many objects to be allocated on a stack or, better still, in machine registers. *Closure packing and hoisting* allow more than one procedure to share an environment without introducing indirection. Move instructions and memory references are reduced by passing arguments in registers and using a dynamic register allocation strategy. Register allocation and code generation are accomplished at the same time, with environment pointers being treated as variables. Environment pointers are kept in a *lazy display*, being brought into registers and cached when needed. The interaction of this strategy with the closure analysis also allows many optimizations based on type information to be performed.

Benchmarks are presented to show that, using these new techniques, the performance of programs written in higher order languages almost equals that of programs written in Pascal in both space and time. Thus the greater expressive power of higher order languages and debugging ease of traditional LISP systems need not be sacrificed to attain good performance.

ORDERS APPROVED AT THE PRIVY COUNCIL HELD BY THE QUEEN AT BUCKINGHAM PALACE ON 19TH MARCH 2015

COUNSELLORS PRESENT

The Rt Hon Theresa May (Acting Lord President)
The Rt Hon Oliver Letwin
The Rt Hon Patrick McLoughlin
The Rt Hon Steve Webb

Privy Counsellors	Two Orders recording that The Rt Hon Dame Eleanor King and The Rt Hon Lord Malcolm were sworn as Members of Her Majesty's Most Honourable Privy Council.
	Four Orders recording that The Rt Hon Sir David Bean, The Rt Hon Sir Ian Burnett, The Rt Hon Sir John Gillen and The Rt Hon Sir Philip Sales made affirmation as Members of Her Majesty's Most Honourable Privy Council.
	Eleven Orders appointing David Evennett MP, Mark Field MP, Baroness Garden of Frognal, Sir Edward Garnier MP, David Heath MP, Charles Hendry MP, Dr Julian Lewis MP, Fiona Mactaggart MP, Anne Milton MP, Baroness Northover and Keith Simpson MP as Members of Her Majesty's Most Honourable Privy Council.
Proclamations	Four Proclamations:—
	1. determining the specifications and design for five pound coins celebrating the second child of the Duke and Duchess of Cambridge;
	2. determining the specifications and design for five pound coins commemorating the bicentenary of the Battle of Waterloo;
	3. determining the specifications and design for a new series of one pound coins;

BeinhockerFM.qxd 3/14/06 1:46 PM Page iii

The Origin of Wealth

EVOLUTION, COMPLEXITY, AND THE RADICAL REMAKING OF ECONOMICS

Eric D. Beinhocker

Harvard Business School Press
Boston, Massachusetts

On the Notation of MAXWELL's Field Equations

André Wuser*

Issued: 28.06.2000
Last revision: -

Maxwell's equations are the cornerstone in electrodynamics. Despite the fact that this equations are more than hundred years old, they still are subject to changes in content or notation. To get an impression over the historical development of Maxwell's equations, the equation systems in different notations are summarized.

Introduction

The complete set of the equations of James Clerk MAXWELL[15] are known in electrodynamics since 1865. These have been defined for 20 field variables. Later Oliver HEAVISIDE[11] and William GIBBS[10] have transformed this equations into the today's most used notation with vectors. This has not been happened without ‚background noise'[3], then at that time many scientists – one of them has been MAXWELL himself – was convinced, that the correct notation for electrodynamics must be possible with quaternions[8] and not with vectors. A century later EINSTEIN introduced Special Relativity and since then it was common to summarize MAXWELL's equations with four-vectors.

The search at magnetic monopoles has not been coming to an end, since DIRAC[9] introduced a symmetric formulation of MAXWELL's equations without using imaginary fields. But in this case the conclusion from the Special Theory of Relativity, that the magnetic field originates from relative motion only, can not be hold anymore.

The non-symmetry in MAXWELL's equations of the today's vector notation may have disturbed many scientists intuitively, what could be the reason, that they published an extended set of equations, which they sometime introduced for different applications. This essay summarizes the main different notation forms of MAXWELL's equations.

* André Wuser, Birchli 35, CH-8840 Einsiedeln; andre.wuser@aw-verlag.ch

copyright © (2000) by AW-Verlag, www.aw-verlag.ch

Orthogonal polynomials

We start with

Definition 1. *A sequence of polynomials $\{p_n(x)\}_{n=0}^{\infty}$ with degree$[p_n(x)] = n$ for each n is called orthogonal with respect to the weight function $w(x)$ on the interval (a,b) with $a < b$ if*

$$\int_a^b w(x) p_m(x) p_n(x)\,dx = h_n\,\delta_{mn} \quad \text{with} \quad \delta_{mn} := \begin{cases} 0, & m \neq n \\ 1, & m = n. \end{cases}$$

The weight function $w(x)$ should be continuous and positive on (a,b) such that the moments

$$\mu_n := \int_a^b w(x)\,x^n\,dx, \quad n = 0, 1, 2, \ldots$$

exist. Then the integral

$$\langle f,\, g\rangle := \int_a^b w(x) f(x) g(x)\,dx$$

denotes an inner product of the polynomials f and g. The interval (a,b) is called the interval of orthogonality. This interval needs not to be finite.

If $h_n = 1$ for each $n \in \{0, 1, 2, \ldots\}$ the sequence of polynomials is called orthonormal, and if

$$p_n(x) = k_n x^n + \text{ lower order terms} \quad \text{with} \quad k_n = 1$$

for each $n \in \{0, 1, 2, \ldots\}$ the polynomials are called monic.

Example. As an example we take $w(x) = 1$ and $(a,b) = (0,1)$. Using the Gram-Schmidt process the orthogonal polynomials can be constructed as follows. Start with the sequence $\{1, x, x^2, \ldots\}$. Choose $p_0(x) = 1$. Then we have

$$p_1(x) = x - \frac{\langle x,\, p_0(x)\rangle}{\langle p_0(x),\, p_0(x)\rangle}\, p_0(x) = x - \frac{\langle x,\, 1\rangle}{\langle 1,\, 1\rangle} = x - \frac{1}{2},$$

since

$$\langle 1,\, 1\rangle = \int_0^1 dx = 1 \quad \text{and} \quad \langle x,\, 1\rangle = \int_0^1 x\,dx = \frac{1}{2}.$$

Further we have

$$\begin{aligned} p_2(x) &= x^2 - \frac{\langle x^2,\, p_0(x)\rangle}{\langle p_0(x),\, p_0(x)\rangle}\, p_0(x) - \frac{\langle x^2,\, p_1(x)\rangle}{\langle p_1(x),\, p_1(x)\rangle}\, p_1(x) \\ &= x^2 - \frac{\langle x^2,\, 1\rangle}{\langle 1,\, 1\rangle} - \frac{\langle x^2,\, x - \frac{1}{2}\rangle}{\langle x - \frac{1}{2},\, x - \frac{1}{2}\rangle}\left(x - \frac{1}{2}\right) = x^2 - \frac{1}{3} - \left(x - \frac{1}{2}\right) = x^2 - x + \frac{1}{6}, \end{aligned}$$

since

$$\langle x^2,\, 1\rangle = \int_0^1 x^2\,dx = \frac{1}{3}, \quad \langle x^2,\, x - \tfrac{1}{2}\rangle = \int_0^1 x^2\left(x - \frac{1}{2}\right)\,dx = \frac{1}{4} - \frac{1}{6} = \frac{1}{12}$$

and

$$\langle x - \tfrac{1}{2},\, x - \tfrac{1}{2}\rangle = \int_0^1 \left(x - \frac{1}{2}\right)^2 dx = \int_0^1 \left(x^2 - x + \frac{1}{4}\right) dx = \frac{1}{3} - \frac{1}{2} + \frac{1}{4} = \frac{1}{12}.$$

The polynomials $p_0(x) = 1$, $p_1(x) = x - \frac{1}{2}$ and $p_2(x) = x^2 - x + \frac{1}{6}$ are the first three monic orthogonal polynomials on the interval $(0,1)$ with respect to the weight function $w(x) = 1$.

Department of Justice

STATEMENT OF

BILL PRIESTAP
ASSISTANT DIRECTOR
COUNTERINTELLIGENCE DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

FOR A HEARING ENTITLED

"ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT ELECTIONS"

PRESENTED

JUNE 21, 2017

ANNALS OF PHYSICS 116, 105–141 (1978)

On Bogoliubov Transformations. II. The General Case*

S. N. M. RUIJSENAARS

Department of Physics, Princeton University, Princeton, New Jersey 08540

Received January 19, 1978

A rigorous treatment of Bogoliubov transformations is presented along the same lines as in a previous paper, which dealt with a special case. As in the previous paper a formulation in terms of unitary resp. pseudo-unitary operators is used, corresponding to the CAR resp. the CCR. This leads to simple proofs of well-known necessary and sufficient conditions for the transformation to be unitarily implementable in Fock space. The normal form of the implementing operator Φ is studied. It is proved that on the subspace of algebraic vectors Φ equals a strongly convergent infinite series of Wick monomials that sums up to a simple exponential expression. A connection between the fermion and boson transformations studied in the previous paper is established. The analogous correspondence in the general case only holds true if the (pseudo) unitary operator equals its own inverse.

1. Introduction

In a previous paper [1] we studied the special type of Bogoliubov transformation that occurs in the treatment of systems of relativistic, charged particles. It is the purpose of the present paper to consider general Bogoliubov transformations in a similar fashion. In particular, as in [1], our main objective is to study the normal form of the unitary operator on Fock space that implements the transformation.

In Section 2 we collect some results on second quantization we have occasion to use. The two definitions of Bogoliubov transformation that can be found in the literature are discussed and their relation is established. In Section 3 we present our own approach in terms of unitary resp. pseudo-unitary operators that commute with the "charge conjugation operator," corresponding to the canonical anticommutation relations (CAR) resp. canonical commutation relations (CCR). This approach and our notation are inspired by the way Bogoliubov transformations occur in theories of relativistic, neutral particles in external fields [2]. At first sight it may seem somewhat artificial to readers who are only familiar with applications of Bogoliubov transformations to nonrelativistic theories. However, it will be seen that it leads to an easy proof of a well-known necessary condition for the transformation to be unitarily implement-

* Work supported in part by NSF Contract MPS 74-22844

0003-4916/78/1161-0105$05.00/0
Copyright © 1978 by Academic Press, Inc.
All rights of reproduction in any form reserved.

A Systematic Analysis of the Juniper Dual EC Incident

Stephen Checkoway[*], Jacob Maskiewicz[†], Christina Garman[‡], Joshua Fried[§], Shaanan Cohney[§], Matthew Green[‡], Nadia Heninger[§], Ralf-Philipp Weinmann[¶], Eric Rescorla[†], Hovav Shacham[†]

[*]University of Illinois at Chicago, [†]University of California, San Diego, [‡]Johns Hopkins University, [§]University of Pennsylvania, [¶]Comsecuris

ABSTRACT

In December 2015, Juniper Networks announced multiple security vulnerabilities stemming from unauthorized code in ScreenOS, the operating system for their NetScreen VPN routers. The more sophisticated of these vulnerabilities was a passive VPN decryption capability, enabled by a change to one of the elliptic curve points used by the Dual EC pseudorandom number generator.

In this paper, we describe the results of a full independent analysis of the ScreenOS randomness and VPN key establishment protocol subsystems, which we carried out in response to this incident. While Dual EC is known to be insecure against an attacker who can choose the elliptic curve parameters, Juniper had claimed in 2013 that ScreenOS included countermeasures against this type of attack. We find that, contrary to Juniper's public statements, the ScreenOS VPN implementation has been vulnerable since 2008 to passive exploitation by an attacker who selects the Dual EC curve point. This vulnerability arises due to apparent flaws in Juniper's countermeasures as well as a cluster of changes that were all introduced concurrently with the inclusion of Dual EC in a single 2008 release. We demonstrate the vulnerability on a real NetScreen device by modifying the firmware to install our own parameters, and we show that it is possible to passively decrypt an individual VPN session in isolation without observing any other network traffic. We investigate the possibility of passively fingerprinting ScreenOS implementations in the wild. This incident is an important example of how guidelines for random number generation, engineering, and validation can fail in practice.

1. INTRODUCTION

In his statement for the record before the Senate Armed Services Committee on February 9, 2016, James Clapper, the U.S. Director of National Intelligence, illustrated the "worldwide threat assessment of the U.S. intelligence community" with an example of vulnerable infrastructure:

> A major U.S. network equipment manufacturer acknowledged last December that someone repeatedly gained access to its network to change source code in order to make its products' default encryption breakable. The intruders also introduced a default password to enable undetected access to some target networks worldwide. [10]

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
CCS '16 October 24–28, 2016, Vienna, Austria
© 2016 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ISBN 978-1-4503-4139-4/16/10…$15.00
DOI: http://dx.doi.org/10.1145/2976749.2978395

The "network equipment manufacturer" was Juniper Networks; it had disclosed the two issues in a security bulletin on December 17, 2015 [23], and released patched versions of ScreenOS, the operating system powering the affected NetScreen devices.

Immediately following Juniper's advisory, security researchers around the world — including our team — began examining the ScreenOS firmware to find the vulnerabilities Juniper claimed to have patched. They found that the change that, per Clapper, rendered ScreenOS encryption "breakable" did nothing but replace a few embedded constants.

In this paper, we explain how these changed constants may have allowed whoever introduced them to decrypt passively recorded VPN traffic to affected devices. The 2012 change took advantage of Juniper's 2008 overhaul of the ScreenOS randomness which introduced the NSA-designed Dual EC random number generator, and included Juniper-selected constants which we are unable to verify are secure. Juniper's December 2015 patch restored these original constants.

Our methods include forensic reverse engineering of dozens of ScreenOS firmware revisions stretching back nearly a decade; experimental testing on NetScreen hardware; and Internet measurement studies.

Juniper's NetScreen devices were FIPS certified, and the affected code implemented the standard IPsec protocol suite. Our findings thus have implications for many of the stakeholders in the development of cryptographic products, including protocol designers, implementers, code reviewers, and policymakers.

Pseudorandom number generators. Random number generation is critical to the implementation of cryptographic systems. Random numbers are used for a variety of purposes, including generation of nonces and cryptographic keys. Because generating a sufficient quantity of true random numbers via physical means is hard, cryptographic systems typically include deterministic *pseudorandom number generators* (PRNGs) which expand a small amount of secret internal state into a stream of values which are intended to be indistinguishable from true randomness.

Historically, random number generators have been a major source of vulnerabilities [8, 19, 22, 28, 45]. This is because an attacker who is able to predict the output of a PRNG will often be able to break any protocol implementation dependent on it. For instance, they may be able to predict any cryptographic keys (which should remain secret) or nonces (which should often remain unpredictable). Past PRNG failures have resulted from a failure to seed with sufficiently random data [19, 22] or from algorithms which are not secure, in

Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

KEN THOMPSON

INTRODUCTION

I thank the ACM for this award. I can't help but feel that I am receiving this honor for timing and serendipity as much as technical merit. UNIX[*] swept into popularity with an industry-wide change from central mainframes to autonomous minis. I suspect that Daniel Bobrow [1] would be here instead of me if he could not afford a PDP-10 and had had to "settle" for a PDP-11. Moreover, the current state of UNIX is the result of the labors of a large number of people.

There is an old adage, "Dance with the one that brought you," which means that I should talk about UNIX. I have not worked on mainstream UNIX in many years, yet I continue to get undeserved credit for the work of others. Therefore, I am not going to talk about UNIX, but I want to thank everyone who has contributed.

That brings me to Dennie Ritchie. Our collaboration has been a thing of beauty. In the ten years that we have worked together, I can recall only one case of miscommunication of work. On that occasion, I discovered that we both had written the same 20-line assembly language program. I compared the sources and was astounded to find that they matched character-for-character. The result of our work together has been far greater than the work that we each contributed.

I am a programmer. On my 1040 form, that is what I put down as my occupation. As a programmer, I write programs. I would like to present to you the cutest program I ever wrote. I will do this in three stages and try to bring it together at the end.

STAGE I

In college, before video games, we would amuse ourselves by posing programming exercises. One of the favorites was to write the shortest self-reproducing program. Since this is an exercise divorced from reality, the usual vehicle was FORTRAN. Actually, FORTRAN was the language of choice for the same reason that three-legged races are popular.

More precisely stated, the problem is to write a source program that, when compiled and executed, will produce as output an exact copy of its source. If you have never done this, I urge you to try it on your own. The discovery of how to do it is a revelation that far surpasses any insight obtained by being told how to do it. The part about "shortest" was just an incentive to demonstrate skill and determine a winner.

Figure 1 shows a self-reproducing program in the C[2] programming language. (The purist will note that the program is not precisely a self-reproducing program, but will produce a self-reproducing program.) This entry is much too large to win a prize, but it demonstrates the technique and has two important properties that I need to complete my story: 1) This program can be easily written by another program. 2) This program can contain an arbitrary amount of excess baggage that will be reproduced along with the main algorithm. In the example, even the comment is reproduced.

[*] UNIX is a trademark of AT&T Bell Laboratories.

© 1984 0001-0782/84/0800-0761 50c

Introduction to Spectral Theory of Schrödinger Operators

A. Pankov
Department of Mathematics
Vinnitsa State Pedagogical University
21100 Vinnitsa
Ukraine
E-mail: pankov@e-math.ams.org

Computing 76, 325–352 (2006)
Digital Object Identifier (DOI) 10.1007/s00607-005-0136-0

Computing
Printed in Austria

Totally Discrete Explicit and Semi-implicit Euler Methods for a Blow-up Problem in Several Space Dimensions

Pablo Groisman, Universidad de Buenos Aires

Received: February 8, 2005; revised: July 7, 2005
Published online: December 5, 2005
© Springer-Verlag 2005

Abstract

The equation $u_t = \Delta u + u^p$ with homogeneous Dirichlet boundary conditions has solutions with blow-up if $p > 1$. An adaptive time-step procedure is given to reproduce the asymptotic behavior of the solutions in the numerical approximations. We prove that the numerical methods reproduce the blow-up cases, the blow-up rate and the blow-up time. We also localize the numerical blow-up set.

Subject Classification: 65M60, 65M20, 35K60, 35B40.

Keywords: Blow-up, adaptive numerical scheme, asymptotic behavior.

1. Introduction

We study the behavior of an adaptive time step procedure for the following parabolic problem

$$\begin{cases} u_t = \Delta u + u^p & \text{in } \Omega \times [0, T), \\ u = 0 & \text{on } \partial\Omega \times [0, T), \\ u(x, 0) = u_0(x) > 0 & \text{on } \Omega. \end{cases} \tag{1.1}$$

Here p is superlinear ($p > 1$) in order to have solutions with blow-up. We assume u_0 is regular and $\Omega \subset \mathbb{R}^d$ is a bounded smooth domain in order to guarantee that $u \in C^{2,1}$. A remarkable fact in this problem is that solutions may develop singularities in finite time, no matter how smooth u_0 is. For many differential equations or systems the solutions can become unbounded in finite time (a phenomena that is known as blow-up). Typical examples where this happens are problems involving reaction terms in the equation like (1.1) where a reaction term of power type is present and so the blow-up phenomenon occurs in the sense that there exists a finite time T such that $\lim_{t \to T} \|u(\cdot, t)\|_\infty = +\infty$ if the initial data is large enough (see [23] and references therein). The blow-up set, which is defined as the set composed of points $x \in \Omega$ such that $u(x, t) \to +\infty$ as $t \to T$, is localized in thin regions of Ω, in [26] is proved that the $(d-1)$ dimensional Hausdorff measure of the blow-up set is finite. The blow-up rate at these points is given by $u(x, t) \sim (T - t)^{-\frac{1}{p-1}}$, moreover

80509 LINEAR DIGITAL FILTERING I

PART V: Finite word length effects in digital filters

1) Output noise due to the multiplication roundoff errors.
2) Filter scaling: various scaling norms.
3) Coefficient quantization errors.
4) Various kinds of oscillations.

- What to read for the examination ?:

1) How to scale a digital filter; the basic scaling norms and their differences in practice?
2) How to estimate output noise due to the multiplication roundoff errors?
3) It is very likely that in the examination there is a simple filter which must be scaled (according to some norm) and then the output noise must be estimated.

Please study carefully exercises in Appendix B.

Large Cardinals and Lebesgue Measurability

Time and Quantum Theory: A History and a Prospectus

Tom Pashby

September 26, 2013

1 Introduction

The conventional wisdom regarding the role of time in quantum theory is this: "time is a parameter in quantum mechanics and *not* an operator" (Duncan & Janssen, 2013, p. 216, original emphasis). The reason for this is 'Pauli's theorem,' a collection of results that show that (subject to a mild restriction on the Hamiltonian) conventional quantum mechanics does not permit the definition of a time observable, i.e. a self-adjoint operator canonically conjugate to energy.[1] If one wishes to have time appear as a genuine observable of the theory, then this is obviously a problem, called by some "the problem of time in quantum mechanics" (Hilgevoord & Atkinson, 2011; Olkhovsky, 2011). Hilgevoord's (2005) attempted resolution of the problem rests on his rejection of a particular motivation that one might have for wishing to regard time as a genuine observable. Hilgevoord's argument is essentially this: there is nothing problematic about time being represented by a parameter rather than an operator since *space* is represented by a parameter rather than an operator as well.

In his otherwise excellent recent historical survey Hilgevoord (2005) contends that the demand that time be an observable can be traced back to a conceptual confusion common among the progenitors of quantum mechanics, in particular Dirac, Heisenberg, Schrödinger, and von Neumann. I will argue that the conceptual confusion is somewhat less severe, and the motivations somewhat more subtle, than Hilgevoord alleges. Hilgevoord claims that the expectation of the authors of quantum mechanics that time should be an

[1] See Srinivas & Vijayalakshmi (1981) for a rigorous derivation of this result.

Probing Complex Systems via Loschmidt Demons

Joshua D. Bodyfelt

Department of Physics

WESLEYAN UNIVERSITY

Complex Quantum Dynamics and Mesoscopic Physics Group

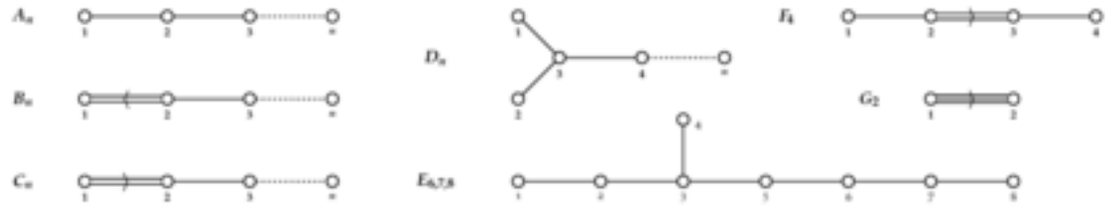
Collaborators: G.S. Ng, M. Hiller, A. Chabanov, J.A. Mendez, U. Kuhl, H.-J. Stöckmann, & T. Kottos

References: Physical Review B, 77, 045103 (2008)
Europhysics Letters, 78, 50003 (2007)
Physical Review Letters, 97, 256404 (2006)

USAF AFRL/RYDP, Dayton, OH – April 28th, 2008

The Periodic Table Of Finite Simple Groups

Dynkin Diagrams of Simple Lie Algebras



$0, C_1, Z_1$ 1 1																C_2 2
$A_1(4), A_1(5)$ A_5 60	$A_1(2)$ $A_1(7)$ 168											$^2A_5(4)$ $B_2(3)$ 25 920	$C_3(3)$ 4 585 351 680	$D_4(2)$ 174 182 400	$^2D_4(2^2)$ 197 406 720	$G_2(2)'$ $^2A_2(9)$ 6 048	C_3 3
$A_1(9), B_1(2)'$ A_6 360	$^2G_2(3)'$ $A_1(8)$ 504											$B_2(4)$ 979 200	$C_3(5)$ 228 501 000 000 000	$D_4(3)$ 4 952 179 814 400	$^2D_4(3^2)$ 10 151 968 619 520	$^2A_2(16)$ 62 400	C_5 5
A_7 2 520	$A_1(11)$ 660	$E_6(2)$ 214 841 575 522 005 575 270 400	$E_7(2)$	$E_8(2)$	$F_4(2)$ 3 311 126 603 366 400	$G_2(3)$ 4 245 696	$^3D_4(2^3)$ 211 341 312	$^2E_6(2^2)$ 76 532 479 683 774 853 939 200	$^2B_2(2^3)$ 29 120	Tits* $^2F_4(2)'$ 17 971 200	$^2G_2(3^3)$ 10 073 444 472	$B_3(2)$ 1 451 520	$C_4(3)$ 65 784 756 654 489 600	$D_5(2)$ 25 499 295 948 800	$^2D_5(2^2)$ 25 015 379 558 400	$^2A_2(25)$ 126 000	C_7 7
$A_8(2)$ A_8 20 160	$A_1(13)$ 1 092	$E_6(3)$	$E_7(3)$	$E_8(3)$	$F_4(3)$ 5 734 420 792 816 671 844 761 600	$G_2(4)$ 251 596 800	$^3D_4(3^3)$ 20 568 831 566 912	$^2E_6(3^2)$	$^2B_2(2^5)$ 32 537 600	$^2F_4(2^3)$ 264 905 352 699 586 178 614 400	$^2G_2(3^5)$ 49 825 657 439 340 552	$B_2(5)$ 4 680 000	$C_3(7)$ 273 457 218 604 953 600	$D_4(5)$ 8 911 539 000 000 000 000	$^2D_4(4^2)$ 67 936 471 195 648 000	$^2A_3(9)$ 3 265 920	C_{11} 11
A_9 181 440	$A_1(17)$ 2 448	$E_6(4)$	$E_7(4)$	$E_8(4)$	$F_4(4)$ 19 009 625 923 840 945 451 297 669 120 000	$G_2(5)$ 5 859 000 000	$^3D_4(4^3)$ 67 802 350 642 790 400	$^2E_6(4^2)$	$^2B_2(2^7)$ 34 093 383 680	$^2F_4(2^5)$	$^2G_2(3^7)$ 239 189 930 264 352 349 332 632	$B_2(7)$ 138 297 600	$C_3(9)$ 54 025 731 402 499 584 000	$D_5(3)$ 1 289 512 799 941 305 139 200	$^2D_4(5^2)$ 17 880 203 250 000 000 000	$^2A_2(64)$ 5 515 776	C_{13} 13
A_n $n!$ 2	$PSL_{n+1}(q), L_{n+1}(q)$ $A_n(q)$	$E_6(q)$	$E_7(q)$	$E_8(q)$	$F_4(q)$	$G_2(q)$	$^3D_4(q^3)$	$^2E_6(q^2)$	$^2B_2(2^{2n+1})$	$^2F_4(2^{2n+1})$	$^2G_2(3^{2n+1})$	$O_{2n+1}(q), O_{2n+1}(q)$ $B_n(q)$	$PSp_{2n}(q)$ $C_n(q)$	$O^+_{2n}(q)$ $D_n(q)$	$O^-_{2n}(q)$ $^2D_n(q^2)$	$PSU_{n+1}(q)$ $^2A_n(q^2)$	$\mathbb{Z}_p$ C_p p

					$J(1), J(11)$ J_1 175 560	HJ J_2 604 800	HJM J_3 50 232 960	J_4 86 775 571 046 077 562 880	HS 44 352 000	McL 898 128 000	F_3, HHM, HTH He 4 030 387 200	Ru 145 926 144 000
Sz Suz 448 345 497 600	$O'NS, O\text{-}S$ $O'N$ 460 815 505 920	$\cdot 3$ Co_3 495 766 656 000	$\cdot 2$ Co_2 42 305 421 312 000	$\cdot 1$ Co_1 4 157 776 806 543 360 000	F_5, D HN 273 030 912 000 000	$Ly5$ Ly 51 765 179 004 000 000	F_3, E Th 90 745 943 887 872 000	$M(22)$ Fi_{22} 64 561 751 654 400	$M(23)$ Fi_{23} 4 089 470 473 293 004 800	$F_{3+}, M(24)'$ Fi'_{24} 1 255 205 709 190 661 721 292 800	F_2 B	F_1, M_1 M

- Alternating Groups
- Classical Chevalley Groups
- Chevalley Groups
- Classical Steinberg Groups
- Steinberg Groups
- Suzuki Groups
- Ree Groups and Tits Group*
- Sporadic Groups
- Cyclic Groups

Alternates†
Symbol
Order‡

*The Tits group $^2F_4(2)'$ is not a group of Lie type, but is the (index 2) commutator subgroup of $^2F_4(2)$. It is usually given honorary Lie type status.

The groups starting on the second row are the classical groups. The sporadic suzuki group is unrelated to the families of Suzuki groups.

Copyright © 2012 Ivan Andrus.

†For sporadic groups and families, alternate names in the upper left are other names by which they may be known. For specific non-sporadic groups these are used to indicate isomorphisms. All such isomorphisms appear on the table except the family $B_n(2^n) \cong C_n(2^n)$.

