CODING THEORY
UNIT-III
Cyclic Codes
CSE 2052

Jayaprakash Kar

Table of contents

Cyclic Codes

Definition

A code C is said to be **Cyclic** if

1. C is linear code and,
2. any cyclic shift of a codeword is also a codeword, $i.e$ if the codeword $a_0 a_1 \dots a_{n-1}$ is in C then $a_{n-1} a_0 \dots a_{n-2}$ is also in C

Example-I

The binary code $C_1 = \{0000, 0101, 1010, 1111\}$ is a cyclic code. However $C_2 = \{0000, 0110, 1001, 1111\}$ is not a cyclic code, but is equivalent to the first code.
The $(5, 2)$ linear code $C_3 = \{00000, 01101, 11010, 10111\}$ is also not cyclic.

Division algorithm for polynomial

Definition

Let $f(x)$ is a fixed polynomial in $F[x]$. Two polynomials $g(x)$ and $h(x)$ in $F[x]$ are said to be **congruent modulo** $f(x)$, depicted by $g(x) \equiv h(x) \bmod f(x)$ if $g(x) - h(x)$ is divisible by $f(x)$.

Division algorithm for polynomial(Cont..)

Let us denote $F[x]/f(x)$ as the set of polynomials in $F[x]$ of degree less than deg $f(x)$, which addition and multiplication carried out modulo $f(x)$ as follows:

1. If $a(x)$ and $b(x)$ belongs to $F[x]/f(x)$, then the sum $a(x) + b(x)$ in $F[x]/f(x)$ is the same as in $F[x]$. This is because of deg $a(x) <$ deg $f(x)$ and deg $b(x) <$ deg $f(x)$ and therefore deg $(a(x) + b(x)) <$ deg $f(x)$.
2. The product $a(x)b(x)$ is unique polynomial of degree less than deg $f(x)$ to which $a(x)b(x)$ (the multiplication being carried out in $F[x]$) is congruent modulo $f(x)$.

Construction of code

A codeword can uniquely be represented by a polynomial. A codeword consists of a sequence of elements. We can use a polynomial to represent the locations and the values of all the elements in the codeword. *e.g*, the codeword $c_0 c_1 \dots c_{n-1}$ can be represented by the polynomial
$c(x) = \; c_0 + c_1 x + c_2 x^2 + \cdots c_{n-1} x^{n-1}$. Another example, the codeword

over $GF(8)$, $c = 207735$ can be represented by the polynomial $c(x) = 2 + 7x^2 + 7x^3 + 3x^4 + 5x^5$.

Construction of Cyclic code

A code C in R_n is a cyclic code if and only if C satisfies the following conditions

1. $a(x), b(x) \in C \implies a(x) + b(x) \in C$
2. $a(x) \in C$ and $r(x) \in R_n \implies a(x)r(x) \in C$

A method for generating Cyclic Codes

1. Take a polynomial $f(x) \in R_n$
2. Obtain a set of polynomials by multiplying $f(x)$ by all possible polynomials in R_n
3. The set polynomials obtained above corresponds to the set of codewords belonging to cyclic code. The block length of code is n.

Example

Consider the polynomial $f(x) = 1 + x^2$ in R_3 defined over $GF(2)$. In general a polynomial in R_3 $(= F[x]/(x^3 - 1))$ can be represented as $r(x) = r_0 + r_1 x + r_2 x^2$, where the coefficient can take the values 0 or 1, since defined over $GF(2)$. There can be a total of 8 polynomials in R_3 defined over $GF(2)$, which are $0, 1, x, x^2, 1 + x, 1 + x^2, x + x^2, 1 + x + x^2$.

Example(Cont..)

To generate the cyclic code, we multiply $f(x)$ with these 8 possible elements of R_3 and reduce the results modulo $(x^3 - 1)$:

$(1 + x^2) \cdot 0 = \ 0$, $(1 + x^2) \cdot 1 = \ 1 + x^2$,
$(1 + x^2) \cdot x = \ (1 + x^2) \cdot x^2 = \ x + x^2$
$(1 + x^2) \cdot (1 + x) = \ x + x^2$
$(1 + x^2) \cdot (1 + x^2) = \ 1 + x$
$(1 + x^2) \cdot (x + x^2) = \ 1 + x^2$
$(1 + x^2) \cdot (1 + x + x^2) = \ 0$

Thus there are four distinct codewords $\{0, 1 + x, 1 + x^2, x + x^2\}$ which corresponding to $\{000, 110, 101, 011\}$

A method for generating Cyclic Codes(Cont..)

