38. Polynomial Description of Cyclic Codes

Most of the known good codes belong to a class of codes called linear codes. However, the implementation complexity of decoders becomes impractical for linear codes with very large block length n. Linear codes with an extra degree of algebraic structure are most welcome, in the hope that the decoding complexity can be reduced. Cyclic codes offer such additional structure.

Cyclic codes form an important subclass of linear codes. These codes are important because their underlying Galois field description leads to encoding and decoding procedures that are computationally efficient. The treatment here will concentrate on the basic principles of binary cyclic codes and the syndrome decoding of the codes [1].

Polynomial Description of Cyclic Codes

Definition 38.1. An (n, k) linear code is cyclic if every cyclic shift of a codeword (codevector) is also a codeword (codevector) in the code.

A cyclic shift of a codeword of length n, represented by an n-tuple codevector $\mathbf{V} = [v_0 \ v_1 \ \ldots \ v_{n-1}]$, j times to the right is another n-tuple codevector $\mathbf{V}^{(j)} = [v_{n-j}, v_{n-j+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-j-1}]$. Clearly, cyclically shifting $\mathbf{V}$ j places to the right is the same as cyclically shifting $\mathbf{V}$ n-j places to the left. For convenience, we always shift $\mathbf{V}$ to the right.

Example 38.1

$\mathbf{V} = [v_0 \ v_1 \ v_2 \ v_3]$
$= [1 \ 0 \ 1 \ 1]$

$\mathbf{V}^{(2)} = [1 \ 1 \ 1 \ 0]$.

The codevector of a cyclic code may also be expressed in polynomial form with indeterminate x.

$$v(x) = v_{n-1}x^{n-1} + v_{n-2}x^{n-2} + \ldots + v_1x + v_0. \qquad (38.1)$$

$v(x)$ is called the code polynomial of the codevector $\mathbf{V}$. For (n, k) cyclic codes, the code polynomial has a degree of n-1 ($v_{n-1} \neq 0$) or less ($v_{n-1} = 0$). Clearly, the code polynomial that corresponds to the codevector $\mathbf{V}^{(j)}$ is

$$v^{(j)}(x) = v_{n-j-1}x^{n-1} + v_{n-j-2}x^{n-2} + \ldots + v_1x^{j+1} + v_0x^j + v_{n-1}x^{j-1} + v_{n-2}x^{j-2} + \ldots + v_{n-j+1}x + v_{n-j} \quad (38.2)$$

$v(x)$ has the following property.

$$x^j v(x) = q(x)(x^n - 1) + v^{(j)}(x) \quad (38.3)$$

where

$$q(x) = v_{n-1}x^{j-1} + v_{n-2}x^{j-2} + \ldots + v_{n-j+1}x + v_{n-j} \quad (38.4)$$

and $v^{(j)}(x)$ is the remainder of $x^j v(x) / (x^n - 1)$, denoted as $\text{Rem}\{x^j v(x) /(x^n - 1)\}$.

An (n, k) cyclic code may be defined in terms of a *generator polynomial* $g(x)$, where

$$g(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \ldots + g_1x + g_0 \quad (38.5)$$

and $g_i \in GF(q)$ for $0 \leq i \leq (n - k)$. $g(x)$ is unique and of minimum degree, because a new polynomial of degree less than $n - k$ can only be constructed by subtraction (modulo-2 addition for binary codes) of $g(x)$ of degree $n - k$ and a polynomial of the same degree if that polynomial exists. All the parameters of a cyclic code can be determined from its generator polynomial $g(x)$. It can be shown that the code polynomial, $v(x)$, is a multiple of $g(x)$ [1]. Furthermore, the code has the following properties:

Theorem 38.1. The generator polynomial $g(x)$ of minimum degree $n - k$ of a (n, k) cyclic code divides $x^n - 1$.

Proof. Dividing $x^n - 1$ by $g(x)$, we get $x^n - 1 = h(x)g(x) + b(x)$, where $h(x)$ is the quotient and $b(x)$ is the remainder. The remainder $b(x)$ can be expressed as $b(x) \equiv [(x^n - 1) - h(x)g(x)]$ modulo-$(x^n - 1) \equiv - h(x)g(x)$ modulo-$(x^n - 1)$. Since $h(x)g(x)$ is a code polynomial, the remainder $b(x)$ is also a code polynomial and has a degree less than the degree of $g(x)$. But the generator polynomial $g(x)$ of minimum degree is unique, the only such code polynomial of degree less than the degree of $g(x)$ is $b(x) = 0$. This says $x^n - 1 = h(x)g(x)$ and $g(x)$ divides $x^n - 1$. □

For large n, $x^n - 1$ may have many factors of degree n-k. Some of these factors (polynomials) generate good cyclic codes and some generate bad cyclic codes.

