Linear code:

A code is 'linear' if the sum of any two code vectors produces another code vector.

$$x = (m_1, m_2, m_3, \ldots\ldots m_k \; c_1, c_2 \ldots\ldots c_q)$$

Here $q = n-k$

$$X = (M|C)$$

where M - 'k' bit message vector
C - 'q' bit check vector

Matrix Description of linear block codes

The code vector can be represented as

$$X = MG$$

where X = code vector of $(1\times n)$ size
M = Message vector of $(1\times k)$ size
G = Generator matrix of $(k\times n)$ size

$$[X]_{1\times n} = [M]_{1\times k} \, [G]_{k\times n}$$

The generator matrix depends upon the linear block code used.

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

where I_k = $k\times k$ Identity matrix
P = $k\times q$ Submatrix

Linear block codes:

Principle of block coding:

For the blocks of 'k' message bits, (n-k) parity bits or check bits are added. Hence the total bits at the output and of channel encoder are 'n'. Such codes are called (n, k) block codes.

Message block input $\longrightarrow$ $\boxed{\text{Channel Decoder}}$ $\longrightarrow$ code block output

Message

$\longleftrightarrow$ K bits

Message	check bits
$\longleftrightarrow$ k	$\longleftrightarrow$ (n-k)

$\longleftrightarrow$ n bits

Systematic codes:

* In the systematic block code, the message bits appear at the begining of the code word.

* Message bits appear first and then check bits are transmitted in a block.

Non-systematic codes:

In non-systematic code, it is not possible to identify message bits and check bits. They are mixed in the block.

The check vector can be obtained as,

$$C = MP$$

$$[c_1\ c_2 \cdots c_q]_{1\times q} = [m_1\ m_2 \cdots m_k]_{1\times k} \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1q} \\ P_{21} & P_{22} & \cdots & P_{2q} \\ \vdots & & & \\ P_{k1} & P_{k2} & \cdots & P_{kq} \end{bmatrix}_{k\times q}$$

$$c_1 = m_1 P_{11} \oplus m_2 P_{21} \oplus m_3 P_{31} \oplus \cdots \cdots \oplus m_k P_{k1}$$

$$c_2 = m_1 P_{12} \oplus m_2 P_{22} \oplus m_3 P_{32} \oplus \cdots \cdots \oplus m_k P_{k2}$$

$$c_3 = m_1 P_{13} \oplus m_2 P_{23} \oplus m_3 P_{33} \oplus \cdots \cdots \oplus m_k P_{k3}$$

* All the additions are mod-2 additions.

Eg: 1. The generator matrix for a (6,3) block code is given below. Find all code vectors of this code.

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

a) To obtain 'P' submatrix

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

$$I_k = I_{3\times 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and $P_{k\times q} = P_{3\times 3} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

b) To obtain the equations for check bits

$k=3$, $q=3$ and $n=6$

S.No.	Bits of message vector in one block m_1	m_2	m_3
1	0	0	0
2	0	0	1
3	0	1	0
4	0	1	1
5	1	0	0
6	1	0	1
7	1	1	0
8	1	1	1

'P' submatrix is given as

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

$$[c_1 \ c_2 \ c_3] = [m_1 \ m_2 \ m_3] \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$$c_1 = (m_1 \times 0) \oplus (m_2 \times 1) \oplus (m_3 \times 1) = m_2 \oplus m_3$$

$$c_2 = (m_1 \times 1) \oplus (m_2 \times 0) \oplus (m_3 \times 1) = m_1 \oplus m_3$$

$$c_3 = (m_1 \times 1) \oplus (m_2 \times 1) \oplus (m_3 \times 0) = m_1 \oplus m_2$$

c) To determine check bits and code vectors for every message vector

$$c_1 = 0 \oplus 0 = 0$$

$$c_2 = 0 \oplus 0 = 0$$

$$c_3 = 0 \oplus 0 = 0$$

S.No.	Bits of message vector in one block	check bits $c_1 = m_2 \oplus m_3$	$c_2 = m_1 \oplus m_3$	$c_3 = m_1 \oplus m_2$	Complete code vector $m_1\ m_2\ m_3\ c_1\ c_2\ c_3$
1	0 0 0	0	0	0	0 0 0 0 0 0
2	0 0 1	1	1	0	0 0 1 1 1 0
3	0 1 0	1	0	1	0 1 0 1 0 1
4	0 1 1	0	1	1	0 1 1 0 1 1
5	1 0 0	0	1	1	1 0 0 0 1 1
6	1 0 1	1	0	1	1 0 1 1 0 1
7	1 1 0	1	1	0	1 1 0 1 1 0
8	1 1 1	0	0	0	1 1 1 0 0 0

Parity check matrix (H)

For every block code, there is a $q \times n$ parity check matrix (H)

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

where P^T is the transpose of P submatrix,

$$P = \begin{bmatrix} P_{11} & P_{12} & P_{13} & \cdots & P_{1q} \\ P_{21} & P_{22} & P_{23} & \cdots & P_{2q} \\ P_{31} & P_{32} & P_{33} & \cdots & P_{3q} \\ \vdots & & & & \\ P_{k1} & P_{k2} & P_{k3} & \cdots & P_{kq} \end{bmatrix}_{k \times q}$$

$$P^T = \begin{bmatrix} P_{11} & P_{21} & P_{31} & \cdots & P_{k1} \\ P_{12} & P_{22} & P_{32} & \cdots & P_{k2} \\ P_{13} & P_{23} & P_{33} & \cdots & P_{k3} \\ \vdots & & & & \\ P_{1q} & P_{3q} & P_{3q} & \cdots & P_{kq} \end{bmatrix}_{\cancel{k \times q}\ q \times k}$$

$$H_{q \times n} = \left[\begin{array}{ccccc|cccc} P_{11} & P_{21} & P_{31} & \cdots & P_{k1} & 1 & 0 & \cdots & 0 \\ P_{12} & P_{22} & P_{32} & \cdots & P_{k2} & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots & \vdots & & & \\ P_{1q} & P_{2q} & P_{3q} & \cdots & P_{kq} & 0 & 0 & \cdots & 1 \end{array}\right]_{q \times n}$$

Hamming codes

Hamming codes are (n, k) linear block codes. These codes satisfy the following conditions,

1) Number of check bits $q \geq 3$
2) Block length $n = 2^q - 1$
3) Number of message bits $k = n - q$
4) Minimum distance $d_{min} = 3$

code rate $r = \frac{k}{n}$ (for Hamming code $k = n - q$)

$$= \frac{n-q}{n} = 1 - \frac{q}{n}$$

$n = 2^q - 1$

$$\boxed{r = 1 - \frac{q}{2^q - 1}}$$

Number of errors detected / corrected	Distance requirement
1. Detect upto 's' errors per word	$d_{min} \geq s+1$
2. Correct upto 't' errors per word	$d_{min} \geq 2t+1$
3. Correct upto 't' errors and detect $s > t$ errors per word	$d_{min} \geq t+s+1$

Eg: 2 The parity check matrix of a particular (7, 4) linear block code is given by

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

a) Find the generator matrix (G).

b) List all the code vectors

c) What is the minimum distance between code vectors?

d) How many errors can be detected? How many errors can be corrected?

