$$n = \frac{M}{N}$$

$$n = \frac{2.2568}{2.38}$$

$$n = 0.99$$

- Code redundancy:

$$w = 1 - n$$

$$w = 1 - 0.99$$

$$w = 0.01$$

Page No.: 19/02/18

"Unit - 4"

Cyclic Codes

Cyclic codes are the subset of linear block codes. The cyclic codes can be in systematic or non-systematic codes. In the systematic form, check bits are calculated seperately by the code vector $x = (M : C)$.

Here, M represent the msg bit & C is check bit.

Defin^n of Cyclic Codes:

A linear code is cyclic code if every cyclic shift of the code vector produces some other code vector. This defin^n includes a fundamental property of cyclic code.

Properties of Cyclic Codes:

1. Linear property
2. Cyclic property

Linear property: This property states dat sum of any 2 code vector is also a valid code vector.

$$X_3 = X_1 \oplus X_2$$

$X_1 \longrightarrow$ valid code vector
$X_2 \longrightarrow$ " " "
$X_3 \longrightarrow$ Also " " "

Cyclic property :

If the cyclic shift of the valid code vector produces another valid code vector.

Eg: If $X_1 = \{x_1, x_2, x_3, x_4, x_5\}$

$X_1 \longrightarrow$ valid code vector

After cyclic shift of x_1 produce new valid code vector.

$X_2 = \{x_5, x_1, x_2, x_3, x_4\}$

$x_2 \longrightarrow$ valid code vector

Then X_1, X_2 is called cyclic code vector

20/2/18

Representation of Code word by a Polynomial:

Generation of Code vector in non-systematic form

Q) The generation polynomial of (7,4) Cyclic code is $G(P) = P^3 + P + 1$. Find all other code vector for the code in non-systematic form.

→ Here, $n = 7$, $k = 4$

$$q = n - k$$
$$q = 7 - 4$$
$$q = 3$$

Let the msg bits $= [m_3 \; m_2 \; m_1 \; m_0]$

$$M = [m_3 \; m_2 \; m_1 \; m_0]$$

Possible Combination of msg msg :

$$2^4 = 16$$

Sr. No.	m_3	m_2	m_1	m_0	$M(P) = P^3 m_3 + P^2 m_2 + P^1 m_1 + m_0$	$X(P) = M(P)G(P)$ x_6	x_5	x_4	x_3	x_2	x_1	x_0
1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	1	1	0	0	0	1	0	1	1
3	0	0	1	0	P	0	0	1	0	1	1	0
4	0	0	1	1	$P+1$	0	0	1	1	1	0	1
5	0	1	0	0	P^2	0	1	0	0	1	0	0
6	0	1	0	1	P^2+1	0	1	0	1	1	1	1
7	0	1	1	0	P^2+P	0	1	1	0	0	1	0
8	0	1	1	1	P^2+P+1	0	1	1	1	0	0	1
9	1	0	0	0	P^3	1	0	0	0	0	0	0
10	1	0	0	1	P^3+1	1	0	0	1	0	1	1
11	1	0	1	0	P^3+P^2	1	0	1	0	1	1	0
12	1	0	1	1	P^3+P^2+1	1	0	1	1	1	0	1
13	1	1	0	0	P^3+P^2	1	1	0	0	1	0	0
14	1	1	0	1	P^3+P^2+1	1	1	0	1	1	0	1
15	1	1	1	0	P^3+P^2+P	1	1	1	0	0	1	0
16	1	1	1	1	P^3+P^2+P+1	1	1	1	1	0	0	1

*) $P \oplus P = 0$
$P^2 \oplus P^2 = 0$
$P^3 \oplus P^3 = 0$
$P^4 \oplus P^4 = 0$

① $M(P) = 0$
$X(P) = 0 \times G(P)$
$= 0 \times (P^3 + P + 1) = 0$
$X(P) = 0$

② $M(P) = 1$
$X(P) = M(P)\, G(P)$
$= 1 \times (P^3 + P + 1)$
$= P^3 + P + 1$
$= P^3 + P + P^0$

③ $M(P) = P$
$= P(P^3 + P + 1)$
$= P^4 + P^2 + P^1$

④ $M(P) = (P+1)$
$X(P) = (P+1)(P^3 + P + 1)$
$= P^4 + P^2 + P + P^3 + P + 1$
$X(P) = P^4 + P^3 + P^2 + 1$

21/2/18

Q 1). The generator Polynomial of (7,4) cyclic code is $G(P) = P^3 + P^2 + 1$. Find all the code vector for the code in non-Systematic form.

Sol.

$n = 7$, $K = 4$, $q = n - K \Rightarrow 7 - 4 = 3$
$K = 4$, No. of message bit $= 4$
$M = (m_1, m_2, m_3, m_4)$
$q = 3$, No. of check bit $= 3$
$C = (C_1, C_2, C_3)$
$X = (M \mid C) = (m_3, m_2, m_1, m_0, C_2, C_1, C_0)$
$X(P) = M(P) \cdot G(P)$
$G(P) = P^3 + P^2 + P^1$.

Sr. No.	msg bit m_3	m_2	m_1	m_0	$M(P) = m_3P^3 + m_2P^2 + m_1P + m_0$	$X(P) = M(P) \cdot G(P)$
1	0	0	0	0	0	0
2	0	0	0	1	1	$P^3 + P^2 + 1$
3	0	0	1	0	P^1	$P^4 + P^3 + P$
4	0	0	1	1	$P + 1$	$P^4 + P^2 + P + 1$
5	0	1	0	0	P^2	$P^5 + P^4 + P^2$
6	0	1	0	1	$P^2 + 1$	$P^5 + P^4 + P^3 + 1$
7	0	1	1	0	$P^2 + P$	$P^5 + P^3 + P^2 + P$
8	0	1	1	1	$P^2 + P + 1$	$P^5 + P^4 + 1$
9	1	0	0	0	P^3	$P^6 + P^5 + P^3$
10	1	0	0	1	$P^3 + 1$	
11	1	0	1	0	$P^3 + P$	
12	1	0	1	1	$P^3 + P + 1$	
13	1	1	0	0	$P^3 + P^2$	
14	1	1	0	1	$P^3 + P^2 + 1$	
15	1	1	1	0	$P^3 + P^2 + P$	
16	1	1	1	1	$P^3 + P^2 + P + 1$	

eg: $(P^2+1)(P^3 + P^2 + 1)$
$\Rightarrow P^5 \oplus P^4 \oplus P^2 \oplus P^3 \oplus P^2 \oplus 1$
$\Rightarrow P^5 + P^4 + P^3 + 1$

$\Rightarrow (P^2)(P^3 + P^2 + 1) = P^5 + P^4 + P^2$
$\Rightarrow (P+1)(P^3 + P^2 + P) = P^4 + P^3 + P + P^3 + P^2 + 1$.
$\Rightarrow P^4 + P^2 + P + 1$

