MA210 Discrete Mathematics

Notes and Exercises 5

March 13 and 20, 2023

Coding Theory

Introduction

Coding theory is not the area of mathematics dealing with the theory of secret codes for CIA, MI5, etc. That subject area is called *cryptography*.

Coding theory deals with the mathematical theory behind the designs of codes for storing and transmitting information in such a way that there is a built-in capacity to recognise and perhaps even correct errors.

Instead of the usual 26 letters of the alphabet, in most of these notes we shall work with two symbols only: "0" and "1". These are, not by accident, also the symbols with which computers work and in which most digital communication is performed.

We almost always assume that our code consists of a number of sequences of length n, for some natural number n. The set of all possible $0, 1$-sequences of length n will be denoted by $\{0,1\}^n$. Each symbol in such a sequence is called a *bit*. An element of $\{0,1\}^n$ (a $0, 1$-sequence of length n) is called a *word*. We usually denote words by bold letters: $\mathbf{x}$, $\mathbf{y}$, etc. (On the board I will write $\underset{\sim}{x}$ rather than $\mathbf{x}$, because I'm not too good at writing boldface.)

Definition 5.1 (binary code, codeword)**.** *A* binary code C *(of* length n*) is a subset of* $\{0,1\}^n$*. An element of* C *is called a* codeword*.*

Distance in codes

Definition 5.2 (Hamming distance, weight of a codeword)**.** *Let* $\mathbf{x}, \mathbf{y}$ *be two words in* $\{0,1\}^n$*. Then the* Hamming distance $d_H(\mathbf{x}, \mathbf{y})$ *of* $\mathbf{x}$ *and* $\mathbf{y}$ *is defined as the number of bits in which* $\mathbf{x}$ *and* $\mathbf{y}$ *are different. Hence, for* $\mathbf{x} = x_1x_2\ldots x_n$*,* $\mathbf{y} = y_1y_2\ldots y_n$*,*

$$d_H(\mathbf{x}, \mathbf{y}) \;=\; |\{\, i : \, x_i \neq y_i, \;\; i = 1, 2, \ldots, n \,\}|.$$

The weight $w(\mathbf{x})$ *of a word* $\mathbf{x}$ *is the number of 1's in the word. Another way to define the weight is by* $w(\mathbf{x}) = d_H(\mathbf{x}, \mathbf{0})$*, where* $\mathbf{0}$ *indicates the word* $00\ldots0$*.*

Theorem 5.3. *The Hamming distance has the following properties. For all* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \{0,1\}^n$ *we have:*

(a) $d_H(\mathbf{x}, \mathbf{y}) = 0$ *if and only if* $\mathbf{x} = \mathbf{y}$*;*

(b) $d_H(\mathbf{x}, \mathbf{y}) = d_H(\mathbf{y}, \mathbf{x})$*;*

(c) $d_H(\mathbf{x}, \mathbf{z}) + d_H(\mathbf{z}, \mathbf{y}) \geq d_H(\mathbf{x}, \mathbf{y})$.

The following property follows immediately from the definition of the Hamming distance.

Proposition 5.4. *Let* $\mathbf{x}$ *be a word in* $\{0,1\}^n$*, and suppose* $\mathbf{y}$ *is a word obtained from* $\mathbf{x}$ *by introducing* d *errors in* $\mathbf{x}$*. Then* $d_H(\mathbf{x}, \mathbf{y}) = d$*.*

Definition 5.5 (minimum distance)**.** *Let* $C \subseteq \{0,1\}^n$ *be a code of length* n*, and* $|C| \geq 2$*. Then the* minimum distance of C *is*

$$\delta(C) \;=\; \min\{\, d_H(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y} \,\}.$$

Error-detecting and error-correction

Let C be a code of length n. Suppose that a codeword $\mathbf{x} \in C$ is transmitted, but some of its bits get changed during the transmission. Hence a word $\mathbf{c}$ of length n is received, with $\mathbf{x} \neq \mathbf{c}$. Then the receiver will only recognise that an error occurred if $\mathbf{c} \notin C$.

