Homework 6
Due 2007/1/4

Oded Regev
Dept. of Computer Science
Tel Aviv University

1. **Achieving Shannon capacity with linear codes:**

   (a) Show that for any $p < \frac{1}{2}$, $\varepsilon > 0$, there exists $c > 0$ such that for any large enough n there exists an encoding function $E : \{0,1\}^k \to \{0,1\}^n$ of a linear code and a decoding function $D : \{0,1\}^n \to \{0,1\}^k$ where $k = (1 - H(p) - \varepsilon)n$ such that for any $m \in \{0,1\}^k$

   $$\Pr_{e \sim \mu_p^n}[D(E(m) + e) \neq m] \leq 2^{-cn}.$$

   (b) Show, moreover, that for any $p < H^{-1}(\frac{1}{2})$ and $\varepsilon = \frac{1}{2} - H(p)$ this is achieved by one of the codes in the Wozencraft ensemble.

2. **Tensors:** Given binary codes C_1 and C_2 with encoding functions $E_1 : \{0,1\}^{k_1} \to \{0,1\}^{n_1}$ and $E_2 : \{0,1\}^{k_2} \to \{0,1\}^{n_2}$ let $E_1 \otimes E_2 : \{0,1\}^{k_1 \times k_2} \to \{0,1\}^{n_1 \times n_2}$ be the encoding function obtained as follows: View a message m as a $k_1 \times k_2$ matrix. Encode each column of m using the function E_1 to get an $n_1 \times k_2$ matrix m'. Now encode each row of m' 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) Describe the parameters of $C_1 \otimes C_2$ in terms of those of C_1 and C_2 (message length, block length, rate, distance, relative distance). Compare the tensor operation with code concatenation.

   (b) (Not to be turned in) Assume C_1, C_2 are linear codes with corresponding generating matrices $G_1 \in \mathbb{F}_2^{k_1 \times n_1}$ and $G_2 \in \mathbb{F}_2^{k_2 \times n_2}$. Notice that in this case the encoding function can be defined as the function mapping a message m viewed as a matrix in $\mathbb{F}_2^{k_1 \times k_2}$ to the codeword $G_1^T m G_2 \in \mathbb{F}_2^{n_1 \times n_2}$. Deduce that in the case of linear codes the order in which we apply E_1 and E_2 does not matter. Is the same true for the general case?

   (c) Consider the Minimum Distance Problem: given a generating matrix of a binary code C, compute or approximate its minimum distance $\Delta(C)$. This problem is known to be NP-hard to approximate to within some constant $c > 1$. Show that for *any* $c > 1$, this problem is NP-hard to approximate to within c.[1]

3. **Welch-Berlekamp algorithm:** Assume we modify the Welch-Berlekamp decoding algorithm described in class and instead of looking for *any* nonzero solution (E, N), we look for one in which the degree of E is as small as possible.

   (a) Show that this can still be done efficiently.

   (b) Describe the set of possible solutions (E, N) in this modified algorithm.

[1] Dumer, Micciancio, and Sudan, FOCS 1999