MATH 240: HOMEWORK #2

DUE IN FLORA'S MAILBOX BY NOON ON OCT. 21.

1. Homework problems

1. Let M be the $3 \times 7 = m \times n$ matrix

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{1.1}$$

with entries in $F = \mathbb{Z}/2 = \{0, 1\}$. Find a reduced row echelon matrix M' which results from applying row reduction to M.

2. Find the column numbers $\{j(1), j(2), j(3)\}$ of the pivot entries of M'.

3. Find a basis $B = \{b(1), b(2), b(3), b(4)\}$ for the nullspace $Null(M) = Null(M')$ of M using the algorithm recalled at the end of this problem set. This algorithm uses the non-pivot columns $\{f(1), f(2), f(3), f(4)\}$ of M'.

4. Suppose we use $Null(M)$ as an alphabet to do error correction. As in the first homework assignment, this means that letters of the alphabet $Null(M)$ are transmitted by sending them as vectors of length 7 with entries in $F = \{0, 1\}$. Recall that the Hamming distance $\mathrm{dist}(x, y)$ between two vectors $x, y \in F^n$ is the number of component at which x and y differ. The number $C(Null(M))$ is the minimal Hamming distance $\mathrm{dist}(\underline{0}, x)$ between the zero vector $\underline{0}$ of $Null(M)$ and a non-zero vector x in $Null(M)$. If fewer than $C(Null(M))/2$ errors are made in transmitting a given letter $x \in Null(M)$, we can recover x by taking the element of $Null(M)$ which has minimal hamming distance from the message y in F^n that was received.
   a. Show that if $x = \sum_{j=1}^{4} x_{f(j)} b(j)$ and q is the number of $x_{f(1)}, x_{f(2)}, x_{f(3)}, x_{f(4)}$ which are not 0, then $\mathrm{dist}(\underline{0}, x) \geq q$.
   b. Show that $\mathrm{dist}(\underline{0}, x) = q$ if and only if when we write

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

   the entry x_j is 0 whenever j is a pivot column index.

5. Show that $C(Null(M)) \geq 3$ as long as $b(i)$ (resp. $b(i)+b(j)$) has at least two non-zero entries (resp. has at least one non-zero entry) at a pivot column coordinate for all distinct pairs of integers $i, j \in \{1, 2, 3, 4\}$. (This condition does in fact hold, so $C(Null(M)) \geq 3$, but you do not have to write out the details of checking the condition.) Since $1 < C(Null(M))/2 = 3/2$, this means we can correct an error of one digit in message transmitted using the alphabet $Null(M)$.

Historical comment: The space $V = Null(M) \subset (\mathbb{Z}/2)^7$ was one of the first examples of an efficient error correcting alphabet proposed by Hamming in the 1940's.

2. An application of column spans

Suppose that the rows of an $m \times n$ matrix $M = (a_{i,j})_{i,j}$ with entries in $\mathbb{Z}/2 = \{0, 1\}$ represent the answers of m people to a sequence of n true/false questions. Thus the i^{th} row

$$(a_{i,1}, \ldots, a_{i,n})$$

signifies that the answer of the i^{th} person to question number j was $a_{i,j} = 1$ if they said "true" and $a_{i,j} = 0$ if they said "false". We discussed in class the problem of picking out a subset J of $\{1, \ldots, n\}$ with the property that if one knows how a person answered each question which has a number j in J, then one can tell how they answered every question.

6. Suppose J is large enough so that the columns of M with indices in J span the column space of M. Is such a J large enough so that the way a person answers questions having an index in J determines their answer to every question? Why or why not?
7. Use what we showed in class about the column space to show that J can be taken to be the set of pivot columns of a reduced row echelon matrix M' which is row equivalent to M.
8. Suppose M is the matrix
$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
Show that the any set of columns which span the column space of M must contain both columns of M. On the other hand, suppose as above that the rows of M represent answers by two people to two true/false questions. Is it true the way each person answers every question is determined by how they answer the first question?

