

# DISCRETE MATHEMATICS

W W L CHEN

© W W L Chen, 1991, 2003.

This chapter is available free to all individuals, on the understanding that it is not to be used for financial gains, and may be downloaded and/or photocopied, with or without permission from the author.

However, this document may not be kept on any information storage and retrieval system without permission from the author, unless such system is not accessible to any individuals other than its owners.

## Chapter 11

### GROUP CODES

#### 11.1. Introduction

In this section, we investigate how elementary group theory enables us to study coding theory more easily. Throughout this section, we assume that  $m, n \in \mathbb{N}$  with  $n > m$ .

**DEFINITION.** Suppose that  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is an encoding function. Then we say that  $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$  is a group code if  $\mathcal{C}$  forms a group under coordinate-wise addition modulo 2 in  $\mathbb{Z}_2^n$ .

We denote by  $0$  the identity element of the group  $\mathbb{Z}_2^n$ . Clearly  $0$  is the string of  $n$  0's in  $\mathbb{Z}_2^n$ .

**PROPOSITION 11A.** Suppose that  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is an encoding function, and that  $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$  is a group code. Then

$$\min\{\delta(x, y) : x, y \in \mathcal{C} \text{ and } x \neq y\} = \min\{\omega(x) : x \in \mathcal{C} \text{ and } x \neq 0\};$$

*in other words, the minimum distance between strings in  $\mathcal{C}$  is equal to the minimum weight of non-zero strings in  $\mathcal{C}$ .*

**PROOF.** Suppose that  $a, b, c \in \mathcal{C}$  satisfy

$$\delta(a, b) = \min\{\delta(x, y) : x, y \in \mathcal{C} \text{ and } x \neq y\} \quad \text{and} \quad \omega(c) = \min\{\omega(x) : x \in \mathcal{C} \text{ and } x \neq 0\}.$$

We shall prove that  $\delta(a, b) = \omega(c)$  by showing that (a)  $\delta(a, b) \leq \omega(c)$ ; and (b)  $\delta(a, b) \geq \omega(c)$ .

(a) Since  $\mathcal{C}$  is a group, the identity element  $0 \in \mathcal{C}$ . It follows that

$$\omega(c) = \delta(c, 0) \in \{\delta(x, y) : x, y \in \mathcal{C} \text{ and } x \neq y\},$$

so  $\omega(c) \geq \delta(a, b)$ .

(b) Note that  $\delta(a, b) = \omega(a + b)$ , and that  $a + b \in \mathcal{C}$  since  $\mathcal{C}$  is a group and  $a, b \in \mathcal{C}$ . Hence

$$\delta(a, b) = \omega(a + b) \in \{\omega(x) : x \in \mathcal{C} \text{ and } x \neq 0\},$$

so  $\delta(a, b) \geq \omega(c)$ .  $\circ$

Note that in view of Proposition 11A, we need at most  $(|\mathcal{C}| - 1)$  calculations in order to calculate the minimum distance between code words in  $\mathcal{C}$ , compared to  $\binom{|\mathcal{C}|}{2}$  calculations. It is therefore clearly of benefit to ensure that  $\mathcal{C}$  is a group. This can be achieved with relative ease if we recall Proposition 9E which we restate below in a slightly different form.

**PROPOSITION 11B.** *Suppose that  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is an encoding function. Then the code  $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$  is a group code if  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is a group homomorphism.*

## 11.2. Matrix Codes – An Example

Consider an encoding function  $\alpha : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^6$ , given for each string  $w \in \mathbb{Z}_2^3$  by  $\alpha(w) = w\mathcal{G}$ , where  $w$  is considered as a row vector and where

$$(1) \quad \mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Since

$$\mathbb{Z}_2^3 = \{000, 001, 010, 011, 100, 101, 110, 111\},$$

it follows that

$$\mathcal{C} = \alpha(\mathbb{Z}_2^3) = \{000000, 001101, 010011, 011110, 100110, 101011, 110101, 111000\}.$$

Note that  $\delta(x, y) > 2$  for all strings  $x, y \in \mathcal{C}$  with  $x \neq y$ . It follows from Proposition 10E that any transmission with single error can always be detected and corrected.

