DETAILED LECTURE NOTES

Unit-4

Cyclic Code

Cyclic Code: These are subclass of linear block code. They can be described using the help of polynomials.

→ it poses a mathematical structure, it is possible to develop codes with error correcting probablity.

→ It can be systematic and non systematic.

In systematic form it represented by $x = (m:c)$ where m is the message bit and 'c' represents the check bit.

A linear code is called cyclic code if every cyclic shift of the codevector produce some other codevector.

Properties of Cyclic Code

1. Linearity The property state that sum of two codeword is also a codeword.

$$x_3 = x_1 \oplus x_2$$

2. Cyclic Property every cyclic shift of the valid code vector produce another valid codeword.

$$X = \{x_{n-1}, x_{n-2} \ldots x_1, x_0\}$$

by one cyclic shift

$$X' = \{x_{n-2}, x_{n-1} \ldots x_1, x_0, x_{n-1}\}$$

Algebric structure of code (Generation of code word in Non systematic form)

$$X = (x_{n-1}, x_{n-2}, x_{n-3} \ldots x_1, x_0)$$

$$X(p) = x_{n-1} p^{n-1} + x_{n-2} p^{n-2} + \ldots x_1 p + x_0$$

$$m(p) = m_{k-1} p^{k-1} + m_{k-2} p^{k-2} + \ldots + m_1 p + m_0$$

$$\boxed{X(p) = m(p)\, G(p)}$$

Q The generator polynomial of a (7,4) cyclic code is $G(p) = p^3 + p + 1$. find all the codeword for the code in nonsystematic form.

Ans $n = 7 \quad k = 4 \quad q = n - k = 3$

there will be $2^4 = 16$ message bit.

for example

$$m = m_3 m_2 m_1 m_0 = 0101$$

$$m(p) = m_3 p^3 + m_2 p^2 + m_1 p^1 + m_0$$

$$m(p) = p^2 + 1$$

Given polynomial is

$G(P) = P^3 + P + 1$

Code vector $X(P) = m(P)\,G(P)$

$= (P^2+1)(P^3+P+1)$

$= P^5 + P^3 + P^3 + P^2 + P + 1 \qquad (1 \oplus 1 = 0,\ 0 \cdot P^3 = 0)$

$= P^5 + P^2 + P + 1$

$= 0 \cdot P^6 + P^5 + 0 \cdot P^4 + 0 \cdot P^3 + P^2 + P + 1$

So the X is

$= (0100111)$

2. Generation of codeword in systematic form

$X = (k \text{ message bit} : (n-k) \text{ check bit})$

$= (m_{k-1}\, m_{k-2} \cdots m_1 m_0 : c_{q-1}\, c_{q-2} \cdots c_1 c_0)$

Check bits form a polynomial

$c(P) = c_{q-1} P^{q-1} + c_{q-2} P^{q-2} + \cdots c_1 P + c_0$

$$c(P) = \text{rem}\left[\frac{P^q\, m(P)}{G(P)}\right]$$

Q. The generator polynomial of a (7,4) cyclic code is $G(p) = p^3 + p + 1$, find all the code vectors for the code in systematic form.

Ans $n = 7 \quad k = 4 \quad q = n - k = 3$

$2^k = 2^4 = 16$ message vectors of 7 bit each.

$m = (m_3 m_2 m_1 m_0) = (0101)$

$m(p) = m_3 p^3 + m_2 p^2 + m_1 p + m_0$

$m(p) = p^2 + 1$

$G(p) = p^3 + p + 1$

To obtain $p^q m(p)$

$q = 3$

$= p^3 m(p)$

$= p^3 (p^2 + 1)$

$= p^5 + p^3 = p^5 + 0 \cdot p^4 + p^3 + 0p^2 + 0p + 0$

$G(p) = p^3 + p + 1 = p^3 + 0 \cdot p^2 + p + 1$

To perform division $\quad \frac{p^q m(p)}{G(p)}$

$$p^3 + 0 \cdot p^2 + p + 1 \;\big)\; p^5 + 0 \cdot p^4 + p^3 + 0 \cdot p^2 + 0 \cdot p + 0 \;\big(\; p^2$$

