UNIT-VI

Linear Block codes

Types of codes

The codes are mainly classified as block codes and convolutional codes.

i) Block codes :- These codes consist of 'n' number of bits in one block or codeword. This codeword consists of 'k' message bits and (n-k) redundant bits.

ii) Convolutional codes :- the coding operation is discrete time convolution of input sequence with the impulse response of the encoder. The convolutional encoder accepts the message bits continuously and generates the encoded sequence continuously.

The codes can also be classified as linear or non linear codes.

i) Linear codes :- If the two codewords of the linear code are added by mod-2 addition, then it produces third codeword in the code.

ii) Non-linear code :- Addition of the nonlinear codewords does not necessarily produce third codeword.

Linear block codes

Consider that the particular code vector consists of $m_1, m_2, m_3, \ldots m_k$ message bits and $c_1, c_2, c_3, \ldots c_q$ check bits. Then this code vector can be written as

$$X = (m_1, m_2, m_3, \ldots m_k \; c_1, c_2, c_3, \ldots c_q)$$

K = no. of message bits

n = no. of bits after encoding is called the block length of the code

$q = n - K$

q is the number of redundant bits added by the encoder.

The code vector can be written as

$$X = (M|C)$$

M = k-bit message vector

C = q-bit check vector

The check bits play the role of error detection and correction. Linear block code generates the check bits.

Matrix Description of Linear block codes

The code vector can be represented as

$$X = MG \quad \text{——— ①}$$

X = Code vector of $1 \times n$ size or n bits

M = message vector of $1 \times k$ size or k-bits

G = generator matrix of $K \times n$ size.

The above equation ① can be represented in matrix form as

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

The generator matrix depends upon the linear block code used.

$$G = [I_K | P_{K \times q}]_{K \times n}$$

I_K = $k \times k$ identity matrix

P = $k \times q$ submatrix

The check vector can be obtained as

$$C = MP$$

The check vector equation can be written in expanded form as

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

By solving the above matrix equation the check vector is obtained as

$$C_1 = m_1 P_{11} \oplus m_2 P_{21} \oplus m_3 P_{31} \oplus \cdots \oplus m_k P_{k1}$$
$$C_2 = m_1 P_{12} \oplus m_2 P_{22} \oplus m_3 P_{32} \oplus \cdots \oplus m_k P_{k2}$$
$$C_3 = m_1 P_{13} \oplus m_2 P_{23} \oplus m_3 P_{33} \oplus \cdots \oplus m_k P_{k3}$$

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

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

Sol:- The code vectors can be obtained using the steps

i) Determine the P submatrix from generator matrix
ii) Obtain equations for check bits using $C = MP$
iii) Determine check bits for every message vector

Step 1: P submatrix

Generator $G = [I_K : P_{K\times q}]$

block code size $= (6,3) = (n,k)$

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

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

Step 2 :- check bits $C = MP$

$M = \text{message} = [m_1\ m_2\ m_3 \cdots m_k]_{1\times k} = [m_1\ m_2\ m_3]$

$[\because k = 3]$

$\therefore$ C = check bits = $[c_1\ c_2\ \cdots\ c_q]_{1\times q} = [c_1\ c_2\ c_3]$

$\because q = 3$

$C = MP$

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

$= [m_1(0)\oplus m_2(1)\oplus m_3(1)\quad m_1(1)\oplus m_2(0)\oplus m_3(1)\quad m_1(1)\oplus m_2(1)\oplus m_3(0)]$

$= [m_2\oplus m_3\quad m_1\oplus m_3\quad m_1\oplus m_2]$

<u>step 3</u> :- check bits and code vectors for every message

message vector = 3 bits, hence there will be a total of 8 possible messages $2^3 = 8$.

