BINARY CYCLIC CODES

Binary Cyclic codes was first studied by Prange in 1957.

Cyclic codes form an important subclass of linear codes. These codes are attractive for two reasons: first, encoding and syndrome computation can be implemented easily by employing shift registers with feedback connections (or linear sequential circuits); and second, because they have considerable inherent algebraic structure, it is possible to find various practical methods for decoding them.

If the components of an n-tuple v = $(v_0, v_1. . ., v_{n-1})$ are cyclically shifted 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 v. If the components of v are cyclically shifted i places to the right, the resultant n-tuple would be

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

Clearly, cyclically shifting v *i* places to the right is equivalent to cyclically shifting v_{n-i} places to the left.

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

The (7, 4) linear code given in Table 1 is a cyclic code. Cyclic codes form an important subclass of the linear codes and they possess many algebraic properties that simplify the encoding and the decoding implementations.

TABLE .1 A (7, 4) CYCLIC CODE GENERATED BY $\mathbf{g}(X) = 1 + X + X^3$

Messages	Code Vectors	Code polynomials
(0 0 0 0)	0 0 0 0 0 0 0	$\mathbf{0} = 0 \cdot \mathbf{g}(X)$
(1 0 0 0)	1 1 0 1 0 0 0	$1 + X + X^3 = 1 \cdot \mathbf{g}(X)$
(0 1 0 0)	0 1 1 0 1 0 0	$X + X^2 + X^4 = X \cdot \mathbf{g}(X)$
(1 1 0 0)	1 0 1 1 1 0 0	$1 + X^2 + X^3 + X^4 = (1 + X) \cdot \mathbf{g}(X)$
(0 0 1 0)	0 0 1 1 0 1 0	$X^2 + X^3 + X^5 = X^2 \cdot \mathbf{g}(X)$
(1 0 1 0)	1 1 1 0 0 1 0	$1 + X + X^2 + X^5 = (1 + X^2) \cdot \mathbf{g}(X)$
(0 1 1 0)	0 1 0 1 1 1 0	$X + X^3 + X^4 + X^5 = (X + X^2) \cdot \mathbf{g}(X)$
(1 1 1 0)	1 0 0 0 1 1 0	$1 + X^4 + X^5 = (1 + X + X^2) \cdot \mathbf{g}(X)$
(0 0 0 1)	0 0 0 1 1 0 1	$X^3 + X^4 + X^6 = X^3 \cdot \mathbf{g}(X)$
(1 0 0 1)	1 1 0 0 1 0 1	$1 + X + X^4 + X^6 = (1 + X^3) \cdot \mathbf{g}(X)$
(0 1 0 1)	0 1 1 1 0 0 1	$X + X^2 + X^3 + X^6 = (X + X^3) \cdot \mathbf{g}(X)$
(1 1 0 1)	1 0 1 0 0 0 1	$1 + X^2 + X^6 = (1 + X + X^3) \cdot \mathbf{g}(X)$
(0 0 1 1)	0 0 1 0 1 1 1	$X^2 + X^4 + X^5 + X^6 = (X^2 + X^3) \cdot \mathbf{g}(X)$
(1 0 1 1)	1 1 1 1 1 1 1	$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (1 + X^2 + X^3) \cdot \mathbf{g}(X)$
(0 1 1 1)	0 1 0 0 0 1 1	$X + X^5 + X^6 = (X + X^2 + X^3) \cdot \mathbf{g}(X)$
(1 1 1 1)	1 0 0 1 0 1 1	$1 + X^3 + X^5 + X^6 = (1 + X + X^2 + X^3) \cdot \mathbf{g}(X)$