$$p^5 + 0 \cdot p^4 + p^3 + p^2$$

mod-2 addition $\leftarrow$ $\oplus \quad \oplus \quad \oplus \quad \oplus$

$$0 + 0 + 0 + p^2 + 0 \cdot p + 0$$

$$c(p) = \text{rem}\left[\frac{p^3 m(p)}{G(p)}\right] = p^2 + 0 \cdot p + 0$$

So $c(p) = c_2 p^2 + c_1 p + c_0$

$= p^2 + 0 \cdot p + 0$

$= (100)$

The code vector is written in the systematic code

$x = (m_{k-1}\ m_{k-2} \cdots m_1 m_0 : c_{q-1}\ c_{q-2} \cdots c_1 c_0)$

$= (0101 : 100)$

$x = 0101100$

Finite field **Galois field** ~~structure~~

~~A~~ field having only a finite number ~~of~~ element is called a ~~G~~ finite field. a galois field is a special case ~~of~~ finite field

Galois field ~~A~~ field in which ~~the~~ number ~~of~~ element is in ~~the~~ form ~~of~~ p^n where p is ~~the~~ prime number. and n is ~~the~~ positive ~~integer~~ number. It is ~~denoted~~ by $GF(p^n)$

Exam $GF(3) = \{0, 1, 2\}$ for mod 3 form a finite field ~~of~~ order 3

The multiplication table for GF-3

⊗	1	2
1	1	2
2	2	1

Table of reciprocal

1	2
1	2

The additional table is

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Example 2 Galois field arithmetic for mod 5

GF(5) = {0, 1, 2, 3, 4}

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

So the additive inverse of 1, 2, 3, 4 are 4, 3, 2, 1

Additive inverse of 0 is 0

DETAILED LECTURE NOTES

multiplication table for GF(5) group.

X	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Theorams of Galois field

→ The multiplicative group of GF(p^n) is cyclic. when p is the prime number and n is an integer.

→ GF(p^n) has a subfield F' with p^m element if and only if m|n. F' is the unique factor

→ Let f be the finite field, Then the nomber of element of f is p^n for some positive integer n.

→ Let f be a finite field with p^n element and let $a \in f$. Then there exist element u and v in f such that $a = u^2 + v^2$

→ Each element of a finite field with elements satisfy the equation $x^{p^n} = x$.

Generator and parity check matrix of cyclic code

Nonsystematic form of Generator matrix

$$G(p) = p^q + g_{q-1}p^{q-1} + \cdots g_1 p + 1$$

multiply both the side by p^i

$$p^i G(p) = p^{i+q} + g_{q-1}p^{i+q-1} + \cdots + g_1 p^{i+1} + p^i$$

and $i = (k-1), (k-2) \cdots 2, 1, 0$

Q Obtain the generator matrix corresponding to $G(p) = p^3 + p^2 + 1$ for a $(7,4)$ cyclic code.

Ans $n = 7 \quad k = 4 \quad q = 7-4 = 3$

$$p^i G(p) = p^{i+3} + p^{i+2} + p^i + \cdots$$

So $k-1 = 3$; $i = 3, 2, 1, 0$

for row 1 : $i = 3 \Rightarrow p^3 G(p) = p^6 + p^5 + p^3$

for row 2 : $i = 2 \Rightarrow p^2 G(p) = p^5 + p^4 + p^2$

for row 3 : $i = 1 \Rightarrow p G(p) = p^4 + p^3 + p$

for row 4 : $i = 0 \Rightarrow G(p) = p^3 + p^2 + 1$

So transform the above set of equation into a matrix 4×7

$$G_{4\times 7} = \begin{array}{c} \\ \text{Row 1} \\ \text{Row 2} \\ \text{Row 3} \\ \text{Row 4} \end{array} \begin{array}{c} \begin{array}{ccccccc} P_6 & P_5 & P_4 & P_3 & P_2 & P_1 & P_0 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}_{4\times 7}$$

