CHAPTER 12

Application to Coding

12.1. Introduction

Consider the transmission of a message in the form of a string of digits 0 and 1. More precisely, consider the transmission of the string $w = w_1 \dots w_m \in \{0,1\}^m$, where $m \in \mathbb{N}$. We can identify this string with the element $\mathbf{w} = (w_1, \dots, w_m)$ of the cartesian product

$$\mathbb{Z}_2^m = \underbrace{\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{m}.$$

Now there may be interference, and a different string $v = v_1 \dots v_m \in \{0,1\}^m$ may be received instead. We can identify this received string with the element $\mathbf{v} = (v_1, \dots, v_m)$ of the cartesian product $\mathbb{Z}_2^m$. Then the error $\mathbf{e} = (e_1, \dots, e_m) \in \mathbb{Z}_2^m$ is defined by

$$\mathbf{e} = \mathbf{w} + \mathbf{v}$$

if we interpret $\mathbf{w}$, $\mathbf{v}$ and $\mathbf{e}$ as elements of the direct group product

$$\underbrace{(\mathbb{Z}_2, +) \times \dots \times (\mathbb{Z}_2, +)}_{m}.$$

Note also that $\mathbf{w} + \mathbf{e} = \mathbf{v}$ and $\mathbf{v} + \mathbf{e} = \mathbf{w}$.

We shall make no distinction between the strings $w, v, e \in \{0,1\}^m$ and their corresponding elements $\mathbf{w}, \mathbf{v}, \mathbf{e} \in \mathbb{Z}_2^m$, and shall henceforth abuse notation and write $w, v, e \in \mathbb{Z}_2^m$ and $e = w + v$ to mean $\mathbf{w}, \mathbf{v}, \mathbf{e} \in \mathbb{Z}_2^m$ and $\mathbf{e} = \mathbf{w} + \mathbf{v}$ respectively.

One way to decrease the possibility of error is to use extra digits. Instead of sending messages in $\mathbb{Z}_2^m$, we shall send messages in $\mathbb{Z}_2^n$ instead, where $n \in \mathbb{N}$ satisfies $n > m$. The following steps represent the idea of the (n, m) block code:

(1) We shall first of all add extra digits to each string in $\mathbb{Z}_2^m$ in order to make it a string in $\mathbb{Z}_2^n$. This process is known as encoding and is represented by a function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$. To ensure that different strings do not end up the same during encoding, we must ensure that the encoding function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is one-to-one.

(2) Suppose now that $w \in \mathbb{Z}_2^m$, and that $c = w\alpha \in \mathbb{Z}_2^n$. Suppose further that during transmission, the string $c \in \mathbb{Z}_2^n$ is received as $c\tau$. As errors may occur during transmission, τ is not a function.

(3) On receipt of the transmission, we now want to decode the message $c\tau$, in the hope that it is c, to recover w. This is known as the decoding process, and is represented by a function $\sigma : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$.

(4) Ideally the composition $\alpha\tau\sigma$ should be the identity function. As this cannot be achieved, we hope to find two functions $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ and $\sigma : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ so that $w\alpha\tau\sigma = w$ or the error $c\tau \neq c$ can be detected with a high probability.

12.2. Group Codes

We are interested in the case of group codes.

DEFINITION. Suppose that $m, n \in \mathbb{N}$ and $n > m$. Consider an encoding function of the type $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$. Then we say that

$$\mathcal{C} = \mathbb{Z}_2^m \alpha = \{w\alpha : w \in \mathbb{Z}_2^m\}$$

is a group code if $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^n$.

In view of Theorem 4.2, we have the following result.

PROPOSITION 12.1. *Suppose that $m, n \in \mathbb{N}$ and $n > m$. Suppose further that the encoding function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is a group homomorphism. Then the code $\mathcal{C} = \mathbb{Z}_2^m \alpha$ is a group code.*

In this chapter, we shall concentrate on the situation when the encoding function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is a group homomorphism.

12.3. Matrix Codes

EXAMPLES. (1) Consider a $(5, 4)$ block code. Define the encoding function $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^5$ in the following way. For each string $w = w_1 \dots w_4 \in \mathbb{Z}_2^4$, let $w\alpha = w\mathcal{G}$, where w is considered as a row vector and where

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

It is not difficult to see that $w\alpha = w_1 \dots w_5$, where

$$w_5 = w_1 + \ldots + w_4. \tag{12.1}$$

It follows that if a message 01011 is received, we know that an error has occurred, as this message does not satisfy (12.1). However, we do not know how to correct this error. On the other hand, if a message 01010 is received, we shall assume that it is correct. Clearly, if a single error occurs in transmission, then the received message will not satisfy (12.1). It follows that this code is capable of detecting single errors but incapable of correcting them.