Extra Credit: Formulate a requirement on how one must be able to determine answers to every question, using the subset of answers represented by questions with column indices in J, which is strong enough to force the columns in J to contain a basis for the column space of M.

3. An algorithm for computing bases for nullspaces.

In lecture we talked about how to find a basis for the null space

$$Null(M) = \{x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : Mx = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\}$$

of an $m \times n$ matrix $M = (a_{i,j})_{1 \le i \le m,\ 1 \le j \le n}$. Here is the algorithm.

A. The nullspace is the same as that of the reduced row echelon matrix M' associated to M. Suppose M' has nonzero rows numbered 1 through ℓ, and that the pivot column of row i has number $j(i)$ for $1 \le i \le \ell$. Here ℓ is the rank of M. The pivot variables are $\{x_{j(i)}\}_{i=1}^{\ell}$. The remaining variables are the free variables $\{x_{f(i)}\}_{i=1}^{n-\ell}$ if we list the columns numbers in $\{1, \ldots, n\} - \{j(i)\}_{i=1}^{\ell}$ as $f(1), \ldots, f(n - \ell)$. In solving

$$M'x = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

for x, one can choose the values of the free variables arbitrarily; there is then a unique way to solve for the pivot variables.

B. For $j = 1, \ldots, n - \ell$, we can find a unique solutioin

$$b(j) = \begin{pmatrix} b_{j,1} \\ \vdots \\ b_{j,n} \end{pmatrix}$$

of

$$M' \cdot b(j) = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

such that

$$b_{j,f(j)} = 1 \quad \text{and} \quad b_{j,f(k)} = 0 \quad \text{if} \quad 1 \le k \ne j \le n - \ell.$$

This determines $b_{j,z}$ whenever $z \in \{f(1), \ldots, f(n-\ell)\}$, i.e. for z which are non-pivot column indices.

We now need to determine $b_{j,z}$ when $z = j(i)$ is a pivot column index for some $1 \le i \le \ell$. Then

$$a_{i,z} = a_{i,j(i)} = 1$$

is the only pivot entry in row i, so $a_{i,q} = 0$ if q is a pivot column index other that $z = j(i)$. We have $b_{j,q'} = 0$ by construction if q' is a non-pivot column index different from $f(j)$, while $b_{j,f(j)} = 1$. So the i^{th} row of the equality

$$M' \cdot b(j) = M' \cdot \begin{pmatrix} b_{j,1} \\ \vdots \\ b_{j,n} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

gives the equation

$$\sum_{t=1}^{\ell} a_{i,j(t)} b_{j(t)} + \sum_{z=1}^{n-\ell} a_{i,f(z)} b_{f(z)} = 1 \cdot b_{j,j(i)} + a_{i,f(j)} \cdot b_{j,f(j)} = b_{j,j(i)} + a_{i,f(j)} = 0.$$

Thus we get

$$b_{j,j(i)} = -a_{i,f(j)}$$

which determines the entries of $b(j)$ at components having pivot indices.

C. The set $B = \{b(j)\}_{j=1}^{n-\ell}$ is a basis for $Null(M) = Null(M')$ for the following reason. Suppose

$$y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

is in $Null(M) = Null(M')$. Then y and $\sum_{j=1}^{n-\ell} y_{f(j)} b(j)$ have the same coordinate $y_{f(j)}$ at each free variable position $f(j)$ as j ranges from 1 to $n - \ell$. Since elements of $Null(M')$ are determined uniquely by their coordinates at the free variables, we have to have $y = \sum_{j=1}^{n-\ell} y_{f(j)} b(j)$. So B spans $Null(M')$, and the elements of B are independent by considering their components at the free variable positions.

D. Suppose

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

is a column vector in $(\mathbb{Z}/2)^n$. We can find if $x \in Null(M)$ simply by checking if Mx is the zero vector. If this is so, then part C above shows

$$x = \sum_{j=1}^{n-\ell} x_{f(j)} b(j).$$