$n = 7 \qquad k = 4$

No. of check bits $q = 7 - 4 = 3$

$n = 2^q - 1 \quad = 2^3 - 1 = 7$

To determine the 'p' submatrix

$$[H]_{3\times7} = \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

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

$$P = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{4\times3}$$

To obtain the generator matrix (G):

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

$$G = [I_4 : P_{4\times 3}]_{4\times 7} = \begin{bmatrix} 1 & 0 & 0 & 0 & : & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & : & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & : & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & : & 0 & 1 & 1 \end{bmatrix}_{4\times 7}$$

To find all the code words

$$[c_1\ c_2\ c_3] = [m_1\ m_2\ m_3\ m_4] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{4\times 3}$$

$\cancel{c_1 = m_1 \oplus m_2 \oplus m_3}$

$\cancel{c_2 = m_1 \oplus m_2}$

$\cancel{c_3 = m_1 \oplus m_3}$

$\cancel{c_4 = m_2 \oplus m_3}$

$c_1 = m_1 \oplus m_2 \oplus m_3$

$c_2 = m_1 \oplus m_2 \oplus m_4$

$c_3 = m_1 \oplus m_3 \oplus m_4$

Message vector				Check bits			code vector	weight of the code
m_1	m_2	m_3	m_4	c_1	c_2	c_3		$w(x)$
0	0	0	0	0	0	0	0000000	0
0	0	0	1	0	1	1	0001 011	3
0	0	1	0	1	0	1	0010 101	3
0	0	1	1	1	1	0	0011 110	4
0	1	0	0	1	1	0	0100 110	3
0	1	0	1	1	0	1	0101 101	4
0	1	1	0	0	1	1	0110 011	4
0	1	1	1	0	0	0	0111000	3
1	0	0	0	1	1	1	1000 111	4

Message vector $m_1\ m_2\ m_3\ m_4$	Check bits $c_1\ c_2\ c_3$	Code vector	Weight of the code $w(x)$
1 0 0 1	1 0 0	1001100	3
1 0 1 0	0 1 0	1010 010	3
1 0 1 1	0 0 1	1011001	4
1 1 0 0	0 0 1	1100 001	3
1 1 0 1	0 1 0	1101010	4
1 1 1 0	1 0 0	1110100	4
1 1 1 1	1 1 1	1111111	7

Minimum distance between code vectors:

The minimum distance of a linear block code is equal to the minimum weight of any non-zero code vector

i.e., $d_{min} = [w(x)]_{min} = 3$

Error detection and correction capabilities

$d_{min} \geq s+1$

$3 \geq s+1$

$s \leq 2$

Thus two errors can be detected

and $d_{min} \geq 2t+1$

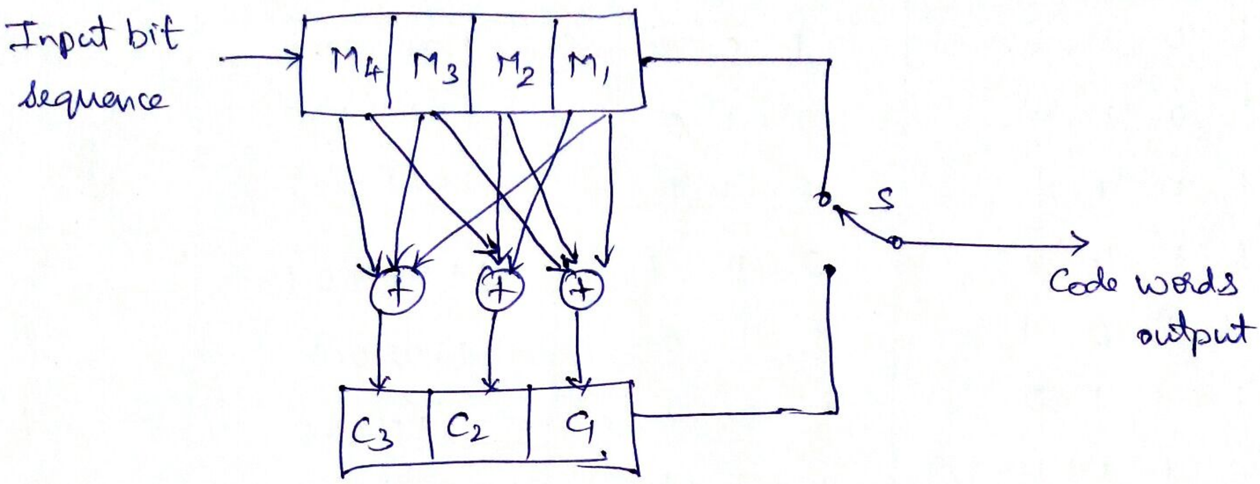
$3 \geq 2t+1$

$2 \geq 2t$

$t \leq 1$

Thus one error can be corrected.

Encoder of (7, 4) Hamming code



Syndrome Decoding

$X = Y$ if there are no transmission errors

and $X \neq Y$ if there are errors created during transmission

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

$$H^T = \begin{bmatrix} P \\ \cdots \\ I_q \end{bmatrix}_{n \times q}$$

Important property used in syndrome decoding

$$X \cdot H^T = (0\,0\,0 \ldots 0)$$

eg:- $H^T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}_{7 \times 3}$ $\quad X = (0\,0\,1\,0\,1\,0\,1)$

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

$$= (0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \quad 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1)$$

$$= (0 \; 0 \; 0)$$

This proves the property.

* At the receiver, the received code vector is Y.

$YH^T = (0 \; 0 \ldots 0)$, if $X = Y$ i.e, No errors

$YH^T =$ Non Zero, if $X \neq Y$ i.e, some errors.

Definition of Syndrome (s)

The Non Zero output of the product YH^T is called Syndrome and it is used to detect the errors in S.

$$S = YH^T$$

(or)

$$[S]_{1 \times q} = [Y]_{1 \times n} [H^T]_{n \times q}$$

Detecting error with the help of Syndrome and error vector (E)

* The non zero elements of 's' represent error in the output.

* when all elements of 's' are zero ~~th~~ two cases are possible.

a) No error in the output and $Y = X$

b) Y is some other valid code other than X. This means the transmission errors are undetectable.