$\Rightarrow (P^2 + P)(P^3 + P^2 + 1) = P^5 + P^4 + P^2 + P^4 + P^3 + P$

$(P^2 + P + 1)(P^3 + P + 1) = P^5 + P^3 + P^2 + P^4 + P^2 + P + P^3 + P + 1$

Generation of cyclic code vector in systematic form:

$$x(P) = M(P) \,/\, c(P)$$

$c(P)$ = remainder of $\left(\frac{P^q M(P)}{G(P)}\right)$

q) The generator polynomial of (7,4) cyclic code is $G(P) = P^3 + P + 1$

⇒ $n = 7$, $k = 4$, $q = n - k \Rightarrow 7 - 4 = 3$

k = no. of msg bit 4 ($m_3\ m_2\ m_1\ m_0$)

q = " " check " 3 ($c_2\ c_1\ c_0$)

$x = m_3\ m_2\ m_1\ m_0\ c_2\ c_1\ c_0$

$c(P) \rightarrow c_2\ c_1\ c_0$ (check bit polynomial)

$M(P) \rightarrow$ msg bit polynomial

$x(P) \rightarrow$ cyclic code vector polynomial

To obtain:

$M(P) = m_3 P^3 + m_2 P^2 + m_1 P + m_0$

a) $m_3\ m_2\ m_1\ m_0 = 0101$

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

$c(P)$ = remainder of $\left(\frac{P^q M(P)}{G(P)}\right)$

$P^q = P^3$

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

$c(P)$ = remainder of $\left(\frac{P^3 (P^2+1)}{P^3+P+1}\right)$

$c(P)$ = remainder of $\left(\frac{P^5 + P^3}{P^3+P+1}\right)$

$$\begin{array}{r|l} & P^2 \\ \hline P^3+P+1 & P^5+P^3 \\ & P^3+P^3+P^2 \\ \hline & P^2 \rightarrow \text{remainder} \end{array}$$

$c(P) = c_2\ c_1\ c_0$

$c(P) = 1\ 0\ 0$

$x(P) = m_3\ m_2\ m_1\ m_0\ c_2\ c_1\ c_0$

$\Rightarrow 0101100$

b) $m_3\ m_2\ m_1\ m_0 = 1101$

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

$c(P)$ = remainder of $\left(\frac{P^q M(P)}{G(P)}\right)$

$c(P)$ = remainder of $\left(\frac{P^3 (P^3+P^2+1)}{P^3+P+1}\right)$

$c(P)$ = remainder of $\left(\frac{P^6 + P^5 + P^3}{P^3+P+1}\right)$

$$\begin{array}{r|l} & P^3+P^2+P+1 \\ \hline P^3+P+1 & P^6+P^5+P^3 \\ & P^6 \quad +P^3+P^4 \\ \hline & P^5+P^4+0+0 \\ & P^5+0+P^3+P^2 \\ \hline & P^4+P^3+P^2 \\ & P^4+0+P^2+P \\ \hline & P^3+P \\ & P^3+P+1 \\ \hline & 1 \rightarrow \text{remainder} \end{array}$$

remainder = 1

$c(P) = c_2\ c_1\ c_0 = 001$

$X(P) = M(P) / c(P) = m_3\ m_2\ m_1\ m_0\ c_2\ c_1\ c_0$

$X(P) = 1\ 1\ 0\ 1\ 0\ 0\ 1$

c) $m_3\ m_2\ m_1\ m_0 = 1001$

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

$c(P) =$ remainder of $\left(\frac{P^3 \cdot M(P)}{G(P)}\right)$

$C(P) =$ remainder of $\left(\frac{P^3\ (P^3+1)}{P^3+P+1}\right)$

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

$$\begin{array}{r|l} P^3+P+1 & P^3+P \\ \hline & P^6+P^3 \\ & \underline{P^6+P^3+P^4} \\ & P^4 \\ & \underline{P^4+P^2+P} \\ & P^2+P \end{array} \Rightarrow \text{remainder}$$

$c(P) = c_2\ c_1\ c_0 = 1+0$

$X(P) = m_3\ m_2\ m_1\ m_0\ c_2\ c_1\ c_0$

$\Rightarrow 1\ 0\ 0\ 1\ 1\ 1\ 0$

S.No.	$M = m_3$	m_2	m_1	m_0	$X = m_3$	m_2	m_1	m_0	c_2	c_1	c_0
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	1	0	0	0	1	0	1	1
3	0	0	1	0	0	0	1	0	1	1	0
4	0	0	1	1	0	0	1	1	1	0	1
5	0	1	0	0	0	1	0	0	1	1	1
6	0	1	0	1	0	1	0	1	1	0	0
7	0	1	1	0	0	1	1	0	0	0	1
8	0	1	1	1	0	1	1	1	0	1	0
9	1	0	0	0	1	0	0	0	1	0	1
10	1	0	0	1	1	0	0	1	1	1	0
11	1	0	1	0	1	0	1	0	0	1	1
12	1	0	1	1	1	0	1	1	0	0	0
13	1	1	0	0	1	1	0	0	0	1	0
14	1	1	0	1	1	1	0	1	0	0	1
15	1	1	1	0	1	1	1	0	1	0	0
16	1	1	1	1	1	1	1	1	1	1	1

#) To obtain the generator matrix of non-systematic form for cyclic code:

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

Soln: $n = 7 \quad k = 4 \quad q = n-k \Rightarrow 7-4 = 3$

rows of generator matrix is given by:

for row 1: $P^3 \cdot G(P) = P^3 \cdot (P^3+P^2+1)$

$\Rightarrow P^6+P^5+P^3$

for row 2: $P^2 \cdot G(P) = P^2 \cdot (P^3+P^2+1)$

$\Rightarrow P^5+P^4+P^2$

for row, 3 : $P \cdot G(P) = P(P^3+P^2+1) \Rightarrow P^4+P^3+P$

" " , 4 : $P^0 \cdot G(P) = 1 \cdot (P^3+P^2+1) \Rightarrow P^3+P^2+1$

$$G_{4\times 7} = \begin{array}{c} \begin{matrix} P^6 & P^5 & P^4 & P^3 & P^2 & P^1 & P^0 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

Systematic form of generator matrix for cyclic code :

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

Soln : $n = 7$, $k = 4$; $q = n-k \Rightarrow 7-4 = 3$

$t = 1$ to k

$t = 1$ to 4

$G_{n\times k} \longrightarrow G_{4\times 7} \longrightarrow$ generator matrix contain 4 rows & 7 columns

① To obtain 1st row of generator matrix

$t = 1$

$P^{n-t} = P^{7-1} = P^6$ (P^6 is divided by $G(P)$)

$$\begin{array}{r|l} P^3+P+1 & P^3+P+1 \\ \hline & P^6 \\ \hline & P^6+P^4+P^3 \\ \hline & P^4+P^3 \\ \hline & P^4+P^3 \\ \hline & P^4+P^2+P \\ \hline & P^3+P^2+P \end{array}$$

$$\begin{array}{r} P^3+P^2+P \\ \hline P^3+P+1 \\ \hline P^2+1 \end{array}$$

Quotient $= P^3+P+1$

Remainder $= P^2+1$

To obtain 1st row = $G(P) \times$ Quotient

$\Rightarrow (P^3+P+1)(P^3+P+1)$

$\Rightarrow P^6+P^4+P^3+P^4+P^2+P+P^3+P+1$

$\Rightarrow P^6+P^2+1$

② To obtain 2nd row :

