CHAPTER 5

Cyclic Codes

Cyclic codes form an important subclass of linear block codes. These codes are attractive for two reasons: first, encoding and syndrome computation can be implemented easily by employing shift registers with feedback connections (known as linear sequential circuits); and second, because they have considerable inherent algebraic structure, it is possible to devise various practical methods for decoding them. Cyclic codes are widely used in communication systems for error control. They are particularly efficient for error detection.

Cyclic codes were first studied by Eugene Prange in 1957 [1]. Since then, progress in the study of cyclic codes for both random-error correction and burst-error correction has been spurred by many algebraic coding theorists. Many classes of cyclic codes have been constructed over the years, including BCH codes, Reed–Solomon codes, Euclidean geometry codes, projective geometry codes, quadratic residue codes, and Fire codes, which will be discussed in later chapters. Excellent expositions of cyclic codes can be found in [2–5]. References [6–9] also provide good coverage of cyclic codes.

5.1 DESCRIPTION OF CYCLIC CODES

If we cyclically shift the components of an n-tuple $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ one place to the right, we obtain another n-tuple,

$$\mathbf{v}^{(1)} = (v_{n-1}, v_0, \cdots, v_{n-2}),$$

which is called a *cyclic shift* of $\mathbf{v}$. If the components of $\mathbf{v}$ are cyclically shifted i places to the right, the resultant n-tuple is

$$\mathbf{v}^{(i)} = (v_{n-i}, v_{n-i+1}, \cdots, v_{n-1}, v_0, v_1, \cdots, v_{n-i-1}).$$

Clearly, cyclically shifting $\mathbf{v}$ i places to the right is equivalent to cyclically shifting $\mathbf{v}$ $n-i$ places to the left.

DEFINITION 5.1 An (n, k) linear code C is called a *cyclic code* if every cyclic shift of a codeword in C is also a codeword in C.

The (7, 4) linear code given in Table 5.1 is a cyclic code.

To develop the algebraic properties of a cyclic code, we treat the components of a codeword $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ as the coefficients of a polynomial as follows:

$$\mathbf{v}(X) = v_0 + v_1X + v_2X^2 + \cdots + v_{n-1}X^{n-1}.$$

Thus, each codeword corresponds to a polynomial of degree $n-1$ or less. If $v_{n-1} \neq 0$, the degree of $\mathbf{v}(X)$ is $n-1$; if $v_{n-1} = 0$, the degree of $\mathbf{v}(X)$ is less than $n-1$. The correspondence between the codeword $\mathbf{v}$ and the polynomial $\mathbf{v}(X)$ is one-to-one. We shall call $\mathbf{v}(X)$ the code polynomial of $\mathbf{v}$. Hereafter, we shall use the terms *codeword* and *code polynomial* interchangeably. The code polynomial that corresponds to codeword $\mathbf{v}^{(i)}$ is

TABLE 5.1: A (7, 4) cyclic code generated by $\mathbf{g}(X) = 1 + X + X^3$.

Messages	Code vectors	Code polynomials
(0000)	0000000	$0 = 0 \cdot \mathbf{g}(X)$
(1000)	1101000	$1 + X + X^3 = 1 \cdot \mathbf{g}(X)$
(0100)	0110100	$X + X^2 + X^4 = X \cdot \mathbf{g}(X)$
(1100)	1011100	$1 + X^2 + X^3 + X^4 = (1 + X) \cdot \mathbf{g}(X)$
(0010)	0011010	$X^2 + X^3 + X^5 = X^2 \cdot \mathbf{g}(X)$
(1010)	1110010	$1 + X + X^2 + X^5 = (1 + X^2) \cdot \mathbf{g}(X)$
(0110)	0101110	$X + X^3 + X^4 + X^5 = (X + X^2) \cdot \mathbf{g}(X)$
(1110)	1000110	$1 + X^4 + X^5 = (1 + X + X^2) \cdot \mathbf{g}(X)$
(0001)	0001101	$X^3 + X^4 + X^6 = X^3 \cdot \mathbf{g}(X)$
(1001)	1100101	$1 + X + X^4 + X^6 = (1 + X^3) \cdot \mathbf{g}(X)$
(0101)	0111001	$X + X^2 + X^3 + X^6 = (X + X^3) \cdot \mathbf{g}(X)$
(1101)	1010001	$1 + X^2 + X^6 = (1 + X + X^3) \cdot \mathbf{g}(X)$
(0011)	0010111	$X^2 + X^4 + X^5 + X^6 = (X^2 + X^3) \cdot \mathbf{g}(X)$
(1011)	1111111	$1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ $= (1 + X^2 + X^3) \cdot \mathbf{g}(X)$
(0111)	0100011	$X + X^5 + X^6 = (X + X^2 + X^3) \cdot \mathbf{g}(X)$
(1111)	1001011	$1 + X^3 + X^5 + X^6$ $= (1 + X + X^2 + X^3) \cdot \mathbf{g}(X)$