(2) Consider a $(12, 4)$ block code. Define the encoding function $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^{12}$ in the following way. For each string $w = w_1 \dots w_4 \in \mathbb{Z}_2^4$, let $w\alpha = w\mathcal{G}$, where w is considered as a row vector and where

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

It is not difficult to see that $w\alpha = w_1 \dots w_4 w_1 \dots w_4 w_1 \dots w_4$. We now use the decoding function $\sigma : \mathbb{Z}_2^{12} \to \mathbb{Z}_2^4$, defined by

$$(v_1 \dots v_4 v_1' \dots v_4' v_1'' \dots v_4'')\sigma = u_1 \dots u_4,$$

where, for every $j = 1, \dots, 4$, the digit u_j is equal to the majority of the three entries v_j, v_j', v_j''. It follows that if at most one entry among v_j, v_j', v_j'' is different from w_j, then we still have $u_j = w_j$. This code is therefore capable of correcting single errors.

These two examples can be generalized to the following situation.

Suppose that $m, n \in \mathbb{N}$ and $n > m$. Consider an encoding function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$, defined for each string $w \in \mathbb{Z}_2^m$ by $w\alpha = w\mathcal{G}$, where w is considered as a row vector and $\mathcal{G}$ is an $m \times n$ matrix over $\mathbb{Z}_2$. The matrix $\mathcal{G}$ is called the generator matrix for the code $\mathcal{C} = \mathbb{Z}_2^m \alpha$, and has the form $\mathcal{G} = (I_m | \mathcal{A})$, where I_m denotes the $m \times m$ identity matrix and $\mathcal{A}$ is an $m \times (n - m)$ matrix over $\mathbb{Z}_2$.

PROPOSITION 12.2. *Suppose that $m, n \in \mathbb{N}$ and $n > m$. Suppose further that $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is an encoding function given by a generator matrix $\mathcal{G} = (I_m | \mathcal{A})$, where I_m denotes the $m \times m$ identity matrix and $\mathcal{A}$ is an $m \times (n - m)$ matrix over $\mathbb{Z}_2$. Then $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is a group homomorphism and $\mathcal{C} = \mathbb{Z}_2^m \alpha$ is a group code.*

PROOF. Simply note that for every $w, z \in \mathbb{Z}_2^m$, we have $(w+z)\alpha = (w+z)\mathcal{G} = w\mathcal{G} + z\mathcal{G} = w\alpha + z\alpha$. ◯

A first step towards decoding is the following observation.

PROPOSITION 12.3. *Suppose that $m, n \in \mathbb{N}$ and $n > m$. Suppose further that $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ 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 for every $c = c_1 \dots c_n \in \mathcal{C}$, we have*

$$\mathcal{H}(c_1 \ \dots \ c_n)^T = \mathbf{0},$$

where $\mathbf{0}$ is the $(n-m)$-dimensional column zero vector and $\mathcal{H} = (\mathcal{B}|I_{n-m})$ where $\mathcal{B} = \mathcal{A}^T$.

PROOF. Let $w = w_1 \dots w_m \in \mathbb{Z}_2^m$ satisfy $c = w\alpha$. Then

$$(c_1 \ \dots \ c_n) = w\mathcal{G} = w(I_m|\mathcal{A}) = (w|w\mathcal{A}).$$

Hence

$$(c_1 \ \dots \ c_m) = (w_1 \ \dots \ w_m) \quad \text{and} \quad (c_{m+1} \ \dots \ c_n) = w\mathcal{A}.$$

It follows that we must have

$$(c_{m+1} \ \dots \ c_n) + (c_1 \ \dots \ c_m)\mathcal{A} = (\underbrace{0 \ \dots \ 0}_{n-m}).$$

This can be described in the equivalent form

$$(c_1 \ \dots \ c_m \ c_{m+1} \ \dots \ c_n) \left(\frac{\mathcal{A}}{I_{n-m}} \right) = (\underbrace{0 \ \dots \ 0}_{n-m}).$$

The result follows on taking transposes. ◯

DEFINITION. The matrix $\mathcal{H}$ in Proposition 12.3 is called the associated parity check matrix of the generator matrix $\mathcal{G}$.

12.4. Error Detection and Correction

Before we continue with our study of matrix codes, let us first consider group codes in general.