$t = 2$

$P^{n-t} = P^{7-2} \Rightarrow P^5$

$$\begin{array}{r|l} P^3+P+1 & P^2+1 \\ \hline & P^5 \\ \hline & P^5+P^3+P^2 \\ \hline & P^3+P^2 \\ \hline & P^3+P+1 \\ \hline & P^2+P+1 \end{array}$$

Quotient $= P^2+1$

remainder $= P^2+P+1$

To obtain 2nd row : $G(P) \times$ Quotient

$\Rightarrow (P^3+P+1) \times (P^2+1)$

$\Rightarrow (P^5+P^3+P^3+P+P^2+1)$

$\Rightarrow P^5+P^2+P+1$

③ To obtain 3rd row :

$t = 3$

$p^{4-t} \Rightarrow p^{7-3} = p^4$ (p^4 is used by $G(p)$)

$p^3+p+1 \;\big|\; p$

p^4

p^4+p^2+p

p^2+p

quotient = p, remainder = p^2+p

To obtain 3rd row = $G(p) \times$ quotient

$\Rightarrow (p^3+p^2+1) \cdot p$

$\Rightarrow p^4+p^2+p$

(4) To obtain 4th row, $t=4$

$p^{4-t} = p^{7-4} \Rightarrow p^3$

$p^3+p+1 \;\big|\; 1$

p^3

p^3+p+1

$p+1$ → remainder

quotient = 1

To obtain 4th row = $G(p) \times$ quotient

$\Rightarrow (p^3+p+1) \cdot 1$

$\Rightarrow p^3+p+1$

$$G_{7\times4} = \left[\begin{array}{ccccc|ccc} p^6 & p^5 & p^4 & p^3 & p^2 & p^1 & p^0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right]$$

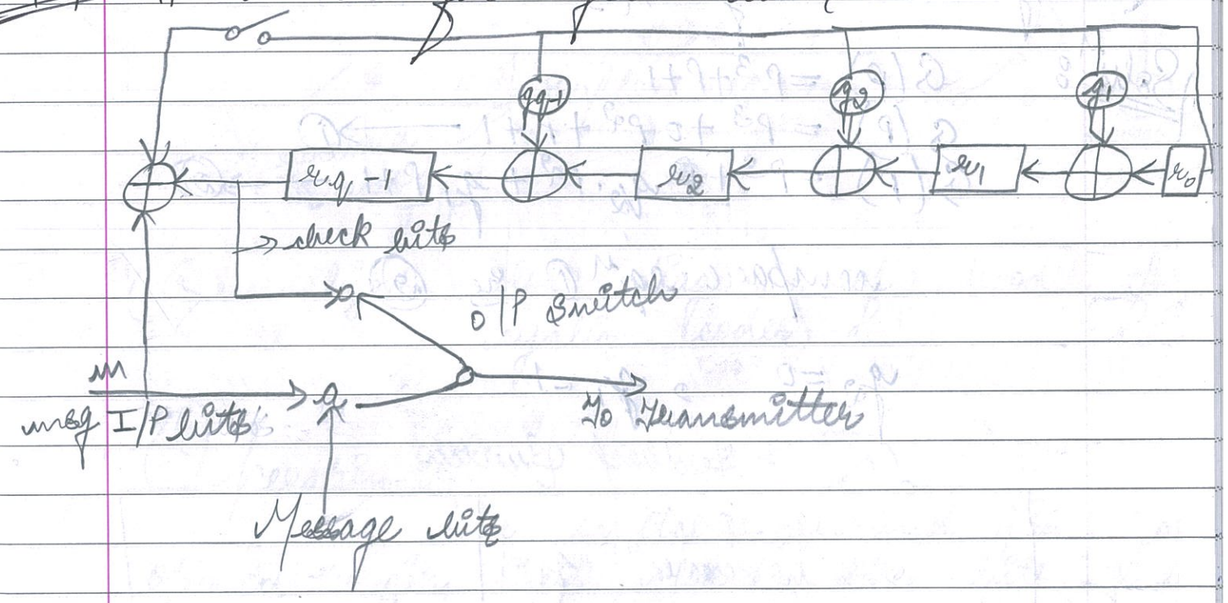
$G = (I_K : P) = [I_4 : P]$

$$P = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad P^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

parity check matrix → $H = [P^T : I_q]$

$$= \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

14/3/18 # encoder for cyclic codes:



Operation:

The feedback switch is first closed. The o/p switch is connected to msg o/p. All the shift registers are initialized to all zero state. The k msg bits are shifted to the transmitter as well as

shifted into the register. After the shift of k msg bits the register contain 'q' check bits. The feedback switch is now opened & o/p switch is connected to check bits position.

k → no. of msg bits
q → " " check "

9) Design the encoder for the (7,4) cyclic code generated by $G(p) = p^3+p+1$

Soln:

