

1. TRUE/FALSE? Prove your answer!

- (a) (5 pts) There exists a binary one-error correcting code of length 9 with 52 codewords.  
 (b) (5 pts) There exists a ternary one-error correcting code of length 6 with 10 codewords.

*Solution* : (a) **FALSE**. Let  $C$  be a binary one-error correcting code of length 9. Then it follows from the Sphere packing bound that

$$|C| \leq \frac{m^n}{\sum_{i=0}^t \binom{n}{i} (m-1)^i} = \frac{2^9}{\sum_{i=0}^1 \binom{9}{i} (2-1)^i} = \frac{2^9}{\binom{9}{0} + \binom{9}{1}} = \frac{512}{10} = 51.2$$

So  $|C| \leq 51$ .

Hence there does not exist a binary one-error correcting code of length 9 with 52 codewords.

(b) **TRUE**. By the Gilbert-Varshamov Bound, there exists a ternary one-error correcting code  $C$  of length 6 with

$$|C| \geq \frac{m^n}{\sum_{i=0}^{2t} \binom{n}{i} (m-1)^i} = \frac{3^6}{\sum_{i=0}^2 \binom{6}{i} (3-1)^i} = \frac{729}{\binom{6}{0} + 2\binom{6}{1} + 4\binom{6}{2}} = \frac{729}{73} > 9$$

So  $|C| \geq 10$ .

Hence there exists a ternary one-error correcting code of length 6 with 10 codewords. □

2. Let  $C$  be the binary code with generator matrix  $\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$ .

- (a) (7 pts) Find a generator matrix in standard form for  $C$ .  
 (b) (3 pts) Find a parity check matrix for  $C$ .

*Solution* : (a) We perform elementary row operations on the given generator matrix to find its row echelon form. This will be a generator matrix in standard form.

We begin by swapping  $R_2$  and  $R_3$  :

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Next we replace  $R_1$  by  $R_1 - R_2$  :

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Finally, we replace  $R_1$  by  $R_1 - R_3$  and we replace  $R_2$  by  $R_2 - R_3$  :

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

(b) Once we have a generator matrix in standard form for  $C$ , we can use Proposition 3.7 to find a parity check matrix for  $C$ . We get

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

3. Let  $C$  be the ternary code with parity check matrix  $\begin{bmatrix} 2 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 2 & 1 \end{bmatrix}$ .

- (a) (7 pts) Find the parameters for  $C$  (so  $n$ ,  $k$  and  $d$ ).  
 (b) (3 pts) How many codewords does  $C$  have?

*Solution* : (a) Recall that a parity check matrix for an  $[n, k, d]$ -code is an  $(n - k) \times n$ -matrix. Hence  $n = 5$  and  $k = 3$ . We use Proposition 3.8 to find  $d$ . Note that the given parity check matrix  $H$  has no zero-column. Hence every column of  $H$  is linearly independent. But

$$C_1 + C_4 = \begin{bmatrix} 2 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

So the first and fourth column of  $H$  are linearly dependent. Hence  $d = 2$ .

(b) In general, if  $C$  is a linear code over  $\mathbb{F}$  of dimension  $k$  then  $|C| = |\mathbb{F}^k| = |\mathbb{F}|^k$ . So here we get that

$$|C| = 3^3 = 27 \quad \square$$

4. Let  $C$  be the binary code word generator matrix  $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ .

- (a) (5 pts) Set up a standard array for  $C$ .  
 (b) (2 pts) Write down the coset leaders of each coset.  
 (c) (3 pts) Use your standard array to decode the following words :
- 1111
  - 1110
  - 1010

*Solution* : (a) First, we find all the codewords. Recall that the codewords are all the linear combinations of the rows of the generator matrix. Hence

$$C = \{0000, 1001, 0110, 1111\}$$

This is the first row of the standard array.

