ECS 452: In-Class Exercise #14

Date: 22 / 03 / 2019			
Name	ID (last 3 digits)		
Prapun	5	5	5

Instructions

1. Separate into groups of no more than three persons. **The group cannot be the same as any of your former groups after the midterm.**
2. **Write down all the steps** that you have done to obtain your answers. You may not get full credit even when your answer is correct without showing how you get your answer.
3. **Do not panic.**

Consider a block code whose generator matrix is

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

1. Find the length *k* of each message block
   G has 6 columns. Therefore, $n = 6$.

2. Find the code length *n*
   G has 3 rows. Therefore, $k = 3$.

3. In the table below, list all possible data (message) vectors $\underline{\mathbf{b}}$ in the leftmost column (one in each row). Then, find the corresponding codewords $\underline{\mathbf{x}}$ and their weights in the second and third columns, respectively.

$\underline{\mathbf{b}}$	$\underline{\mathbf{x}}$	$w(\underline{\mathbf{x}})$
$b_1 b_2 b_3$	$x_1 x_2 x_3 x_4 x_5 x_6$	
000	000000	0
001	101010	3
010	001101	3
011	100111	4
100	110001	3
101	011011	4
110	111100	4
111	010110	3

First, we list all possible $\underline{\mathbf{b}}$.

Next, from $\underline{\mathbf{x}} = \underline{\mathbf{b}}\mathbf{G}$, we can calculate the codeword $\underline{\mathbf{x}}$ corresponding to each $\underline{\mathbf{b}}$ one by one. Alternatively, by considering $\underline{\mathbf{b}} = [b_1 b_2 b_3]$ and carrying out the multiplication $\underline{\mathbf{x}} = [b_1 b_2 b_3]\mathbf{G}$, we have

$\underline{\mathbf{x}} = [b_1 \oplus b_3 \quad b_1 \quad b_2 \oplus b_3 \quad b_2 \quad b_3 \quad b_1 \oplus b_2]$.

So, each "column" of the answer for $\underline{\mathbf{x}}$ can be calculated accordingly. In particular,

- the 2nd, 4th, and 5th columns are simply copied from the columns for b_1, b_2, and b_3 respectively,
- the 1st column is simply the sum of the columns for b_1 and b_3,
- the 3rd column is simply the sum of the columns for b_2 and b_3
- the 6th column is simply the sum of the columns for b_1 and b_2.

4. Find the minimum distance $d_{\min}$ for this code.
   If the code is linear, then $d_{\min} = \min_{\underline{\mathbf{x}} \neq \underline{\mathbf{0}}} w(\underline{\mathbf{x}}) = 3$.

   Is this a linear code? On page 34 of the lecture slides, we noted that if a code is generated by plugging in every possible $\underline{\mathbf{b}}$ into $\underline{\mathbf{x}} = \underline{\mathbf{b}}\mathbf{G}$, then the code will automatically be linear. This is exactly how the code in this problem is created. [See the next page for the proof of this property.]

Fact: If a code is generated by plugging in every possible $\underline{\mathbf{b}}$ into $\underline{\mathbf{x}} = \underline{\mathbf{b}}\mathbf{G}$, then the code will automatically be linear.

Proof

If $\mathbf{G}$ has k rows. Then, $\underline{\mathbf{b}}$ will have k bits. We can list them all as $\underline{\mathbf{b}}^{(1)}, \underline{\mathbf{b}}^{(2)}, \ldots, \underline{\mathbf{b}}^{(2^k)}$. The corresponding codewords are

$$\underline{\mathbf{x}}^{(i)} = \underline{\mathbf{b}}^{(i)}\mathbf{G} \text{ for } i = 1, 2, \ldots, 2^k.$$

Let's take two codewords, say, $\underline{\mathbf{x}}^{(i_1)}$ and $\underline{\mathbf{x}}^{(i_2)}$. By construction, $\underline{\mathbf{x}}^{(i_1)} = \underline{\mathbf{b}}^{(i_1)}\mathbf{G}$ and $\underline{\mathbf{x}}^{(i_2)} = \underline{\mathbf{b}}^{(i_2)}\mathbf{G}$. Now, consider the sum of these two codewords:

$$\underline{\mathbf{x}}^{(i_1)} \oplus \underline{\mathbf{x}}^{(i_2)} = \underline{\mathbf{b}}^{(i_1)}\mathbf{G} \oplus \underline{\mathbf{b}}^{(i_2)}\mathbf{G} = \left(\underline{\mathbf{b}}^{(i_1)} \oplus \underline{\mathbf{b}}^{(i_2)}\right)\mathbf{G}$$

Note that because we plug in ***every possible*** $\underline{\mathbf{b}}$ to create this code, we know that $\underline{\mathbf{b}}^{(i_1)} \oplus \underline{\mathbf{b}}^{(i_2)}$ should be one of these $\underline{\mathbf{b}}$. Let's suppose $\underline{\mathbf{b}}^{(i_1)} \oplus \underline{\mathbf{b}}^{(i_2)} = \underline{\mathbf{b}}^{(i_3)}$ for some $\underline{\mathbf{b}}^{(i_3)}$. This means

$$\underline{\mathbf{x}}^{(i_1)} \oplus \underline{\mathbf{x}}^{(i_2)} = \underline{\mathbf{b}}^{(i_3)}\mathbf{G}.$$

But, again, by construction, $\underline{\mathbf{b}}^{(i_3)}\mathbf{G}$ gives a codeword $\underline{\mathbf{x}}^{(i_3)}$ in this code. Because the sum of any two codewords is still a codeword, we conclude that the code is linear.