(67902) Topics in Theory and Complexity Nov 29, 2006

Lecture 5

Lecturer: Irit Dinur *Scribe: Yoad Lustig*

1 Preliminaries

First, let us recall some relevant material from the last lecture.

For a graph $G = (V, E)$ and two sets of vertices $A, B \subseteq V$ we denote by

$$E(A, B) = \{\, \{u, v\} \in E \mid u \in A, v \in B\}$$

the set edges between A and B. For a set of vertices $S \subseteq V$ we denote the complement set by $\overline{S} = V \setminus S$. We defined the *expansion* of G to be

$$h(G) = \min_{\substack{S \subseteq V \\ |S| \leq \frac{|V|}{2}}} \frac{|E(S, \overline{S})|}{|S|}.$$

Intuitively, the expansion measures "the bottle neck" of the number of edges across cuts (normalized by the size of the sets involved). A family of graphs $\{G_i\}_{i=1}^{\infty}$ is ϵ-*expanding* if for every $i \geq 0$ we have $h(G_i) \geq \epsilon$. The *Adjacency matrix* of G is a matrix $A_{|V|\times|V|}$ in which $(A)_{uv} = \begin{cases} 1 & (u,v) \in E \\ 0 & (u,v) \notin E \end{cases}$. Throughout the lecture we use G to denote a graph with n vertices and A to denote its adjacency matrix.

2 Expansion and eigenvalues

In this section we will look into the connection between expansion properties of graphs and the eigenvalues of its adjacency matrix. This can be seen as an algebraic view of expansion and expanders.

Note that in a d-regular graph we have that for every vertex x the sum of entries of the x row in the adjacency matrix, and the sum of entries of the x column in the adjacency matrix are both d. Formally, for every vertex v we have $\sum_{u \in V} (A)_{vu} = d = \sum_{u \in V} (A)_{uv}$.

Note also, that as our graph is undirected A is a symmetric real matrix. Therefore A is diagonalizable with an orthonormal base of eigenvectors and all its eigenvalues are real. It is customary to denote the eigenvalues of A, in descending order, by $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{n-1}$. (Note that we allow multiplicity and different eigenvalues might be equal.)

The proof of the following claim will be given as an exercise.

Claim 1 *For a d-regular graph G with adjacency matrix A whose eigenvalues are (in descending order) $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{n-1}$ the following are true:*

1. $\lambda_0 = d$.
2. $\lambda_{n-1} \geq -d$
3. *G is connected iff $\lambda_0 > \lambda_1$.*
4. *G is bipartite iff $\lambda_{n-1} = -\lambda_0$.*

It turns out that the eigenvalue that has the second largest absolute value has very interesting properties. We denote $\lambda(G) = \max\{|\lambda_1|, |\lambda_{n-1}|\}$ (by our claim $\lambda(G)$ is the eigenvalue that has the second largest absolute value). In case the graph G is fixed we abuse notation and use λ to denote $\lambda(G)$.

A graph $G = (V, E)$ is a (n, d, λ)-*expander* (for $\lambda < d$) if $|V| = n$, the graph G is d regular, and $\lambda(G) = \lambda$.

Before proceeding to the next theorem we would like to recall some linear algebra we need in its proof.

For $u, v \in \mathbb{R}^n$ the *inner product* of u and v, denoted $\langle u, v \rangle$, is $\sum_{i=1}^{n} u_i v_i$. The l^2*-norm* (or *Euclidean norm*) of $v \in \mathbb{R}^n$, denoted $\|v\|_2$ (or simply $\|v\|$), is $\sqrt{\langle v, v \rangle} = \sqrt{\sum_{i=1}^{n} |v_i|^2}$. The l^1*-norm* of $v \in \mathbb{R}^n$, denoted $\|v\|_1$, is $\sum_{i=1}^{n} |v_i|$. A known inequality is Cauchy-Schwartz inequality that states that for every $u, v \in \mathbb{R}^n$ we have $\langle u, v \rangle \leq \|v\|_2 \cdot \|u\|_2$. For $x, v_0, \ldots, v_n \in \mathbb{R}^n$ we denote by $x \perp v_0, \ldots, v_n$ the statement that x is orthogonal to $v_0, \ldots, v_n$.

We proceed to define the *Rayleigh quotients*.