S.No	Message bits m_1	m_2	m_3	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	weight of code
1	0	0	0	0	0	0	000000	0
2	0	0	1	1	1	0	001110	3
3	0	1	0	1	0	1	010101	3
4	0	1	1	0	1	1	011011	4
5	1	0	0	0	1	1	100011	3
6	1	0	1	1	0	1	101101	4
7	1	1	0	1	1	0	110110	4
8	1	1	1	0	0	0	111000	3

Error detection and correction

Hamming code

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

i) No. of check bits $q \geq 3$

ii) Block length $n = (2^q - 1)$

No. of message bits $k = n - q$

Minimum distance $d_{min} = 3$

Code rate $r = \frac{k}{n} = \frac{n-q}{n} = 1 - \frac{q}{n} = \left(1 - \frac{q}{2^q - 1}\right)$

$r = 1$ if $q >> 1$

<u>problem</u> :- The parity check matrix of a (7,4) linear block code is expressed as

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

i) obtain the generator matrix

ii) List all code vectors

iii) what is the minimum distance between code vectors

iv) How many errors can be detected and how many errors can be corrected.

Sol:- given $n = 7$, $k = 4$ $(n,k) = (7,4)$

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

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

This indicates that the given code is a Hamming code

The parity check matrix is of $q \times n$ size and is given below.

$$[H]_{3\times 7} = \begin{bmatrix} P_{11} & P_{21} & P_{31} & P_{41} & \ldots & 1 & 0 & 0 \\ P_{12} & P_{22} & P_{32} & P_{42} & \ldots & 0 & 1 & 0 \\ P_{13} & P_{23} & P_{33} & P_{43} & \ldots & 0 & 0 & 1 \end{bmatrix}$$

$$= [P^T : I_3]$$

On comparing parity check matrices, we have

$$P^T = \begin{bmatrix} P_{11} & P_{21} & P_{31} & P_{41} \\ P_{12} & P_{22} & P_{32} & P_{42} \\ P_{13} & P_{23} & P_{33} & P_{43} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Hence the P submatrix may be obtained as

$$P = \begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \\ P_{41} & P_{42} & P_{43} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{4\times 3}$$

The generator matrix G is expressed as under

$$G = [I_K : P_{K\times q}]_{K\times n}$$

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

$$G = [I_4 : P_{4\times 3}]_{4\times 7}$$

ii) <u>To find all codewords</u>

The check bits can be obtained using the equation

$$C = MP$$

$$[c_1 \;\; c_2 \;\; c_3]_{1\times 3} = [m_1 \;\; m_2 \;\; m_3 \;\; m_4]_{1\times 4} [P]_{4\times 3}$$

$$= [m_1 \;\; m_2 \;\; m_3 \;\; m_4] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$c_1 = m_1(1) \oplus m_2(1) \oplus m_3(1) \oplus m_4(0) = m_1 \oplus m_2 \oplus m_3$$

$$c_2 = m_1(1) + m_2(1) + m_3(0) + m_4(1) = m_1 \oplus m_2 \oplus m_4$$

$$c_3 = m_1(1) + m_2(0) + m_3(1) + m_4(1) = m_1 \oplus m_3 \oplus m_4$$

For example if $(m_1 \; m_2 \; m_3 \; m_4) = 1011$, we get

$$c_1 = 1 \oplus 0 \oplus 1 = 0$$

$$c_2 = 1 \oplus 0 \oplus 1 = 0$$

$$c_3 = 1 \oplus 1 \oplus 1 = 1$$

Using the same procedure, the other code words code vector may be obtained.

S.No.	Message vector $m_1\, m_2\, m_3\, m_4$	check bits $C_1 = m_1 \oplus m_2 \oplus m_3$	$C_2 = m_1 \oplus m_2 \oplus m_4$	$C_3 = m_1 \oplus m_3 \oplus m_4$	complete codeword	weight of code vec
1	0 0 0 0	0	0	0	0 0 0 0 0 0 0	0
2	0 0 0 1	0	1	1	0 0 0 1 0 1 1	3
3	0 0 1 0	1	1	0	0 0 1 0 1 1 0	3
4	0 0 1 1	1	0	1	0 0 1 1 1 0 1	4
5	0 1 0 0	1	0	1	0 1 0 0 1 0 1	3
6	0 1 0 1	1	1	0	0 1 0 1 1 1 0	4
7	0 1 1 1	0	0	0	0 1 1 1 0 0 0	3
8	1 0 0 0	1	1	1	1 0 0 0 1 1 1	4
9	1 0 0 1	1	0	0	1 0 0 1 1 0 0	3
10	1 0 1 0	0	0	1	1 0 1 0 0 0 1	3
11	1 0 1 1	0	1	0	1 0 1 1 0 1 0	4
12	1 1 0 0	0	1	0	1 1 0 0 0 1 0	3
13	1 1 0 1	0	0	1	1 1 0 1 0 0 1	4
14	1 1 1 0	1	0	0	1 1 1 0 1 0 0	4
15	1 1 1 1	1	1	1	1 1 1 1 1 1 1	7
16	0 1 1 0	0	1	1	0 1 1 0 0 1 1	4