Example :

$X = (1 \quad 0 \quad 1 \quad 1 \quad 0)$ be a transmitted vector

$Y = (1 \quad 0 \quad 0 \quad 1 \quad 1)$ be a received vector

Then $E = (0 \quad 0 \quad 1 \quad 0 \quad 1)$ represents the error vector

using the mod-2 addition,

$$Y = X \oplus E$$
$$= (1 \oplus 0 \quad 0 \oplus 0 \quad 1 \oplus 1 \quad 1 \oplus 0 \quad 0 \oplus 1)$$
$$= (1 \quad 0 \quad 0 \quad 1 \quad 1)$$

(or)

$$X = Y \oplus E$$
$$= (1 \oplus 0 \quad 0 \oplus 0 \quad 0 \oplus 1 \quad 1 \oplus 0 \quad 1 \oplus 1)$$
$$= (1 \quad 0 \quad 1 \quad 1 \quad 0)$$

Relationship between syndrome vector (s) and error vector (E)

$$S = Y H^T$$

Since $Y = X \oplus E$

$$S = (X \oplus E) H^T$$
$$= X H^T \oplus E H^T$$

$X H^T = 0$

So, $\boxed{S = E H^T}$

This relation shows that syndrome depends upon the error pattern only. It does not depend upon a particular message.

Ex: 4 The parity check matrix of a (7, 4) hamming code is given as follows

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

Calculate the syndrome vector for single bit errors.

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

S.NO.	Bit in error	Bits of Error vector (E)
1	1^{st}	1 0 0 0 0 0 0
2	2^{nd}	0 1 0 0 0 0 0
3	3^{rd}	0 0 1 0 0 0 0
4	4^{th}	0 0 0 1 0 0 0
5	5^{th}	0 0 0 0 1 0 0
6	6^{th}	0 0 0 0 0 1 0
7	7^{th}	0 0 0 0 0 0 1

$S = EH^T$

$$[S]_{1\times 3} = [E]_{1\times 7}\,[H^T]_{7\times 3}$$

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

Syndrome for first bit in error

$$S = E.H^T = [1\ 0\ 0\ 0\ 0\ 0\ 0] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= (1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0$$

$$1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0)$$

$$= (1\ 0\ 0)$$

Syndrome vectors are rows of H^T

S.NO.	Error vector 'E'	Syndrome vector
1	0 0 0 0 0 0 0	0 0 0
2	1 0 0 0 0 0 0	1 0 1
3	0 1 0 0 0 0 0	1 1 1
4	0 0 1 0 0 0 0	1 1 0
5	0 0 0 1 0 0 0	0 1 1
6	0 0 0 0 1 0 0	1 0 0
7	0 0 0 0 0 1 0	0 1 0
8	0 0 0 0 0 0 1	0 0 1

Error correction using syndrome vector

Let the transmitted code vector be

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

Let there be error created in the 3rd bit in the received code vector Y.

$$Y = (1\,0\,1\,1\,1\,1\,0)$$

a) To obtain syndrome vector (S)

$$S = Y \cdot H^T = [1\,0\,1\,1\,1\,1\,0]\begin{bmatrix}1&0&1\\1&1&1\\1&1&0\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}$$

$$= (1\oplus 0\oplus 1\oplus 0\;1\oplus 0\oplus 0 \quad 0\oplus 0\oplus 1\oplus 1\oplus 0\oplus 1\oplus 0 \quad 1\oplus 0\oplus 0\oplus 1\oplus 0\oplus 0\oplus 0)$$

$$= (1\;\;1\;\;0)$$

b) To determine the row of H^T which is same as 'S'

$S = 1\,1\,0$ is the 3rd row of H^T

c) To determine 'E'

$$E = (0\,0\,1\,0\,0\,0\,0)$$

(d) To obtain correct vector

$$X = Y \oplus E$$

$$X = [1\ 0\ 1\ 1\ 1\ 1\ 0] \oplus [0\ 0\ 1\ 0\ 0\ 0\ 0]$$

$$= [1\ 0\ 0\ 1\ 1\ 1\ 0]$$

Thus a single bit errors can be corrected using syndrome decoding.

Ex. 5 For a systematic linear block code, the three parity check digits c_4, c_5 and c_6 is given by

$$c_4 = d_1 \oplus d_2 \oplus d_3$$

$$c_5 = d_1 \oplus d_2$$

$$c_6 = d_1 \oplus d_3$$

i) construct generator matrix
ii) Construct code generated by this matrix
iii) Determine error correcting capability
iv) Prepare a suitable decoding table
v) Decode the received words 101100 and 000110.

To obtain the generator matrix

$$[c_4\ c_5\ c_6] = [d_1\ d_2\ d_3]\,[P]_{3\times3}$$

$$[c_4 \ c_5 \ c_6] = [d_1 \ d_2 \ d_3]\begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{bmatrix}$$

$$c_4 = d_1 P_{11} \oplus d_2 P_{21} \oplus d_3 P_{31}$$

$$c_5 = d_1 P_{12} \oplus d_2 P_{22} \oplus d_3 P_{32}$$

$$c_6 = d_1 P_{13} \oplus d_2 P_{23} \oplus d_3 P_{33}$$

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

$$G = [I_k : P_{k \times q}] = [I_3 : P_{3\times 3}]$$

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

To obtain the code vectors

Message vector d_1	d_2	d_3	Check bits c_4	c_5	c_6	Code vector X	Weight of the code $w(X)$
0	0	0	0	0	0	0 0 0 0 0 0	0
0	0	1	1	0	1	0 0 1 1 0 1	3
0	1	0	1	1	0	0 1 0 1 1 0	3
0	1	1	0	1	1	0 1 1 0 1 1	4
1	0	0	1	1	1	1 0 0 1 1 1	4
1	0	1	0	1	0	1 0 1 0 1 0	3
1	1	0	0	0	1	1 1 0 0 0 1	3
1	1	1	1	0	0	1 1 1 1 0 0	4

To obtain error correcting capability

$$d_{min} = [w(x)]_{min} = 3$$

$$d_{min} \geq s+1$$

$$3 \geq s+1$$

$$s \leq 2$$ Thus two errors will be detected

$$d_{min} \geq 2t+1$$

$$3 \geq 2t+1$$

$$t \leq 1$$ Thus one error will be corrected

To prepare the decoding table

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

$$H^T = \begin{bmatrix} P^T \\ \cdots \\ I_q \end{bmatrix}_{n \times q}$$

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

$$S = E \cdot H^T$$

Here E is the 1x6 size error vector.

$$E = [1\ 0\ 0\ 0\ 0\ 0] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \quad 1 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0)$$

$$= (1\ 1\ 1)$$

S.NO.	Error vector 'E' showing single bit error pattern	Syndrome vector 'S'
1	0 0 0 0 0 0	0 0 0
2	1 0 0 0 0 0	1 1 1
3	0 1 0 0 0 0	1 1 0
4	0 0 1 0 0 0	1 0 1
5	0 0 0 1 0 0	1 0 0
6	0 0 0 0 1 0	0 1 0
7	0 0 0 0 0 1	0 0 1