Next, we fill the standard array : we find a word  $\mathbf{x}$  that is not in the array yet and add the coset  $\mathbf{x} + C$  as a new row to the standard array. We make sure that a coset leader is in the first column. Let's say we start with  $\mathbf{x} = 1000$ . Then we get

0000 1001 0110 1111  
 1000 0001 1110 0111

We continue with  $\mathbf{x} = 0100$  and find

0000 1001 0110 1111  
 1000 0001 1110 0111  
 0100 1101 0010 1011

Finally, we pick any remaining word, say  $\mathbf{x} = 1100$  and get the following standard array :

0000 1001 0110 1111  
 1000 0001 1110 0111  
 0100 1101 0010 1011  
 1100 0101 1010 0011

It's important to realize that this array is not unique. We could have picked 0001 as choice for a coset leader. Then the second row would have been

0001 1000 0111 1110

(b) Using our standard array, we easily get

Coset	Coset Leaders
{0000, 1001, 0110, 1111}	0000
{1000, 0001, 1110, 0111}	1000, 0001
{0100, 1101, 0010, 1011}	0100, 0010
{1100, 0101, 1010, 0011}	1100, 0101, 1010, 0011

Note that this is independent of the standard array we choose.

(c) Decoding using a standard array is quite simple : we look up the received word in the standard array and decode as the codeword (in the first row) that is in the same column as the received word. This clearly depends on the standard array we choose. We get

We decode 1111 as 1111.  
 We decode 1110 as 0110.  
 We decode 1010 as 0110.

5. Let  $C$  be the binary code with parity check matrix  $\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$ .

- (a) (7 pts) Set up a syndrome table for  $C$ .
- (b) (3 pts) Use your syndrome table to decode the word 11010.

*Solution* : We pick words of small weight (first weight zero, then weight one, then weight two,...) and evaluate their syndrome until we get every single syndrome exactly once. We find

coset leader	syndrome
00000	000
10000	100
01000	110
00100	111
00010	001
00001	101
00101	010
10100	011

Note that the first six rows are unique since these cosets have exactly one coset leader. The last two rows are not unique since those cosets have more than one coset leader. We could have chosen 11000 instead of 00101 in the seventh row.

(b) First, we calculate

$$\text{syn}(11010) = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = 011$$

Next, we look up this syndrome in the syndrome table. We decode by subtracting the coset leader from the received word. So we decode 11010 as

$$11010 - 10100 = 01110$$

Again, this depends on which coset leader we choose for our syndrome table. □

1. (5 pts) Decode the word

010000000000011

using the binary Hamming code  $Ham(2, 4)$ .

*Solution* : Recall that we have a simple decoding algorithm for  $Ham(2, 4)$ .

First, we calculate  $\text{syn}(010000000000011)$ . For  $1 \leq i \leq 15$ , let  $C_i$  be the  $i$ -th column of the special parity check matrix for  $Ham(2, r)$  (so the  $i$ -th column is the binary expansion of the integer  $i$ ). Then we get that (writing syndromes as a four-tuple)

$$\text{syn}(010000000000011) = C_2 + C_{14} + C_{15} = 0010 + 1110 + 1111 = 0011$$

Since this is the binary expansion of three, we decode by changing the third digit in the received word. So we decode 010000000000011 as

011000000000011

□

2. (10 pts) Prove there does not exist a binary two-error correcting code of length 8 with 5 codewords.

*Proof* : Suppose that there exists a binary two-error correcting code  $C$  of length 8 with 5 codewords. Then there are at least three codewords with the same digit in the first position, say  $\mathbf{x}$ ,  $\mathbf{y}$  and  $\mathbf{z}$ .

Since  $C$  is two-error correcting, we know that  $d(C) \geq 5$ . So  $\mathbf{x}$  and  $\mathbf{y}$  (resp.  $\mathbf{x}$  and  $\mathbf{z}$ , resp.  $\mathbf{y}$  and  $\mathbf{z}$ ) are different in at least five positions. Put

$$A = \{2 \leq i \leq 8 : x_i = y_i\}, \quad B = \{2 \leq i \leq 8 : x_i = z_i\} \text{ and } C = \{2 \leq i \leq 8 : y_i = z_i\}$$