Note that if  $w = w_1w_2w_3$ , then

$$\alpha(w) = (w_1 \quad w_2 \quad w_3) \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = (w_1 \quad w_2 \quad w_3 \quad w_4 \quad w_5 \quad w_6),$$

where

$$(2) \quad \begin{aligned} w_4 &= w_1 + w_3, \\ w_5 &= w_1 + w_2, \\ w_6 &= w_2 + w_3. \end{aligned}$$

Since  $1 + 1 = 0$  in  $\mathbb{Z}_2$ , the system (2) can be rewritten in the form

$$\begin{aligned} w_1 + w_3 + w_4 &= 0, \\ w_1 + w_2 + w_5 &= 0, \\ w_2 + w_3 + w_6 &= 0; \end{aligned}$$

or, in matrix notation,

$$(3) \quad \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (w_1 \ w_2 \ w_3 \ w_4 \ w_5 \ w_6)^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Let

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

Then the matrices  $\mathcal{G}$  and  $\mathcal{H}$  are related in the following way. If we write

$$\mathcal{G} = (I_3 | \mathcal{A}) \quad \text{and} \quad \mathcal{H} = (\mathcal{B} | I_3),$$

then the matrices  $\mathcal{A}$  and  $\mathcal{B}$  are transposes of each other; in other words,  $\mathcal{B} = \mathcal{A}^t$ .

Note now that if  $c = c_1c_2c_3c_4c_5c_6 \in \mathcal{C}$ , then

$$(4) \quad \mathcal{H}c^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Note, however, that (4) does not imply that  $c \in \mathcal{C}$ .

Consider next the situation when the message  $\tau(c) = 101110$  is received instead of the message  $c = 100110$ , so that there is an error in the third digit. Then

$$(5) \quad \mathcal{H}(\tau(c))^t = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} (1 \ 0 \ 1 \ 1 \ 1 \ 0)^t = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Note that  $\mathcal{H}(\tau(c))^t$  is exactly the third column of the matrix  $\mathcal{H}$ . Note also that  $\tau(c) = c + e$ , where  $e = 001000$ . It follows that

$$\mathcal{H}(\tau(c))^t = \mathcal{H}(c + e)^t = \mathcal{H}(c^t + e^t) = \mathcal{H}c^t + \mathcal{H}e^t = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + \mathcal{H}(0 \ 0 \ 1 \ 0 \ 0 \ 0)^t.$$

Hence (5) is not a coincidence. Note now that if we change the third digit of  $\tau(c)$ , then we recover  $c$ .

However, this method, while effective if the transmission contains at most one error, ceases to be effective if the transmission contains two or more errors. Consider the string  $v = 101110$ . Then writing  $c' = 100110$  and  $c'' = 011110$ , we have  $e' = v + c' = 001000$  and  $e'' = v + c'' = 110000$ . Hence if the transmission contains possibly two errors, then we may have  $v = \tau(c')$  or  $v = \tau(c'')$ ; we shall not be able to decide which is the case. Our method will give  $c'$  but not  $c''$ .

### 11.3. Matrix Codes – The General Case

We now summarize the ideas behind the example in the last section. Suppose that  $m, n \in \mathbb{N}$ , and that  $n > m$ . Consider an encoding function  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$ , given for each string  $w \in \mathbb{Z}_2^m$  by  $\alpha(w) = w\mathcal{G}$ , where  $w$  is considered as a row vector and where, corresponding to (1) above,  $\mathcal{G}$  is an  $m \times n$  matrix over  $\mathbb{Z}_2$ .

The matrix  $\mathcal{G}$  is called the generator matrix for the code  $\mathcal{C}$ , and has the form

$$\mathcal{G} = (I_m | \mathcal{A}),$$

where  $\mathcal{A}$  is an  $m \times (n - m)$  matrix over  $\mathbb{Z}_2$ . The code is given by  $\mathcal{C} = \alpha(\mathbb{Z}_2^m) \subset \mathbb{Z}_2^n$ .

We also consider the  $(n - m) \times n$  matrix

$$\mathcal{H} = (\mathcal{B} | I_{n-m}),$$

where  $\mathcal{B} = \mathcal{A}^t$ . This is known as the parity check matrix. Note that if  $w = w_1 \dots w_m \in \mathbb{Z}_2^m$ , then  $\alpha(w) = w_1 \dots w_m w_{m+1} \dots w_n$ , where, corresponding to (3) above,

$$\mathcal{H} (w_1 \dots w_m \ w_{m+1} \dots w_n)^t = \mathbf{0},$$

with  $\mathbf{0}$  denoting the  $(n - m)$ -dimensional column zero vector.