The above table lists $2^k = 2^4 = 16$ code vectors along with their weights. The smallest weight of any nonzero code vector is 3.

Minimum distance $d_{min} = 3$

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

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

(iii) No of errors detected $= s$

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

$$3 \geq s+1 \quad \therefore s \leq 2$$

Hence 2 errors will be detected

(iv) No of errors corrected $= t$

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

$$3 \geq 2t+1$$

$$t \leq 1$$

one error will be corrected

Syndrome decoding method to correct errors

Let the transmitted code vector be 'X'
The corresponding received code vector = 'Y'
Then we can write

$X = Y$ (if there are no transmission errors)

$X \neq Y$ if there are errors produced during transmission

The decoder detects or corrects these errors in Y by using the stored bit pattern in the decoder. For larger block lengths, more and more bits are needed. This increases the memory requirement, adds to the complexity and cost. Hence to avoid these problems syndrome decoding is used in linear block codes

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

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

The transpose of parity check matrix has a very important property

3) $X H^T = [0 \; 0 \; 0 \; \ldots \; 0]$

4) $[H]_{1 \times n} [H^T]_{n \times 1} = [0 \; 0 \; 0 \; \ldots \; 0]$

5) $Y H^T = [0 \; 0 \; 0 \; \ldots \; 0]$ if $X = Y$ (no errors)

$Y H^T$ = non zero if $X \neq Y$

6) $Y = X \oplus E$

$X = Y \oplus E$

7) Syndrome vector

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

But $XH^T = 0$

$$\therefore S = EH^T$$

problem

$X = (1\ 0\ 1\ 1\ 0)$ - transmitted vector

$Y = (1\ 0\ 0\ 1\ 1)$ - received vector

error E = errors in the received vector, error in 3rd bit and 5th bit position (1 received as 0 and 0 received as 1) $= (0\ 0\ 1\ 0\ 1)$

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

problem :- the parity check matrix of a (7,4) Hamming code is expressed as under

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

Find the syndrome vector for single bit errors.

sol:- This is a (7,4) code $(n,k) = (7,4)$

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

The table shows the single error pattern for a 7-bit error vector.

S.No	Bit in error	Bits of error vector (Nonzero = error)						
1	1st	1	0	0	0	0	0	0
2	2nd	0	1	0	0	0	0	0
3	3rd	0	0	1	0	0	0	0
4	4th	0	0	0	1	0	0	0
5	5th	0	0	0	0	1	0	0
6	6th	0	0	0	0	0	1	0
7	7th	0	0	0	0	0	0	1

<u>syndrome calculation</u>

$$S = EH^T \qquad [S]_{1\times q} = [E]_{1\times n}\,[H]_{n\times q}$$

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

From H, we obtain H^T as follows

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

Syndrome for first bit error vector

$$S_1 = E_1 H^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

Syndrome for 2^{nd} bit error vector

$$S_2 = E_2 H^T = [0\ 1\ 0\ 0\ 0\ 0\ 0] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [1\ 1\ 1]$$

In a similar manner the syndromes can be calculated

S.No.	Syndrome vector		
1	1	0	1
2	1	1	1
3	1	1	0
4	0	1	1
5	1	0	0
6	0	1	0
7	0	0	1

Error correction using syndrome vector

Let the transmitted code vector

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

Let there be error in the 3^{rd} bit in the received code vector Y.

