ENEE739C: Homework 2. Date due 11/20/2003. (no e-mails please).

1. Prove Theorem 7.7: information set decoding is max-likelihood. In other words, prove that for every coset leader $\mathbf{x}$, the subset $E = [n] \backslash \operatorname{supp}(\mathbf{x})$ contains an information set: $\operatorname{rk}(\mathbf{G}(E)) = k$.

2. Let $\mathcal{C}$ be an $[n, k]$ binary linear code. Define

$$\epsilon_{\mathcal{C}}(t) = \frac{|D(0, \mathcal{C}) \cap \mathcal{S}_t(0)|}{\binom{n}{t}}$$

to be the proportion of correctable errors (coset leaders) of weight t ($\mathcal{S}_t(0)$ is the sphere of radius t around zero).

(a) Prove that $\epsilon_{\mathcal{C}}(t) \geq \epsilon_{\mathcal{C}}(t+1), t = 0, 1, \ldots, n-1$.

(b) Prove that for any $t = 0, 1, \ldots, n$

$$\epsilon_{\mathcal{C}}(t) \leq \frac{2^{n-k}}{\sum_{i=0}^{t} \binom{n}{i}}.$$

(c) Use part (b) to prove that if $R > 1 - h_2(p)$ then the error probability of ML decoding of $\mathcal{C}$ on a BSC(p) tends to one (it is not possible to transmit with linear codes at rates above capacity).

3. Prove that the error-correcting capability of GMD decoding is unchanged if instead erasing the least reliable symbols one by one, we proceed by erasing in each step

(a) the two least reliable nonerased symbols,

(b) all of the least reliable nonerased symbols with *equal* reliability.

Hint: (b) rewrite the convex combination in the proof of Thm. 8.9 appropriately.

4. You are given an algorithm that finds a codeword of minimum weight in a $[n, k, d]$ linear code $\mathcal{C}$. Show that the same algorithm can be used (as a black box) to perform decoding of $\mathcal{C}$ up to $\lfloor (d-1)/2 \rfloor$ errors.

Hint: Let $\mathbf{y}$ be a received vector which is at most $\lfloor (d-1)/2 \rfloor$ away from some codeword. Consider the linear code spanned by $\mathcal{C}$ and $\mathbf{y}$.

5. Let $R = \mathscr{C} - \epsilon$, where $\mathscr{C}$ is the capacity of a BSC(p). Prove that the complexity of ML decoding of a random $[n, nR]$ linear binary code behaves as $O(2^{\epsilon^{-2}})$ as $\epsilon \to 0$.

6. Show that the encoding order of product codes (first columns then rows, or first rows then columns) does not matter: in both cases we get the same code.