DEFINITION. Suppose that $x = x_1 \dots x_n \in \mathbb{Z}_2^n$. Then the weight of x is given by

$$\omega(x) = |\{j = 1, \dots, n : x_j = 1\}|;$$

i.e. $\omega(x)$ denotes the number of non-zero entries among the digits of x.

DEFINITION. Suppose that $m, n \in \mathbb{N}$ and $n > m$. Suppose further that $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is a group homomorphism, and that $\mathcal{C} = \mathbb{Z}_2^m\alpha$. Then the weight $\omega(\mathcal{C})$ of the code $\mathcal{C}$ is defined by

$$\omega(\mathcal{C}) = \min\{\omega(x) : x \in \mathcal{C}, \ x \neq 0\}.$$

PROPOSITION 12.4. *Suppose that $m, n \in \mathbb{N}$ and $n > m$. Suppose further that $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is a group homomorphism, and that $\mathcal{C} = \mathbb{Z}_2^m\alpha$. Let $k \in \mathbb{N} \cup \{0\}$. If $\omega(\mathcal{C}) = 2k+1$ or $\omega(\mathcal{C}) = 2k+2$, then*

(i) *any received string $v \in \mathbb{Z}_2^n$ with at most k errors can be corrected; and*
(ii) *it is not possible to correct all received strings with more than k errors.*

PROOF. (i) Suppose that the received string $v \in \mathbb{Z}_2^n$ has at most k errors. Then $v = c + e$, where $c \in \mathcal{C}$ and $\omega(e) \leqslant k$. Suppose now that $c' \in \mathcal{C}$ and $c' \neq c$. If $v = c' + e'$, then we must have $\omega(e') > k$. For otherwise, $\omega(e') \leqslant k$. Since $v + v = 0$, we must have $c + e + c' + e' = 0$. Since $\mathcal{C}$ is a group, we must therefore have $e + e' = c + c' \in \mathcal{C}$. But clearly $\omega(c + c') = \omega(e + e') \leqslant \omega(e) + \omega(e') \leqslant 2k$, a contradiction. It follows that

$$\omega(v + c) = \omega(e) \leqslant k < \omega(e') = \omega(v + c')$$

for every $c' \in \mathcal{C}$ such that $c' \neq c$. This means that $c \in \mathcal{C}$ is the code word *closest* to v.

(ii) Suppose that $c \in \mathcal{C}$ satisfies $\omega(c) = 2k+1$ or $\omega(c) = 2k+2$. Let $v \in \mathbb{Z}_2^n$ be obtained from c by changing precisely $k+1$ of the digits in c from 1 to 0, so that $\omega(v) = k$ or $\omega(v) = k+1$. Note also that $\omega(c + v) = k + 1$. We then have

$$\omega(v + 0) \leqslant k + 1 = \omega(v + c),$$

so that $c \in \mathcal{C}$ is not the code word *closest* to v. ◯

12.5. Decoding in Matrix Codes

Returning to matric codes, we have the following result.

PROPOSITION 12.5. *In the notation of Proposition 12.3, suppose that $\mathcal{H}$ does not contain a zero column or two identical columns. Then we must have $\omega(\mathcal{C}) \geqslant 3$, so that single errors in transmission can always be corrected.*

PROOF. It is sufficient to show that no element $c \in \mathcal{C}$ satisfies $\omega(c) = 1$ or $\omega(c) = 2$. Suppose that $c \in \mathcal{C}$. Then in view of Proposition 12.3, we must have

$$\mathcal{H}(c_1 \ \ldots \ c_n)^T = \mathbf{0}.$$

Suppose that $\omega(c) = 1$. Let c_j be the only non-zero entry in c. Then $\mathcal{H}(c_1 \ \ldots \ c_n)^T$ represents the j-th column of $\mathcal{H}$, which must then be a zero column. Suppose that $\omega(c) = 2$. Let c_i and c_j be the only non-zero entries in c. Then $\mathcal{H}(c_1 \ \ldots \ c_n)^T$ represents the sum of the i-th and j-th columns of $\mathcal{H}$, so that these two columns must be identical. ◯

REMARK. Let us return to the two examples in Section 12.3. Note that Proposition 12.5 supports our conclusion in Example (2). On the other hand, try to see that the proof of Proposition 12.5 explains our conclusion in Example (1).

PROPOSITION 12.6. *In the notation of Proposition 12.3, for every $c \in \mathcal{C}$ and every element*

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

the $(n-m)$-dimensional column vector

$$\mathcal{H}(c+e)^T$$

is identical to the j-th column of $\mathcal{H}$.