Definition 5.6 (d-error-detecting)**.** *A code* C *is* d*-error-detecting if for any codeword* $\mathbf{x} \in C$ *and any word* $\mathbf{c} \in \{0,1\}^n$ *with* $\mathbf{x} \neq \mathbf{c}$ *such that* $d_H(\mathbf{x}, \mathbf{c}) \leq d$ *we have* $\mathbf{c} \notin C$*.*

Theorem 5.7. *A code* C *with* $|C| \geq 2$ *is* d*-error-detecting if and only if* $\delta(C) \geq d + 1$*.*

Definition 5.8 (nearest neighbour, nearest-neighbour decoding)**.** *Given a code* $C \subseteq \{0,1\}^n$*, and a word* $\mathbf{c} \in \{0,1\}^n$*, suppose that for some* $\mathbf{x} \in C$ *we have* $d_H(\mathbf{x}, \mathbf{c}) = d$ *and for each* $\mathbf{y} \in C$ *with* $\mathbf{y} \neq \mathbf{x}$ *we have* $d_H(\mathbf{y}, \mathbf{c}) > d$*. Then we say that* $\mathbf{x}$ *is the* nearest neighbour *of* $\mathbf{c}$ *in* C*.*

By nearest-neighbour decoding *we mean that if* $\mathbf{c}$ *is received and* $\mathbf{x}$ *is the nearest neighbour of* $\mathbf{c}$*, then we assume* $\mathbf{x}$ *is the word which was transmitted.*

It is important to be aware that given C and $\mathbf{c}$ there is not necessarily a nearest neighbour of $\mathbf{c}$ in C.

Definition 5.9 (d-error-correcting)**.** *A code* C *is* d-error-correcting *if for every codeword* $\mathbf{x} \in C$ *and every* $\mathbf{c}$ *such that* $d_H(\mathbf{x}, \mathbf{c}) \leq d$ *the nearest neighbour of* $\mathbf{c}$ *exists and is* $\mathbf{x}$*.*

Theorem 5.10. *A code* C *with* $|C| \geq 2$ *is* d*-error-correcting if and only if* $\delta(C) \geq 2d + 1$*.*

Example 5.11. The code $C = \{000000, 111000, 000111, 111111\}$ is 1-error-correcting.

Some examples of elementary binary codes

Example 5.12. Let C_e be the set of all sequences in $\{0,1\}^n$ with even weight. This code is 1-error-detecting.

Definition 5.13 (parity check code)**.** *Given $n \geq 2$, the* parity check code C_e *with codewords of length n is obtained as follows. We start with all words $\{0,1\}^{n-1}$. To each word $\mathbf{x} \in \{0,1\}^{n-1}$ we add one extra bit, which is 1 if $\mathbf{x}$ has odd weight and 0 if $\mathbf{x}$ has even weight. This gives us the parity check code C_e with words of length n.*

The extra bit we added is sometimes called the *parity check bit.*

Example 5.14. The parity check code with words of length 4 is

$$\{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}.$$

Definition 5.15 (d-repetition code)**.** *Let k and d be positive integers, and set $n = k \cdot d$. Then the* d-repetition code of length n *is obtained as follows: For every $\mathbf{y} \in \{0,1\}^k$, form $\mathbf{c}$ by repeating each bit of $\mathbf{y}$ d times. Thus, if $\mathbf{y} = y_1 y_2 \dots y_k$ we have $\mathbf{c} = \underbrace{y_1 \dots y_1}_{d} \underbrace{y_2 \dots y_2}_{d} \cdots \underbrace{y_k \dots y_k}_{d}$.*

Example 5.16. The minimum distance of the d-repetition code of length n is d.

Introduction to linear codes

From now on we no longer consider $\{0,1\}$ as just a set with two elements, but as a set with additional algebraic structure. We define addition in $\{0,1\}$ modulo 2:

$$0+0 \;=\; 0, \quad 1+0 \;=\; 1, \quad 0+1 \;=\; 1, \quad 1+1 \;=\; 0.$$

For two words $\mathbf{x} = x_1 x_2 \dots x_n \in \{0,1\}^n$ and $\mathbf{y} = y_1 y_2 \dots y_n \in \{0,1\}^n$, we define the sum $\mathbf{z} = \mathbf{x} + \mathbf{y}$ as $\mathbf{z} = z_1 z_2 \dots z_n$, where $z_i = x_i + y_i$ for $i = 1, 2, \dots, n$.

With the addition defined above, the set $\{0,1\}^n$ becomes an Abelian group with identity $\mathbf{0} = \underbrace{00\dots0}_{n}$ in which every element is its own inverse.