$$\mathbf{v}^{(i)}(X) = v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1} + v_0X^i + v_1X^{i+1} + \cdots + v_{n-i-1}X^{n-1}.$$

There exists an interesting algebraic relationship between $\mathbf{v}(X)$ and $\mathbf{v}^{(i)}(X)$. Multiplying $\mathbf{v}(X)$ by X^i, we obtain

$$X^i\mathbf{v}(X) = v_0X^i + v_1X^{i+1} + \cdots + v_{n-i-1}X^{n-1} + \cdots + v_{n-1}X^{n+i-1}.$$

The preceding equation can be manipulated into the following form:

$$\begin{aligned} X^i\mathbf{v}(X) &= v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1} + v_0X^i + \cdots + v_{n-i-1}X^{n-1} \\ &\quad + v_{n-i}(X^n + 1) + v_{n-i+1}X(X^n + 1) + \cdots + v_{n-1}X^{i-1}(X^n + 1) \qquad (5.1) \\ &= \mathbf{q}(X)(X^n + 1) + \mathbf{v}^{(i)}(X), \end{aligned}$$

where $\mathbf{q}(X) = v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^{i-1}$. From (5.1) we see that the code polynomial $\mathbf{v}^{(i)}(X)$ is simply the remainder resulting from dividing the polynomial $X^i\mathbf{v}(X)$ by $X^n + 1$.

Next, we prove a number of important algebraic properties of a cyclic code that make possible the simple implementation of encoding and syndrome computation.

THEOREM 5.1 The nonzero code polynomial of minimum degree in a cyclic code C is unique.

Proof. Let $\mathbf{g}(X) = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$ be a nonzero code polynomial of minimum degree in C. Suppose that $\mathbf{g}(X)$ is not unique. Then, there exists another code polynomial of degree r, say $\mathbf{g}'(X) = g'_0 + g'_1X + \cdots + g'_{r-1}X^{r-1} + X^r$. Because C is linear, $\mathbf{g}(X) + \mathbf{g}'(X) = (g_0 + g'_0) + (g_1 + g'_1)X + \cdots + (g_{r-1} + g'_{r-1})X^{r-1}$ is a code polynomial of degree less than r. If $\mathbf{g}(X)+\mathbf{g}'(X) \neq 0$, then $\mathbf{g}(X)+\mathbf{g}'(X)$ is a nonzero code polynomial of degree less than the minimum degree r. This is impossible. Therefore, $\mathbf{g}(X) + \mathbf{g}'(X) = 0$. This implies that $\mathbf{g}'(X) = \mathbf{g}(X)$. Hence, $\mathbf{g}(X)$ is unique. **Q.E.D.**

Theorem 5.2 Let $\mathbf{g}(X) = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$ be the nonzero code polynomial of minimum degree in an (n, k) cyclic code C. Then, the constant term g_0 must be equal to 1.

