Math 5251 Error-correcting codes and finite fields
Spring 2007, Vic Reiner
Midterm exam 2- Due Wednesday April 4, in class

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)
(a) (10 points) We know $\alpha = \overline{20}$ in $\mathbb{F}_{53}$ has a multiplicative inverse α^{-1}. Find α^{-1} explicitly, using Euclid's algorithm.

(b) (10 points) We know that $f(x) = x^2 + 1$ and $g(x) = x^3 + x + 1$ in $\mathbb{F}_2[x]$ are relatively prime. Hence there will exist some polynomials $a(x), b(x) \in \mathbb{F}_2[x]$ satisfying $a(x)f(x) + b(x)g(x) = 1$. Find a, b explicitly, using Euclid's algorithm.

2. (24 points total) My friend and I set up a cyclic redundancy check system using the generator $g(x) = x^2 + x + 1$ in $\mathbb{F}_2[x]$.

(a) (6 points) I want to send my friend the message with bits 111000, by tacking on two extra bits a, b and sending $111000ab$ in such a way that the CRC my friend computes from this will be 0. What are a, b?

(b) (6 points) For this $g(x)$, will single bit errors in a message always be detected? Explain why, or give an example where this fails.

(c) (6 points) For this $g(x)$, will odd numbers of bit errors in a message always be detected? Explain why, or give an example where this fails.

(d) (6 points) Consider two-bit errors in which the two positions containing the errors are exactly N bits aparts. What is the smallest value of N for which such a two-bit error will be undetected by $g(x)$?

3. (21 points total) Let G be the following matrix

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

(a) (7 points) Think of the three rows of G as vectors in $(\mathbb{F}_2)^8$, generating a binary code $\mathcal{C}_1$ equal to the row space of G over $\mathbb{F}_2$. What is the (binary) rate of $\mathcal{C}_1$?

(b) (7 points) What is the minimum distance of $\mathcal{C}_1$, and up to how many errors can it correct?

(c) (7 points) Think of the three rows of G as vectors in $(\mathbb{F}_3)^8$, generating a ternary code $\mathcal{C}_2$ equal to the row space of G, this time over $\mathbb{F}_3$, not $\mathbb{F}_2$. What is the (ternary) rate of $\mathcal{C}_2$?

4. (20 points total)
(a) (3 points) Find a representative for $\overline{1000}$ in $\mathbb{Z}/37$ that lies within the set of residues $\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{36}\}$.

(b) (3 points) Do the same for $\overline{1,000,000}$ in $\mathbb{Z}/37$.

(c) (14 points) Prove that if a number N is written in decimal notation with digits $a_\ell a_{\ell-1} \cdots a_2 a_1 a_0$ (so that a_0 is the ones digit, a_1 is the tens digit, a_2 the hundreds digit, etc) then in $\mathbb{Z}/37$ one has

$$\overline{N} = \cdots + \overline{a_5 a_4 a_3} + \overline{a_2 a_1 a_0}.$$

For example, in $\mathbb{Z}/37$ one has $\overline{41,246,789,963} = \overline{41} + \overline{246} + \overline{789} + \overline{963}$.

5. (15 points total) For a ring R, a subset I of R is called an *ideal* if I is closed under

- addition, meaning that $a, b \in I$ implies $a + b \in I$, and
- multiplication by elements of R, meaning that $a \in I, r \in R$ implies $ra \in I$.

(a) (10 points) Prove that if R is a field then it has exactly two ideals, namely $I_1 = \{0\}$ and $I_2 = R$ itself.

(b) (5 points) Prove the converse: if a ring R has exactly two ideals (namely $I_1 = \{0\}$ and $I_2 = R$ itself), then R is a field.