PROOF. In view of Proposition 12.3, we see that

$$\mathcal{H}(c+e)^T = \mathcal{H}c^T + \mathcal{H}e^T = \mathcal{H}e^T = \mathcal{H}(\underbrace{0 \ldots 0}_{j-1} 1 \underbrace{0 \ldots 0}_{n-j})^T$$

represents the j-th column of $\mathcal{H}$. ◯

It follows that the following decoding algorithm is reasonable. Suppose that $v \in \mathbb{Z}_2^n$ 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 equal to the j-th column of $\mathcal{H}$, then we alter the j-th entry of the received string. The decoded message consists of the first m digits of the altered string.

(3) If $\mathcal{H}v^T$ is non-zero and not equal to any of the columns of $\mathcal{H}$, then we conclude that more than one error has occurred. We may have no reliable way of correcting the transmission.

EXAMPLES. (1) Consider an encoding function $\alpha : \mathbb{Z}_2^3 \to \mathbb{Z}_2^5$, given by the generator matrix

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

Then since

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

it is easy to check that

$$\mathcal{C} = \mathbb{Z}_2^3\alpha = \{00000, 00101, 01011, 01110, 10010, 10111, 11001, 11100\},$$

so that $\omega(\mathcal{C}) = 2$. It follows from Proposition 12.4 that it is not possible to correct all received strings with single error. Note that the parity check matrix

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

contains identical columns.

(2) Consider an encoding function $\alpha : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$, given by the generator matrix

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

It is easy to check that

$$\mathcal{C} = \mathbb{Z}_2^3\alpha = \{000000, 001011, 010110, 011101, 100101, 101110, 110011, 111000\},$$

so that $\omega(\mathcal{C}) = 3$. It follows from Proposition 12.5 that single errors in transmission can always be corrected. Note that

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

Suppose now that $v = 011110$ is received, with one error in the third entry from $c = 010110$. Then it is easily checked that

$$\mathcal{H}v^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

the third column of $\mathcal{H}$. We correct v by $v + 001000 = 010110$. Clearly, if $v = 011110$ is received, with errors in the fifth and sixth entries from $c = 011101$, then the decoding process will be erroneous. Finally, suppose that $v = 111111$ is received, with at least two errors from any code word $c \in \mathcal{C}$. Then it is easily checked that

$$\mathcal{H}v^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix},$$

not equal to any column of $\mathcal{H}$.

12.6. Coset Leaders

Suppose that we are interested in correcting all errors in the most plausible way. Then we may approach the problem in the following way. Note that $\mathcal{C}$ is a subgroup of $\mathbb{Z}_2^n$.

PROPOSITION 12.7. *In the notation of Proposition 12.3, suppose that v and z belong to the same coset of $\mathcal{C}$ in $\mathbb{Z}_2^n$. Then*

$$\mathcal{H}v^T = \mathcal{H}z^T.$$

PROOF. If v and z belong to the same coset of $\mathcal{C}$ in $\mathbb{Z}_2^n$, then $v+z \in \mathcal{C}$. It follows that $\mathcal{H}(v+z)^T = \mathbf{0}$. The result follows. ◯

DEFINITION. Suppose that S is a coset of $\mathcal{C}$ in $\mathbb{Z}_2^n$. Then an element of smallest weight in S is called a coset leader in S.

REMARK. The interpretation of all this is that in view of Proposition 12.7, the elements of the coset S arise from the same error pattern applied to the elements of $\mathcal{C}$. The coset leader is therefore the most plausible error pattern. It follows that if we *add* the coset leader to the received message, then we have the most plausible correction of the transmission error.

EXAMPLE. Let us return to Example (2) in Section 12.5, and consider the encoding function $\alpha : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$, given by the generator matrix

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

Recall that $\mathcal{C} = \{000000, 001011, 010110, 011101, 100101, 101110, 110011, 111000\}$. Then the cosets are

$$\begin{aligned}
\mathcal{C} &= \{000000, 001011, 010110, 011101, 100101, 101110, 110011, 111000\},\\
100000 + \mathcal{C} &= \{100000, 101011, 110110, 111101, 000101, 001110, 010011, 011000\},\\
010000 + \mathcal{C} &= \{010000, 011011, 000110, 001101, 110101, 111110, 100011, 101000\},\\
001000 + \mathcal{C} &= \{001000, 000011, 011110, 010101, 101101, 100110, 111011, 110000\},\\
000100 + \mathcal{C} &= \{000100, 001111, 010010, 011001, 100001, 101010, 110111, 111100\},\\
000010 + \mathcal{C} &= \{000010, 001001, 010100, 011111, 100111, 101100, 110001, 111010\},\\
000001 + \mathcal{C} &= \{000001, 001010, 010111, 011100, 100100, 101111, 110010, 111001\},\\
100010 + \mathcal{C} &= \{100010, 101001, 110100, 111111, 000111, 001100, 010001, 011010\}.
\end{aligned}$$

