ECS 452: Digital Communication Systems **2015/2**

HW 6 — Due: Apr 20

Lecturer: Asst. Prof. Dr. Prapun Suksompong

Instructions

(a) Solve all non-optional problems. (5 pt)

(i) Write your first name and the last three digit of your student ID on the upper-right corner of ***every*** submitted page.

(ii) For each part, write your explanation/derivation and answer **in the space provided**.

(b) ONE part of a question will be graded (5 pt). Of course, you do not know which part will be selected; so you should work on all of them.

(c) Late submission will be rejected.

(d) **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.

Problem 1. Consider a block code whose generator matrix is

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

(a) Suppose the message is $\underline{\mathbf{b}} = [1\,0\,1]$. Find the corresponding codeword $\underline{\mathbf{x}}$.

There are several equivalent ways to approach this problem.

1) We can simply use

$$\underline{x} = \underline{b}\,G = [1\;0\;1]\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} = [1\;0\;1\;0\;1\;1].$$

2) Recall that $\underline{b}\,G = \sum_{j=1}^{n} b_j \underbrace{\underline{g}^{(j)}}_{\text{the } j^{\text{th}} \text{ row of } G} = (1\times\underline{g}^{(1)}) + (0\times\underline{g}^{(2)}) + (1\times\underline{g}^{(3)}) = \underline{g}^{(1)} \oplus \underline{g}^{(3)} = [1\;0\;1\;0\;1\;1].$

3) See next part.

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

Derivation of the recipe for calculating the codewords in Q1b:

Suppose we want to encode many message vectors $\underline{b}^{(1)}, \underline{b}^{(2)}, \underline{b}^{(3)}, \dots$

We can first stack them up in the form of a big matrix $B = \begin{bmatrix} \underline{b}^{(1)} \\ \underline{b}^{(2)} \\ \vdots \end{bmatrix}$. Then, $BG = \begin{bmatrix} \underline{b}^{(1)}G \\ \underline{b}^{(2)}G \\ \vdots \end{bmatrix} = \begin{bmatrix} \underline{x}^{(1)} \\ \underline{x}^{(2)} \\ \vdots \end{bmatrix} \equiv X$

So, the i^{th} row of BG gives the codeword corresponding to the i^{th} message $\underline{b}^{(i)}$

Now, let's view the columns inside matrices G, X, and B:

$$X = BG = B\underbrace{\begin{bmatrix} \vec{v}^{(1)} & \vec{v}^{(2)} & \cdots & \vec{v}^{(n)} \end{bmatrix}}_{G} = \begin{bmatrix} B\vec{v}^{(1)} & B\vec{v}^{(2)} & \cdots & B\vec{v}^{(n)} \end{bmatrix}$$

Observe that the j^{th} column of X is $B\vec{v}^{(j)} = \begin{bmatrix} \vec{u}^{(1)} & \vec{u}^{(2)} & \cdots \end{bmatrix} \begin{bmatrix} v_1^{(j)} \\ v_2^{(j)} \\ \vdots \\ v_k^{(j)} \end{bmatrix} = \sum_i v_i^{(j)} \vec{u}^{(i)}$

= a linear combination of the columns of B

Here, the linear combination is simply the sum of the columns of B whose position corresponds to the 1s' positions in the j^{th} column of G.

The 4^{th} column of G is $[1\ 0\ 1]^T$. Therefore, the 4^{th} element of $\underline{x}$ is the sum of the 1^{st} and 3^{rd} elements of $\underline{b}$.

The 5^{th} column of G is $[0\ 1\ 1]^T$. Therefore, the 5^{th} element of $\underline{x}$ is the sum of the 2^{nd} and 3^{rd} elements of $\underline{b}$.

The 6^{th} column of G is $[1\ 1\ 0]^T$. Therefore, the 6^{th} element of $\underline{x}$ is the sum of the 1^{st} and 2^{nd} elements of $\underline{b}$.