Let C be a (n, k) non-zero cyclic code in R_n, then

1. there exists a unique monic polynomial $g(x)$ of the smallest degree in C.
2. the cyclic code consists of all multiples of the generator polynomial $g(x)$ by polynomials of degree $k-1$ or less.
3. $g(x)$ is a factor of $x^n - 1$

Note: A cyclic code C may contain polynomials other than the generator polynomial which also generates C. But the polynomial with minimum degree is called generator.

Note: The degree of $g(x)$ is $n-k$.

Example

Find all the binary code of block length 3, we first factorise $x^3 - 1$, Note that for $GF(2)$, $1 = -1$, since $1 + 1 = 0$. Hence $x^3 - 1 = x^3 + 1 = (x + 1)(x^2 + x + 1)$.

- Let the generator polynomial is 1, Code in polynomial is $\{R_3\}$ and the corresponding code is $\{000, 001, 010, 011, 100, 101, 110, 111\}$
- Generator polynomial- $x + 1$, code in polynomial $\{0, x + 1, x^2 + x, x^2 + 1\}$, corresponding binary code is $\{000, 011, 110, 101\}$.
- Generator polynomial- $x^2 + x + 1$, code in polynomial $\{0, x^2 + x + 1\}$, corresponding binary code is $\{000, 111\}$.
- Generator polynomial- $x^3 + 1 = 0$, code in polynomial $\{0\}$, corresponding binary code is $\{000\}$.

Encoding rule to generate the codewords from generator polynomial

Let $g(x)$ be generator polynomial, $i(x)$ is the information polynomial and $c(x)$ is the code polynomial.

$$c(x) = \; i(x)g(x)$$

So the received vector $v(x)$ is given by

$$v(x) = \; c(x) + e(x)$$

We define the **Syndrome Polynomial** $s(x)$ as reminder of $v(x)$ under division of $g(x)$

Example

Consider the generator polynomial $g(x) = x^2 + 1$ for ternary cyclic codes ($i.e$ over $GF(3)$) of block length $n = 4$. Here we are dealing with cyclic codes, the highest power of $g(x)$ is $n - k$. Since $n = 4$, k must be 2. So we are going to construct a $(4, 2)$ cyclic code. There will be total of $q^k = 3^k = 9$ codewords.

Example(Cont..)

Table: Ternary cyclic code constructed using $g(x) = x^2 + 1$

I	$i(x)$	$c(x) = i(x)g(x)$	C
00	0	0	0000
01	1	$x^2 + 1$	0101
02	2	$2x^2 + 2$	0202
10	x	$x^3 + x$	1010
11	$x + 1$	$x^3 + x^2 + x + 1$	1111
12	$x + 2$	$x^3 + 2x^2 + x + 2$	1212
20	$2x$	$2x^3 + 2x$	2020
21	$2x + 1$	$2x^3 + x^2 + 2x + 1$	2121
22	$2x + 2$	$2x^3 + 2x^2 + 2x + 2$	2222

Minimum distance of this code is 2. Therefore the code is capable of detecting one error and correcting zero errors.