Note now that $v = 011110$ is in the coset $001000 + \mathcal{C}$, with coset leader 001000. However, $v = 111111$ is in the coset $100010 + \mathcal{C}$, with no unique coset leader.

12.7. 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 $\mathcal{H}$ 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 $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$.

Let us alter our viewpoint somewhat from before. Suppose that we start with a parity check matrix $\mathcal{H}$ with k rows. The maximal number of columns of the matrix $\mathcal{H}$ without having a zero column or 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.

Examples. (1) With $k = 4$, a possible Hamming code is given by the parity check matrix

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

The corresponding generator matrix $\mathcal{G}$ is 11×15.

(2) With $k = 5$, a possible Hamming code is given by the parity check matrix

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

The corresponding generator matrix $\mathcal{G}$ is 26×31.

In view of Proposition 12.5, we have $\omega(\mathcal{C}) \geqslant 3$ if $\mathcal{C}$ is a Hamming code. We shall show that for any Hamming code $\mathcal{C}$, we have $\omega(\mathcal{C}) = 3$.

PROPOSITION 12.8. *In the notation of this section, suppose that $k \in \mathbb{N}$ and $k \geqslant 3$, and consider a Hamming code given by a generator matrix $\mathcal{G}$ with its associated parity check matrix $\mathcal{H}$ with k rows. Then there exists $c \in \mathcal{C}$ such that $\omega(c) = 3$. Furthermore, any message containing precisely two errors will be decoded wrongly.*

PROOF. Suppose that $v \in \mathbb{Z}_2^n$ satisfies $v = c + e$, where $c \in \mathcal{C}$ and

$$e = (\underbrace{0 \ \ldots \ 0}_{i-1} \ 1 \ 0 \ \ldots \ 0 \ 1 \ \underbrace{0 \ \ldots \ 0}_{n-j}),$$

where $i < j$. Then since $\mathcal{H}$ contains all possible non-zero columns of entries 0 and 1,

$$\mathcal{H}v^T = \mathcal{H}(c+e)^T = \mathcal{H}e^T,$$

equal to the sum of the i-th and j-th columns of $\mathcal{H}$, must also be equal to one of the columns of $\mathcal{H}$. Let this be the s-th column of $\mathcal{H}$. Clearly i, j, s are distinct. It follows that the decoding

$$v + (\underbrace{0 \ \ldots \ 0}_{s-1} \ 1 \ \underbrace{0 \ \ldots \ 0}_{n-s}) \neq c.$$

However,

$$c' = v + (\underbrace{0 \ \ldots \ 0}_{s-1} \ 1 \ \underbrace{0 \ \ldots \ 0}_{n-s}) \in \mathcal{C},$$

for there are $2^n/2^m = 2^k = n+1$ cosets of $\mathcal{C}$ in $\mathbb{Z}_2^n$, with coset leaders

$$0 \ldots 0, \quad 10 \ldots 0, \quad 010 \ldots 0, \quad \ldots, \quad 0 \ldots 01.$$

Since $\mathcal{C}$ is a group, it follows that

$$c + c' = e + (\underbrace{0 \ \ldots \ 0}_{s-1} \ 1 \ \underbrace{0 \ \ldots \ 0}_{n-s}) \in \mathcal{C}$$

satisfies $\omega(c + c') = 3$. ◯

12.8. Polynomial Codes

The basic idea of a polynomial code is the following. Again, suppose that $m, n \in \mathbb{N}$ and $n > m$. We shall define an encoding function $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ in the following way. For every $w = w_1 \ldots w_m \in \mathbb{Z}_2^m$, let

$$w(X) = w_1 + w_2 X + \ldots + w_m X^{m-1} \in \mathbb{Z}_2[X]. \tag{12.2}$$

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

$$w(X)g(X) = c_1 + c_2 X + \ldots + c_n X^{n-1}, \tag{12.3}$$

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

$$w\alpha = c_1 \ldots c_n \in \mathbb{Z}_2^n. \tag{12.4}$$

PROPOSITION 12.9. *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 $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is defined for every $w = w_1 \ldots w_m \in \mathbb{Z}_2^m$ by (12.2)–(12.4). Then $\mathcal{C} = \mathbb{Z}_2^m \alpha$ is a group code.*

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

REMARK. The polynomial $g(X)$ in Proposition 12.9 is sometimes known as the multiplier.