$\underline{\mathbf{b}}$	$\underline{\mathbf{x}}$	$w(\underline{\mathbf{x}})$	$d(\underline{x}, \underline{y})$
000	000000	0	5
001	001110	3	4
010	010011	3	4
011	011101	4	1
100	100101	3	2
101	101011	4	3
110	110110	4	3
111	111000	3	2

for part (d.i)

The first three columns in G is the identity matrix. So, we simply copy $\underline{b}$ here.

(c) Find the minimum distance $d_{\min}$ for this code.

$$d_{min} = \min_{\underline{x} \neq 0} w(\underline{x}) = 3$$

(d) Suppose we receive $\underline{\mathbf{y}} = [1\,1\,1\,1\,0\,1]$.

(i) Minimum distance decoding:

i. Find the distance $d(\underline{\mathbf{x}}, \underline{\mathbf{y}})$ between this received vector $\underline{\mathbf{y}}$ and each of the possible codewords $\underline{\mathbf{x}}$. Put your answers in a new column in the table above.

ii. Use the answer in the previous part to find $\hat{\underline{\mathbf{x}}}$ and $\hat{\underline{\mathbf{b}}}$

$$\hat{\underline{x}} = \arg\min_{\underline{x}} d(\underline{x}, \underline{y}) = [0\ 1\ 1\ 1\ 0\ 1] \Rightarrow \hat{\underline{b}} = [0\ 1\ 1]$$

(ii) Decoding via the syndrome:

i. Find the parity check matrix $\mathbf{H}$ of this code.

$$G = \left[\ \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{I}\ \ \underbrace{\begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{matrix}}_{P}\ \right] \Rightarrow H = \left[\ \underbrace{\begin{matrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{matrix}}_{P^T}\ \ \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{I}\ \right]$$

ii. Find the syndrome vector $\underline{\mathbf{s}}$.

$$\underline{y} = 1\ 1\ 1\ 1\ 0\ 1$$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} \xrightarrow{\Sigma} 1 \\ \xrightarrow{\Sigma} 0 \\ \xrightarrow{\Sigma} 1 \end{matrix}$$

$\underline{s} = \underline{y} H^T$

$= (\text{sum of all columns of } H \text{ except the } 5^{th} \text{ column})^T$

$= [1\ 0\ 1]$

iii. Use the answer in the previous parts to find $\hat{\underline{\mathbf{x}}}$ and $\hat{\underline{\mathbf{b}}}$

$\underline{s}$ is the same as the first column of H. Hence, $\hat{\underline{e}} = [1\ 0\ 0\ 0\ 0\ 0]$.

$$\hat{\underline{x}} = \underline{y} \oplus \hat{\underline{e}} = [0\ 1\ 1\ 1\ 0\ 1] \Rightarrow \hat{\underline{b}} = [0\ 1\ 1]$$

Problem 2. Consider the following encoding and decoding for a systematic linear block code:

- Encoding
  - The bit positions that are powers of 2 (1, 2, 4, 8, 16, etc.) are check bits.
  - The rest (3, 5, 6, 7, 9, etc.) are filled up with the k data bits.
  - Each check bit forces the parity of some collection of bits, including itself, to be even.
    - To see which check bits the data bit in position i contributes to, rewrite i as a sum of powers of 2. A bit is checked by just those check bits occurring in its expansion.

This is a general statement about systematic linear block code

- Decoding
  - When a codeword arrives, the receiver initializes a counter to zero. It then examines each check bit at position i ($i = 1, 2, 4, 8, \ldots$) to see if it has the correct parity.
  - If not, the receiver adds i to the counter. If the counter is zero after all the check bits have been examined (i.e., if they were all correct), the codeword is accepted as valid. If the counter is nonzero, it contains the position of the incorrect bit.

We will consider the case when the codeword's length $n = 7$.

(a) How many bits are check bits?
Hint: How many bit positions are powers of 2?