‡Finite simple groups are determined by their order with the following exceptions:
$B_n(q)$ and $C_n(q)$ for q odd, $n > 2$;
$A_8 \cong A_3(2)$ and $A_2(4)$ of order **20160**.

Pacific Journal of Mathematics

THE TOTAL SPACE OF UNIVERSAL FIBRATIONS

DANIEL H. GOTTLIEB

Vol. 46, No. 2 December 1973

playhack

www.playhack.net

EIGENVALUES OF THE LAPLACE OPERATOR ON CERTAIN MANIFOLDS

By J. Milnor

PRINCETON UNIVERSITY

Communicated February 6, 1951

To every compact Riemannian manifold M there corresponds the sequence $0 = \lambda_1 \leq \lambda_2 \leq \lambda_3 \leq \ldots$ of eigenvalues for the Laplace operator on M. It is not known just how much information about M can be extracted from this sequence.[1] This note will show that the sequence does not characterize M completely, by exhibiting two 16-dimensional tori which are distinct as Riemannian manifolds but have the same sequence of eigenvalues.

By a *flat torus* is meant a Riemannian quotient manifold of the form R^n/L, where L is a lattice (= discrete additive subgroup) of rank n. Let L^* denote the dual lattice, consisting of all $y \in R^n$ such that $x \cdot y$ is an integer for all $x \in L$. Then each $y \in L^*$ determines an eigenfunction $f(x) = \exp(2\pi i x \cdot y)$ for the Laplace operator on R^n/L. The corresponding eigenvalue λ is equal to $(2\pi)^2 y \cdot y$. Hence, the number of eigenvalues less than or equal to $(2\pi r)^2$ is equal to the number of points of L^* lying within a ball of radius r about the origin.

According to Witt[2] there exist two self-dual lattices $L_1, L_2 \subset R^{16}$ which are distinct, in the sense that no rotation of R^{16} carries L_1 to L_2 such that each ball about the origin contains exactly as many points of L_1 as of L_2. It follows that the Riemannian manifolds R^{16}/L_1 and R^{16}/L_2 are not isometric, but do have the same sequence of eigenvalues.

In an attempt to distinguish R^{16}/L_1 from R^{16}/L_2 one might consider the eigenvalues of the Hodge-Laplace operator $\Delta = d\delta + \delta d$, applied to the space of differential p-forms. However, both manifolds are flat and parallelizable, so the identity

$$\Delta(f\, dx_{i_1} \wedge \ldots \wedge dx_{i_p}) = (\Delta f) dx_{i_1} \wedge \ldots \wedge dx_{i_p}$$

shows that one obtains simply the old eigenvalues, each repeated $\binom{16}{p}$ times.

[1] Compare Avakumović, V., "Über die Eigenfunktionen auf geschlossenen Riemannschen Mannigfaltigkeiten," *Math. Zeits.*, 65, 327–344 (1956).

[2] Witt, E., "Eine Identität zwischen Modulformen zweiten Grades," *Abh. Math. Sem. Univ. Hamburg*, 14, 323–337 (1941). See p. 331. I am indebted to K. Barnasullan for pointing out this reference.

Setting $n = 2$, we obtain $a_{22} = 1$, since $(0) = \Gamma(-1, 0)$ vanishes, as do all the terms on the right save (21^0) and (2^2), which are $-\Gamma(2)$ and $\Gamma(2)$, respectively. Setting $n = 3$, we obtain, similarly, $a_{33} = 1$.

* Present address: 6202 Sycamore Road, Baltimore 12, Md.

[1] F. D. Murnaghan, "The Analysis of the Kronecker Product of Irreducible Representations of the Symmetric Group," *Am. J. Math.*, **60**, 761–784, 1938.

[2] A. Censbo and L. A. Radicati, "Sopra un teorema per la riduzione di talune rappresentazioni del gruppo simmetrico," *Atti accad. naz. Lincei, Rend. Classe sci. fis., mat. e nat.*, **14**, 623–634, 1953.

[3] G. de B. Robinson and O. E. Taulbee, "The Reduction of the Inner Product of Two Irreducible Representations of S_n," these PROCEEDINGS, **40**, 723–726, 1954.

[4] Ruey H. Maksi, "On the Analysis of the Kronecker Product of Irreducible Representations of the Symmetric Group," *Proc. Edinburgh Math. Soc.*, **8**, 132–137, 1949.

---

*AN APPLICATION OF ALGEBRAIC TOPOLOGY TO NUMERICAL ANALYSIS: ON THE EXISTENCE OF A SOLUTION TO THE NETWORK PROBLEM**

By J. F. Horn

UNIVERSITY OF CALIFORNIA, BERKELEY

Communicated by C. C. Grosz, May 16, 1955

The electrical network problem was first treated comprehensively by Kirchhoff[1] in 1847. A complete proof for the existence of a solution was given by Hermann Weyl[2] in 1923 for the case of a purely resistive network when sources of electromotive force are placed in series with the branches. This proof was elaborated by Eckmann[3] in 1945. A condition for the existence of a solution given by Synge,[4] attempting to cover a more general case, was unfortunately incorrect, as simple counterexamples show. In this paper we show the existence and uniqueness of a solution to the network problem under a condition which amounts to assuming that the dissipative power is positive definite. Since this condition is satisfied by any physically realizable network, it may be said that this result covers the general physical case (steady state). Actually, we state the electrical network problem in a purely algebraic-topological way. This is of interest since "electrical" networks are used to solve certain ordinary and partial differential equations. The results of this paper are essential to the proof of the validity of Kron's method of tearing,[5] established in a second paper.[6] Our first task is to describe a mathematical model for the quantities and relations which exist in an electrical network.

Let K be an electrical network. We shall consider K as an oriented one-dimensional complex. A set of currents flowing through the branches of K may be considered as the assigning of a complex number to each branch ("coil," in Kron's terminology). Hence such a set of currents will be treated as a vector or oriented 1-chain. The space of such sets of branch currents thus coincides with the group $C^1(K)$ of oriented 1-chains over the coefficient field of complex numbers. A mesh current, the current flowing around an oriented closed loop, corresponds to a 1-cycle, but, as we shall see, it is more appropriate to identify it with an element of the first homology group $H^1(K)$ of K. In fact, the space of such loop currents

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 16-1650

RICHARD FIELDS,
Appellant

v.

CITY OF PHILADELPHIA; SISCA,
POLICE OFFICER, BADGE NO. 9547;
JOE DOE, AN UNKNOWN PHILADELPHIA
POLICE OFFICER

No. 16-1651

AMANDA GERACI,
Appellant

v.

CITY OF PHILADELPHIA; DAWN BROWN,
POLICE OFFICER, BADGE NO. 2454;
TERRA M. BARROW, POLICE OFFICER,
BADGE NO. 1147; NIKKI L. JONES,
POLICE OFFICER, BADGE NO. 2549;

1

Three wonders of symplectic geometry

This is a rough draft of a chapter from a forthcoming book by Polterovich and Rosen. The material presented here (except Section 1.2.2) is relevant to Lecture 1 and to the beginning of Lecture 2 on "Function theory on symplectic manifolds". The draft does not yet contain references to the literature, but it still contains many mistakes. Use it on your own risk.

1.1 First wonder: C^0-rigidity

Let M^{2n} be a smooth connected manifold without boundary, and let ω be a closed 2-form on M which satisfies the following condition:

$$\omega^n = \underbrace{\omega \wedge \ldots \wedge \omega}_{n \text{ times}} \neq 0. \tag{1.1}$$

Then ω is called a *symplectic form*, and (M, ω) a *symplectic manifold*.
Note that ω^n is a top degree form, and hence by (1.1) a volume form, so in particular every symplectic manifold is orientable.

A diffeomorphism of a symplectic manifold (M, ω) is called a *symplectomorphism* if $f^*\omega = \omega$. The symplectomorphisms of (M, ω) form a group with respect to composition. We denote by $\mathrm{Symp}(M, \omega)$ the subgroup of all symplectomorphisms with compact support. By the C^k-topology, for $0 \leq k \leq \infty$, on $\mathrm{Symp}(M, \omega)$, and more generally, on the set of all diffeomorphisms of M, we mean the strong Whitney C^k-topology, (see chapter 2 in Hirsch's book [?]).

Note that symplectomorphisms are defined via their first derivatives, and hence the group $\mathrm{Symp}(M, \omega)$ is by its definition C^1-closed in the group of all compactly supported diffeomorphisms of M. However, for the same reason, a priori it is not obvious whether it is also C^0-closed.

Analysis of Bitcoin Pooled Mining Reward Systems

Meni Rosenfeld

November 17, 2011

Full Abstraction for Signal Flow Graphs

Filippo Bonchi
ENS Lyon, U. Lyon, CNRS, INRIA
filippo.bonchi@ens-lyon.fr

Paweł Sobociński
U. Southampton, UK
ps@ecs.soton.ac.uk

Fabio Zanasi
ENS Lyon, U. Lyon, CNRS, INRIA
fabio.zanasi@ens-lyon.fr

Abstract

Network theory uses the string diagrammatic language of monoidal categories to study graphical structures formally, eschewing specialised translations into intermediate formalisms. Recently, there has been a concerted research focus on developing a network theoretic approach to signal flow graphs, which are classical structures in control theory, signal processing and a cornerstone in the study of feedback. In this approach, signal flow graphs are given a relational denotational semantics in terms of formal power series.

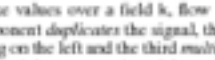
Thus far, the operational behaviour of such signal flow graphs has only been discussed at an intuitive level. In this paper we equip them with a structural operational semantics. As is typically the case, the purely operational picture is too concrete – two graphs that are denotationally equal may exhibit different operational behaviour. We classify the ways in which this can occur and show that any graph can be *realised* – rewritten, using the graphical theory, into an *executable* form where the operational behavior and the denotation coincides.

Categories and Subject Descriptors D.3.1 [*Formal Definitions and Theory*]: Semantics; F.3.2 [*Semantics of Programming Languages*]: Algebraic approaches to semantics

Keywords Signal Flow Graphs, String Diagrams, PROPs, Structural Operational Semantics, Full Abstraction

1. Introduction

Signal flow *graphs* (SFGs) are foundational structures in control theory and signal processing studied since at least the 1950s [23]. They can be constructed from small set of basic components (displayed below) and feedbacks.



(1)

Signals, which take values over a field k, flow from left to right. The leftmost component *duplicates* the signal, the second *sums* the two signals arriving on the left and the third *multiplies* the signal by a scalar $k \in \mathrm{k}$. The rightmost one is a *delay*: when a sequence of signals $k_0, k_1, k_2, \ldots$ arrives on the left, it outputs the sequence $0, k_0, k_1 \ldots$ It can thus be thought as a synchronous one place buffer initialised with 0.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

POPL '15, January 15–17, 2015, Mumbai, India.
Copyright © 2014 ACM 978-1-4503-3300-9/15/01…$15.00.
http://dx.doi.org/10.1145/2676726.2676993

A simple mathematical meaning can be given to those SFGs where feedbacks pass through (at least) one delay component. It is well known (see e.g. [21]) that SFGs with this restriction, one input and one ouput port denote so-called rational linear functions. In traditional approaches, however, SFGs are not treated as interesting mathematical structures per se: formal analyses typically mean the introduction of latent variables and translations into systems of linear equations—although, more recently, they have also attracted the use of coalgebraic tools [4, 26]. This paper, instead, follows the series of recent works [3, 5, 7, 14, 31] where SFGs are understood as structures known as *string diagrams* and studied as mathematical objects of interest in their own right—this approach is known as *network theory* [2]. The majority of the attention so far has been focused on what we call the *denotational semantics*: differently from the classical approach, string diagrams, in general, give rise to *linear relations* rather than functions. The string diagrams that are considered are not restricted by any side conditions on feedbacks, being all those diagrams generated from the basic components (1), together with their duals:

(2)

Intuitively, in (2) the signal flows from right to left. This means that diagrams constructed using both components in (1) and (2) have no univocal flow direction and require a relational model.

Network theory brings fundamentally new ingredients to the field of signal flow graphs. First, the relational semantics is a *compositional* account of their behavior that enjoys a sound and complete axiomatisation independently discovered in [5, 7] and [3]. Second, the axiomatisation has uncovered a rich underlying mathematical playground – featuring two Hopf algebras and two Frobenius algebras – which also reveals connections with quantum phenomena [3, 6, 31]. Third, it has resulted in a subtle re-evaluation of *causality* as a central ingredient of SFGs. In 1953 Mason [23] wrote: "flow graphs differ from electrical network graphs in that their branches are directed. In accounting for branch directions it is necessary to take an entirely different line of approach from that adopted in electrical network topology." Instead, our results suggest that *direction of signal flow is not a primitive notion*: this argument has been made informally already in [3, 5] but is rigorously shown at the end of this paper (Section 6). Similar ideas are prominent in the *behavioural approach* in control theory [30].

In this paper, we introduce *operational semantics* to the network theoretic accounts of signal flow graphs: we show that string diagrams can be thought of as terms of a process calculus and executed as state machines. For this reason we shall call our string diagrams *circuit diagrams* or simply *circuits*. Reconciling the operational perspective with the established denotational model turns out to be quite subtle. Indeed, the denotational semantics is in a sense too abstract: finite computations that reach *deadlocks* are ignored. Such deadlocks can arise for instance when components of (1) are composed with the those of (2) and, intuitively, the signal

A Modular Soft Processor Core in VHDL

Jack Whitham

2002-2003

This is a Third Year project submitted for the degree of MEng in the Department of Computer Science at the University of York. The project will attempt to demonstrate that a modular soft processor core can be designed and implemented on an FPGA, and that the core can be optimised to run a particular embedded application using a minimal amount of FPGA space.

The word count of this project (as counted by the Unix `wc` command after `detex` was run on the LaTeX source) is 33647 words. This includes all text in the main report and Appendices A, B and C. Excluding source code, the project is 70 pages in length.

Fractal measures and their singularities: The characterization of strange sets

Thomas C. Halsey, Mogens H. Jensen, Leo P. Kadanoff, Itamar Procaccia,* and Boris I. Shraiman†
The James Franck Institute, The Enrico Fermi Institute for Nuclear Studies, and Department of Chemistry, The University of Chicago, 5640 South Ellis Avenue, Chicago, Illinois 60637
(Received 26 August 1985)

We propose a description of normalized distributions (measures) lying upon possibly fractal sets, for example those arising in dynamical systems theory. We focus upon the scaling properties of such measures, by considering their singularities, which are characterized by two indices: α, which determines the strength of their singularities; and f, which describes how densely they are distributed. The spectrum of singularities is described by giving the possible range of α values and the function $f(\alpha)$. We apply this formalism to the 2^∞ cycle of period doubling, to the devil's staircase of mode locking, and to trajectories on 2-tori with golden-mean winding numbers. In all cases the new formalism allows an introduction of smooth functions to characterize the measures. We believe that this formalism is readily applicable to experiments and should result in new tests of global universality.

I. INTRODUCTION

Nonlinear physics presents us with a perplexing variety of complicated fractal objects and strange sets. Notable examples include strange attractors for chaotic dynamical systems,[1–3] configurations of Ising spins at critical points,[3] the region of high vorticity in fully developed turbulence,[4,5] percolating clusters and their backbones,[6] and diffusion-limited aggregates.[7,8]. Naturally one wishes to characterize the objects and describe the events occurring on them. For example, in dynamical systems theory one is often interested in a strange attractor (the object) and how often a given region of the attractor is visited (the event). In diffusion-limited aggregation, one is interested in the probability of a random walker landing next to a given site on the aggregate.[7] In percolation, one may be interested in the distribution of voltages across the different elements in a random-resistor network.[6]

In general, one can describe such events by dividing the object into pieces labeled by an index i which runs from 1 up to N. The size of the ith piece is l_i and the event occurring upon it is described by a number M_i. For example, in critical phenomena, we can let M_i be the magnetization of the region labeled by i. Such a picture is natural in the droplet theory of the Ising model, where one argues that if the region i has a size of order l, the magnetization has a value of the order of

$$M_i \sim l^y , \tag{1.1}$$

where y (or y_a) is one of the standard critical indices.[9] Since these droplets are imagined to fill the entire space, the density of such droplets is simply

$$\rho(l) \sim \frac{1}{l^d} , \tag{1.2}$$

where d is the Euclidean dimension of space. In fact, in critical phenomena we define a whole sequence of y_q's by saying that the typical values of $(M_i)^q$ vary with q and have the form[10]

$$(M_i)^q \sim l^{y_q}, \quad q=1,2,3,\ldots . \tag{1.3}$$

Typically, our attention focuses upon the values of y_q that are greater than zero and *we have only a few distinct values of these*.[11]

In this paper we are interested not in critical phenomena but instead in a broad class of strange objects. However, we specialize our treatment to the case in which M_i has the meaning of a probability that some event will occur upon the ith piece. For example, in experiments on chaotic systems one measures a time series $\{\mathbf{x}_i\}_{i=1}^N$. These points belong to a trajectory in some d-dimensional phase space. Typically, the trajectory does not fill the d-dimensional space even when $N\to\infty$, because the trajectory lies on a strange attractor of dimension ν, $D<d$. One can ask now how many times, N_i, the time series visits the ith box. Defining $p_i=\lim_{N\to\infty}(N_i/N)$, we generate the measure on the attractor $d\mu(\mathbf{x})$, because

$$p_i = \int_{i\text{th box}} d\mu(\mathbf{x}) .$$

In many nonlinear problems, the possible scaling behavior is richer and more complex than is the case in critical phenomena. If a scaling exponent α is defined by saying that

$$p_i \sim l_i^{\alpha} , \tag{1.4}$$

then α [roughly equivalent to y_q/q in Eq. (1.3)] can take on a range of values, corresponding to different regions of the measure. In particular, if the system is divided into pieces of size l, we suggest that the number of times α takes on a value between α' and $\alpha'+d\alpha'$ will be of the form

$$d\alpha' \rho(\alpha') l^{-f(\alpha')} , \tag{1.5}$$

where $f(\alpha')$ is a continuous function. The exponent $f(\alpha')$ reflects the differing dimensions of the sets upon which the singularities of strength α' may lie. This expression is roughly equivalent to Eq. (1.2), except that now, instead of the dimension d, we have a fractal dimension $f(\alpha)$

 ©1986 The American Physical Society

THE GENERALIZED STOKES' THEOREM

RICK PRĚSMAN

Abstract. This paper will prove the generalized Stokes Theorem over k-dimensional manifolds. We will begin from the definition of a k-dimensional manifold as well as introduce the notion of boundaries of manifolds. Using these, we will construct the necessary machinery, namely tensors, wedge products, differential forms, exterior derivatives, and integrals over manifolds, in order to prove the main result of this paper. Please note that, unless otherwise noted, all material is provided by [1].

Contents

1. Manifolds and Other Preliminaries 1
2. Exterior Algebra: Tensors and Wedge Products 3
3. Differential Forms and Exterior Derivatives 6
4. Integration on Manifolds 8
5. The Generalized Stokes' Theorem 9
Acknowledgments 11
References 11

1. Manifolds and Other Preliminaries

Manifolds are the fundamental setting in which the Generalized Stokes' Theorem will be constructed. We begin by defining the idea of a smooth map.

Definition 1.1. A map f of an open set $U \subset \mathbb{R}^n$ into $\mathbb{R}^m$ is called *smooth* if it has continuous partial derivatives of all orders. Let X be an arbitrary open subset of $\mathbb{R}^n$. Then we say that a map $f : X \to \mathbb{R}^m$ is smooth if it may be locally extended to a smooth map on open sets; that is, if around each point $x \in X$ there is an open set $U \subset \mathbb{R}^n$ and a smooth map $F : U \to \mathbb{R}^m$ such that F equals f on $U \cap X$.

Using this idea of smoothness, we now define the most important type of function that we will need to understand manifolds: a diffeomorphism.

Definition 1.2. Let X and Y be open sets in $\mathbb{R}^n$. We say $f : X \to Y$ is a *diffeomorphism* if it is bijective and smooth, and if the inverse map $f^{-1} : Y \to X$ is also smooth.

Intuitively, manifolds are sets that may be locally described using Euclidean space. In other words, we are able to construct a bijective continuously smooth map, whose inverse is smooth as well, between the local region of the manifold and

Date: DEADLINE AUGUST 24, 2012.

Bitcoin and Cryptocurrency Technologies

**Arvind Narayanan, Joseph Bonneau, Edward Felten,
Andrew Miller, Steven Goldfeder**

with a preface by Jeremy Clark

Draft — Feb 9, 2016

Feedback welcome! Email bitcoinbook@lists.cs.princeton.edu

For the latest draft and supplementary materials including programming assignments, see our Coursera course.

The official version of this book will be published by Princeton University Press in 2016.
If you'd like to be notified when it's available, please sign up here.

A Critical Analysis of the Jhanas

in Theravada Buddhist Meditation (Print Version)

Henepola Gunaratana

E-mail: bdea@buddhanet.net
Web site: www.buddhanet.net

Buddha Dharma Education Association Inc.

PROBABILITY IN QUANTUM THEORY[†]

E. T. Jaynes
Wayman Crow Professor of Physics
Washington University, St. Louis MO 63130

Abstract: For some sixty years it has appeared to many physicists that probability plays a fundamentally different role in quantum theory than it does in statistical mechanics and analysis of measurement errors. It is a commonly heard statement that probabilities calculated within a pure state have a different character than the probabilities with which different pure states appear in a mixture, or density matrix. As Pauli put it, the former represents "Eine prinzipielle *Unbestimmtheit*, nicht nur *Unbekanntheit*". But this viewpoint leads to so many paradoxes and mysteries that we explore the consequences of the unified view, that all probability signifies only incomplete human information. We examine in detail only one of the issues this raises: the reality of zero–point energy.

CONTENTS

INTRODUCTION: HOW WE LOOK AT THINGS	1
HOW DO WE LOOK AT GRAVITATION AND QED?	2
HOW DO WE LOOK AT BASIC QUANTUM THEORY?	4
PROBABILITY THEORY AS THE LOGIC OF SCIENCE	7
HOW WOULD QUANTUM THEORY BE DIFFERENT?	9
IS ZERO–POINT ENERGY REAL?	11
THE LAMB SHIFT IN CLASSICAL MECHANICS	13
CLASSICAL SUBTRACTION PHYSICS	15
CONCLUSION	18
REFERENCES	19

INTRODUCTION: HOW WE LOOK AT THINGS

In this workshop we are venturing into a smoky area of science where nobody knows what the real truth is. Such fields are always dominated by the compensation phenomenon: supreme self–confidence takes the place of rational arguments. Therefore we shall try to avoid dogmatic assertions, and only point out some of the ways in which quantum theory would appear different if we were to adopt a different viewpoint about the meaning and functional use of probability theory. We think that the original viewpoint of James Bernoulli and Laplace offers some advantages today in both conceptual clarity and technical results for currently mysterious problems.

[†] A revised and extended version of a paper presented at the Workshop on *Complexity, Entropy, and the Physics of Information*, Santa Fe, New Mexico, May 29 – June 2, 1989. The original version is in the Proceedings Volume, *Complexity, Entropy and the Physics of Information*, W. H. Zurek Editor, Addison–Wesley Publishing Co., Reading, MA (1990).

Stanford Encyclopedia of Philosophy

Process Theism

First published Thu Jul 29, 2004; substantive revision Tue Jan 28, 2014

Process theism typically refers to a family of theological ideas originating in, inspired by, or in agreement with the metaphysical orientation of the English philosopher-mathematician Alfred North Whitehead (1861–1947) and the American philosopher-ornithologist Charles Hartshorne (1897–2000). For both Whitehead and Hartshorne, it is an essential attribute of God to be fully involved in and affected by temporal processes. This idea contrasts neatly with traditional forms of theism that hold God to be or at least conceived as being, *in all respects* non-temporal (eternal), unchanging (immutable,) and unaffected by the world (impassible). Process theism does not deny that God is *in some respects* eternal, immutable, and impassible, but it contradicts the classical view by insisting that God is *in some respects* temporal, mutable, and passible. The views of Whitehead and Hartshorne should also be distinguished from those that affirm that the divine being, by an act of self-limitation, opens itself to influence from the world. Some neo-Thomists hold this view and a group of Evangelical Christian philosophers, calling themselves "open theists," promote similar ideas. These forms of theism were influenced by process theism, but they deny its claim that God is *essentially* in a give-and-take relationship with the world. Moreover, process theism is a genuinely *philosophical* theology in the sense that it is not grounded in claims of special insight or revealed truth but in philosophical reflection. Specifically, process theism is a product of theorizing that takes the categories of becoming, change, and time as foundational for metaphysics. The metaphysical underpinning of process theism is often called process philosophy, a label suggested by the title of Whitehead's magnum opus, *Process and Reality*. In order to bring out this philosophy's emphasis on relatedness, many scholars follow Bernard Loomer in calling it process-relational philosophy. Whitehead's preferred expression for his metaphysical viewpoint is "the philosophy of organism." This article concerns primarily the concept of God in process theism, although we shall conclude with a brief discussion of arguments for the existence of God in process thought and a note on the historical influences on process theism.

- 1. God and Creativity
- 2. Real Relations in God
- 3. Dual Transcendence in Whitehead and Hartshorne
  - 3.1 Whitehead on the two natures of God
  - 3.2 Hartshorne on existence and actuality
- 4. Panentheism
- 5. Divine Power and the Problem of Evil
- 6. Divine Knowledge and the Problem of Future Contingents
- 7. Transforming Traditional Theism and Process Theism
- 8. Arguments for the Existence of God in Process Theism
- 9. Historical Notes on Process Theism
- Bibliography
- Academic Tools
- Other Internet Resources
- Related Entries

---

1. God and Creativity

The question of the metaphysical relation of God and creativity is a watershed between process theism and more traditional forms of theism. Process philosophy, modifying a statement from Plato's *Sophist* (247e), affirms that the most concrete real beings—in Whitehead's language, actual entities—are characterized by the power to act *and* to be acted upon (Plato says real beings act *or* are acted upon). In process metaphysics no actual entity is wholly determined by the activity of another; or phrased positively, every actual entity retains *some* power of self-determination, however minimal or slight it may be. According to this view, to

Banff International Research Station

for Mathematical Innovation and Discovery

Entanglement in Curved Spacetime

(13w5153)

22-27 September 2013

MEALS

*Breakfast (Buffet): 7:00 – 9:30 am, Sally Borden Building, Monday – Friday
*Lunch (Buffet): 11:30 am – 1:30 pm, Sally Borden Building, Monday – Friday
*Dinner (Buffet): 5:30 – 7:30 pm, Sally Borden Building, Sunday – Thursday
Coffee Breaks: As per daily schedule, in the foyer of the TransCanada Pipeline Pavilion (TCPL)
***Please remember to scan your meal card at the host/hostess station in the dining room for each meal.**

MEETING ROOMS

All lectures will be held in the TransCanada Pipelines Pavilion (TCPL). LCD projector and blackboards are available for presentations. Ceiling-mounted video cameras are installed in the main lecture room of 201, TCPL. But do bring your own laptop. There are two lecture rooms and BIRS will run two workshops in parallel. Our workshop has all lectures in the morning in room 202 and those in the evening in room 201.

We will not have lectures in the afternoons. This is to enable informal discussions and collaborations. *For collaborations, the two breakout rooms 106 and 107 on the lower level are reserved for us.* The breakout room 102 may also be available, though the parallel workshop has priority there. These breakout rooms each accommodate up to 6 people and have blackboards and white boards. Also the reading room in the Corbet Hall is available. It has computer, printer, scanner and white board. Permanently available to us is also the seminar room 202.

SCHEDULE

Sunday

16:00	Check-in begins (Front Desk – Professional Development Centre - open 24 hours)
17:30-19:30	Buffet Dinner
20:00	Informal gathering in 2nd floor lounge, Corbett Hall Beverages and small assortment of snacks are available on a cash honor system.