You can also view $\{0,1\}^n$ as a vector space over the field $\mathbb{F}_2$ (the integers modulo 2, which you saw in MA103 is a field; sometimes this is written $\mathbb{Z}_2$). This is a slightly stronger statement: remember from MA103 that every vector space is an Abelian group (under vector addition) where in addition we have an operation 'scalar multiplication' under which the vector space is closed. Here, though, the 'scalars' available are 0 and 1; multiplying by either is boring (we get respectively the zero vector and the same thing back again).

What is however worth remembering is that more or less all the linear algebra you learned in MA100 applies to vector spaces over $\mathbb{F}_2$.

Definition 5.17 (linear code)**.** *A code $C \subseteq \{0,1\}^n$ is called a* linear binary code*, or simply a* linear code*, if for all $\mathbf{x}, \mathbf{y} \in C$ we have $\mathbf{x} + \mathbf{y} \in C$.*

Proposition 5.18. *If C is a linear code with at least one codeword, then $\mathbf{0} \in C$.*

Example 5.19. If C is a linear code in $\{0,1\}^n$ then $|C| = 2^k$ for some integer $k \leq n$.

Definition 5.20 (dimension of a linear code)**.** *Let C be a linear code in $\{0,1\}^n$. If $|C| = 2^k$, then we say k is the* dimension of C*.*

Theorem 5.21. *Let C be a linear code with $|C| \geq 2$. Then the minimum distance of C is the minimum weight of a non-zero codeword in C. In other words:*

$$\delta(C) \;=\; \min\{\, w(\mathbf{x}) \mid \mathbf{x} \in C,\ \mathbf{x} \neq \mathbf{0} \,\}.$$

Construction of linear codes

Let H be a binary matrix (i.e. all entries of H are 0 or 1) with n columns. For a word $\mathbf{x} \in \{0,1\}^n$, we write $\mathbf{x}^T$ for the word $\mathbf{x}$ considered as a *column vector*. Then $H\mathbf{x}^T$ is a column vector with r entries.

Theorem 5.22. *Let H be a binary matrix with n columns. Then the set*

$$C = \{\, \mathbf{x} \in \{0,1\}^n \mid H\mathbf{x}^T = \mathbf{0}^T \,\}$$

is a linear code.

It is important to note here that we are doing addition as defined above, i.e. addition modulo 2.

Definition 5.23 (parity-check matrix)**.** *Given a binary matrix H and a code $C \subseteq \{0,1\}^n$, if we have*

$$C = \{\, \mathbf{x} \in \{0,1\}^n \mid H\mathbf{x}^T = \mathbf{0}^T \,\}$$

then we say H is a parity-check matrix*, or simply* check matrix*, of C.*

Example 5.24. If H is a binary matrix with n columns and $r < n$ rows, then H is a check matrix of a code C with $|C| \geq 2$.

In what follows, we will always assume that our codes have at least two words (A one-word code is not very useful!). And usually we will guarantee this by giving a check matrix with less rows than columns, as in Example 5.24.

Example 5.25. What is the code C with check matrix

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

Example 5.26. Given $r \leq n$, what is the code C with check matrix

$$H = \begin{bmatrix} 1 & 0 & \cdots & 0 & b_{11} & b_{12} & \cdots & b_{1n-r} \\ 0 & 1 & \cdots & 0 & b_{21} & b_{22} & \cdots & b_{2n-r} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & b_{r1} & b_{r2} & \cdots & b_{rn-r} \end{bmatrix},$$

where $b_{11}, \ldots, b_{rn-r} \in \{0,1\}$? What is its dimension?

Correcting errors in linear codes

Theorem 5.27. *Let H be a binary matrix in which no column consists entirely of zeros, and in which no two columns are the same. Suppose the code C whose check matrix is H has at least two codewords. Then C is 1-error-correcting.*

Suppose that C is a code with minimum distance at least 3. Hence we know we must be able to correct it if at most one error occurs. So suppose that a codeword $\mathbf{x} \in C$ is transmitted and a word $\mathbf{y}$ with at most one error is received. How can we determine whether $\mathbf{y}$ is a correct word or, if not, what the error is?

Remember that the receiver only knows $\mathbf{y}$. So, in order to check whether $\mathbf{y}$ is a codeword, the receiver can compare $\mathbf{y}$ with all the codewords in C. If there is no match, then the receiver should check again and find a codeword that differs from $\mathbf{y}$ in exactly one bit.