DETAILED LECTURE NOTES

Systematic form of Generator matrix

$$G = [I_k : P_{k \times q}]_{k \times n}$$

The i^{th} row of this matrix will be represented in the polynomial form.

$$t^{th} \text{ row of } G = P^{n-t} + R_t(P)$$

when $t = 1, 2, 3 \ldots k$

$$\frac{P^{n-t}}{G(P)} = \text{Quotient} + \frac{\text{Remainder}}{G(P)}$$

Remainder $= R_t(P)$

Quotient $= Q_t(P)$

$$\frac{P^{n-t}}{G(P)} = Q_t(P) + \frac{R_t(P)}{G(P)}$$

$$P^{n-t} = Q_t(P) G(P) \oplus R_t(P)$$

$\because z = y \oplus t$ then $z \oplus y = t$ or $z \oplus t = y$.

thus the equation can be changed into

$$P^{n-t} \oplus R_t(P) = Q_t(P) G(P)$$

Q. Find out the generator matrix for a systematic (7,4) cyclic code if $G(P) = P^3 + P + 1$. Also find the parity check matrix.

Ans 1. To obtain generator polynomial.

t^{th} row of generator matrix

$$P^{n-t} + R_t(P) = Q_t(P)\, G(P) \qquad t = 1, 2, \ldots k$$

given that $n = 7$ $k = 4$ and $q = n - k = 3$

$$P^{7-t} + R_t(P) = Q_t(P)\,(P^3 + P + 1)$$

with $t = 1$ the above equation converted

$$P^6 + R_t(P) = Q_t(P)\,(P^3 + P + 1)$$

i To obtain $R_t(P)$ and $Q_t(P)$ for 1st Row

$$\frac{P^6 + R_t(P)}{P^3 + P + 1} = Q_t(P)$$

To find $Q_t(P)$

$$\begin{array}{r|l} P^3 + P + 1 & P^6 + 0 + 0 \quad (P^3 + P + 1 \\ & P^6 + P^4 + P^3 \\ & \oplus \quad \oplus \quad \oplus \\ \hline & 0 + P^4 + P^3 + 0 + 0 \\ & P^4 + P^2 + P \\ & \oplus \quad \oplus \quad \oplus \\ \hline & P^3 + P^2 + P + 0 \\ & P^3 + P + 1 \\ & \oplus \quad \oplus \\ \hline & P^2 + 1 \leftarrow \text{Remainder} \end{array}$$

mod 2 addition

$Q(+)P = P^3 + P + 1$

$R(+)P = P^2 + 1$

So ~~that~~

$$p^6+p^2+1 = (p^3+p+1)(p^3+p+1)$$

~~it~~ represents the 1st Row of generator ~~matrix~~.

others Row Polynomial

2^{nd} Row $= p^5+p^2+p+1$

3^{rd} Row $= p^4+p^2+p$

4^{th} Row $= p^3+p+1$

(iii) Conversion of Row polynomial into matrix

$$G = \begin{array}{c} \\ \text{Row 1} \\ \text{Row 2} \\ \text{Row 3} \\ \text{Row 4} \end{array} \begin{array}{c} \begin{array}{ccccccc} p^6 & p^5 & p^4 & p^3 & p^2 & p^1 & p^0 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}_{4\times 7}$$

The code vector can be obtained by equation

$$X = mG$$

Take any 4 bit message vector and find corresponding code vector

$$M = (m_3\ m_2\ m_1\ m_0) = (1\ 1\ 0\ 0)$$

$$X = mG = [1100] \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$= (1100010)$$

To obtain Parity check matrix

$$G = [I_k : P_{k \times q}]_{k \times n}$$

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}_{4 \times 3}$$

Parity check matrix

$$H = [P^T : I_q]_{q \times n}$$ I_q is the $q \times q$ matrix

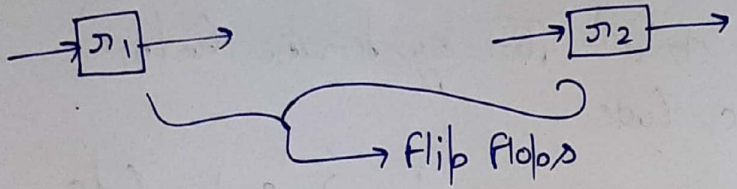
$$H = \left[\begin{array}{cccc:ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]_{3 \times 7}$$

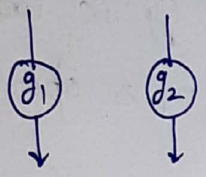
P^T I_3

DETAILED LECTURE NOTES

Encoding Using an (n-k) Bit shift Register

The symbol used for generating the encoder is





it represents closed path

if $g=1$ and $g=0$ if no connection.

