MATH 4450/6450
HOMEWORK 8
DUE 4/2/07

Do the following book problems:

18.12: 3, 4, 5, 8, 9, 15, 16, 17.

18.13: 2.

Your instructions for the extra problems this week are: 4450 students should do Extra Problem 1. As usual, 6450 students have to do everything.

Extra Problem 1: (Operations on codes) Let C be a q-ary $[n, k, d]$ code with generating matrix G.

(a) When $q = 2$, we define the extended code C' by adding a parity check column to G; the parity check column is defined to be the sum of all the columns of G (we did an example in class with the Hamming $[7, 4, 3]$ code). Show that C' is an $[n + 1, k, d']$ code, where $d' = 2\lceil d/2 \rceil$. (Make sure you verify that it is linear!)

(b) Let j be an integer, $1 \leq j \leq n$. We define the punctured code $C(j)$ by removing the jth column of G and taking the new matrix to be the generating matrix of $C(j)$. Show that $C(j)$ is an $[n - 1, k'', d'']$ code, where $k'' = k - 1$ or k, and $d'' = d - 1$ or d. (Note: don't assume $q = 2$.)

(c) Let j be an integer, $1 \leq j \leq n$. We define the shortened code

$$C^s(j) = \{\mathbf{c} \in C(j) |\ \mathbf{c} \text{ comes from a codeword with a 0 in the } j\text{th spot}\}$$

Show that $C^s(j)$ is an $[n-1, k, d]$ code if the jth column of G is zero, and otherwise G is an $[n - 1, k - 1, d']$ code with $d' \geq d$. (Note: don't assume $q = 2$.)

(d) Let C be a q-ary $[n, k]$ code. Suppose that G has no column of zeroes. Show that

$$\sum_{\mathbf{c} \in C} wt(\mathbf{c}) = nq^{k-1}(q - 1).$$

(Hint: count how much is contributed to the sum from each coordinate of $\mathbf{c}$. You may want to use ideas from part (b) or (c).)

Extra Problem 2: Let C be a q-ary $[n, k, d]$ code, and let $\mathbf{c} \in C$ have weight d. Define $\text{Res}(C, \mathbf{c})$ to be the code obtained by eliminating all the coordinate positions where $\mathbf{c}$ has nonzero entries, i.e.

$$\text{Res}(C, \mathbf{c}) = \{\text{res}(\mathbf{x}) |\ \mathbf{x} \in C\}$$

where $\text{res}(\mathbf{x})$ is the vector obtained by deleting the d coordinates of $\mathbf{x}$ where $\mathbf{c}$ has nonzero entries.

(a) Show that Res$(C, \mathbf{c})$ is an $[n-d, k-1, d']$ code, where $d' \geq \left\lceil \frac{d}{q} \right\rceil$.

(b) Show that if C is a q-ary $[n, k, d]$ code, then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil .$$

(Hint: keep "residualizing"...probably it's cleanest to induct on k.)

(c) Recall that an MDS code is a code for which the Singleton bound holds with equality. Notice that the Singleton bound applied to linear codes says that $k + d \leq n + 1$. Show that the only binary MDS codes are $\mathbb{F}_2^n$, the $[n, n-1, 2]$ parity check code, and its dual (which, by the way, we have seen before–what is it?).

Hint: you might use the sphere packing bound, and you might try doing some operations a la Extra Problem 2. Whatever you do, I suggest induction on n.

(d) Now for the coup de grâce: Show that there is no $[16, 8, 6]$ binary code. (Hint: restrict to get a $[10, 7, d]$ code; then rule out all the possibilities for d.)

Remark: This is a good example of how one shows that no codes exist with given q, n, k, d. Notice that the Singleton and sphere-packing bounds do not imply the nonexistence of a $[16, 8, 6]$ code immediately (and equality holds in the bound from part (b)!).