$$Y = (1\,0\,1\,1\,1\,1\,0) \quad (\text{error in } 3^{rd} \text{ bit})$$

The syndrome is obtained as

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

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

But $S = YH^T$

$$= (X \oplus E)H^T = XH^T \oplus EH^T = EH^T \quad (\because XH^T = 0)$$

$$\therefore S = [1\ 1\ 0] = EH^T$$

Comparing this syndrome with H^T, we observe that $S = [110]$ is the third row of H^T. From the error bit table we get the error pattern corresponding to this syndrome as

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

This shows that there is error in the third bit of Y. The corrected vector can be obtained as

$$X = Y \oplus E$$

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

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

which is the same as the transmitted code vector

Problem For a (6,3) code, the parity check matrix is given by

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

Determine whether a received code vector is erroneous. The received code vector is 100101

sol:- Find the transpose of H i.e H^T

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

In polynomial form

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

where p is an arbitrary variable and the power of p represents the position of the codeword bits..

$(n-1)$ represents MSB and 0 represents LSB.

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

where $M(p)$ = message polynomial

$G(p)$ = generator polynomial

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

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

$$X(p) = p^q M(p) \oplus C(p) = M(p)\, G(p)$$

Divide by $G(p)$

$$\frac{p^q M(p)}{G(p)} \oplus \frac{C(p)}{G(p)} = M(p)$$

Ex:- $\frac{14}{3} = 4 + \frac{2}{3}$

$\frac{\text{num}}{\text{deno}} = \text{Quotient} \oplus \frac{\text{Rem}}{\text{deno}}$

or $$\frac{p^q M(p)}{G(p)} = M(p) \oplus \frac{C(p)}{G(p)}$$

The check bit polynomial is obtained as

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

problem :- The generator polynomial of a (7, 4) cyclic code is $G(p) = p^3 + p + 1$. Obtain all code vectors for the code in non systematic and systematic form.

sol:- Here $n = 7$ and $k = 4$

$$q = n - k = 3$$

There will be total 2^k message vectors of 4-bits each.

$$2^k = 2^4 = 16 \text{ message vectors}$$

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

Let $M = (0101)$

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

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

The generator polynomial $G(p) = p^3 + p + 1$

Non-systematic code vectors

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

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

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

$$= p^5 + (p^3 \oplus p^3) + p^2 + p + 1 \quad \text{(XOR or mod-2 addition)}$$

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

Degree of the polynomial $= (n-1) = (7-1) = 6$

$$X = (x_6\ x_5\ x_4\ x_3\ x_2\ x_1\ x_0)$$

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

$$= (0100111)$$

This is the code vector for message (0101)

The received code vector is $Y = [1\,0\,0\,1\,0\,1]$.

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

As the syndrome vector is zero, there are no errors in the received code vector

<u>problem</u>

A (7,4) linear block code is generated according to the following parity check matrix H. The received code word Y is [1000011] for a transmitted code word X. Find the corresponding data transmitted.

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

Sol:- Transpose of H = H^T

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

$$S = YH^T = [1000011]\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix} = [1\,0\,0] = \text{fifth row in } H^T$$

The error pattern corresponding to the 5^{th} bit is

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

$$\therefore X = Y \oplus E$$

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

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

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

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

Therefore the transmitted vector X has 3 check bits (q) and 4 data or message bits

$$X = [\underbrace{1\ 0\ 0\ 0}_{\text{data or message bits}}\ \underbrace{1\ 1\ 1}_{\text{check bits}}]$$

Cyclic codes

Cyclic codes may be described as the subclass of linear block codes. They have the property that the cyclic shift of one code produces another code word.

