Math 5251 Error-correcting codes and finite fields
Spring 2006, Vic Reiner
Midterm exam 2- Due Wednesday May 3, in my Vincent Hall 105 mailbox by 4pm

Instructions: This is an open book, open library, open notes, open web, take-home exam, but you are *not* allowed to collaborate. The instructor is the only human source you are allowed to consult.

1. (15 points total, 5 points each) For each of the following alphabets Σ and codeword lengths $(\ell_1, \ldots, \ell_n)$, decide whether there exists a *instantaneous (prefix)* code whose words have those lengths. For those where no such code exists, explain why. For those where one exists, exhibit one.
(a) $\Sigma = \{0, 1\}$ and $(\ell_1, \ldots, \ell_7) = (1, 2, 3, 4, 4, 4, 4)$.
(b) $\Sigma = \{0, 1, 2\}$ and $(\ell_1, \ldots, \ell_7) = (1, 1, 2, 2, 3, 3, 3)$.
(c) $\Sigma = \{0, 1, 2, 3\}$ and $(\ell_1, \ldots, \ell_6) = (1, 1, 2, 2, 2, 2)$.

2. (15 points total) Let W be a memoryless source having five source words $\{w_1, \ldots, w_5\}$ which appear with probabilities $(\frac{1}{3}, \frac{1}{5}, \frac{1}{5}, \frac{2}{15}, \frac{2}{15})$.
(a) (5 points) Compute the entropy $H(W)$ for this source W.
(b) (3 points) Compute the entropy $H(W^{(10)})$ for the 10^{th} extension $W^{(10)}$ of this source.
(c) (5 points) Write down a Huffman encoding $\mathcal{H}$, using a binary alphabet $\{0, 1\}$, for this source W.
(d) (2 points) Compute the average word length for this Huffman code $\mathcal{H}$.

3. (15 points total) Let G be the following matrix with entries in $\mathbb{F}_2$:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Let $\mathcal{C}$ be the binary code equal to the row space of G, with parameters (n, m, d) as a binary code, and parameters $[n, k, d]$ when thought of as an $\mathbb{F}_2$-linear code.
(a) (5 points) Write down any parity check matrix H, that is, one whose row space is $\mathcal{C}^{\perp}$.
(b) (5 points) Write down the parameters n, m, k, d.
(c) (3 points) Write down a collection of coset leaders for $\mathcal{C}$.
(d) (2 points) Decode the received word $y = [1011]$ with minimum distance decoding.

4. (15 points total) Let k be the largest possible dimension for an $\mathbb{F}_2$-linear $[n, k, d]$-code with $n = 13$ and $d = 5$. Use the bounds in Chapter 13 of Garrett's text to show that k is either $4, 5$, or 6.

5. (10 points total) How many primitive elements will there be in $\mathbb{F}_8$, a field with 8 elements?

6. (15 points) Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear code with blocklength n, and minimum distance d. Let $e_1, \ldots, e_n$ denote the standard basis vectors in $(\mathbb{F}_q)^n$, that is, e_i is the vector with a one in the i^{th} coordinate and zeroes elsewhere.

Prove that $d \geq 3$ if and only if there exists a choice of coset leaders for $\mathcal{C}$ in which $e_1, \ldots, e_n$ all appear (among the other coset leaders).

7.(15 points total) Let $\mathcal{C}_1, \mathcal{C}_2$ be $\mathbb{F}_2$-linear codes with the same blocklength n. Construct a new code $\mathcal{C}_1 \oplus \mathcal{C}_2$ with blocklength $2n$ having these codewords:

$$\mathcal{C}_1 \oplus \mathcal{C}_2 = \{(v_1, v_1 + v_2)\}_{\substack{v_1 \in \mathcal{C}_1 \\ v_2 \in \mathcal{C}_2}}.$$

Here $(v_1, v_1 + v_2)$ denotes the vector of length $2n$ which is the juxtaposition of the two length n vectors v_1 and $v_1 + v_2$.
(a) (5 points) Prove that $\mathcal{C}_1 \oplus \mathcal{C}_2$ is $\mathbb{F}_2$-linear.
(b) (10 points) Prove that the minimum distance

$$d(\mathcal{C}_1 \oplus \mathcal{C}_2) = \min\{2d(\mathcal{C}_1), d(\mathcal{C}_2)\}.$$

This $\oplus$ construction gives one way of recursively defining the higher-order Reed-Muller codes $R(r, m)$, and calculating their parameters, as we now explain. One first defines $R(0, m)$ to be the 2^m-fold binary repetition code with parameters $[2^m, 1, 2^m]$, and defines $R(r, r)$ to be $(\mathbb{F}_2)^{2^r}$ (that is, *all* possible binary codewords of length 2^r). One then recursively defines

$$R(r, m) := R(r, m-1) \oplus R(r-1, m-1).$$

Can you (just for fun, not for points on this exam) use (a), (b) to show that $R(r, m)$ is an $[2^m, 1 + \binom{m}{1} + \cdots + \binom{m}{r}, 2^{m-r}]$ $\mathbb{F}_2$-linear code?