To decode received words

a) $Y = [1\ 0\ 1\ 1\ 0\ 0]$

$$S = YH^T = [1\ 0\ 1\ 1\ 0\ 0]\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix} = (1\oplus 0\oplus 1\oplus 1\oplus 0\oplus 0$$

$$1\oplus 0\oplus 0\oplus 0\oplus 0\oplus 0$$

$$1\oplus 0\oplus 1\oplus 0\oplus 0\oplus 0)$$

$$= (1\ 1\ 0)$$

$[1\ 1\ 0]$ is second syndrome in the table and corresponding error pattern is, $E = [0\ 1\ 0\ 0\ 0\ 0]$

$$X = Y \oplus E$$

$$= (1\ 0\ 1\ 1\ 0\ 0) \oplus (0\ 1\ 0\ 0\ 0\ 0)$$

$$= (1\ 1\ 1\ 1\ 0\ 0)$$

b) $Y = [0\ 0\ 0\ 1\ 1\ 0]$

$$S = YH^T = [0\ 0\ 0\ 1\ 1\ 0]\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix} = (0\oplus 0\oplus 0\oplus 1\oplus 0\oplus 0$$

$$0\oplus 0\oplus 0\oplus 0\oplus 1\oplus 0$$

$$0\oplus 0\oplus 0\oplus 0\oplus 0\oplus 0)$$

$$= (1\ 1\ 0)$$

$E = [0\ 1\ 0\ 0\ 0\ 0]$

$X = Y \oplus E$

$= [0\ 0\ 0\ 1\ 1\ 0] \oplus [0\ 1\ 0\ 0\ 0\ 0]$

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

This ~~Y~~ is the correct word

Binary cyclic codes

* cyclic codes are the sub class of linear block codes.
* cyclic codes can be in systematic or non: ~~symmetric~~ systematic form.

Definition

A linear code is called cyclic code if every cyclic shift of the code vector produces some other code vector.

Properities of cyclic codes

a) Linearity property

This property states that sum of any two code words is also a valid codeword.

$X_3 = X_1 \oplus X_2$

Here X_3 is also a valid code word.

b) cyclic property

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

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

one cyclic shift of x gives $x' = (x_{n-2}, x_{n-3}, \dots x_1, x_0, x_{n-1})$

Algebraic structures of cyclic codes

* The code words can be represented by a polynomial

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

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

Here $X(p)$ is the polynomial of degree $(n-1)$

p is the arbitrary variable of the polynomial.

Generation of code vectors in Non systematic form

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

$$X(p) = M(p) \cdot G(p)$$

Here $G(p)$ is the generating polynomial of degree 'q'.

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

Ex: 1 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 nonsystematic form.

$n = 7, \quad k = 4, \quad q = 3$

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

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

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

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

To obtain non-systematic code vectors

$$X(p) = M(p)\, G(p)$$

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

$$= p^5 + p^3 + p^2 + p^3 + p + 1$$

$$= p^5 + p^3 + p^3 + p^2 + p + 1$$

$$= p^5 + (1 \oplus 1) p^3 + p^2 + p + 1$$

$$= p^5 + p^2 + p + 1$$

$$= 0p^6 + p^5 + 0p^4 + 0p^3 + p^2 + p + 1$$

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

S.NO.	Message bits m_1	m_2	m_3	m_4	Non systematic code vectors 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
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	1	1	0	0
6	0	1	0	1	0	1	0	0	1	1	1
7	0	1	1	0	0	1	1	1	0	1	0
8	0	1	1	1	0	1	1	0	0	0	1
9	1	0	0	0	1	0	1	1	0	0	0
10	1	0	0	1	1	0	1	0	0	1	1
11	1	0	1	0	1	0	0	1	1	1	0
12	1	0	1	1	1	0	0	0	1	0	1
13	1	1	0	0	1	1	1	0	1	0	0
14	1	1	0	1	1	1	1	1	1	1	1
15	1	1	1	0	1	1	0	0	0	1	0
16	1	1	1	1	1	1	0	1	0	0	1

To check whether cyclic property is satisfied

Let us consider code vector X_9 which is given in previous table as

$$X_9 = (1011000)$$

Let us shift this code vector cyclically to left side by '1' bit position, then

$$X' = (0110001)$$

From table, $X' = X_8 = (0110001)$

Thus cyclic shift of X_9 produces X_8. This can be verified for other code vectors also.

Generation of code vectors in systematic form

$$X = (\text{'k' message bits : 'q' check bits})$$

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

$$c(p) = c_{q-1}\, p^{q-1} + c_{q-2}\, p^{q-2} + \ldots + c_1 p + c_0$$

The check bit polynomial is

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

Ex. 2 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.

$n = 7 \quad k = 4, \quad q = 3$

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

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

$= p^2 + 1$

$\boxed{m(p) = p^2 + 1}$

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

To obtain: $p^q M(p)$

$q = 3, \quad p^q M(p)$ will be,

$p^3 M(p) = p^3(p^2 + 1) = p^5 + p^3$

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

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

$= p^3 + 0p^2 + p + 1$

To perform the division $\dfrac{p^q M(p)}{G(p)}$:

$$
\begin{array}{r|l}
 & p^2 \quad \leftarrow \text{Quotient} \\
\hline
p^3+0p^2+p+1 & p^5+0p^4+p^3+0p^2+0p+0 \\
 & \oplus \quad \oplus \quad \oplus \quad \oplus \quad \leftarrow \text{Mod 2 } \oplus \text{ Addition} \\
 & p^5+0p^4+p^3+p^2 \\
\hline
 & 0+0+0+p^2 \quad \leftarrow \text{Remainder}
\end{array}
$$

Remainder polynomial is p^2

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

$$C(p) = C_2 p^2 + C_1 p + C_0$$

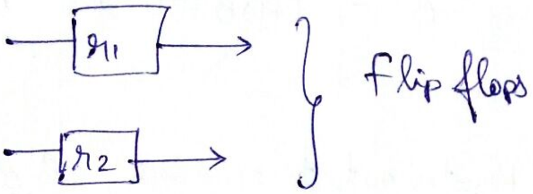
$$= p^2 + 0p + 0 \qquad = (1\ 0\ 0)$$

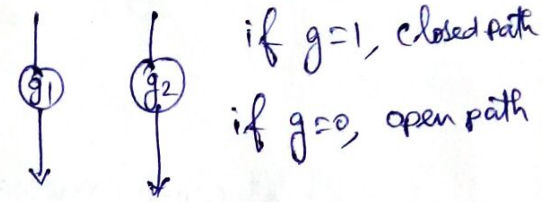
$$X = (0101 : 100)$$

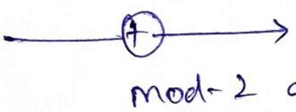
S.NO.	Message bits $M_3\ M_2\ M_1\ M_0$	Systematic code vectors $M_3\ M_2\ M_1\ M_0\ C_2\ C_1\ C_0$
1	0 0 0 0	0 0 0 0 000
2	0 0 0 1	0 0 0 1 0 1 1
3	0 0 1 0	0 0 1 0 1 1 0
4	0 0 1 1	0 0 1 1 1 0 1
5	0 1 0 0	0 1 0 0 1 1 1
6	0 1 0 1	0 1 0 1 1 0 0
7	0 1 1 0	0 1 1 0 0 0 1
8	0 1 1 1	0 1 1 1 0 1 0
9	1 0 0 0	1 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