Claim 2 *For a graph G with a real and symmetric adjacency matrix A whose eigenvalues (in descending order) are $\lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{n-1}$, and their corresponding (orthonormal) eigenvectors are $v_0, \ldots, v_{n-1}$ we have:*

1. $\lambda_0 = \max_{x \in \mathbb{R}^n} \frac{\langle a, Ax \rangle}{\langle x, x \rangle}$
2. *For every $i \leq n-1$ we have*

$$\lambda_i = \max_{\substack{x \in \mathbb{R}^n \\ x \perp v_0, \ldots, v_{i-1}}} \frac{\langle a, Ax \rangle}{\langle x, x \rangle}$$

Proof We begin by proving the claim for λ_0. Let $x \in \mathbb{R}^n$ be a vector. Since the eigenvectors are a base we have $x = \sum_{i=1}^{n} \alpha_i v_i$ for some scalars $\{\alpha_i\}_{i=1}^{n}$. Therefore,

$$\begin{aligned}
\langle x, x \rangle &= \left\langle \sum_{i=1}^{n} \alpha_i v_i, \sum_{i=1}^{n} \alpha_i v_i \right\rangle \\
&= \sum_{i,j} \alpha_i \alpha_j \langle v_i, v_j \rangle \\
&= \sum_{i \neq j} \alpha_i \alpha_j \langle v_i, v_j \rangle + \sum_{i} \alpha_i^2 \langle v_i, v_i \rangle \\
&= \sum_{i \neq j} \alpha_i \alpha_j \cdot 0 + \sum_{i} \alpha_i^2 \cdot 1 = \sum_{i} \alpha_i^2
\end{aligned}$$

In a similar fashion,

$$\begin{aligned}
\langle x, Ax \rangle &= \left\langle \sum_{i=1}^{n} \alpha_i v_i, A\left(\sum_{i=1}^{n} \alpha_i v_i \right) \right\rangle \\
&= \left\langle \sum_{i=1}^{n} \alpha_i v_i, \sum_{i=1}^{n} \alpha_i A v_i \right\rangle \\
&= \left\langle \sum_{i=1}^{n} \alpha_i v_i, \sum_{i=1}^{n} \alpha_i \lambda_i v_i \right\rangle \\
&= \sum_{i,j} \alpha_i \alpha_j \lambda_j \langle v_i, v_j \rangle \\
&= \sum_{i \neq j} \alpha_i \alpha_j \lambda_j \langle v_i, v_j \rangle + \sum_{i} \alpha_i^2 \lambda_i \langle v_i, v_i \rangle
\end{aligned}$$

$$= \sum_{i \neq j} \alpha_i \alpha_j \lambda_j \cdot 0 + \sum_i \alpha_i^2 \lambda_i \cdot 1 = \sum_i \alpha_i^2 \lambda_i$$

Therefore,

$$\frac{\langle x, Ax \rangle}{\langle x, x \rangle} = \frac{\sum_i \alpha_i^2 \lambda_i}{\sum_i \alpha_i^2} \leq \frac{\max_i\{\lambda_i\} \cdot \sum_i \alpha_i^2}{\sum_i \alpha_i^2} = \max_i\{\lambda_i\} = \lambda_0.$$

Clearly, for $x = v_0$ we get the equality.

The proof for the λ_i case, for $i > 0$, is very similar. For $x \perp v_0, \ldots, v_{i-1}$ we have $\alpha_0, \ldots, \alpha_{i-1} = 0$. Therefore, by the same technical derivations we get

$$\max_{\substack{x \in \mathbb{R}^n \\ x \perp v_0, \ldots, v_{i-1}}} \frac{\langle x, Ax \rangle}{\langle x, x \rangle} = \max_{j \geq i}\{\lambda_j\} = \lambda_i$$

■

Returning to our main theme we can now prove (at least one side of):

Theorem 3 *For a d-regular graph G we have $\frac{h(G)^2}{2d} \leq d - \lambda(G) \leq 2h(G)$.*

Proof We will only proof the easier inequality which is $d - \lambda(G) \leq 2h(G)$. It is not hard to see that (as the graph is d-regular) $v_0 = \overline{1} = (1, \ldots, 1)$. Using reasoning similar to the one used to prove the Rayleigh quotients claim it is not hard to arrive at $\max_{\substack{x \in \mathbb{R}^n \\ x \perp \overline{1}}} \frac{|\langle x, Ax \rangle|}{\langle x, x \rangle} = \lambda(G) = \lambda$. Therefore, presenting a vector $x \perp \overline{1}$ for which $\frac{|\langle x, Ax \rangle|}{\langle x, x \rangle} \geq d - 2h(G)$ implies that $\lambda \geq d - 2h(G)$ from which $d - \lambda(G) \leq 2h(G)$ follows. We proceed to present such a vector x.