Monday

7:00-8:45	Breakfast
8:55-9:00	Introduction and Welcome by BIRS Station Manager, TCPL
9:00-9:30	Lecture 1 (Mann)
9:30-10:00	Lecture 2 (Donnelly)
10:00-11:00	Coffee Break, TCPL
11:00-11:30	Lecture 3 (Hotta)
11:30-13:00	Lunch
13:00-14:00	Guided Tour of The Banff Centre; meet in the 2nd floor lounge, Corbett Hall Time for walks, discussions and collaborations (talk and walk)

At Our Own Peril:

DoD Risk Assessment in a Post-Primacy World

Project Director & Principal Author

Nathan P. Freier

Contributing Authors

Christopher M. Bado

Christopher J. Bolan

Robert S. Hume

J. Matthew Lissner

Contributing Researchers

Heather Bellusci

John R. Beurer

Ralph Borja

Steven Buelt

Michael Lechlitner

Robert D. Montz

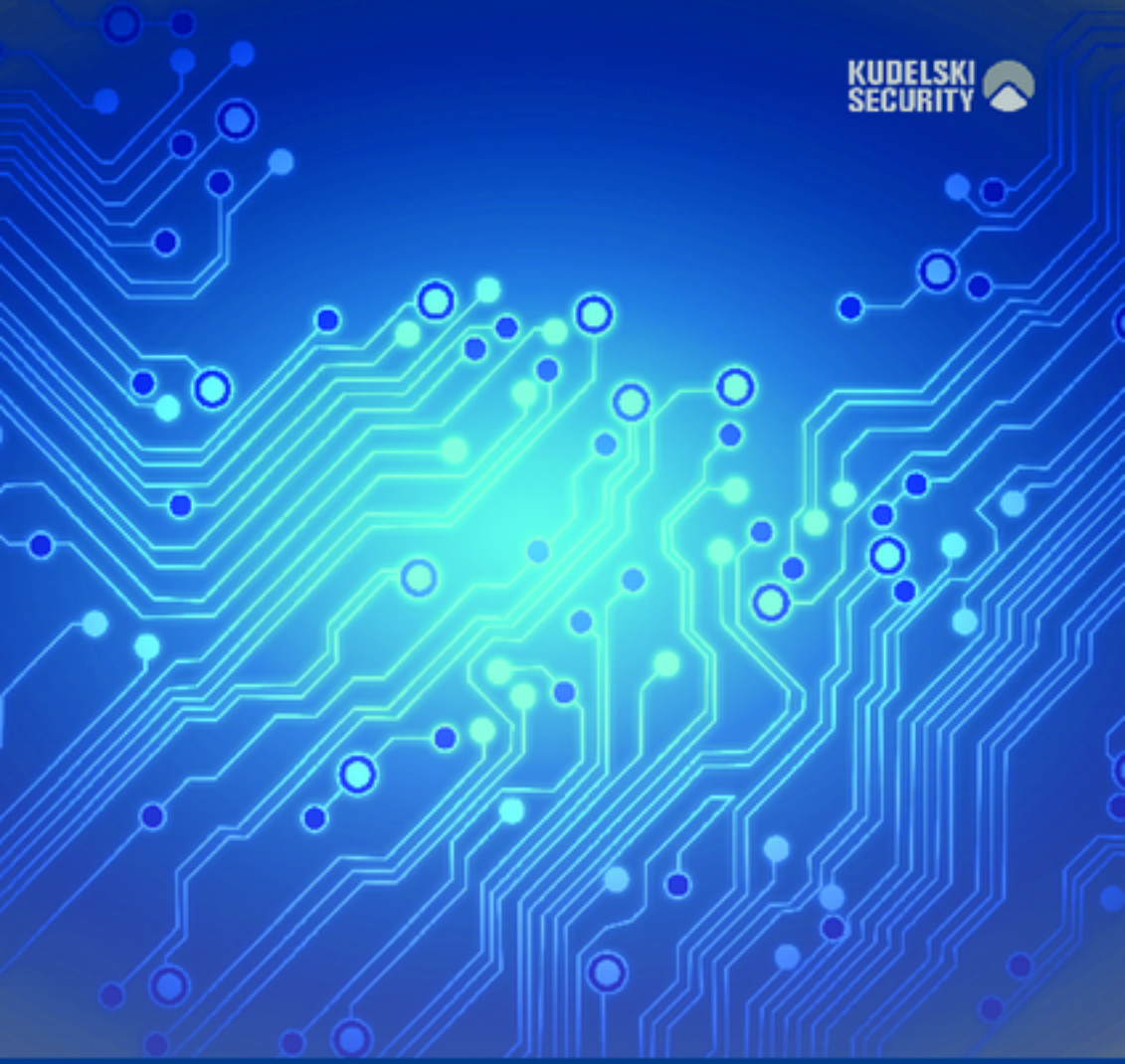
Robert Phillips

Kelsey Smith

U.S. ARMY WAR COLLEGE

SSI

UNITED STATES ARMY WAR COLLEGE PRESS



SGX SECURE ENCLAVES IN PRACTICE: SECURITY AND CRYPTO REVIEW

JFM RAPIDS
journals.cambridge.org/rapids

1 2 1 1
1 †

1. Introduction

2005

2006

2015*a b*

2010

2014 2014 2016 2014 2014*a b*

bush@math.mit.edu

Downloaded from http://www.cambridge.org/core. MIT Libraries, on 19 Sep 2016 at 19:41:48, subject to the Cambridge Core terms of use, available at http://www.cambridge.org/core/terms. http://dx.doi.org/10.1017/jfm.2016.527

Special Issue

Examining the Existence of the Multiverse

James J. Hurtak[a], Desiree E. Hurtak[a] and Elizabeth A. Rauscher[†]

Abstract

Guth's (1997) inflationary universe model has been widely accepted in modern physics. Expanding upon this concept, Linde (1994) introduced the Chaotic and Eternal inflationary model. The inflationary universe structure allows for multiple universes or various "bubble" universes connected through scalar and tensor fields and making the structure of space self similar on larger scales. In this paper we briefly examine these and other theories - including M-Theory - associated with a multiverse, which consider that our universe and others are created by collisions between membranes in an 11-dimensional space.

Key Words: : cosmology, quantum mechanics, multiverse, scalar fields

***Quantum Biosystems* 2015; 6 (1): 115-130**

1 - Introduction: Why a Multiverse?

Use of the observational data, in the study of CMB and WMAP, indicates that the universe is accelerating its expansion. If this acceleration is caused by a positive energy density of the vacuum (i.e., cosmological constant, $\Lambda>0$), the process could continue forever. With a variety of theories researchers have sought to explain this phenomena including abstract theories of elementary particles, such as M-theory, string theory, supergravity and the standard model (SM). Many of them lead to the conclusion that our known universe is part of a multiverse.

There are numerous ideas of how a multiverse came into existence, including Linde's Bubble Theory, the many worlds interpretation (MWI) of quantum physics, braneworlds predicted by string theory and M-branes, and other models which we examine in this paper.

There are at least six different classifications of a multiverse: the Quilted Multiverse, Inflationary Multiverse, Brane, Cyclic and Landscape Multiverses, MWI, and the Holographic Universe. In most of these theories—string theory, the inclusion of the cosmological constant and quantum physics—have shown certain mathematical congruities.

According to Rauscher and Hurtak (2012), Jenkins (2010) and others, our ability to exist, that is, for life to form as we know it, depends on a precise set of conditions, physical constants that exist in our universe. Specifically, in this observable universe, the parameters seem to be "fine-tuned" into particular values, including the Planck length, such that if they had other values, known forms of life would not exist.

A critical constant that had been generally overlooked, the cosmological constant, Λ, is now beginning to occupy a major role following the research of Perlmutter (2005) and the High-z Supernova Search Team. Sorkin (2007) examined the data, to provide an explanation of the importance of Λ, stating

Corresponding author: Elizabeth A. Rauscher
Address: [a]AFPS-Europe, 4058 Basel, Switzerland
E-mail: dh@afps.org, [†]Technic Research Laboratory, 3500, S. Tomahawk Rd. Bldg. 188, Apache Junction, AZ 85119 USA.
E-mail: lsr1001@mse.com

Interacting Frobenius Algebras are Hopf

Ross Duncan Kevin Dunne
University of Strathclyde, 26 Richmond Street, Glasgow G1 1XH, UK.
{ross.duncan,kevin.dunne}@strath.ac.uk

Theories featuring the interaction between a Frobenius algebra and a Hopf algebra have recently appeared in several areas in computer science: concurrent programming, control theory, and quantum computing, among others. Bonchi, Sobocinski, and Zanasi [10] have shown that, given a suitable distributive law, a pair of Hopf algebras forms two Frobenius algebras. Here we take the opposite approach, and show that interacting Frobenius algebras form Hopf algebras. We generalise [10] by including non-trivial dynamics of the underlying object—the so-called phase group—and investigate the effects of finite dimensionality of the underlying model. We recover the system of Bonchi et al as a subtheory in the prime power dimensional case, but the more general theory does not arise from a distributive law.

This is a short contribution based on the pre-print arxiv:1601.04964, which has been submitted elsewhere.

1 Summary

Frobenius algebras and bialgebras are structures which combine a monoid and a comonoid on a single underlying object. They have a long history[1] in group theory, but have applications in many other areas: natural language processing [36, 37], topological quantum field theory [30], game semantics [32], automata theory [41], and distributed computing [8], to name but a few.

In quantum computation, the bialgebraic interplay between two Frobenius algebras describes the behaviour of complementary observables [13, 15], a central concept in quantum theory. This interaction is the basis of the ZX-calculus, a formal language for quantum computation. Using these ideas, a significant fraction of finite dimensional quantum theory can be developed without reference to Hilbert spaces [3, 4, 5, 6, 16, 17, 18, 19, 40, 20, 21, 22, 23, 26, 27, 28, 29, 33, 34, 35, 39]. Surprisingly, almost exactly the same axioms have also appeared in totally different settings: Petri nets [12, 38] and control theory [7, 11]. This combination of structures seems to have broad relevance in computer science.

The approach of the current paper is directly inspired by the recent work of Bonchi, Sobociński, and Zanasi [10], who investigated the theory of interacting Hopf algebras[2] and showed that Hopf algebras which obey a certain distributive law form Frobenius algebras [9, 10]. Using Lack's technique of composing PROPs [31], they show the resulting theory $\mathbb{IH}_R$ is isomorphic to that of linear relations[3].

Do interacting quantum observables [15] admit such a beautiful description? In this paper we present a rational reconstruction of theory of strongly complementary observables and show that, except under quite restrictive circumstances, the theory does not arise by composing PROPs via a distributive law. Along the way we also clarify the structure of the theory of complementary observables and show that some assumptions used in earlier work are unnecessary.

[1] See Fauser [25] for much detail on Frobenius algebras, including their history; for the history of Hopf algebras see [2].
[2] A Hopf algebra is a bialgebra with some extra structure; see later ??.
[3] Baez and Erbele [7] prove the same result with different techniques.

Submitted to:
QPL2016

© R. Duncan & K. Dunne

Categorifying the zx-calculus

Daniel Cicala

Department of Mathematics
University of California, Riverside
USA

cicala@math.ucr.edu

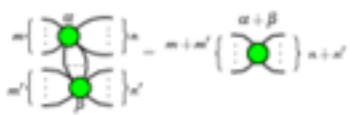
Compositionality is becoming increasingly recognized as a viable method to model complex systems such as those found in physics, computer science, and biology. The idea is to study smaller, simpler systems and ways of connecting them together. The word *compositionality* suggests that category theory can play a key role, and indeed it does. Systems are morphisms and connections are morphism composition.

This paper [3] looks at one example of compositionality in action: the zx-calculus. The backstory dates to Penrose's tensor networks and, more recently, to the relationship between graphical languages and monoidal categories explored by Joyal, Street, and Selinger. Abramsky and Coecke capitalized on this relationship when inventing a categorical framework for quantum physics [1]. Through this perspective, Coecke and Duncan presented early results on a diagrammatic language in which to reason about *complementary quantum observables*. After a fruitful period of development, the first complete presentation of the zx-calculus was published [5].

The zx-calculus begins with the wire, green spider, red spider, Hadamard, and diamond diagrams

(1)

Observe that there are dangling wires on the left and right. Think of those on the left as inputs and those on the right as outputs. A pair of diagrams are composable when the inputs of one match the outputs of another. Formalizing this perspective, we let these diagrams generate the morphisms of a dagger compact category **zx** whose objects are the non-negative integers. The meaning of these objects is to give the number of inputs and outputs for a morphism $n \to m$. These morphisms are then subjected to a number of relations which are listed in full in the preprint [3]. For illustrative purposes, we will present one of the relations:



(2)

Our main result is the construction of a symmetric monoidal and compact closed bicategory $\underline{\mathbf{zx}}$ that categorifies the dagger compact category **zx**. The process of building $\underline{\mathbf{zx}}$ begins with (directed) graphs and adding additional structure that mimics the **zx**-morphisms.

The first difference between graphs and **zx**-morphisms we recognize is that the former have single-sorted nodes while the latter have multi-sorted nodes. We address this by considering the graph S_{zx}

$\alpha, \beta \in [-\pi, \pi)$

Submitted to:
QPL 2017

© Daniel Cicala
This work is licensed under the
Creative Commons Attribution License.

ETSI White Paper No. 8

Quantum Safe Cryptography and Security

An introduction, benefits, enablers and challenges

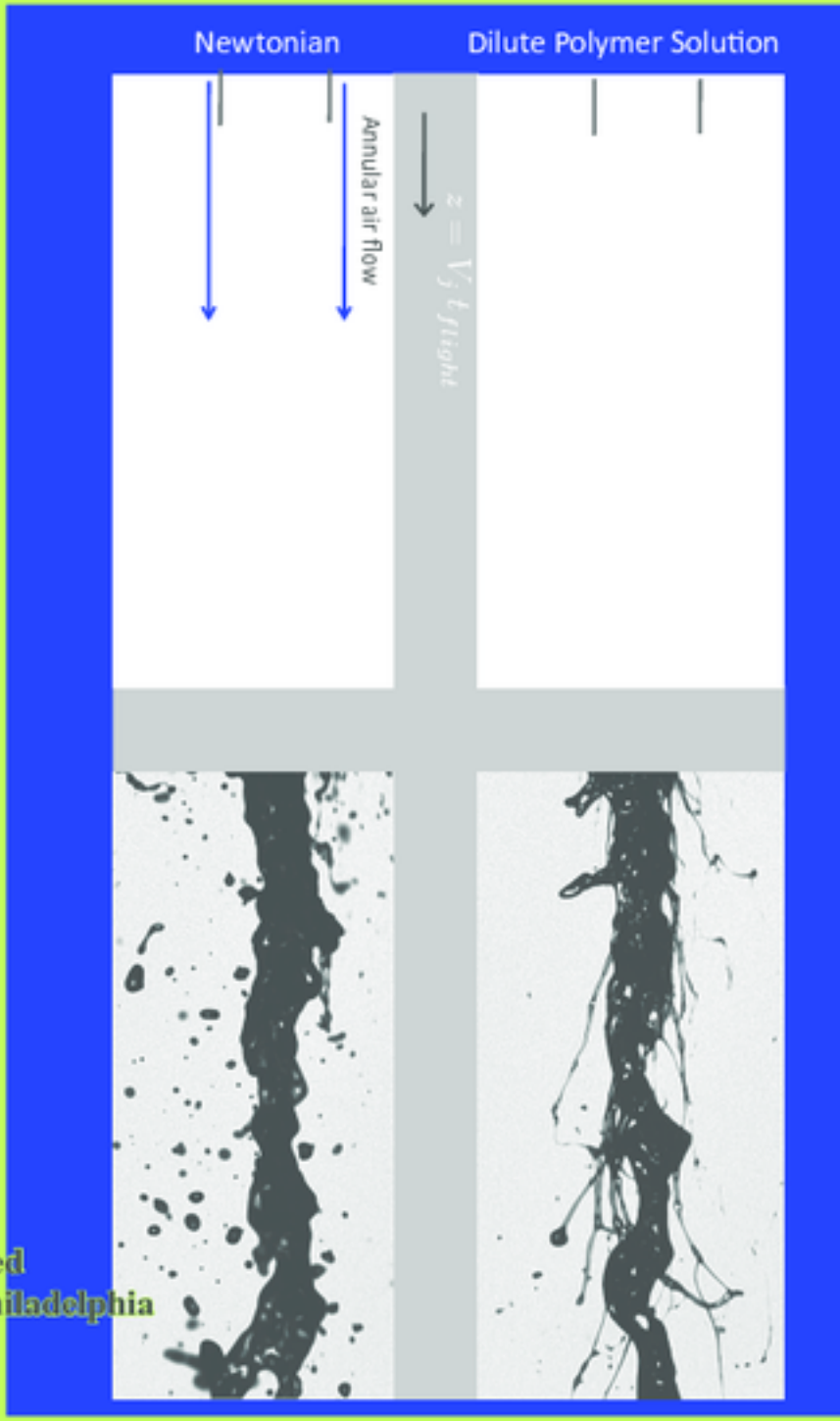
June 2015

ISBN No. 979-10-92620-03-0

ETSI (European Telecommunications Standards Institute)
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

The News and Information Publication of The Society of Rheology
Volume 83 Number 2 July 2014

Rheology Bulletin



Inside:

- Rheology of ... Cats?
- Open Access Explained
- Annual Meeting in Philadelphia
- 2014 Society Awards

Getting Physical With USB Type-C

WINDOWS 10 RAM FORENSICS AND UEFI ATTACKS

ALEX IONESCU [@AIONESCU]
RECON BRUSSELS 2017

Optimization Over Hyperbolicity Cones

Jim Renegar

MICHAEL L. KAPLAN
Director, Atmospheric Sciences Program
Associate Research Professor
Division of Atmospheric Sciences
Desert Research Institute
2215 Raggio Parkway, Reno, Nevada 89512

Tel: (775) 674-7051
Fax: (775) 674-7007
Email: Mike.Kaplan@dri.edu

Education:

B.A.	Rutgers University	Meteorology	1967
M.S.	Rutgers University	Meteorology	1968
Ph.D.	State University of New York, Albany	Atmospheric Sciences	1972

Dissertations:

- M.S. -"A Four-Level Air Mass Analyses for Washington, D.C. Using the Equivalent Potential Temperature", Rutgers University, University Microfilms, Ann Arbor, Michigan, 1968.
- Ph.D. -"A Macroscale-Mesoscale Numerical Model and Lake-Effect Snowstorms", State University of New York at Albany, University Microfilms, Ann Arbor, Michigan, 1972.

Professional Experience:

2013 - 2015	Research Professor, Desert Research Institute, Division of Atmospheric Sciences, Reno, NV
2005 – 2013	Associate Research Professor, Desert Research Institute, Division of Atmospheric Sciences, Reno, NV
1999 – 2005	Research Associate Professor, North Carolina State University
1990 – 1999	Visiting Associate, North Carolina State University
1985 – 1990	President/Senior Research Scientist, MESO Inc.
1979 – 1985	Principal Research Scientist, Systems and Applied Sciences Corporation
1975 – 1979	Visiting Professor, George Washington University, Joint Institute for Acoustics and Flight Sciences, Department of Environmental Modeling
1971 – 1975	Captain/Active Duty Officer/Research Scientist US Air Force, Air Weather Service, Air Force Global Weather Central
1968 – 1971	Graduate Research Assistant, Department of Atmospheric Sciences, State University of New York, Albany

Professional Interests:

Forty-eight years of experience in synoptic and dynamical meteorology and mesoscale numerical weather prediction with emphasis in the following problem areas: aviation turbulence, fire meteorology, extreme rainfall, severe convective storms, mesoscale convective complex systems, terrain-induced circulations, nocturnal low-level jets, geostrophic adjustment processes, gravity waves, lake-effect snowstorms, cyclogenesis, sea-breeze convection, frontogenesis/frontolysis, density currents, flooding from landfalling tropical cyclones, North American monsoon dynamics, nuclear winter, Martian meteorology, wind/solar power/renewable energy, dust storms, mountain meteorology, weather modification, and multi-scale jet streak dynamics.

Available online at www.sciencedirect.com
ScienceDirect
Renewable and Sustainable Energy Reviews
12 (2008) 1822–1842

RENEWABLE & SUSTAINABLE ENERGY REVIEWS

www.elsevier.com/locate/rser

Review of Ranque–Hilsch effects in vortex tubes

Smith Eiamsa-ard[a,1], Pongjet Promvonge[b,*]

[a]*Department of Mechanical Engineering, Faculty of Engineering, Mahanakorn University of Technology, Bangkok 10530, Thailand*
[b]*Department of Mechanical Engineering, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand*

Received 2 February 2007; received in revised form 2 February 2007; accepted 22 March 2007

Abstract

The vortex tube or Ranque–Hilsch vortex tube is a device that enables the separation of hot and cold air as compressed air flows tangentially into the vortex chamber through inlet nozzles. Separating cold and hot airs by using the principles of the vortex tube can be applied to industrial applications such as cooling equipment in CNC machines, refrigerators, cooling suits, heating processes, etc. The vortex tube is well-suited for these applications because it is simple, compact, light, quiet, and does not use Freon or other refrigerants (CFCs/HCFCs). It has no moving parts and does not break or wear and therefore requires little maintenance. Thus, this paper presents an overview of the phenomena occurring inside the vortex tube during the temperature/energy separation on both the counter flow and parallel flow types. The paper also reviews the experiments and the calculations presented in previous studies on temperature separation in the vortex tube. The experiment consisted of two important parameters, the first is the geometrical characteristics of the vortex tube (for example, the diameter and length of the hot and cold tubes, the diameter of the cold orifice, shape of the hot (divergent) tube, number of inlet nozzles, shape of the inlet nozzles, and shape of the cone valve. The second is focused on the thermo-physical parameters such as inlet gas pressure, cold mass fraction, moisture of inlet gas, and type of gas (air, oxygen, helium, and methane). For each parameter, the temperature separation mechanism and the flow-field inside the vortex tubes is explored by measuring the pressure, velocity, and temperature fields.

The computation review is concentrated on the quantitative, theoretical, analytical, and numerical (finite volume method) aspects of the study. Although many experimental and numerical studies on the vortex tubes have been made, the physical behaviour of the flow is not fully understood due to its complexity and the lack of consistency in the experimental findings. Furthermore, several different

*Corresponding author. Tel.: +662 3264197; fax: +662 3264198.
E-mail addresses: smith@mut.ac.th (S. Eiamsa-ard), kppongje@kmitl.ac.th (P. Promvonge).
[1]Tel./fax: +662 9883666x241.

1364-0321/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.rser.2007.03.006

Manipulating Spatial Boundaries or Time Boundaries:

New Approaches for Wave Control in Complex Medium

Mathias A Fink

Institut Langevin, ESPCI Paris Tech, France

Email of Presenting Author: mathias.fink@espci.fr

Time-reversal processing is based on Huygens principles and on wavefield manipulation on spatial boundaries. It provided an elegant way to back propagate a wave field towards its initial source allowing to create, through any complex medium, a wave pattern of any required shape restricted only by diffraction limits.

Here we want to revisit these approaches by introducing another point of view, the one that Loschmidt proposed in his famous argument to create a time-reversal experiment by inversing instantaneously all velocities of the particles in a gas. The extension of this concept to wave will be discussed through the concept of time boundaries manipulation. Experiments, conducted with water waves, validating this approach will be presented. They allow to revisit the role of Huygens wavelets in diffraction theory.

In the second part of this talk, we will discussed another approach to manipulate a wave field in reverberating medium by introducing tunable metasurfaces as spatial boundaries and we will emphasize this concept for microwaves.

HAL
archives-ouvertes.fr

A Boundary Operator for Computing the Homology of Cellular Structures

Sylvie Alayrangues, Guillaume Damiand, Pascal Lienhardt, Samuel Peltier

▶ **To cite this version:**

Sylvie Alayrangues, Guillaume Damiand, Pascal Lienhardt, Samuel Peltier. A Boundary Operator for Computing the Homology of Cellular Structures. 2011.

HAL Id: hal-00683031

https://hal.archives-ouvertes.fr/hal-00683031v1

Submitted on 27 Mar 2012 (v1), last revised 2 Jan 2013 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Chapter 3

Almost complex structures

3.1 Decomposition of 1-forms

For an open set $U \subset \mathbb{C}$ the 1-forms $dz, d\bar{z}$ generate $\mathcal{A}^1_U$, i.e. every local section ω can be written as $\omega_z dz + \omega_{\bar{z}} d\bar{z}$. Moreover $\omega_z, \omega_{\bar{z}}$ are unique. Let $f : V \cong U$ be a change of coordinates, where $V \subset \mathbb{C}$ is open. Then by using the formulas 2.1.1.2 and $\bar{\partial}(f) = 0$ we get

$$\begin{aligned} f^*(\omega) &= (\omega_z \circ f)df + (\omega_{\bar{z}} \circ f)\overline{df} \\ &= (\omega_z \circ f)(\partial_z(f)dz + \bar{\partial}_z(f)d\bar{z}) + (\omega_{\bar{z}} \circ f)(\overline{\partial_z(f)}dz + \overline{\partial_z(f)}d\bar{z}) \\ &= (\omega_z \circ f)\partial_z(f)dz + (\omega_{\bar{z}} \circ f)\overline{\partial_z(f)}d\bar{z}. \end{aligned}$$

Thus f^* respects the decomposition of $\mathcal{A}^1$:

$$\mathcal{A}^1_U = \mathcal{A}^{1,0}_U \oplus \mathcal{A}^{0,1}_U, \quad \mathcal{A}^{1,0}_U = \mathcal{A}_U dz, \quad \mathcal{A}^{0,1}_U = \mathcal{A}_U d\bar{z}.$$

Since it is independent of coordinate changes we get a decomposition of sheaves for every Riemann surface X:

$$\mathcal{A}^1_X = \mathcal{A}^{1,0}_X \oplus \mathcal{A}^{0,1}_X.$$

Let $\mathcal{A}^1_{X,\mathbb{R}}$ for the sheaf of real-valued 1-forms, then

$$\mathcal{A}^1_X = \mathcal{A}^1_{X,\mathbb{R}} \otimes_{\mathbb{R}} \mathbb{C},$$

and $\mathcal{A}^1_{X,\mathbb{R}}$ are the invariants of the conjugation. Since $\overline{dz} = d\bar{z}$, we get

$$\mathcal{A}^{0,1}_X = \overline{\mathcal{A}^{1,0}_X}.$$

3.2 Definition of an almost complex structure

Let X be a differentiable 2-dimensional manifold. We write $\mathcal{A}_{X,\mathbb{R}}$ for the sheaf of real-valued functions, and $\mathcal{A}^1_{X,\mathbb{R}}$ for the sheaf of real-valued 1-forms.

Hermitage Capital Management

Heather H. Hunt, Chief
FARA Registration Unit
Counterintelligence and Export Control Section
National Security Division
U.S Department of Justice

By Email: [redacted]@usdoj.gov

15 July 2016

Dear Ms. Hunt,

Complaint regarding the violation of US Lobbying Laws by the Human Rights Accountability Global Initiative Foundation and others by Hermitage Capital Management ("Hermitage")

Further to our recent call, on information and belief, we write to set out in more detail several violations of US lobbying laws by lobbyists and entities acting under the direction/control/influence of the Russian Government.

I. Executive Summary

1. There is an ongoing lobbying campaign to repeal the Magnitsky Act (the "Campaign") and rewrite the history of the Magnitsky story. This campaign has been conducted by the following entities
   A. Prevezon Holdings Limited ("Prevezon") - a Russian owned Cyprus registered company
   B. The Human Rights Accountability Global Initiative Foundation ("HRAGIF") - a Delaware NGO created on 18 February 2016.

2. To assist them in the Campaign, based on information and belief, the following people have been hired to lobby on their behalf:
   A. **Rinat Akhmetshin** – Russian national living in Washington D.C.
   B. **Robert Arakelian**
   C. **Chris Cooper** – CEO Potomac Square Group
   D. **Glenn Simpson -** SNS Global and Fusion GPS
   E. **Mark Cymrot** – Partner, Baker Hosteler
   F. **Ron Dellums** - Former Republican Congressman
   G. **Howard Schweitzer** – Managing Partner of Cozen O'Connor Public Strategies

For Correspondence only:
3rd Floor, Grafton House, 2-3 Golden Square, London W1F 9HR
Tel: +44 (0)207 440 1777 / Fax: +44 (0)207 440 1778

Available online at www.sciencedirect.com
SCIENCE DIRECT®
Theoretical Computer Science 343 (2005) 443–481
Theoretical Computer Science
www.elsevier.com/locate/tcs

A tutorial on coinductive stream calculus and signal flow graphs

J.J.M.M. Rutten*
CWI and VUA, P.O. Box 94079, 1090 GB Amsterdam, Netherlands

Abstract

This paper presents an application of coinductive stream calculus to signal flow graphs. In comparison to existing approaches, which are usually based on Z-transforms (a discrete version of Laplace transforms) and transfer functions, the model presented in these notes is very elementary. The formal treatment of flow graphs is interesting because it deals with two fundamental phenomena in the theory of computation: memory (in the form of register or delay elements) and infinite behaviour (in the form of feedback).
© 2005 Elsevier B.V. All rights reserved.

MSC: 68Q10; 68Q55; 65A85

Keywords: Streams; Coinduction; Cnalgebra; Signal flow graphs

1. Introduction

Infinite sequences or *streams* occur at many different places, both in mathematics and computer science, and in every day life. For the latter, think of bit streams flowing through the chips of your computer, or through the ether carrying messages from your mobile telephone. More generally, signals in the theory of signal processing are commonly represented by streams of real numbers. Also functions on streams are relevant in that setting, as they are the building blocks for filters and converters (such as the digital to analog converter in cd-players). An example of streams appearing in computer science is dataflow, which

* Tel.: +31 20 592 4116; fax: +31 20 592 4199.
E-mail address: jan.rutten@cwi.nl.

