**Math 5251 Error-correcting codes and finite fields**
**Spring 2007, Vic Reiner**
**Final exam - Due Wednesday May 2, 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. (20 points total) Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear $[n, k, d]$-code with blocklength $n = 9$ and minimum distance $d = 5$ that achieves the *highest possible* dimension $k$ among all such $\mathbb{F}_2$-linear $[9, k, 5]$ codes. For these specific values of $n$ and $d$, what ...

(a) (4 points) does Hamming's sphere-packing bound say about $k$?
(b) (4 points) does the Singleton bound say about $k$?
(c) (4 points) does the Gilbert-Varshamov bound say about $k$?
(d) (4 points) does the Plotkin bound say about $k$?
(e) (4 points) are the only two possibilities for the *exact* number $m$ of codewords in $\mathcal{C}$?
(Your answer to (e) should be two specific integers, say in the range 1 to $1,000,000$)

2. (20 points total) Let $G$ be the following matrix with entries in $\mathbb{F}_2$:

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

Let $\mathcal{C}$ be the binary code equal to the row space of $G$, with parameters $(n, m, d)$ when thought of as a binary code, and with parameters $[n, k, d]$ when thought of as an $\mathbb{F}_2$-linear code.

(a) (6 points) Write down any parity check matrix $H$, that is, one whose row space is $\mathcal{C}^\perp$.
(b) (6 points) Write down the parameters $n, m, k, d$.
(c) (5 points) Write down a collection of coset leaders for $\mathcal{C}$.
(d) (3 points) Use syndrome decoding to decode the received word $y = [11111]$, that is, to find a code word in $\mathcal{C}$ nearest to $y$ in the Hamming distance.

3. (20 points total)

(a) (10 points) Let $f(x) = x^5 + x^3 + x^2 + x + 1$ in $\mathbb{F}_2[x]$. Is the quotient ring $\mathbb{F}_2[x]/(f(x))$ a field or not? Justify your answer.
(b) (10 points) Let $f(x) = x^3 + x^2 + x + 2$ in $\mathbb{F}_3[x]$. Is the quotient ring $\mathbb{F}_3[x]/(f(x))$ a field or not? Justify your answer.

4. (20 points total) Let $W$ be a memoryless source having $m$ source words $\{w_1, \ldots, w_m\}$ which appear with probabilities $p_1, \ldots, p_m$. Let $\mathcal{C}$ be a binary Huffman encoding of $W$.

(a) (10 points) Show that if all codewords in $\mathcal{C}$ have the same length $\ell$ then $m = 2^\ell$.
(b) (10 points) Show that $\mathcal{C}$ has no codewords longer than $m-1$ letters (bits).

5. (20 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 (or concatenation) of the two length $n$ vectors $v_1$ and $v_1 + v_2$.
(a) (10 points) Prove that $\mathcal{C}_1 \oplus \mathcal{C}_2$ is $\mathbb{F}_2$-linear.
(b) (10 points) Prove this formula for the minimum distance

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

**Remark:** 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?