S.NO.	Message bits $m_3\ m_2\ m_1\ m_0$	Systematic form code vectors
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

Encoding using an (n−k) bit shift register

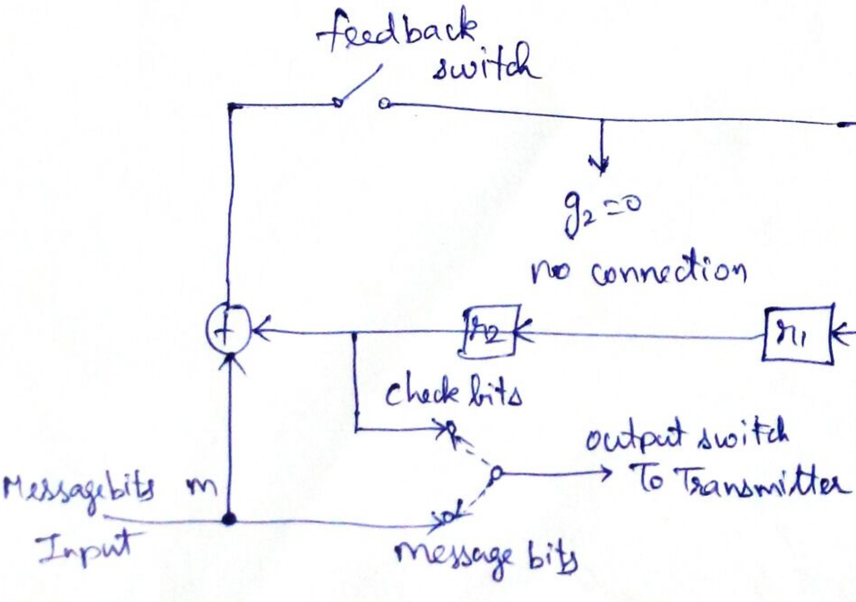






EX:3 Design the encoder for the (7,4) cyclic code generated by $G(P) = P^3 + P + 1$. and verify its operation for any message vector.

$$G(P) = P^3 + 0P^2 + P + 1 \qquad G(P) = P^3 + g_2 P^2 + g_1 P + 1$$



r_{q-1}

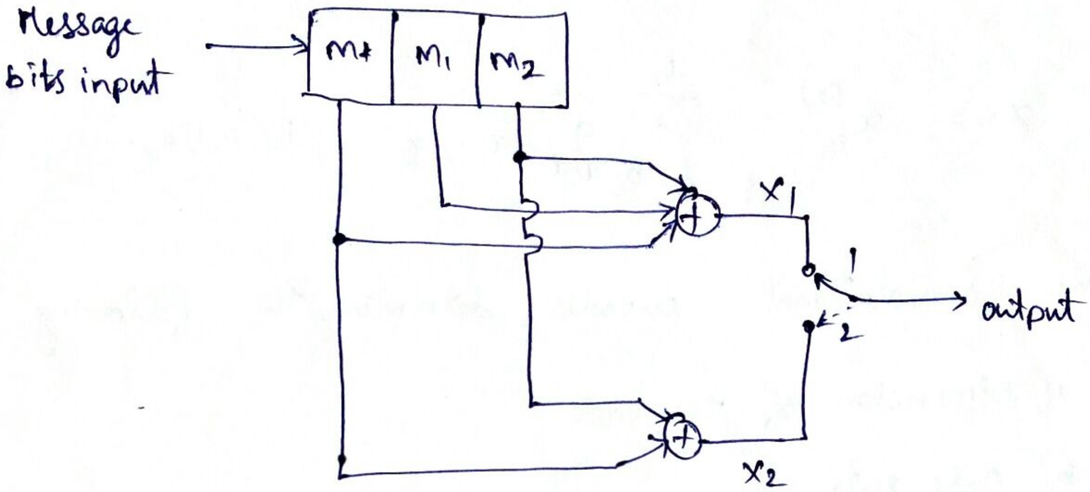
g_{q-1}

Input message bit m	Register bit inputs before shift $r_2 = r_2'$	$r_1 = r_1'$	$r_0 = r_0'$	Register bit outputs after shift $r_2' = r_1$	$r_1' = r_0 \oplus r_2 \oplus m$	$r_0' = r_2 \oplus m$
-	0	0	0	0	0	0
1	0	0	0	0	$0 \oplus 0 \oplus 1 = 1$	$0 \oplus 1 = 1$
1	0	1	1	1	$1 \oplus 0 \oplus 1 = 0$	$0 \oplus 1 = 1$
0	1	0	1	0	$1 \oplus 1 \oplus 0 = 0$	$1 \oplus 0 = 1$
0	0	0	1	0	$1 \oplus 0 \oplus 0 = 1$	$0 \oplus 0 = 0$

Shift clock	message bit m	Shift Register outputs r_2'	r_1'	r_0'	Feedback switch on/off	output switch position	Transmitted bits
1	1	0	1	1	ON	Message	1
2	1	1	0	1	ON	Message	1
3	0	0	0	1	ON	message	0
4	0	0	1	0	ON	Message	0
5	-	0	1	0	off	check	0 (r_2')
6	-	1	0	0	off	check	1 (r_2')
7	-	0	0	0	off	check	0 (r_2')

Convolutional codes

A convolutional coding is done by combining the fixed number of input bits. The input bits are stored in the fixed length shift register and they are combined with the help of mod-2 adders.



$X_1 = m \oplus m_1 \oplus m_2$

$X_2 = m \oplus m_2$

$X = x_1 x_2 \, x_1 x_2 \, x_1 x_2 \, x_1 x_2 \ldots$ and so on

Code Rate:

$$r = \frac{k}{n} = \frac{1}{2}$$

Constraint length

It is defined as the number of shifts over which a single message bit can influence the encoder output.

Dimension of the code :

It is represented as (n, k).