Let $u(x)$ be the information polynomial of the information vector $\mathbf{U} = [u_0\ u_1\ \ldots\ u_{k-1}]$, where

$$u(x) = u_{k-1}x^{k-1} + u_{k-2}x^{k-2} + \ldots + u_1x + u_0 \tag{38.6}$$

and $u_i \in GF(q)$ for $0 \le i \le (k - 1)$. The encoding operation can be expressed as

$$v(x) = u(x)\, g(x) \tag{38.7}$$

Since the generator polynomial $g(x)$ of degree n-k for an (n, k) cyclic code divides $x^n - 1$, we can write

$$x^n - 1 = h(x)g(x) \tag{38.8}$$

where

$$h(x) = h_kx^k + h_{k-1}x^{k-1} + \ldots + h_1x + h_0 \tag{38.9}$$

and $h_j \in GF(q)$ for $0 \le j \le k$. $h(x)$ is called the *parity-check polynomial* of an (n, k) cyclic code.

Theorem 38.2. Let $g(x)$ of minimum degree n-k and $h(x)$ of degree k be the generator and parity-check polynomials of an (n, k) cyclic code C, respectively. $C^{\perp}$, the dual code of C, is generated by the polynomial $g^{\perp}(x) = x^k h(x^{-1}) = h_0x^k + h_1x^{k-1} + \ldots + h_{k-1}x + h_k$ of degree k, where $x^k h(x^{-1})$ is the *reciprocal polynomial* of $h(x)$.

Proof. By Theorem 38.1, the generator polynomial $g(x)$ of minimum degree n-k for an (n, k) cyclic code divides $x^n - 1$, we can write $x^n - 1 = h(x)g(x)$. $x^n - 1 = h(x)g(x)$ implies

$$x^{-n} - 1 = h(x^{-1})g(x^{-1})$$
$$1 - x^n = x^n\, h(x^{-1})g(x^{-1})$$
$$-(x^n - 1) = x^k h(x^{-1})x^{n-k}g(x^{-1}).$$

Thus, $x^k h(x^{-1})$ divides $x^n - 1$ and the polynomial $x^k h(x^{-1})$ of degree k is the generator polynomial for the dual code of C. □

There is an interesting relationship between the weight structure of a code and the weight structure of its dual code. Let a polynomial $A(x) = A_n x^n + A_{n-1}x^{n-1} + ... + A_1 x + A_0$ be the *weight enumerator* of an (n, k) linear code, where A_i denotes the number of codewords of weight i in the (n, k) linear code. Also, let $B(x) = B_n x^n + B_{n-1}x^{n-1} + ... + B_1 x + B_0$ be the weight enumerator of its dual code, where B_i denotes the number of codewords of weight i in the $(n, n - k)$ dual code. The weight enumerator $A(x)$ is related to $B(x)$ by the MacWilliams identity [2] as

$$A(x) = 2^{-(n-k)}(x+1)^n B\left[\frac{-(x-1)}{x+1}\right] \qquad (38.10)$$

Often, the weight distribution of a code is not readily determined, but the weight distribution of its dual code is known. In this case, we can determine the weight distribution of the code from its dual code, and the probability of undetected word error of the code.

Given $g(x)$ of an (n, k) cyclic code, we can put the code into systematic form. Let $u(x) = u_{k-1}x^{k-1} + u_{k-2}x^{k-2} + ... + u_1 x + u_0$ be an information polynomial. Dividing $x^{n-k}u(x)$ by $g(x)$, we get $x^{n-k}u(x) = a(x)g(x) + b(x)$, where $a(x)$ is the quotient and $b(x) = b_{n-k-1}x^{n-k-1} + b_{n-k-2}x^{n-k-2} + ... + b_1 x + b_0$ is the remainder. Write $x^{n-k}u(x) - b(x) = a(x)g(x)$. Since $a(x)g(x)$ is a code polynomial, this implies $x^{n-k}u(x) - b(x)$ is also a code polynomial. Hence, systematic encoding of cyclic codes consists of the following operations:

1. Form $x^{n-k}u(x)$.

2. Find the remainder $b(x)$ from $x^{n-k}u(x) / g(x)$.

3. Form

$$v(x) = x^{n-k}u(x) - b(x) \qquad (38.11)$$

where

$$b(x) = b_{n-k-1}x^{n-k-1} + b_{n-k-2}x^{n-k-2} + ... + b_1 x + b_0. \qquad (38.12)$$

Substituting equations (38.6) and (38.12) into equation (38.11), we get

$$\begin{aligned} v(x) = \quad & u_{k-1}x^{n-1} + u_{k-2}x^{n-2} + \ldots + u_1x^{n-k+1} + u_0x^{n-k} \\ & -b_{n-k-1}x^{n-k-1} - b_{n-k-2}x^{n-k-2} - \ldots - b_1x - b_0 \end{aligned} \qquad (38.13)$$

For binary cyclic codes, $-b_i = b_i$ and $0 \le i \le n - k - 1$.

