Homework 4
Due 2006/12/7

Oded Regev
Department of Computer Science
Tel Aviv University

Instructions: As before.

Problems

1. **Finite fields:** Let $\mathbb{F}_q$ be the field with $q = p^m$ elements for some prime p and $m \geq 1$.

   (a) Show that there is a bijection $f : \mathbb{F}_q \to \mathbb{F}_p^m$ which is $\mathbb{F}_p$ linear (i.e., $f(x+y) = f(x)+f(y)$ and $f(\alpha x) = \alpha f(x)$ for all $x, y \in \mathbb{F}_q, \alpha \in \mathbb{F}_p$). This shows that we can think of the field $\mathbb{F}_q$ as the set of m-dimensional vectors over $\mathbb{F}_p$ with standard addition of vectors, and some rule for the multiplication of two vectors. Hint: Recall/show that $\mathbb{F}_q$ is an m-dimensional vector space over $\mathbb{F}_p$.

   (b) Show that for any $a, b \in \mathbb{F}_q$, $(a + b)^p = a^p + b^p$. Deduce that $(a + b)^{p^l} = a^{p^l} + b^{p^l}$ for any $l \geq 0$. Hint: In $\mathbb{F}_q$, the element $p = \underbrace{1 + \cdots + 1}_{p}$ is equal to 0 (why?).

   (c) Prove the following equality in $\mathbb{F}_q[x]$:
   $$\prod_{\alpha \in \mathbb{F}_q^*} (x - \alpha) = x^{q-1} - 1.$$
   Hint: Do not expand the left hand side.

   (d) Assume p is odd. An element $\alpha \in \mathbb{F}_q$ is called a *quadratic residue* if it is the square of a nonzero element in $\mathbb{F}_q$. Show that there are exactly $(q - 1)/2$ quadratic residues in $\mathbb{F}_q$. Hint: Recall that the nonzero elements in $\mathbb{F}_q$ are given by $1, \gamma, \gamma^2, \ldots, \gamma^{q-2}$ where γ is a generator of $\mathbb{F}_q^*$.

2. **Binary BCH codes:** Let $q = 2^m$ for some $m \geq 1$, $n = q - 1$ and $k = n - 2t$ for some $t \geq 1$. The generator matrix of a primitive $[n, k, 2t + 1]_q$ RS code is given by
   $$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}$$
   where $\alpha_1, \ldots, \alpha_n$ are all nonzero elements of $\mathbb{F}_q$. In class we showed that the parity check matrix of this code is given by
   $$H = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{2t} & \alpha_2^{2t} & \cdots & \alpha_n^{2t} \end{pmatrix}$$
   (make sure you remember why).

   (a) Show that any $2t = n - k$ columns of H are linearly independent (over $\mathbb{F}_q$).

(b) By removing all even rows, we obtain the $t \times n$ matrix

$$H' = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^3 & \alpha_2^3 & \cdots & \alpha_n^3 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{2t-1} & \alpha_2^{2t-1} & \cdots & \alpha_n^{2t-1} \end{pmatrix}.$$

Show that any $2t$ columns of H' are linearly independent over $\mathbb{F}_2$ (i.e., any sum of at most $2t$ columns of H' is nonzero). Hint: Use (1b).

(c) Let H'' be the $tm \times n$ matrix over $\mathbb{F}_2$ obtained from H' by replacing each element of $\mathbb{F}_q$ with an m-bit column vector, as in (1a). Show that any $2t$ columns of H'' are linearly independent (over $\mathbb{F}_2$).

(d) Deduce the existence of a $[n, \geq n - t\log(n+1), \geq 2t+1]_2$ code. Notice that for any constant t, this code almost matches the Hamming bound.

3. **Hadamard matrices:** Recall that an $n \times n$ matrix H all of whose entries are from $\{+1, -1\}$ is a Hadamard matrix if $H \cdot H^T = n \cdot I$ where the matrix product is over the reals and I is the $n \times n$ identity matrix.

(a) Show that the determinant of an $n \times n$ Hadamard matrix is $n^{n/2}$ in absolute value and that this is the largest achievable by any ± 1 matrix. Hint: Use Hadamard's inequality.

(b) Show that if there is an $n \times n$ Hadamard matrix then n is either 1 or 2 or a multiple of 4. It is conjectured that this condition is also sufficient.

(c) Given an $n \times n$ Hadamard matrix H_n and an $m \times m$ Hadamard matrix H_m, construct an $nm \times nm$ Hadamard matrix.

(d) (Not to be turned in) Let q be a prime power equivalent to 3 modulo 4. Let $H = \{h_{ij}\}$ be the $q \times q$ matrix with $h_{ij} = 1$ if $i = j$, and $h_{ij} = (j - i)^{(q-1)/2}$ otherwise where we think of i, j as running over all elements of $\mathbb{F}_q$. Let H' be the $(q+1) \times (q+1)$ matrix obtained from H by adding one row and one column of 1s. Verify that H' is a Hadamard matrix. This is Paley's construction of Hadamard matrices. The first dimension not covered by Paley's nor Sylvester's construction is $n = 36$. Other constructions are known there. The first dimension where no Hadamard matrix is known is 668.

4. **Wozencraft ensemble:** Show that for any $0 \leq \delta \leq 1$ and $\varepsilon > 0$ there is a family of 2^k codes such that all but an ε fraction of them are $[(1+\delta)k, k, (H^{-1}(1 - \frac{1}{1+\delta}) - \varepsilon)(1+\delta)k]_2$-codes, i.e., almost all codes nearly match the Gilbert-Varshamov bound for rate $\frac{1}{1+\delta}$. Use the family of linear codes $\{S_\alpha \mid \alpha \in \mathbb{F}_{2^k}\}$ where S_α is obtained from the linear code $\{(x, \alpha x) \mid x \in \mathbb{F}_{2^k}\} \subseteq \mathbb{F}_2^{2k}$ by removing some arbitrary $(1-\delta)k$ coordinates from all codewords. Deduce that Justesen codes can match the Zyablov bound for all large enough rates.