Then  $A \cup B \cup C = \{2, 3, 4, 5, 6, 7, 8\}$ . Indeed, let  $2 \leq i \leq 8$ . If  $x_i = y_i$  then  $i \in A$ . If  $x_i \neq y_i$  then  $\{x_i, y_i\} = \{0, 1\}$  since the code is binary and so  $z_i \in \{x_i, y_i\}$  and thus  $i \in B$  or  $i \in C$ . Hence

$$7 = |\{2, 3, 4, 5, 6, 7, 8\}| = |A \cup B \cup C| \leq |A| + |B| + |C|$$

So  $|A| \geq 3$  or  $|B| \geq 3$  or  $|C| \geq 3$ . But then  $d_H(\mathbf{x}, \mathbf{y}) \leq 4$  or  $d_H(\mathbf{x}, \mathbf{z}) \leq 4$  or  $d_H(\mathbf{y}, \mathbf{z}) \leq 4$ , a contradiction.

Hence there does not exist a binary one-error correcting code of length 8 with 5 codewords. □

3. Let  $\mathbb{F}$  be a field and  $n \in \mathbb{N}$ . Use the Triangle Inequality (regarding the Hamming distance) to prove the following :

(a) (5 pts)  $w(\mathbf{a} - \mathbf{b}) \leq w(\mathbf{a}) + w(\mathbf{b})$  for all  $\mathbf{a}, \mathbf{b} \in \mathbb{F}^n$ .

(b) (5 pts)  $w(\mathbf{x} - \mathbf{y}) \geq |w(\mathbf{x}) - w(\mathbf{y})|$  for all  $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ .

*Proof* : Recall that

$$w(\mathbf{x} - \mathbf{y}) = d_H(\mathbf{x}, \mathbf{y}) \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{F}^n$$

In particular, we get that

$$w(\mathbf{x}) = w(\mathbf{x} - \mathbf{0}) = d_H(\mathbf{x}, \mathbf{0}) \quad \text{for all } \mathbf{x} \in \mathbb{F}^n$$

(a) Let  $\mathbf{a}, \mathbf{b} \in \mathbb{F}^n$ . By the Triangle Inequality, we get that

$$d_H(\mathbf{a}, \mathbf{b}) \leq d_H(\mathbf{a}, \mathbf{0}) + d_H(\mathbf{0}, \mathbf{b})$$

Hence

$$w(\mathbf{a} - \mathbf{b}) \leq w(\mathbf{a}) + w(\mathbf{b})$$

(b) Let  $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ . By (a), we get that

$$w(\mathbf{y}) = w(\mathbf{x} - (\mathbf{x} - \mathbf{y})) \leq w(\mathbf{x}) + w(\mathbf{x} - \mathbf{y})$$

Hence

$$w(\mathbf{x} - \mathbf{y}) \geq w(\mathbf{y}) - w(\mathbf{x})$$

Similarly, we find that

$$w(\mathbf{x}) = w(\mathbf{y} - (\mathbf{y} - \mathbf{x})) \leq w(\mathbf{y}) + w(\mathbf{y} - \mathbf{x}) = w(\mathbf{y}) + w(\mathbf{x} - \mathbf{y})$$

and so

$$w(\mathbf{x} - \mathbf{y}) \geq w(\mathbf{x}) - w(\mathbf{y})$$

Since  $|w(\mathbf{x}) - w(\mathbf{y})| \in \{w(\mathbf{x}) - w(\mathbf{y}), w(\mathbf{y}) - w(\mathbf{x})\}$ , we get that  $w(\mathbf{x} - \mathbf{y}) \geq |w(\mathbf{x}) - w(\mathbf{y})|$ . □

---

4. (10 pts) Let  $C$  be a linear  $t$ -error correcting code of length  $n$  over the field  $\mathbb{F}$  and  $\mathbf{x} \in \mathbb{F}^n$  with  $w(\mathbf{x}) \leq t$ . Prove that  $\mathbf{x}$  is the unique coset leader of its coset.

*Proof* : First, we prove the following claim :

If  $\mathbf{y}$  is a coset leader of the coset containing  $\mathbf{x}$  then  $\mathbf{y} = \mathbf{x}$ .