Example 38.2

An (7, 4) binary cyclic code generated by $g(x) = x^3 + x + 1$. Given $u(x) = x^3 + x^2 + x$, find $v(x)$.

1. $x^{7-4}u(x) = x^6 + x^5 + x^4$.

2. By long division and modulo-2 addition, the remainder

   $b(x) = \text{Rem}\ \{x^{7-4}u(x) / g(x)\} = x^2$.

3. $v(x) = x^{7-4}u(x) + b(x)$
   $= x^6 + x^5 + x^4 + x^2$.

The generator polynomial $g(x)$ of degree 3 generates an (7, 4) binary cyclic code because $g(x)$ divides $x^{n=7} + 1$.

$$\begin{array}{rl} & x^4 + x^2 + x + 1 \\ \hline x^3+x+1 \ ) & x^7 \qquad\qquad\qquad\qquad\quad +1 \\ & x^7 + x^5 + x^4 \\ \hline & \quad x^5 + x^4 \\ & \quad x^5 \qquad + x^3 + x^2 \\ \hline & \qquad\quad x^4 + x^3 + x^2 \\ & \qquad\quad x^4 \qquad + x^2 + x \\ \hline & \qquad\qquad\quad x^3 \qquad + x + 1 \\ & \qquad\qquad\quad x^3 \qquad + x + 1 \\ \hline \end{array}$$

Matrix Description of Cyclic Codes

A convenient way to construct the generator matrix from the generator polynomial of an (n, k) q-ary cyclic code is as follows. Let $g(x) = g_{n-k}x^{n-k} + g_{n-k-1}x^{n-k-1} + \ldots + g_1x + g_0$ be the generator polynomial of an (n, k) cyclic code C. The code polynomials are of the form $v(x) = u(x)g(x) = u_{k-1}x^{k-1}g(x) + u_{k-2}x^{k-2}g(x) + \ldots + u_1xg(x) + u_0g(x)$, and there are q^k number of code polynomials. Putting the coefficients of the code polynomials $g(x)$, $xg(x)$, ..., $x^{k-1}g(x)$ in vector form, we have

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \vdots \\ \mathbf{G}_{k-1} \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & & \vdots \\ 0 & 0 & & \cdots & g_0 & g_1 & \cdots & g_{n-k} & 0 \\ 0 & 0 & & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix} \tag{38.14}$$

The set of k row vectors of the k-by-n matrix $\mathbf{G}$ are linearly independent vectors and all the linear combinations of $\mathbf{G}_0$, $\mathbf{G}_1$, ..., $\mathbf{G}_{k-1}$ of the form $\mathbf{V} = u_0\,\mathbf{G}_0 + u_1\,\mathbf{G}_1 + \ldots + u_{k-1}\,\mathbf{G}_{k-1}$ form a k-dimensional subspace of the vector space of all n-tuples over $GF(q)$. $\mathbf{G}$ as constructed is indeed a generator matrix of an (n, k) cyclic code C.

In a similar fashion, we can form an $(n\text{-}k)$-by-n matrix $\mathbf{H}$ from the generator polynomial $x^k h(x^{-1})$ of code $C^{\perp}$, where

$$\mathbf{H} = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & & \vdots \\ 0 & 0 & & \cdots & h_k & h_{k-1} & \cdots & h_0 & 0 \\ 0 & 0 & & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix} \tag{38.15}$$

$\mathbf{H}$ is the generator matrix of the dual code $C^{\perp}$. Any codevector in C is orthogonal to every row of $\mathbf{H}$. Thus, $\mathbf{H}$ is the parity-check matrix of the code C.