**PROPOSITION 11C.** *In the notation of this section, consider a generator matrix  $\mathcal{G}$  and its associated parity check matrix  $\mathcal{H}$ . Suppose that the following two conditions are satisfied:*

(a) *The matrix  $\mathcal{H}$  does not contain a column of 0's.*

(b) *The matrix  $\mathcal{H}$  does not contain two identical columns.*

*Then the distance  $\delta(x, y) > 2$  for all strings  $x, y \in \mathcal{C}$  with  $x \neq y$ . In other words,  $\delta(w'\mathcal{G}, w''\mathcal{G}) > 2$  for every  $w', w'' \in \mathbb{Z}_2^m$  with  $w' \neq w''$ . In particular, single errors in transmission can be corrected.*

**PROOF.** It is sufficient to show that the minimum distance between different strings in  $\mathcal{C}$  is not 1 or 2.

(a) Suppose that the minimum distance is 1. Let  $x, y \in \mathcal{C}$  be strings such that  $\delta(x, y) = 1$ . Then  $y = x + e$ , where the string  $e$  has weight  $w(e) = 1$ , so that

$$\mathbf{0} = \mathcal{H}y^t = \mathcal{H}x^t + \mathcal{H}e^t = \mathcal{H}e^t,$$

a column of  $\mathcal{H}$ . But  $\mathcal{H}$  has no zero column.

(b) Suppose now that the minimum distance is 2. Let  $x$  and  $y$  be strings such that  $\delta(x, y) = 2$ . Then there exist distinct strings  $e'$  and  $e''$  with  $w(e') = w(e'') = 1$  and  $x + e' = y + e''$ , so that

$$\mathcal{H}(e')^t = \mathcal{H}x^t + \mathcal{H}(e')^t = \mathcal{H}y^t + \mathcal{H}(e'')^t = \mathcal{H}(e'')^t.$$

The left-hand side and right-hand side represent different columns of  $\mathcal{H}$ . But no two columns of  $\mathcal{H}$  are the same.

The result now follows from the case  $k = 1$  of Proposition 10E(b).  $\circ$

We then proceed in the following way.

**DECODING ALGORITHM.** *Suppose that the string  $v \in \mathbb{Z}_2^n$  is received.*

- (1) *If  $\mathcal{H}v^t = \mathbf{0}$ , then we feel that the transmission is correct. The decoded message consists of the first  $m$  digits of the string  $v$ .*
- (2) *If  $\mathcal{H}v^t$  is identical to the  $j$ -th column of  $\mathcal{H}$ , then we feel that there is a single error in the transmission and alter the  $j$ -th digit of the string  $v$ . The decoded message consists of the first  $m$  digits of the altered string  $v$ .*
- (3) *If cases (1) and (2) do not apply, then we feel that there are at least two errors in the transmission. We have no reliable way of decoding the string  $v$ .*

We conclude this section by showing that the encoding functions obtained by generator matrices  $\mathcal{G}$  discussed in this section give rise to group codes.

**PROPOSITION 11D.** Suppose that  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is an encoding function given by a generator matrix  $\mathcal{G} = (I_m | \mathcal{A})$ , where  $\mathcal{A}$  is an  $m \times (n - m)$  matrix over  $\mathbb{Z}_2$ . Then  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is a group homomorphism and  $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$  is a group code.

PROOF. For every  $x, y \in \mathbb{Z}_2^m$ , we clearly have

$$\alpha(x + y) = (x + y)\mathcal{G} = x\mathcal{G} + y\mathcal{G} = \alpha(x) + \alpha(y),$$

so that  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is a group homomorphism. The result now follows from Proposition 11B.  $\circ$

#### 11.4. Hamming Codes

Consider the matrix

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

Note that no non-zero column can be added without resulting in two identical columns. It follows that the number of columns is maximal if  $\mathcal{H}$  is to be the associated parity check matrix of some generator matrix  $\mathcal{G}$ .

The matrix  $\mathcal{H}$  here is in fact the associated parity check matrix of the generator matrix

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

of an encoding function  $\alpha : \mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^7$ , giving rise to a (7, 4) group code. On the other hand,  $\mathcal{H}$  is determined by 3 parity check equations.

