Coding Theory Spring 2009

Problem Set # 1

Due: April 7th, 2009 *Lecturer: Irit Dinur*

General Instructions:

- Please submit the exercise in the mailbox of Or Meir.
- Try to solve each problem first without consulting references. If you need references, please indicate clearly which reference you used.
- Team work: Allowed, but please limit yourself to groups of at most 3.14.

Questions:

1. **Hat Puzzle:** n people enter a room and a black or white hat is placed on each persons head (the hats are chosen independently at random). Each person can see all hats except his/her own, and no communication is allowed. Each person tries to guess his/her own hat color and writes down "Black", "White", or "Abstain". If everyone abstains, the game is lost. If someone guesses incorrectly, the game is lost. Otherwise, the game is won. What's the optimal strategy and the corresponding probability of winning?

   (a) Lets say that a directed graph G is a subgraph of the n-dimensional hypercube if its vertex set is $\{0,1\}^n$ and if $u \to v$ is an edge in G, then u and v differ in at most one coordinate. Let $K(G)$ be the number of vertices of G with in-degree at least one, and out-degree zero. Show that the probability of winning the hat problem equals the maximum, over directed subgraphs G of the n-dimensional hypercube, of $K(G)/2^n$.

   (b) Using the fact that the out-degree of any vertex is at most n, show that $K(G)/2^n$ is at most $\frac{n}{n+1}$ for any directed subgraph G of the n-dimensional hypercube.

   (c) Show that if $n = 2^\ell - 1$, then there exists a directed subgraph G of the n-dimensional hypercube with $K(G)/2^n = \frac{n}{n+1}$. (This is where the Hamming code comes in.)

2. **Extending Hamming Codes:** For any prime power q, find a family of perfect q-ary codes of minimum distance 3. (Recall that a perfect code is one that meets the Hamming Bound).

3. **Codes from other codes:** Prove the following statements. (Recall that the notation $(n,k,d)_q$ code is used for general codes where k need not be an integer, and $[n,k,d]_q$ codes are linear codes of dimension k).

   - If there exists an $(n,k,d)_q$ code then there also exists an $(n-1,k,d' \geq d-1)_q$ code.
   - If there exists an $(n,k,d)_2$ code with d odd, then there also exists an $(n+1,k,d+1)_2$ code.
   - If there exists an $(n,k,d)_{2^m}$ code, then there also exists an $(mn,mk,d' \geq d)_2$ code.

4. **Maximum Likelihood Decoding problem (MLD):** The MLD problem is the following problem: given a generator matrix of a linear code and a possibly corrupt word w, find the codeword nearest to w. In this exercise we will prove that MLD is NP-hard.

   Given an undirected graph $G = (V,E)$ consider the binary code $C_G \subset \{0,1\}^{|E|}$ where every codeword corresponds to a cut in the graph G. Namely, $w \in \{0,1\}^{|E|}$ is in the code iff there is a subset $S \subseteq V$ such that $w_e = 1$ iff $e = \{u,v\}$ crosses the cut (i.e. $u \in S$ and $v \notin S$).

   (a) Prove that C_G is a linear code.

(b) Prove that if there is a polynomial-time algorithm for MLD for the code C_G (i.e., for finding the nearest codeword to a given word) then one can solve (the NP-hard problem) maximum cut.

5. **Dual of Reed-Solomon Codes:** Let F_q be a finite field with q elements, let $n = q$ and let α be a generator of $F^* = F \setminus \{0\}$. Define the Reed-Solomon code by

$$RS_F[n,k] = \left\{ (p(0), p(1), p(\alpha), \ldots, p(\alpha^{n-2})) \;\middle|\; p \in F[X] \text{ has degree } \leq k-1 \right\}$$

Prove that the dual of the $[n,k]_q$ Reed-Solomon code is an $[n, n-k]_q$ Reed Solomon code.

Hint: consider the relevant Vandermonde matrix, and prove the following claim: For every $k \in F$

$$\sum_{a \in F} a^k = \begin{cases} 0 & k \neq q-1 \\ -1 & k = q-1 \end{cases}$$