Assignment # 2 Due 2-8-05

3.15, 3.16, 3.17, 3.18

3.15 $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ is a generator matrix for the triple check code:

By defn (p. 7) $C = \{abcxyz \in \mathbb{Z}_2^6 \mid abx, acy, \text{ and } bcz \text{ have even \# of 1's}\}$

Note that for the columns of the matrix, we have

column	abx	acy	bcz
1	110	101	101
2	110	110	110
3	011	011	110

So the columns belong to C. Since the matrix has rank 3 (rows 6, 4+5, and 4 are an identity matrix) it is a generator matrix for C by the proposition on p. 38

3.16 $$H = \begin{bmatrix} 111\ 000 & 1000 \\ 100\ 110 & 0100 \\ 010\ 101 & 0010 \\ 001\ 011 & 0001 \end{bmatrix} = (B, I)$$

So by the proposition, p. 41

$$G = \begin{bmatrix} I_6 \\ A \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$A = -B$
$= B$ in $\mathbb{Z}_2$

is a generator matrix

G is a rank 6 ~~[illegible]~~ 10×6 matrix, so C has block size 10 and rank 6. The columns of G are codewords of weight 3, so $d(C)$ is at most 3. Suppose $x = (x_1 x_2 \ldots x_{10})$ is a codeword of weight 2. Being a codeword, $Hx^T = 0$, so

~~$x_1 + x_2 + x_3 = 0, x_1 + x_4 + x_5$~~
$$x_1 + x_2 + x_3 + x_7 = 0$$
$$x_1 + x_4 + x_5 + x_8 = 0$$
$$x_2 + x_4 + x_6 + x_9 = 0$$
$$x_3 + x_5 + x_6 + x_{10} = 0.$$

If $wt(x_1 \ldots x_6) = 0$, then $x_7 = x_8 = x_9 = x_{10} = 0$ and $wt(x) = 0$.
If $wt(x_1 \ldots x_6) = 1$, then x is one of the columns of G and $wt(x) = 3$, not 2.
If $wt(x_1 \ldots x_6) = 2$ and $wt(x) = 2$ then $x_7 = x_8 = x_9 = x_{10} = 0$.
Let x_i, x_j $1 \le i < j \le 6$ be the non-zero entries. Then

i	j	
1	2	~~$0 = x_1 + x_4 + x_5 + x_8 = 1$~~ $0 = x_1 + x_4 + x_5 + x_8 = 1$
1	3	$0 = x_1 + x_4 + x_5 + x_8 = 1$
1	4	$0 = x_1 + x_2 + x_3 + x_7 = 1$
1	5	$0 = x_1 + x_2 + x_3 + x_7 = 1$
1	6	$0 = x_1 + x_2 + x_3 + x_7 = 1$
2	3	$0 = x_2 + x_4 + x_6 + x_9 = 1$
2	4	$0 = x_1 + x_2 + x_3 + x_7 = 1$
2	5	$0 = x_2 + x_4 + x_6 + x_9 = 1$
2	6	$0 = x_1 + x_2 + x_3 + x_7 = 1$
3	4	$0 = x_1 + x_2 + x_3 + x_7 = 1$
3	5	$0 = x_1 + x_2 + x_3 + x_7 = 1$
3	6	$0 = x_1 + x_2 + x_3 + x_7 = 1$

i	j	
4	5	$0 = x_2 + x_4 + x_6 + x_9 = 1$
4	6	$0 = x_1 + x_4 + x_5 + x_8 = 1$
5	6	$0 = x_1 + x_4 + x_5 + x_8 = 1$

In all cases, we have a contradiction. So there is no such word and $d(C) = 3$

3.17

$$H \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+0+1+1 \\ 1+0+1+0 \\ 0+0+1+1 \\ 1+1+1+1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Not a codeword. But Hx^T = column 7 of H.
If change 7th entry, get (1 0 1 0 1 1 0 0 1 1) which H multiplies to 0.

$$H \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0+1+0+1 \\ 0+1+0+1 \\ \cancel{0+1+0+1+1} \\ 1+1+1+1 \\ 0+1+0+1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

(0 1 0 1 0 1 1 1 1) is a codeword

$$H \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1+0+1+1 \\ 1+1+1+1 \\ 0+1+0+1 \\ 1+1+0+1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Not a codeword. But Hx^T = column 3 of H.
If change 3rd entry, get (1 0 0 1 1 0 1 1 1 1) which H multiplies to 0.

$$H \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1+1+1+0 \\ 1+0+1+1 \\ 1+0+1+1 \\ 1+1+1+0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Not a column of H. So $(1\,1\,0\,1\,1\,0\,1\,1\,0)$ is at least distance 2 from a codeword.

__3.18__ C has $2^m = 64$ elements. There are $2^{10} = 1024$ words of blocksize 10. For a given codeword c, there are 11 words at distance 0 or 1. Thus there are $64 \times 11 = 704$ words that can be corrected to words in C by changing at most one bit. Hence there are $1024 - 704 = 320$ words of length 10 that cannot be corrected to codewords by correcting at most one bit.