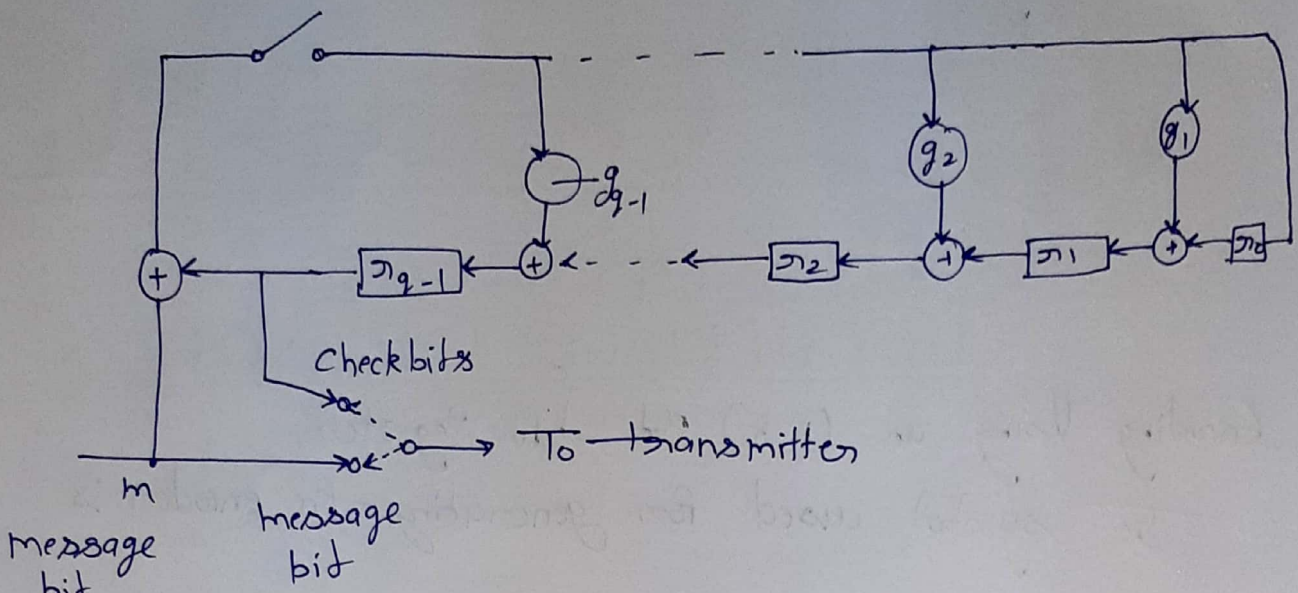
Operation The feedback switch is first closed. The output switch is connected to message input.

All the shift Register initialized to zero state

The k message bit shifted to transmitter as well as to the Register.

After the shift of k message bit and register contain q check bits. The feedback switch is now opened and output switch is connected to check bit position.

The block diagram perform the division operation and generate the remainder These bit stored in the shift Register.



