ENEE739C: Homework 1. Date due 10/23/2003. (no e-mails please).

1. We have proved (Thm. 2.6) that there exists an $[n,k]$ binary linear code whose weight distribution $A_1, A_2, \dots, A_n$ is bounded above as

$$A_w \le n^2 \binom{n}{w} 2^{k-n}$$

if the right-hand side is at least one (and $A_w = 0$ otherwise). Prove that it is possible to improve this estimate by replacing n^2 with n : there exists a binary linear $[n,k]$ code with

$$A_w \le n \binom{n}{w} 2^{k-n}.$$

Hint: consider the ensemble of all linear $[n,k]$ codes. Find the probability that a nonzero vector is contained in a random code from the ensemble. Compute the expected number of weight-w vectors, use the Markov inequality.

2. Consider a finite metric space X in which the volume of the ball $\mathcal{B}_r(\mathbf{x})$ depends on its center. Let

$$\langle B_r \rangle = \frac{1}{|X|} \sum_{\mathbf{x} \in X} \mathrm{vol}(\mathcal{B}_r(\mathbf{x}))$$

be the average volume of the ball of radius r. Prove that X contains a code of minimum distance d and size $M \ge |X|/(4\langle B_{d-1}\rangle)$.

Hint: perform the Gilbert procedure on the subset of all the points $\mathbf{y} \in X$ such that $\mathrm{vol}(\mathcal{B}_{d-1}(\mathbf{y})) \le 2\langle B_r \rangle$.

3. (GV bound in the Johnson space) Let $\mathscr{J}^{n,w}$ be the space of all binary vectors of length n and weight w.

(a) Let $\mathbf{x}, \mathbf{y} \in \mathscr{J}^{n,w}$. Prove that the Hamming distance $d(\mathbf{x}, \mathbf{y})$ is even.

(b) Let $\mathcal{C}$ be a code of rate R and minimum distance $d = 2\delta n$. Prove that $\mathscr{J}^{n,w}$ contains codes of rate approaching the bound

$$R = h_2(\omega) - \omega h_2\Big(\frac{\delta}{\omega}\Big) - (1-\omega) h_2\Big(\frac{\delta}{1-\omega}\Big).$$

4. Recall the inequality used to prove Thm. 5.1

$$P_e(\mathcal{C}) \le \min_t [P_e(\mathcal{C}, \mathbf{y} \in \mathcal{B}_t(0)) + P(\mathbf{y} \notin \mathcal{B}_t(0))]. \tag{1}$$

where $\mathbf{y}$ is the the error vector. In the proof we took $\mathcal{C}$ a random linear code and chose $t = d_{\mathrm{GV}}$. Prove that for large n this choice is optimal, i.e., furnishes the minimum on t in (1).

Hint: Find the smallest t satisfying, for large n,

$$2^{-n(1-R)} \sum_{w=d}^{2t} \binom{n}{w} \sum_{r=\lceil w/2 \rceil}^{t} \Big[\sum_{i=w/2}^{w} \binom{w}{i} \binom{n-w}{r-i} \Big] p^r (1-p)^{n-r} \ge \sum_{r=t+1}^{n} \binom{n}{r} p^r (1-p)^{n-r}.$$

5. Consider an $[n=8, k, d]$ linear code $\mathcal{C}$ given by the row space of the matrix

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Find k, d. Write out a parity-check matrix of $\mathcal{C}$. Let $E = \{1,2,3\}$. Write out the parameters of the codes $\mathcal{C}_E, \mathcal{C}^E, (\mathcal{C}^\perp)_E, (\mathcal{C}^\perp)^E$. Explain all answers.

6. Let $\mathcal{C}[n,k,d]$ be a linear q-ary MDS code, i.e., a code with $d = n-k+1$. Prove that the dual code $C^\perp$ is also MDS.