CSC 2414H - Assignment 2

Due Mar 4 , 2008

General rules : In solving this you may consult books and you may also consult with each other, but you must each write your own solution. In each problem list the people you consulted. This list will not affect your grade.

1. Prove the following statement (that was needed to complete the Plotkin bound): Let $v_1, v_2, \ldots, v_r$ be unit vectors in $\mathbb{R}^n$ such that $v_i \cdot v_j \leq 0$ for all $i \neq j$. Then

$$\sum_{i \neq j} (v_i \cdot v_j)^2 \leq r.$$

2. Consider the following scenario. There are n people who share a treasure. The treasure is held in a safe which is protected by a passowrd. We will think of the passowrd as an element of some finite field $\mathbb{F}_q$ with q elements. You, as a trustee, are responsible for distributing 'keys', which are again elements in $\mathbb{F}_q$, to all of the people so that (i) any set of less than k people (k is some number smaller than n) cannot infer any information about the passowrd by sharing their keys, and (ii) every set of $\geq k$ people can recover the password by sharing their keys.

   To make this precise, your goal is to find a protocol that for each password $a \in \mathbb{F}_q$ randomly assigns a key to every person according to some distribution. In other words, a protocol is a randomized function $f : \mathbb{F}_q \times [n] \mapsto \mathbb{F}_q$. To satisfy the conditions we need that

   - for every $S \subseteq [n], |S| < k$, and any values $a_i \in \mathbb{F}_q$ for $i \in S$ and any $a' \in F$

$$\Pr\left[a = a' | \forall i \in S, f(i, a) = a_i\right] = 1/q$$

     where the probability above is over the random choices of f and over a choice of a uniformly at random.

   - for every $S \subseteq [n], |S| \geq k$, and any values $a_i \in \mathbb{F}_q$ for $i \in S$ there is at most one value $a \in \mathbb{F}_q$ for which

$$\Pr[\forall i \in S, f(i, a) = a_i] > 0$$

   (verify for yourself why this reflects the requirements from the protocol described informally above.)

Your goal is to show that a $[n+1, k, n-k+2]_q$ code that meets the singleton bound can be used to define such a protocol. You may use the following hint: for $a \in \mathbb{F}_q$, let $(a_0, a_1, \ldots, a_n)$ be a random codeword with $a_0 = a$. Define $f(a, i) = a_i$ (notice that this defines a random function). Show that f is a good protocol with respect to the properties above.

3. Let $\mathbb{F}_q$ be a field of q elements and let $n = q - 1$. Recall that the nonzero elements of a finite filed form a cyclic multiplicative group, and so there is $\alpha \in \mathbb{F}_q$ such that $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1})\} = \mathbb{F}_q$. Consider a Reed-Solomon $[n, k, n-k+1]_q$ code over $\mathbb{F}_q$ as follows:

$$C = \{(p(1), p(\alpha), \ldots, p(\alpha^{n-1}) \mid p \text{ is a polynomial of degree } \leq k-1 \text{ over } \mathbb{F}_q\}$$

   (a) Prove and use the indentity $\sum_{i=0}^{n-1} \alpha^{ij} = 0$ for all $1 \leq j < n$ in order to show that the matrix $H_{ij} = \alpha^{ij}$ (with $0 \leq i < n$ and $1 \leq j \leq n-k$), is a parity check matrix for C.

   (b) From here on, let $q = 2^m$. Consider $B = C \cap \mathbb{F}_2^n$. Clearly, B is a *binary, linear* code. We now wish to analyze the rate and distance of B. Start by showing that the distance of B is at least $d = n - k + 1$.

   (c) Show that B has dimension at least $n - (d-1)m$. Hint: remember that there is a way to view an element of $\mathbb{F}_q$ as a vector in $\{0,1\}^m$ that respects addition. Namely, there is a $\phi : \mathbb{F}_q \mapsto \{0,1\}^m$ so that for all $x, y \in F, \phi(x+y) = \phi(x) + \phi(y)$ (why?).

   (d) Remove all even column of H and call the resulting matrix H'. Show that

$$xH = 0 \iff xH' = 0$$

   for $x \in \mathbb{F}_2^n$. Prove and use the identity in $(a+b)^2 = a^2 + b^2$ that holds in $\mathbb{F}_q$ in order to show that. Deduce that the dimension of B is at least $n - \lceil \frac{d-1}{2} \rceil m$.

   (e) To summarize, we got a $[n, \geq n - \lceil \frac{d-1}{2} \rceil m, \geq d]$ code. Show that this is nearly optimal in the following sense: There is no $[n, n - tm, d]_2$ code for $t < \frac{d-1}{2}$.

4. (a) Let C be a linear $[n, k, d]_q$ code. Consider the rank of the parity check matrtix of C and give a new proof of the singleton bound $d \leq n - k + 1$.

   (b) Call a code that attains the singleton bound a singleton-code. Show that if C is a linear singleton code, then $C^\perp$, the dual code of C defined as

$$C^\perp = \{y \mid y \cdot x = 0 \ \forall x \in C\}$$

   is also a singleton code.

5. (a) Let $\mathcal{C}$ be an infinite family of codes of rate at least R such that for every code $C \in \mathcal{C}$ of length n, C is (β, n) list decodable. Show that $R \leq 1 - H(\beta)$.

   (b) Let R, β be reals between zero and one, such that $R < 1 - H(\beta)$. Prove that there exists an infinite family of codes $\mathcal{C}$ with rate R and that is $(\beta, O(n))$ list-decodable.