ITC : Mod 4

- **Cyclic codes**

A (n,k) LBC C is said to be a cyclic code if every cyclic shifts of the code is also a code vector of C

Eg if $C_1 = 0111001$ is a code-vector of C

if last 1 is moved to 1st position, we get $C_2 = 1011100$,

if C_2 is also a code vector of C, then its a cyclic code.

- **Properties of Cyclic codes**

1. $g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_{n-k} x^{n-k}$ for (n,k) cyclic codes.
   ↳ degree (n-k)
2. g(x) of a (n,k) cyclic code is a factorial of $x^n + 1$
   i.e. $x^n + 1 = g(x) \cdot h(x)$
   ↳ degree K, Polynomial check Polynomial
3. Cyclic code in a non-systematic format : $V(x) = D(x) g(x)$
   message-vector polynomial of degree K
4. Cyclic codes in a systematic format = $[x^{n-k} \; d(x)] / g(x)$
   $V(x) = R(x) : d(x)$

- **Modulo 2 Algebra**

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

Subtraction is same as addition.

$x \cdot x = x^2$

Division: Eg. $f_2(x) = x^6 + x^5 + x^2$

$$x^3 + x + 1 \;\big)\; x^6 + x^5 + x^2 \;\big(\; x^3 + x^2 + x \quad : Q(x) : \text{Quotient Polynomial}$$

$x^6 + x^4 + x^3$

$x^5 + x^4 + x^3 + x^2$

$x^5 + x^3 + x^2$

x^4

$x^4 + x^2 + x$

$x^2 + x \quad : R(x)$

↳ Remainder Polynomial

• Questions

1. For the (7,4) single error correcting cyclic code, $D(x) = d_0 + d_1 x + d_2 x^2 + d_3 x^3$ and $x^{n+1} = x^7 + 1 = (1+x+x^3)(1+x+x^2+x^3)$ Using $g(x) = 1+x+x^3$. Find all 16 code-vectors of the cyclic code both in non-systematic and systematic form

→ i) Non systematic Cyclic code :-

$$V(x) = D(x)\, g(x)$$

given $g(x) = 1+x+x^3$ $\quad 2^k = 16$ code vectors

$D(x) = d_0 + d_1 x + d_2 x^2 + d_3 x^3$

Taking $D = 1001$ [Calculate for 0-15 or 0000 to 1111]

$\therefore$ if $D(x) = 1 + 0(x) + 0(x^2) + 1(x^3) = 1 + x^3$

$V(x) = D(x) \cdot g(x) = (1+x^3)(1+x+x^3)$

$= 1 + x + x^4 + x^6$.

$[V] = [1100101]$ ← coefficients of $V(x)$

Make a Message (D), Code-vectors table

Message (D)	Code-vectors
0000	0000000
0001	0001101
⋮	⋮

ii) Systematic Cyclic Code :-

1st 3 bits : check bits. last 4 bits : message bits.

$$R(x) = \frac{x^{n-k}\, D(x)}{g(x)}$$

So for eg. $D = [1001]$

$D(x) = d_0 + d_1 x + d_2 x^2 + d_3 x^3 = 1 + x^3$

$x^{n-k}\, D(x) = x^{7-4}(1+x^3) = x^3 + x^6$

$R(x) = x^{n-k}\, D(x) / g(x)$

$$x^3+x+1 \;\overline{)\; x^6+x^3 \;(\; x^3+x}$$

$$x^6 + x^4 + x^3$$

$$x^4$$

$$x^4 + x^2 + x$$

$$x^2 + x$$

$R(x) = x^2 + x$

$= [011]$

Code vector : [V] = R : D :: 011 : 1001

Make the table for every message & code-vector

Given: x^7+1, $g(x) = 1+x+x^3$

to find $h(x)$, we have $x^n+1 = g(x).h(x)$

$h(x) = [x^7+1]/g(x) = (x^7+1)/(1+x+x^3)$

$$
\begin{array}{l}
x^3+x+1 \;\big)\; x^7+1 \;\big(\; x^4+x^2+x+1 \\
\underline{x^7+x^5+x^4} \\
1+x^5+x^4 \\
\underline{x^5+x^3+x^2} \\
x^4+x^3+x^2+1 \\
\underline{x^4+x^2+x^2} \\
x^3+x+1 \\
\underline{x^3+x+1} \\
0
\end{array}
$$

$h(x) = x^4+x^2+x+1$

- Generator and Parity Check Matrices of (7,4) Cyclic Codes

Let us consider polynomials as $g(x)$, $xg(x)$, $x^2g(x)$, $x^3g(x)$

$g(x) = 1+x+x^3 = 1+1(x)+0(x^2)+1(x^3)+0x^4+0x^5+0x^6$

code vector of $g(x)$ = [1101000]

Similarly for $x^2g(x) = x^2+x^3+x^5 = 0011010$

$xg(x) = 0110100$ $x^3g(x) = 0001101$

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

Systematic code vectors can be found using $[V] = [D][G]$

$[D] = [d_0\ d_1\ d_2\ d_3]$

For Parity Check Matrix, we take an example of

$h(x) = 1+x+x^2+x^4$

Reciprocal of $h(x)$ is $x^k h(x^{-1})$ which is a factor of x^n+1

For (7,4) we have $x^4h(x^{-1})$

$h(x^{-1}) = 1+1/x+1/x^2+1/x^4$

$x^4(x^{-1}) = 1+x^2+x^3+x^4$ code : 1011100

$x^5(x^{-1}) = 0101110$ $x^6h(x^{-1}) = 0010111$

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}_{3\times 7}$$

$$[H] = [I_{n-k} : P^T]$$
$$= [I_3 : P^T]$$

Add 1st and last row, and replace it with 1st

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

- **Encoder Circuit :-**

R : n-k flipflops that makeup a shift register.

⊕ : modulo 2 adder.

g_i : a max of (n-k) switches. if $g_i = 1$ its closed path / shortckt
if $g_i = 0$ its open path / open ckt

Gate : AND gate

For (7,4) cyclic code if $g(x) = 1 + x + x^3$
verify it using message vectors (1001) and (1011)

$g_0 = 1$ $g_1 = 1$ $g_2 = 0$ $g_3 = 1$

$(n-k) \rightarrow (7-4) = 3$ • 3 flip-flops ie R_0, R_1, R_2
2 modulo-2 adders, $g_{n-k-1} = g_2$

To Be Continued