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

$$\mathbf{v}(X) = v_0 + v_1 X + v_2 X^2 + \cdots + v_{n-1} X^{n-1}.$$

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

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

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

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

The equation above can be manipulated into the following form:

$$\begin{aligned} X^i \mathbf{v}(X) &= v_{n-i} + v_{n-i+1} X + \cdots + v_{n-1} X^{i-1} + v_0 X^i + \cdots + v_{n-i-1} X^{n-1} \\ &\quad + v_{n-i}(X^n + 1) + v_{n-i+1} X(X^n + 1) + \cdots + v_{n-1} X^{i-1}(X^n + 1) \\ &= \mathbf{q}(X)(X^n + 1) + \mathbf{v}^{(i)}(X), \qquad (.1) \end{aligned}$$

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

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

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

Every code polynomial v*(X)* in an *(n, k)* cyclic code can be expressed in the following form:

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

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

If g(X) is a polynomial of degree $n — k$ and is a factor of $X^n + 1$, then g(X) generates an *(n, k)* cyclic code.

Example 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; each generates a (7, 4) cyclic code. The (7, 4) cyclic code given by Table 1 is generated by $g(X) = 1 + X + X^3$. This code has minimum distance 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 $g(X) = 1 + X + X^3$.

For example, let u = (1010) be the message to be encoded. The corresponding message polynomial is $u(X) = 1 + X^2$. Multiplying u(X) *by* g(X) results in 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 code vector (1 1 1 0 0 1 0).

H.W: Construct Binary Cyclic codes of (4,7) using $g(X)=1+X^2+X^3$?

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

The corresponding message polynomial is

$$\mathbf{u}(X) = u_0 + u_1 X + \cdots + u_{k-1} X^{k-1}.$$

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

$$X^{n-k}\mathbf{u}(X) = u_0 X^{n-k} + u_1 X^{n-k+1} + \cdots + u_{k-1} X^{n-1}.$$

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

$$X^{n-k}\mathbf{u}(X) = \mathbf{a}(X)\mathbf{g}(X) + \mathbf{b}(X) \qquad 2)$$

Where *a(X)* and *b(X)* are the quotient and the remainder, respectively. Since the degree of *g(X)* is $n — k$, the degree of *b(X)* must be $n — k — 1$ or less, that is,

$$\mathbf{b}(X) = b_0 + b_1 X + \cdots + b_{n-k-1} X^{n-k-1}.$$

Rearranging (2), we obtain the following polynomial of degree n — 1 or less:

$$\mathbf{b}(X) + X^{n-k}\mathbf{u}(X) = \mathbf{a}(X)\mathbf{g}(X). \qquad ...(3)$$

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

$$\mathbf{b}(X) + X^{n-k}\mathbf{u}(X) = b_0 + b_1 X + \cdots + b_{n-k-1} X^{n-k-1} + u_0 X^{n-k} + u_1 X^{n-k+1} + \cdots + u_{k-1} X^{n-1}, \qquad ....(4)$$

Which corresponds to the code vector

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

We see that the code vector consists of *k* unaltered information digits $(u_0, u_u \ldots, u_{k-1})$ 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} u(X) by the generator polynomial g(X). The process above yields an (n, *k)* cyclic code in systematic form.

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

$$\begin{array}{r l}
 & X^3 + X \quad \text{(quotient)} \\
X^3 + X + 1 \,\big) & X^6 \qquad\qquad + X^3 \\
 & \underline{X^6 \quad + X^4 + X^3} \\
 & \qquad\quad X^4 \\
 & \qquad\quad \underline{X^4 \qquad + X^2 + X} \\
 & \qquad\qquad\qquad X^2 + X \quad \text{(remainder)},
\end{array}$$

We obtain the remainder $b(X) = X + X^2$. Thus, the code polynomial is $v(X) = b(X) + X^3u(X) = X + X^2 + X^3 + X^6$ and the corresponding code vector is v = (0 1 1 1 0 0 1), where the four rightmost digits are the information digits. The 16 code vectors in systematic form are listed in Table 2.