0304-3975/$- see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2005.06.019

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 2, Pages 563–570
S 0002-9939(02)06565-6
Article electronically published on May 29, 2002

ON THE BOUNDEDNESS OF HAMILTONIAN OPERATORS

TOMÁS YA. AZIZOV, AAD DIJKSMA, AND IRINA V. GRIDNEVA

(Communicated by Joseph A. Ball)

ABSTRACT. We show that a non-negative Hamiltonian operator whose domain contains a maximal uniformly positive subspace is bounded.

INTRODUCTION

Let $\{\mathcal{G}, (\cdot\,,\cdot)\}$ be a Hilbert space and consider the orthogonal direct sum

$$\mathcal{H} = \mathcal{G} \oplus \mathcal{G}, \tag{1}$$

which is a Hilbert space whose inner product we also denote by $(\cdot\,,\cdot)$. A bounded operator $\mathfrak{A}$ on $\mathcal{H}$ is called a *Hamiltonian* operator if with respect to the decomposition (1) it has the 2×2 block matrix representation

$$\mathfrak{A} = \begin{bmatrix} A & B \\ C & -A^* \end{bmatrix},$$

where B and C are self-adjoint operators on $\mathcal{G}$. If additionally B and C are both non-negative, then $\mathfrak{A}$ is called a *non-negative* Hamiltonian operator. In the space $\mathcal{H}$ we consider the block matrices

$$J = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}, \quad \mathfrak{J} = \begin{bmatrix} 0 & iI \\ -iI & 0 \end{bmatrix}$$

and introduce two Krein spaces (for the definition see (i) below) $\mathcal{K}_J := \{\mathcal{H}, |\cdot\,,\cdot|_J\}$ and $\mathcal{K}_{\mathfrak{J}} := \{\mathcal{H}, |\cdot\,,\cdot|_{\mathfrak{J}}\}$ whose indefinite inner products are defined by

$$|\cdot\,,\cdot|_J = (J\cdot\,,\cdot), \quad |\cdot\,,\cdot|_{\mathfrak{J}} = (\mathfrak{J}\cdot\,,\cdot),$$

respectively. Evidently, the bounded operator $\mathfrak{A}$ on the Hilbert space $\mathcal{H} = \mathcal{G} \oplus \mathcal{G}$ is Hamiltonian if and only if $i\mathfrak{A}$ is self-adjoint in the Krein space $\mathcal{K}_{\mathfrak{J}}$, and $\mathfrak{A}$ is a non-negative Hamiltonian operator if it is a Hamiltonian operator such that $i\mathfrak{A}$ is dissipative (for the definition see (ii) below) in the Krein space $\mathcal{K}_J$. The extension of these definitions to the case of an unbounded operator $\mathfrak{A}$ is now evident: A closed densely defined operator $\mathfrak{A}$ on $\mathcal{H} = \mathcal{G} \oplus \mathcal{G}$ will be called Hamiltonian if $i\mathfrak{A}$ is self-adjoint in the Krein space $\mathcal{K}_{\mathfrak{J}}$ and $\mathfrak{A}$ will be called a non-negative Hamiltonian operator if it is Hamiltonian and $i\mathfrak{A}$ is dissipative in the Krein space $\mathcal{K}_J$. The aim of this note is to give conditions which imply the boundedness of Hamiltonian operators. The main results in this paper, Theorems 5 and 6, show that non-negative

Received by the editors March 13, 2001 and, in revised form, September 28, 2001.
2000 *Mathematics Subject Classification.* Primary 47B50, 46C20, 47B44, 47B25.
This research was supported by grants NWO 047-008-008 and RFBR 99-01-00391.

©2002 American Mathematical Society

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 350, Number 8, August 1998, Pages 3055–3064
S 0002-9947(98)02100-X

HOMOGENEITY IN POWERS OF SUBSPACES OF THE REAL LINE

L. BRIAN LAWRENCE

ABSTRACT. Working in ZFC, we prove that for every zero-dimensional subspace S of the real line, the Tychonoff power ${}^{\omega}S$ is homogeneous (ω denotes the nonnegative integers). It then follows as a corollary that ${}^{\omega}S$ is homogeneous whenever S is a separable zero-dimensional metrizable space. The question of homogeneity in powers of this type was first raised by Ben Fitzpatrick, and was subsequently popularized by Gary Gruenhage and Hao-xuan Zhou.

0. INTRODUCTION

A topological space X is homogeneous if for all $x, y \in X$, there is a homeomorphism $\Phi : X \to X$ with $\Phi(x) = y$. At the opposite extreme, a space X is rigid if the only homeomorphism of X onto itself is the identity function. Let $\mathbb{R}$ denote the real line with the usual topology. Examples of homogeneous spaces include $\mathbb{R}$ and each of the following subspaces: the open unit interval, the rationals, the irrationals, and the Cantor set. Using transfinite recursion and the axiom of choice, it is also possible to construct rigid subspaces of $\mathbb{R}$ (see the proposition below).

A topological space is zero-dimensional if there is a base for the topology consisting of sets that are simultaneously open and closed. For a subspace $S \subseteq \mathbb{R}$, S is zero-dimensional iff there is a dense countable subset of $\mathbb{R}$ lying in the complement of S; it follows that $S \subseteq \mathbb{R}$ is zero-dimensional iff S is homeomorphic to a subspace of the irrationals (usual topology) (see [3], 348). A rigid subspace of $\mathbb{R}$ is necessarily zero-dimensional.

As usual, we let ω denote the set of all nonnegative integers, and for a set S, we let ${}^{\omega}S$ denote $\{x : x \text{ is a function } \& \operatorname{Dom} x = \omega \,\&\, \operatorname{Ran} x \subseteq S\}$ ($\operatorname{Dom} x$ and $\operatorname{Ran} x$ denote the domain and range of x respectively). We assume that every cartesian product of topological spaces carries the Tychonoff topology of pointwise convergence. A power of a topological space S is a Tychonoff product space where every factor is S. Let $\mathbb{P}$ denote the power ${}^{\omega}\omega$ (ω has the discrete topology). Then $\mathbb{P}$ is homeomorphic to the space of irrationals ([3], 348).

Every power of a homogeneous space is of course homogeneous. However, it is possible for homogeneity to hold in a power of a nonhomogeneous factor space. For instance, the Hilbert Cube is homogeneous (O. H. Keller, 1931, [5]); and for any first countable space S in which the isolated points are dense, ${}^{\omega}S$ is homogeneous (D. B. Motorov, 1989, [9]; this result was obtained independently by Gary

Received by the editors September 7, 1994 and, in revised form, June 1, 1995.
1991 *Mathematics Subject Classification.* Primary 54B10; Secondary 54E35, 54F99.
Key words and phrases. Real line, separable metric space, zero-dimensional, subspace, product space, power, homogeneous, rigid.

©1998 American Mathematical Society

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

High-Performance Cryptology on GPUs

Joppe W. Bos

Microsoft Research, Redmond

GTC 2013 – Session S3018

Joint work with the Laboratory for Cryptologic Algorithms, EPFL

Paper SAS054-2014

Advanced Security Configuration Options for SAS® 9.4 Web Applications and Mobile Devices

Heesun Park, SAS Institute Inc., Cary, NC

ABSTRACT

SAS 9.4 has overhauled web authentication schemes, and the integration with enterprise security infrastructure is quite different from that of SAS 9.3. This paper examines advanced security features such as Secure Sockets Layer (SSL) configuration, single sign-on (SSO) support through Integrated Windows authentication (IWA), and third-party security packages like CA SiteMinder and IBM® Tivoli Access Manager WebSEAL. FIPS 140-2 compliance efforts that enforce the use of a stronger encryption algorithm for web communication and the SAS® system itself are also described. The authentication support for mobile devices such as the iPad is different. The secure Wi-Fi connection from a mobile device to the IT internal resources, as well as how it can be safely integrated into the enterprise security configuration by using the same user repository as the SAS web applications, is explained. The configuration example is shown with SAS® Visual Analytics 6.3.

SAS 9.4 MIDDLE TIER AUTHENTICATION CHANGES

Even though it is not visible to most end users of SAS 9.4 web applications, internal user authentication logic for web applications has been overhauled. SAS Logon Manager that handles the user authentication for all SAS web applications, adopted and customized open-source Central Authentication Service (CAS) [1]. CAS, which is similar to Kerberos, is a ticket-based authentication service. After successful initial user authentication through SAS® Metadata Server or through external web authentication, SAS Logon Manager generates and manages CAS tickets for all SAS web applications with user identity that determines the operation permission level. The CAS ticket and SAS metadata based authorization model replaces traditional security role mapping provided for each web application through deployment descriptor (web.xml file) by the web application server.

Another noticeable change is the inclusion of SAS® Web Application Server (called tcServer, it is the enhanced version of Tomcat 7 by VMware) in the product packages. It comes with many enterprise level management features such as SAS® Environment Manager, and it is free. Since SAS has full control of the web application server, we were able to add more features that make external web authentication support more efficient. Java Authentication and Authorization Service (JAAS) is a separate and independent specification that can be integrated with Java Enterprise Edition (JEE) based web application server.

Use of JAAS-based authentication by web application servers is common, but it requires some investment when you try to integrate with third security packages such as CA SiteMinder or IBM Tivoli Access Manager WebSEAL, because you have to license their JAAS based "application server agent", which decrypts the incoming authentication token and initializes JAAS "Subject" for consumption by web applications. Similar functionality can be provided by the internal web application server logic called "Valve". SAS Web Application Server includes SAS developed SiteMinder valve and support of free version of AMTomcatValve from IBM. The valve implementation has less overhead compared to JAAS agent implementation and thus is more efficient.

SECURE SOCKET LAYER BASICS AND CONFIGURATION

SECURE SOCKET LAYER OVERVIEW

When it comes to the protection of data traffic that goes on the unsecured network, use of SSL protocol on top of HTTP (and making it HTTPS) is the first line of defense from any security exposure. SAS 9.4 deployment process includes SSL configuration for some components as options, but it is very important to

SCALE UNIFICATION – A UNIVERSAL SCALING LAW FOR ORGANIZED MATTER

Nassim Haramein,[†] Michael Hyson,[‡] E. A. Rauscher[§]

Abstract. From observational data and our theoretical analysis, we demonstrate that a scaling law can be written for all organized matter utilizing the Schwarzschild condition, describing cosmological to sub-atomic structures. Of interest are solutions involving torque and Coriolis effects in the field equations. Significant observations have led to theoretical and experimental advancement describing systems undergoing gravitational collapse, including vacuum interactions. The universality of this scaling law suggests an underlying polarizable structured vacuum of mini white holes/black holes. We briefly discuss the manner in which this structured vacuum can be described in terms of resolution of scale analogous to a fractal-like scaling as a means of renormalization at the Planck distance. Finally, we describe a new horizon we term the "spin horizon" which is defined as a result of a spacetime torque producing boundary conditions in a magnetohydrodynamic structure.

INTRODUCTION

In astrophysics, black holes have been ubiquitously confirmed from large scale super-giants such as quasars and galactic centers to smaller stellar size black hole systems. These new discoveries represent a long term progress to confirm the 1916 Schwarzschild solution to Einstein's field equations. The observed black hole at the center of the Milky Way galaxy was first discovered by its gravitational influence on nearby stars. So far, black holes seem to have been found at the center of all galaxies that have been carefully examined [1]. Now, quasars and globular clusters, have been found to host large black holes and stellar black holes are well documented [1].

In this paper we develop a scaling law utilizing the Schwarzschild condition as well as discuss charge and rotation within a modified Kerr-Newman metric (the Haramein-Rauscher solution involving torque and Coriolis effects in the field equations [2]) for cosmological, galactic, stellar and micro physical black holes. It is important to note that all observed objects, from macro to micro, are predominantly x-ray emitters, which is typical of black hole horizons. At the horizon the gravitational force balances the electromagnetic radiation, a state previously thought to be only present at cosmogenesis, which implies a continuous creation model. This is based on the topology of "Schwarzschild's zones" generating cells depicting a dynamic expanding and contracting universe first described by Wheeler and Lindquist [3]. Thermodynamic and acoustic processes occupy an important role in energy transfer between gravitational attraction, magnetohydrodynamic (MHD) and electrodynamic repulsion [4]. Solving the collective and coherent behavior of plasma MHD soliton structures, their thermo and acoustic dynamics, results in a good description of the processes occurring externally, near and at the horizons of black holes [4]. A dual brane torus model of a U_4 group and the cuboctahedral cover group is utilized (see Appendix A). This approach leads to a polarized structured vacuum and an extended unified model. This model is a central feature of the Haramеinian topological picture [4, 5, 6].

At the cosmological resolution, plasma dynamics surrounding the event horizon give us a good indication of the fundamental structure underlying the dynamical vacuum state polarization, its relationship to the event horizon [4, 7] and the topology of the spacetime manifold. Some recent observations by the Wide Field Planetary Camera 2 of the Hubble Space Telescope of Supernova SN1987A and Nebula MyCn18 (so-called Hourglass Nebula) and large galactic superstructures display certain qualities that relate to the plasma state field and its interaction with the vacuum structure producing double torus-like dynamics [8, 9, 10].

In this paper, we have developed a scaling law for the universal, galactic, stellar – solar and atomic scale frequencies vs. radius of the system, with the consideration of a fundamental response of these systems within the surrounding structured vacuum polarization, and we briefly discuss a new approach to renormalization. In this paper, we will touch on the details of the field topology and its interaction with the vacuum structure, and focus mostly on describing our scaling law where we compare our scaling rotation to the standard atomic model in which $1A \sim 10^{-8}$ cm. By way of comparison, we find the Big Bang cosmogenic parameters, $R \sim 10^{-33}$cm and $\omega \sim 2 \times 10^{43}$ Hz and the current universe at $R \sim 10^{28}$ cm. We derive a scaling law and discuss possible explanations of the missing

[†] Director of Research, The Resonance Project Foundation, haramein@theresonanceproject.org
[‡] Research Director, Sirius Institute, michaelhyson@yahoo.com
[§] Tecnic Research Laboratory, 3500 S. Tomahawk Road, Bldg. 188, Apache Junction, AZ 85219

Preprint: N. Haramein, M. Hyson, E. A. Rauscher, *Proceedings of The Unified Theories Conference (2008)*. Scale Unification: A Universal Scaling Law for Organized Matter, in Cs Varga, I. Dienes & R.L. Amoroso (eds.)

IWR White Paper

US Army Corps of Engineers

IWR

www.iwr.usace.army.mil

HHL

Center for Scenario Planning

A Scenario-based Approach to Strategic Planning

– Integrating Planning and Process Perspective of Strategy

Prof. Dr. Torsten Wulf, Philip Meissner and Dr. Stephan Stubner

Working Paper 1/2010

Leipzig, March, 25th, 2010

Computational Physics

Prof. Matthias Troyer

ETH Zürich, 2005/2006

On Breaking SAML: Be Whoever You Want to Be

Juraj Somorovsky[1], Andreas Mayer[2], Jörg Schwenk[1], Marco Kampmann[1], and Meiko Jensen[1]

[1]Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany
[2]Adolf Würth GmbH & Co. KG, Künzelsau-Gaisbach, Germany
{*Juraj.Somorovsky, Joerg.Schwenk, Marco.Kampmann, Meiko.Jensen*}*@rub.de*,
Andreas.Mayer@wuerth.com

Abstract

The **S**ecurity **A**ssertion **M**arkup **L**anguage (*SAML*) is a widely adopted language for making security statements about subjects. It is a critical component for the development of federated identity deployments and Single Sign-On scenarios. In order to protect integrity and authenticity of the exchanged SAML assertions, the XML Signature standard is applied. However, the signature verification algorithm is much more complex than in traditional signature formats like PKCS#7. The integrity protection can thus be successfully circumvented by application of different XML Signature specific attacks, under a weak adversarial model.

In this paper we describe an in-depth analysis of 14 major SAML frameworks and show that 11 of them, including Salesforce, Shibboleth, and IBM XS40, have critical XML Signature wrapping (XSW) vulnerabilities. Based on our analysis, we developed an automated penetration testing tool for XSW in SAML frameworks. Its feasibility was proven by additional discovery of a new XSW variant. We propose the first framework to analyze such attacks, which is based on the information flow between two components of the Relying Party. Surprisingly, this analysis also yields efficient and practical countermeasures.

1 Introduction

The **S**ecurity **A**ssertion **M**arkup **L**anguage (*SAML*) is an XML based language designed for making security statements about subjects. SAML assertions are used as security tokens in WS-Security, and in REST based Single Sign-On (SSO) scenarios. SAML is supported by major software vendors and open source projects, and is widely deployed. Due to its flexibility and broad support, new application scenarios are defined constantly.

SAML Assertions. Since SAML assertions contain security critical claims about a subject, the validity of these claims must be certified. According to the standard, this shall be achieved by using XML Signatures, which should either cover the complete SAML assertion, or an XML document containing it (e.g. a SAML Authentication response).

However, roughly 80% of the SAML frameworks that we evaluated could be broken by circumventing integrity protection with novel XML Signature wrapping (XSW) attacks. This surprising result is mainly due to two facts:

- **Complex Signing Algorithm:** Previous digital signature data formats like PKCS#7 and OpenPGP compute a single hash of the whole document, and signatures are simply appended to the document. The XML Signature standard is much more complex. Especially, the position of the signature and the signed content is variable. Therefore, many permutations of the same XML document exist.
- **Unspecified internal interface:** Most SAML frameworks treat the Relying Party (i.e. the Web Service or website consuming SAML assertions) as a single block, assuming a joint common state for all tasks. However, logically this block must be subdivided into the signature verification module (later called RP_{sig}) which performs a cryptographic operation, and the SAML processing module (later called RP_{Claims}) which processes the claims contained in the SAML assertion. Both modules have different views on the assertion, and they typically only exchange a Boolean value about the validity of the signature.

Contribution. In this paper, we present an in-depth analysis of 14 SAML frameworks and systems. During this analysis, we found critical XSW vulnerabilities in 11 of these frameworks. This result is alarming given the importance of SAML in practice, especially since SSO frameworks may become a single point of attack. It clearly indicates that the security implications behind SAML and XML Signature are not understood yet.

GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies

Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici, ***Ben-Gurion University of the Negev***

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/guri

This paper is included in the Proceedings of the 24th USENIX Security Symposium

August 12–14, 2015 • Washington, D.C.

ISBN 978-1-931971-232

Open access to the Proceedings of the 24th USENIX Security Symposium is sponsored by USENIX

The Million-Key Question—Investigating the Origins of RSA Public Keys

Petr Švenda, Matúš Nemec, Peter Sekan, Rudolf Kvašňovský, David Formánek, David Komárek, and Vashek Matyáš, *Masaryk University*

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/svenda

This paper is included in the Proceedings of the 25th USENIX Security Symposium

August 10–12, 2016 • Austin, TX

ISBN 978-1-931971-32-4

Open access to the Proceedings of the 25th USENIX Security Symposium is sponsored by USENIX

Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys

Mathy Vanhoef and Frank Piessens, *Katholieke Universiteit Leuven*

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/vanhoef

This paper is included in the Proceedings of the 25th USENIX Security Symposium

August 10–12, 2016 • Austin, TX

ISBN 978-1-931971-32-4

Open access to the Proceedings of the 25th USENIX Security Symposium is sponsored by USENIX

Understanding the Mirai Botnet

Manos Antonakakis, *Georgia Institute of Technology;* Tim April, *Akamai;* Michael Bailey, *University of Illinois, Urbana-Champaign;* Matt Bernhard, *University of Michigan, Ann Arbor;* Elie Bursztein, *Google;* Jaime Cochran, *Cloudflare;* Zakir Durumeric and J. Alex Halderman, *University of Michigan, Ann Arbor;* Luca Invernizzi, *Google;* Michalis Kallitsis, *Merit Network, Inc.;* Deepak Kumar, *University of Illinois, Urbana-Champaign;* Chaz Lever, *Georgia Institute of Technology;* Zane Ma and Joshua Mason, *University of Illinois, Urbana-Champaign;* Damian Menscher, *Google;* Chad Seaman, *Akamai;* Nick Sullivan, *Cloudflare;* Kurt Thomas, *Google;* Yi Zhou, *University of Illinois, Urbana-Champaign*

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

This paper is included in the Proceedings of the
26th USENIX Security Symposium

August 16–18, 2017 • Vancouver, BC, Canada

ISBN 978-1-931971-40-9

Open access to the Proceedings of the
26th USENIX Security Symposium
is sponsored by USENIX

Detecting Credential Spearphishing Attacks in Enterprise Settings

Grant Ho, *UC Berkeley;* Aashish Sharma, *The Lawrence Berkeley National Laboratory;* Mobin Javed, *UC Berkeley;* Vern Paxson, *UC Berkeley and ICSI;* David Wagner, *UC Berkeley*

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/ho

This paper is included in the Proceedings of the 26th USENIX Security Symposium

August 16–18, 2017 • Vancouver, BC, Canada

ISBN 978-1-931971-40-9

Open access to the Proceedings of the 26th USENIX Security Symposium is sponsored by USENIX

CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management

Adrian Tang, Simha Sethumadhavan, and Salvatore Stolfo, ***Columbia University***

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/tang

This paper is included in the Proceedings of the 26th USENIX Security Symposium

August 16–18, 2017 • Vancouver, BC, Canada

ISBN 978-1-931971-40-9

Open access to the Proceedings of the 26th USENIX Security Symposium is sponsored by USENIX

Physics 195
Course Notes
Second Quantization
030304 F. Porter

1 Introduction

This note is an introduction to the topic of "second quantization", and hence to quantum "field theory". In the Electromagnetic Interactions note, we have already been exposed to these ideas in our quantization of the electromagnetic field in terms of photons. We develop the concepts more generally here, for both bosons and fermions. One of the uses of this new formalism is that it provides a powerful structure for dealing with the symmetries of the states and operators for systems with many identical particles.

2 Creation and Annihilation Operators

We begin with the idea that emerged in our quantization of the electromagnetic field, and introduce operators that add or remove particles from a system, similar to the changing of excitation quanta of a harmonic oscillator.

To follow an explicit example, suppose that we have a potential well, $V(\mathbf{x})$, with single particle eigenstates $\phi_0(\mathbf{x}), \phi_1(\mathbf{x}), \ldots$ Suppose we have an n (identical) boson system, where all n bosons are in the lowest, ϕ_0, level. Denote this state by $|n\rangle$. We assume that $|n\rangle$ is normalized: $\langle n|n\rangle = 1$. Since the particles are bosons, we can have $n = 0, 1, 2, \ldots$, where $|0\rangle$ is the state with no particles (referred to as the "vacuum").

Now define "annihilation" (or "destruction") operators according to:

$$b_0|n\rangle = \sqrt{n}|n-1\rangle \quad (1)$$

$$b_0^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \quad (2)$$

Note that these operators subtract or add a particle to the system, in the state ϕ_0. They have been defined so that their algebraic properties are identical to the raising/lowering operators of the harmonic oscillator. For example, consider the commutator:

$$[b_0, b_0^\dagger]|n\rangle = (b_0 b_0^\dagger - b_0^\dagger b_0)|n\rangle \quad (3)$$

$$= [(n+1) - (n)]\,|n\rangle \quad (4)$$

$$= |n\rangle. \quad (5)$$

Solve the Secular Equations: $\mathcal{H}\Psi = ES\Psi$

Outline:

Introduction
Extended Hückel Molecular Orbital Theory
Instructions for Using the Applet
Frequently Asked Questions
Literature Cited

Introduction

A general eigenvalue problem is given by $\underset{\sim}{A}\ \underset{\sim}{x}_i = \lambda_i\ \underset{\sim}{B}\ \underset{\sim}{x}_i$, where $\underset{\sim}{A}$ and $\underset{\sim}{B}$ are symmetric matrices, and x_i is an eigenvector with eigenvalue λ_i. This applet solves this general matrix equation. While not specific to molecular orbital theory, the applet finds its use primarily in solving the secular equation that arises from extended Hückel molecular orbital theory: $\underset{\sim}{H}\ \underset{\sim}{c}_i = E_i\ \underset{\sim}{S}\ \underset{\sim}{c}_i$. In the secular equation, $\underset{\sim}{H}$ is the matrix of Hamiltonian integrals, $\underset{\sim}{S}$ is the overlap matrix, $\underset{\sim}{c}_i$ are the molecular orbital coefficients, and E_i are the corresponding eigenvalues.

Extended Hückel Molecular Orbital Theory

The extended Hückel method is a useful teaching tool that introduces important concepts used in more rigorous electronic structure methods. Extended Hückel theory is applicable to both σ- and π-molecular orbitals and easily incorporates all the atoms in the periodic table. While not as rigorous as MNDO, AM1, PM3, or *ab initio* methods, extended Hückel calculations are commonly used for an initial approach to polymers, large macrocyclic systems, solids, and surfaces.[1] The first step is to note that the atomic integrals in the secular equations, H_{ii}, are approximately given by valence atomic orbital ionization energies, VOIEs, Table 1.

Table 1*: Valence Orbital Ionization Energies.[2,3]

Atom	1s	2s	2p
H	13.60		
He	24.5		
Li		5.45	3.50
Be		9.30	6.00
B		14.0	8.30
C		19.5	10.7
N		25.5	13.1
O		32.3	15.9
F		40.4	18.7

* Additional values listed in the Applet

These VOIEs are the configuration averaged energy necessary to remove an electron from a specific atomic orbital in a given atom. For example, the VOIE for the 2p-orbital of carbon is the ionization energy for the gas phase process:

SEI
New ways.
New answers.
Annual
Investor
Conference
SEPTEMBER 9-10, 2015 | OAKS, PA

AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—115th Cong., 1st Sess.

H. R. 1628

To provide for reconciliation pursuant to title II of the concurrent resolution on the budget for fiscal year 2017.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by _____

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Better Care Reconciliation Act of 2017".

TITLE I

SEC. 101. ELIMINATION OF LIMITATION ON RECAPTURE OF EXCESS ADVANCE PAYMENTS OF PREMIUM TAX CREDITS.

Subparagraph (B) of section 36B(f)(2) of the Internal Revenue Code of 1986 is amended by adding at the end the following new clause:

A Categorical Semantics of Signal Flow Graphs

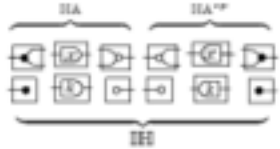
Filippo Bonchi[1], Paweł Sobociński[2] and Fabio Zanasi[1]

[1] ENS de Lyon, Université de Lyon, CNRS, INRIA, France
[2] ECS, University of Southampton, UK

Abstract. We introduce $\mathbb{B}$, a sound and complete graphical theory of vector subspaces over the field of polynomial fractions, with relational composition. The theory is constructed in modular fashion, using Lack's approach to composing PROPs with distributive laws.
We then view string diagrams of $\mathbb{B}$ as generalised stream circuits by using a formal Laurent series semantics. We characterize the subtheory where circuits adhere to the classical notion of signal flow graphs, and illustrate the use of the graphical calculus on several examples.

1 Introduction

We introduce a graphical calculus of string diagrams, which we call *circuits*, consisting of the following constants, sequential ; and parallel $\oplus$ composition.



These circuits can be given a *stream semantics*. The intuition is that wires carry elements of a field $\mathbb{k}$ that enter and exit through boundary ports. In particular, for circuits built from components in the leftmost three columns, which we hereafter refer to as being in $\mathbf{HA}$, the signal enters from the left and exits from the right boundary. Computation in the circuit proceeds synchronously according to a global "clock", where at each iteration fresh elements are processed from input streams on the left and emitted as elements of output streams on the right.

Intuitively, is a *copier*, duplicating its input signal; its counit accepts any signal and discards it, producing no output; is an *adder* that takes two inputs and emits their sum, and its unit constantly outputs the signal 0; is a *delay*, or 1-place buffer that initially holds the 0 value. Finally, is an *amplifier*, multiplying its input by the scalar $k \in \mathbb{k}$. For circuits resulting from the other three columns, $\mathbf{HA}^{\mathrm{op}}$, the signal flows on the opposite direction: from right to left. The behaviour is symmetric. Formally, the stream semantics of circuits in $\mathbf{HA}$ and $\mathbf{HA}^{\mathrm{op}}$ consists of linear transformations of streams.

Sieve Methods

Denis Xavier Charles

Introduction to Sieve Methods

Frank Thorne

March 30, 2006

Introduction

> Silent Bob is Silent

An authentication bypass vulnerability, which will be later known as CVE-2017-5689, was originally discovered in mid-February of 2017 while doing side-research on the internals of Intel ME firmware. The first objects of interest were network services and protocols.