Proof. Suppose that $g_0 = 0$. Then,

$$\begin{aligned}\mathbf{g}(X) &= g_1X + g_2X^2 + \cdots + g_{r-1}X^{r-1} + X^r\\ &= X(g_1 + g_2X + \cdots + g_{r-1}X^{r-2} + X^{r-1}).\end{aligned}$$

If we shift $\mathbf{g}(X)$ cyclically $n - 1$ places to the right (or one place to the left), we obtain a nonzero code polynomial, $g_1 + g_2X + \cdots + g_{r-1}X^{r-2} + X^{r-1}$, of degree less than r. This is a contradiction to the assumption that $\mathbf{g}(X)$ is the nonzero code polynomial with minimum degree. Thus, $g_0 \neq 0$. **Q.E.D.**

It follows from Theorem 5.2 that the nonzero code polynomial of minimum degree in an (n, k) cyclic code C is of the following form:

$$\mathbf{g}(X) = 1 + g_1X + g_2X^2 + \cdots + g_{r-1}X^{r-1} + X^r. \tag{5.2}$$

Consider the (7, 4) cyclic code given in Table 5.1. The nonzero code polynomial of minimum degree is $\mathbf{g}(X) = 1 + X + X^3$.

Consider the polynomials $X\mathbf{g}(X), X^2\mathbf{g}(X), \cdots, X^{n-r-1}\mathbf{g}(X)$, of degrees $r + 1, r+2, \cdots, n-1$, respectively. It follows from (5.1) that $X\mathbf{g}(X) = \mathbf{g}^{(1)}(X)$, $X^2\mathbf{g}(X) = \mathbf{g}^{(2)}(X), \cdots, X^{n-r-1}\mathbf{g}(X) = \mathbf{g}^{(n-r-1)}(X)$; that is, they are cyclic shifts of the code polynomial $\mathbf{g}(X)$. Therefore, they are code polynomials in C. Since C is linear, a linear combination of $\mathbf{g}(X), X\mathbf{g}(X), \cdots, X^{n-r-1}\mathbf{g}(X)$,

$$\begin{aligned}\mathbf{v}(X) &= u_0\mathbf{g}(X) + u_1X\mathbf{g}(X) + \cdots + u_{n-r-1}X^{n-r-1}\mathbf{g}(X)\\ &= (u_0 + u_1X + \cdots + u_{n-r-1}X^{n-r-1})\mathbf{g}(X).\end{aligned} \tag{5.3}$$

is also a code polynomial, where $u_i = 0$ or 1. The following theorem characterizes an important property of a cyclic code.

Theorem 5.3 Let $\mathbf{g}(X) = 1+g_1X+\cdots+g_{r-1}X^{r-1}+X^r$ be the nonzero code polynomial of minimum degree in an (n, k) cyclic code C. A binary polynomial of degree $n - 1$ or less is a code polynomial if and only if it is a multiple of $\mathbf{g}(X)$.

Proof. Let $\mathbf{v}(X)$ be a binary polynomial of degree $n - 1$ or less. Suppose that $\mathbf{v}(X)$ is a multiple of $\mathbf{g}(X)$. Then,

$$\begin{aligned}\mathbf{v}(X) &= (a_0 + a_1X + \cdots + a_{n-r-1}X^{n-r-1})\mathbf{g}(X)\\ &= a_0\mathbf{g}(X) + a_1X\mathbf{g}(X) + \cdots + a_{n-r-1}X^{n-r-1}\mathbf{g}(X).\end{aligned}$$

Because $\mathbf{v}(X)$ is a linear combination of the code polynomials $\mathbf{g}(X), X\mathbf{g}(X), \cdots, X^{n-r-1}\mathbf{g}(X)$, it is a code polynomial in C. This proves the first part of the theorem—that if a polynomial of degree $n - 1$ or less is a multiple of $\mathbf{g}(X)$, it is a code polynomial.

Now, let $\mathbf{v}(X)$ be a code polynomial in C. Dividing $\mathbf{v}(X)$ by $\mathbf{g}(X)$, we obtain

$$\mathbf{v}(X) = \mathbf{a}(X)\mathbf{g}(X) + \mathbf{b}(X).$$

where either $\mathbf{b}(X)$ is identical to zero, or the degree of $\mathbf{b}(X)$ is less than the degree of $\mathbf{g}(X)$. Rearranging the preceding equation, we have

$$\mathbf{b}(X) = \mathbf{v}(X) + \mathbf{a}(X)\mathbf{g}(X).$$

It follows from the first part of the theorem that $\mathbf{a}(X)\mathbf{g}(X)$ is a code polynomial. Because both $\mathbf{v}(X)$ and $\mathbf{a}(X)\mathbf{g}(X)$ are code polynomials, $\mathbf{b}(X)$ must also be a code polynomial. If $\mathbf{b}(X) \neq 0$, then $\mathbf{b}(X)$ is a nonzero code polynomial whose degree is less than the degree of $\mathbf{g}(X)$. This contradicts the assumption that $\mathbf{g}(X)$ is the nonzero code polynomial of minimum degree. Thus, $\mathbf{b}(X)$ must be identical to zero. This proves the second part of the theorem—that a code polynomial is a multiple of $\mathbf{g}(X)$. **Q.E.D.**