There are $n=7$ bits in each codeword.
The check bits are defined to be the bits whose positions are powers of 2.
Among the possible positions $(1, 2, 3, \ldots, 7)$, three positions $2^0 = 1$, $2^1 = 2$, $2^2 = 4$ are powers of 2.
So, there are three check bits. (Note that $k = 7-3 = 4$ bits)

position of p_1 position of p_2 position of p_3

(b) Find the generator matrix **G** for this code.

Let p_1, p_2, p_3 be the check bits and d_1, d_2, d_3, d_4 be the data bits

positions that are powers of 2

Then each codeword is of the form $\underline{x} = [x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7] = [p_1\ p_2\ d_1\ p_3\ d_2\ d_3\ d_4]$

For example, d_1 is in the $i = 3^{rd}$ position. $= 2^0 + 2^1 + 0$.

So, it is used in the eqn. of p_1 and p_2

Following the encoding instructions, we express the position values in binary

$$
\begin{array}{ccccccc}
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{array}
\quad
\begin{array}{l}
\rightarrow p_1 \oplus d_1 \oplus d_2 \oplus d_4 = 0 \quad \ldots (1) \\
\rightarrow p_2 \oplus d_1 \oplus d_3 \oplus d_4 = 0 \quad \ldots (2) \\
\rightarrow p_3 \oplus d_2 \oplus d_3 \oplus d_4 \underbrace{= 0}_{} \quad \ldots (3)
\end{array}
$$

forcing even parity

$$\Downarrow$$

$$p_1 = d_1 \oplus d_2 \oplus d_4$$
$$p_2 = d_1 \oplus d_3 \oplus d_4$$
$$p_3 = d_2 \oplus d_3 \oplus d_4$$

$$
G = \begin{array}{c}
\begin{array}{ccccccc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\ p_1 & p_2 & d_1 & p_3 & d_2 & d_3 & d_4 \end{array} \\
\left[\begin{array}{ccccccc}
1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1
\end{array}\right]
\end{array}
\Leftarrow
$$

(c) Find the corresponding parity check matrix **H**.

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

(d) Explain, from the elements inside the matrix **H**, how this is a Hamming code.

The columns of H cover all the nonzero binary vectors of length 3.

(e) Explain how the decoding instruction above is the "same" as the decoding via the syndrome described in class.

The provided decoding instruction starts with calculations of the bits inside the syndrome $\underline{s} = \underline{y} H^T$.
Note that p_j is at position $i = 2^{j-1}$.

If s_j is 1 (received vector does not satisfy eq. (j)), the value $i = 2^{j-1}$ is added to the counter.

At the end, the value in the counter is $I = \sum_j s_j 2^{j-1}$ which is exactly the same as converting the binary vector $\underline{s}$ to a decimal number.

Note that the columns of H are arranged in increasing values (treating the top element as the LSB).
Therefore, the value I in the counter simply indicates the index of the column of H that matches $\underline{s}$.
We know that this is the most-likely position of the incorrect bit.

Problem 3. Construct a generator matrix **G** and a corresponding parity check matrix **H** for a (15,11) Hamming code.

(15,11) Hamming code
$\left.\begin{array}{l} k = 11 \\ n = 15 \end{array}\right\} \Rightarrow m = 4.$

First, we construct the parity check matrix H.

$m = 4 \Rightarrow$ Put all $2^4 - 1 = 15$ nonzero 4-bit column vectors as columns of H. They can be arranged in any order but for simplicity, we put the columns corresponding to the identity matrix in the front:

$$\mathbf{H} = \left(\begin{array}{cccc|ccccccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{array}\right)$$

I_4 P

P^T I_{11}

$$\mathbf{G} = \left(\begin{array}{cccc|ccccccccccc}
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