Let us alter our viewpoint somewhat from before. Suppose that  $k \in \mathbb{N}$  and  $k \geq 3$ , and that we start with  $k$  parity check equations. Then the parity check matrix  $\mathcal{H}$  has  $k$  rows. The maximal number of columns of the matrix  $\mathcal{H}$  without having a column of 0's or having two identical columns is  $2^k - 1$ . Then  $\mathcal{H} = (\mathcal{B} | I_k)$ , where the matrix  $\mathcal{B}$  is a  $k \times (2^k - 1 - k)$  matrix. Hence  $\mathcal{H}$  is the associated parity check matrix of  $\mathcal{G} = (I_m | \mathcal{A})$ , where  $m = 2^k - 1 - k$  and where  $\mathcal{A} = \mathcal{B}^t$  is an  $m \times k$  matrix. It is easy to see that  $\mathcal{G}$  gives rise to a  $(2^k - 1, 2^k - 1 - k)$  group code; this code is known as a Hamming code. The matrix  $\mathcal{H}$  is known as a Hamming matrix.

Note that the rate of the code is

$$\frac{2^k - 1 - k}{2^k - 1} = 1 - \frac{k}{2^k - 1} \rightarrow 1 \quad \text{as } k \rightarrow \infty.$$

EXAMPLE 11.4.1. With  $k = 4$ , a possible Hamming matrix is

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

With  $k = 5$ , a possible Hamming matrix is

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

The rate of the two codes are  $11/15$  and  $26/31$  respectively.

In view of Proposition 11C, it is clear that for a Hamming code, the minimum distance between code words is at least 3. We shall now show that for any Hamming code, the minimum distance between code words is exactly 3.

**PROPOSITION 11E.** *In the notation of this section, suppose that  $k \in \mathbb{N}$  and  $k \geq 3$ , and consider a Hamming code given by generator matrix  $\mathcal{G}$  and its associated parity check matrix  $\mathcal{H}$ . Then there exist strings  $x, y \in \mathcal{C}$  such that  $\delta(x, y) = 3$ .*

**PROOF.** With given  $k$ , let  $m = 2^k - 1 - k$  and  $n = 2^k - 1$ . Then the Hamming code has an encoding function of the type  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{N}_2^n$ . It follows that the elements of the code  $\mathcal{C}$  are strings of length  $n$ . Let  $x \in \mathcal{C}$ . Then there are exactly  $n$  strings  $z \in \mathbb{Z}_2^n$  satisfying  $\delta(x, z) = 1$ . It follows that the closed ball  $B(x, 1)$  has exactly  $n + 1 = 2^k$  elements. Suppose now that  $x, y \in \mathcal{C}$  are different code words. Let  $z \in B(x, 1)$  and let  $u \in B(y, 1)$ . Then it follows from Proposition 10D(d) that

$$3 \leq \delta(x, y) \leq \delta(x, z) + \delta(z, u) + \delta(u, y) \leq 1 + \delta(z, u) + 1,$$

so that  $\delta(z, u) \geq 1$ , and so  $z \neq u$ . It follows that  $B(x, 1) \cap B(y, 1) = \emptyset$ . Note now that for each  $x \in \mathcal{C}$ , we have  $B(x, 1) \subset \mathbb{Z}_2^n$ . On the other hand,  $\mathcal{C}$  has  $2^m$  elements, so that the union

$$\bigcup_{x \in \mathcal{C}} B(x, 1)$$

has  $2^m 2^k = 2^n$  elements. It follows that

$$(6) \quad \bigcup_{x \in \mathcal{C}} B(x, 1) = \mathbb{Z}_2^n.$$

Now choose any  $x \in \mathcal{C}$ , and let  $e \in \mathbb{Z}_2^n$  satisfy  $\omega(e) = 2$ , and consider the element  $z = x + e$ . Since  $\delta(x, z) = 2$ , it follows that  $z \notin \mathcal{C}$ . In view of (6), there exists  $y \in \mathcal{C}$  such that  $z \in B(y, 1)$ . We therefore must have  $\delta(z, y) = 1$ . Finally it follows from Proposition 10D(d) that

$$\delta(x, y) \leq \delta(x, z) + \delta(z, y) = 3.$$

The result follows on noting that we also have  $\delta(x, y) \geq 3$ .  $\circ$

It now follows that for a Hamming code, the minimum distance between code words is exactly 3. Furthermore, the decoding algorithm guarantees that any message containing exactly one error can be corrected. However, it also guarantees that any message containing exactly two errors will be decoded wrongly!