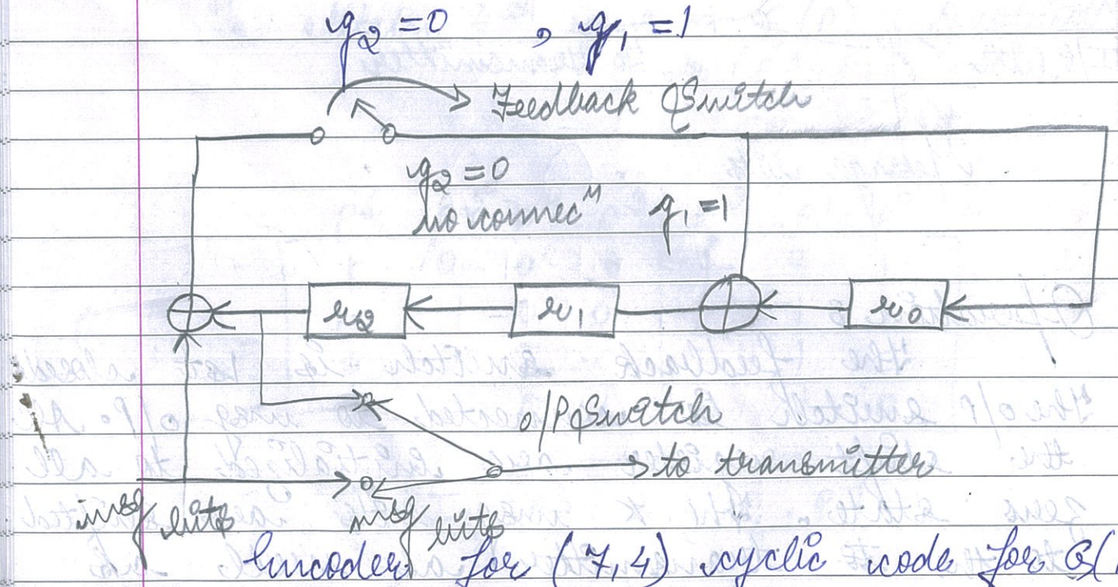
$G(p) = p^3+p+1$

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

$G(p) = p^3 + q_2 p^2 + q_1 p + 1 \longrightarrow (2)$

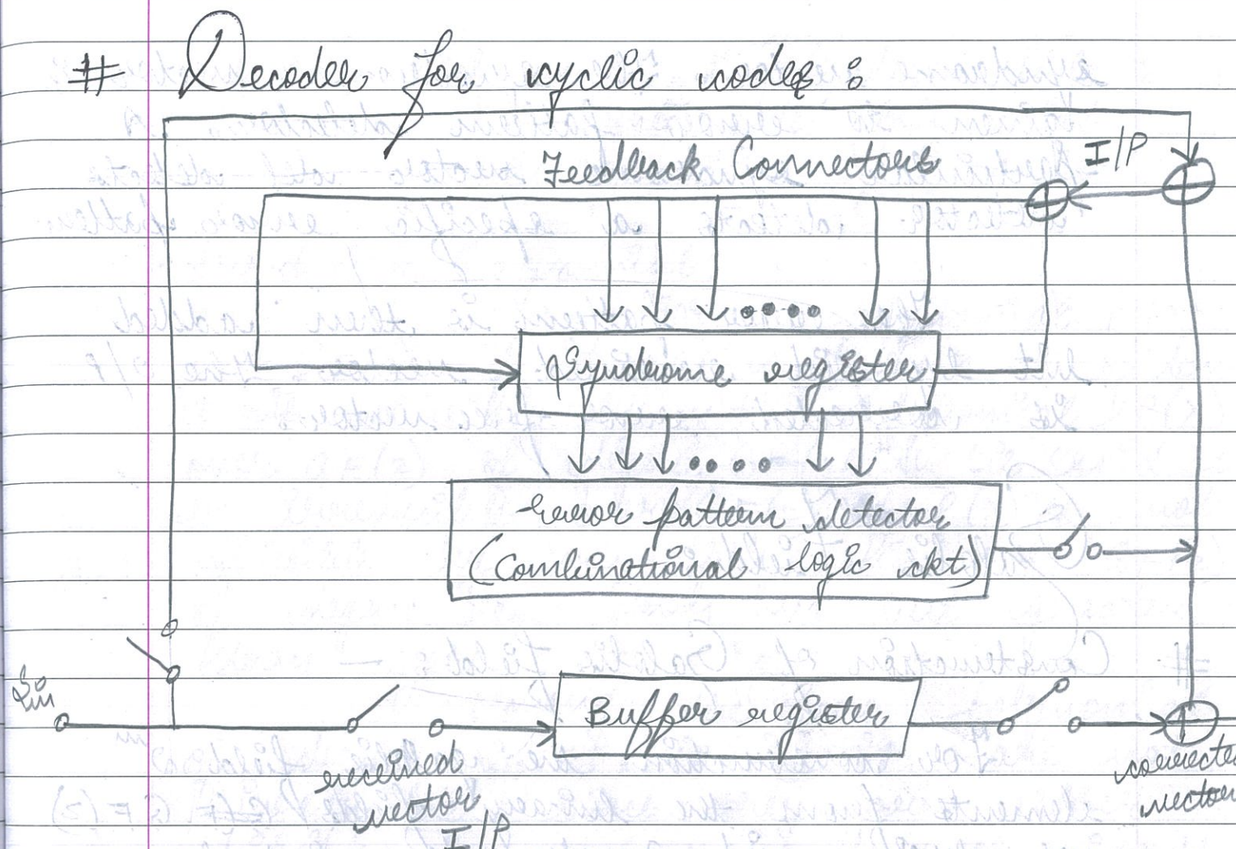
compare eq^n (1) & (2)

$q_2 = 0$, $q_1 = 1$



Encoders for (7,4) cyclic code for $G(p) = p^3+p+1$

Decoder for cyclic codes:



(Generalized block diagram of decoder for cyclic codes)

Operation:

The switches named Sout are opened & Sin are closed. The bits of the received vector Y are shifted into the buffer register as well as they are shifted into the syndrome calculator. When all the 'n' bits of received vector 'Y' are shifted into buffer register & syndrome calculates the syndrome register holds a

syndrome vector. The syndrome vector is given to error pattern detector. A particular syndrome ~~vector det detects~~ detector detects a specific error pattern.

The error pattern is then added bit by bit received vector. The o/p is corrected error free vector.

Galois Field:

Construction of Galois field :—

For construction the galois field 2^m elements from the binary fields GF GF(2) we begin with 2 elements 0 & 1 from the GF(2) & new symbol α.

Then we define a multiply to introduce a sequence of power of α as follows:

GF(2)

$0 \cdot 0 = 0$

$0 \cdot 1 = 1 \cdot 0 = 0$

$1 \cdot 1 = 01$

$0 \cdot \alpha = \alpha \cdot 0 = 0$

$1 \cdot \alpha = \alpha \cdot 1 = \alpha$

$\alpha^2 = \alpha \cdot \alpha$

$\alpha^3 = \alpha \cdot \alpha \cdot \alpha$

$\alpha^j = \alpha \cdot \alpha \cdot \alpha - - - \alpha$ (j times)

Types of Polynomial in Galois field :

① Irreducible polynomial

② Primitive polynomial

Irreducible Polynomial:

For a polynomial F(x) over GF(2), if it has an even no. of terms it is divisible by x+1. A polynomial P(x) over GF(2) of degree ~~GF(2)~~ m is said to be irreducible over GF(2) if P(x) is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.

Among the four polynomial of degree 2; x^2, x^2+1 & x^2+x are not irreducible, since they are either divisible by x or x+1. However, x^2+x+1 does not have either "0" or "1" as a root & therefore, it is not divisible by any polynomial of degree 1. Therefore, x^2+x+1 is an irreducible polynomial of degree 2.

Similarly, x^3+x+1 is an irreducible polynomial of degree 3. We note that x^3+x+1 does not divisible by x or x+1. Since it is not divisible by any polynomial of degree 1, it cannot be divisible by polynomial of degree 2.

Pg → 4.39

9) Using suitable example prove that Irreducible polynomial over GF(2) of degree m divides $x^{2^m-1}+1$.

Soln: For m = 4, we can check that x^4+x+1 divides $x^{2^4-1} = x^{15}+1$.

$$
\begin{array}{l}
x^4+x+1 \;\big)\; x^{15}+1 \\
\quad x^{15}+x^{12}+x^{11} \\
\quad x^{12}+x^{11}+1 \\
\quad x^{12}+x^9+x^8+1 \\
\quad x^{11}+x^9+x^8+1 \\
\quad x^{11}+x^8+x^7 \\
\quad x^9+x^7+1 \\
\quad x^9+x^6+x^5 \\
\quad x^7+x^6+x^5+1 \\
\quad x^7+x^4+x^3 \\
\quad x^6+x^5+x^4+x^3+1 \\
\quad x^6+x^3+x^2 \\
\quad x^5+x^4+x^2+1 \\
\quad x^5+x^2+x \\
\quad x^4+x+1 \\
\quad x^4+x+1 \\
\quad 0\;0\;0
\end{array}
$$

which proves that any irreducible polynomial over GF(2) of degree m divides the polynomial $x^{2^m-1}+1$.

Primitive Polynomial:

An irreducible polynomial P(x) of degree (m) is said to be primitive if the smallest (+ve) integer n for which P(x) divides x^n+1 is $n = 2^m-1$. We may check that $P(x) = x^4+x+1$ divides any x^n+1 for $1 \le n \le 15$.

Hence x^4+x+1 is a primitive polynomial.