Now, this can be a rather tedious process, especially when the code is large. However, for linear codes we can do much better. Let C be a linear code determined by some check matrix H with minimum distance at least 3. Suppose that a codeword $\mathbf{x} \in C$ is sent, and an error occurs in the i-th bit. Hence, the word $\mathbf{y}$ that is received satisfies

$$\mathbf{y} \;=\; \mathbf{x} + \mathbf{e}_i,$$

where $\mathbf{e}_i$ is the word with all bits equal to 0, except the i-th bit, which is 1. Then we can calculate

$$H\mathbf{y}^T \;=\; H(\mathbf{x} + \mathbf{e}_i) \;=\; H\mathbf{x}^T + H\mathbf{e}_i^T.$$

Since $\mathbf{x}$ is a codeword, we have $H\mathbf{x} = \mathbf{0}'$. And so we find

$$H\mathbf{y}^T \;=\; H\mathbf{e}_i^T.$$

Now $H\mathbf{e}_i^T$ is equal to the i-th column of H.

So, we have the following procedure to detect and correct single errors in a linear code C which has a check matrix H in which no column is equal to $\mathbf{0}^T$ and in which no two columns are identical.

(1) Upon receiving the word $\mathbf{y}$, compute $H\mathbf{y}^T$.

(2) If $H\mathbf{y}^T = \mathbf{0}^T$, then $\mathbf{y}$ is a codeword, and we assume that $\mathbf{y}$ was sent.

(3) If $H\mathbf{y}^T \neq \mathbf{0}^T$ and the i-th column of H is equal to $H\mathbf{y}^T$, then we assume that the i-bit of $\mathbf{y}$ is wrong. Correct that i-th bit to obtain what we assume was the sent codeword.

(4) If $H\mathbf{y}^T \neq \mathbf{0}^T$ and no column of H is equal to $H\mathbf{y}^T$, then we don't know what was sent.

Hamming codes

Let r be a positive integer. Let H_r be a matrix with r rows and with the maximum number of columns such that no column is equal to $\mathbf{0}^T$ and no two columns are identical. In other words, the columns of H_r are simply the $2^r - 1$ different column vectors in which all entries are 0 or 1, excluding the all-zero vector. Let C_r be the code determined by this matrix. So C_r has length $2^r - 1$.

By rearranging columns, we can always assume that H_r has the form

$$H_r \;=\; \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 & b_{1\,1} & b_{1\,2} & \cdots & b_{1\,n-r} \\ 0 & 1 & 0 & \cdots & 0 & b_{2\,1} & b_{2\,2} & \cdots & b_{2\,n-r} \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \vdots & \vdots & & \vdots \\ 0 & \cdots & \cdots & 0 & 1 & b_{r\,1} & b_{r\,2} & \cdots & b_{r\,n-r} \end{bmatrix}.$$

As in Example 5.26, this means that C_r has dimension $2^r - r - 1$.

Finally, from Theorem 5.27 we see that $\delta(C_r) \geq 3$. It is not difficult to find a codeword $\mathbf{x} \in C_r$ with $w(\mathbf{x}) = 3$; for example, we can set the first two coordinates to be 1, then look in H for the column $(1, 1, 0, \ldots, 0)^T$ and set that entry 1 as well. This means $\delta(C_r) = 3$.

Combining everything we get the following result.

Theorem 5.28. *Let r be a positive integer, H_r a matrix with r rows and with the maximum number of columns such that no column consists of 0's only and no two columns are the same, and C_r the code with H_r as check matrix. Then the code C_r is a linear code of length $n = 2^r - 1$, dimension $k = 2^r - r - 1$, and with minimum weight $\delta(C_r) = 3$.*

The codes constructed as above are known as *Hamming codes*.

Example 5.29. What is the length of codewords in the Hamming code C_3? And how many codewords are there?

Exercises

1. Prove Theorem 5.3.

2. Find the minimum distance for the following codes:

(a) $C_1 = \{10000, 01010, 00001\}$;

(b) $C_2 = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$;

(c) $C_3 = \{000000, 101010, 010101\}$.

Suppose we want to add extra codewords to the codes above. For which of C_1, C_2, C_3 is that possible without altering the minimum distance?