Let $S \subseteq V$ be a set of vertices for which $|S| \leq \frac{n}{2}$ and $\frac{|E(S, \overline{S})|}{|S|} = h(G)$. Let x be the vector defined by

$$x_v = \begin{cases} |\overline{S}| & v \in S \\ -|S| & v \in \overline{S} \end{cases}$$

(we index x coordinates by vertices).

First, we prove that $x \perp \overline{1}$. We simply calculate

$$\langle x, \overline{1} \rangle = \sum_{v \in V} x_v \cdot 1 = \sum_{v \in S} |\overline{S}| + \sum_{v \in \overline{S}} (-|S|) = |S| \cdot |\overline{S}| - |\overline{S}| \cdot |S| = 0$$

Next, we calculate

$$\langle x, x \rangle = \sum_{v \in V} x_v^2 = \sum_{v \in S} |\overline{S}|^2 + \sum_{v \in \overline{S}} |S|^2 = |S| \cdot |\overline{S}|^2 + |\overline{S}| \cdot |S|^2 = |S| \cdot |\overline{S}| \cdot (|S| + |\overline{S}|) = |S| \cdot |\overline{S}| \cdot n$$

Finally we calculate

$$\langle x, Ax \rangle = \sum_{v \in V} x_v (Ax)_v = \sum_{v \in V} x_v \sum_{u \sim v} x_u = 2 \sum_{(u,v) \in E} x_u x_v.$$

Note that $|E(S, S)|$ equals the number of edges touching S (i.e. $d|S|$) minus the number of edges leaving S (i.e. $|E(S, \overline{S})|$). Therefore,

$$\begin{aligned}
\sum_{(u,v) \in E} x_u x_v &= 2|E(S, \overline{S})|(|\overline{S}| \cdot (-|S|)) + (d|S| - |E(S, \overline{S})|)|\overline{S}|^2 + (d|\overline{S}| - |E(S, \overline{S})|)|S|^2 \\
&= |E(S, \overline{S})|(-2|S| \cdot |\overline{S}| - |\overline{S}|^2 - |S|^2) + d|S| \cdot |\overline{S}|^2 + d|\overline{S}| \cdot |S|^2 \\
&= |E(S, \overline{S})| \cdot (-(|S| + |\overline{S}|)^2) + d|S| \cdot |\overline{S}|(|S| + |\overline{S}|) \\
&= |E(S, \overline{S})| \cdot (-(n^2)) + d|S| \cdot |\overline{S}| \cdot n \\
&= -(n^2)h(G)|S| + d|S| \cdot |\overline{S}| \cdot n = n|S| \cdot |\overline{S}|(d - \frac{n}{|\overline{S}|} h(G))
\end{aligned}$$

Since $|S| \leq \frac{n}{2}$, we have $|\overline{S}| \geq \frac{n}{2}$. Therefore, $\frac{n}{|\overline{S}|} \leq 2$, and $\langle x, Ax \rangle \geq n|S| \cdot |\overline{S}|(d - 2h(G))$.
Finally, $\frac{\langle x,Ax \rangle}{\langle x,x \rangle} \geq d - 2h(G)$ as needed. ■

For a d-regular graph G the *spectral gap* of G is $d - \lambda(G)$. Note that the theorem above allows us to prove that a family of graphs is ϵ-expanding by showing for every $i \geq 1$ the spectral gap of G_i is greater or equal 2ϵ (i.e. $d - \lambda(G_i) \geq 2\epsilon$).

3 Algorithmic issues

Given a d-regular graph G can we compute $h(G)$ efficiently? Clearly, since we can compute eigenvalues, we can bound $h(G)$ since by the theorem above $h(G) \in [\frac{d-\lambda}{2}, \sqrt{2d(d-\lambda)}]$.

It is also clear that for any number a, showing that $h(G) \leq a$ is in NP, since if $h(G) \leq a$ then there must be a witness set S for which $\frac{|E(S,\overline{S})|}{|S|} \leq a$. On the other hand, it turns out that computing $h(G)$ exactly is NP-hard.