Encoder circuit for systematic (n, k) cyclic code

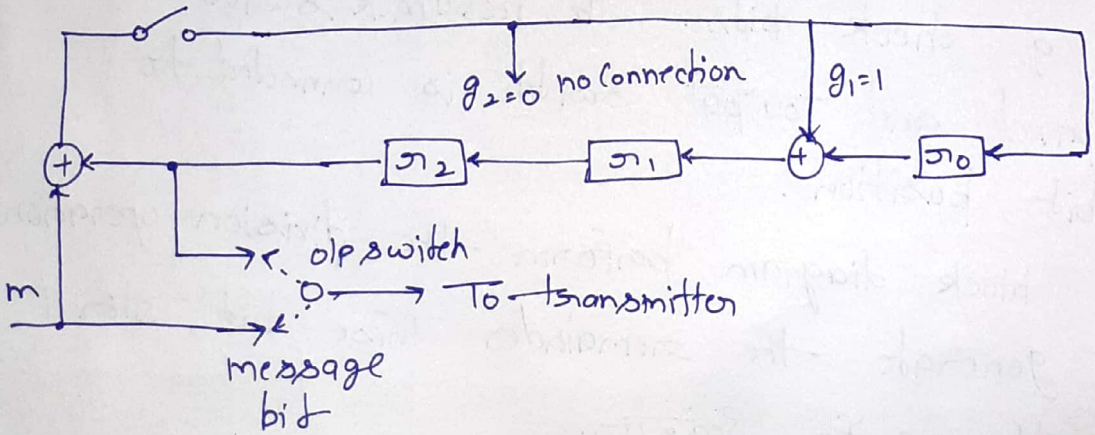
Q Design the encoder for the (7, 4) cyclic code generated by $G(p) = p^3 + p + 1$ and verify its operation for any message vector.

Ans The generator polynomial is

$$G(p) = p^3 + 0 \cdot p^2 + p + 1$$

$$G(p) = p^3 + g_2 p^2 + g_1 p + 1$$

$g_1 = 1$ $g_2 = 0$ and $q = 7 - 4 = 3$



DETAILED LECTURE NOTES

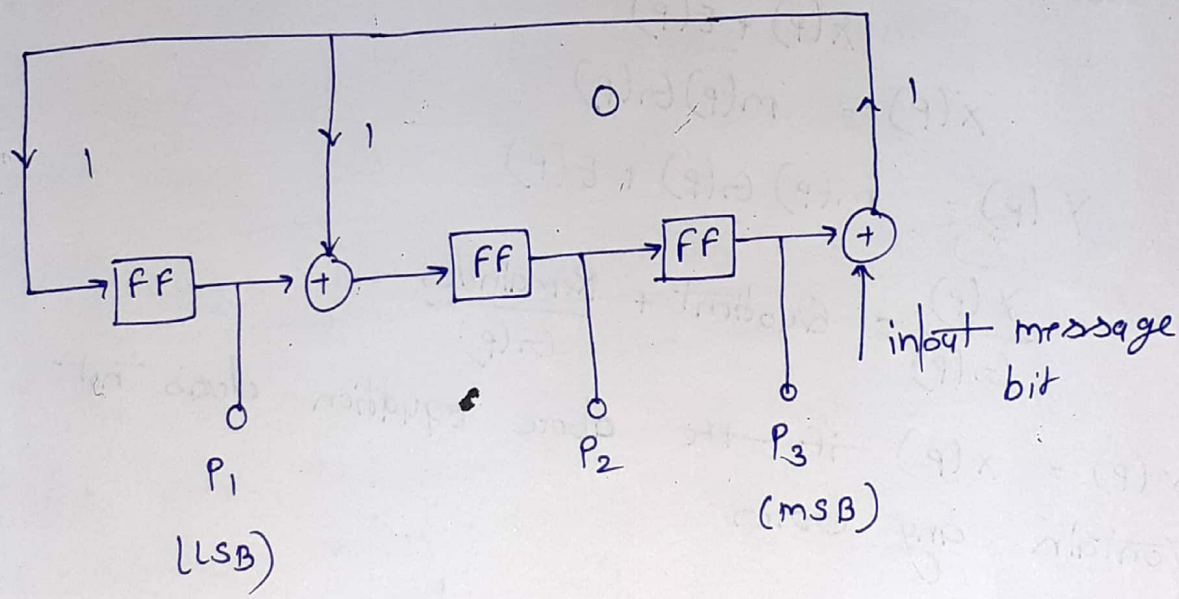
Cyclic Encoder Designing

$G(x) = 1 + x + x^3$

Calculate (1) Cyclic Encoder
(2) Codeword ~~if~~ message 1110

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

$= 1 + x + 0 \cdot x^2 + x^3$



m	P_1	P_2	P_3
	0	0	0
1	1	1	0
1	1	0	1
1	0	1	0
0	0	0	1

P_1	P_2	P_3
0	0	1

Code word = [message , parity]

= [1110 , 100]

Syndrome decoding, Error detection and Error Correction

Syndrome decoding can be used to correct those error.