Time Domain Approach to Analysis of Convolutional Encoder

$$x_1 = x_i^{(1)} = \sum_{l=0}^{i} g_l^{(1)} \cdot m_{i-l} \qquad i = 0, 1, 2, \ldots$$

$$x_2 = x_i^{(2)} = \sum_{l=0}^{i} g_l^{(2)} \cdot m_{i-l} \qquad i = 0, 1, 2, \ldots$$

1. For the convolutional encoder, determine the following

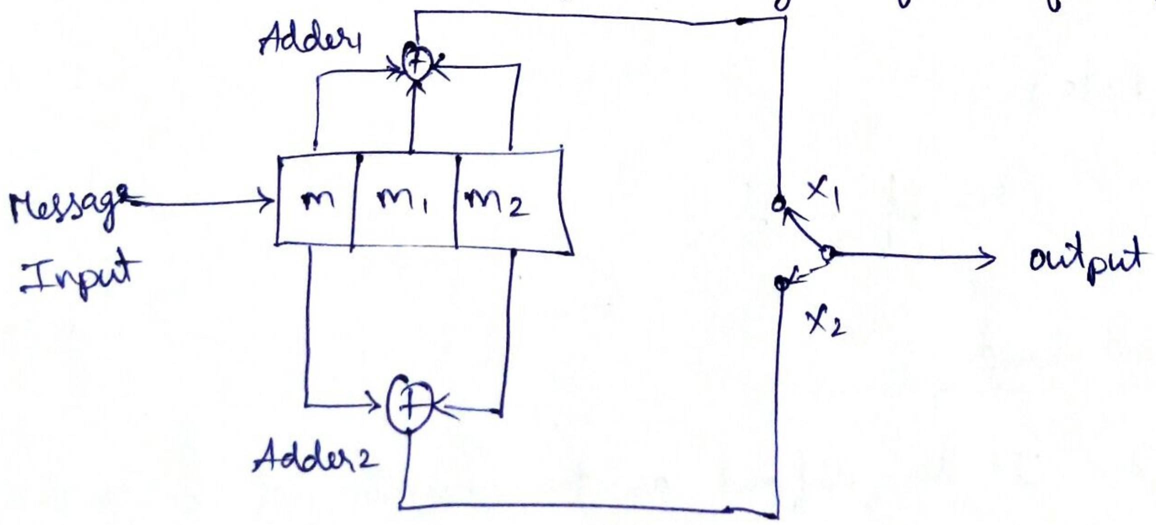
a) Dimension of the code

b) Code rate

c) Constraint length

d) Generating sequences (impulse responses)

e) Output sequence for message sequence of m = (1 0 0 1 1).



a) Dimension of the code

$$(2,1)$$

b) Code rate

$$r = \frac{k}{n} = \frac{1}{2}$$

c) Constraint length

$$K = 3 \text{ bits}$$

d) Generating sequences

$$g_i^{(1)} = (111)$$

$$g_i^{(2)} = (101)$$

e) output sequences

$$m = (m_0 \ m_1 \ m_2 \ m_3 \ m_4) = (1 \ 0 \ 0 \ 1 \ 1)$$

$$x_i^{(1)} = \sum_{l=0}^{i} g_l^{(1)} \cdot m_{i-l}$$

$i=0$

$$x_0^{(1)} = \sum_{l=0}^{0} g_l^{(1)} \cdot m_{-l}$$

$$= g_0^{(1)} \cdot m_0 = 1$$

$i=1$

$$x_1^{(1)} = \sum_{l=0}^{1} g_l^{(1)} \cdot m_{1-l} = g_0^{(1)} m_1 \oplus g_1^{(1)} m_0$$

$$= (1 \times 0) \oplus (1 \times 1) = 1$$

$i=2$

$$x_2^{(1)} = \sum_{l=0}^{2} g_l^{(1)} \cdot m_{2-l} = g_0^{(1)} m_2 + g_1^{(1)} m_1 + g_2^{(1)} m_0$$

$$= (0) \oplus (0) \oplus (1) = 1$$

$i=3 \quad x_3^{(1)} = g_0^{(1)} m_3 \oplus g_1^{(1)} m_2 \oplus g_2^{(1)} m_1$

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

$i=4 \quad x_4^{(1)} = g_0^{(1)} m_4 \oplus g_1^{(1)} m_3 \oplus g_2^{(1)} m_2$

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

$i=5 \quad x_5^{(1)} = \cancel{g_0^{(1)} m_5} \oplus g_1^{(1)} m_4 \oplus g_2^{(1)} m_3$

$= 1 \oplus 1 = 0$

$i=6 \quad x_6^{(1)} = \cancel{g_0^{(1)}} m_6 \oplus \cancel{g_1^{(1)}} m_5 \oplus g_2^{(1)} m_4$

$= 1$

$$\boxed{x_1 = x_i^{(1)} = (1 \; 1 \; 1 \; 1 \; 0 \; 0)}$$

$$x_2 = x_i^{(2)} = \sum_{l=0}^{i} g_l^{(2)} \cdot m_{i-l}$$

$i=0$	$x_0^{(2)} = 1$	$i=3$	$x_3^{(2)} = 1$	$i=6$	$x_6^{(2)} = 1$
$i=1$	$x_1^{(2)} = 0$	$i=4$	$x_4^{(2)} = 1$		
$i=2$	$x_2^{(2)} = 1$	$i=5$	$x_5^{(2)} = 1$		

$$x_2 = x_i^{(2)} = (1 \; 0 \; 1 \; 1 \; 1 \; 1 \; 1)$$

$$\boxed{x_i = \{11, 10, 11, 11, 01, 01, 11\}}$$

Transform Domain Approach to Analysis of convolutional encoder

$x^1(p) = g^1(p) \cdot m(p)$

$x^2(p) = g^2(p) \cdot m(p)$

where $g(p)$ is the generating sequences.

2) For the given convolutional encoder, determine the following using transform domain calculation.

a) output sequence for the message $m = (1\ 0\ 0\ 1\ 1)$

First generating sequence $g_i^{(1)} = (1\ 1\ 1) \quad = 1+p+p^2$

Second generating sequence $g_i^{(2)} = (1\ 0\ 1) \quad = 1+p^2$

message polynomial as for $(1\ 0\ 0\ 1\ 1)$ is

$$m(p) = 1 + 0p + 0p^2 + p^3 + p^4$$
$$= 1+p^3+p^4$$

$$x^1(p) = g^{(1)}(p) \cdot m(p) = (1+p+p^2)(1+p^3+p^4)$$
$$= 1+p+p^2+p^3+p^6$$
$$= 1+p+p^2+p^3+0p^4+0p^5+p^6$$