The number of binary polynomials of degree $n - 1$ or less that are multiples of $\mathbf{g}(X)$ is 2^{n-r}. It follows from Theorem 5.3 that these polynomials form all the code polynomials of the (n, k) cyclic code C. Because there are 2^k code polynomials in C, then 2^{n-r} must be equal to 2^k. As a result, we have $r = n - k$ [i.e., the degree of $\mathbf{g}(X)$ is $n - k$]. Hence, the nonzero code polynomial of minimum degree in an (n, k) cyclic code is of the following form:

$$\mathbf{g}(X) = 1 + g_1X + g_2X^2 + \cdots + g_{n-k-1}X^{n-k-1} + X^{n-k}.$$

Summarizing the preceding results, we have the following theorem:

Theorem 5.4 In an (n, k) cyclic code, there exists one and only one code polynomial of degree $n - k$,

$$\mathbf{g}(X) = 1 + g_1X + g_2X^2 + \cdots + g_{n-k-1}X^{n-k-1} + X^{n-k}. \tag{5.4}$$

Every code polynomial is a multiple of $\mathbf{g}(X)$, and every binary polynomial of degree $n - 1$ or less that is a multiple of $\mathbf{g}(X)$ is a code polynomial.

It follows from Theorem 5.4 that every code polynomial $\mathbf{v}(X)$ in an (n, k) cyclic code can be expressed in the following form:

$$\begin{aligned}\mathbf{v}(X) &= \mathbf{u}(X)\mathbf{g}(X)\\ &= (u_0 + u_1X + \cdots + u_{k-1}X^{k-1})\mathbf{g}(X).\end{aligned}$$

If the coefficients of $\mathbf{u}(X)$, $u_0, u_1, \cdots, u_{k-1}$, are the k information digits to be encoded, $\mathbf{v}(X)$ is the corresponding code polynomial. Hence, the encoding can be achieved by multiplying the message $\mathbf{u}(X)$ by $\mathbf{g}(X)$. Therefore, an (n, k) cyclic code is completely specified by its nonzero code polynomial of minimum degree, $\mathbf{g}(X)$, given by (5.4). The polynomial $\mathbf{g}(X)$ is called the *generator polynomial* of the code. The degree of $\mathbf{g}(X)$ is equal to the number of parity-check digits of the code. The generator polynomial of the (7, 4) cyclic code given in Table 4.1 is $\mathbf{g}(X) = 1+X+X^3$. We see that each code polynomial is a multiple of $\mathbf{g}(X)$.

The next important property of a cyclic code is given in the following theorem.

THEOREM 5.5 The generator polynomial $\mathbf{g}(X)$ of an (n, k) cyclic code is a factor of $X^n + 1$.

Proof. Multiplying $\mathbf{g}(X)$ by X^k results in a polynomial $X^k\mathbf{g}(X)$ of degree n. Dividing $X^k\mathbf{g}(X)$ by $X^n + 1$, we obtain

$$X^k\mathbf{g}(X) = (X^n + 1) + \mathbf{g}^{(k)}(X), \tag{5.5}$$

where $\mathbf{g}^{(k)}(X)$ is the remainder. It follows from (5.1) that $\mathbf{g}^{(k)}(X)$ is the code polynomial obtained by shifting $\mathbf{g}(X)$ to the right cyclically k times. Hence, $\mathbf{g}^{(k)}(X)$ is a multiple of $\mathbf{g}(X)$, say $\mathbf{g}^{(k)}(X) = \mathbf{a}(X)\mathbf{g}(X)$. From (5.5) we obtain

$$X^n + 1 = \{X^k + \mathbf{a}(X)\}\mathbf{g}(X).$$

Thus, $\mathbf{g}(X)$ is a factor of $X^n + 1$. **Q.E.D.**

At this point, a natural question is whether, for any n and k, there exists an (n, k) cyclic code. This question is answered by the following theorem.