List of Primitive Polynomial:

m	Primitive polynomial of degree (m)
3	x^3+x+1
4	x^4+x+1
5	x^5+x^2+1
6	x^6+x+1
7	x^7+x+1
8	$x^8+x^4+x^3+x^2+1$
9	x^9+x^4+1
10	$x^{10}+x^3+1$

9) The polynomial $P(x) = x^4+x+1$ is a primitive polynomial over GF(2) for m = 4. Construct the Galois field $m=4$ $GF(2^4)$ from the binary field GF(2).

Soln: $P(\alpha) = x^4+x+1$

$P(\alpha) = \alpha^4+\alpha+1$

$\Rightarrow P(\alpha) = 0$

$\Rightarrow \alpha^4 + \alpha + 1 = 0$

$\Rightarrow \alpha^4 = 1 + \alpha$

$\Rightarrow \alpha^5 = \alpha \cdot \alpha^4 = \alpha(1+\alpha)$

$\Rightarrow \alpha + \alpha^2$

$\Rightarrow \alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha + \alpha^2) \Rightarrow \alpha^2 + \alpha^3$

$\Rightarrow \alpha^7 = \alpha \cdot \alpha^6 \Rightarrow \alpha(\alpha^2 + \alpha^3)$

$\Rightarrow \alpha^3 + \alpha^4$

$\Rightarrow \alpha^7 = \alpha^3 + \alpha + 1$

Representation for the element of $GF(2^4)$ generated by $P(x) = 1 + x + x^4$

Power representation	Polynomial representation	4-Tuple representation
0	0	0000
1	1	1000
2	α	0100
3	α^2	0010
4	$1+\alpha$	0110
5	$\alpha + \alpha^2$	0011
6	$\alpha^2 + \alpha^3$	1101
7	$1 + \alpha + \alpha^3$	1010

Properties :

A number of properties of GF are given as :

① The galois polynomial $\phi(x)$ of a field element β is irreducible.

Proof : Suppose that $\phi(x)$ is not irreducible and $\phi(x) = \phi_1(x)\phi_2(x)$, where both $\phi_1(x)$ & $\phi_2(x)$ have degrees greater than 0 & less than the degree of $\phi(x)$. Since $\phi(\beta) = \phi_1(\beta)\phi_2(\beta) = 0$, either $\phi_1(\beta) = 0$ or $\phi_2(\beta) = 0$. This contradicts the hypothesis that $\phi(x)$ is a polynomial of smallest degree such that $\phi(\beta) = 0$. Therefore, $\phi(x)$ must be irreducible.

② Consider $f(x)$ be a polynomial over GF(2), and $\phi(x)$ be the galois polynomial of a field element β. If β is a root of $f(x)$ then $f(x)$ is divisible by $\phi(x)$.

Proof : Dividing $f(x)$ by $\phi(x)$, we obtain

$$f(x) = a(x)\,\phi(x) + r(x)$$

where the degree of remainder $r(x)$ is less than the degree of $\phi(x)$. Substituting the β into the equation above & using the fact that $f(\beta) = \phi(\beta) = 0$, we have $r(\beta) = 0$.

If $r(x) \neq 0$, $r(x)$ would be a polynomial of lower degree than $\phi(x)$, so has β as root. This is the

contradiction to the fact that $\phi(x)$ is the polynomial of element β. Hence, $x(x)$ must be identical to or $\phi(x)$ divides $f(x)$.

(3) Let $\phi(x)$ be the galois polynomial of an element β in $GF(2^m)$. Let e be the smallest integer such that $\beta^{2^e} = \beta$. Then:

$$\phi(x) = \prod_{i=0}^{e-1} (x + \beta^{2^i})$$

Page No.: 16/03/18

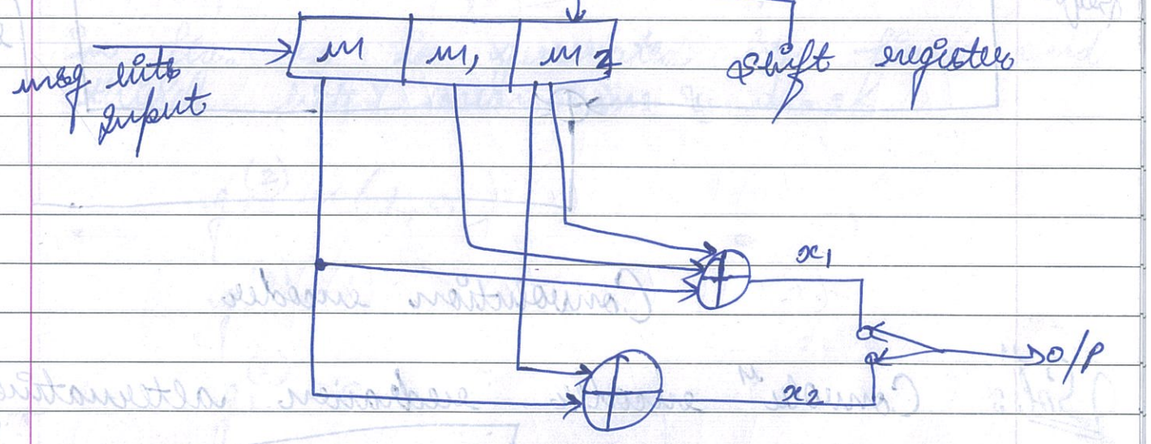
"Unit - 5"

Convolution Codes

Defination of Convolution Coding:

A convolution coding is done by combining the fixed number of input bits. The input bits are stored in the fixed length shift register & they are combined with the help of mod-2 adders. This operation is equivalent to binary convolution and hence it is k/n a convolu" coding.

Block diagram of Convolution encoder with $k=3$, $k=1$, $n=2$.



$K \longrightarrow$ Constraint length

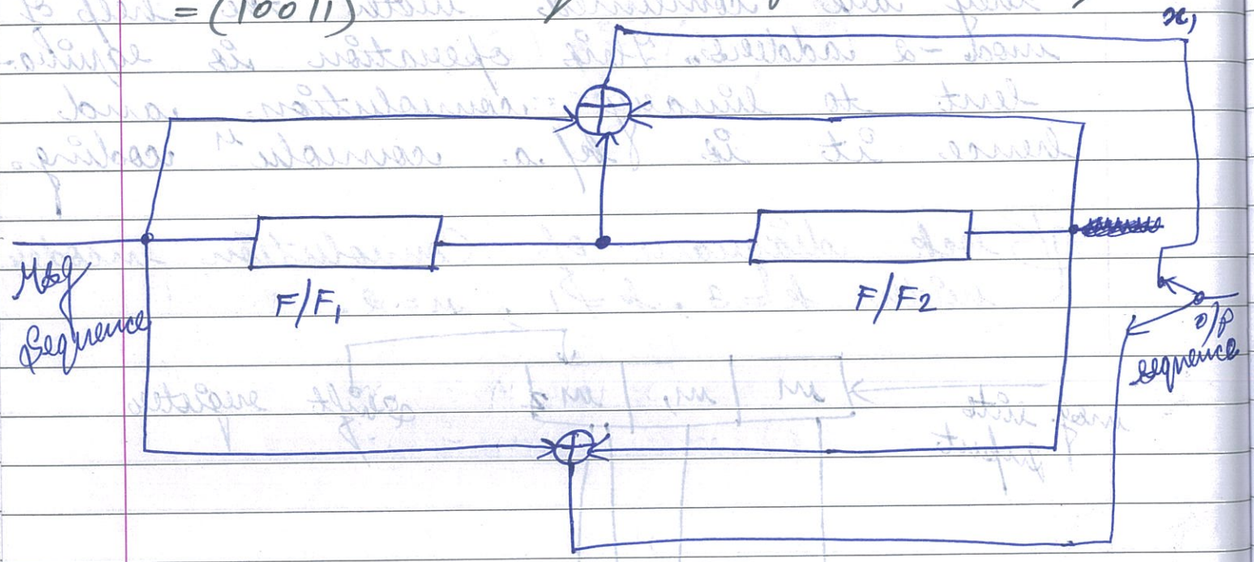
$(n, k) \longrightarrow$ Dimension of codes