### 11.5. Polynomials in $\mathbb{Z}_2[X]$

**DEFINITION.** We denote by  $\mathbb{Z}_2[X]$  the set of all polynomials of the form

$$p(X) = p_k X^k + p_{k-1} X^{k-1} + \dots + p_1 X + p_0, \quad \text{where } k \in \mathbb{N} \cup \{0\} \text{ and } p_0, \dots, p_k \in \mathbb{Z}_2;$$

in other words,  $\mathbb{Z}_2[X]$  denotes the set of all polynomials in variable  $X$  and with coefficients in  $\mathbb{Z}_2$ . Suppose further that  $p_k = 1$ . Then  $X^k$  is called the leading term of the polynomial  $p(X)$ , and  $k$  is called the degree of the polynomial  $p(X)$ . In this case, we write  $k = \deg p(X)$ .

REMARK. We have defined the degree of any non-zero constant polynomial to be 0. Note, however, that we have not defined the degree of the constant polynomial 0. The reason for this will become clear from Proposition 11F.

DEFINITION. Suppose that

$$p(X) = p_k X^k + p_{k-1} X^{k-1} + \dots + p_1 X + p_0$$

and

$$q(X) = q_m X^m + q_{m-1} X^{m-1} + \dots + q_1 X + q_0$$

are two polynomials in  $\mathbb{Z}_2[X]$ . Then we write

$$(7) \quad p(X) + q(X) = (p_n + q_n)X^n + (p_{n-1} + q_{n-1})X^{n-1} + \dots + (p_1 + q_1)X + (p_0 + q_0),$$

where  $n = \max\{k, m\}$ . Furthermore, we write

$$(8) \quad p(X)q(X) = r_{k+m}X^{k+m} + r_{k+m-1}X^{k+m-1} + \dots + r_1X + r_0,$$

where, for every  $s = 0, 1, \dots, k+m$ ,

$$(9) \quad r_s = \sum_{j=0}^s p_j q_{s-j}.$$

Here, we adopt the convention that addition and multiplication is carried out modulo 2, and  $p_j = 0$  for every  $j > k$  and  $q_j = 0$  for every  $j > m$ .

EXAMPLE 11.5.1. Suppose that  $p(X) = X^2 + 1$  and  $q(X) = X^3 + X + 1$ . Note that  $k = 2$ ,  $p_0 = 1$ ,  $p_1 = 0$  and  $p_2 = 1$ . Note also that  $m = 3$ ,  $q_0 = 1$ ,  $q_1 = 1$ ,  $q_2 = 0$  and  $q_3 = 1$ . If we adopt the convention, then  $k+m = 5$  and  $p_3 = p_4 = p_5 = q_4 = q_5 = 0$ . Now

$$p(X) + q(X) = (0+1)X^3 + (1+0)X^2 + (0+1)X + (1+1) = X^3 + X^2 + X.$$

On the other hand,

$$\begin{aligned} r_5 &= p_0q_5 + p_1q_4 + p_2q_3 + p_3q_2 + p_4q_1 + p_5q_0 = p_2q_3 = 1, \\ r_4 &= p_0q_4 + p_1q_3 + p_2q_2 + p_3q_1 + p_4q_0 = p_1q_3 + p_2q_2 = 0 + 0 = 0, \\ r_3 &= p_0q_3 + p_1q_2 + p_2q_1 + p_3q_0 = p_0q_3 + p_1q_2 + p_2q_1 = 1 + 0 + 1 = 0, \\ r_2 &= p_0q_2 + p_1q_1 + p_2q_0 = 0 + 0 + 1 = 1, \\ r_1 &= p_0q_1 + p_1q_0 = 1 + 0 = 1, \\ r_0 &= p_0q_0 = 1, \end{aligned}$$

so that

$$p(X)q(X) = X^5 + X^2 + X + 1.$$

Note that our technique for multiplication is really just a more formal version of the usual technique involving distribution, as

$$\begin{aligned} p(X)q(X) &= (X^2 + 1)(X^3 + X + 1) \\ &= (X^2 + 1)X^3 + (X^2 + 1)X + (X^2 + 1) \\ &= (X^5 + X^3) + (X^3 + X) + (X^2 + 1) \\ &= X^5 + X^2 + X + 1. \end{aligned}$$