so, $x^1(p) = (1\ 1\ 1\ 1\ 0\ 0\ 1)$

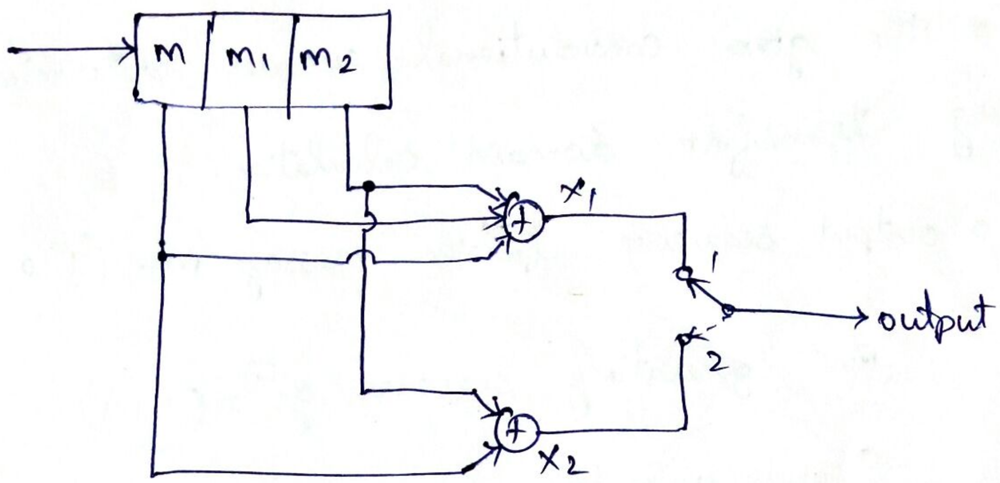
$$x^2(p) = g^{(2)}(p) \cdot m(p) = (1+p^2)(1+p^3+p^4)$$
$$= 1+p^2+p^3+p^4+p^5+p^6$$
$$= 1+0p+p^2+p^3+p^4+p^5+p^6$$

so, $x^2(p) = (1\ 0\ 1\ 1\ 1\ 1\ 1)$

Multiplexed output sequence is

$$\{x_i\} = \{11, 10, 11, 11, 01, 01, 11\}$$

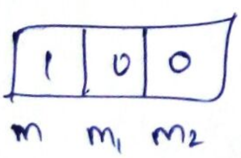
Code Tree, Trellis and state diagram for a convolutional encoder



State of the encoder

m_2	m_1	state
0	0	a
0	1	b
1	0	c
1	1	d

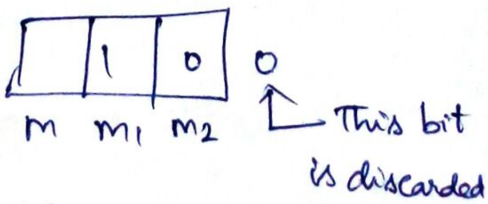
Development of code tree



Before shift

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

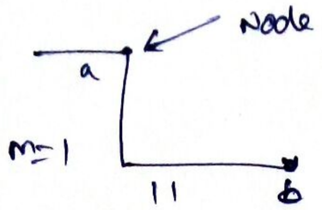
$x_2 = 1 \oplus 0 = 1$



After shift

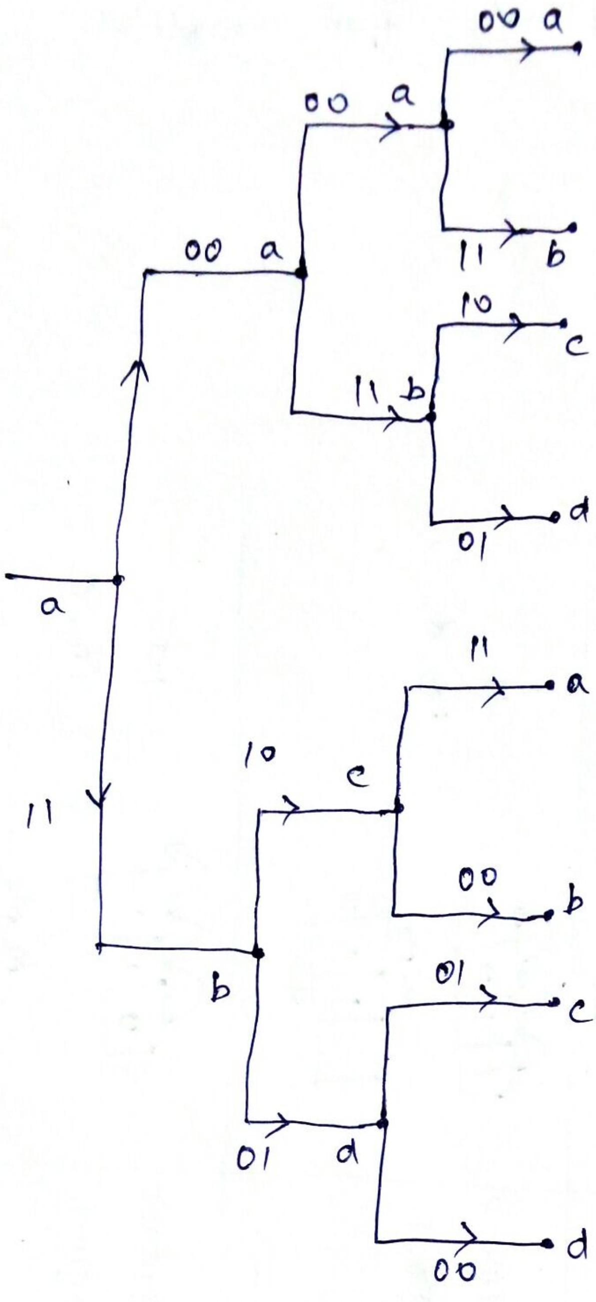
If $m=1$, we go downward from node 'a'

If $m=0$, we go upward from node 'a'

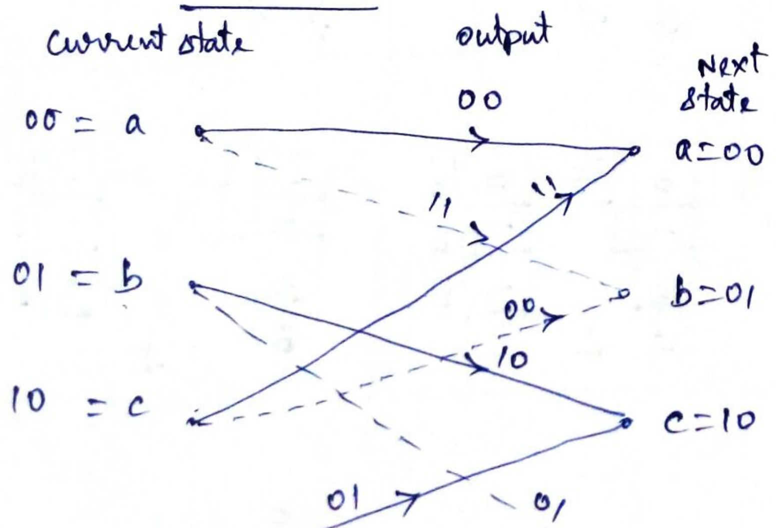


Input message bit m	Status of shift register after entry of m	Calculation of outputs x_1 and x_2	Status of shift register after transmission of o/p and shift right by one bit	New state of encoder $m_2 m_1$
1	$1 \rightarrow$ [m | m_1 0 | m_2 0] i.e., [1 | 0 | 0] (m m_1 m_2)	$x_1 = 1 \oplus 0 \oplus 0 = 1$ $x_2 = 1 \oplus 0 = 1$	[1 | 0 | 0] i.e., [| 1 | 0] 0 (m_1 m_2)	01 i.e., b
1	$1 \rightarrow$ [| 1 | 0] 'b' i.e., [1 | 1 | 0] (m m_1 m_2)	$x_1 = 1 \oplus 1 \oplus 0 = 0$ $x_2 = 1 \oplus 0 = 1$	[1 | 1 | 0] [| 1 | 1] 0 (m_1 m_2)	11 i.e., d
0	$0 \rightarrow$ [| 1 | 1] 'd' i.e., [0 | 1 | 1] (m m_1 m_2)	$x_1 = 0 \oplus 1 \oplus 1 = 0$ $x_2 = 0 \oplus 1 = 1$	[0 | 1 | 1] [| 0 | 1] 1 (m_1 m_2)	10 i.e., c