Code rate $= r = k/n$

[10-16 M]

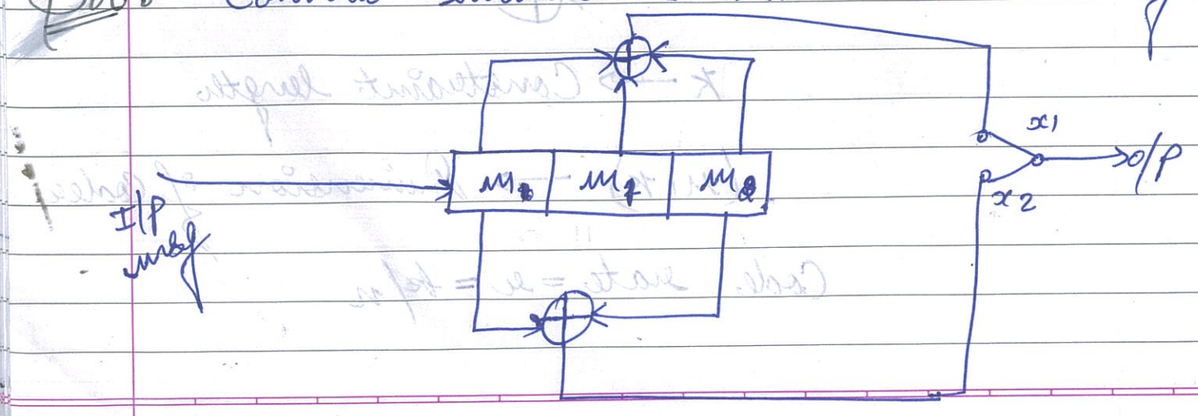
Q) For the convolution encoder of figure determine the follg:

① Dimension of the code
② code rate
③ Constraint length
④ Generating sequence
⑤ o/p sequence for msg sequence of m = (10011)



Convolution encoder

Sol: Convolu" encoder redrawn alternatively:



$x_1 = m \oplus m_1 \oplus m_2$

$x_2 = m \oplus m_2$

① Dimension of the code:
$n = 2 \quad k = 1$
$(n, k) = (2, 1)$

② $r = k/n = 1/2$ (code rate)

③ Constraint length $= k = 3$

④ Generating sequence:
In fig. x_1 is generated by adding all three bits :-

$g_i^{(1)} = (1, 1, 1)$

$g_0^{(1)} = 1 \quad , g_1^{(1)} = 1 \quad , g_2^{(1)} = 1$

In fig. x_2 is generated by first and thirdd bits means in m_2:

$g_i^{(2)} = (1, 0, 1)$

$g_0^{(2)} = 1$

$g_1^{(2)} = 0$

$g_2^{(2)} = 1$

⑤ obtain the o/p sequence for (10011)

$m = (10011)$

$x_1 = m \oplus m_1 \oplus m_2$

$x_2 = m \oplus m_2$

a) $m = 1$, $m_1 = 0$, $m_2 = 0$ } (initial)

$x_1 = 1 \oplus 0 \oplus 0 = 1$

$x_2 = 1 \oplus 0 = 1$

$\Rightarrow 11$

b) $m = 0$

$m_1 = 1$

$m_2 = 0$

$x_1 = 0 \oplus 1 \oplus 0 = 1$

$x_2 = 0 \oplus 0 = 0$

$\Rightarrow 10$

c) $m = 0$

$m_1 = 0$

$m_2 = 1$

$x_1 = 0 \oplus 0 \oplus 1 = 1$

$x_2 = 0 \oplus 1 = 1$

$\Rightarrow 11$

d) $m = 1$

$m_1 = 0$

$m_2 = 0$

$x_1 = 1 \oplus 0 \oplus 0 = 1$

$x_2 = 1 \oplus 0 = 1$

$\Rightarrow 11$

e) $m = 1$

$m_1 = 1$

$m_2 = 0$

$x_1 = 1 \oplus 0 \oplus 0 = 0$

$x_2 = 1 \oplus 0 = 1$

$\Rightarrow 01$

f) $m = 0$

$m_1 = 1$

$m_2 = 1$

$x_1 = 0 \oplus 1 \oplus 1 = 0$

$x_2 = 0 \oplus 1 = 1$

$\Rightarrow 01$

g) $m = 0$

$m_1 = 0$

$m_2 = 1$

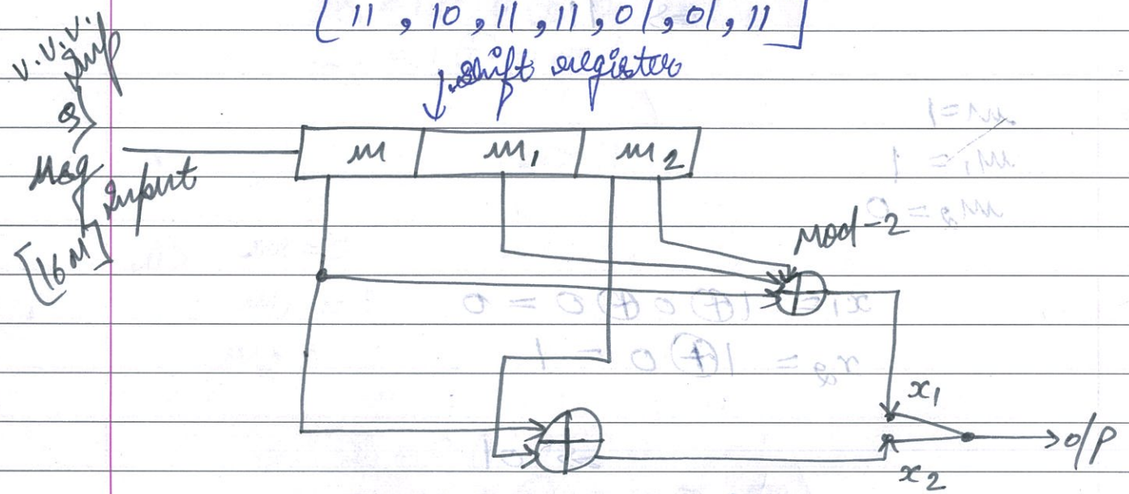
$x_1 = 0 \oplus 0 \oplus 1 = 1$

$x_2 = 0 \oplus 1 = 1$

$\Rightarrow 11$

Final o/p Sequence :

$[11, 10, 11, 11, 01, 01, 11]$



a) Find out the state table.

b) Draw code tree for convolution encoder.

c) Draw code trellis for convolution encoder.

d) State diagram for convolution encoder.

