Cyclic Codes

Introduction

Binary cyclic codes form a subclass of linear block codes.

Easier to encode and decode

Definition

A (n, k) linear block code C is called a cyclic code if

1. The sum of any two codewords in the code is also a codeword. (Linear)

Example: $C_i + C_j = C_k$

2. Any cyclic shift of a codeword in the code is also a codeword. (Cyclic)

Example: If $C = [C_0 \quad C_1 \quad \cdots \quad C_{n-1}]$ is a codeword,

$$
\begin{aligned}
C^{(1)} &= [C_{n-1} \quad C_0 \quad \cdots \quad C_{n-3} \quad C_{n-2}] \\
C^{(2)} &= [C_{n-2} \quad C_{n-1} \quad \cdots \quad C_{n-4} \quad C_{n-3}] \\
&\vdots \\
C^{(n-1)} &= [C_1 \quad C_2 \quad \cdots \quad C_{n-1} \quad C_0]
\end{aligned}
$$

are also codewords.

C and $C^{(i)}$

We can represent the code word $C=[C_0\ C_1\ \ldots\ C_{n-1}]$ by a code polynomial

$$C(X) = C_0 + C_1 X + C_2 X^2 + \ldots + C_{n-1} X^{n-1}$$

The coefficients $C_i = \{0, 1\}$ and each power of X in the polynomial $C(X)$ represents a one-bit shift in time. Hence, multiplication of the polynomial $C(X)$ by X may be viewed as a shift to the right.

Example: $C= [1101]$ can be represented by

$$C(X) = 1 + X + X^3$$

$C^{(i)}(X)$ is recognized as the code polynomial of the code word $[C_{n-i}\ \ldots\ C_{n-1}\ C_0\ C_1\ \ldots\ C_{n-i-1}]$ obtained by applying i cyclic shifts to the code word $[C_0\ C_1\ \ldots\ C_{n-1}]$.

It can be shown that $C^{(i)}(X)$ is the **remainder** resulting from dividing $X^i C(X)$ by $X^n + 1$. That is,

$$X^i C(X) = q(X)\,(X^n + 1) + C^{(i)}(X)$$

where $q(X) = C_{n-i} + C_{n-i+1} X + \ldots.. + C_{n-1} X^{i-1}$

Example:

C=[0111110] $\Longrightarrow$ $C(X) = X+X^2+X^3+X^4+X^5$

$X^2C(X) = X^3+X^4+X^5+X^6+X^7$

Remainder

$$
\begin{array}{r l}
 & 1 \\
X^7+1 \,\big)\!\! & \overline{X^7+X^6+X^5+X^4+X^3} \\
 & \underline{X^7+1} \\
 & \quad X^6+X^5+X^4+X^3+1
\end{array}
$$

$X^6+X^5+X^4+X^3+1$ $\Longrightarrow$ $C^{(2)} = [1001111]$

Therefore, if $C(X)$ is a code polynomial, then the polynomial

$$\boxed{c^{(i)}(X) = X^i C(X) \bmod (X^n+1) \qquad \text{mod} \equiv \text{modulo}}$$

is also a code polynomial for any cyclic shift i.

Generator Polynomial

Theorem

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 in which the code polynomial $C(X)$ for a data vector $M = [\ m_0\ \ m_1\ m_2\ \ldots\ m_{k-1}\ ]$ is generated by $C(X) = M(X)\ g(X)$

where $C(X) = C_0 + C_1 X + C_2 X^2 + \ldots + C_{n-1} X^{n-1}$

$$M(X) = m_0 + mX + m_2 X^2 + \ldots + m_{k-1} X^{k-1}$$

$$g(X) = g_0 + g_1 X + g_2 X^2 + \ldots + g_{n-k} X^{n-k}$$

$g(X)$ is the generating polynomial

Example

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

we can use either $(1 + X + X^3)$ or $(1 + X^2 + X^3)$ to generate a **(7, 4)** cyclic code.

For $M = [1\ 0\ 0\ 1]$ and $g(X) = (1 + X + X^3)$.

$$C(X) = M(X)g(X) = (1 + X^3)(1 + X + X^3)$$
$$= 1 + X + X^4 + X^6$$

$C = [1100101] \neq [\mathbf{b}:\mathbf{m}]$ (not systematic)

The remaining code vectors are

Message	Code vectors obtained using $C(X)=M(X)g(X)$	
0 0 0 0	0 0 0 0 0 0 0	
0 0 0 1	0 0 0 1 1 0 1	Right-shifted **6** bit
0 0 1 0	0 0 1 1 0 1 0	
0 0 1 1	0 0 1 0 1 1 1	Right-shifted **5** bit
0 1 0 0	0 1 1 0 1 0 0	Right-shifted **2** bit
0 1 0 1	0 1 1 1 0 0 1	
0 1 1 0	0 1 0 1 1 1 0	Right-shifted **4** bit
0 1 1 1	0 1 0 0 0 1 1	
1 0 0 0	1 1 0 1 0 0 0	
:	:	

Systematic cyclic code generation

Suppose we are given the generator polynomial $g(X)$ and the requirement is to encode the message sequence $(m_0, m_1, \ldots, m_{k-1})$ into an (n, k) systematic cyclic code. That is, the message bits are transmitted in unaltered form, as shown by the following structure for a code word

$$(\underbrace{b_0, b_1, \ldots, b_{n-k-1}}_{n-k \text{ parity bits}}, \quad \underbrace{m_0, m_1, \ldots, m_{k-1}}_{k \text{ message bits}})$$

Let the message polynomial be defined by

$$M(X) = m_0 + m_1 X + \ldots + m_{k-1} X^{k-1}$$

and let $B(X) = b_0 + b_1 X + \ldots + b_{n-k-1} X^{n-k-1}$

We want the code polynomial to be in the form

$$C(X) = B(X) + X^{n-k} M(X)$$

Hence,

$$A(X)g(X) = B(X) + X^{n-k} M(X)$$

Equivalently, we may write

$$\frac{X^{n-k}M(X)}{g(X)} = A(X) + \frac{B(X)}{g(X)}$$

This equation states that the polynomial $B(X)$ is the **remainder** left over after dividing $X^{n-k}M(X)$ by $g(x)$.

We may now summarize the steps involved in the encoding procedure for an (n, k) cyclic code assured of a systematic structure. Specifically, we proceed as follows:

1. Multiply the message polynomial $M(X)$ by X^{n-k}.

2. Divide $X^{n-k}M(X)$ by the generator polynomial $g(X)$, obtaining the remainder $B(X)$.

3. Add $B(X)$ to $X^{n-k}M(X)$ obtaining the code polynomial $C(X)$.

Example

Consider the (7,4) cyclic code in CC.8:

For $M = [1\ 1\ 1\ 0]$ and $g(X) = (1 + X + X^3)$.

$$M(X) = 1 + X + X^2$$

$$X^{n-k}M(X) = X^3(1 + X + X^2) = X^3 + X^4 + X^5$$

The division of $X^3 + X^4 + X^5$ by $g(X) = (1 + X + X^3)$. can be done as

$$\begin{array}{r} X^2 + X \\ X^3 + X + 1 \overline{\smash{\big)}\, X^5 + X^4 + X^3} \\ \underline{X^5 + X^3 + X^2 } \\ X^4 + X^2 \\ \underline{X^4 + X^2 + X} \\ X \end{array}$$

(Subtraction is the same as addition in modulo-2 arithmetic)

Hence, $B(X) = X$ and then $C(X) = B(X) + X^{n-k}M(X)$

$$= X + X^3 + X^4 + X^5$$

$$C = [0101110]$$