ECE/MATH 641 MIDTERM, SPRING 2008

Nigel Boston

For full credit you must explain your reasoning. Each question is worth an equal amount. Answer them in any order.

1. (a) State the Singleton bound for the minimum distance d of a linear $[n, k]$ code.

(b) Consider binary linear $[6, k, 4]$ codes. What is the largest possible value of k? Give a generator matrix of such a code.

(c) Is your code in (b) optimal? (I.e. is there a binary $(6, 2^k+1)$ code, containing your code in (b), with minimum distance 4)?

2. Consider the binary linear $[5, 2]$ code C with generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(a) Find a parity-check matrix for C.

(b) Find the minimum distance and weight enumerator of C.

(c) Is C perfect?

(d) Suppose vector $y = (1, 1, 0, 0, 1)$ is received. Find its syndrome and hence decode it.

3. (a) Define the binary linear Hamming code $\mathcal{H}_m$ of length 2^m-1. State without proof its parameters (i.e. n, k, d) and the parameters of its dual, the simplex code.

(b) If C is a binary linear code, does $(C^{ext})^{\perp}$ necessarily equal $(C^{\perp})^{ext}$?

(c) The Reed-Muller code $RM(1, m)$ is defined to be the dual of the extended code $\mathcal{H}_m^{ext}$. Find the parameters of $RM(1, 3)$.

4. Let $f(x) = x^2 + 1 \in \mathbf{F}_7[x]$.

(a) Show that f is irreducible and explain how it can be used to construct a field F with 49 elements (i.e. what are the elements of F and how are addition and multiplication defined? Don't write more than two or three sentences on this!).

(b) Let α be a root of f in F. Is α a primitive element of F?

(c) Explain how to obtain a linear $[48, 28]$ code over F that corrects any 10 errors (again, don't write more than two or three sentences).