If E is the error vector then the corrected word can be obtained as.

$$X = Y \oplus E$$

$$Y = X \oplus E$$

in the polynomial form the above equation can be written as

$$X(P) + E(P)$$

$$X(P) = m(P)G(P)$$

$$Y(P) = m(P)G(P) + E(P)$$

$$\frac{Y(P)}{G(P)} = \text{Quotient} + \frac{\text{Remainder}}{G(P)}$$

$Y(P) = X(P)$ if the above equation does not contain any error

$$\frac{X(P)}{G(P)} = \text{Quotient} + \frac{\text{Remainder}}{G(P)}$$

$$X(P) = m(P)G(P)$$

Quotient will be equal to $m(P)$ and Remainder will be zero. This shows that it doesn't contain any error

R(p) will be polynomial of degree less than or equal to q-1. multiply both the equation by G(p)

$$Y(p) = Q(p)\,G(p) + R(p)$$

So by compairing both the equation

$$m(p)\,G(p) \oplus E(p) = Q(p)\,G(p) \oplus R(p)$$

So $$E(p) = m(p)\,G(p) \oplus Q(p)\,G(p) \oplus R(p)$$

The abore equation has mod-2 addition So the addition and subtraction is the same.

$$E(p) = [m(p) + Q(p)]\,G(p) + R(p)$$

So the error pattern depend on the remainder 'R'. for every Remainder 'R' there will be the specific error vector. it is called syndromic vector 's'. or $R(p) = S(p)$

$$\frac{Y(p)}{G(p)} = Q(p) + \frac{S(p)}{G(p)}$$

Thus syndrome vector is obtained by diviging Y(p) and G(p)

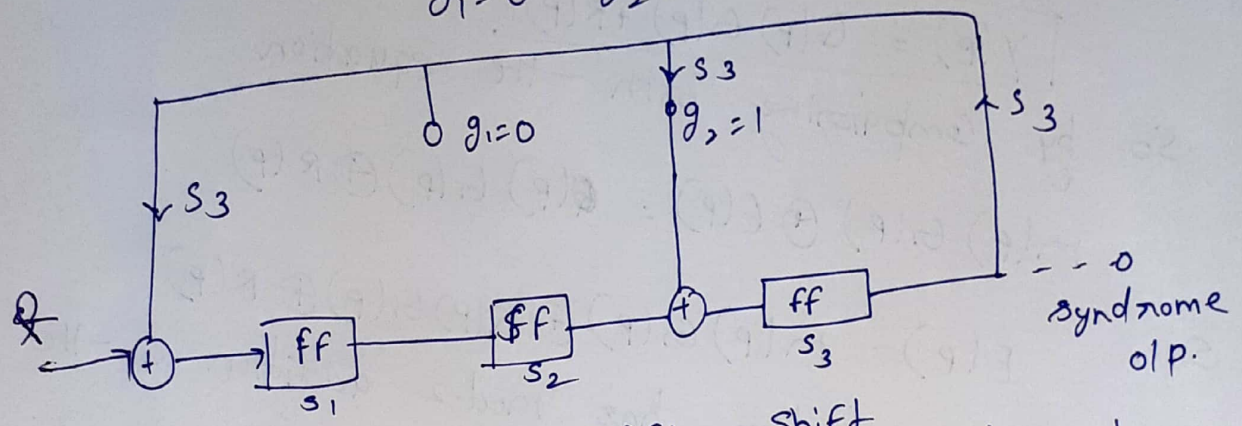
$$S(p) = \text{rem}\left[\frac{Y(p)}{G(p)}\right]$$

Q Design a Syndrome calculator for (7,4) cyclic hamming code generated by the polynomial $G(p) = x^3 + x^2 + 1$. Calculate the syndrome for Y (1001011)

