MATH 240: HOMEWORK #1

TO BE TURNED IN DURING RECITATION ON 9/16 OR 9/18 OR AT THE END OF LECTURE ON 9/19.

I. Linear algebra over $\mathbb{Z}/2$.

The object of these problems is to get some experience working with linear algebra over $\mathbb{Z}/2 = \{\underline{0}, \underline{1}\}$. Recall that if a is an integer, then $\underline{a}$ means a mod 2. Thus either a is even and $\underline{a} = \underline{0}$ or a is odd and $\underline{a} = \underline{1}$. One adds and multiplies integers mod 2 by adding and multiplying integers in the usual way and then considering whether the result is even or odd. In other words:

$$\underline{a} + \underline{b} = \underline{a+b} \quad \text{and} \quad \underline{a} \cdot \underline{b} = \underline{a \cdot b}.$$

So, for instance, $\underline{1} + \underline{1} = \underline{2} = \underline{0}$.

1. Computations with entries in $\mathbb{Z}/2$ work the same way as with matrices with entries in $\mathbb{R}$. Find the reduced row reduced form of the matrix

$$M' = \begin{pmatrix} \underline{1} & \underline{0} & \underline{1} & \underline{1} \\ \underline{1} & \underline{1} & \underline{0} & \underline{1} \\ \underline{0} & \underline{1} & \underline{1} & \underline{0} \end{pmatrix}$$

Find the rank of M', which is the number of non-zero rows in the row reduction of M'.

2. Use your work in problem # 1 to find all vectors $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ with entries $x_1, x_2, x_3 \in \mathbb{Z}/2$ such that

$$Mx = \begin{pmatrix} \underline{1} \\ \underline{1} \\ \underline{0} \end{pmatrix}$$

when

$$M = \begin{pmatrix} \underline{1} & \underline{0} & \underline{1} \\ \underline{1} & \underline{1} & \underline{0} \\ \underline{0} & \underline{1} & \underline{1} \end{pmatrix}$$

II. The beginning of error correction

Suppose $n \geq 1$. Let $(\mathbb{Z}/2)^n$ be the set of all column vectors

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

of size n with entries x_i in $\mathbb{Z}/2 = \{\underline{0}, \underline{1}\}$. Define an alphabet to be a non-empty subset V of $(\mathbb{Z}/2)^n$ which is closed under addition. Think of V as the set of binary digit strings of length n which are allowed to use as the blocks of a message.

Given two elements x and y of $(\mathbb{Z}/2)^n$, the Hamming distance $\mathrm{dist}(x, y)$ is the number of $\underline{1}$ entries which appear in the vector $x - y$. This is the same as the number of components where x and y have different entries.

3. Show that $\text{dist}(x, y) = \text{dist}(x - y, e)$ when e is the zero vector

$$e = \begin{pmatrix} \underline{0} \\ \vdots \\ \underline{0} \end{pmatrix} \tag{0.1}$$

whose entries are all $\underline{0}$. Explain why this shows that

$$C(V) = \min\{\text{dist}(v, e) : e \neq v \in V\}$$

is the minimal Hamming distance between any two distinct elements of V. (Here we define $C(V) = 0$ if V consists of just the element e.)

4. One reason that $C(V)$ is useful is in detecting errors in transmission. Suppose someone tries to send us the message represented by the element v of V. We receive an element v' of $(\mathbb{Z}/2)^n$, but some of the digits of v may have been garbled during the transmission, so that v' might not be equal to v. Show that if $0 < \text{dist}(v', e) < C(V)$, we will know v' cannot be an element of the alphabet V, so that some garbling must have occurred. Explain why it is useful to find V for which $C(V)$ is large.

5. Let $f : (\mathbb{Z}/2)^n \to (\mathbb{Z}/2)^{2n}$ be the function which sends a column vector

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

to the column vector

$$f(x) = \begin{pmatrix} y_1 \\ \vdots \\ y_{2n} \end{pmatrix}$$

defined by $y_{2i-1} = y_{2i} = x_i$ for $i = 1, \ldots, n$. Thus one gets the entries of $f(x)$ by repeating each entry of x twice in succession.

a. Show that f is additive, in the sense that $f(x+x') = f(x)+f(x')$ when $x, x' \in (\mathbb{Z}/2)^n$.

b. Conclude that $f(V) = \{f(x) : x \in V\}$ is a subset of $(\mathbb{Z}/2)^{2n}$ which is closed under addition.

c. Show that if e is the zero vector of length n defined in equation (2.1), $f(e)$ is the zero vector of length $2n$

d. Show $\text{dist}(f(x), f(e)) = 2 \cdot \text{dist}(x, e)$ for all x in $(\mathbb{Z}/2)^n$. Use this and problem #3 to conclude that $C(f(V)) = 2C(V)$.

III. Extra Credit

A. Suppose $n \geq 4$. Is there a $2 \times n$ matrix M' such that when

$$V = \{x \in (\mathbb{Z}/2)^n : M'x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$$

one has $C(V) > 2$? (Hint: First show that two of the first four columns of M' must be equal.)