THEOREM 5.6 If $\mathbf{g}(X)$ is a polynomial of degree $n - k$ and is a factor of $X^n + 1$, then $\mathbf{g}(X)$ generates an (n, k) cyclic code.

Proof. Consider the k polynomials $\mathbf{g}(X), X\mathbf{g}(X), \cdots, X^{k-1}\mathbf{g}(X)$, all of degree $n - 1$ or less. A linear combination of these k polynomials,

$$\begin{aligned}\mathbf{v}(X) &= a_0\mathbf{g}(X) + a_1X\mathbf{g}(X) + \cdots + a_{k-1}X^{k-1}\mathbf{g}(X)\\ &= (a_0 + a_1X + \cdots + a_{k-1}X^{k-1})\mathbf{g}(X),\end{aligned}$$

is also a polynomial of degree $n - 1$ or less and is a multiple of $\mathbf{g}(X)$. There are a total of 2^k such polynomials, and they form an (n, k) linear code.

Let $\mathbf{v}(X) = v_0 + v_1X + \cdots + v_{n-1}X^{n-1}$ be a code polynomial in this code. Multiplying $\mathbf{v}(X)$ by X, we obtain

$$\begin{aligned}X\mathbf{v}(X) &= v_0X + v_1X^2 + \cdots + v_{n-2}X^{n-1} + v_{n-1}X^n\\ &= v_{n-1}(X^n + 1) + (v_{n-1} + v_0X + \cdots + v_{n-2}X^{n-1})\\ &= v_{n-1}(X^n + 1) + \mathbf{v}^{(1)}(X),\end{aligned}$$

where $\mathbf{v}^{(1)}(X)$ is a cyclic shift of $\mathbf{v}(X)$. Since both $X\mathbf{v}(X)$ and $X^n + 1$ are divisible by $\mathbf{g}(X)$, $\mathbf{v}^{(1)}(X)$ must be divisible by $\mathbf{g}(X)$. Thus, $\mathbf{v}^{(1)}(X)$ is a multiple of $\mathbf{g}(X)$ and is a linear combination of $\mathbf{g}(X), X\mathbf{g}(X), \cdots, X^{k-1}\mathbf{g}(X)$. Hence, $\mathbf{v}^{(1)}(X)$ is also a code polynomial. It follows from Definition 5.1 that the linear code generated by $\mathbf{g}(X), X\mathbf{g}(X), \cdots, X^{k-1}\mathbf{g}(X)$ is an (n, k) cyclic code. **Q.E.D.**

Theorem 5.6 says that any factor of $X^n + 1$ with degree $n - k$ generates an (n, k) cyclic code. For large n, $X^n + 1$ may have many factors of degree $n - k$. Some of these polynomials generate good codes, and some generate bad codes. How to select generator polynomials to produce good cyclic codes is a very difficult problem, and coding theorists have expended much effort in searching for good cyclic codes. Several classes of good cyclic codes have been discovered, and they can be practically implemented.

EXAMPLE 5.1

The polynomial $X^7 + 1$ can be factored as follows:

$$X^7 + 1 = (1 + X)(1 + X + X^3)(1 + X^2 + X^3).$$

There are two factors of degree 3, and each generates a (7, 4) cyclic code. The (7, 4) cyclic code given by Table 5.1 is generated by $\mathbf{g}(X) = 1 + X + X^3$. This code has a minimum distance of 3 and it is a single-error-correcting code. Notice that the code is not in systematic form. Each code polynomial is the product of a message polynomial of degree 3 or less and the generator polynomial $\mathbf{g}(X) = 1 + X + X^3$. For example, let $\mathbf{u} = (1\,0\,1\,0)$ be the message to be encoded. The corresponding message polynomial is $\mathbf{u}(X) = 1 + X^2$. Multiplying $\mathbf{u}(X)$ by $\mathbf{g}(X)$ gives us the following code polynomial:

$$\begin{aligned}\mathbf{v}(X) &= (1 + X^2)(1 + X + X^3)\\ &= 1 + X + X^2 + X^5,\end{aligned}$$

or the codeword $(1\,1\,1\,0\,0\,1\,0)$.