Answer for $g(x) = 1 + x^2 + x^3$

$g(x) = 1 + g_1 x^1 + g_2 x^2 + x^3$

$g_1 = 0 \quad g_2 = 1$



R	Before shift S_1	S_2	S_3	After shift S_1' $R \oplus S_3$	S_2' S_1	S_3' $S_2 \oplus S_3$
1	0	0	0	1	0	0
0	1	0	0	0	1	0
0	0	1	0	0	0	1
1	0	0	1	0	0	1
0	0	0	1	1	0	1
1	1	0	1	0	1	1
1	0	1	1	0	0	0

LSB ↑ MSB ↑

DETAILED LECTURE NOTES

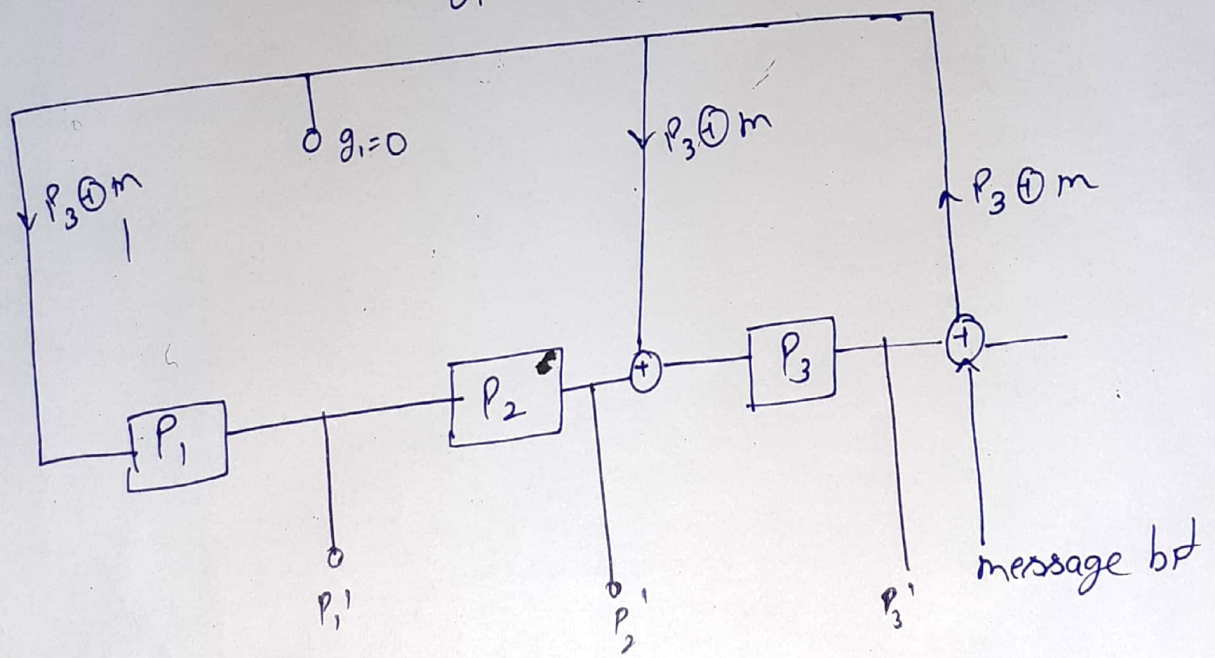
Cyclic Encoder Example

Q. Consider a (7,4) cyclic code with $g(x) = 1+x^2+x^3$
a) Draw block diagram of cyclic Encoder with
0110.

Ans $g(x) = 1+x^2+x^3$

$g(x) = 1+g_1x^1+g_2x^2+g_3x^3$

$g_1 = 0 \quad g_2 = 1$



Input (m)	Before Shift			After shift		
m	P_1	P_2	P_3	$P_1' = P_3 + m$	$P_2' = P_1$	$P_3' = P_2 + P_3 + m$
0	0	0	0	0	0	0
1	0	0	0	1	0	1
1	1	0	1	0	1	0
0	0	1	0	0	0	1
				↑ LSB		↑ MSB