What about approximation algorithms? Is there a factor k, and a polynomial time algorithm that approximates $h(G)$ to multiplicative factor k? In the case of an undirected graph (not necessarily regular) this problem is known as the *sparsest cut* problem. The state of the art is a $\sqrt{\log(n)}$-approximation algorithm due to Arora-Rao-Vazirani in 2004. The sparsest cut problem is considered important since it rises naturally when tackling many graph problems. One of the natural algorithmic schemes is divide and conquer. In the context of graphs it is many times natural to divide the graph into subgraphs, solve the problem on each of the subgraphs and then combine the results. In many cases the complexity of combining the results depends (also) on the sparsity of the cuts between the subgraphs. Thus, finding good sparse cuts is beneficial for many algorithms that apply the divide and conquer scheme.

It is known today that approximating sparsest cut to some constant factor is NP-hard. If we assume the a certain conjecture (a strong version of the so-called unique games conjecture) then approximating the sparsest cut to $\log(\log(n))$ is also NP-hard.

4 Random walks on expanders

Let $\{X_i\}_{i=1}^{\infty}$ be a sequence of random variables that get as values vertices of a d-regular graph $G = (V, E)$ with n vertices and adjacency matrix A.

The sequence $\{X_i\}_{i=1}^{\infty}$ is a *Markov chain* if for every $i \geq 0$, and states $v_i \in V$ it holds that

$$Pr[X_{i+1} = v_{i+1} \mid X_i = v_i, X_{i-1} = v_{i-1}, \ldots, X_1 = v_1] = Pr[X_{i+1} = v_{i+1} \mid X_i = v_i]$$

and this probability does not depend on i. Note that in such a case we can look at the matrix $T_{n\times n}$ for which $(T)_{uv} = Pr[X_{i+1} = u \mid X_i = v]$. The matrix T is called the *transition* matrix of the Markov chain.

A *random walk* on a graph G is a Markov chain whose transition matrix is the normalized adjacency matrix $\tilde{A} = \frac{1}{d}A$. Intuitively, a transition in a random walk from a vertex v, chooses at random some edge originating at v, and moves along that edge.

It is not hard to see that the eigenvalues of $\tilde{A}$ are $\tilde{\lambda}_0 = \frac{1}{d}\lambda_0 = 1, \ldots, \tilde{\lambda}_{n-1} = \frac{1}{d}\lambda_{n-1}$.

A vector $\mathbf{p} \in \mathbb{R}^n$ is a *probability vector* if for every $i \geq 0$ we have $p_i \geq 0$ and $\sum_{i=1}^{n} p_i = 1$. Intuitively, a probability vector $\mathbf{p}$ represents a distribution on the vertices that assigns the vertex v the probability p_v. We denote by $\mathbf{u}$ (for uniform) the vector $\frac{1}{n}\overline{1}$ which corresponds to the uniform distribution.

Claim 4 *If at the i^{th} stage of a random walk the probability distribution on the vertices is $\mathbf{p}$, then at the $(i+1)^{\text{th}}$ stage, the probability distribution is $\tilde{A}\mathbf{p}$.*

Proof $(\tilde{A}\mathbf{p})_u = \sum_{v \in V} A_{uv} p_v = \sum_{v \in V} Pr[X_{i+1} = u \mid X_i = v] \cdot Pr[X_i = v] = Pr[X_{i+1} = v]$. ■

Therefore, if we start a random walk by choosing a vertex v according to the distribution $\mathbf{p}$ and then apply $t \geq 0$ random walk moves then the resulting distribution is $\tilde{A}^t\mathbf{p}$.

Note that since $\mathbf{u}$ is an eigenvector of $\tilde{A}$ with eigenvalue 1 we get $\tilde{A}\mathbf{u} = \mathbf{u}$ (and for every $t \geq 0$ we get $\tilde{A}^t\mathbf{u} = \mathbf{u}$). Intuitively, this corresponds to the fact that a random walk (on a regular graph G) that begins at a uniform distribution remains at a uniform distribution.

Next we prove, that whatever the starting distribution is, a random walk on G approaches the uniform distribution. Furthermore,we bound the rate of the convergence by a function of $\tilde{\lambda} = \frac{1}{d}\lambda(G)$.