We are interested in polynomial codes with an extra structure.

DEFINITION. Suppose that $m, n \in \mathbb{N}$ and $n > m$. Suppose further that $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ is an encoding function. Then the code $\mathcal{C} = \mathbb{Z}_2^m \alpha$ is said to be cyclic if the following condition is satisfied:

(CC) If the string $c_1 \ldots c_n \in \mathcal{C}$, then the cyclically shifted string $c_n c_1 \ldots c_{n-1} \in \mathcal{C}$.

EXAMPLE. Consider an encoding function $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^6$ defined by the multiplier polynomial $1 + X + X^2$. We have the following table, where the rows are specially ordered so that we can check the right hand column to convince ourselves that this gives rise to a cyclic code.

w	$w(X)$	$w(X)(1 + X + X^2)$	$w\alpha = c$
0000	0	0	000000
1100	$1 + X$	$1 + X^3$	100100
0110	$X + X^2$	$X + X^4$	010010
0011	$X^2 + X^3$	$X^2 + X^5$	001001
1000	1	$1 + X + X^2$	111000
0100	X	$X + X^2 + X^3$	011100
0010	X^2	$X^2 + X^3 + X^4$	001110
0001	X^3	$X^3 + X^4 + X^5$	000111
1101	$1 + X + X^3$	$1 + X^4 + X^5$	100011
1011	$1 + X^2 + X^3$	$1 + X + X^5$	110001
1110	$1 + X + X^2$	$1 + X^2 + X^4$	101010
0111	$X + X^2 + X^3$	$X + X^3 + X^5$	010101
1010	$1 + X^2$	$1 + X + X^3 + X^4$	110110
0101	$X + X^3$	$X + X^2 + X^4 + X^5$	011011
1111	$1 + X + X^2 + X^3$	$1 + X^2 + X^3 + X^5$	101101
1001	$1 + X^3$	$1 + X + X^2 + X^3 + X^4 + X^5$	111111

DEFINITION. Suppose that $n \in \mathbb{N}$. For every $c = c_1 \dots c_n \in \mathbb{Z}_2^n$ and every non-negative integer $k \leqslant n$, we write

$$c^{(k)} = c_{n-k+1} \dots c_n c_1 \dots c_{n-k}.$$

In other words, $c^{(k)}$ is obtained from c by removing the last k digits of c and replacing them at the front.

PROPOSITION 12.10. *Suppose that $n \in \mathbb{N}$, and that the non-negative integer $k \leqslant n$. Then the polynomial $c^{(k)}(X) \in \mathbb{Z}_2[X]$ is equal to the remainder on dividing the polynomial $X^k c(X)$ by the polynomial $X^n + 1$ in $\mathbb{Z}_2[X]$.*

PROOF. Clearly $q(X) + q(X) = 0$ for any $q(X) \in \mathbb{Z}_2[X]$. It follows that

$$\begin{aligned} X^k c(X) &= X^k(c_1 + c_2 X + \ldots + c_n X^{n-1}) \\ &= (c_1 X^k + c_2 X^{k+1} + \ldots + c_{n-k} X^{n-1}) + (c_{n-k+1} X^n + c_{n-k+2} X^{n+1} + \ldots + c_n X^{k+n-1}) \\ &= (c_{n-k+1} + c_{n-k+2} X + \ldots + c_n X^{k-1}) + (c_1 X^k + c_2 X^{k+1} + \ldots + c_{n-k} X^{n-1}) \\ &\quad + (c_{n-k+1} + c_{n-k+2} X + \ldots + c_n X^{k-1}) + (c_{n-k+1} X^n + c_{n-k+2} X^{n+1} + \ldots + c_n X^{k+n-1}) \\ &= c^{(k)}(X) + (X^n + 1)(c_{n-k+1} + c_{n-k+2} X + \ldots + c_n X^{k-1}). \end{aligned}$$

The result follows. ◯

PROPOSITION 12.11. *In the notation of Proposition 12.9, $\mathcal{C}$ is a cyclic code if and only if the polynomial $g(X)$ divides the polynomial $X^n + 1$ in $\mathbb{Z}_2[X]$.*