While studying the Intel AMT Implementation and Reference Guide we found out that various AMT features are available through the *AMT* Web-panel, which is supported by the integrated Web server, which listens to ports 16992 and 16993.

To protect the AMT from unauthorized access, the Web server provides several methods of authentication and authorization of a remote user. As stated in Authentication Options section of the «Intel AMT Implementation and Reference Guide»:

> Intel AMT supports both Digest and Kerberos authentication...
>
> An exception to this is the admin account, which always uses digest authentication.
>
> Continuous use of digest authentication implies that each HTTP request must be sent twice, since the first attempt results in a 401 Digest challenge response.

«An admin account which is present by default and always uses digest authentication» seemed like an interesting thing to dig deeper into.

Reverse-engineering the firmware

Take a look at the example of the negotiation between AMT Web server and a remote client:

```
GET /index.htm HTTP/1.1
Host: 192.168.1.2:16992
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.2:16992/logon.htm
Connection: keep-alive

HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest
realm="Digest:048A0000000000000000000000000000",
nonce="Q0UGAAQEAAAV4M41GF4+N15ZafuMWy9J",stale="false",qop="auth"
Content-Type: text/html
Server: AMT
```

Higher-derivative Lagrangians, nonlocality, problems, and solutions

Jonathan Z. Simon*
Department of Physics, University of California, Santa Barbara, California 93106
Received 15 November 1989

Higher-derivative theories are frequently avoided because of undesirable properties, yet they occur naturally as corrections to general relativity and cosmic strings. We discuss some of their more interesting and disturbing problems, with examples. A natural method of removing all the problems of higher derivatives is reviewed. This method of "perturbative constraints" is required for at least one class of higher-derivative theories—those which are associated with nonlocality. Nonlocality often appears in low-energy theories described by effective actions. The method may also be applied to a wide class of other higher-derivative theories. An example system is solved, exactly and perturbatively, for which the perturbative solutions approximate the exact solutions only when the method of "perturbative constraints" is employed. Ramifications for corrections to general relativity, cosmic strings with rigidity terms, and other higher-derivative theories are explored.

I. INTRODUCTION

Theories with higher derivatives (third derivative or higher in time in the equations of motion, second derivative or higher in the Lagrangian) occur naturally for various reasons in different areas of physics. Quite often the higher-derivative terms are added to a more standard lower-derivative theory as a correction. This occurs in general relativity, for instance, where quantum corrections naturally contain higher derivatives of the metric (see, e.g., Birrell and Davies[1], or where nonlinear σ models of string theory predict terms of order R^2 and higher (see, e.g., de Alwis[2]). It occurs in the case of cosmic strings where higher-order corrections, dependent on the "rigidity" of the string, contain higher derivatives,[3,4] and in Dirac's relativistic model of the classical radiating electron.[5] Unlike lower-derivative corrections, however, it is false to assume that adding a higher-derivative correction term with a small coefficient will only perturb the original theory. The presence of an unconstrained higher-derivative term, no matter how small it may naively appear, makes the new theory dramatically different from the original.

Unconstrained higher-derivative theories have very distinctive features. As will be shown below, they have more degrees of freedom than lower-derivative theories, and they lack a lower-energy bound. There is nothing mathematically inconsistent with these features, but they make two almost identical-looking theories, one a lower-derivative theory and the other the same theory with a higher-derivative correction added, very different. The lack of a lowest-energy state for the higher-derivative theory is probably the most dramatic change. This always occurs when higher-derivative terms are present (assuming no degeneracy or constraints), independently of how small their coefficients are. The addition of more degrees of freedom might be physically more accurate, but then it means that the original lower-derivative theory was incomplete and missing (the most interesting) new families of solutions. It is particularly disturbing if there is a progression of higher-order, higher-derivative corrections, each system of which has more and more degrees of freedom. Classically, more degrees of freedom means that more initial data are required to specify motion. Quantum mechanically this means that, for a particle, x and $\dot{x}$ now commute since they are freely specifiable, and it becomes possible to measure the position and velocity at the same time. The momentum conjugate to x, π_x, still does not commute with x: $[x,\pi_x]=i\hbar$, but $\pi_x \neq m\dot{x}$. From the path integral point of view, the paths which dominate the functional integral are of a different class where once they were nowhere differentiable, now they are everywhere once differentiable. Examples of all these types of behavior are presented below. No familiarity with any of the properties of higher-derivative theories is assumed.

There is a large class of theories naturally containing higher derivatives that do not suffer the above problems. Nonlocal theories, where the nonlocality is regulated by a naturally small parameter, have perturbation expansions with higher derivatives. They avoid the above problems because they are constrained systems. They contain implicit constraints which keep the number of degrees of freedom constant and maintain a lower-energy bound. Higher-derivative theories that are truncated expansions of a nonlocal theory also avoid these problems, once the proper constraints are imposed. Any theory for which the higher-derivative terms have been added as small corrections can be treated in the same manner, also avoiding the above problems.

Nonlocality naturally appears in effective theories, valid only in a low-energy limit and derived from a larger theory with some degrees of freedom frozen out. A good example is Wheeler-Feynman electrodynamics[6] in which the degrees of freedom of the electromagnetic field are frozen out. For two particles of mass m,

 © 1990 The American Physical Society

Simplified Set Theory

(Herbert E. Müller, october 2016, herbert-mueller.info)

In set theory one distinguishes between an element e (which cannot be broken up into parts) and the set with the element e, which is written {e}. e and {e} are not the same thing. One says: "e is an element of the set {e}", or "the set {e} contains the element e". Thus a kind of hierarchy is introduced: e is "below", {e} is "above". One can go on and introduce higher levels: {{e}}, {{{e}}} etc. Figuratively speaking a thing is wrapped, then wrapped once more, then - why not? - once more etc. Historically this wrapping led to objects such as the empty set {} = Ø (consists only of wrapping), the set of all sets (self-contradictory), or Neumanns axiomatisation of the natural numbers: 0:=Ø, 1:= {Ø}, 2:= {Ø, {Ø}} usw. (now try to write the set for the number 3 😊).

This wrapping business may be sensible for mathematicians - it must be, since many genius mathematicians do it like this since over a hundred years - but for engineers and physicists it is - pardon me - nonsense. Now this is my proposal how to simplify set theory for us non-mathematicians: abolish the difference between an element e and the elementary set {e}. Henceforth the element e is already a set. The curly brackets {} can be read as union of elementary sets: {e,f} = e∪f. The expression {e} doesn't make sense anymore, since for a union you need at least two things. (But one may write: e = {e,Ø}.) The solution of an equation could be the set L = Ø or L = 5 or L = {−2,5}. Here, the only difference to the usual set theory is L = 5 instead of L = {5}. The set of all sets becomes new the set of all things. It is "everything", but it is not a new thing by itself. (You can't wrap everything.) The empty set is "nothing". (There is no wrapping anymore.)

Is this simplified set theory sufficient for non-mathematicians? I believe yes. What's your opinion?

CA SiteMinder®

SAML Affiliate Agent Guide

6.x QMR 6

CA SiteMinder®

Web Agent Guide

r6.x QMR6

Second Edition

CA SiteMinder®

Web Agent Installation Guide for Apache-based Servers

r12.5

2nd Edition

CA SiteMinder®

Web Agent Installation Guide

r12.0 SP3

6th Edition

CA SiteMinder®

Web Agent Release Notes

r12.0 SP3

Fourth Edition

Mismorphism: a Semiotic Model of Computer Security Circumvention

S.W. Smith[1], R. Koppel[2], J. Blythe[3], V. Kothari[1]
[1]Dartmouth College, [2]University of Pennsylvania, [3]USC ISI
Contact author: sws@cs.dartmouth.edu

Abstract

In real world domains, from healthcare to power to finance, computer systems are deployed with the intention of streamlining and improving the activities of human agents in the corresponding non-cyber worlds. However, talking to actual users (instead of just computer security experts) reveals endemic circumvention of the computer-embedded rules. Well-intentioned users, trying to get their jobs done, systematically work around security and other controls embedded in their IT systems. This paper reports on our work compiling a large corpus of such incidents and developing a model based on *semiotic triads* to examine security circumvention. This model suggests that *mismorphisms*—mappings that *fail* to preserve structure—lie at the heart of circumvention scenarios; differential perceptions and needs explain users' actions. This paper supports this claim with empirical data from the corpus.

Keywords

Circumvention, authentication, authorization, usability.

1. Introduction

Users systematically work around security controls. The security community can pretend this does not happen, but it does. This paper reports on research addressing this problem via observation and grounded theory (Bernard and Ryan, 2010; Charmaz, 2003; Pettigrew, 2000). Rather than assuming that users behave perfectly or that only bad users do bad things, this approach instead observes and records what really goes on compared to the various expectations. Then, after data items are reviewed, structure and models are developed, and additional data is brought in to support, reject, and refine these models. Over the last several years, via interviews, observations, surveys, and literature searches, the authors have explored the often-tenuous relationship among computer rules, users' needs, and designers' goals of computer systems. A corpus of hundreds of circumvention and unusability scenarios has been collected and analyzed. This corpus cataloged close to 300 examples of these "misunderstandings" and the circumventions users undertook to accomplish their needed tasks. The examples were derived from 285 different sources and categorized into 60 fine-grained codes. Because several examples reflect multiple codes, there were 646 applications of the codes linked to the examples.

Semiotic triads, proposed almost a century ago (e.g., Ogden and Richards, 1927), offer models to help understand why human agents so often circumvent computer-embedded

Factoring RSA keys from certified smart cards: Coppersmith in the wild

Daniel J. Bernstein[1,2], Yun-An Chang[3], Chen-Mou Cheng[3], Li-Ping Chou[4], Nadia Heninger[5], Tanja Lange[2], and Nicko van Someren[6]

[1] Department of Computer Science, University of Illinois at Chicago, USA
djb@cr.yp.to
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, the Netherlands
tanja@hyperelliptic.org
[3] Research Center for Information Technology Innovation
Academia Sinica, Taipei, Taiwan
{ghfjdksl,doug}@crypto.tw
[4] Department of Computer Science and Information Engineering
Chinese Culture University, Taipei, Taiwan
randomalg@gmail.com
[5] Department of Computer and Information Science, University of Pennsylvania
nadiah@cis.upenn.edu
[6] Good Technology Inc.
nicko@good.com

Abstract. This paper explains how an attacker can efficiently factor 184 distinct RSA keys out of more than two million 1024-bit RSA keys downloaded from Taiwan's national "Citizen Digital Certificate" database. These keys were generated by government-issued smart cards that have built-in hardware random-number generators and that are advertised as having passed FIPS 140-2 Level 2 certification.

These 184 keys include 103 keys that share primes and that are efficiently factored by a batch-GCD computation. This is the same type of computation that was used last year by two independent teams (USENIX Security 2012: Heninger, Durumeric, Wustrow, Halderman; Crypto 2012: Lenstra, Hughes, Augier, Bos, Kleinjung, Wachter) to factor tens of thousands of cryptographic keys on the Internet.

The remaining 81 keys do not share primes. Factoring these 81 keys requires taking deeper advantage of randomness-generation failures: first using the shared primes as a springboard to characterize the failures, and then using Coppersmith-type partial-key-recovery attacks. This is the first successful public application of Coppersmith-type attacks to keys found in the wild.

Keywords: RSA, smart cards, factorization, Coppersmith, lattices

This work was supported by NSF (U.S.) under grant 1018836, by NWO (Netherlands) under grants 639.073.005 and 040.09.003, and by NSC (Taiwan) under grant 101-2915-I-001-019. Cheng worked on this project while at Technische Universität Darmstadt under the support of Alexander von Humboldt-Stiftung. Heninger worked on this project while at Microsoft Research New England. Permanent ID of this document: 278505a8b16015f4fd8acae818080edd. Date: 2013.09.16.

User Circumvention of Cybersecurity: A Cross-Disciplinary Approach

Sean W. Smith

Professor---Department of Computer Science
Director---Institute for Security, Technology, and Society

Dartmouth College

24 April 2017

CA SiteMinder® Web Services Security

Programming Guide for Java

12.52

Social Anarchism and Organisation

by Federação Anarquista do Rio de Janeiro - FARJ

Translation by Jonathan Payn

Davison v. Loudoun County Board of Supervisors et al Doc. 132

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

BRIAN C. DAVISON,	)	
	)	
Plaintiff,	)	
	)	
v.	)	1:16cv932 (JCC/IDD)
	)	
LOUDOUN COUNTY BOARD OF SUPERVISORS, et al.,	)	
	)	
	)	
Defendants.	)	

MEMORANDUM OF DECISION

This case raises important questions about the constitutional limitations applicable to social media accounts maintained by elected officials. Plaintiff *pro se* Brian C. Davison brings suit against Defendant Phyllis J. Randall, Chair of the Loudoun County Board of Supervisors, under 42 U.S.C. § 1983. Plaintiff's claims stem from an incident during which Defendant banned him from her Facebook page - titled "Chair Phyllis J. Randall" - for a period of roughly 12 hours. Plaintiff alleges that this violated his rights to free speech and due process under the United States and Virginia Constitutions. A bench trial was held on May 16, 2017, and the Court took the matter under advisement.

The Court makes the following findings of fact and, for the reasons set forth below, concludes that: (1) Defendant

Dockets.Justia.com

The notion of space in mathematics

Matilde Marcolli

general audience lecture at Revolution Books
Berkeley 2009

SPECTER OPS

Subverting Trust in Windows

Matt Graeber

The statistics of polynomial roots

Herbert E. Müller
Published in 2014 on http://herbert-mueller.info/

Abstract

A population of real numbers can be described summarily by its statistics *mean value*, *standard deviation*, *skewness* and *kurtosis*. How can one find a population of N real numbers to given statistics? Answer: construct a polynomial of degree N with coefficients that depend on the statistics in a certain way. The roots of this polynomial are the sought population.

Contents

1 Two Problems 2

2 The statistics of a population in R 2

3 The statistics of polynomial roots 3
- 3.1 Roots of a polynomial of degree N . . . 3
- 3.2 Roots of a quadratic polynomial . . . 4
- 3.3 Roots of a cubic polynomial . . . 5
- 3.4 Roots of a quartic polynomial . . . 5
- 3.5 Allowed values of Skewness and Kurtosis . . . 6

4 Examples 7

The figures in this article were created with the mathematics freeware OCTAVE (GNU Octave, J. W. Eaton, D. Bateman & S. Hauberg, http://www.octave.org.). I thank the Octave development community for their excellent work.

A Classification of Pointcut Language Constructs

Maximilian Stoerzer
University of Passau
Passau, Germany
stoerzer@fmi.uni-passau.de

Stefan Hanenberg
University of Duisburg-Essen
Essen, Germany
shanenbe@cs.uni-essen.de

ABSTRACT

Aspect-oriented systems provide *pointcut languages* in order to specify selection criteria for join points which in turn will be adapted. However, a closer look into current pointcut languages reveals that there are large differences among them. Consequently different aspect-oriented system permit to specify different selection criteria. This also means that it is in general hard to state whether a certain aspect-oriented system is adequate for a given problem without detailed system knowledge.

This paper analyzes and classifies pointcut language constructs based on the objects they reason on. Based on this analysis, we propose three conceptual classes of pointcut constructs. These classes represent an abstract framework for pointcut languages allowing to better understand and compare existing approaches. They also describe a design space for potential new language constructs.

1. MOTIVATION

Aspect Oriented Programming (AOP) as first introduced in [13] addresses the problem of *crosscutting concerns*. The term crosscutting concern describes parts of a software system that logically belong to one single module, but which cannot be modularized due to limited abstractions of the underlying programming language. Aspect-oriented software aims to overcome the problem of crosscutting concerns by introducing a new kind of module - the aspect.

Aspects extend the underlying application by providing additional functionality "at certain points". These points are called *join points* in the aspect-oriented terminology. In order to specify *where* aspects extend the base application, aspect-oriented systems provide language constructs that permit to *select* those join points where aspects should be woven to. In correspondence to [12, 6, 11] the term pointcut language is used to describe these selection languages. In order to specify how a certain selected join point should be adapted, aspect-oriented systems provide additional language constructs like *advice* in AspectJ.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
SPLAT March 14-18, 2005, Chicago, Illinois, USA
Copyright 200X ACM X-XXXXX-XX-X/XX/XX ...$5.00.

Meanwhile, there are a number of systems available permitting to develop software in an aspect-oriented way, like AspectJ [13, 12], Hyper/J [9, 4], AspectS [11] or Sally [8]. Although all of them provide aspect-oriented features – the selection and adaption of join points – there are a number of differences among them.

First, different aspect-oriented systems provide *different kinds of join points*. For example, AspectJ permits to select those points in the execution of a program where an object's field value is set. Approaches like for example Hyper/J or AspectS do not permit to select these kinds of join points.

Second, the features distinctive pointcut languages in current approaches provide to select join points differ. For example, the `cflow`-construct in AspectJ (allowing to select join points based on properties of the call-stack) is a feature that is not directly available in Hyper/J or Sally.

Third, different aspect-oriented systems differ in the kind of adaptations they provide for each kind of join point. For example, AspectJ provides the `proceed`-construct within `around`-advice which permits to decide at runtime whether or not execution should proceed with the original join point. A similar join point adaptation does not exist for example in Hyper/J.

These different facets of aspect-oriented systems make it hard to compare them. As a consequence, it is hardly possible to determine whether or not a certain aspect can easily be implemented in a given system. Furthermore, whenever a new proposal for a language constructs appears, it is hard to determine whether this feature differs *conceptually* from known ones. The overall problem is that conceptual models are missing that permit to compare different aspect-oriented systems.

In this paper we put the focus the different pointcut language constructs and abstract as far as possible from the underlying join point model and the adaption mechanism. We propose a classification of pointcut language constructs (pointcut constructs for short) which provides a conceptual view on them. These classes also permit to classify aspect-oriented systems based on the features provided by their pointcut languages. Furthermore, they represent an abstract, general framework for the development of pointcut languages.

In section 2 we briefly discuss different facets of aspect-oriented systems and introduce a simple execution model our classification uses. In section 3 we introduce our classification of pointcut constructs. Section 4 applies the classification to a number of aspect-oriented systems - namely AspectJ, Hyper/J, Sally and AspectS. After referring to re-

CA Siteminder Web Access Manager R12 SP1-CR3 Security Target

Version 0.8
May 29, 2009

Prepared for:
CA
100 Staples Drive
Framingham, MA 01702

Prepared by:
Booz Allen Hamilton
Common Criteria Testing Laboratory
900 Elkridge Landing Road, Suite 100
Linthicum, MD 21090-2950

Nine formulations of quantum mechanics

Daniel F. Styer,[a)] Miranda S. Balkin, Kathryn M. Becker, Matthew R. Burns, Christopher E. Dudley, Scott T. Forth, Jeremy S. Gaumer, Mark A. Kramer, David C. Oertel, Leonard H. Park, Marie T. Rinkoski, Clait T. Smith, and Timothy D. Wotherspoon
Department of Physics, Oberlin College, Oberlin, Ohio 44074

(Received 18 July 2001; accepted 29 November 2001)

Nine formulations of nonrelativistic quantum mechanics are reviewed. These are the wavefunction, matrix, path integral, phase space, density matrix, second quantization, variational, pilot wave, and Hamilton–Jacobi formulations. Also mentioned are the many-worlds and transactional interpretations. The various formulations differ dramatically in mathematical and conceptual overview, yet each one makes identical predictions for all experimental results. © 2002 *American Association of Physics Teachers.*
[DOI: 10.1119/1.1445804]

I. WHY CARE ABOUT VARIOUS FORMULATIONS?

A junior-level classical mechanics course devotes a lot of time to various formulations of classical mechanics—Newtonian, Lagrangian, Hamiltonian, least action, and so forth (see Appendix A). But not a junior-level quantum mechanics course! Indeed, even graduate-level courses emphasize the wavefunction formulation almost to the exclusion of all variants. It is easy to see why this should be so—learning even a single formulation of quantum mechanics is difficult enough—yet at the same time students must wonder why it is so important to learn several formulations of classical mechanics but not of quantum mechanics. This article surveys nine different formulations of quantum mechanics. It is a project of the Spring 2001 offering of Oberlin College's Physics 412, "Applied Quantum Mechanics."

Why should one care about different formulations of mechanics when, in the end, each provides identical predictions for experimental results? There are at least three reasons. First, some problems are difficult in one formulation and easy in another. For example, the Lagrangian formulation of classical mechanics allows generalized coordinates, so it is often easier to use than the Newtonian formulation. Second, different formulations provide different insights.[1] For example, the Newtonian and least action principles provide very different pictorializations of "what's really going on" in classical mechanics. Third, the various formulations are variously difficult to extend to new situations. For example, the Lagrangian formulation extends readily from conservative classical mechanics to conservative relativistic mechanics, whereas the Newtonian formulation extends readily from conservative classical mechanics to dissipative classical mechanics. In the words of the prolific chemist E. Bright Wilson:[2]

> "I used to go to [J. H. Van Vleck] for quantum mechanical advice and found him always patient and ready to help, sometimes in a perplexing flow of mixed wave mechanical, operator calculus, and matrix language which often baffled this narrowly Schrödinger-equation-oriented neophyte. I had to learn to look at things in these alternate languages and, of course, it was indispensable that I do so."

Any attempt to enumerate formulations must distinguish between "formulations" and "interpretations" of quantum mechanics. Our intent here is to examine only distinct mathematical formulations, but the mathematics of course influences the conceptual interpretation, so this distinction is by no means clear cut,[3] and we realize that others will draw boundaries differently. Additional confusion arises because the term "Copenhagen interpretation" is widely used but poorly defined: For example, of the two primary architects of the Copenhagen interpretation, Werner Heisenberg maintained that[4] "observation of the position will alter the momentum by an unknown and undeterminable amount," whereas Niels Bohr[5] "warned specifically against phrases, often found in the physical literature, such as 'disturbing of phenomena by observation.' "

II. CATALOG OF FORMULATIONS

A. The matrix formulation (Heisenberg)

The matrix formulation of quantum mechanics, developed by Werner Heisenberg in June of 1925, was the first formulation to be uncovered. The wavefunction formulation, which enjoys wider currency today, was developed by Erwin Schrödinger about six months later.

In the matrix formulation each mechanical observable (such as the position, momentum, or energy) is represented mathematically by a matrix (also known as "an operator"). For a system with N basis states (where in most cases $N=\infty$) this will be an $N\times N$ square Hermitian matrix. A quantal state $|\phi\rangle$ is represented mathematically by an $N\times 1$ column matrix.

Connection with experiment. Suppose the measurable quantity $\mathcal{A}$ is represented by the operator $\hat{A}$. Then for any function $f(x)$ the expectation value for the measurement of $f(\mathcal{A})$ in state $|\phi\rangle$ is the inner product

$$\langle\phi|f(\hat{A})|\phi\rangle. \tag{1}$$

Because the above statement refers to $f(\mathcal{A})$ rather than to $\mathcal{A}$ alone, it can be used to find uncertainties [related to $f(\mathcal{A})=\mathcal{A}^2$] as well as expectation values. Indeed, it can even produce the eigenvalue spectrum, as follows:[6] Consider a set of real values $a_1, a_2, a_3, \ldots$, and form the non-negative function

$$g(x)=(x-a_1)^2(x-a_2)^2(x-a_3)^2\cdots. \tag{2}$$

Mathematical Surveys and Monographs

Volume 151

The Geometry of Heisenberg Groups

With Applications in Signal Theory, Optics, Quantization, and Field Quantization

Ernst Binz
Sonja Pods

with an Appendix by
Serge Preston

American Mathematical Society

Notes on Seiberg-Witten Theory

Liviu I. Nicolaescu

SymbOS

Installation and user manual for SymbOS 3.0

Z80 based multitasking operating system

MSX AMSTRAD ENTERPRISE SymbOS

Warwick Symposium on Geometric Mechanics and Symmetry GR/R09619/01

FINAL REPORT

October 2003

Contents

1 Overview **1**

2 The Programme **2**
2.1 Schools . . . 2
2.1.1 Mechanics and Symmetry European Summer School: 2-15 September 2001 . . . 2
2.1.2 Semi-Classical and Quantum Multibody Systems: 18-22 March 2002 . . . 3
2.2 Workshops at Warwick . . . 4
2.2.1 Geometry and Symmetry in Continuum Mechanics: 9-15 December 2001 . . . 4
2.2.2 Semi-Classical and Quantum Multibody Systems: 24-27 March 2002 . . . 5
2.2.3 Classical N-Body Systems and Applications: 14-20 April 2002 . . . 5
2.2.4 Geometry, Symmetry and Mechanics II: 21-27 July 2002 . . . 6
2.2.5 Calculus of Variations: 15-18 May 2003 . . . 6
2.3 Outreach: Workshops elsewhere in the UK . . . 7
2.3.1 Astrodynamics: 22-23 April 2002, University of Surrey . . . 7
2.3.2 Simulation Algorithms for N-Body Problems: 25-26 April 2002, University of Leicester . . . 7
2.3.3 Geometry of Momentum Maps and Hamiltonian Dynamics: 3-5 July 2002, UMIST . . . 7

3 Publications **8**
3.1 Papers on talks given during the Symposium . . . 8
3.2 Papers arising from discussions and work conducted during the Symposium . . . 10

4 Participants **13**

5 Selected Comments from Participants **14**

1 Overview

The 2001-2002 Warwick Symposium was on *Geometric Mechanics and Symmetry*. The principal organiser was Mark Roberts (Warwick/Surrey), assisted by a Scientific Advisory Board: Tom Bridges (Surrey), Richard Cushman (Utrecht), Jeroen Lamb (Imperial), Ben Leimkuhler (Leicester), Robert Littlejohn (Berkeley), Jerry Marsden (Caltech), Ken Meyer (Cincinnati), James Montaldi (UMIST), Tudor Ratiu (Lausanne) and Gregor Tanner (Nottingham). Altogether there were over 200 participants (see list in Section 4), of whom approximately 80 were from the UK.

The Symposium focused on the symplectic and differential geometry of symmetric Hamiltonian systems and applications of geometry and symmetry techniques to the classical, semiclassical and quantum mechanics of N-body problems (gravitational, atomic, molecular) and to fluid mechanics. The Symposium began with a European Summer School held in France, followed by a further Spring School and four workshops at Warwick. In addition three satellite workshops were held at Surrey, Leicester and UMIST. These were 'peaks' within a sea of research activity, seminars etc that took place throught the year and which continued into the year 2002-2003. During the second year the Symposium grant also provided partial support for a workshop on the Calculus of Variations at Warwick. Details of all the Schools and Workshops are given below.

Reference: Chester, M. (2002) Is symmetry identity?, *International Studies in the Philosophy of Science* 16, 111–124

Is symmetry identity?

Marvin Chester

Physics emeritus, UCLA, Los Angeles, California, USA

Abstract *Wigner found unreasonable the "effectiveness of mathematics in the natural sciences". But if the mathematics we use to describe nature is simply a coded expression of our experience then its effectiveness is quite reasonable. Its effectiveness is built into its design. We consider group theory, the logic of symmetry. We examine the premise that symmetry is identity; that group theory encodes our experience of identification; that symmetry is so elemental that it coincides with the concept of identity itself. To decide whether group theory describes the world in such an elemental way we catalogue the detailed correspondence between elements of the physical world and elements of the formalism. Providing an unequivocal match between concept and mathematical statement completes the case. It makes effectiveness appear reasonable. The case that symmetry is identity is a strong one but it is not complete. The further validation required suggests that unexpected entities might be describable by the irreducible representations of group theory.*

Windows for Reverse Engineers

- **T-110.6220 Special Course in Information Security**

Kimmo Kasslin, 26th Feb 2014

F-Secure.

Taking Back Control for Brexit and Beyond

Delegated Legislation, Parliamentary Scrutiny and the European Union (Withdrawal) Bill

September 2017

HANSARD SOCIETY

The Jhanas

By Ajahn Brahmavamso

Buddhist Fellowship
Singapore

www.buddhistfellowship.org

RF

Resolution Foundation

REPORT

The Living Standards Audit 2017

Adam Corlett, Stephen Clarke, Dan Tomlinson

July 2017

The Market for "Lemons": Quality Uncertainty and the Market Mechanism

George A. Akerlof

The Quarterly Journal of Economics, Vol. 84, No. 3. (Aug., 1970), pp. 488-500.

Stable URL:
http://links.jstor.org/sici?sici=0033-5533%28197008%2984%3A3%3C488%3ATMF%22QU%3E2.0.CO%3B2-6

The Quarterly Journal of Economics is currently published by The MIT Press.