**PROPOSITION 11G.** *Suppose that  $a(X), b(X) \in \mathbb{Z}_2[X]$ , and that  $a(X) \neq 0$ . Then there exist unique polynomials  $q(X), r(X) \in \mathbb{Z}_2[X]$  such that  $b(X) = a(X)q(X) + r(X)$ , where either  $r(X) = 0$  or  $\deg r(X) < \deg a(X)$ .*

PROOF. Consider all polynomials of the form  $b(X) - a(X)Q(X)$ , where  $Q(X) \in \mathbb{Z}_2[X]$ . If there exists  $q(X) \in \mathbb{Z}_2[X]$  such that  $b(X) - a(X)q(X) = 0$ , our proof is complete. Suppose now that

$$b(X) - a(X)Q(X) \neq 0$$

for any  $Q(X) \in \mathbb{Z}_2[X]$ . Then among all polynomials of the form  $b(X) - a(X)Q(X)$ , where  $Q(X) \in \mathbb{Z}_2[X]$ , there must be one with smallest degree. More precisely,

$$m = \min\{\deg(b(X) - a(X)Q(X)) : Q(X) \in \mathbb{Z}_2[X]\}$$

exists. Let  $q(X) \in \mathbb{Z}_2[X]$  satisfy  $\deg(b(X) - a(X)q(X)) = m$ , and let  $r(X) = b(X) - a(X)q(X)$ . Then  $\deg r(X) < \deg a(X)$ , for otherwise, writing  $a(X) = X^n + \dots + a_1x + a_0$  and  $r(X) = X^m + \dots + r_1x + r_0$ , where  $m \geq n$  and noting that  $a_n = r_m = 1$ , we have

$$r(X) - X^{m-n}a(X) = b(X) - a(X)(q(X) + X^{m-n}) \in \mathbb{Z}_2[X].$$

Clearly  $\deg(r(X) - X^{m-n}a(X)) < \deg r(X)$ , contradicting the minimality of  $m$ . On the other hand, suppose that  $q_1(X), q_2(X) \in \mathbb{Z}_2[X]$  satisfy

$$\deg(b(X) - a(X)q_1(X)) = m \quad \text{and} \quad \deg(b(X) - a(X)q_2(X)) = m.$$

Let  $r_1(X) = b(X) - a(X)q_1(X)$  and  $r_2(X) = b(X) - a(X)q_2(X)$ . Then

$$r_1(X) - r_2(X) = a(X)(q_2(X) - q_1(X)).$$

If  $q_1(X) \neq q_2(X)$ , then  $\deg(a(X)(q_2(X) - q_1(X))) \geq \deg a(X)$ , while  $\deg(r_1(X) - r_2(X)) < \deg a(X)$ , a contradiction. It follows that  $q(X)$ , and hence  $r(X)$ , is unique.  $\circ$

## 11.6. Polynomial Codes

Suppose that  $m, n \in \mathbb{N}$  and  $n > m$ . We shall define an encoding function  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  in the following way: For every  $w = w_1 \dots w_m \in \mathbb{Z}_2^m$ , let

$$(10) \quad w(X) = w_1 + w_2X + \dots + w_mX^{m-1} \in \mathbb{Z}_2[X].$$

Suppose now that  $g(X) \in \mathbb{Z}_2[X]$  is fixed and of degree  $n - m$ . Then  $w(X)g(X) \in \mathbb{Z}_2[X]$  is of degree at most  $n - 1$ . We can therefore write

$$(11) \quad w(X)g(X) = c_1 + c_2X + \dots + c_nX^{n-1},$$

where  $c_1, \dots, c_n \in \mathbb{Z}_2$ . Now let

$$(12) \quad \alpha(w) = c_1 \dots c_n \in \mathbb{Z}_2^n.$$

**PROPOSITION 11H.** *Suppose that  $m, n \in \mathbb{N}$  and  $n > m$ . Suppose further that  $g(X) \in \mathbb{Z}_2[X]$  is fixed and of degree  $n - m$ , and that the encoding function  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is defined such that for every  $w = w_1 \dots w_m \in \mathbb{Z}_2^m$ , the image  $\alpha(w)$  is given by (10)–(12). Then  $\mathcal{C} = \alpha(\mathbb{Z}_2^m)$  is a group code.*

PROOF. Suppose that  $w = w_1 \dots w_m \in \mathbb{Z}_2^m$  and  $z = z_1 \dots z_m \in \mathbb{Z}_2^m$ . Then clearly  $(w + z)(X) = w(X) + z(X)$ , so that  $(w + z)(X)g(X) = w(X)g(X) + z(X)g(X)$ , whence  $\alpha(w + z) = \alpha(w) + \alpha(z)$ . It follows that  $\alpha : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$  is a group homomorphism.  $\circ$

REMARK. The polynomial  $g(X)$  in Propsoition 11H is sometimes known as the multiplier polynomial.

