Cyclic Codes:

→ Introduction
→ Code algebra of cyclic codes
→ Basic properties of Galois field (GF) polynomial operations over Galois fields.
→ Generating cyclic code by generating polynomial
→ Parity check polynomial
→ Encoder and decoder for cyclic codes

Introduction to Cyclic codes:

→ subclass of linear block code
→ (n, k) linear code is said to be cyclic code, if it make follows 2 properties:

n → length of the codeword
k → length of the message bits

(i) linearity property
(ii) Cyclic shift property.

eg: LBC = {0000, 0101, 1010, 1111}

(i) Linear Property:

* All zero word is a valid codeword

* The sum of two codewords also forms a valid codeword : 0101 + 1010 ⟷ 1111

* The min distance between two codewords = min hamming weight.

i.e $d_{min} = \min w(c)$

{0000, 0101, 1010, 1111}
w=2, w=2, w=4
d=2, d=4, d=2

$d_{min} = 2 = \min w = 2$

(ii) Cyclic shift Property:

Right & Left cyclic shift codeword is also a valid codeword.

Code Algebra of cyclic codes:

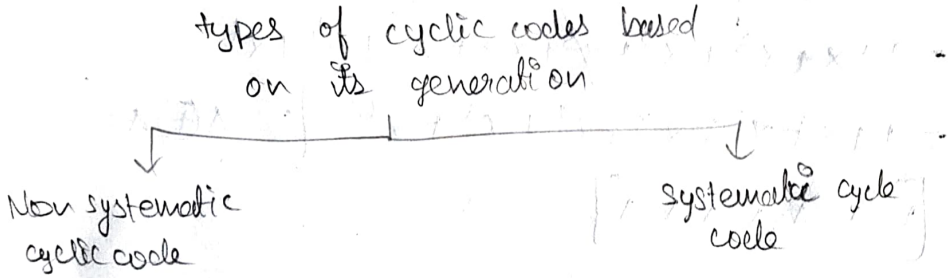
In case of (n,k) cyclic code,

(i) the message polynomial m(X) is given as

$$m(X) = m_0 X^0 + m_1 X^1 + m_2 X^2 + \dots + m_{k-1} X^{k-1}$$

(ii) the generator polynomial g(X) is given as

$$g(X) = g_0 X^0 + g_1 X^1 + g_1 X^2 + \dots + g_{n-1} X^{k-1}$$



Non-systematic Cyclic code:

* The position of parity bits is not defined
* The codeword polynomial V(X) in non systematic form is given as: $V(X) = m(X) \cdot g(X)$

Systematic Cyclic code:

* position of parity bits is well defined
* $V(X) = X^{n-k} \cdot m(X) + r(X)$

where,

$$r(X) = \text{Rem}\left[\frac{X^{n-k} \cdot m(X)}{g(X)}\right]$$

eg:- generator polynomial of (7,4) cyclic is $g(x) = 1 + x + x^3$
Find the codeword (V) for message vector 1011 by forming code polynomial $v(x)$
(i) in non systematic form
(ii) in systematic form

Sol:

Given, $m(x)$; $g(x)$

$g(x) = 1 + x + x^3$
$\quad\quad\uparrow \quad\uparrow$
$1 \cdot x^0 \quad 1 \cdot x^1 \quad 1 \cdot x^3$

msg vector = 1011 $\rightarrow m(x) = 1 \cdot x^0 + 1 \cdot x^2 + 1 \cdot x^3$ (or) $1 + x^2 + x^3$

(i) $V(x) = m(x) \cdot g(x)$
$= 1 + x + x^3 + x^2 + x^3 + x^5 + x^3 + x^4 + x^6$
$= 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ $\quad [\because A \oplus A = 0]$

$\therefore V = [1\ 1\ 1\ 1\ 1\ 1\ 1]$

(ii) $n=7, k=4$

$x^{n-k} \cdot m(x) = x^{7-4} \cdot (1 + x^2 + x^3) = x^3 + x^5 + x^6$

Rem $\left[\frac{x^{n-k} \cdot m(x)}{g(x)}\right] = \frac{x^3 + x^5 + x^6}{1 + x + x^3} \Rightarrow \frac{x^6 + x^5 + x^3}{x^3 + x + 1}$

$$
\begin{array}{r|l}
x^3 + x + 1 & x^6 + x^5 + x^3 \quad (x^3 + x^2 + x + 1) \\
 & x^6 + x^4 + x^3 \\
\hline
 & x^5 + x^4 \\
 & x^5 + x^3 + x^2 \\
\hline
 & x^4 + x^3 + x^2 \\
 & x^4 + x^2 + x \\
\hline
 & x^3 + x \\
 & x^3 + x + 1 \\
\hline
 & 1
\end{array}
$$

$\therefore r(x) = 1.$

$\therefore V(x) = 1 + x^3 + x^5 + x^6$

$V(x) = [1\ 0\ 0\ 1\ 0\ 1\ 1]$

GF → is a mathematical field that contains a finite no. of elements, which makes it essential in areas like coding theory, cryptography and digital communication.