CSE 533: Error-Correcting Codes **Autumn 2006**

Problem Set 1
Due on Monday, October 30

Homework policy: Students are encouraged to work on the problems in small groups (of up to 3 people); however, all writeups should be done individually and must clearly cite any collaborators. You are strongly urged to try and solve the problems without consulting any reference material besides what we cover in class (such as any textbooks or material on the web where the solution may appear either fully or in part). If for some reason you feel the need to consult some source, please acknowledge the source and try to explain what difficulty you couldn't overcome before consulting the source and how it helped you overcome that difficulty.

---

1. **Operations on Codes.** Prove the following statements (the notation $(n, k, d)_q$ code is used for general codes with q^k codewords where k need not be an integer, whereas the notation $[n, k, d]_q$ code stands for a *linear code* of dimension k):

   (a) If there exists an $(n, k, d)_q$ code, then there also exists an $(n-1, k, d' \geq d-1)_q$ code.

   (b) If there exists an $(n, k, d)_2$ code with d odd, then there also exists an $(n+1, k, d+1)_2$ code.

   (c) If there exists an $(n, k, d)_{2^m}$ code, then there also exists an $(nm, km, d' \geq d)_2$ code.

   (d) If there exists an $[n, k, d]_{2^m}$ code, then there also exists an $[nm, km, d' \geq d]_2$ code.

   (e) If there exists an $[n, k, d]_q$ code, then there also exists an $[n-d, k-1, d' \geq \lceil d/q \rceil]_q$ code.

   (f) If there exists an $[n, k_1, d_1]_q$ code and an $[n, k_2, d_2]_q$ code, then there exists an $[2n, k_1 + k_2, \min(2d_1, d_2)]_q$ code.

2. Prove the following version of the Plotkin bound for general alphabets. If $C \subseteq \Sigma^n$ is a (not necessarily linear) code over an alphabet of size $|\Sigma| = q$ with minimum distance $d > (1-1/q)n$, then $|C| \leq \frac{qd}{qd-(q-1)n}$.

3. (a) Prove that for an $[n, k, d]_q$ linear code, we must have

   $$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil \ . \tag{1}$$

   Hint: Try induction together with Problem (1e) above.

   (b) Deduce the Singeton bound for linear codes from bound (1) above.

   (c) Show that the simplex codes (dual of the Hamming codes) meet the bound (1).

4. (a) Briefly argue (full proof not required) why the proof of Shannon's theorem for the binary symmetric channel that we did in class holds even if the encoding function E is restricted to be linear.

   (b) Prove that for communication on BSC_p, if an encoding function E achieves a maximum decoding error probability (taken over all messages) that is exponentially small, i.e., at most $2^{-\gamma n}$ for some $\gamma > 0$, then there exists a $\delta = \delta(\gamma, p) > 0$ such that the code defined by E has relative distance at least δ. In other words, good distance is *necessary* for exponentially small maximum decoding error probability.

(c) Prove that if the encoding function E is restricted to be linear, a similar conclusion holds even if only the *average* decoding error probability (computed for a message chosen uniformly at random) is exponentially small.

5. (a) For positive integers $k \leq n$, show that less than a fraction q^{k-n} of the $n \times k$ matrices G over $\mathbb{F}_q$ fail to generate a linear code of block length n and dimension k. (Or equivalently, except with probability less than q^{k-n}, the rank of G is k.)

   (b) Consider the q-ary erasure channel with erasure probaility α ($q\mathrm{EC}_\alpha$, for some α, $0 \leq \alpha \leq 1$): the input to this channel is a field element $x \in \mathbb{F}_q$, and the output is x with probability $1 - \alpha$, and an erasure '?' with probability α. For a linear code C generated by an $n \times k$ matrix G over $\mathbb{F}_q$, let $D : (\mathbb{F}_q \cup \{?\})^n \to C \cup \{\mathsf{fail}\}$ be the following decoder:

$$D(y) = \begin{cases} c & \text{if } y \text{ agrees with exactly one } c \in C \text{ on the unerased entries in } \mathbb{F}_q \\ \mathsf{fail} & \text{otherwise} \end{cases}$$

   For a set $J \subseteq \{1, 2, \ldots, n\}$, let $P_{\mathrm{err}}(G|J)$ be the probability (over the channel noise and choice of a random message) that D outputs fail conditioned on the erasures being indexed by J. Prove that the average value of $P_{\mathrm{err}}(G|J)$ taken over all $G \in \mathbb{F}_q^{n \times k}$ is less than $q^{k-n+|J|}$.

   (c) Let $P_{\mathrm{err}}(G)$ be the decoding error probability of the decoder D for communication using the code generated by G on the $q\mathrm{EC}_\alpha$. Show that when $k = Rn$ for $R < 1 - \alpha$, the average value of $P_{\mathrm{err}}(G)$ over all $n \times k$ matrices G over $\mathbb{F}_q$ is exponentially small in n.

   (d) Conclude that one can reliably communicate on the $q\mathrm{EC}_\alpha$ at any rate less than $1 - \alpha$ using a linear code.

6. We now define the tensor product operation that was used in class to discuss Elias' construction of iterated product of Hamming codes to achieve reliable communication at positive rate for BSC_p for some positive p with an explicit construction and polynomial time decoding. We only focus on binary codes, but the definition applies over any field. Let C_1 be an $[n_1, k_1, d_1]_2$ code with generator matrix $G_1 \in \{0,1\}^{n_1 \times k_1}$ and let C_2 be an $[n_2, k_2, d_2]_2$ code with generator matrix $G_2 \in \{0,1\}^{n_2 \times k_2}$. The tensor product (or simply product) of C_1 and C_2, denoted $C_1 \otimes C_2$, is a code of block length $n_1 n_2$ defined as

$$C_1 \otimes C_2 = \{G_1 M G_2^T \mid M \in \{0,1\}^{k_1 \times k_2}\} .$$

   (a) Prove that $C_1 \otimes C_2$ is an $[n_1 n_2, k_1 k_2, d_1 d_2]$ binary linear code.

   (b) Prove that codewords of $C_1 \otimes C_2$ correspond to $n_1 \times n_2$ matrices all of whose columns are codewords of C_1 and all of whose rows are codewords of C_2.