Let us now turn to the question of decoding. Suppose that the string  $v = v_1 \dots v_n \in \mathbb{Z}_2^n$  is received. We consider the polynomial

$$v(X) = v_1 + v_2X + \dots + v_nX^{n-1}.$$

If  $g(X)$  divides  $v(X)$  in  $\mathbb{Z}_2[X]$ , then clearly  $v \in \mathcal{C}$ . This is the analogue of part (1) of the Decoding algorithm for matrix codes.

Corresponding to part (2) of the Decoding algorithm for matrix codes, we have the following result.

**PROPOSITION 11J.** *In the notation of Proposition 11H, for every  $c \in \mathcal{C}$  and every element*

$$e = \underbrace{0 \dots 0}_{j-1} 1 \underbrace{0 \dots 0}_{n-j} \in \mathbb{Z}_2^n,$$

*the remainder on dividing the polynomial  $(c + e)(X)$  by the polynomial  $g(X)$  is equal to the remainder on dividing the polynomial  $X^{j-1}$  by the polynomial  $g(X)$ .*

PROOF. Note that  $(c + e)(X) = c(X) + X^{j-1}$ . The result follows immediately on noting that  $g(X)$  divides  $c(X)$  in  $\mathbb{Z}_2[X]$ .  $\circ$

Suppose that we know that single errors can be corrected. Then we proceed in the following way.

**DECODING ALGORITHM.** *Suppose that the string  $v \in \mathbb{Z}_2^n$  is received.*

- (1) *If  $g(X)$  divides  $v(X)$  in  $\mathbb{Z}_2[X]$ , then we feel that the transmission is correct. The decoded message is the string  $q \in \mathbb{Z}_2^m$  where  $v(X) = g(X)q(X)$  in  $\mathbb{Z}_2[X]$ .*
- (2) *If  $g(X)$  does not divide  $v(X)$  in  $\mathbb{Z}_2[X]$  and the remainder is the same as the remainder on dividing  $X^{j-1}$  by  $g(X)$ , then we add  $X^{j-1}$  to  $v(X)$ . The decoded message is the string  $q \in \mathbb{Z}_2^m$  where  $v(X) + X^{j-1} = g(X)q(X)$  in  $\mathbb{Z}_2[X]$ .*
- (3) *If  $g(X)$  does not divide  $v(X)$  in  $\mathbb{Z}_2[X]$  and the remainder is different from the remainder on dividing  $X^{j-1}$  by  $g(X)$  for any  $j = 1, \dots, n$ , then we conclude that more than one error has occurred. We may have no reliable way of correcting the transmission.*

EXAMPLE 11.6.1. Consider the cyclic code with encoding function  $\alpha : \mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^7$  given by the multiplier polynomial  $1 + X + X^3$ . Let  $w = 1011 \in \mathbb{Z}_2^4$ . Then  $w(X) = 1 + X^2 + X^3$ , so that  $c(X) = w(X)g(X) = 1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ , giving rise to the code word  $1111111 \in \mathcal{C}$ . Suppose that  $v = 1110111$  is received, so that there is one error. Then

$$v(X) = 1 + X + X^2 + X^4 + X^5 + X^6 = g(X)(X^2 + X^3) + (X + 1).$$

On the other hand,

$$X^3 = g(X) + (X + 1).$$

It follows that if we add  $X^3$  to  $v(X)$  and then divide by  $g(X)$ , we recover  $w(X)$ . Suppose next that  $v = 1010111$  is received, so that there are two errors. Then

$$v(X) = 1 + X^2 + X^4 + X^5 + X^6 = g(X)(X^2 + X^3) + 1.$$

On the other hand,

$$1 = g(X)0 + 1.$$

It follows that if we add 1 to  $v(X)$  and then divide by  $g(X)$ , we get  $X^2 + X^3$ , corresponding to  $w = 0011 \in \mathbb{Z}_2^4$ . Hence our decoding process gives the wrong answer in this case.