Claim 5 *For any probability distribution* $\mathbf{p}$ *and* $t \geq 0$ *we have* $\left\|\tilde{A}^t\mathbf{p} - \mathbf{u}\right\|_1 \leq \tilde{\lambda}^t\sqrt{n}$.

Proof Let $\mathbf{e} = \mathbf{u} - \mathbf{p}$ (i.e. $\mathbf{p} = \mathbf{u} + \mathbf{e}$). First, lets note that $\mathbf{e}$ and $\mathbf{u}$ are orthogonal.
$\langle \mathbf{e}, \mathbf{u} \rangle = \langle \mathbf{u} - \mathbf{p}, \mathbf{u} \rangle = \langle \mathbf{u}, \mathbf{u} \rangle - \langle \mathbf{p}, \mathbf{u} \rangle = \sum_{i=1}^{n} \frac{1}{n} \cdot \frac{1}{n} - \sum_{i=1}^{n} p_i \frac{1}{n} = \frac{1}{n} \cdot 1 - \frac{1}{n} \cdot 1 = 0.$

We proceed to calculate $\tilde{A}\mathbf{p} - \mathbf{u}$. Note that expanding $\mathbf{e}$ according to the eigenvectors base we get $\mathbf{e} = \sum_{i=0}^{n-1} \alpha_i v_i$ where $\alpha_0 = 0$. Therefore:

$||\tilde{A}\mathbf{p} - \mathbf{u}||_2 = \left\|\tilde{A}\mathbf{u} - \tilde{A}\mathbf{e} - \mathbf{u}\right\|_2 = \left\|\tilde{A}\mathbf{e}\right\|_2 = \left\|\tilde{A}(\sum_{i=1}^{n-1} \alpha_i v_i)\right\|_2 = \left\|\sum_{i=1}^{n-1} \alpha_i \tilde{A} v_i\right\|_2 =$
$\left\|\sum_{i=1}^{n-1} \alpha_i \lambda_i v_i\right\|_2 \leq \left\|\tilde{\lambda} \sum_{i=1}^{n-1} \alpha_i v_i\right\|_2 = \left\|\tilde{\lambda}\mathbf{e}\right\|_2.$

Since $\mathbf{u} + \mathbf{e} = \mathbf{p}$, the vectors $\mathbf{u}, \mathbf{p}$, and $\mathbf{e}$ can be used to form a triangle. Since $\mathbf{u}$ and $\mathbf{e}$ are orthogonal, by Pythagoras theorem we know that $\|\mathbf{p}\|_2 \geq \|\mathbf{e}\|_2$. Another easy fact is that the l^2-norm of every probability vector is lesser or equal 1. Therefore $\left\|\tilde{A}\mathbf{p} - \mathbf{u}\right\|_2 \leq \left\|\tilde{\lambda}\mathbf{e}\right\|_2 \leq \left\|\tilde{\lambda}\mathbf{p}\right\|_2 \leq \tilde{\lambda}$.

The eigenvalues of $\tilde{A}^t$ are $\tilde{\lambda}_0^t, \ldots, \tilde{\lambda}_{n-1}^t$. Therefore, by the same reasoning we get that $\left\|\tilde{A}^t\mathbf{p} - \mathbf{u}\right\|_2 \leq \tilde{\lambda}^t = (\frac{\lambda}{d})^t$.

Finally, to phrase our results in l^1-norm terms, we note that for every $v \in \mathbb{R}^n$ we have $\|v\|_1 \leq \sqrt{n}\|v\|_2$. The latter follows quite easily from Cauchy-Schwartz. Let $sign(v) \in \{-1, 1\}^n$ be a vector of the signs of v. Namely, $sign(v)_i = \begin{cases} 1 & v_i \geq 0 \\ -1 & v_i < 0 \end{cases}$. It is not hard to see that $\|v\|_1 = \langle v, sign(v) \rangle$. By Cauchy-Schwartz we get $\|v\|_1 \leq \|v\|_2 \cdot \|sign(v)\|_2 = \sqrt{n}\|v\|_2$.

Thus we arrived at our desired result: $\left\|\tilde{A}^t\mathbf{p} - \mathbf{u}\right\|_1 \leq \sqrt{n}\tilde{\lambda}^t$. ■

5 Expanders and approximation-hardness amplification

For a graph G, denote by $\omega(G)$ the size of the largest clique G.