Matrix Description of Cyclic Codes

Let C be a cyclic code with generator polynomial
$g(x) = g_0 + g_1x + g_2x^2 \ldots g_rx^r$ of degree r
Generator matrix of C is given by

$$G = \begin{bmatrix} g_0 & g_1 & \ldots & g_r & 0 & 0 & 0 & \ldots 0 \\ 0 & g_0 & g_1 & \ldots & g_r & 0 & 0 & \ldots 0 \\ 0 & 0 & g_0 & g_1 & \ldots & g_r & 0 & \ldots 0 \\ \vdots & \vdots & & & & & & \\ 0 & 0 & 0 & 0 & 0 & g_0 & g_1 & \ldots g_r \end{bmatrix}$$

Example

Find the generator matrices of all ternary codes ($i.e$ over $GF(3)$) of block length $n =\ 4$.
We first factories
$x^4 - 1 =\ (x-1)(x^3+x^2+x+1) =\ (x-1)(x+1)(x^2+1)$
This all the divisor of $x^4 - 1$ are
$1, (x-1), (x+1), (x^2+1), (x-1)(x+1) =\ (x^2-1), (x-1)(x^2+1) = (x^3-x^2+x+1), (x+1)(x^2+1) =\ (x^3+x^2+x+1)$ and (x^4-1).
All these polynomial are capable of generating cyclic code. Here we can note that $-1 =\ 2$ for $GF(3)$.

Example(Cont..)

$g(x) = 1$. *i.e* 1000 form $(4,4)$ code of $d^* = 1$. The corresponding generator matrix is

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

For $g(x) = x - 1 = -1 + x$ *i.e* -1100 form $(4,3)$ code of $d^* = 2$

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

In this way, we can find the generator matrix using all other polynomials $(x+1)$, (x^2+1), (x^2-1), $x^3 - x^2 + x + 1$, $x^3 + x^2 + x + 1$, $x^4 - 1$

Parity Check Polynomial

Let $g(x)$ is the generator polynomial. We can find **Parity Check Polynomial** corresponding to $g(x)$. $g(x)$ is the factor of $x^n - 1$. We can write as

$$x^n - 1 = h(x)g(x)$$

Where $h(x)$ is some polynomial. We can observe the following

1. Since $g(x)$ is monic, $h(x)$ has to be monic, because left hand side of the equation is also monic.(the leading co-efficient is unity).
2. Since degree of $g(x)$ is $n - k$, the degree of $h(x)$ must be k

Parity Check Polynomial

Let C is cyclic code in R_n with generator polynomial $g(x)$. $F[x]/f(x)$ is denoted by R_n, where $f(x) = x^n - 1$. In R_n $h(x)g(x) = x^n - 1 = 0$. Then any codeword belonging to C can be written as $c(x) = a(x)g(x)$, where $a(x) \in R_n$. Therefore in R_n

$$c(x)h(x) = a(x)g(x)h(x) = c(x) \cdot 0 = 0$$

Thus $h(x)$ behaves like a **Parity Check Polynomial**.

- *Any valid codeword when multiplied by the parity check polynomial yields zero polynomial.*
- *The parity check polynomial can be used to generate another cyclic code since it is a factor of $x^n - 1$ and is called* **Dual code of** C

Parity Check Polynomial

Consider the generator polynomial $g(x) = x^3 + 1$ for the $(9, 6)$ binary cyclic codes. The parity check polynomial can be found by simply dividing $x^9 - 1$ by $g(x)$. Thus $h(x) = (x^9 - 1)/(x^3 + 1) = x^6 + x^3 + 1$. Therefore, the dual code of $g(x) = x^3 + 1$ is $h(x) = x^6 + x^3 + 1$.

Parity Check Polynomial

Let C is a cyclic code with the parity check polynomial $h(x) = h_0 + h_1 x + \cdots + h_k x^k$. **Parity check matrix** of C is given by

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & 0 & \dots 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots 0 \\ 0 & 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots 0 \\ \vdots & \vdots & & & & & & \\ 0 & 0 & 0 & 0 & 0 & h_k & h_{k-1} & \dots h_0 \end{bmatrix}$$

We have $cH^T = 0$. Therefore $iGH^T = 0$ for any information vector i. Hence $GH^T = 0$. Further $s = vH^T$, where s is the syndrome vector and v is the received vector.

Example

Let the binary codes of block length $n = 7$, we have

$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1)$$

Consider $g(x) = (x^3+x+1)$. Since $g(x)$ ia factor of x^7-1. There is a cyclic code that can be generated by it. The generator matrix corresponding to $g(x)$ is

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

The parity check polynomial $h(x)$ is
$(x-1)(x^3+x^2+1) = (x^4+x^2+x+1)$

Example(cont..)