Consider an n-bit code vector X

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

If the above code is shifted cyclically, we get another code vector X'

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

One more cyclic shift provides another code vector X''.

$$X'' = (x_{n-3}, x_{n-4}, \ldots \ldots x_1, x_0, x_{n-1}, x_{n-2})$$

Problem :- The generator polynomial of a (7,4) cyclic code is p^3+p+1. Obtain the systematic and non systematic code vectors

$G(p) = p^3+p+1$, $M(p) = 0101 = (p^2+1)$

a) Systematic code vectors

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

$q = 3$

$$p^q M(p) = p^3 M(p)$$
$$= p^3(p^2+1) = (p^5+p^3) \quad (\text{message } 0101)$$
$$= (p^5 + 0p^4 + p^3 + 0p^2 + 0p + 0)$$

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

Now we have $p^q(Mp)$ and $G(p)$. Now perform the division to find the remainder of this division

$$
\begin{array}{r|l}
 & p^2 \\
\hline
p^3+0p^2+p+1 & p^5+0p^4+p^3+0p^2+0p+0 \\
 & p^5 \oplus 0 \oplus p^3 \oplus p^2 \\
\hline
 & 0+0+0+\underbrace{p^2+0p+0}_{\text{remainder}}
\end{array}
$$

$\therefore C(p) = (p^2+0p+0)$

$q = 3$

$\therefore C(p) = C_2p^2 + C_1p + C_0 = p^2+0p+0$

$C_2 = 1, C_1 = 0, C_0 = 0$

$\therefore C = (1\,0\,0)$

$\therefore X = (M : C)$

$= (m_3\, m_2\, m_1\, m_0 : c_2\, c_1\, c_0)$

$= (0101 : 100)$

b) Non systematic code vectors

$$X(P) = M(P)\,G(P)$$
$$= (P^2+1)(P^3+P+1)$$
$$= P^5+P^3+P^3+P+P^2+1$$
$$= P^5+(P^3 \oplus P^3)+P^2+P+1$$
$$= (P^5+P^2+P+1)$$
$$X(P) = (0P^6+P^5+0P^4+0P^3+P^2+P+1)$$

The degree of the polynomial is $(n-1)$

$$\text{degree} = (n-1) = (7-1) = 6$$

The code vector corresponding to the polynomial $X(P)$ is

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

This is the code vector for message vector (0101). The code vector corresponding to other messages (0000), (0001), ---- to (1111) can be obtained using the same procedure

Syndrome decoding for cyclic codes

In cyclic codes also, during transmission some errors may occur. Syndrome decoding can be used to correct these errors.

If X = transmitted code vector

Y = received code vector

E = error vector

The correct code can be obtained as

$$X = Y \oplus E$$

or $$Y = X \oplus E$$

In polynomial form

$$Y(P) = X(P) \oplus E(P)$$

But $X(P) = M(P)\,G(P)$

$$\therefore Y(P) = M(P)\,G(P) \oplus E(P)$$

Divide through out by $G(P)$

$$\frac{Y(P)}{G(P)} = M(P) \oplus \frac{E(P)}{G(P)}$$

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

If $X(P) = Y(P)$, no errors are present

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

The syndrome vector is obtained as

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

problem 1:- Evaluate the syndrome for $Y = (1001101)$ (7,4) cyclic code generated by the polynomial $G(P) = P^3 + P + 1$.

sol:- For the (n,k) code, $n = 7$, $k = 4$

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

The generator polynomial is

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

The syndrome is obtained using

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

$Y = 1001101$

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

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

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

$$= \text{rem}\left[\frac{p^6 + 0p^5 + 0p^4 + p^3 + p^2 + 0p + 1}{p^3 + p + 1}\right]$$

$$p^3 + 0p^2 + p + 1 \overline{\Big) p^6 + 0p^5 + 0p^4 + p^3 + p^2 + 0p + 1} \Big(p^3 + p$$

$$\oplus p^6 \oplus 0p^5 \oplus p^4 \oplus p^3$$

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

$$\oplus p^4 \oplus 0p^3 \oplus p^2 \oplus p$$

$$S(p) = (p+1) = \text{remainder}$$

No. of syndrome bits $= q = 3$

$$S = (S_1\, S_2\, S_3)$$

$$S(p) = p + 1$$

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

$\therefore S_1 = 0$

$S_2 = 1$

$S_3 = 1$

$S = (011)$