

**Homework 5**  
**Algebraic Coding Theory**  
**Math 525**  
**Stephen Giang RedID: 823184070**

**Problem 1:**

- (a) **Exercise 3.1.5:** Find an upper bound for the size or dimension of a linear code with the given values of  $n$  and  $d$ .

Let  $n = 8$  and  $d = 3$ . Notice the following:  $t = \lfloor \frac{d-1}{2} \rfloor$ , such that  $t = 1$ . So we get:

$$|C| \leq \frac{2^n}{\sum_{i=0}^t \binom{n}{i}} = \frac{2^8}{\binom{8}{0} + \binom{8}{1}} = \frac{2^8}{1+8} = 28.44$$

Because  $|C|$  has to be a power of 2, we get  $|C| = 16$ , so  $k = 4$ .

- (b) **Exercise 3.1.6:** Verify the Hamming bound for the linear code C with the given generator matrix.

$$G = \begin{bmatrix} 11111000000000 \\ 000001111100000 \\ 000001111111111 \end{bmatrix}$$

Notice this is a  $(n = 15, k = 3, d = 5)$  code. Because  $k = 3$ , we have that:

$$|C| = 8 \leq \frac{2^{15}}{\binom{15}{0} + \binom{15}{1} + \binom{15}{2}} = \frac{32768}{1 + 15 + 105} = \frac{32768}{121} = 270.8$$

**Problem 2:**

- (a) **Exercise 3.1.10:** Columns 2, 3, and 5 of the generator matrix

$$G = \begin{bmatrix} 11001 \\ 01110 \\ 00101 \end{bmatrix}$$

are linearly dependent. Find a codeword which has zeros in positions 2, 3, and 5.

Notice that based off this, we have codewords of length 5. But we get the information vector of size 3. So notice we have an information vector,  $u(a, b, c)$  such that we get the following:

$$uG = (a, a + b, b + c, b, a + c)$$

So we get that  $a + b = 0$ ,  $b + c = 0$ , and  $a + c = 0$ . We also have that  $a = 1$  and  $b = 1$ . Thus we get that  $c = 1$ . Thus we get the information vector  $u(1, 1, 1)$  with a codeword  $uG$

- (b) **Exercise 3.1.11:** Show that if a  $k \times n$  generator matrix has  $k$  linearly dependent columns then there is a nonzero codeword with zeros in those  $k$  positions.

Without loss of generality, we can take the generator matrix,  $G$ , and say that its linearly dependent columns are the first  $k$  columns. We can now see that the submatrix,  $A$ , formed from the first  $k$  columns is a singular matrix. Thus there exists a nonzero vector  $u = (u_1, u_2, \dots, u_k)$  such that  $uA = 0$ . Thus we get the following:

$$uG = u[A|X] = [uA|uX] = [0|w]$$

where  $w = (w_1, w_2, \dots, w_{n-k}) \neq 0$

**Problem 3:** Use the Hamming bound to determine the maximum dimension  $k$  a linear code of length  $n$  and distance  $d$  can have when:

(a)  $n = 8, d = 3$ .

$$|C| \leq \frac{2^8}{\binom{8}{0} + \binom{8}{1}} = \frac{256}{9} = 28.444$$

Thus we have that  $|C| \leq 16$  with  $k \leq 4$

(b)  $n = 7, d = 3$ .

$$|C| \leq \frac{2^7}{\binom{7}{0} + \binom{7}{1}} = \frac{128}{8} = 16$$

Thus we have that  $|C| \leq 16$  with  $k \leq 4$

**Problem 4:**

- (a) Determine the largest  $M$  for which you can guarantee the existence of a linear code of size  $M$ , length  $n = 10$ , and distance  $d = 5$ .

$$|C| \geq \frac{2^{n-1}}{\sum_{i=0}^{d-2} \binom{n-1}{i}} = \frac{2^9}{\binom{9}{0} + \binom{9}{1} + \binom{9}{2} + \binom{9}{3}} = 3.9384$$

Because  $|C|$  has to be a power of 2, we get  $|C| \geq 4$ , thus  $M = 4$

- (b) Find an upper bound for the size of a linear code with length  $n = 10$  and distance  $d = 5$ .

$$|C| \leq \frac{2^{10}}{\binom{10}{0} + \binom{10}{1} + \binom{10}{2}} = 18.2857$$

Thus we get  $|C| \leq 16$ , with  $k = 4$ .

