Math 259: Spring 2019
Quiz 3

NAME: SOLUTIONS

Are you taking this class for graduate credit?

Time: **30 minutes**

Problem	Value	Score
1	6	
2	3	
3	11	
TOTAL	20	

Problem 1 : (6 points) Consider a binary linear code given by the generating matrix

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

a) (3 points) Write down a parity check matrix for this code.

$P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad H = (P^T \; I) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

b) (3 points) Is the following vector a codeword for this code? Support your answer with a computation. (In other words, please do not just guess "yes" or "no.")

$$v = (1 \;\; 1 \;\; 1 \;\; 0 \;\; 1)$$

Check if $vH^T = 0$:

$$(1\;1\;1\;0\;1)\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (0\;0)$$

yes it is!

Problem 2 : (3 points) Recall the Hamming [7,4] code from class. It has generating matrix and parity check matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \text{and} \quad H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

respectively. Decode the following received message:

$$v = (1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1)$$

First compute $vH^T = (1100001)\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (0\,1\,0)$

This is the 6th column of H, so v has an error in its 6th bit. The decoded codeword is

$$c = (1100011)$$

Problem 3 : (11 points) The rest of the quiz will all have to do with the binary linear code given by the generating matrix

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

a) (2 points) Please enumerate all of the codewords of this code.

(00) $G = (0\ 0\ 0\ 0\ 0) = C_1$

(10) $G = (1\ 0\ 1\ 0\ 1) = C_2$

(01) $G = (0\ 1\ 0\ 1\ 1) = C_3$

(11) $G = (1\ 1\ 1\ 1\ 0) = C_4$

b) (2 points) What is the minimum distance of this code?

Since this is linear, $d(C) = \min wt \text{ of } 0 \neq C$

$wt(C_2) = 3$

$wt(C_3) = 3$

$wt(C_4) = 4$

$d(C) = 3$

c) (1 point) How many errors can this code correct?

$d(C) \geq 2t+1$

$3 \geq 2t+1$

$2 \geq 2t$

$1 \geq t$

this can correct at most one error

d) (3 points) Alice wants to use this code to receive encrypted messages using the McEliece cryptosystem. Before she begins, she wants to practice decoding a vector. To decode, she will use brute-force, by finding the nearest codeword to a message she receives.

Please use brute-force to decode the following received message. In other words, from your list above, find the codeword nearest (in the Hamming distance) to the received message:

$$v = (1\ 0\ 0\ 0\ 1).$$

$d(c_1, v) = 2$ $d(c_4, v) = 4$ decodes to (1 0 1 0 1)

$d(c_2, v) = 1$

$d(c_3, v) = 3$

e) (3 points) Now that she has practiced, Alice is ready to receive encrypted messages. She sets up her McEliece cryptosystem so that

$$S^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad P^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

(Note that these are already the inverse matrices that she needs for decryption!)

She receives the following encrypted message. Please decrypt it.

$$y = (1\ 1\ 1\ 1\ 0)$$

First do $yP^{-1} = (1\ 1\ 1\ 1\ 0)\begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} = (1\ 0\ 1\ 1\ 1)$

Decode $v = (1\ 0\ 1\ 1\ 1)$ $d(c_1, v) = 4$ $d(c_3, v) = 3$ to (1 0 1 0 1)

$d(c_2, v) = 1$ $d(c_4, v) = 2$

"premessage" is (1 0)

Do $(1\ 0)S^{-1} = (1\ 0)\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (1\ 1)$

Decrypted to (1 1)