From the recipe discussed in class,

when $H = [I \,\vdots\, A]$,

we know that the generator matrix is

$G = [A^T \,\vdots\, I]$

the size of this I is easily determined from the # rows in A^T

Problem 4 (Carlson and Crilly, 2009, P13.2-1)**.** (Optional) In mathematical analysis, a function $d(\underline{\mathbf{x}}, \underline{\mathbf{y}})$ is a "true" distance if it satisfies all of the following properties:

(i) positivity: $d(\underline{\mathbf{x}}, \underline{\mathbf{y}}) \geq 0$ with equality if and only if $\underline{\mathbf{x}} = \underline{\mathbf{y}}$

(ii) symmetry: $d(\underline{\mathbf{x}}, \underline{\mathbf{y}}) = d(\underline{\mathbf{y}}, \underline{\mathbf{x}})$

(iii) triangle inequality: $d(\underline{\mathbf{x}}, \underline{\mathbf{z}}) \leq d(\underline{\mathbf{x}}, \underline{\mathbf{y}}) + d(\underline{\mathbf{y}}, \underline{\mathbf{z}})$

Is the Hamming distance a "true" distance? (Prove or disprove)

Hint: For the triangle inequality, first consider the number of 1s in $\underline{\mathbf{u}}$, $\underline{\mathbf{v}}$, and $\underline{\mathbf{u}} \bigoplus \underline{\mathbf{v}}$ and confirm that $d(\underline{\mathbf{u}}, \underline{\mathbf{v}}) \leq w(\underline{\mathbf{u}}) + w(\underline{\mathbf{v}})$. Then, from this inequality, replace $\underline{\mathbf{u}}$ by $\underline{\mathbf{x}} \bigoplus \underline{\mathbf{y}}$ and $\underline{\mathbf{v}}$ by $\underline{\mathbf{y}} \bigoplus \underline{\mathbf{z}}$.

First, by definition, we can write $d(\underline{x}, \underline{y}) = w(\underline{x} \oplus \underline{y})$.

(i) Because $d(\underline{x}, \underline{y})$ is the weight of the vector $\underline{x} \oplus \underline{y}$, which is simply counting #1s in $\underline{x} \oplus \underline{y}$, it is always ≥ 0.

Next, suppose $\underline{x} = \underline{y}$. Then, $\underline{x} \oplus \underline{y} = \underline{0}$ and $d(\underline{x}, \underline{y}) = w(\underline{x} \oplus \underline{y}) = w(\underline{0}) = 0$.

suppose $\underline{x} \neq \underline{y}$. Then, there must be at least one position whose corresponding values are different in $\underline{x}$ and $\underline{y}$. This implies there must be at least a 1 in $\underline{x} \oplus \underline{y}$ and hence

$$d(\underline{x}, \underline{y}) = w(\underline{x} \oplus \underline{y}) \geq 1 > 0$$
$$\neq 0$$

Therefore, $d(\underline{x}, \underline{y}) = 0$ if and only if $\underline{x} = \underline{y}$.

(ii) Because $\underline{x} \oplus \underline{y} = \underline{y} \oplus \underline{x}$,

$$d(\underline{x}, \underline{y}) = w(\underline{x} \oplus \underline{y}) = w(\underline{y} \oplus \underline{x}) = d(\underline{y}, \underline{x})$$

(iii) Triangle inequality

First we show that for any pair of vector $\underline{u}$ and $\underline{v}$,

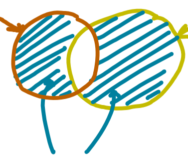
$$d(\underline{u}, \underline{v}) \leq w(\underline{u}) + w(\underline{v})$$

Recall that $d(\underline{u}, \underline{v}) \equiv w(\underline{u} \oplus \underline{v})$.

and that the XOR operation will give a 1 iff we have $1 \oplus 0$ or $0 \oplus 1$.

Let A be the set of the positions of 1s in $\underline{u}$

$|A| = w(\underline{u})$



Let B be the set of the positions of 1s in $\underline{v}$.