Given $g(x)$ of an (n, k) cyclic code, we can also put the code generator matrix into systematic form $\mathbf{G}_{SEF}$. Recall equation (38.11)

$$v(x) = x^{n-k}u(x) - b(x) \tag{38.16}$$

where

$$b(x) = \text{Rem}\ \{x^{n-k}u(x) / g(x)\} \tag{38.17}$$

which transforms the cyclic code into systematic form. Suppose we form a remainder $b_i(x)$ from $x^{n-k+i}\ u(x) / g(x)$, we obtain

$$a_i(x)g(x) = x^{n-k+i}u(x) - b_i(x), \tag{38.18}$$

$a_i(x)g(x)$ is a multiple of $g(x)$; i.e., a code polynomial corresponding to a codevector (codeword) for $0 \le i \le k\text{-}1$ and

$$b_i(x) = b_{i,n-k-1}x^{n-k-1} + b_{i,n-k-2}x^{n-k-2} + \ldots + b_{i,1}x + b_{i,0}. \tag{38.19}$$

The codevector form of $x^{n-k+i}\ u(x) - b_i(x)$ is

$$\mathbf{V}_i = [-b_{i,0}\ \ -b_{i,1}\ \ \ldots\ -b_{i,n-k-1}\ \ u_0\ \ u_1\ \ \ldots\ u_i\ \ \ldots\ u_{k-1}] \tag{38.20}$$

with $u_i = 1$ and $u_j = 0$ for $j \ne i$. Cyclically shifting the vector $\mathbf{V}_i$ k times to the right, we get $\mathbf{V}_i^{(k)} = [u_0\ \ u_1\ \ \ldots\ u_i\ \ \ldots\ u_{k-1}\ -b_{i,0}\ \ -b_{i,1}\ \ \ldots\ -b_{i,n-k-1}]$. By placing the vector $\mathbf{V}_i^{(k)}$ as the i-th row of $\mathbf{G}_{\text{SEF}}$, we obtain

$$\mathbf{G}_{\text{SEF}} = \begin{bmatrix} 1 & 0 & \ldots & 0 & -b_{0,0} & -b_{0,1} & \ldots & -b_{0,n-k-1} \\ 0 & 1 & \ldots & 0 & -b_{1,0} & -b_{1,1} & \ldots & -b_{1,n-k-1} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 1 & -b_{k-1,0} & -b_{k-1,1} & \ldots & -b_{k-1,n-k-1} \end{bmatrix} \tag{38.21}$$

which is the generator matrix of code C in systematic form. The corresponding systematic parity-check matrix $\mathbf{H}_{\text{SEF}}$ is

$$\mathbf{H}_{\text{SEF}} = \begin{bmatrix} b_{0,0} & b_{1,0} & \ldots & b_{k-1,0} & 1 & 0 & \ldots & 0 \\ b_{0,1} & b_{1,1} & \ldots & b_{k-1,1} & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ b_{0,n-k-1} & b_{1,n-k-1} & \ldots & b_{k-1,n-k-1} & 0 & 0 & \ldots & 1 \end{bmatrix} \tag{38.22}$$

We can also obtain the standard-echelon-form $\mathbf{G}_{\text{SEF}}$ from the generator matrix $\mathbf{G}$ of the code by row/column transformations. For an (n, k) cyclic code, we only perform row interchange and combination operations on the generator matrix $\mathbf{G}$ to obtain $\boldsymbol{G}_{\text{SEF}}$.

Column interchange and combination operations are not possible, as this destroys the cyclic properties of the code. $\mathbf{H}_{SEF}$ can then be found by taking the corresponding elements in $\mathbf{G}_{SEF}$ as the elements in $\mathbf{H}_{SEF}$ according to equations (38.21) and (38.22).

Example 38.3

Given the generator matrix of an (7, 4) binary cyclic code of $\mathbf{G} = \begin{bmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \mathbf{G}_2 \\ \mathbf{G}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$, the standard-echelon-form of $\mathbf{G}$ is

$$\mathbf{G}_{SEF} = \begin{bmatrix} \mathbf{G}'_0 \\ \mathbf{G}'_1 \\ \mathbf{G}'_2 \\ \mathbf{G}'_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

where $\mathbf{G}'_0 := \mathbf{G}_0 + \mathbf{G}_1 + \mathbf{G}_2$, $\mathbf{G}'_1 := \mathbf{G}_1 + \mathbf{G}_2 + \mathbf{G}_3$, $\mathbf{G}'_2 := \mathbf{G}_2 + \mathbf{G}_3$, $\mathbf{G}'_3 := \mathbf{G}_3$ and

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

References

[1] Lee, L. H. C., Error-Control Block Codes for Communications Engineers, Artech House, 2000.

[2] MacWilliams, F. J., "A Theorem on the Distribution of Weights in a Systematic Code," *Bell System Techical Journal*, Vol. 42, 1963, pp. 79-94.