It is known that the following theorem is true.

Theorem 6 *There exists* $\alpha \leq 1$ *and* $\eta > 0$ *for which the gap problem of deciding, for a graph* G*, between the two options:*

1. $\omega(G) < \alpha n$
2. $\omega(G) \geq (1 + \eta)\alpha n$

is NP-hard.

Corollary 7 *If P does not equal NP then there is no polynomial time algorithm that given a graph G finds a clique in G of size at least* $\frac{1}{1+\eta}\omega(G)$.

Proof Assume, toward contradiction, otherwise and we will see how to distinguish between the cases 1 and 2 in polynomial time.

Given a graph G, run the approximation algorithm whose existence we assumed. If the algorithm returns a clique of size αn or more output 2. Otherwise, output 1.

If $\omega(G) \geq (1+\eta)\alpha n$ then the approximation algorithm is sure to return a clique of size αn and we will output 2. If, on the other hand, $\omega(G) < \alpha n$ then clearly the approximation algorithm cannot return a clique of size αn and we will output 1. ■

Our next goal is to show that from Theorem 6 we can derive a stronger result namely:

Theorem 8 *There exists* $\epsilon > 0$ *such that if P does not equal NP there is no algorithm A that given a graph G finds a clique A(G) of size at least* $\frac{1}{n^\epsilon}\omega(G)$.

We will not be able to complete the proof in this lecture, however, we will begin by presenting a failed attempt at a proof. The failed attempt will only prove a weaker result. Next lecture, however, we will combine the ideas from the failed attempt with techniques involving expander graphs to arrive at the desired result.

Before engaging in our failed attempt, we would like to comment about the state of our knowledge regarding approximating clique size. It is known that the hardness factor is in fact $n^{1-o(1)}$. The best approximation algorithm known gives us an approximation factor of $\frac{n}{(\log(n))^2}$.

proof attempt:

We will try to reduce the gap problem in Theorem 6 to our problem. Given a graph $G = (V, E)$ (which we think of as an instance given to the gap problem in Theorem 6) we construct a graph $H = (V_H, E_H)$ in the following manner: Let $t \geq 1$ be a natural number. The vertices of H are t-tuples of vertices of G (i.e. $V_H = V^t$). The edges of H are defined as follows:
$E_H = \{\langle (v_1, \ldots, v_t), (u_1, \ldots, u_t)\rangle \mid \{v_1, \ldots, v_t\} \cup \{u_1, \ldots, u_t\}$ is a clique in $G\}$.

Our first observation is that $\omega(H) = \omega(G)^t$. Clearly every clique of size m in G induces a clique of size m^t in H (all the tuples whose vertices are included in the clique). So, $\omega(H) \geq \omega(G)^t$. On the other hand, given a clique in H, the set of vertices of G that appear in the tuples in the clique must constitute a clique in G. If we start with less then m vertices in G then there are less then m^t tuples containing them. Therefore a clique of size m^t in H must contain tuples that contain at least m vertices in G. The result follows.

Therefore, $\omega(G) < \alpha n$ iff $\omega(H) \leq (\alpha n)^t = \alpha^t n^t$. On the other hand, $\omega(G) \geq (1+\eta)\alpha n$ iff $\omega(H) \geq (1+\eta)^t \alpha^t n^t$. Therefore, if we could have distinguished between the cases that the clique in H is of size smaller then $\alpha^t n^t$ or greater or equal $(1+\eta)^t \alpha^t n^t$ then we could have distinguished between cases 1 and 2 in G. (That is assuming we can compute H from G in polynomial time.)

For $t = O(\log(n))$ we get that $|V_H| = n^{O(\log(n))}$, and $(1+\eta)^t = n^{O(1)}$ as needed. However, there are two caveats. First, since H is not polynomial, it cannot be constructed in polynomial time from G. Therefore, this is not a polynomial time reduction but only a quasi-polynomial time reduction.

The second problem is that the input to the problem involving H is of the size of H, namely $N = n^{O(\log(n))}$. Therefore, the hardness factor $n^{O(1)}$ should be measured in terms of N. Since $N = 2^{O(\log(n)^2)}$ we get that the hardness factor is in fact $2^{\sqrt{O(\log(N))}}$.

In the next lecture we will combine the ideas presented here with expander constructions to get an improved result.