## PROBLEMS FOR CHAPTER 11

1. Consider the code discussed in Section 11.2. Use the parity check matrix  $\mathcal{H}$  to decode the following strings:
- a) 101010                      b) 001001                      c) 101000                      d) 011011

2. The encoding function  $\alpha : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^5$  is given by the generator matrix

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

- a) Determine all the code words.  
 b) Discuss the error-detecting and error-correcting capabilities of the code.  
 c) Find the associated parity check matrix  $\mathcal{H}$ .  
 d) Use the parity check matrix  $\mathcal{H}$  to decode the messages 11011, 10101, 11101 and 00111.
3. The encoding function  $\alpha : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^6$  is given by the generator matrix

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

- a) How many elements does the code  $\mathcal{C} = \alpha(\mathbb{Z}_2^3)$  have? Justify your assertion.  
 b) Explain why  $\mathcal{C}$  is a group code.  
 c) What is the parity check matrix  $\mathcal{H}$  of this code?  
 d) Explain carefully why the minimum distance between code words is not equal to 1.  
 e) Explain carefully why the minimum distance between code words is not equal to 2.  
 f) Explain why single errors in transmission can always be corrected.  
 g) Can the message 011000 be decoded? Justify carefully your conclusion.
4. The encoding function  $\alpha : \mathbb{Z}_2^3 \rightarrow \mathbb{Z}_2^6$  is given by the parity check matrix

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

- a) Determine all the code words.  
 b) Can all single errors be detected?
5. Consider a code given by the parity check matrix

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

- a) What is the generator matrix  $\mathcal{G}$  of this code?  
 b) How many elements does the code  $\mathcal{C}$  have? Justify your assertion.  
 c) Decode the messages 1010111 and 1001000.  
 d) Can all single errors in transmission be detected and corrected? Justify your assertion.  
 e) Explain why the minimum distance between code words is at most 2.  
 f) Write down the set of code words.  
 g) What is the minimum distance between code words? Justify your assertion.

6. Suppose that

$$\mathcal{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

is the parity check matrix for a Hamming (7, 4) code.

- Encode the messages 1000, 1100, 1011, 1110, 1001 and 1111.
  - Decode the messages 0101001, 0111111, 0010001 and 1010100.
7. Consider a Hamming code given by the parity check matrix

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

- What is the generator matrix  $\mathcal{G}$  of this code?
  - How many elements does the code have? Justify your assertion.
  - Decode the messages 1010101, 1000011 and 1000000.
  - Prove by contradiction that the minimum distance between code words cannot be 1.
  - Prove by contradiction that the minimum distance between code words cannot be 2.
  - Can all single errors in transmission be corrected? Justify your assertion.
8. Consider a Hamming code given by the parity check matrix

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

- What is the generator matrix  $\mathcal{G}$  of this code?
  - How many elements does the code  $\mathcal{C}$  have? Justify your assertion.
  - Decode the messages 1010111 and 1111111.
  - Can all single errors in transmission be detected and corrected? Justify your assertion.
  - Suppose that  $c \in \mathcal{C}$  is a code word. How many elements  $x \in \mathbb{Z}_2^7$  satisfy  $\delta(c, x) \leq 1$ ? Justify your assertion carefully.
  - What is the minimum distance between code words? Justify your assertion.
  - Write down the set of code words.
9. Consider a Hamming code given by the parity check matrix

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

- What is the generator matrix  $\mathcal{G}$  of this code?
  - How many elements does the code  $\mathcal{C}$  have? Justify your assertion.
  - Decode the messages 0101010101010 and 111111111111111.
  - Can all single errors in transmission be detected and corrected?
  - Suppose that  $c \in \mathcal{C}$  is a code word. How many elements  $x \in \mathbf{Z}_2^{15}$  satisfy  $\delta(c, x) \leq 1$ ? Justify your assertion.
  - What is the minimum distance between code words? Justify your assertion.
10. Consider a polynomial code with encoding function  $\alpha : \mathbb{Z}_2^4 \rightarrow \mathbb{Z}_2^6$  defined by the multiplier polynomial  $1 + X + X^2$ .
- Find the 16 code words of the code.
  - What is the minimum distance between code words?
  - Can all single errors in transmission be detected?
  - Can all single errors in transmission be corrected?
  - Find the remainder term for every one-term error polynomial on division by  $1 + X + X^2$ .