Coding Theory Spring 2009

Problem Set # 2

Due: May 14th, 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. Each person must submit the entire exercise.

Questions:

1. (Review, not to be handed in:) Let K be a field, and $F \supset K$ a finite extension field. Show that there is a K-linear mapping φ from F to K^n for some n. Fix any $a \in F$ and let $m_a : F \to F$ be defined by $m_a(x) = a \cdot x$ where multiplication is in F. Prove that m_a is a K-linear mapping.
2. Decoding from errors and erasures.
   (a) Prove that given a generator matrix of an $[n, k, d]$ code, there is a polynomial time algorithm that decodes from $e < d$ erasures.
   (b) Show how to decode any Reed-Solomon code simultaneously from s erasures and e errors, as long as $s + 2e < d$.
3. Tensors of codes. Given codes C_1 and C_2 with encoding functions $E_1 : \{0,1\}^{k_1} \to \{0,1\}^{n_1}$ and $E_2 : \{0,1\}^{k_2} \to \{0,1\}^{n_2}$. Define an encoding function $E_1 \otimes E_2 : \{0,1\}^{k_1 k_2} \to \{0,1\}^{n_1 n_2}$ as follows: View a message m as a k_1 by k_2 matrix. Encode the columns of m individually using the function E_1 to get an $n_1 \times k_2$ matrix m_0. Now encode the rows of m_0 individually using E_2 to get an $n_1 \times n_2$ matrix that is the final encoding under $E_1 \otimes E_2$ of m. Let $C_1 \otimes C_2$ be the code associated with $E_1 \otimes E_2$.
   (a) What is the rate and distance of the new code, as a function of the parameters of C_1, C_2.
   (b) Assume C_1, C_2 are linear codes. Prove that the codewords of $C_1 \otimes C_2$ are exactly $n_1 \times n_2$ matrices whose rows are codewords of C_2 and whose columns are codewords of C_1.
   (c) ~~Suppose C_1, C_2 are Hadamard codes. Prove that $C_1 \otimes C_2$ is a Hadamard code.~~ (oops, wrong!)
4. Reed Muller Codes. The following code family is an extension of the Reed Solomon codes, that has smaller alphabet size. Let $\mathbb{F}_q$ be a field, and let $S \subset \mathbb{F}_q$. Given a message $(m_{ij})_{0 \le i,j, < \sqrt{k}}$, define a bivariate polynomial $P_m(X, Y) := \sum_{i,j} m_{ij} X^i Y^j$. The encoding of m is defined to be $(P_m(\alpha, \beta))_{\alpha,\beta \in S} \in \mathbb{F}_q^{|S|^2}$.
   (a) The definition of tensor products of codes from question 3 can be extended to work over large alphabets in a natural way. Prove that the code described above is $C \otimes C$ for C an appropriate Reed Solomon code.
   (b) What are the rate and distance of the code defined above.
   (c) Extend the definition of Reed Muller codes to m-variate polynomials, such that the resulting code equals $C^{\otimes m}$ for a Reed-Solomon code C (where $C^{\otimes m}$ denotes $C \otimes \cdots \otimes C$, m times).

(d) Another (important) variant of Reed Muller codes, is defined by interpreting the message symbols as coefficients of a polynomial in m variables of total degree at most d. (The total degree is the maximum, over monomials, of the sum of individual degrees in the monomial). The encoding is simply the evaluation of that polynomial on all of $\mathbb{F}_q^m$. Prove that $k = \binom{d+m}{d}$. Prove (by induction) that the relative distance of this code is at least $1-d/q$ (aka the Schwartz-Zippel Lemma).

(e) Can either of these variants be asymptotically good for a constant size alphabet q ? (Recall that a code is asymptotically good if it has non-vanishing rate and distance).

5. We discussed the following scheme for constructing codes. To encode k bits, find the smallest m such that the message length is $k \leq m \cdot 2^{m-1}$. Exhaustively search for a good $[2m, m, \delta m]$ linear code for some predefined positive $\delta > 0$. The code will be the concatenation of a Reed-Solomon code over alphabet 2^m and rate $1/2$ with the linear code above.

(a) Show that the obtained code family is asymptotically good. What is the running time of the above procedure in terms of the input length k?

(b) Describe a polynomial-time variant of the above scheme, obtained by two levels of concatenation (polynomial time means that the encoding of a message can be computed in deterministic polynomial time). Analyze the rate and distance of your scheme.

(c) ~~Describe another polynomial-time variant of the above scheme, obtained by replacing the Reed-Solomon code by a bivariate Reed-Muller code. Analyze the rate and distance of your scheme.~~