PROOF. ($\Rightarrow$) For every $c \in \mathcal{C}$, there exists $w \in \mathbb{Z}_2^m$ such that $c(X) = w(X)g(X)$. Since $\mathcal{C}$ is a cyclic code, it follows that for every $k = 1, \dots, n$, $c^{(k)} \in \mathcal{C}$, so that there exists $v \in \mathbb{Z}_2^m$ such that $c^{(k)}(X) = v(X)g(X)$. By Proposition 12.10, there exists $q(X) \in \mathbb{Z}_2[X]$ such that

$$X^k c(X) = (X^n + 1)q(X) + c^{(k)}(X), \tag{12.5}$$

so that

$$X^k c(X) + c^{(k)}(X) = (X^n + 1)q(X).$$

Since $g(X)$ divides both $c(X)$ and $c^{(k)}(X)$ in $\mathbb{Z}_2[X]$, it follows that $g(X)$ divides $(X^n + 1)q(X)$ in $\mathbb{Z}_2[X]$. We now choose c and k to satisfy $\deg X^k c(X) = n$, so that $q(X) = 1$. Then clearly $g(X)$ divides $(X^n + 1)$ in $\mathbb{Z}_2[X]$.

($\Leftarrow$) Suppose that $c \in \mathcal{C}$. We need to show that for every $k = 1, \ldots, n$, the polynomial $g(X)$ divides the polynomial $c^{(k)}(X)$ in $\mathbb{Z}_2[X]$. Rearranging (12.5), we have

$$c^{(k)}(X) = X^k c(X) + (X^n + 1)q(X).$$

Since $g(X)$ divides $c(X)$ and $(X^n + 1)$ in $\mathbb{Z}_2[X]$, the result follows. ◯

Naturally we would like to identify polynomials $g(X) \in \mathbb{Z}_2[X]$ which will give rise to cyclic codes. Observe the following as a useful step.

PROPOSITION 12.12. *In the notation of Proposition 12.9, if $\mathcal{C}$ is a cyclic code, then the constant term of the polynomial $g(X)$ is non-zero.*

PROOF. This follows from the observation that $g(X)$ must divide $X^n + 1$ in $\mathbb{Z}_2[X]$. If the constant term of $g(X)$ is zero, then X divides $g(X)$ in $\mathbb{Z}_2[X]$, and so must also divide $X^n + 1$ in $\mathbb{Z}_2[X]$, clearly impossible. ◯

EXAMPLES. (1) Consider $\alpha : \mathbb{Z}_2^3 \to \mathbb{Z}_2^5$. Then any multiplier polynomial $g(X)$ must be of degree 2, have constant term 1 and divide $X^5 + 1$ in $\mathbb{Z}_2[X]$ in order to give a cyclic code. Note that the only polynomials in $\mathbb{Z}_2[X]$ of degree 2 and with constant term 1 are $1 + X^2$ and $1 + X + X^2$. Neither divides $X^5 + 1$ in $\mathbb{Z}_2[X]$. Hence no cyclic code exists in this situation.

(2) Consider $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$. Then any multiplier polynomial $g(X)$ must be of degree 3, have constant term 1 and divide $X^7 + 1$ in $\mathbb{Z}_2[X]$ in order to give a cyclic code. Note that the only polynomials in $\mathbb{Z}_2[X]$ of degree 3 and with constant term 1 are $1+X^3$, $1+X+X^3$, $1+X^2+X^3$ and $1+X+X^2+X^3$. Of these, only $1 + X + X^3$ and $1 + X^2 + X^3$ divide $X^7 + 1$ in $\mathbb{Z}_2[X]$, giving rise to two cyclic codes.

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

$$v(X) = c_1 + c_2 X + \ldots + c_n X^{n-1}.$$

If $g(X)$ divides $v(X)$ in $\mathbb{Z}_2[X]$, then clearly $v \in \mathcal{C}$. This is the analogue of Proposition 12.3.

Corresponding to Proposition 12.6, we have the following result.

PROPOSITION 12.13. *In the notation of Proposition 12.9, for every $c \in \mathcal{C}$ and every element*

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

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 on noting that $g(X)$ divides $c(X)$ in $\mathbb{Z}_2[X]$. ◯

It follows that the following decoding algorithm is reasonable. Suppose that we know that single errors can be corrected, and that $v \in \mathbb{Z}_2^n$ 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 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 $j = 1, \ldots, n$, then we conclude that more than one error has occurred. We may have no reliable way of correcting the transmission.