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at http://www.jstor.org/about/terms.html. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at http://www.jstor.org/journals/mitpress.html.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

The JSTOR Archive is a trusted digital repository providing for long-term preservation and access to leading academic journals and scholarly literature from around the world. The Archive is supported by libraries, scholarly societies, publishers, and foundations. It is an initiative of JSTOR, a not-for-profit organization with a mission to help the scholarly community take advantage of advances in technology. For more information regarding JSTOR, please contact support@jstor.org.

http://www.jstor.org
Mon Mar 3 14:37:00 2008

KASPERSKY lab

GREAT

THE DUQU 2.0

Technical Details

Version: 2.1 (11 June 2015)

www.kaspersky.com

Theory of Electromagnetic Fields

Andrzej Wolski
University of Liverpool, and the Cockcroft Institute, UK

Abstract

We discuss the theory of electromagnetic fields, with an emphasis on aspects relevant to radiofrequency systems in particle accelerators. We begin by reviewing Maxwell's equations and their physical significance. We show that in free space, there are solutions to Maxwell's equations representing the propagation of electromagnetic fields as waves. We introduce electromagnetic potentials, and show how they can be used to simplify the calculation of the fields in the presence of sources. We derive Poynting's theorem, which leads to expressions for the energy density and energy flux in an electromagnetic field. We discuss the properties of electromagnetic waves in cavities, waveguides and transmission lines.

1 Maxwell's equations

Maxwell's equations may be written in differential form as follows:

$$\nabla \cdot \vec{D} = \rho, \tag{1}$$

$$\nabla \cdot \vec{B} = 0, \tag{2}$$

$$\nabla \times \vec{H} = \vec{J} + \frac{\partial \vec{D}}{\partial t}, \tag{3}$$

$$\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}. \tag{4}$$

The fields $\vec{B}$ (magnetic flux density) and $\vec{E}$ (electric field strength) determine the force on a particle of charge q travelling with velocity $\vec{v}$ (the Lorentz force equation):

$$\vec{F} = q\left(\vec{E} + \vec{v} \times \vec{B}\right).$$

The electric displacement $\vec{D}$ and magnetic intensity $\vec{H}$ are related to the electric field and magnetic flux density by the *constitutive relations*:

$$\vec{D} = \epsilon \vec{E},$$
$$\vec{B} = \mu \vec{H}.$$

The electric permittivity ϵ and magnetic permeability μ depend on the medium within which the fields exist. The values of these quantities in vacuum are fundamental physical constants. In SI units:

$$\mu_0 = 4\pi \times 10^{-7}\,\mathrm{Hm}^{-1},$$
$$\epsilon_0 = \frac{1}{\mu_0 c^2},$$

where c is the speed of light in vacuum. The permittivity and permeability of a material characterize the response of that material to electric and magnetic fields. In simplified models, they are often regarded as constants for a given material; however, in reality the permittivity and permeability can have a complicated dependence on the fields that are present. Note that the *relative permittivity* ϵ_r and the *relative permeability* μ_r are frequently used. These are dimensionless quantities, defined by:

$$\epsilon_r = \frac{\epsilon}{\epsilon_0}, \quad \mu_r = \frac{\mu}{\mu_0}. \tag{5}$$

THÈSE

en vue d'obtenir le grade de

Docteur de l'Université de Lyon

délivré par l'École Normale Supérieure de Lyon

Discipline : Informatique

Laboratoire de l'Informatique du Parallélisme

École Doctorale en Informatique et Mathématiques de Lyon

présentée et soutenue publiquement le 5 Octobre 2015
par Monsieur Fabio ZANASI

Interacting Hopf Algebras

the theory of linear systems

Directeurs de thèse :	M.	Filippo	BONCHI	
	M.	Daniel	HIRSCHKOFF	
Après l'avis de :	M.	Samson	ABRAMSKY	
	M.	Pierre-Louis	CURIEN	
	M.	Peter	SELINGER	
Devant le jury composée de :	M.	Samson	ABRAMSKY	*Rapporteur*
	M.	Filippo	BONCHI	*Directeur*
	M.	Pierre-Louis	CURIEN	*Rapporteur*
	M.	Daniel	HIRSCHKOFF	*Directeur*
	M.	Samuel	MIMRAM	*Examinateur*
	M.	Prakash	PANANGADEN	*Examinateur*

Supersymmetric Partition Functions in the AdS/CFT Conjecture

A dissertation presented

by

Suvrat Raju

to

The Department of Physics

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in the subject of

Physics

Harvard University

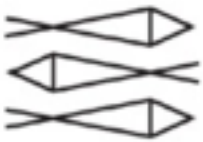
Cambridge, Massachusetts

June 2008

THE SPIRIT CATCHES YOU AND YOU FALL DOWN

A HMONG CHILD,
HER AMERICAN DOCTORS,
AND THE COLLISION OF TWO CULTURES

ANNE FADIMAN



Integer Module LWE key exchange and encryption: The three bears (draft)

Mike Hamburg*
might add Hart Montgomery and/or Arnab Roy†

September 12, 2017

Abstract

We propose a new post-quantum key exchange algorithm based on the integer module learning with errors (I-MLWE) problem. Our ThreeBears algorithm is simple and performant, but our main goal is to suggest MLWE over a generalized Mersenne field instead of a polynomial ring. We also show how to secure the system against chosen ciphertext attacks so that it can be used for public-key encryption.

1 Introduction

All widely-deployed key exchange and public-key encryption algorithms are threatened by the possibility of a quantum computer powerful enough to run Shor's algorithm [33]. Consequently, there is a growing interest in developing a suite of "post-quantum" algorithms which would resist attack by these computers [25]. The most common approaches to addressing this threat rely on the hardness of lattice problems, including variants such as learning

*Rambus Security Division
†Fujitsu research

Manipulating Light with a Magnetic Field

Bart A. van Tiggelen[1] and Geert L. J. A. Rikken[2]

[1] CNRS/Laboratoire de Physique et Modélisation des Milieux Condensés
Université Joseph Fourier, Maison des Magistères,
B.P. 166, 38042 Grenoble, France
tiggelen@belledonne.polycnrs-gre.fr
[2] Grenoble High Magnetic Field Laboratory, Max Planck Institut für
Festkörperforschung/CNRS, B.P. 166, 38042 Grenoble, France

Abstract. We review our theoretical and experimental work done on light propagation and scattering in magnetic fields.

1 Introduction

For more than one century, we have known that Maxwell's equations provide a complete description of the propagation of classical electromagnetic waves. For applications in daily life, it has become customary to describe the interaction of matter on a macroscopic level, i.e., without worrying about individual atoms, but looking only at charge distributions on scales large compared to the atomic scale. Microscopic charges and currents are described by the polarization density vector $\boldsymbol{P}$ and the magnetization $\boldsymbol{M}$. It is important to realize that this description is only approximate. Cases are known for which the macroscopic Maxwell equations seem to break down since they do not predict the observed behavior [1,2,3]. Macroscopically, it is still possible to consider a charge density ρ and a current density $\boldsymbol{J}$, but we will focus on dielectric materials for which both of them vanish.

A solution of Maxwell's equations becomes feasible when so-called *constitutive* relations are put forward that relate the microscopic parameters $\boldsymbol{P}$ and $\boldsymbol{M}$ to the macroscopic electromagnetic fields $\boldsymbol{E}$ and $\boldsymbol{B}$. Constitutive relations are subject to symmetry relations [4]. For instance $\boldsymbol{P}$ is, like the electrical field $\boldsymbol{E}$, a polar (parity-odd) vector that changes sign upon space inversion. On the other hand, the magnetic field $\boldsymbol{B}$ is a pseudovector, invariant under a space inversion, but variant upon time-reversal. One symmetry allowed, a constitutive relation for the polarization density $\boldsymbol{P}$ could be [4]

$$\boldsymbol{P} = \chi_0 \boldsymbol{E} + \chi_1 \partial_t \boldsymbol{E} \times \boldsymbol{B} + \chi_2 (\boldsymbol{B} \cdot \boldsymbol{B}) \boldsymbol{E} + \chi_3 (\boldsymbol{E} \cdot \boldsymbol{B}) \boldsymbol{B} + \cdots . \tag{1}$$

For simplicity, we have adopted an isotropic medium so that all constitutive parameters χ_n are scalars and not second-rank tensors. In the above equation, many other terms are possible, and we have — for future use — just collected the terms linear in the electrical field and without time derivatives of the magnetic field. They are still nonlinear in the magnetic field, which complicates

V. M. Shalaev (Ed.): Optical Properties of Nanostructured Random Media,
Topics Appl. Phys. **82**, 275–302 (2002)
© Springer-Verlag Berlin Heidelberg 2002

The Arrow of Time in Physics

David Wallace

April 5, 2012

1 Introduction

Essentially any process in physics can be described as a sequence of physical states of the system in question, indexed by times. Some such processes, even at the macroscopic, everyday level, do not appear in themselves to pick out any difference between past and future: the sequence run backwards is as legitimate a physical process as the original. Consider, for instance,a highly elastic ball bouncing back and forth, or the orbits of the planets. If these processes — in isolation — were filmed and played to an audience both forwards and backwards, there would be no way for the audience to know which was which.

But *most* physical processes are not like that. The decay of radioactive elements, the melting of ice in a glass of water, the emission of light by a hot object, the slowing down by friction of a moving object, nuclear or chemical reactions ... each of these processes seems to have a direction to it. None of them, run backwards, is a physical process that we observe in nature; any of them, if filmed and played backwards, could easily be identified as incorrect.[1] In the standard terminology, these processes define *arrows of time*.

So: some physical processes are undirected in time, but most are directed. So what? The problem is that among the physical processes that seem to be undirected in time (at least, so it seems) are essentially all the processes that govern fundamental physics. Yet we have strong reasons to think that the equations that govern larger-scale physical processes are somehow derivative on, or determined by, those that govern fundamental physics. So we have a puzzle at least, a paradox at worst: if there is no fundamental directedness in fundamental physics, how does it come to be present in other areas of physics? The purpose of this essay is first to sharpen and make more precise this dilemma, and then to review the main strategies for solving or dissolving it.

Many processes beyond physics are also directed. Indeed, virtually every process studied in any science other than physics defines an arrow of time — to say nothing for the directedness of the processes of causation, inference, memory, control, counterfactual dependence and the like that occur in everyday

[1] And indeed, even our examples of everyday processes without a direction of time actually experience small asymmetric effects — friction, emission of gravitational radiation, etc, — so that sufficiently careful observation would pick out a direction of time there too.

Mathematical Models
Underlying Governing Equations, Principles and Variables

Math Model	**Underlying Principle**	**Primary Variable**	**Secondary Variables**	**Material Constants**
Heat Conduction	Energy Balance	Temperature	Temp-Gradient Heat Flux	Conductivity Density Heat Capacity
Solid Mechanics	Force Balance	Displacements	Strains Stresses	Young's Modulus Poisson's ratio Density
Fluid Flow (with Heat transfer)	Mass Balance Force Balance Energy Balance (?)	Velocity Temperature Pressure	Velocity gradient Shear stresses	Conductivity Density Heat Capacity Viscosity Bulk modulus
Electrodynamics				

TP 2: Coppersmith Attacks against RSA

Jean-Sébastien Coron

Université du Luxembourg

1 Preliminaries

1.1 SAGE

Download and install the Sage library [1].

1.2 Basic Coppersmith Attack

The following code generates an RSA key with a modulus N of n bits, generates a random polynomial:

$$f(x) = x^2 + ax + b \mod N$$

with a small root $|x_0| < 2^{n/3}$, and recovers this root using Coppersmith's technique.

```
def keyGen(n=256):
  "Generates an RSA key"
  while True:
    p=random_prime(2^(n//2));q=random_prime(2^(n//2));e=3
    if gcd(e,(p-1)*(q-1))==1: break
  d=inverse_mod(e,(p-1)*(q-1))
  Nn=p*q
  print "p=",p,"q=",q
  print "N=",Nn
  print "Size of N:",Nn.nbits()
  return Nn,p,q,e,d

def CopPolyDeg2(a,b,Nn):
  "Finds a small root of polynomial x^2+ax+b=0 mod N"
  n=Nn.nbits()
  X=2^(n//3-5)
  M=matrix(ZZ,[[X^2,a*X,b],\
               [0  ,Nn*X,0],\
               [0  ,0   ,Nn]])
  V=M.LLL()
  v=V[0]
  return [v[i]/X^(2-i) for i in range(3)]

def test():
  """Generates a random polynomial with a small root x0 modulo Nn
     and recovers his root."""
  Nn,p,q,e,d=keyGen()
  n=Nn.nbits()
  x0=ZZ.random_element(2^(n//3-10))
  a=ZZ.random_element(Nn)
  b=mod(-x0^2-a*x0,Nn)
  print "x0=",x0
```

Black and Latino people are full human beings, not people to be denied the right even to live, gunned down by the police with impunity, incarcerated in genocidal numbers, and denied basic rights.

The Trump/Pence Regime on White Supremacy, Police Brutality, and Mass Incarceration:

What they have done

- Attorney General Jeff Sessions called for maximum charges and penalties for non-violent drug offenders, reversing policies reducing them, at a time when 2.3 million people, disproportionately Black and Latino, are already incarcerated.
- Sessions has put a halt on consent decrees with cities that aim to address some of the most egregious police abuses, such as in Baltimore.
- Police across the U.S. have already shot and killed over 508 people in the first 6 months of 2017, over 200 of them Black or Latino, with many unarmed.
- In the name of stopping the "carnage," the Department of Justice is working with local police in 12 cities, and Trump has sent feds into Chicago. These forces are an advance guard for a stepped-up reign of terror on Black and Latino people.
- Under Betsy DeVos, the Department of Education is rolling back investigations of civil rights abuses against people of color, women, and LGBTQ people in public schools.

What they said they will do

- The Republicans are moving to end Obamacare, which will result in an additional 217,000 deaths over the next decade and 22 million more people without health insurance—hitting poor, Black, Latino, and Native American people hardest.
- A proposed "Back the Blue Act" would make it harder to sue for damages for unjustified police violence; turn even minor, often non-existent, assaults on police into federal crimes with severe mandatory minimum sentences; and expand the federal death penalty to cover killings of police.
- Trump's proposed budget will cut $192 million from the Food Stamps program over the next 10 years, taking food from many of the nearly 44 million recipients—about 26 percent Black—depriving basic nutritional assistance from children and elderly, disabled, working poor, and homeless people.
- Funding for the Special Nutrition Program for Women, Infants and Children (WIC) will be reduced. Latinos make up 40 percent of WIC recipients, Black people about 20 percent, and Native people about 12 percent.
- Trump's budget would cut 13 percent of the Department of Education budget—$9 billion—which will lead to further deterioration of public schools in oppressed neighborhoods, while $1.4 billion will be added to encourage and support private, charter, and religious schools, including vouchers for religious fundamentalist charter schools.
- Other education cuts affecting oppressed nationalities in particular include elimination of $1.2 billion allocated for after school and summer programs serving 1.6 million students of working families, including after school food programs for low-income students.

What they have unleashed nationally

- The Trump regime has fostered a climate in which white supremacists feel empowered and emboldened, including a Mississippi legislator who declared that anyone wanting to take down Confederate monuments "should be lynched."
- In just the first 5 months following Trump's election, there were nearly 300 acts of racist threats directed against Black people.
- There is an epidemic of lynching nooses appearing across the country—clearly meant to deliver a hateful, racist, threatening message. One appeared in May at the exhibit on segregation at the National Museum of African American History and Culture in Washington, DC—4 days after another noose had been found at another Smithsonian museum, the Hirshhorn.
- In June, another lynching noose was hung near the National Gallery of Art in Washington, DC.
- Other lynching nooses have appeared, since Trump's election, at a construction site and a middle school in Maryland; a frat house at the University of Maryland; the Duke University campus and Wakefield High School in North Carolina; the Port of Oakland in California; a high school in Lakewood, California; and a New York City butcher shop.
- One hundred racists with burning torches, and some armed with automatic weapons, held a nighttime rally in May in Charlottesville, Virginia, against the taking down of a Confederate monument, shouting "We [white people] will not be replaced!"
- After Texas congressman Al Green said on the House floor that Trump should be impeached, he was flooded with telephone lynching threats, like "You're not going to impeach anybody, you fucking nigger. You'll be hanging from a tree."

This Nightmare Must End: The Trump/Pence Regime Must GO!

In the Name of Humanity, We REFUSE to Accept a Fascist America!

RefuseFascism.org #TrumpPenceMustGo ***NOV 4–IT BEGINS...***

TECHNICAL REPORT

DSL Forum
TR-111

Applying TR-069 to Remote Management of Home Networking Devices

December 2005

Produced by:
DSLHome-Technical Working Group

Editors:
Jeff Bernstein, 2Wire
Tim Spets, Westell
Christele Bouchat, Alcatel

Working Group Co-Chairs:
Greg Bathrick, Texas Instruments
Heather Kirksey, Motive
Wayne Daniel, Siemens

Abstract:
This specification extends the mechanism defined in TR-069 for remote management of customer premises equipment to allow a management system to more easily access and manage devices connected via LAN through an Internet gateway.

Reprints in Theory and Applications of Categories, No. 11, 2005, pp. 1–35.

AN ELEMENTARY THEORY OF THE CATEGORY OF SETS (LONG VERSION) WITH COMMENTARY

F. WILLIAM LAWVERE

Received by the editors 2005-04-01.
Transmitted by M. Hyland, A. Kock, R. Rosebrugh. Reprint published on 2005-05-23.
2000 Mathematics Subject Classification: 18B05, 00A30, 03A05.
Key words and phrases: Category of sets, Axiom of choice, Mathematical logic and foundations.
This article is an expanded version of 'An elementary theory of the category of sets', *Proceedings of the National Academy of Science of the U.S.A* **52**, 1506–1511. Article and commentary ©F. William Lawvere and Colin McLarty. Permission to copy for private use granted.

A Discrete Global Minimization Algorithm for Continuous Variational Problems

Danil Kirsanov
Harvard University
kirsanov@fas.harvard.edu

Steven J. Gortler
Harvard University
sjg@eecs.harvard.edu

Abstract

In this paper, we apply the ideas from combinatorial optimization to find *globally* optimal solutions to continuous variational problems. At the heart of our method is an algorithm to solve for globally optimal discrete minimal surfaces. This discrete surface problem is a natural generalization of the planar-graph shortest path problem.

1 Introduction

We are given a variational problem to solve for the function $f(x) : \Omega \subset \mathbb{R}^n \mapsto \mathbb{R}$ that minimizes some functional

$$\int_{\Omega} \cdots \int G(f(x), \nabla f(x), x)\, dx. \tag{1.1}$$

with boundary conditions $f(\partial\Omega) = \Gamma$.

The standard numerical approach is to discretize the domain Ω and then use floating point numbers to represent functions $\Omega \subset \mathbb{R}^n \mapsto \mathbb{R}$. Then, descent methods are used to find a local optimum. In this paper we study how combinatorial algorithms may be applied to these problems to find global minima. First we discretize the space $\Omega \times \mathbb{R}$. With this discretization, the optimization becomes completely combinatorial in nature. We then solve the resulting combinatorial optimization problem with a polynomial time discrete algorithm.

For example, suppose $\Omega = \mathbb{R}$, then a discretization of $\Omega \times \mathbb{R}$ might be describable as a planar graph (described with a set of vertices and edges) over $\mathbb{R}^2$. In this case, a two point boundary value problem reduces to the problem of finding the optimal path in a graph, and it is well known that one can solve for the global discrete minimal path using Dijkstra's algorithm [5] (see Figure 1).

Contribution In particular, in this paper we present the following contributions

- In order to solve the given continuous variational problem, we must be assured that, with enough discretization, the solution to the combinatorial problem will be close to the continuous one. Here we show conditions sufficient to ensure this, and we demonstrate that these conditions can be met with a sequence of deterministic and random grids we construct.
- We prove that, in arbitrary dimension, the resulting combinatorial optimization problem can be reduced to an instance of min-cut, over an appropriate dual graph. In 3D, for example, this gives us a simple algorithm for finding globally minimum discrete surfaces.
- Finally, we describe some important details about the implementation of our algorithm and we show some experimental results demonstrating our method's superiority to traditional numerical approaches.

TR445

ORBIT: An Optimizing Compiler for Scheme

David Kranz*, Richard Kelsey*, Jonathan Rees#
Paul Hudak*, James Philbin*, and Norman Adams*

*Yale University
Department of Computer Science
Box 2158 Yale Station
New Haven, CT 06520

#Mass. Institute of Technology
Artificial Intelligence Lab
545 Technology Square
Cambridge, MA 02139

*Tektronix, Inc.
Beaverton, OR 97077

1. Introduction

[1] In this paper we describe an optimizing compiler for Scheme [R. 85] called *Orbit* that incorporates our experience with an earlier Scheme compiler called TC [10, 85], together with some ideas from Steele's Rabbit compiler [84]. The three main design goals have been correctness, generating very efficient compiled code, and portability.

In spirit, Orbit is similar to the Rabbit compiler in that it depends on a translation of source code into "continuation-passing style" (CPS), a convenient intermediate form that makes control-flow explicit. After CPS conversion, procedures take an extra argument called a *continuation* (another procedure) that represents the next logical execution point after execution of the procedure body. Thus procedures do not "return" but rather "continue into" the code represented by the continuation. This permits, for example, a general but simple way to optimize tail-recursions into loops.

Steele's seminal work on Rabbit demonstrated the general benefits of this approach to compiler design. However, his work was primarily research oriented, and Rabbit was essentially a prototype compiler (consider, for example, that it generated MACLISP code). TC, on the other hand, was one of the first *practical* compilers for a Scheme dialect, and much was learned through its design and construction.[2] Orbit now represents a culmination of that learning process, in which CPS conversion has been implemented thoroughly, extended in critical ways, and set in a framework of other important compiler innovations to yield a practical compiler that generates production-quality code competitive with the best compilers for Lisp as well as more-Lisp languages.[3] The new ideas in Orbit include:

1. An extension to CPS conversion called *assignment conversion* that facilitates treatment of assigned variables. (See section 3.1)
2. Compact and efficient runtime data representations, the most important being those for *lexical closures*, which are represented in different ways depending on information gleaned from a static analysis of their use. (See sections 4 and 5.)
3. A register allocation strategy based on *trace scheduling* that optimizes register usage across forks and joins (and which, because of CPS conversion, includes procedure calls). (See section 6.)
4. An integral table-driven assembler that uses hints from the code generator to order blocks so as to minimize the number and size of jumps. (See section 7.)
5. A technique for defining the behavior of primitive operations in Scheme source modules rather than in the internal logic of the compiler. (See section 9.1.)
6. Flexibility in configuring the runtime support system for user programs. (See section 9.2.)

---

[1] This work was supported in part by NSF Grants DCR-8403204 and DCR-8451141, and a Faculty Development Award from IBM. In addition some of the work was supported at DEC Western Research Laboratory in the summer of 1986.

[2] Both TC and the S-1 Common Lisp compiler described in [R] have as a common ancestor a Lisp compiler which Steele wrote during the summer of 1976. From this compiler TC was derived by making modifications for compilation of a different source language for different target machines, and adding the logic necessary for supporting lexical closures moderately well.

[3] Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or republish, requires a fee and/or specific permission.

Preprint of an article to appear in Proceedings of the SIGPLAN '86 Symposium on Compiler Construction

The World Transformed

Programme

Preliminary program for a seminar on

Types, Categories & Logic

Hanno Becker, habecker@satà.uni-bonn.de

Overview. *Type theories* are formal calculi that allow for the study of aspects of functional programming, set theory and logic through the following principles:

(1) Data types, sets and propositions are subsumed under the notion of a *type*.
(2) Programs, elements and proofs are subsumed under the notion of a *term*.
(3) The judgements
   - "m is an algorithm producing a value of the data type T",
   - "x is an element of the set A", and
   - "p is a proof of P"

   are subsumed under the *typing judgement* "t is a term of type T".

Here are two informal reasons why one might expect such a wondrous thing:

- Consider assigning to a proposition φ the set of all its proofs $\mathscr{P}(\varphi)$. Then, at least in intuitionistic mathematics, this assignment intertwines the logical connectives $\wedge, \vee, \Rightarrow$ with the set theoretic operations $\times, \amalg, \mathrm{Maps}(-,-)$: Providing a proof of $\varphi \wedge \psi$ means providing *both* a proof of φ *and* a proof of ψ, i.e. $\mathscr{P}(\varphi \wedge \psi) = \mathscr{P}(\varphi) \times \mathscr{P}(\psi)$. Similarly, providing a proof of $\varphi \vee \psi$ means providing *either* a proof of φ *or* a proof of ψ, i.e. $\mathscr{P}(\varphi \vee \psi) = \mathscr{P}(\varphi) \amalg \mathscr{P}(\psi)$. Finally, providing a proof of $\varphi \Rightarrow \psi$ means providing a *method* for turning a proof of φ into a proof of ψ, so $\mathscr{P}(\varphi \Rightarrow \psi) = \mathrm{Maps}(\mathscr{P}(\varphi), \mathscr{P}(\psi))$. This suggests that it should be possible to build logic on set theory by identifying a proposition with the set of its proofs (as is indeed done in type theory).
- Algorithms are implicit in our daily mathematical work: When constructing elements of sets we usually don't specify them explicitly, but instead describe a *procedure* for how to compute them. For example, consider the set of natural numbers $\mathbb{N}$ as freely generated by $0 \in \mathbb{N}$ and the successor function $(-)' : \mathbb{N} \to \mathbb{N}$. This means that the canonical elements of $\mathbb{N}$ are precisely $0, 1 := 0', 2 := 0''$ and so on. Further, suppose we define addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ inductively by $0 + n := n$ and $m' + n := (m + n)'$, and similarly the multiplication $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Then, an expression like $5 + 4 \cdot 7$ is rather a *program* for the computation of the canonical element $33 := 0^{\prime}$ in $\mathbb{N}$ than this element itself: it is only by repeated application of the definitions of $+$ and $\cdot$ that the expression gets *reduced* to its canonical form. Since the understanding of computation as the successive evaluation of syntactic objects according to fixed rules is characteristic for functional programming, this gives an idea why one should expect a relation between (constructive) mathematics and functional programming.

Moreover, the last point already hints at another similarity between programming, set theory and logic, namely the concept of *computation*:

International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Explanation of the Effect of Magnetic Field on laser Intensity on the Basic of Generalized Special Relativity

Ahmed Zakaria[1], M. Dirar Abd- Allah[1], Rasha Abd ALhi[1], Kh. M. Haroun[2, 3], Ahmed EL Hassan ELfaki[1], R. Abd Elgani[1], Hilo, M. H. M[1]

[1]Department of Physics, Faculty of Science, Sudan University of Science and Technology, Khartoum11113, Sudan

[2]Department of Physics, Faculty of Education, Al-Azhari University, Khartoum Bahri – Sudan

[3]Department of Physics,

[3]Department of Physics, College of Arts and Science in ALmikhwah, ALbaha University, ALmikhwah- Saudi Arabia

Abstract: ***Laser technology recently becomes one of the widespread technologies in many applications. This attracts attention to generation of laser and the mechanisms affecting this generation. One of the recent developments in lasing is the so-called free-electron laser (FEL) which is based on special relativity (SR). FEL shows that lasing intensity is affected by a magnetic field. However, the theoretical framework of this effect is complex and cannot explain the effect of the magnetic field on lasers produced by materials. These setbacks motivate to search for a new model based on generalized special relativity to account for these theoretical defects. In this work, the generalized special relativity accounts for the effect of magnetic fields on laser intensity produced by matter theoretically. These theoretical relations agree with the empirical ones for plasma, discharge gas and semiconductor lasers.***

Keywords: Free electron laser, Magnetic field. Potential, Laser intensity, Generalized, special relativity, amplification factor

1. Introduction

Laser technology is one of the biggest achievements of theoretical physics [1, 2]. It comes directly from the discovery and prediction of the so called stimulation emission which was proposed by Einstein [3]. This phenomenon shows the possibility of light amplification by stimulated emission of radiation to produce laser [4]. Laser can be produced by different mechanisms [5]. It can be produced by population inversion [6], or by non inversion process by polarized atoms or by free electrons in a magnetic field [7, 8, 9]. The effect of magnetic field on free electrons shows the possibility of observing the same effect on matter. This was really observed experimentally as shown in section (2). This effect is explained theoretically in section (3). Sections (4) and (5) are devoted for discussion and conclusion.

2. The Effect of Magnetic field on Laser Intensity

The first demonstration of large soft-x-ray amplification in a discharge-driven plasma was recently realised using a fast capillary discharge to generate a hot and dense plasma column in which collisional electron excitation of Ne-like Ar ions produced amplification in the J = 0 – 1 line of Ne-like Ar at 46.9 nm. In this excitation scheme, a fast current pulse rapidly compresses the plasma, creating a hot and narrow plasma column with length-to-diameter ratios approaching 1000:1. During the final stage of the compression, plasma conditions for soft-x-ray amplification by collisional excitation are obtained. In the initial experiments, a gain-length product of gl ~7.2 at 46.9 nm was reported for a 12-cm -long plasma column.

