ECE/MATH 641 FINAL, SPRING 2008

Nigel Boston

For full credit you must explain your reasoning. Each question is worth an equal amount. Answer them in any order. Don't overlook any parts to a question!

1. (a) Let C be the binary linear code with generator matrix $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$
Find its minimum distance and its weight enumerator. Is C optimal?

(b) How many cosets does C have? Find a parity check matrix for C. Use syndrome decoding to decode the received vector 11000010.

(c) State MacWilliams' Theorem relating the weight enumerators of a binary linear code and its dual.

(d) Find a generator matrix for the dual code $C^{\perp}$. Find its minimum distance and its weight enumerator.

2. (a) Let $f(x) = x^3 + x^2 + 1 \in \mathbf{F}_2[x]$. Let α be a root of $f(x)$. Show that $f(x)$ is irreducible.

(b) Define what a primitive element of a field is. Show that α is a primitive element of $\mathbf{F}_8$. Write $1, \alpha, \alpha^2, ..., \alpha^6$ as linear combinations of $1, \alpha, \alpha^2$ and give the minimal polynomial over $\mathbf{F}_2$ of each element of $\mathbf{F}_8$.

(c) Using α, define the Hamming code $\mathcal{H}_3$. Prove that its parameters are $[7, 4, 3]$ and that it is a perfect code.

(d) Show that $\mathcal{H}_3$ has no codewords of weight 5 or 6.

3. (a) Let α be a primitive element of $\mathbf{F}_{64}$. Let $m_i(x)$ denote the minimal polynomial of α^i over $\mathbf{F}_2$. What are the degrees of $m_1(x), m_3(x)$, and $m_9(x)$?

(b) Let $g(x) = m_1(x)m_3(x)$. What are the parameters $[n, k, d]$ of the cyclic code with generator polynomial $g(x)$ (you may give the designed lower bound for d)?

(c) Let $v(x) = c(x) + e(x)$ be the received vector, where $c(x)$ is a codeword and $e(x)$ has at most 2 nonzero coefficients. If the syndromes $v(\alpha) = 1 + \alpha$ and $v(\alpha^3) = 1 + \alpha^3$, find $e(x)$.

(d) How many binary cyclic codes of length 63 are there?

4. (a) Give the Singleton bound and define what it means for a linear code to be Maximum Distance Separable (MDS). Show that for every n there exist $[n, 1]$ and $[n, n]$ MDS binary linear codes.

(b) Carefully define the $[63, 53]$ Reed-Solomon code over $\mathbf{F}_{64}$. What is its minimum distance?

(c) If C is a binary linear $[n, k, d]$ code, let $R(C) = k/n$ and $\delta(C) = d/n$. Consider the set $S = \{(\delta(C), R(C)) : C \text{ is a binary linear code } \}$. State briefly the main facts known about S.

(d) Why do MDS codes produce very few points in S (and so do not contradict your answer to (c))?

5. (a) Define the Binary Erasure Channel (BEC) and the Binary Symmetric Channel (BSC).

(b) State Shannon's theorem for random codes on the BSC.

(c) Let C be the binary linear code with parity check matrix $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ Draw its Tanner graph. Suppose $10ee1e$ is received using a BEC (where e denotes an erased bit). Decode this word.

(d) Explain briefly how this can be interpreted as iterative decoding or belief propagation on the Tanner graph. Show that this method can fail if the 3 erased bits are in other positions.