$|B| = w(\underline{v})$

Observe that these areas give the positions of 1s in $\underline{u} \oplus \underline{v}$

Therefore, $w(\underline{u} \oplus \underline{v}) = | \quad | \leq w(\underline{u}) + w(\underline{v})$ (by comparing the area in the Venn's diagram)

Now, let $\underline{u} = \underline{x} \oplus \underline{y}$ and $\underline{v} = \underline{y} \oplus \underline{z}$.

From the above inequality, we have

$$w(\underline{x} \oplus \underbrace{\underline{y} \oplus \underline{y}}_{\underline{0}} \oplus \underline{z}) \leq w(\underline{x} \oplus \underline{y}) + w(\underline{y} \oplus \underline{z})$$

(In GF(2), $\underline{v} \oplus \underline{v} = \underline{0}$)

Hence, $d(\underline{x}, \underline{z}) \leq d(\underline{x}, \underline{y}) + d(\underline{y}, \underline{z})$

Problem 5 (Carlson and Crilly, 2009, P13.2-2 and P13.2-3). (Optional) Consider a block code. Suppose $\underline{\mathbf{x}}$ is the transmitted codeword and that $\underline{\mathbf{y}}$ is the vector that results when $\underline{\mathbf{x}}$ is received with $i > 0$ bit errors. Use the triangle inequality for the Hamming distance to show that

(a) if the code has $d_{\min} \geq \ell + 1$ and if $i \leq \ell$, then the errors are detectable.

Recall that, to detect error(s), we simply check whether the received vector $\underline{y}$ is a valid codeword.

The errors in $\underline{y}$ are detectable iff $\underline{y}$ is not a valid codeword.

Consider any codeword $\underline{c} \in \mathcal{C}$ that is not $\underline{x}$.

From $$\ell+1 \underbrace{\leq}_{\text{given}} d_{\min} \underbrace{\leq}_{\text{by definition of being } d_{\min}} d(\underline{x},\underline{c}) \underbrace{\leq}_{\text{triangle inequality}} d(\underline{x},\underline{y}) + d(\underline{y},\underline{c}) \underbrace{=}_{\underline{x}\oplus\underline{y}=\underline{e}} w(\underline{e}) + d(\underline{y},\underline{c}) \underbrace{\leq}_{\text{given } (w(\underline{e})\leq \ell)} \ell + d(\underline{y},\underline{c}),$$

we have $d(\underline{y},\underline{c}) \geq 1 > 0$. So, $\underline{y}$ cannot be the same as any codeword in $\mathcal{C}$.
(unless $\underline{y} = \underline{x}$, in which case, the is no error to detect.)
Hence, the errors in $\underline{y}$ are detectable.

(b) if the code has $d_{\min} \geq 2t + 1$ and if $i \leq t$, then the errors are correctable by the minimum distance decoder.

Consider any codeword $\underline{c} \in \mathcal{C}$ that is not $\underline{x}$.

From $$2t+1 \underbrace{\leq}_{\text{given}} d_{\min} \underbrace{\leq}_{\text{by definition of being } d_{\min}} d(\underline{x},\underline{c}) \underbrace{\leq}_{\text{triangle inequality}} d(\underline{x},\underline{y}) + d(\underline{y},\underline{c}) \underbrace{=}_{\underline{x}\oplus\underline{y}=\underline{e}} w(\underline{e}) + d(\underline{y},\underline{c}) \underbrace{\leq}_{\text{given } (w(\underline{e})\leq t)} t + d(\underline{y},\underline{c}),$$

we have $d(\underline{y},\underline{c}) \geq t+1 > t$

However, $d(\underline{y},\underline{x}) = w(\underline{e}) \leq t$. So, $\underline{y}$ is closer to $\underline{x}$ than any other valid codeword.
Hence, when $\underline{y}$ is observed, the min distance decoder will output $\underline{x}$ correcting all the errors in $\underline{y}$.