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

Binary (n, k) CRC codes

k message or data bits are encoded into n code bits by appending to message bits a sequence of $N = n - k$ bits.
Polynomial representation of message bits
$m = [m_{k-1} m_{k-2} \dots m_1 m_0]$ is given by

$$m(x) = m_{k-1}x^{k-1} + m_{k-2}x^{k-2} + \dots m_1 x + m_0 \text{ of degree } (k-1).$$

Appended bits $R = [r_{N-1} r_{N-2} \dots r_1 r_0]$. Polynomial representation is

$$R(x) = r_{N-1}x^{N-1} + r_{N-2}x^{N-2} \dots r_1 x + r_0 \text{ of degree } N-1$$

CRC code bits
$C = [c_{n-1} c_{n-2} \dots c_1 c_0] = [m_{k-1} m_{k-2} \dots m_1 m_0 r_{N-1} r_{N-2} \dots r_1 r_0]$

Binary (n, k) CRC codes(Cont..)

$$C(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} \ldots c_1 x + c_0 \text{ of degree } (n-1)$$
$$= x^N m(x) + R(x)$$

Example

Let $k = 10, n = 13, N = n - k = 3$ CRC code
$m = [1010100101]$
$m(x) = x^9 + x^7 + x^5 + x^2 + 1$
$R = [111],\ R(x) = x^2 + x + 1$
$C(x) = x^N m(x) + R(x)$
Hence $C(x) = x^3(x^9 + x^7 + x^5 + x^2 + 1) + x^2 + x + 1 =$
$x^{12} + x^{10} + x^8 + x^5 + x^3 + x^2 + x + 1$

How to obtain the polynomial $R(x)$(the appended bits)

CRC codes are designed by the generator polynomial $g(x)$ with degree N.
$g = [g_N g_{N-1} \dots g_1 g_0]$

$$g(x) = g_N x^N + g_{N-2} x^N + \dots g_1 x + g_0 \text{ of degree } N.$$

Divide $x^N m(x)$ by $g(x)$ and obtain the reminder, which is $R(x)$.
$x^N m(x) = p(x) g(x) + R(x)$.

Example

Message [11100110] of 8 bits. Polynomial representation

$m(x) = x^7 + x^6 + x^5 + x^2 + x$

Given $n - k = N = 4$, generator polynomial

$g(x) = x^4 + x^3 + 1 = [11001]$

$\frac{x^N m(x)}{g(x)} = \frac{x^{11}+x^{10}+x^9+x^6+x^5}{x^4+x^3+1}$

$= x^7 + x^5 + x^4 + x^2 + x + \frac{x^2+x}{x^4+x^2+x}$

$R(x) = x^2 + x$, therefor appended bits are [0110], since $N = 4$

The CRC code bits are [111001100110]

Error Detection

The polynomial for the received codeword $T(x)$ is divided by the generator polynomial $g(x)$. $T(x) = C(x) = x^N m(x) + R(x)$
The reminder of $T(x)/g(x) = R(x) + R(x) =$ all zero.

Example

$g(x) = x^4 + x^3 + 1$

The transmitted CRC code bits are [111001100110]

$T(x) = C(x) = x^{11} + x^{10} + x^9 + x^6 + x^5 + x^2 + x$

$= (x^7 + x^5 + x^4 + x^2 + x)g(x)$

The reminder of $[C(x)/g(x)] = 0 \rightarrow [0000]$

Example(Cont..)

The reminder is not zero

An indication that an error has occurred in transmission and the received codeword is not a valid codeword.

Let $g(x) = x^4 + x^3 + 1$.

The transmitted CRC code bits are [111001100110]

The received CRC code bits are [110011100110]

$T(x) = x^{11} + x^{10} + x^7 + x^5 + x^2 + x = C(x) + x^9 + x^7$

$\frac{T(x)}{g(x)} = \frac{C(x)+x^9+x^7}{x^4+x^3+1} = (x^7 + x^2) + \frac{x}{x^4+x^3+1}$

The reminder of $[T(x)/g(x)] = x \rightarrow [0010]$