EXAMPLE. Consider the cyclic code with encoding function $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$ 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. We shall return to this example later.

Suppose again that we are interested in correcting all errors in the most plausible way. Then we again use coset leaders. Corresponding to Proposition 12.7, we have the following result.

PROPOSITION 12.14. *In the notation of Proposition 12.9, suppose that v and z belong to the same coset of $\mathcal{C}$ in $\mathbb{Z}_2^n$. Then the remainder on dividing $v(X)$ by $g(X)$ is equal to the remainder on dividing $z(X)$ by $g(X)$.*

PROOF. Since v and z belong to the same coset of $\mathcal{C}$ in $\mathbb{Z}_2^n$, we have $v + z \in \mathcal{C}$, so that $g(X)$ divides $x(X) + z(X)$ in $\mathbb{Z}_2[X]$. The result follows. ◯

REMARK. Again, the coset leader is therefore the most plausible error pattern. It follows that if we *add* the coset leader to the received message, then we have the most plausible correction of the transmission error.

12.9. Connection with Field Theory

In this section, we look for the analogue of a Hamming code.

PROPOSITION 12.15. *Suppose that $g(X) \in \mathbb{Z}_2[X]$ is irreducible and of degree k, and that $g(X)$ divides $X^n + 1$ in $\mathbb{Z}_2[X]$, where $n = 2^k - 1$. Consider the field extension $F = \mathbb{Z}_2[X]/\langle g(X)\rangle$, and suppose further that there is a root of $g(X)$ that generates the cyclic multiplicative group F^*. Then the polynomial code $\alpha : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$, where $m = n - k = 2^k - 1 - k$ and with multiplier $g(X)$ is a cyclic code which corrects all received messages that contain precisely one error. Furthermore, any message containing precisely two errors will be decoded wrongly.*

PROOF. Note that the field $F = \mathbb{Z}_2[X]/\langle g(X)\rangle$ has 2^k elements, in view of Proposition 9.6. Furthermore, by Theorem 9.5, these elements can be expressed in the form

$$a_1 + a_2X + \ldots + a_kX^{k-1} + \langle g(X)\rangle, \quad a_1, a_2 \ldots, a_k \in \mathbb{Z}_2.$$

On the other hand, the multiplicative group F^* is generated by $X + \langle g(X)\rangle$. It follows that

$$F = \{\langle g(X)\rangle, 1 + \langle g(X)\rangle, X + \langle g(X)\rangle, X^2 + \langle g(X)\rangle, \ldots, X^{n-1} + \langle g(X)\rangle\}.$$

This gives a one-to-one correspondence between all single error patterns of the polynomials X^{j-1}, where $j = 1, \ldots, n$, and the non-zero remainders $a_1 + a_2X + \ldots + a_kX^{k-1}$ on division by $g(X)$ in $\mathbb{Z}_2[X]$. Hence we have shown that the error patterns of the polynomials X^{j-1}, where $j = 1, \ldots, n$, give all the non-zero coset leaders. This ensures that all received messages containing precisely one error will be corrected, while ensuring that any message containing precisely two errors will be decoded wrongly. ◯

REMARK. Note that the cyclic code in our last example is such a code.

Problems for Chapter 12

1. The encoding function $\alpha : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$ is given by the parity-check matrix

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

   (i) Determine all the code words.
   (ii) Can all single errors be detected?
   (iii) Determine all the coset leaders. Are they all uniquely determined?

2. 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.

   (i) Encode the messages 1000, 1100, 1011, 1110, 1001 and 1111.
   (ii) Decode the messages 0101001, 0111111, 0010001 and 1010100.
   (iii) Give all the coset leaders without writng down any of the cosets.

3. Consider the cyclic code with encoding function $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$ given by the multiplier polynomial $1 + X + X^3$.

   (i) Decode the messages 0011010, 1101101, 0000000 and 0101111.
   (ii) Write down the coset leaders and their remainders on division by the multiplier polynomial.

4. Show that there is no multiplier polynomial that will give a cyclic code with encoding function $\alpha : \mathbb{Z}_2^5 \to \mathbb{Z}_2^7$.

5. Consider the cyclic code with encoding function $\alpha : \mathbb{Z}_2^4 \to \mathbb{Z}_2^6$ given in the example on page 76.

   (i) Consider the field $F = \mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle$. Show that a root of $X^2 + X + 1$ generates the cyclic group F^*.
   (ii) Find the remainder of every one-term error polynomial on division by $X^2 + X + 1$.
   (iii) Can all single errors in transmission be corrected? Justify your assertion.