Soln :

$x_1 = m \oplus m_1 \oplus m_2$

$x_2 = m \oplus m_2$

a) State table for convolution encoder :

m_2	m_1	State of encoder
0	0	a
0	1	b
1	0	c
1	1	d

b) ① $m_2 = 0$, $m_1 = 0$ ($00 \rightarrow a \rightarrow$ current state)

a) Let $m = 0$

$m = 0$, $m_1 = 0$, $m_2 = 0$

$x_1 = 0 \oplus 0 \oplus 0 = 0$

$x_2 = 0 \oplus 0 = 0$ $(00 \rightarrow o/p)$

Next state :

$m = 0 \rightarrow m_1 = 0$, $m_2 = 0$

$m_2 = 0$

$m_1 = 0$

$\Rightarrow (00 - o/p)$

b) $m = 1$

$m = 1$, $m_1 = 0$, $m_2 = 0$

$x_1 = 1 \oplus 0 \oplus 0 = 1$

$x_2 = 1 \oplus 0 = 1$

$(11 \rightarrow o/p)$

Next state :

$m_1 = 1$

$m_2 = 0$

$m_2 = 0$, $m_1 = 1$

(01 → b → Next state)

(2) $m_2 = 0$, $m_1 = 1$

(0,1) → b → current state

a) Let $m = 0$

$m = 0$, $m_1 = 1$, $m_2 = 0$

$x_1 = 0 \oplus 1 \oplus 0 = 1$

$x_2 = 0 \oplus 0 = 0$

(1,0 → 0/P)

Next state :

$m_1 = 0$, $m_2 = 1$

$m_2 = 1$, $m_1 = 0$

(1,0 → c → next state)

b) $m = 1$

$m = 1$

$m_1 = 1$

$m_2 = 0$

$x_1 = 1 \oplus 1 \oplus 0 = 0$

$x_2 = 1 \oplus 0 = 1$

(11 → 0/P)

Next state :

$m_1 = 1$

$m_2 = 1$

(11 → d → next state)

(3) $m_2 = 1$, $m_1 = 0$

a) $m = 0$, $m_1 = 0$, $m_2 = 1$ (CS)

~~$m = 0$, $m_1 = 0$, $m_2 = 0$ (NS)~~

$x_1 = 1$, $x_2 = 1$

m_2 (11 → 0/P)

$m_1 = 0$, $m_2 = 0$

$m_2 = 0$, $m_1 = 0$

(00 → a → NS)

b) $m = 1$

$m = 1$, $m_1 = 0$, $m_2 = 1$ (CS)

$x_1 = 0$, $x_2 = 0$

⇒ (00 → 0/P)

$m_1 = 1$, $m_2 = 0$

$m_2 = 0$, $m_1 = 1$

(01 → b → NS)

Page No.:

Page No.: 23/3/18

④ $m_2 = 1$, $m_1 = 1$

$(11 \rightarrow d \rightarrow CS)$

a) $m = 0$

$m = 0$, $m_1 = 1$, $m_2 = 1$

$x_1 = 0$

$x_2 = 1$ $\quad (01 \rightarrow 0/P)$

$m_1 = 0$

$m_2 = 1$

$m_2 = 1$, $m_1 = 0$

$(10 \rightarrow NS)$

b) $m = 1$

$m = 1$, $m_1 = 1$, $m_2 = 1$

$x_1 = 1$

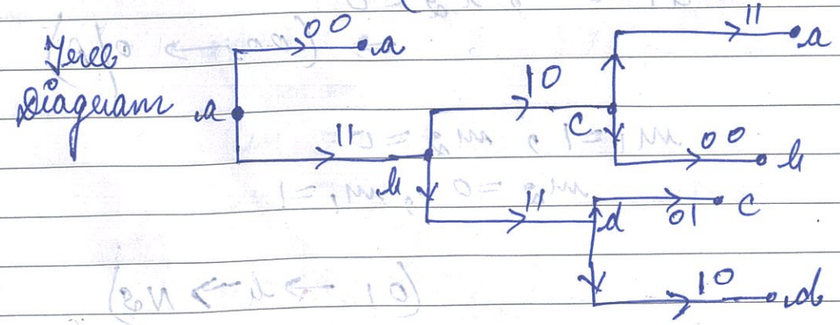
$x_2 = 0$ $\quad (10 \rightarrow 0/P)$

$m_1 = 1$, $m_2 = 1$

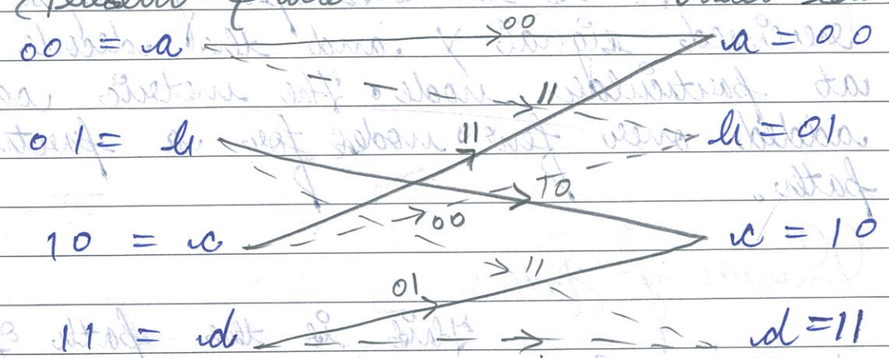
$m_2 = 1$, $m_1 = 1$ $\quad (11 \rightarrow d \rightarrow$ next state)

$(11 \rightarrow d \rightarrow NS)$

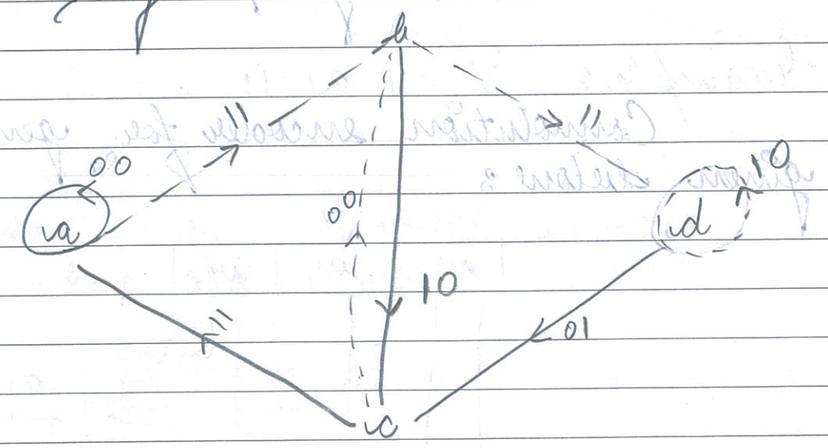
Tree Diagram



c) Trellis Diagram



d) State Diagram :



Viterbi Algorithm for Decoding of convolution codes (Maximum likehood Decoding)

Let's represents the received signal is Y. Convolution encoding operates continiously on input data. Hence there are no code vectors and blocks as such. Let's assume the transmission error probability

of symbols 1's & 0's same.