The experiments were conducted in a capillary discharge excited, collisionally pumped 46.9-nm Ne-like Ar amplifier [7]. In the experiments the generator was used to excite plasmas in polyacetal capillaries 4 mm in diameter and 10 cm in length with current pulses having a first half cycle duration of approximately 64 ns. The axial magnetic field was generated by a 9-cm diameter, 15-cm long coil positioned concentrically with the capillary channel. The coil, which was excited by a current pulse with a period of 200 μs is obtained by discharging a 420-μF capacitor through a spark gap, was used to produce magnetic fields up to 0.3 T. The intensity of the magnetic field was selected by varying either the capacitor charging voltage or the delay time between the triggering of the laser spark gap and the firing of the fast capillary discharge. The soft-x-ray radiation exited the capillary through the hollowed ground electrode. The laser radiation was collected by a cylindrical copper mirror of 13 cm in radius and focused onto the slit of a 2.2-m vacuum spectrometer provided with a 1200 l/mm diffraction grating placed at 4.2° with respect to the incoming radiation. The detection system consisted of an intensified charge-coupled device (CCD) array detector that was gated by pulsing the gain on the multichannel plate intensifier with a high voltage pulse with duration of about 25 ns. The variation of the measured integrated intensity of the Ar IX 46.9-nm laser line as a function of the magnetic field strength is shown in Fig (1) [7]. The laser intensity increases with the magnetic field and reaches a maximum at approximately 0.15 T decreasing monotonically for higher field strengths. The same figure also shows the calculated variation of the intensity corresponding to two calculations

Licensed Under Creative Commons Attribution CC BY

14 June 2017

PRESS SUMMARY

R (on the application of Kiarie) (Appellant) v Secretary of State for the Home Department (Respondent)
R (on the application of Byndloss) (Appellant) v Secretary of State for the Home Department (Respondent)
[2017] UKSC 42
On appeal from [2015] EWCA Civ 1020

JUSTICES: Lady Hale (Deputy President), Lord Wilson, Lord Carnwath, Lord Hodge, Lord Toulson.

BACKGROUND TO THE APPEAL

Mr Kiarie has Kenyan nationality. He came to the UK in 1997 with his family at the age of three. Mr Byndloss has Jamaican nationality. He has lived in the UK since the age of 21 and has a wife and children living in the UK. Following their separate convictions for serious drug related offences, in October 2014 the respondent made orders for their deportation to Kenya and Jamaica respectively and rejected the appellants' claims that deportation would breach their right to respect for their private and family life under article 8 of the European Convention on Human Rights ("ECHR").

When making the deportation orders, the Home Secretary issued certificates under section 94B of the Nationality, Immigration and Asylum Act 2002. In certifying the appellants' claims under section 94B, the respondent chose not to instead certify their human rights claims as "clearly unfounded" under section 94, indicating that their appeals were arguable. The effect of section 94B certification is that the appellants can bring their appeals against the respondent's immigration decisions only after they have returned to Kenya and Jamaica. Until 30 November 2016, section 94B provided that where a human rights claim had been made by a person liable to deportation, the Secretary of State may certify the claim if she considers that the removal of the person pending the outcome of their appeal would not be unlawful under section 6 of the Human Rights Act 1998 and that the person would not face a real risk of serious irreversible harm if removed to that country.

The court stresses that this appeal is not about the circumstances in which a person can successfully resist deportation by reference to his private or family life. It recently addressed that question in the case of *Ali* and ruled that he can do so only if the circumstances are "very compelling". The question in this appeal is: where the law gives such a person a right to appeal to a tribunal against a deportation order, then, however difficult it may be for him to succeed, does the Home Secretary breach his human rights by deporting him before he can bring the appeal and without making proper provision for him to participate in the hearing of it? The Court of Appeal's answer was no.

JUDGMENT

The Supreme Court unanimously allows the appeal of Mr Kiarie and Mr Byndloss and quashes the certificates. Lord Wilson gives the lead judgment, with which Lady Hale, Lord Hodge and Lord Toulson agree. Lord Carnwath gives a concurring judgment.

REASONS FOR THE JUDGMENT

The fundamental objective of section 94B arises from the fact that the appellants are "foreign criminals" and, by virtue of section 32(4) of the UK Borders Act 2007, the deportation of a "foreign criminal" is conducive to the public good **[32-33]**. However, Parliament gave foreign criminals a right of appeal against a deportation order by enacting

Advance unedited version

Distr.: General
24 February 2017

Original: English

Human Rights Council
Thirty-fourth session
27 February-24 March 2017
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*

Note by the Secretariat

In this report, the Special Rapporteur on the right to privacy (SRP) focuses on governmental surveillance activities from a national and international perspective. The SRP will elaborate on the characteristics and the interpretation of the international legal framework. The SRP will also describe recent developments and trends, how these can be studied, and how they interact with the enjoyment of the right to privacy and other interconnected human rights. Consequently, first approaches to a more privacy-friendly oversight of government surveillance will be outlined. Before concluding, the SRP will report on his activities in the relevant period for this report.

* The present document was submitted late so as to include the most up-to-date information possible.

Master Erasmus Mundus in

Color in Informatics and Media Technology (CIMET)

Mobile Phone Camera Possibilities for Spectral Imaging

Master Thesis Report

Catalin Matasaru

Academic Supervisors: Prof. Markku HAUTA-KASARI (UEF)

CTO Petri PIIRAINEN (SoftColor Oy Ltd)

Jury Committee:

Defended at the University of Eastern Finland, Joensuu, Finland

June, 13, 2014

Abusing Windows Management Instrumentation (WMI) to Build a Persistent, Asyncronous, and Fileless Backdoor

Matt Graeber

Black Hat 2015

Introduction

As technology is introduced and subsequently deprecated over time in the Windows operating system, one powerful technology that has remained consistent since Windows NT 4.0[1] and Windows 95[2] is Windows Management Instrumentation (WMI). Present on all Windows operating systems, WMI is comprised of a powerful set of tools used to manage Windows systems both locally and remotely.

While it has been well known and utilized heavily by system administrators since its inception, WMI was likely introduced to the mainstream security community when it was discovered that it was used maliciously as one component in the suite of exploits and implants used by Stuxnet[3]. Since then, WMI has been gaining popularity amongst attackers for its ability to perform system reconnaissance, AV and VM detection, code execution, lateral movement, persistence, and data theft.

As attackers increasingly utilize WMI, it is important for defenders, incident responders, and forensic analysts to have knowledge of WMI and to know how they can wield it to their advantage. This whitepaper will introduce the reader to WMI, actual and proof-of-concept attacks using WMI, how WMI can be used as a rudimentary intrusion detection system (IDS), and how to perform forensics on the WMI repository file format.

WMI Architecture

---

1 https://web.archive.org/web/20050115045451/http://www.microsoft.com/downloads/details.aspx?FamilyID=c174cfb1-ef67-471d-9277-4c2b1014a31e&displaylang=en

2 https://web.archive.org/web/20051106010729/http://www.microsoft.com/downloads/details.aspx?FamilyId=98A4C5BA-3378-4E92-8C18-A63847760EA5&displaylang=en

3 http://poppopret.blogspot.com/2011/09/playing-with-mof-files-on-windows-for.html

black hat®
USA 2016
JULY 30 - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS

Recover a RSA private key from a TLS Session with Perfect Forward Secrecy

Marco Ortisi

July 25th, 2016

The Adventures of AV and the Leaky Sandbox

A **SafeBreach Labs** research by

Itzik Kotler, CTO and co-founder, SafeBreach

Amit Klein, VP Security Research, SafeBreach

SafeBreach

#BHUSA / @BLACKHATEVENTS

USBird4.1.1

RAVEN / RAVEN-16 / SD-RAVEN / MICRO-RAVEN / RAVEN-EYE / RAVEN-RX / RAVEN-MONITOR / RAVEN-REPEATER

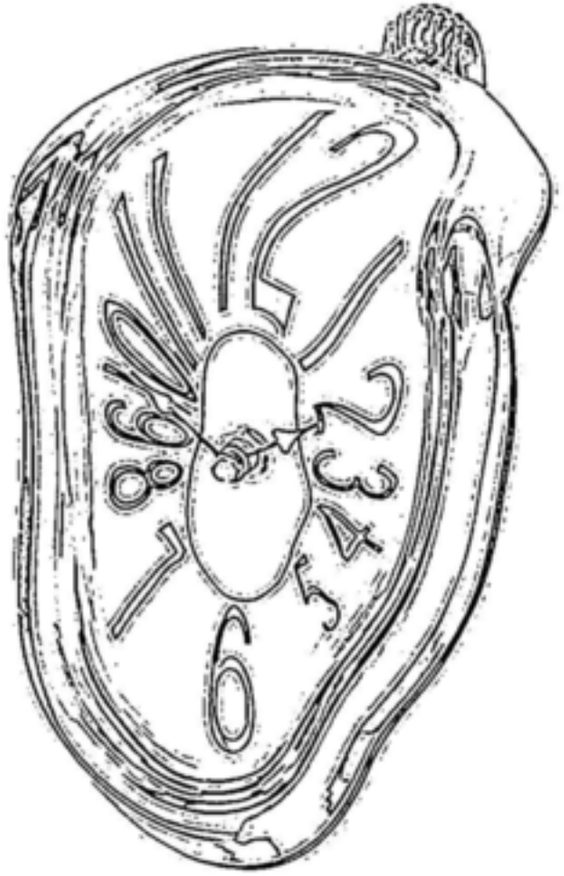
AUDIO / VIDEO RECORDERS

USERS MANUAL

WINDOWS VERSION

RELEASE 2.0

10/15/2010



CLKSCREW

Exposing the Perils of Security-Oblivious Energy Management

Adrian Tang, Simha Sethumadhavan, Salvatore Stolfo

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

USENIX Security 2017

Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys

Mathy Vanhoef
iMinds-DistriNet, KU Leuven
Mathy.Vanhoef@cs.kuleuven.be

Frank Piessens
iMinds-DistriNet, KU Leuven
Frank.Piessens@cs.kuleuven.be

Abstract

We analyze the generation and management of 802.11 group keys. These keys protect broadcast and multicast Wi-Fi traffic. We discovered several issues and illustrate their importance by decrypting all group (and unicast) traffic of a typical Wi-Fi network.

First we argue that the 802.11 random number generator is flawed by design, and provides an insufficient amount of entropy. This is confirmed by predicting randomly generated group keys on several platforms. We then examine whether group keys are securely transmitted to clients. Here we discover a downgrade attack that forces usage of RC4 to encrypt the group key when transmitted in the 4-way handshake. The per-message RC4 key is the concatenation of a public 16-byte initialization vector with a secret 16-byte key, and the first 256 keystream bytes are dropped. We study this peculiar usage of RC4, and find that capturing 2^{31} handshakes can be sufficient to recover (i.e., decrypt) a 128-bit group key. We also examine whether group traffic is properly isolated from unicast traffic. We find that this is not the case, and show that the group key can be used to inject and decrypt unicast traffic. Finally, we propose and study a new random number generator tailored for 802.11 platforms.

1 Introduction

In the last decennia, Wi-Fi became a de facto standard for medium-range wireless communications. Not only is it widely supported, several new enhancements also make it increasingly more performant. One downside is that (encrypted) traffic can easily be intercepted. As a result, securing Wi-Fi traffic has received considerable attention from the research community. For example, they showed that WEP is utterly broken [11, 42, 4], demonstrated attacks against WPA-TKIP [43, 45, 47, 41], performed security analysis of AES-CCMP [24, 39, 13], studied the security of the 4-way handshake [17, 18, 34], and so on. However, most research only focuses on the security of pairwise keys and unicast traffic. Group keys and group traffic have been given less attention, if mentioned at all.

In this paper we show that generating and managing group keys is a critical, but underappreciated part, of a modern Wi-Fi network. In particular we investigate the generation of group keys, their transmission to clients, and the isolation between group and unicast traffic. We discovered issues during all these phases of a group key's lifetime. To address some of our findings, we propose and implement a novel random number generator that extracts randomness from the physical Wi-Fi channel.

First we study the random number generator proposed by the 802.11 standard. Among other things, the Access Point (AP) uses it to generate group keys. Surprisingly, we find that it is flawed by design. We argue that implementing the algorithm as specified, results in an unacceptably slow algorithm. This argument is supported empirically: all implementations we examined, modified the generator to increase its speed. We demonstrate that these modified implementations can be broken by predicting the generated group key within mere minutes.

The generated group keys are transferred to clients during the 4-way WPA2 handshake. We found that it is possible to perform a (type of) downgrade attack against the 4-way handshake, causing RC4 to be used to encrypt the transmission of the group key. We analyze the construction of the per-message RC4 key and its effect on biases in the keystream. This reveals that an attacker can abuse biases to recover an 128-bit group key by capturing 2^{39} to 2^{32} encryptions of the group key, where the precise number depends on the configuration of the network.

Group keys should only be used to protect broadcast or multicast frames. In other words, pairwise and group keys should be properly isolated, and unicast packets should never be encrypted with a group key. An AP can enforce this by only sending, but never receiving, group addressed frames. However, all APs we tested did not provide this isolation. We demonstrate that this allows

DK METER
User Manual

DK METER – **Audio & Loudness** Metering Complete

SYMPLECTIC GEOMETRY AND HAMILTONIAN SYSTEMS

E. LERMAN

Contents

1. Lecture 1. Introduction and basic definitions 2
2. Lecture 2. Symplectic linear algebra 5
3. Lecture 3. Cotangent bundles and the Liouville form 7
4. Lecture 4. Isotopies and time-dependent vector fields 10
Detour: vector fields and flows. 10
5. Lecture 5. Poincaré lemma 12
6. Lecture 6. Lagrangian embedding theorem 15
Vector bundles 16
Normal bundles 18
7. Lecture 7. Proof of the tubular neighborhood theorem 20
8. Lecture 8. Proof of the Lagrangian embedding theorem. Almost complex structures 24
Almost Complex Structure 26
9. Lecture 9. Almost complex structures and Lagrangian embeddings 29
10. Lecture 10. Hamilton's principle. Euler-Lagrange equations 31
10.1. Classical system of N particles in $\mathbb{R}^3$ 31
10.2. Variational formulation 32
11. Lecture 11. Legendre transform 35
12. Lecture 12. Legendre transform and some examples 40
13. Lecture 13. Constants of motion. Lie and Poisson algebras 43
13.1. Lie algebras 44
14. Lecture 14. Lie groups: a crash course 48
14.1. Homomorphisms 49
14.2. The exponential map 50
15. Lecture 15. Group actions 53
Lifted actions 54
16. Lecture 16. Moment map 57
Adjoint and coadjoint representations 60
17. Lecture 17. Coadjoint orbits 63
18. Lecture 18. Reduction 67
19. Lecture 19. Reduction at nonzero values of the moment map 75

Virginia

List of Official Convention Participants prepared by the Office of the Secretary. As of Tuesday, August 05, 2008.

DELEGATION CHAIR

Cranwell, C. Richard Richmond, VA	Delegation Chair, Automatic Unpledged State Party Chair	

Delegation Chair Total: 1

DISTRICT LEVEL DELEGATES

Alexander, Kenneth Norfolk, VA	District Level Delegates	Pledged To: Obama	Congressional District 3
Allen, Georgia Virginia Beach, VA	District Level Delegates	Pledged To: Obama	Congressional District 2
Ambrose, Christopher Lorton, VA	District Level Delegates	Pledged To: Obama	Congressional District 11
Bieber, Christie Ann Richmond, VA	District Level Delegates	Pledged To: Clinton	Congressional District 7
Black, Allida Arlington, VA	District Level Delegates	Pledged To: Clinton	Congressional District 8
Blue, Penny Union Hall, VA	District Level Delegates	Pledged To: Obama	Congressional District 5
Bredemeyer, Arthur Suffolk, VA	District Level Delegates	Pledged To: Obama	Congressional District 4
Brink, Robert H. Arlington, VA	District Level Delegates	Pledged To: Obama	Congressional District 8
Brooks, Linda Newport News, VA	District Level Delegates	Pledged To: Obama	Congressional District 3
Brown, Willie Chesapeake, VA	District Level Delegates	Pledged To: Obama	Congressional District 4
Cerillo, Mary Lee Centreville, VA	District Level Delegates	Pledged To: Obama	Congressional District 10
Chiappe, Ada Cristina Falls Church, VA	District Level Delegates	Pledged To: Obama	Congressional District 8
Chitwood, Elizabeth Pulaski, VA	District Level Delegates	Pledged To: Clinton	Congressional District 9
Clark, Marjorie Richmond, VA	District Level Delegates	Pledged To: Obama	Congressional District 7

# indicates that the individual is new with this release.

Paid for by the Democratic National Convention Committee, www.demconvention.com. Not authorized by any candidate or candidate's committee.

T.J. Watson Research Center

Hardware Virtualization Trends

Leendert van Doorn

 © 2006 IBM Corporation

The Variation Principle

The variation theorem states that given a system with a Hamiltonian H, then if ϕ is any normalised, well-behaved function that satisfies the boundary conditions of the Hamiltonian, then

$$\langle\phi|H|\phi\rangle \geq E_0 \qquad (1)$$

where E_0 is the true value of the lowest energy eigenvalue of H. This principle allows us to calculate an upper bound for the ground state energy by finding the trial wavefunction ϕ for which the integral is minimised (hence the name; trial wavefunctions are varied until the optimum solution is found). Let us first verify that the variational principle is indeed correct.

We first define an integral

$$\begin{aligned} I &= \langle\phi|H-E_0|\phi\rangle \\ &= \langle\phi|H|\phi\rangle - \langle\phi|E_0|\phi\rangle \\ &= \langle\phi|H|\phi\rangle - E_0\langle\phi|\phi\rangle \\ &= \langle\phi|H|\phi\rangle - E_0 \qquad \text{(since } \phi \text{ is normalised)} \end{aligned}$$

If we can prove that $I \geq 0$ then we have proved the variation theorem.

Let ψ_i and E_i be the true eigenfunctions and eigenvalues of H, so $H\psi_i = E_i\psi_i$. Since the eigenfunctions ψ_i form a complete basis set for the space spanned by H, we can expand any wavefunction ϕ in terms of the ψ_i (so long as ϕ satisfies the same boundary conditions as ψ_i).

$$\phi = \Sigma_k a_k\psi_k$$

Substituting this function into our integral I gives

$$\begin{aligned} I &= \langle \Sigma_k a_k\psi_k \,|\, H-E_0 \,|\, \Sigma_j a_j\psi_j \rangle \\ &= \langle \Sigma_k a_k\psi_k \,|\, \Sigma_j (H-E_0)\, a_j\psi_j \rangle \end{aligned}$$

If we now use $H\psi = E\psi$, we obtain

$$\begin{aligned} I &= \langle \Sigma_k a_k\psi_k \,|\, \Sigma_j a_j (E_j-E_0)\, \psi_j \rangle \\ &= \Sigma_k \Sigma_j a_k^* a_j (E_j-E_0) \langle \psi_k \,|\, \psi_j \rangle \\ &= \Sigma_k \Sigma_j a_k^* a_j (E_j-E_0)\, \delta_{jk} \end{aligned}$$

We now perform the sum over j, losing all terms except the j=k term, to give

$$\begin{aligned} I &= \Sigma_k a_k^* a_k (E_k-E_0) \\ &= \Sigma_k |a_k|^2 (E_k-E_0) \end{aligned}$$

Since E_0 is the lowest eigenvalue, E_k-E_0 must be positive, as must $|a_k|^2$. This means that all terms in the sum are non-negative and $I \geq 0$ as required.

For wavefunctions that are not normalised, the variational integral becomes:

Multibody System Dynamics (2006) 15: 1–24
DOI: 10.1007/s11044-006-2359-z © Springer 2006

A Modified Implicit Euler Algorithm for Solving Vehicle Dynamic Equations

GEORG RILL
FH Regensburg, University of Applied Sciences, Galgenbergstr. 30, 93053 Regensburg, Germany; E-mail: georg.rill@maschinenbau.fh-regensburg.de

(Received: 27 May 2005; accepted in revised form: 6 June 2005)

Abstract. Vehicle modelling is usually done by Multibody Systems. Very often the overall model consists of several subsystems, like the vehicle framework, the drive train and the steering system. Due to the tire forces and torques and due to small but essential compliances in the axle/wheel suspension systems the resulting differential equations are stiff. To improve the model quality dynamic models for some components like damper, and rubber elements are used. Again these models contain stiff parts.

If the implicit Euler Algorithm is adopted to the specific problems in vehicle dynamics a very effective numerical solution can be achieved. Applied to vehicle dynamic equations the algorithm produces good and stable results even for integration step sizes in the magnitude of milliseconds. As it gets along with a minimum number of operations a very good run time performance is guaranteed. Hence, even with very sophisticated vehicle models real time applications are possible. Due to its robustness the presented algorithm is very well suited for co-simulations. The modifications in the implicit Euler Algorithm also make it possible to use a simple model for describing the dry friction in the damper and in the brake disks.

A quarter car vehicle model with a longitudinal and a vertical compliancy in the wheel suspension and a dynamic damper model including dry friction is used to explain the algorithm and to show its benefits.

Keywords: multibody systems, vehicle dynamics, stiff differential equations, dry friction, implicit integration algorithm, real-time simulation

1. Modelling Aspects

1.1. OVERALL VEHICLE MODEL

Vehicle modelling is normally based on Multibody Systems [3]. Usually the overall vehicle model is separated into different subsystems [7]. Figure 1 shows the components of a passenger car model which can be used to investigate the handling and ride properties.

The vehicle framework consisting of the vehicle chassis and the wheel/axle suspension system is the kernel of the model. It directly interacts with most of the other subsystems. The equations of motion for the vehicle framework can be derived from Jourdain's principle [11].

An enhanced vehicle model with an elastically suspended engine, four passengers and complex axle models comes up to $n_D \approx 80$ degrees of freedom. Due to the tire forces and torques and due to small but essential compliances in the axle/wheel

VIRGINIA DELEGATE SELECTION PLAN

FOR THE
2016 DEMOCRATIC NATIONAL CONVENTION

ISSUED BY THE DEMOCRATIC PARTY OF VIRGINIA

MAY 1, 2016

NBER WORKING PAPER SERIES

ORCHESTRATING IMPARTIALITY: THE IMPACT OF "BLIND" AUDITIONS ON FEMALE MUSICIANS

Claudia Goldin
Cecilia Rouse

Working Paper 5903

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
January 1997

We are indebted to the staff members of the orchestras that gave us access to their audition records and who provided other assistance and to the musicians who responded to our questionnaire. We are particularly grateful to Joanne Berry, Brigit Carr, Ruth DeSarno, Stefanie Dyson, Josh Feldman, Barbara Haws, Oren Howard, Cindy Hubbard, Carol Jacobs, Lynn Larsen, Bennett McClellan, Stephen Molina, Bill Moyer, Jeffrey Neville, Stephen Novak, Deborah Oberschalp, Stacey Pelinka, Carl Schnebler, Alison Scott-Williams, Robert Sirineck, Harold Steiman, and Brenda Nelson Strauss. We also thank Gretchen Jackson of the University of Michigan School of Music. Rashid Alvi, Brigit Chen, Eric Hilfers, Serena Mayeri, LaShawn Richburg, Melissa Schettini, Thomas Tucker, Linda Toth, and Lavelle (Yvette) Warfield served as our extremely able research assistants. And, David Howell of the Princeton University Department of East Asian Studies and Jin Heum Park kindly helped to determine the gender of Japanese and Korean names. We thank them all. We are grateful to our colleagues David Card, Anne Case, Angus Deaton, Hank Farber, Larry Katz, David Lee, and Aaron Yelowitz for helpful conversations, and to seminar participants at the School of Industrial and Labor Relations at Cornell University, Princeton University, and Vanderbilt University for comments. Rouse acknowledges The National Academy of Education and the NAE Spencer Postdoctoral Fellowship Program and the Mellon Foundation for financial support. All errors are ours. This paper is part of NBER's research program in Labor Studies. Any opinions expressed are those of the authors and not those of the National Bureau of Economic Research.

© 1997 by Claudia Goldin and Cecilia Rouse. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

JODY WAGNER FOR LIEUTENANT GOVERNOR
PETITION INSTRUCTION AND TIP SHEET

1. Under the words "We, the qualified voters," which is near the top of the form, write in the name of the county or city of the registered voters who are signing a form.

   a. Only people from that county or city may sign that form. If you meet someone from a different county or city, start a new form for voters from that city or county.

   b. If a city or county has more than one Congressional District, then you will also need to try to keep the sheets separated by Congressional District.

2. Anyone who is a **qualified voter** and a Virginia resident may sign the petition. Signers **must** print and sign their name, provide their home street address and city/county, zip code, and write the date they signed the petition.

3. By signing, the voter is merely agreeing that Jody should be on the ballot for the June 9, 2009 Democratic Primary for Lieutenant Governor. (To be on the ballot for any statewide election, state law requires the submission of at least 10,000 signatures of qualified Virginia voters, with a minimum of 400 from each of Virginia's 11 Congressional Districts.) Voters are permitted to sign the petitions of all the Democratic candidates.

4. Anyone who is a qualified voter and a Virginia resident may circulate petitions.

5. When a form is completed, the person circulating the petition must (a) print their name, address, county/city, and social security number in the blank spaces on the bottom of the backside of the form and (b) sign the form in the space provided and have their signature notarized. (Banks, real estate offices and law offices often have notaries that will notarize the forms at no cost.) Once the circulator signs, dates, and has his/her signature notarized, the form may not be used to collect any more signatures.

6. Make as many additional copies of the petition form as you need. You must, however, make copies of *both* sides of the form on 14 inch paper.

7. Please return all signed and notarized forms to:
   Kevin Wolf; 4946 Rock Spring Rd.; Arlington, VA 22207.

8. Kevin and Mike Tutor will periodically hold training sessions to explain the rules and tips in more detail, but if you have any questions at any time about the petitions, contact Kevin at wolfkann@verizon.net or 703-307-8415 or Michael at mike@jodyforva.com or 757-777-4019.

Thank you so much for helping out in this critical effort to get Jody Wagner elected as our next Lieutenant Governor!

Paid for and authorized by Virginians for Wagner. Printed in House.

Development of the Method of Preparation of the Boiler and Heating Water by Phase Transfer in a Vortex Flow

A.L. Kartashev, S.D. Vaulin, M.A. Kartasheva, E.V. Safonov

***Abstract*—In this paper, development of the method of preparation of the boiler and heating water by phase transfer in a vortex is considered. Ranque-Hilsch effect in a vortex flow is researched. The devices for realization this effect is presented. Problems of modeling the eddy currents with phase transitions, realizing Ranque-Hilsch effect are described.**

***Index Terms*– vortex flow, Ranque-Hilsch effect, phase transitions, mathematical modeling.**

The water treatment plant for the generation of steam and creating a flow of coolant can be used effects arising from eddy currents, including phase transitions representing the evaporation and condensation of water vapor.

Devices that are implemented vortex motion are called differently: centrifugal cyclone, the cyclone vortex chamber and the vortex, the vortex pipe (Ranque-Hilsch effect) and hydro cyclones, vortex separators, vortex combustor and combustion chambers, etc. [1, 2]. Their common feature is the presence of the working area (typically cylindrical or conical shape) and the vortex flow (generally tangential or axial).

The term "vortex chamber" was introduced in the simulation of atmospheric vortices in the lab. According to the accepted terminology, the vortex chamber – is a device which implements a uniform distribution around the periphery of the medium input chamber and in which a working medium performs a rotary-translational movement.

Manuscript received July 16, 2015; revised July 28, 2015. The work was conducted with the financial support of the Ministry of Education and Science of the Russian Federation in the framework of the project "Applied research and development of the method of preparation of the boiler and heating water by phase transitions in the vortex under high vacuum" according to the contract no. 14.579.21.0063 d.d. 20.10.2014, identifier RFMEFI57914X0063 between the Ministry of Education and Science of the Russian Federation and Federal State Educational Institution of Higher Professional Education "South Ural State University" (National Research University).

A. L. Kartashev. Doctor of engineering science. Professor of Flying Machines and Automatic Apparatus Department of South Ural State University, Chelyabinsk, Russia. Tel.: +79193458556, e-mail: al_kartashev@mail.ru.

S. D. Vaulin. Doctor of engineering science. Promotor for scientific work. Head of Aircraft Engines Department of South Ural State University, Chelyabinsk, Russia. Tel.: +79028993852, e-mail: s.d.vaulin@susu.ac.ru.