- (c) Is there a perfect code with  $n = 10$  and  $d = 5$ ?

Because  $|C| = \frac{2^{10}}{\binom{10}{0} + \binom{10}{1} + \binom{10}{2}} = 18.25$ , and there doesn't exist a code with 18.25 codewords, so there does not exist a perfect code.

**Problem 5:** Use the Gilbert-Varshamov bound to determine the smallest  $n$  for which there exists a code of length  $n$  and rate  $1/3$  that can correct 2 errors.

Notice, because  $C$  is a 2 error correcting code, then  $d = 5$ . Also because the rate is  $1/3$ , we get can say the following code has a rate of  $k/n = k/3k = 1/3$ . Now we use the GV bound on a code  $(3k, k, 5)$ .

$$2^{2k} > \binom{3k-1}{0} + \binom{3k-1}{1} + \binom{3k-1}{2} + \binom{3k-1}{3}$$

Through plug and chug, we get that  $k = 4$  is the smallest integer for this inequality to be true. Thus the smallest  $n$  is  $n = 12$ .

**Problem 6:**

- (a) **Exercise 3.1.18:** For each part of Exercise 3.1.5, let  $k = 2d$  and decide, if possible, whether or not a linear code with the given parameters exists. Find a lower and upper bound for the maximum number of codewords such a code can have, assuming that  $k$  is unrestricted.

Let  $n = 8$ ,  $d = 3$ ,  $k = 6$ .

$$|C| \leq \frac{2^8}{\binom{8}{0} + \binom{8}{1}} = \frac{2^8}{1 + 8} = 28.44$$

So we get an upper bound of  $|C| \leq 16$ . We find upper bound from the hamming bound.

$$|C| \geq \frac{2^7}{\binom{7}{0} + \binom{7}{1}} = 16$$

So we get a lower bound of  $|C| \geq 16$ . We find the lower bound from the GV bound. So we have  $16 \leq |C| \leq 16$ , such that  $|C| = 16$  with  $k = 4$ . So there doesn't exist a code with  $k = 6$ .

- (b) **Exercise 3.1.20:** Is it possible to have a linear code with parameters  $(8, 3, 5)$ ? Notice the following bounds of the given code:

$$\begin{aligned} |C| &\leq \frac{2^8}{\binom{8}{0} + \binom{8}{1} + \binom{8}{2}} = \frac{256}{37} = 6.9189 \\ &\geq \frac{2^7}{\binom{7}{0} + \binom{7}{1} + \binom{7}{2} + \binom{7}{3}} = 2 \end{aligned}$$

This means we get  $2 \leq |C| \leq 4$ , which means  $k = 1$  or  $k = 2$ . Thus we can not have a linear code with  $k = 3$ .

**Problem 7:** Consider an  $(n, k)$  linear code  $C$  whose generator matrix  $G$  contains no zero column. Arrange all the codewords of  $C$  as rows of a  $2^k$  by  $n$  array.

(a) Show that each column of the array consists of  $2^{k-1}$  zeroes and  $2^{k-1}$  ones.

(b) Conclude that

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

**Problem 8:**

- (a) **Exercise 3.2.5:** Show that for  $n = 2^r - 1$ ,  $\binom{n}{0} + \binom{n}{1} = 2^r$

$$\binom{n}{0} + \binom{n}{1} = 1 + n = 1 + 2^r - 1 = 2^r$$

- (b) Can there exist perfect codes for the following values of  $n$  and  $d$ ?

$$n = 15, d = 3$$

$$C = \frac{2^{15}}{\binom{15}{0} + \binom{15}{1}} = 2048$$

Notice we can have a perfect code  $|C| = 2048$ , such that  $k = 11$