67902 - Topics in Theory - Complexity

Problem Set 1

(due November 22)

1. Prove the Projection Bound (also called Singleton's bound): for any $(n, k, d)_q$-code,

$$d + k \leq n + 1.$$

Hint: show that it suffices to find a pair of codewords that agree on $k - 1$ coordinates.

2. (Concatenation) Let C_1 be an $(n_1, k_1, d_1)_q$ code, and let C_2 be an $(n_2, k_2, d_2)_2$ code. Define the *concatenation* of C_1 and C_2, denoted $C_2 \circ C_1$, to be the following code. Let $x \in \{0,1\}^{k_1 \cdot \log_2 q}$. First view x as if it were a string in $[q]^{k_1}$ and apply the encoding C_1 to x. Next, for each symbol of $C_1(x)$, apply the code C_2 on the binary representation of that symbol. Concatenate the results together, and that is the resulting codeword.

   (a) For what value of k_2 is this transformation well-defined?

   (b) What are the (n, k, d) parameters of the new code? prove your answer.

   (c) Assume both C_1 and C_2 are linear codes. Is $C_2 \circ C_1$ linear?

3. (*) Suppose $C : [2^k]^K \to [2^k]^N$ is an $(N, K, D)_{2^k}$-code, with rate $r > 0$ and relative distance $\delta > 0$.

   Consider the following algorithm. Let $G_1, G_2, \ldots, G_{2^{3k^2}}$ be an enumeration of all possible $k \times 3k$ binary matrices. Given a string $x \in \{0,1\}^{kK}$ first encode it via C, and then encode the i-th symbol of $C(x)$ with the code generated by $G_{(i \bmod 2^{3k^2})}$. Concatenate the resulting encodings. This is a type of Justesen Code.

   Assuming $N \gg 2^{3k^2}$, what is the rate and distance of this binary code?

4. Recall that the Hadamard code has $(n \times 2^n - 1)$-generating matrix

$$\begin{pmatrix} 0 & 0 & 0 & & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 1 & 1 & & 1 \\ 1 & 0 & 1 & & 1 \end{pmatrix}$$

   Prove that a string $A \in \{0,1\}^{2^n}$ is a legal Hadamard codeword if and only if

$$\forall x, y \in \{0,1\}^n, \quad A[x] + A[y] = A[x + y]$$

   where all additions are modulo 2.