Given the generator polynomial $\mathbf{g}(X)$ of an (n, k) cyclic code, we can put the code into systematic form (i.e., the rightmost k digits of each codeword are the unaltered information digits, and the leftmost $n - k$ digits are parity-check digits). Suppose that the message to be encoded is $\mathbf{u} = (u_0, u_1, \cdots, u_{k-1})$. The corresponding message polynomial is

$$\mathbf{u}(X) = u_0 + u_1X + \cdots + u_{k-1}X^{k-1}.$$

Multiplying $\mathbf{u}(X)$ by X^{n-k}, we obtain a polynomial of degree $n - 1$ or less:

$$X^{n-k}\mathbf{u}(X) = u_0X^{n-k} + u_1X^{n-k+1} + \cdots + u_{k-1}X^{n-1}.$$

Dividing $X^{n-k}\mathbf{u}(X)$ by the generator polynomial $\mathbf{g}(X)$, we have

$$X^{n-k}\mathbf{u}(X) = \mathbf{a}(X)\mathbf{g}(X) + \mathbf{b}(X) \tag{5.6}$$

where $\mathbf{a}(X)$ and $\mathbf{b}(X)$ are the quotient and the remainder, respectively. Because the degree of $\mathbf{g}(X)$ is $n - k$, the degree of $\mathbf{b}(X)$ must be $n - k - 1$ or less; that is,

$$\mathbf{b}(X) = b_0 + b_1X + \cdots + b_{n-k-1}X^{n-k-1}.$$

Rearranging (5.6), we obtain the following polynomial of degree $n-1$ or less:

$$\mathbf{b}(X) + X^{n-k}\mathbf{u}(X) = \mathbf{a}(X)\mathbf{g}(X). \tag{5.7}$$

This polynomial is a multiple of the generator polynomial $\mathbf{g}(X)$ and therefore it is a code polynomial of the cyclic code generated by $\mathbf{g}(X)$. Writing out $\mathbf{b}(X)+X^{n-k}\mathbf{u}(X)$, we have

$$\begin{aligned}\mathbf{b}(X) + X^{n-k}\mathbf{u}(X) &= b_0 + b_1X + \cdots + b_{n-k-1}X^{n-k-1}\\ &\quad + u_0X^{n-k} + u_1X^{n-k+1} + \cdots + u_{k-1}X^{n-1},\end{aligned} \tag{5.8}$$

which corresponds to the codeword

$$(b_0, b_1, \cdots, b_{n-k-1}, u_0, u_1, \cdots, u_{k-1}).$$

We see that the codeword consists of k unaltered information digits $(u_0, u_1, \cdots, u_{k-1})$ followed by $n-k$ parity-check digits. The $n-k$ parity-check digits are simply the coefficients of the remainder resulting from dividing the message polynomial $X^{n-k}\mathbf{u}(X)$ by the generator polynomial $\mathbf{g}(X)$. The preceding process yields an (n, k) cyclic code in systematic form. In connection with cyclic codes in systematic form, the following convention is used: the first $n-k$ symbols, the coefficients of $1, X, \cdots, X^{n-k-1}$, are taken as parity-check digits, and the last k symbols, the coefficients of $X^{n-k}, X^{n-k+1}, \cdots, X^{n-1}$, are taken as the information digits. In summary, encoding in systematic form consists of three steps:

Step 1. Premultiply the message $\mathbf{u}(X)$ by X^{n-k}.

Step 2. Obtain the remainder $\mathbf{b}(X)$ (the parity-check digits) from dividing $X^{n-k}\mathbf{u}(X)$ by the generator polynomial $\mathbf{g}(X)$.

Step 3. Combine $\mathbf{b}(X)$ and $X^{n-k}\mathbf{u}(X)$ to obtain the code polynomial $\mathbf{b}(X) + X^{n-k}\mathbf{u}(X)$.