Code Tree



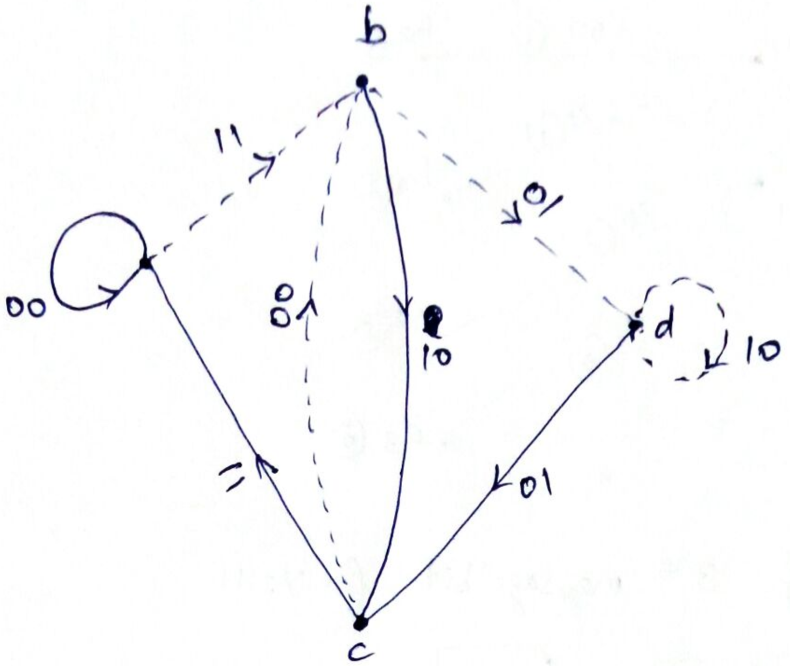
Code Trellis



If m='0' solid transition line

m='1' Broken line

State diagram



Decoding methods of convolutional codes

* viterbi Algorithm (Maximum Likelihood Decoding)

Metric:

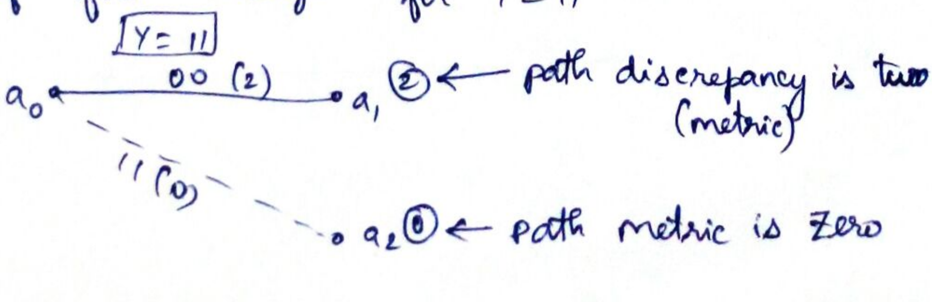
It is the discrepancy between the received signal Y and the decoded signal at particular node.

surviving path:

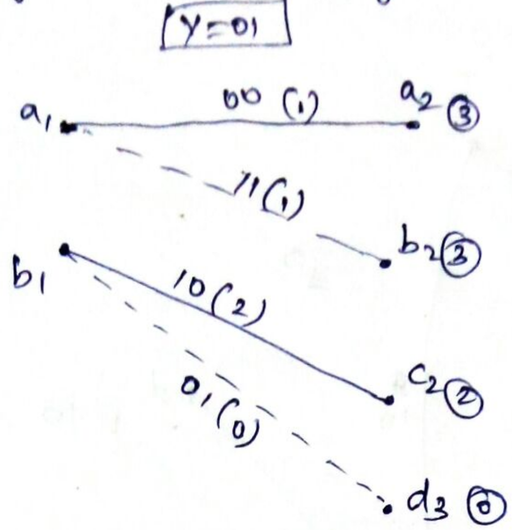
This is the path of the decoded signal with minimum metric.

Y = 11 01 11

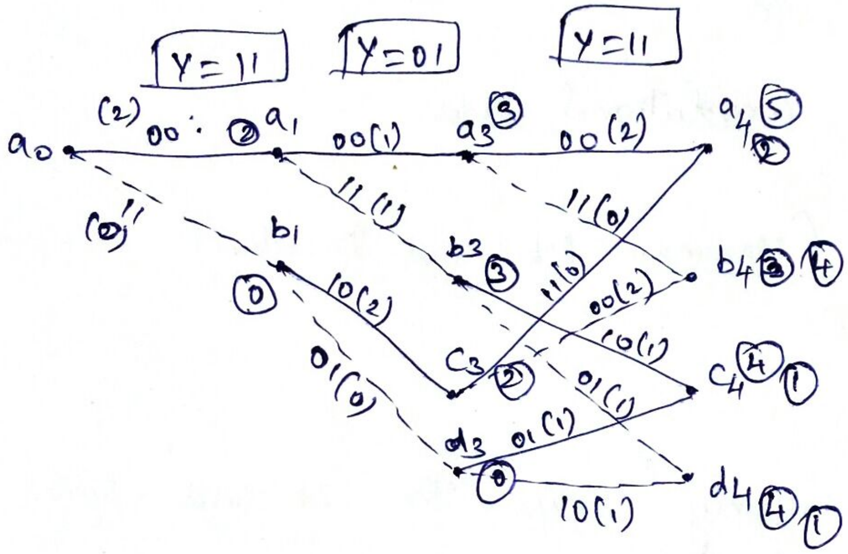
a) Decoding of first message for Y = 11



b) Decoding of second message bit for Y=01



c) Decoding of 3rd message bit for Y=11



Y =	11	01	11	00	01	10	00	11	~~10~~	10	~~00~~ 11	00
Y+E =	11	01	01	00	01	10	01	11	11	10	11	00
M =	1	1	0	1	1	1	0	0	1	0	0	0

'1' → Dotted line

'0' → Solid line