3. You are asked to design a binary code for a certain application. For technical reasons, the code must satisfy the following conditions:

(i) at most three consecutive 1s are allowed in every codeword;

(ii) every 0 must be preceded or followed by another 0. (In other words, no codeword should start like $01\ldots$, end like $\ldots 10$, or look like $\ldots 101\ldots$.)

(a) Give all possible codewords of length 5.

You must design a code of length 125. So let C be the code formed by taking all words of length 125 that satisfy the two conditions above.

(b) Show that for every codeword $\mathbf{x} \in C$, the weight $w(\mathbf{x})$ of $\mathbf{x}$ satisfies $w(\mathbf{x}) \leq 75$.

(c) What is the minimum distance of the code C?

(d) How many errors can C detect? And how many errors can C correct?

4. Construct a binary code C of length 6 such that $|C| = 5$ and C is 1-error-correcting.

5. (a) Let C be a code of length n. Suppose that C is 1-error-correcting. Prove that $|C| \leq \dfrac{2^n}{n+1}$.

(b) Show there is no 1-error-correcting code of length 5 with $|C| = 6$.

6. Let C be any binary code of length n.

(a) Define the code C' as follows: pick a certain index j, $1 \leq j \leq n$, and for each codeword $\mathbf{x} \in C$, if the j-th bit of $\mathbf{x}$ is 0, then replace it by 1; while if the j-th bit of $\mathbf{x}$ is 1, then replace it by 0.

Prove that $|C'| = |C|$ and $\delta(C') = \delta(C)$.

(b) Prove that there exists a code C^* of length n that has the same number of codewords and the same minimum distance as C, but with $\mathbf{0} \in C^*$.

7. (a) Determine which of the following ISBN's are correct book codes:

0854397383, 2-85120-460-2, 179469506, 085245710X.

(b) Somebody writes down an ISBN, but you can't decipher the 6th digit. So all you can read is that the ISBN is 01383*0943. Determine the missing digit where the star is.

8. Let C be the linear code of length n with check matrix

$$H = [\underbrace{1\ 1\ 1 \ldots\ 1}_{n}].$$

Show that C is a parity check code.

9. Let C be the d-repetition code of length n. Show that C is a linear code.

10. Determine, justifying your answer, which of the following codes are linear binary codes:

(a) The code C_1 consisting of all 0,1-words of length n with an even number of 1's.

(b) The code C_2 consisting of all 0,1-words of length n with an odd number of 1's.

(c) The code C_3 consisting of all 0,1-words of length n such that the number of 1's in the word is divisible by 3.

11. Suppose that H is the parity check matrix of a code C. Let H' be the matrix obtained from H by rearranging the columns of H in a certain way. Let C' be the code belonging to H' as a parity check matrix.

(a) Give an example of a matrix H and an arrangement H' such that C and C' are not the same.

(b) Explain the relation between the words in C and in C'.

(c) Prove that $|C| = |C'|$ and $\delta(C) = \delta(C')$.

12. Let C be the linear code with check matrix

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

(a) Explain why C is 1-error-correcting.

(b) If the word 110110 is received, and at most one error has been made, what was the intended codeword?

13. Let C_H be the linear code with check matrix

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

(a) Determine the length n of C_H, the dimension k of C_H, and the minimum distance d of C_H.

(b) You receive the following words:

$$11111, \quad 01101, \quad 01100.$$

Decide which of the above are codewords, and correct those which are not codewords, assuming that only one error has been made.

14. Find a parity check matrix H such that the linear code C_H defined by H is 1-error-correcting, has length 6 and is able to send 8 different messages.

15. Let C be the binary code of length 5 with check matrix

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

(a) Give two codewords $\mathbf{x}, \mathbf{y} \in C$ such that $d_H(\mathbf{x}, \mathbf{y}) = 2$.

(b) Prove that in fact $\delta(C) = 2$.

(c) Explain carefully why the result in (b) means that you cannot always correct a single error when using the code C.

When using the code C, the word $\mathbf{x} = 00100$ is received.

(d) Show that $\mathbf{x} \notin C$ and find the words in C that are nearest to $\mathbf{x}$.

16. Let C be a binary code of length n. Define the code C^2 of length $2n$ by

$$C^2 = \{ (\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in C \}.$$

Hence codewords in C^2 are formed by putting two codewords from C behind another.