GENERATOR AND PARITY CHECK MATRICE 0F CYCLIC CODES

To construct the 4 by 7 generator generator matrix G , we start with four polynomials represented by g(X) and three cyclic shifted versions of it as shown by:-

$$g(X) = 1 + X + X^3 \qquad \text{(zero shift)}$$

$$X \bullet g(X) = X + X^2 + X^4 \qquad \text{(1 – cyclic shift).}$$
$$X^2 \bullet g(X) = X^2 + X^3 + X^5 \qquad \text{(2 – cyclic shift).}$$
$$X^3 \bullet g(X) = X^3 + X^4 + X^6 \qquad \text{(3 – cyclic shift).}$$

If the coefficients of these polynomials are used as elements of the rows of a 4 by 7 matrix, we got:-

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

TABLE 2 A (7, 4) CYCLIC CODE GENERATED BY $g(X) = 1 + X + X^3$

Message	Code word	
(0 0 0 0)	(0 0 0 0 0 0 0)	$0 = 0 \cdot g(X)$
(1 0 0 0)	(1 1 0 1 0 0 0)	$1 + X + X^3 = g(X)$
(0 1 0 0)	(0 1 1 0 1 0 0)	$X + X^2 + X^4 = Xg(X)$
(1 1 0 0)	(1 0 1 1 1 0 0)	$1 + X^2 + X^3 + X^4 = (1 + X)g(X)$
(0 0 1 0)	(1 1 1 0 0 1 0)	$1 + X + X^2 + X^5 = (1 + X^2)g(X)$
(1 0 1 0)	(0 0 1 1 0 1 0)	$X^2 + X^3 + X^5 = X^2g(X)$
(0 1 1 0)	(1 0 0 0 1 1 0)	$1 + X^4 + X^5 = (1 + X + X^2)g(X)$
(1 1 1 0)	(0 1 0 1 1 1 0)	$X + X^3 + X^4 + X^5 = (X + X^2)g(X)$
(0 0 0 1)	(1 0 1 0 0 0 1)	$1 + X^2 + X^6 = (1 + X + X^3)g(X)$
(1 0 0 1)	(0 1 1 1 0 0 1)	$X + X^2 + X^3 + X^6 = (X + X^3)g(X)$
(0 1 0 1)	(1 1 0 0 1 0 1)	$1 + X + X^4 + X^6 = (1 + X^3)g(X)$
(1 1 0 1)	(0 0 0 1 1 0 1)	$X^3 + X^4 + X^6 = X^3g(X)$
(0 0 1 1)	(0 1 0 0 0 1 1)	$X + X^5 + X^6 = (X + X^2 + X^3)g(X)$
(1 0 1 1)	(1 0 0 1 0 1 1)	$1 + X^3 + X^5 + X^6 = (1 + X + X^2 + X^3)g(X)$
(0 1 1 1)	(0 0 1 0 1 1 1)	$X^2 + X^4 + X^5 + X^6 = (X^2 + X^3)g(X)$
(1 1 1 1)	(1 1 1 1 1 1 1)	$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = (1 + X^2 + X^5)g(X)$

If the first row is added to the third row and the sum of the first two rows is added to the fourth row, we obtain the following matrix:

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

Which is in systematic form. This matrix generates the same code as G.

'The generator matrix in systematic form can also be formed easily. Dividing X^{n-k+i} by the generator polynomial $\mathbf{g}(X)$ for $i = 0, 1, \ldots, k-1$, we obtain

$$X^{n-k+i} = \mathbf{a}_i(X)\mathbf{g}(X) + \mathbf{b}_i(X),$$

where $\mathbf{b}_i(X)$ is the remainder with the following form:

$$\mathbf{b}_i(X) = b_{i0} + b_{i1}X + \cdots + b_{i,n-k-1}X^{n-k-1}.$$

Since $\mathbf{b}_i(X) + X^{n-k+i}$ for $i = 0, 1, \ldots, k-1$ are multiples of $\mathbf{g}(X)$, they are code polynomials. Arranging these k code polynomials as rows of a $k \times n$ matrix, we obtain