EXAMPLE 5.2

Consider the (7, 4) cyclic code generated by $\mathbf{g}(X) = 1 + X + X^3$. Let $\mathbf{u}(X) = 1 + X^3$ be the message to be encoded. Dividing $X^3\mathbf{u}(X) = X^3 + X^6$ by $\mathbf{g}(X)$,

$$\begin{array}{r|llll} & X^3+X & \text{(quotient)} & & \\ \cline{2-4} X^3+X+1 & X^6 & & X^3 & \\ & X^6 & +X^4+ & X^3 & \\ \cline{2-4} & & X^4 & & \\ & & X^4 & & +X^2+X \\ \cline{3-5} & & & & X^2+X \quad \text{(remainder)} \end{array}$$

we obtain the remainder $\mathbf{b}(X) = X+X^2$. Thus, the code polynomial is $\mathbf{v}(X) = \mathbf{b}(X)+X^3\mathbf{u}(X) = X + X^2 + X^3 + X^6$, and the corresponding codeword is $\mathbf{v} = (0\,1\,1\,1\,0\,0\,1)$, where the four rightmost digits are the information digits. The 16 codewords in systematic form are listed in Table 5.2.

TABLE 5.2: A (7, 4) cyclic code in systematic form generated by $\mathbf{g}(X) = 1 + X + X^3$.

Message	Codeword	
(0000)	(0000000)	$0 = 0 \cdot \mathbf{g}(X)$
(1000)	(1101000)	$1 + X + X^3 = \mathbf{g}(X)$
(0100)	(0110100)	$X + X^2 + X^4 = X\mathbf{g}(X)$
(1100)	(1011100)	$1 + X^2 + X^3 + X^4 = (1 + X)\mathbf{g}(X)$
(0010)	(1110010)	$1 + X + X^2 + X^5 = (1 + X^2)\mathbf{g}(X)$
(1010)	(0011010)	$X^2 + X^3 + X^5 = X^2\mathbf{g}(X)$
(0110)	(1000110)	$1 + X^4 + X^5 = (1 + X + X^2)\mathbf{g}(X)$
(1110)	(0101110)	$X + X^3 + X^4 + X^5 = (X + X^2)\mathbf{g}(X)$
(0001)	(1010001)	$1 + X^2 + X^6 = (1 + X + X^3)\mathbf{g}(X)$
(1001)	(0111001)	$X + X^2 + X^3 + X^6 = (X + X^3)\mathbf{g}(X)$
(0101)	(1100101)	$1 + X + X^4 + X^6 = (1 + X^3)\mathbf{g}(X)$
(1101)	(0001101)	$X^3 + X^4 + X^6 = X^3\mathbf{g}(X)$
(0011)	(0100011)	$X + X^5 + X^6 = (X + X^2 + X^3)\mathbf{g}(X)$
(1011)	(1001011)	$1 + X^3 + X^5 + X^6 = (1 + X + X^2 + X^3)\mathbf{g}(X)$
(0111)	(0010111)	$X^2 + X^4 + X^5 + X^6 = (X^2 + X^3)\mathbf{g}(X)$
(1111)	(1111111)	$1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ $= (1 + X^2 + X^5)\mathbf{g}(X)$

5.2 GENERATOR AND PARITY-CHECK MATRICES OF CYCLIC CODES

Consider an (n, k) cyclic code C with generator polynomial $\mathbf{g}(X) = g_0 + g_1X + \cdots + g_{n-k}X^{n-k}$. In Section 5.1 we showed that the k code polynomials $\mathbf{g}(X), X\mathbf{g}(X), \cdots, X^{k-1}\mathbf{g}(X)$ span C. If the n-tuples corresponding to these k code polynomials are used as the rows of a $k \times n$ matrix, we obtain the following generator matrix for C:

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} & 0 & \cdot & \cdot & 0 \\ \cdot & & & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & & & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 0 & g_0 & g_1 & g_2 & \cdot & \cdot & \cdot & \cdot & \cdot & g_{n-k} \end{bmatrix}. \tag{5.9}$$

(Note that $g_0 = g_{n-k} = 1$.) In general, $\mathbf{G}$ is not in systematic form; however, we can put it into systematic form with row operations. For example, the (7, 4) cyclic code given in Table 5.1 with generator polynomial $\mathbf{g}(X) = 1 + X + X^3$ has the following matrix as a generator matrix:

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