(a) If C contains $|C|$ words, then how many words does C^2 have?

(b) Decide if the following is true or false: "The minimum distance of C^2 is twice the minimum distance of C." Justify your answer!

(c) Suppose C is a linear code with check matrix H. What is the check matrix of C^2?

17. Suppose that D_1 and D_2 are two linear codes of length n.

(a) Prove that $D_1 \cap D_2$ is a linear code.

(b) Suppose D_1 has check matrix H_1 and D_2 has check matrix H_2. What is the check matrix of $D_1 \cap D_2$?

(c) Is $D_1 \cup D_2$ a linear code in general? Justify your answer.

18. (a) Let $\mathbf{x}$ be a word in $\{0,1\}^n$. Prove that the number of words in $\{0,1\}^n$ that have distance exactly i to $\mathbf{x}$ is equal to $\binom{n}{i}$.

(b) Let $\mathbf{x}$ be a word in $\{0,1\}^n$ and let r be an integer. Define

$$B_r(\mathbf{x}) \;=\; \{\, \mathbf{y} \in \{0,1\}^n \mid d_H(\mathbf{x},\mathbf{y}) \leq r \,\}.$$

Show that $|B_r(\mathbf{x})| = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}$.

(c) Let C be a code of length n. Suppose that C is r-error-correcting. Prove that the number of codewords in C satisfies

$$|C| \;\leq\; \frac{2^n}{1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{r}}.$$

19. All codes in this question are binary. The *sum* of two codes C_1 and C_2 of equal length is

$$C_1 + C_2 \;=\; \big\{\mathbf{x}_1 + \mathbf{x}_2 \mid \mathbf{x}_1 \in C_1,\ \mathbf{x}_2 \in C_2\big\}.$$

(a) Show that for any two codes C_1, C_2 we have: $\delta(C_1 + C_2) \leq \min\{\, \delta(C_1),\, \delta(C_2) \,\}$.

Give an example of a pair C_1, C_2 showing that it is possible to have strict inequality.

(b) Show that for any code C with m elements we have $|C + C| \leq 1 + \binom{m}{2}$.

For every integer $m \geq 1$, give an example of a code C showing that it is possible to have equality.

(c) Prove that $C = C + C$ if and only if C is a linear code.

20. Suppose that instead of just the symbols 0 and 1, we allow each digit of a codeword to be a symbol from $0, 1, \ldots, q-1$. Hence there are q symbols. So now we can see a word of length n as an element of $\{0,1,\ldots,q-1\}^n$. And a code of length n as a subset of $\{0,1,\ldots,q-1\}^n$.

(a) How many words are possible in this case?

(b) Suppose a code C is defined as all words in $\{0,1,\ldots,q-1\}^n$ that are non-zero in exactly k places. How many codewords does C contain?

The Hamming distance for two codewords $\mathbf{x}, \mathbf{y} \in \{0,1,\ldots,q-1\}^n$ is defined similarly as the Hamming distance for binary codes. Hence

$$d_H(\mathbf{x},\mathbf{y}) \;=\; |\{\, i \mid x_i \neq y_i \,\}|.$$

(c) Prove the triangle inequality for the Hamming distance in $\{0, 1, \ldots, q-1\}^n$. So prove that for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \{0, 1, \ldots, q-1\}^n$ we have

$$d_H(\mathbf{x}, \mathbf{z}) + d_H(\mathbf{z}, \mathbf{y}) \ \geq \ d_H(\mathbf{x}, \mathbf{y}).$$

(d) What is the minimum distance of the code defined in (b) ?

(e) Let $\mathbf{x}$ be a word in $\{0, 1, \ldots, q-1\}^n$. Show that the number of words in $\{0, 1, \ldots, q-1\}^n$ that have Hamming distance exactly i to $\mathbf{x}$ is equal to $\binom{n}{i} \cdot (q-1)^i$.

Additional Reading and Exercises from the Text Books

From *Biggs,* ***Discrete Mathematics***
– **Reading**: Sections 24.1 – 24.4.
– **Exercises**: Section 24.1: 1 – 4; Section 24.2: 1, 2, 4; Section 24.3: 1 – 4;
Section 24.4: 1 – 3; Section 24.7: 1 – 9.

From *Cameron,* ***Combinatorics***
– **Reading**: Sections 17.1, 17.2, and selected parts of 17.3, 17.4 and 17.5.