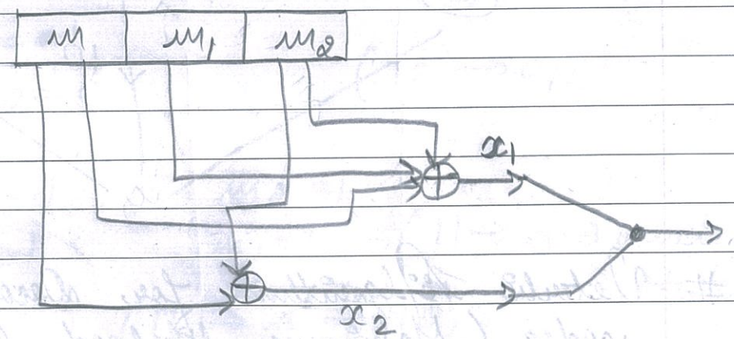
Metric: It is the discrepency (difference) b/w the received signal y and the decode signal at particular node. The metric can be added over few nodes for a particular path.

Surviving Path:

This is the path of the decoded signal with min. metric. In veterbi decoding a metric is assigned to each surviving path.

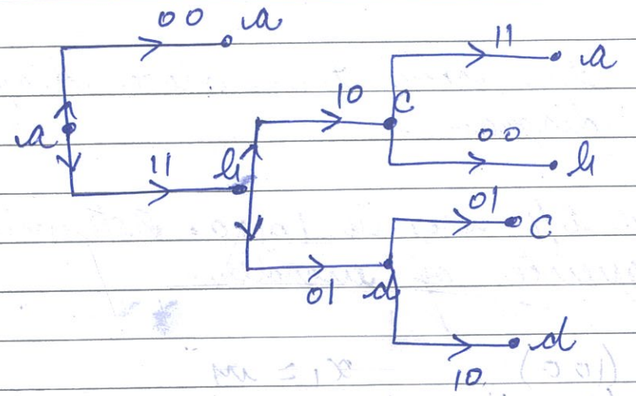
Example: $Y = 11\ 01\ 11$

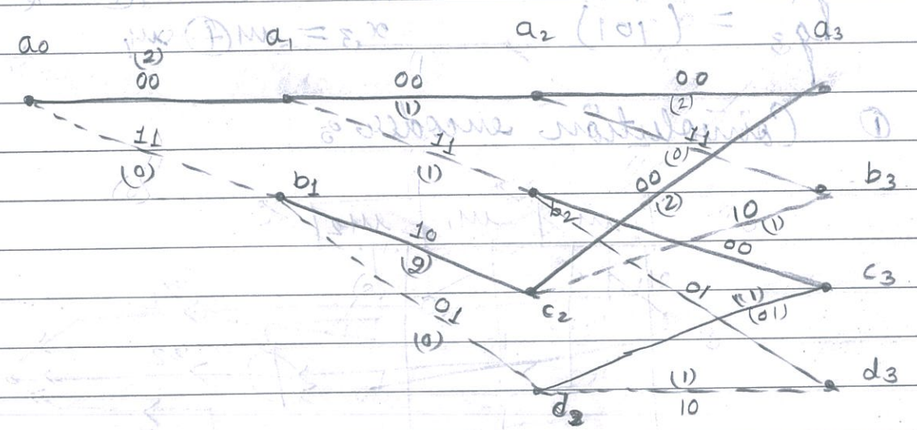
Convolution encoder for generate Y is given below:



Soln: $Y = 11\ 01\ 11$ → received signal

Trellis diagram for given convolu" encoder —





$a_0\ a_1\ a_2\ a_3$ = 5 metric (2+1+2)

$a_0\ b_1\ c_2\ a_3$ = 2 metric (0+2+0)

Surviving Path = $a_0\ b_1\ c_2\ a_3$

Because it has min. metric of 2.

Q) A convolution encoder (3,1) has generating vectors as:

$g_1 = (100)$

$g_2 = (111)$

$g_3 = (101)$

① Sketch encoder

② Draw the code tree, state diagram, trellis diagram.

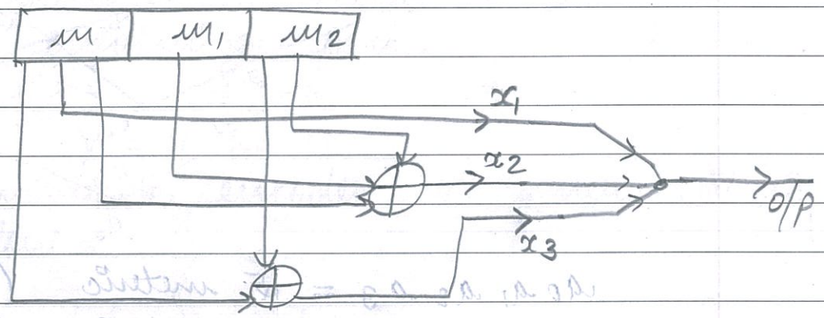
② If the i/p msg is 10110. Determine the o/p sequence of encoder.

$\Rightarrow$ $g_1 = (100)$ $\quad x_1 = m$

$g_2 = (111)$ $\quad x_2 = m \oplus m_1 \oplus m_2$

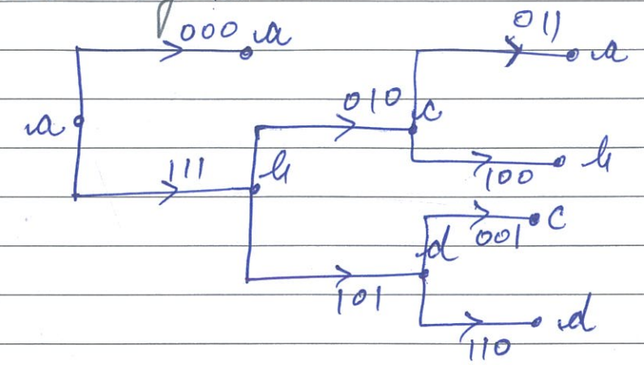
$g_3 = (101)$ $\quad x_3 = m \oplus m_1$

① Convolution encoder :

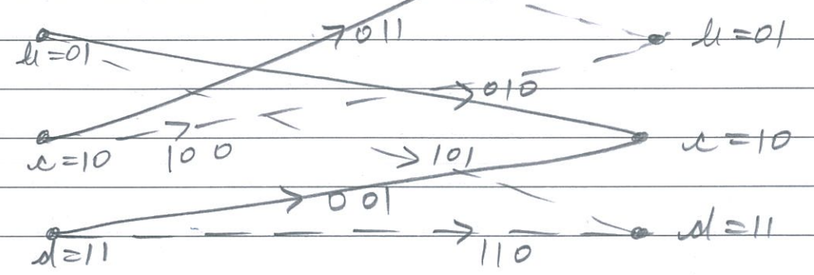


Sr. No.	Current state m_2 m_1	Input (m)	o/p $x_1 = m$; $x_2 = m \oplus m_1 \oplus m_2$; $x_3 = m \oplus m_2$
1	a = 0 0	0	0 0 0
		1	1 1 1
2	b = 0 1	0	0 1 0
		1	1 0 1
3	c = 1 0	0	0 1 1
		1	1 0 0
4	d = 1 1	0	0 0 1
		1	1 1 0

② Tree diagram :



Trellis Diagram :



State Diagram :