$$\mathbf{G}=\begin{bmatrix} b_{00} & b_{01} & b_{02} & \cdots & b_{0,n-k-1} & 1 & 0 & 0 & \cdots & 0 \\ b_{10} & b_{11} & b_{12} & \cdots & b_{1,n-k-1} & 0 & 1 & 0 & \cdots & 0 \\ b_{20} & b_{21} & b_{22} & \cdots & b_{2,n-k-1} & 0 & 0 & 1 & \cdots & 0 \\ & \vdots & & & \vdots & & & & & \vdots \\ b_{k-1,0} & b_{k-1,1} & b_{k-1,2} & \cdots & b_{k-1,n-k-1} & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}, \quad \ldots.(5)$$

which is the generator matrix of C in systematic form. The corresponding parity-check matrix for C is

$$\mathbf{H}=\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & b_{00} & b_{10} & b_{20} & \cdots & b_{k-1,0} \\ 0 & 1 & 0 & \cdots & 0 & b_{01} & b_{11} & b_{21} & \cdots & b_{k-1,1} \\ 0 & 0 & 1 & \cdots & 0 & b_{02} & b_{12} & b_{22} & \cdots & b_{k-1,2} \\ & \vdots & & & & & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & b_{0,n-k-1} & b_{1,n-k-1} & b_{2,n-k-1} & \cdots & b_{k-1,n-k-1} \end{bmatrix}. \quad \ldots(6)$$

Example 3

Again, let us consider the (7, 4) cyclic code generated by $\mathbf{g}(X) = 1 + X + X^3$. Dividing X^3, X^4, X^5, and X^6 by $\mathbf{g}(X)$, we have

$$X^3 = \mathbf{g}(X) + (1 + X),$$

$$X^4 = X\mathbf{g}(X) + (X + X^2),$$

$$X^5 = (X^2 + 1)\mathbf{g}(X) + (1 + X + X^2),$$

$$X^6 = (X^3 + X + 1)\mathbf{g}(X) + (1 + X^2).$$

Rearranging the equations above, we obtain the following four code polynomials:

$$\mathbf{v}_0(X) = 1 + X \qquad + X^3,$$

$$\mathbf{v}_1(X) = \qquad X + X^2 \qquad + X^4,$$

$$\mathbf{v}_2(X) = 1 + X + X^2 \qquad\qquad + X^5,$$

$$\mathbf{v}_3(X) = 1 \qquad + X^2 \qquad\qquad\qquad + X^6.$$

Taking these four code polynomials as rows of a 4×7 matrix, we obtain the following generator matrix in systematic form for the (7, 4) cyclic code:

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

which is identical to the matrix $\mathbf{G}'$ obtain earlier in this section.

EXAMPLE 4 : Construct Parity Check Matrix H of example 2?
We simply find the party polynomial H(X) as follow:

$$\mathbf{h}(X) = \frac{X^7 + 1}{\mathbf{g}(X)}$$

$$= 1 + X + X^2 + X^4.$$

The reciprocal of $\mathbf{h}(X)$ is

$$X^4\mathbf{h}(X^{-1}) = X^4(1 + X^{-1} + X^{-2} + X^{-4}).$$

$$= 1 + X^2 + X^3 + X^4.$$

Also $X^5 \bullet h(X^{-1}) = X + X^3 + X^4 + X^5$,
And $X^6 \bullet h(X^{-1}) = X^2 + X^4 + X^5 + X^6$.

Then using the coefficients of these three equations as the elements of the rows of the 3 by 7 parity check matrix, we got

$$H' = \begin{matrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}$$

Here H' is not in systematic form therefore we must put it into a systematic by add 3rd row with the 1st row to obtain :-

$$H = \begin{matrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{matrix}$$