M. A. Kartasheva. Candidate of technical science, reader of "Flying machines and automatic apparatus" department of the South Ural State University. Chelyabinsk, Russia. Tel.: 8(351)2679461, e-mail: ma_kartasheva@mail.ru.

E. V. Safonov. Candidate of engineering science. Dean of Aerospace Faculty, reader of Aircraft Engines Department of South Ural State University, Chelyabinsk, Russia. Tel.: +7519049585, e-mail: e-safonov@yandex.ru.

In the study of vortex motion and application swirling flows were discovered their unusual features – counter and "recirculation zone" energy separation (Ranque-Hilsch effect). The presence in the flow field considerable centrifugal forces and significantly affects the properties of the eddy currents, causing those flow characteristics, which can be successfully used in the design of the vortex chambers for various purposes.

In the gas dynamics of vortex flows is nontrivial phenomenon known as the Ranque effect (effect Ranka-Hilsch or vortex effect), which consists in the fact that in vortex tubes fairly simple geometry (Fig. 1) is a division of the gas flow into two, one of which – peripheral – has a temperature above the temperature of the source gas and the second – center – correspondingly lower. This effect is all the more strange when you consider that, as in the case of vortex stabilization of gaseous discharges [3], the buoyancy forces would have to lead to a "surfacing" in the center of the vortex hotter gas.

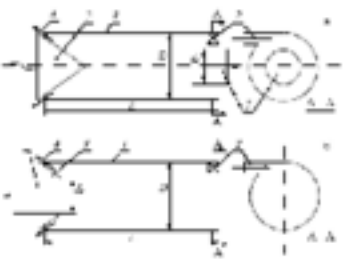


Fig. 1. Schematic diagram of the vortex tubes:
(A) counterstream type, (b) u-turn type
1 – smooth cylindrical tube, 2 – swirl tangential or snail type for compressed gas, 3 – throttle valve (throttle valve), 4 – out of the hot gas through the annular gap 5 – aperture to quit cold gas.

Vortex tubes realizing Ranque-Hilsch effect can be used in the composition of the evaporating section for the simultaneous production of hot water, followed by evaporation to produce steam using vacuum vessel with hot water or water vapor directly into the vortex tube and the cold water used in condensing section for cooling the steam.

For a better understanding of the processes and structure of the flow in the vortex tubes should be, except for the considered planar vortices present features swirling three-dimensional flows in cylindrical channels. Consider a long tube (Fig. 2) near the closed end which is located swirler – a gas distribution device that provides spin when entering the gas pipe.

ISBN: 978-988-19253-6-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Computing Complex Singularities of Differential Equations with Chebfun

Marcus Webb

Cambridge Centre for Analysis,
University of Cambridge

Based on work supervised by Nick Trefethen in 2011, funded by EPSRC

25th Biennial Conference on Numerical Analysis
University of Strathclyde, Glasgow

27th June 2013

WEEKLY UPDATE

BROUGHT TO YOU BY THE DNC COMMUNICATIONS DEPARTMENT

September 5, 2014

Michigan Democrats Launch Online Ballot-Application Tool

On Thursday, DNC Chair Rep. Debbie Wasserman Schultz joined Michigan Democratic Party Chair Lon Johnson and Democratic Secretary of State candidate Godfrey Dillard to announce the launch of a new tool that will allow Michigan voters to apply for absentee ballots online.

At the press conference Rep. Wasserman Schultz said, "There is a clear contrast in the fundamental priorities of the Democratic and Republican parties. While Republicans in Michigan attempt to implement unnecessary voting restrictions, Democrats like those here in Michigan will continue working to remove these voting barriers to ensure that every eligible citizen can cast their ballot."

Godfrey Dillard echoed Rep. Wasserman Schultz, saying, "I'm thrilled to join this announcement, because we should be promoting common sense, secure ways for more people to have access to the democratic process in our state."

He continued, "As Michigan's Secretary of State, I will work tirelessly to protect the fundamental right to vote, restore transparency, and promote accessibility for all. Increasing access to the ballot and empowering more Michiganders to vote should be job #1 for elections officials in our state - not more partisan Republican politics aimed at keeping Michigan citizens from the polls."

Chair Lon Johnson highlighted the importance of the program, saying, "With many voters having to be away from their communities on Election Day due to work, childcare and other responsibilities, more and more voters are using absentee voting as a way of casting their ballot – as shown by the fact that more than 27 percent of votes cast in Michigan's 2012 election were absentee ballots."

Since 2002, the percentage of votes cast as absentee ballots has increased from 16.5% to more than 27%. Currently, clerks across Michigan receive absentee ballot requests through option such as mail, email, and fax. Like the previous methods, this new online tool will allow voters to send applications directly and securely to the clerk from a smartphone.

Paid for and authorized by the Democratic National Committee, www.democrats.org. This communication is not authorized by any candidate or candidate's committee.

What is quantum information?

Olimpia Lombardi[1] – Federico Holik[2] – Leonardo Vanni[3]

[1] CONICET – Universidad de Buenos Aires
[2] CONICET – Universidad Nacional de la Plata
[3] Universidad de Buenos Aires

1.- Introduction

The word 'information' refers to a polysemantic concept associated with very different phenomena, such as communication, knowledge, reference and meaning (Floridi 2010, 2011). In the discussions about this matter, the first distinction to be introduced is that between a semantic view, according to which information carries semantic content and, thus, is related to notions as reference and meaning, and a statistical view, concerned with the statistical properties of a system and/or the correlations between the states of two systems. Although the *locus classicus* of the statistical concept is the famous article by Claude Shannon (1948), there are many other formal concepts of information, such as the Fisher information (see Fisher 1925), or the algorithmic information (Chaitin 1987). However, the problems of interpretation do not disappear even when the attention is restricted to a single formal concept (see Lombardi, Holik and Vanni 2014).

During the last decades, new interpretive problems have arisen with the advent of quantum information, which combine the difficulties in the understanding of the concept of information with the well-known foundational puzzles derived from quantum mechanics itself. This situation contrasts with the huge development of the research field named 'quantum information', where new formal results multiply rapidly. In this context, the question 'What is quantum information?' is still far from having an answer on which the whole quantum information community agrees. In fact, the positions about the matter range from those who seem to deny the existence of quantum information (Duwell 2003), those who consider that it refers to information when it is encoded in quantum systems (Caves and Fuchs 1996), and those who conceive it as a new kind of information absolutely different than Shannon information (Jozsa 1998; Brukner and Zeilinger 2001).

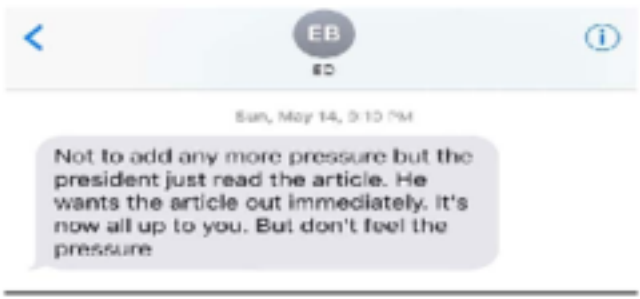
In the present article we will address the question 'What is quantum information?' from a conceptual viewpoint. For this purpose, in Section 2 Schumacher's formalism is introduced by contrast with Shannon's theory. In Section 3 the definition of quantum information in terms of a quantum source is discussed. Section 4 is devoted to analyze the definition of information in terms of coding theorems. These tasks lead us to focus on the relationship between Shannon entropy and von Neumann entropy in Section 5, and to discuss the differences between the concepts of bit and

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ROD WHEELER,	:	
Plaintiff,	:	Civil Action No.:
v.	:	
	:	**COMPLAINT**
TWENTY-FIRST CENTURY FOX, INC., FOX NEWS NETWORK LLC, MALIA ZIMMERMAN, in her individual and professional capacities and ED BUTOWSKY, in his individual and professional capacities,	:	**Jury Trial Demanded**
Defendants.	:	

PRELIMINARY STATEMENT

1. On May 14, 2017, Mr. Wheeler received the following text message from Defendant Ed Butowsky:



2. The "president" referred to in this text message is President Donald Trump. The "article" – which was published by Fox News's Malia Zimmerman less than 36 hours after this text message was sent – reported that a murdered Democratic National Committee ("DNC") staffer, Seth Rich, was the source of the now infamous DNC emails leaked by WikiLeaks during the 2016 Presidential primaries. The motivation behind the article: establish that Seth Rich provided WikiLeaks with the DNC emails to shift the blame from Russia and help put to bed

GATTACKING BLUETOOTH SMART DEVICES

Sławomir Jasek, SecuRing (slawomir.jasek@securing.pl)

Whitney forms: a class of finite elements for three-dimensional computations in electromagnetism

Alain Bossavit

Indexing terms: Electromagnetic theory, Eddy currents, Mathematical techniques

Abstract: It has been recognised that numerical computations of magnetic fields by the finite-element method may require new types of elements, whose degrees of freedom are not field values at mesh nodes, but other field-related quantities like e.g. circulations along edges of the mesh. A rationale for the use of these special 'mixed' elements can be obtained if one expresses basic equations in terms of *differential forms* instead of vector fields. The paper gives an elementary introduction to this point of view, presents Whitney forms (the mixed finite elements alluded to) and sketches two numerical methods (dual, in some sense) for eddy-current studies based on these elements.

1 Introduction

For those familiar with differential forms, Maxwell's equations are best expressed in the language they provide: h and e are 1-forms, i.e. forms of degree one, b and j are 2-forms. Thus, as we shall show in Section 3 of this paper, which consists in an elementary introduction to differential forms, words (but the *circulations* of h and e along paths make sense from the physical point of view, while the *fluxes* of b and j may be understood through surfaces. Differential forms are, therefore, a useful tool, and some have argued that they should be used in electrodynamics, at least at the research level [3, 10, 12, 14], and even for teaching [13]. But it is often felt that, at least in the case of eddy-current studies, which never venture out of the nonrelativistic realm, the full power of this tool is not called for. Indeed, it can be observed that most numerical analysts and engineers engaged in the study of electromagnetism prefer to think in terms of vector fields. Moreover, representations in coordinates are often preferred to vector expressions. It is therefore understandable that the bulk of the effort towards finite-element modelling has consisted, up to now, in adapting to vector-field methods which worked well for scalar fields, like e.g. those used for solving the heat equation.

Paper 6262A (E8), first received 4th January and in revised form 5th June 1990

The author is with Electricité de France, Département des Etudes de Gestion, 92141 Clamart, France

If such a trend were to continue, it would contrast with the present tendency to parsimonization which can be seen to pervade all physics. According to this tendency, attention should focus on geometrical entities, and not on their representations as multiples of values in some coordinate system. If we accept this trend, it will not be difficult to argue further than differential forms, and not vector fields, are the appropriate geometrical entities. But this will fail to convince the practising programmer who has to deal with such objects as finite-element shape functions. These seem to require a co-ordinate system for their manipulation. The situation will be different if we can define geometrical objects that are to differential forms what finite-element interpolating functions are to scalar fields.

This is precisely the definition of Whitney forms. Briefly stated (Section 3 of the paper gives a more comprehensive description), they are a family of differential forms on a simplicial mesh (i.e. a network of tetrahedra, as used in finite-element studies), defined in such a way that p forms are determined by their integrals on p-simplices. One-forms (such as, in electricity, h and e) can then be approximated by a suitable linear combination of Whitney forms of degree 1, the coefficients being the circulations of the field along the edges of the mesh. In other words, Whitney 1-forms play the role of finite elements for h or e, but the so-called degrees of freedom are associated with edges of the mesh, and are not the values of the components of the field at mesh nodes. This justifies the nickname of 'edge elements' for Whitney 1-forms. Similarly, there are 'facet elements' which accommodate 2-forms, the degrees of freedom being fluxes across facets. 'Nodal elements' are just piecewise-linear functions (they are commonly called P^1), and 'volume elements' are piecewise-constant functions (similarly known as P^0).

Section 4 of the paper shows how these concepts can be used to devise approximation methods for the eddy-current equations. The two methods we propose look, in some sense, symmetrical. This symmetry, or rather this duality, is rooted in the duality properties of the mathematical structure that differential forms constitute.

All these arguments, we think, converge to suggest that differential forms should be used as a working tool in numerical modelling of electromagnetic problems.

This does not imply such a radical change of thinking habits as we might fear. We have tried to present the topic to simplify the transition from vector fields to differential forms, albeit at the risk of criticism from the side

Who steers who steers?

A note on identifying vulnerable moral propensities

Steven Kaas & Steve Rayhawk
stevenkaas@gmail.com

There are a variety of processes that steer the future; that is, they move it toward certain states and away from others dynamically, with changing behaviors in response to changing conditions. Our decisions now don't just steer the future directly, but influence what the major steering processes in the future will be. Certain dangers attend such a project. Often the replacement of part of an ecosystem or a society with an engineered substitute, designed on the basis of a partial understanding, meets with severe drawbacks from unrecognized missing functionality that was demolished or displaced. In the same way, a project to take into hand the steering of the future, to fulfill its potential according to some moral vision, risks demolishing or displacing some unrecognized steering processes that generated and preserved the correctness of the moral sense behind the vision. While this risk cannot be avoided entirely, it can be mitigated by developing better tools for identifying or avoiding interference with unrecognized steering processes. In light of modern physical ontology, and in light of the abstractness of some of the plausible processes (such as the relative market success of firms, or historical evolutionary selection), we suggest that such tools should be rooted in a very conservatively general theoretical framework, based on finding factorizations of the world's state space into potential "steering" and "steered" state subspaces, with partially coupled dynamics.

> *Quis custodiet ipsos custodes?* (Who will guard the guardians themselves?)
>
> Juvenal, Roman poet, on the problem of engineering stably moral governance

> Yo dawg, I heard you like cars, so we put a car in your car, so you can drive while you drive.
>
> Xzibit, television presenter, on upgrading a car to contain a racing simulation

Just as our evolutionary history has selected for brains that select courses of action expected to achieve goals previously associated with reproductive success, and just as the authors of constitutions have written laws designed to cause good laws to be written, when we attempt to think about "steering the future", we engage in a project to "drive while we drive": to strategically influence the main factors that will strategically influence the future.

LPE vulnerabilities exploitation on Windows 10 Anniversary Update

Drozdov Yurii

Drozdova Liudmila

SPEAKE(a)R: Turn Speakers to Microphones for Fun and Profit

Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici
Ben-Gurion University of the Negev
Cyber Security Research Center
gurim@post.bgu.ac.il; yosef.solewicz@gmail.com; daidakul@post.bgu.ac.il; elovici@post.bgu.ac.il

Demo video: https://www.youtube.com/watch?v=ez3o8aIZCDM

Abstract

It's possible to manipulate the headphones, earphones, and simple earbuds connected to a computer, silently turning them into a pair of eavesdropping microphones. This paper focuses on the cyber security threat this behavior poses. We introduce 'SPEAKE(a)R,' a new type of espionage malware that can covertly turn the headphones, earphones, or simple earbuds connected to a PC into microphones when a standard microphone is not present, muted, taped,[1] or turned off. We provide technical background at the hardware and OS levels, and explain why most of the motherboards and audio chipsets of today's PCs are susceptible to this type of attack. We implemented a malware prototype and tested the signal quality. We also performed a series of speech and recording quality measurements and discuss defensive countermeasures. Our results show that by using SPEAKE(a)R, attackers can record human speech of intelligible quality and eavesdrop from nine meters away.

1. Introduction

Audio playing equipment such as loudspeakers, headphones, and earphones are widely used in PCs, laptops, smartphones, media entertainment systems, and more. In this section we refer to any audio playing equipment that contains speakers (loudspeakers, headphones, earphones, etc.) as speakers.

Speakers aim at amplifying audio streams out, but a speaker can actually be viewed as a microphone working in reverse mode: loudspeakers convert electric signals into a sound waveform, while microphones transform sounds into electric signals. Speakers use the changing magnetic field induced by electric signals to move a diaphragm in order to produce sounds. Similarly, in microphone devices, a small diaphragm moves through a magnetic field according to a sound's air pressure, inducing a corresponding electric signal [1]. This bidirectional mechanism facilitates the use of simple headphones as a feasible microphone, simply by plugging them into the PC microphone jack. It should be clear that in practice, speakers were *not* designed to perform as microphones and the recorded signals will be of low quality.

1.1. Jack retasking

A typical computer chassis contains a number of audio jacks, either on the front panel, rear panel, or both. These jacks are the sockets for plugging in various audio equipment such as speakers, headphones, and microphones. Each jack is used either for input (line in), or output (line out). The audio ports usually have a conventional coloring system; typically green is used for speakers (output jack), blue for line in (input jack), and pink for microphones (input jack).

Interestingly, the audio chipsets in modern motherboards and sound cards include an option to change the function of an audio port at software level, a type of audio port programming sometimes referred to as jack retasking or jack remapping. This option is available on Realtek's (Realtek Semiconductor Corp.) audio chipsets, which are integrated into a wide range of PC motherboards today. Jack retasking, although documented in applicable technical specifications, is not well-known, as was mentioned by the Linux audio developer, David Henningsson, in his blog:

"Most of today's built-in sound cards are to some degree retaskable, which means that they can be used for more than one thing. ...the kernel exposes an interface that makes it possible to retask your jacks, but almost no one seems to use it, or even know about it" [2].

1.2. Microphone-less eavesdropping

The fact that headphones, earphones, and earbuds are physically built like microphones, coupled with the fact

[1] "Why has Mark Zuckerberg taped over the webcam and microphone on his MacBook?" [4]

Work Capability Assessment:
deaths and suicides

"I say to those watching today and who are genuinely sick, disabled or are retired. You have nothing to fear. This government and this party don't regard caring for the needy as a burden. It is a proud duty to provide financial security to the most vulnerable members of our society and this will not change. This is our contract with the most vulnerable."

Iain Duncan Smith - October 2010

Introduction

The Work Capability Assessment is the assessment (initially carried out by Atos) that was introduced as part of the Government's 'reforms' to Incapacity Benefit. The Work Related Activity Group is defined as a group for people whose condition makes it unreasonable to require them to work. The Support Group is for people with more severe levels of disability who are considered to have limited capability even for work related activity.

Very quickly stories emerged of the terrible impact that the assessment was having on people's lives. In particular, many people have been found fit to work despite severe and diagnosed health conditions. Some people have taken their own lives and many have died shortly after this assessment.

The following testimony is taken directly from two produced reports produced by the Spartacus Network:

- Spartacus Network (2012) The People's Review of the Work Capability Assessment. We Are Spartacus.
- Spartacus Network (2013) The People's Review of the Work Capability Assessment - Further Evidence. We Are Spartacus.

For reference purposes this document is:

Spartacus Network (2015) *Work Capability Assessment: deaths and suicides*. We Are Spartacus.

The short-link to access this file is bit.ly/WCA-deaths

For more information go to: www.spartacusnetwork.org.uk

Author: Spartacus Network
Publisher: We Are Spartacus
Revised Version Published: 28th April 2015

An Introduction to the Theory of Elliptic Curves

Joseph H. Silverman

Brown University and
NTRU Cryptosystems, Inc.

Summer School on
Computational Number Theory and Applications to Cryptography
University of Wyoming

June 19 – July 7, 2006

The Python Bites your Apple

Fuzzing and exploiting OSX Kernel bugs

Flanker

KeenLab Tencent

XKungfoo Shanghai, April 2016

Axion Training workshop
Patras, 18 May 2006

Polarized laser beams in external magnetic fields

Yannis K. Semertzidis

Brookhaven National Lab

- **PVLAS result**
- **History of the result**
- **Possible exotic solutions (not likely)**
- **Possible new systematic error**
- **Future/Summary**

Book Review

Rudolf Taschner, The Continuum. A Constructive Approach to Basic Concepts of Real Analysis. Vieweg-Verlag Wiesbaden 2005, XI, 136 pp., Hardcover, EUR 36.90, ISBN 3-8348-0040-6.

The real numbers, visualised as the unbroken, perfectly homogeneous real line, form the foundation upon which all of analysis rests. The logically consistent and rigorous construction of real numbers, starting out with nothing more than the naturals and their evident properties, ranks among the greatest intellectual achievements of mankind. It has not been achieved easily though. From the ancient Greeks' disturbing discovery of irrational numbers via the vagueness of infinitesimals to the fierce foundational debate of the early twentieth century, the understanding of what exactly real numbers are has gone through many a revolution and crisis. While hardly anyone would disagree that, after two and a half millenia, satisfactory clarification has finally been reached, there is truth also in the quote, attributed to G.-C. Rota, that "every generation re-examines the reals in the light of its values and mathematical objectives". It is under this quote that *The Continuum* sets out to present an approach to the real numbers in the decidedly constructive spirit of L.E.J. Brouwer and H. Weyl. To the latter's famed (and identically titled) German text of 1918 the author pays explicit deference.

In which respect is the formal theory of the real numbers, as advocated by G. Cantor and R. Dedekind, deficient? In its first chapter, *The Continuum* explains through striking examples why a statement about real numbers may be easy to prove *formally* yet at the same time may forever remain beyond the reach of even the most powerful *actual* verification. It becomes apparent that for all reasonable purposes most real numbers can only be dealt with by means of approximations, regardless of whether they are as prominent as π and e or as mysterious as γ. Together with historical remarks highlightening Weyl's role in the formation of a constructive theory of the continuum, these examples provide motivation for the subsequent rigorous part of the text. To develop the basic properties of real numbers, first a workable definition has to be given: a real number is simply a sequence (a_n) of n-digit decimal numbers (i.e., $10^n a_n$ is an integer) such that $|a_m - a_n| < 10^{-m} + 10^{-n}$ holds for all m and n. From this pragmatic definition all the well-known algebraic, order and topological properties of the continuum follow. So smoothly do they follow that the reader familiar with classical (i.e., formal) real analysis may fail to notice any discrepancies at all, except perhaps for some slightly unusual terminology. Discrepancies exist, however, and they become more pronounced as the text proceeds. Most of these discrepancies are addressed carefully, e.g. through a discussion of the concepts of apartness and locatedness which, though indispensable in the constructive context, are void in classical analysis. In a few instances, however, the presentation is not as clear. For example, the proof of the important bar theorem dissolves into a rather slick play with words, and the discussion of the amazing Weyl–Brouwer continuity theorem (which, simply put, asserts that a function between complete metric spaces is automatically continuous) would benefit from the simple observation that the classical analyst's obvious counterexample, the *sign* function, simply is not a function at all according to the constructive definition. Though unedifying, this is the only blemish on an overall pleasant text which leads elegantly and on little more than one hundred pages from the definition of a real number to compactness questions concerning families of continuous functions on arbitrary metric spaces (with the surprising Dini–Brouwer theorem as yet another gem). Since the text is quite fast-paced, and also since it does not offer any concrete exercises or problems, the reader should have absorbed some sound real analysis beforehand.

Much has been said in the past about the overall world outlook of mathematicians being either idealist, formalist, or constructivist, with the latter representing an almost negligible minority attitude. About a century ago, H. Poincaré declared that formalism was a sickness from which mathematics would have to recover. Even at the time, not everybody agreed, and today the formal-axiomatic view of the reals is evidently all-dominant. This, however, may change as computational aspects pervade and influence ever wider parts of mathematics. From a computational perspective, a constructive theory of the continuum is clearly preferable to a theory which for instance has no difficulties yielding the unique existence of a number with some property or other but which at the same time cannot possibly provide a means to find this number. The eminent constructive mathematician D. Bridges has argued that constructivism addresses mathematical reality, whereas idealism and formalism both deal with a form of mathematical virtual reality. Every reader of *The Continuum* is thus in for a reality-check as Taschner's elegant, solid text offers an eye-opening and refreshing view on supposedly well-known facts. It has been the author's objective to provide a natural, constructive and short path to the real numbers. Notwithstanding the minor reservations made earlier, the text largely lives up to its goals; it can be recommended for everyone seriously interested in the foundations of analysis.

Canterbury (NZ) **A. Berger**

© 2007 WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim

Physica A 177 (1991) 31–37
North-Holland

The zeroes of the partition function of the random energy model

B. Derrida
Service de Physique Théorique de Saclay [1], F 91191 Gif-sur-Yvette Cedex, France

The random energy model is one of the simplest disordered models containing some of the physics of spin glasses. The zeroes of the partition function in the complex temperature plane are determined for this model. They either lie on simple lines or are dense in some regions of the complex plane.

Locating the zeroes of partition functions in the complex plane of the physical variables (magnetic field, temperature) has been a subject of constant interest in the theory of phase transitions for the last decades [1–9]. Phase transitions are expected to show up as accumulation points on the real axis of these complex zeroes. In the case of ferromagnetic interactions, the Lee and Yang theorem [1,2] guarantees that the zeroes in the complex plane of the magnetic field are all located along the imaginary axis. By contrast, in the complex plane of temperature, the patterns of zeroes can have more complicated structures [3]: isolated points, lines, areas and even fractals [10].

Several attempts of understanding disordered systems by looking at the distribution of zeroes in the complex plane have been tried [11,12]. Except for establishing the existence of Griffiths [13] singularities in dilute ferromagnets, where the proof is based on an estimation of the density of zeroes in the complex plane of the magnetic field, little progress has been made so far in disordered systems by looking at the complex zeroes of the partition function. Analyzing the patterns of zeroes calculated numerically is usually very hard because of the system sizes (the number of zeroes is very small) and of the sample to sample fluctuations, which are usually very large for small systems.

Recently, the zeroes of the partition function [14] of the random energy [15] model (which is one of the simplest models containing some of the physics of spin glasses) have been studied numerically, and they were found to have rather simple structures: lines and areas. The goal of the present paper is to describe these zeroes by an analytical approach. The main part of the argument is a direct generalization of an idea presented recently in the case of directed paths [16]. The main result is shown in fig. 1.

The random energy model (REM) was introduced as a very simplified spin glass

[1] Laboratoire de la Direction des Sciences de la Matière du Commissariat à l'Energie Atomique.

0378-4371/91/$03.50 © 1991 – Elsevier Science Publishers B.V. (North-Holland)

Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for Services

Matteo Campanelli[1], Rosario Gennaro[1], Steven Goldfeder[2], and Luca Nizzardo[3,4]

[1] City College of New York, USA
{rosario@cs.ccny, ncampanelli@gc}.cuny.edu
[2] Princeton University, USA
stevenag@cs.princeton.edu
[3] IMDEA Software Institute, Madrid, Spain.
luca.nizzardo@imdea.org
[4] Universidad Politécnica de Madrid, Spain.

Abstract. Zero Knowledge Contingent Payment (ZKCP) protocols allow fair exchange of sold goods and payments over the Bitcoin network. In this paper we point out two main shortcomings of current proposals for ZKCP.

First we show an attack that allows a buyer to learn partial information about the digital good being sold, without paying for it. This break in the zero-knowledge condition of ZKCP is due to the fact that in the protocols we attack, the buyer is allowed to choose common parameters that normally should be selected by a trusted third party. We present ways to fix this attack that do not require a trusted third party.

Second, we show that ZKCP are not suited for the purchase of digital *services* rather than goods. Current constructions of ZKCP do not allow a seller to receive payments after proving that a certain service has been rendered, but only for the sale of a specific digital good. We define the notion of *Zero-Knowledge Contingent Service Payment* (ZKCSP) protocols and construct two new protocols, for either public or private verification.

We implemented and tested the attack on ZKCP, and our two new ZKCSP protocols, showing their feasibility for very realistic examples. We present code that learns, without paying, the value of a Sudoku cell in the "Pay-to-Sudoku" ZKCP implementation [17]. We also implement ZKCSP protocols for the case of *Proof of Retrievability*, where a client pays the server for providing a proof that the client's data is correctly stored by the server. A side product of our implementation effort is a new optimized circuit for `SHA256` with less than a quarter than the number of AND gates of the best previously publicly available one. Our new `SHA256` circuit may be of independent use for circuit-based MPC and FHE protocols that require `SHA256` circuits.

1 Introduction

The problem of fair exchange in which two parties want to swap digital goods such that neither can cheat the other has been studied for decades, and indeed it has been shown that fairness is unachievable without the aid of a trusted third party [22]. However, using Bitcoin or other blockchain-based cryptocurrencies, it has been demonstrated that fair-exchange can be achieved in a completely trustless manner. The previous results were not incorrect; a third party is definitely necessary, but the key innovation that Bitcoin brings to fair exchange is that the blockchain can fill the role of the trusted party, and essentially eliminate trust.

Consider Alice, an avid fan of braintensers that has a Sudoku puzzle that she is stumped on. After trying for days to solve the puzzle, Alice gives up and posts the puzzle on an online message board proclaiming, "I will pay whoever provides me the solution to this puzzle". Bob sees this message, solves the puzzle, and wants to sell Alice the solution. But there's a problem: Alice wants Bob to first provide the solution so that she can verify it's correct before she pays him, whereas