Indeed, let  $\mathbf{y}$  be a coset leader of the coset containing  $\mathbf{x}$ . Then  $w(\mathbf{y}) \leq t$  and  $\mathbf{y} \in \mathbf{x} + C$ . Hence  $\mathbf{y} = \mathbf{x} + \mathbf{c}$  for some  $\mathbf{c} \in C$ . Using Ex#3a, we get that

$$w(\mathbf{c}) = w(\mathbf{y} - \mathbf{x}) \leq w(\mathbf{y}) + w(\mathbf{x}) \leq t + t = 2t < 2t + 1 \leq d(C) = w(C)$$

So  $\mathbf{c} \in C$  and  $w(\mathbf{c}) < w(C)$ . This is only possible if  $\mathbf{c} = \mathbf{0}$ . Thus  $\mathbf{y} = \mathbf{x} + \mathbf{c} = \mathbf{x} + \mathbf{0} = \mathbf{x}$ , which proves the claim.

It follows immediately from this claim that the coset of  $x$  has at most one coset leader (namely  $x$ ). Since every coset has a coset leader, it follows from the claim that  $\mathbf{x}$  is indeed a coset leader of the coset containing  $\mathbf{x}$ . So  $\mathbf{x}$  is the unique coset leader of the coset containing  $\mathbf{x}$ . □

---

5. Let  $C$  be a non-trivial binary  $[n, k, d]$ -code.

(a) (5 pts) Prove that the sum of the weights of all the codewords in  $C$  is at most  $n2^{k-1}$ .

Hint: Hw 3 #3 may be useful.

(b) (5 pts) Prove that  $d \leq \frac{n2^{k-1}}{2^k - 1}$ .

(c) (5 pts) Suppose that  $2d > n$ . Prove that  $|C| \leq \frac{2d}{2d - n}$ .

Proof : (a) Let  $SW(C)$  denote the sum of the weights of all the codewords. So

$$SW(C) = \sum_{\mathbf{x} \in C} w(\mathbf{x})$$

We write all the codewords in a matrix, each row being a codeword. Then  $SW(C)$  is the number of ones in this matrix. Since  $C$  is a binary  $[n, k, d]$ -code, we end up with a  $2^k \times n$ -matrix. We add up all the ones in the first column, then all the ones in the second column, etc. Finally, we add up all these sums.

Let  $1 \leq i \leq n$ . It follows from HW 3 #3 that at most half of the codewords have a one in the  $i$ -th position. Hence the number of ones in the  $i$ -th column of the matrix is at most half of  $|C|$ , which is  $2^{k-1}$ . Since there are  $n$  columns in the matrix, we get that

$$SW(C) \leq n \cdot 2^{k-1}$$

(b) Recall that the minimum distance of a linear code equals its minimum weight. By definition of minimum weight, we have that  $w(\mathbf{x}) \geq w(C)$  for all  $\mathbf{x} \in C$  with  $\mathbf{x} \neq \mathbf{0}$ . Since  $|C| = 2^k$ , we get

$$SW(C) = \sum_{\mathbf{x} \in C} w(\mathbf{x}) = \sum_{\mathbf{0} \neq \mathbf{x} \in C} w(\mathbf{x}) \geq \sum_{\mathbf{0} \neq \mathbf{x} \in C} w(C) = (|C| - 1)w(C) = (2^k - 1)d$$

Combining this with (a), we get

$$(2^k - 1)d \leq SW(C) \leq n \cdot 2^{k-1}$$

Hence

$$d \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$$

(c) Recall that  $C$  is a binary  $[n, k, d]$ -code and so  $|C| = 2^k$ . From (b), it follows that

$$2d \leq 2 \frac{n \cdot 2^{k-1}}{2^k - 1} = \frac{n \cdot 2^k}{2^k - 1} = \frac{n|C|}{|C| - 1}$$

Hence

$$2d(|C| - 1) \leq n|C|$$

and so

$$(2d - n)|C| \leq 2d$$

Since  $2d - n > 0$ , we get that

$$|C| \leq \frac{2d}{2d - n}$$

□