Information bits = K

$i = [i_1, i_2, i_3 \ldots i_k]$

Parity bits / Redundant bits = r

$P = [P_1, P_2, P_3 \ldots P_r]$

Total ~~no of~~ bits of code = $n = k + r$

$n = [i_1\, i_2\, i_3 \ldots i_k,\ P_1\, P_2\, P_3 \ldots P_r]$

(n, K) is block code representation

Tot. code words required as per n Block codes = 2^n

Tot. code words required as per K information = 2^k

Tot. redundant code words required as per r parity bits = $2^n - 2^k$

$\therefore$ Code rate = $R = \frac{K}{n}$

Code word, $C = [I, P]$

$C = [i_1, i_2, i_3 \ldots i_k, P_1, P_2, P_3 \ldots P_r]$ $\alpha^6 + \alpha^2 + 1$

Error Code word :

$e = [e_1, e_2, e_3 \ldots e_n]$ $(\alpha^2)^3 + (\alpha^2) + 1$

where $e_j = 1$ means error, $e_j = 0$ means no error.

So valid data = recieved codeword + error code word. $(\alpha^2)^3 + \alpha^2 + 1$

$g(\alpha) = \alpha^3 + \alpha + 1$ $\alpha^3 + \alpha + 1$

g

$\alpha^{-23} \cdot \alpha^{28}$ $\alpha^{-13} = \alpha^{-13} \cdot 1 \cdot 1 = \alpha^{-13} \cdot \alpha^7 \cdot \alpha^7$ $\alpha^{-17} \cdot \alpha^{21}$

α^5 $\alpha^{-23} \cdot \alpha^{21} = \alpha^{-2} \cdot \alpha^7 = \alpha^5$ $= \alpha^{-13} \cdot \alpha^{14} = \alpha$ $= \alpha^4$

Q1) Given the (5,4) even parity block code, find codewords corresponding to I = (1011) and (1010)

$k = 4$, $r = 5-4 = 1$

For Information I = 1011 = $I_1 I_2 I_3 I_4$

For Even Parity, $P = I_1 + I_2 + I_3 + I_4$

$P = 1 + 0 + 1 + 1$

$P = 1$

So Code word = [Information, Parity]

$C = [i_1, i_2, i_3, i_4, P]$

$C = [1, 0, 1, 1, 1]$

For Information I = 1010 = $I_1 I_2 I_3 I_4$

For even Parity $P = I_1 + I_2 + I_3 + I_4$

$P = 1 + 0 + 1 + 0$

$P = 0$

Codeword C = [1, 0, 1, 0, 0]

Q2) Given the (8,7), even parity block code, determine whether V_1 = (10110110) and V_2 = (01101001) gives parity failure

V_1 = (10110110)

Check sum S = 1+0+1+1+0+1+1+0

· For Even received codeword, it is the parity failure.

· Means there is error in received data.

V_2 = (01101001)

Check sum S = 0+1+1+0+1+0+0+1

S = 0

For Even received codeword, it is parity success

Means there is no error in received data

Definition and Basics for Block codes for Product.

- As we have seen single parity check codes have no error correction capability.
- However error correction can be achieved by combing two single parity check codes in the form of rectangular array.

Example of Block Code for Product code

	Data bits				Row parity check
	1	1	0	1	1
	0	1	1	0	0
6	1	0	0	0	1
	0	0	0	0	0
	1	1	1	0	1
	1	0	0	1	0
Column parity check	0	1	0	0	1 (overall parity check)

← 9 →

out of 35 bits 24 are information bits

So given block code is (35, 24)

It is used to detect & correct one bit error

Example of Block Code for Repetition code

Let's have an example of (3,1) repetition code.

$(3,1) = (n,k)$

Info. bits $= k = 1$

Parity bits $= r = n-k = 3-1 = 2$

- Encoding process

Info bits	Parity bits		Codeword		
0	0	0	0	0	0
1	1	1	1	1	1

- Decoding process, it is done based on majority vote decoding.

Received data			Decoding Decision	Output Data			Infor.
0	0	0	No error	0	0	0	0
0	0	1	One Bit Error	0	0	0	0
0	1	0		0	0	0	0
1	0	0		0	0	0	0
1	1	1	No error	1	1	1	1
1	1	0	One bit error	1	1	1	1
1	0	1		1	1	1	1
0	1	1		1	1	1	1

Majority of vote for (V_1, V_2, V_3) is taken per $i = V_1 V_2 + V_1 V_3 + V_2 V_3$

Hamming Code

- It is used to detect and correct error.
- In Hamming code, we send data along with parity bits or Redundant bits.
- It is represented by (n, k) code

n → Total bits
k → message bits

- Parity bits $P = n - k$
- To identify parity bits, it should satisfy given condition

$$\Rightarrow 2^P \geq P + k + 1$$

So for $k = 4$ message bits

$$\Rightarrow 2^P \geq P + 4 + 1$$
$$\Rightarrow 2^P > P + 5$$

For $P = 1$
$2^1 \geq 6$ ✗

For $P = 2$
$2^2 \geq 7$ ✗

For $P = 3$
$2^3 = 8$ ✓

$P = 3$ for $k = 4$ bits.
$n = 3 + 4 = 7$ bits
∴ This code is $(7, 4)$ code

7	6	5	4	3	2	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1

$P_1 = 2^0 = 1$
$P_2 = 2^1 = 2$
$P_4 = 2^2 = 4$

$P_1 \rightarrow D_3\ D_5\ D_7$ (XOR)
$P_2 \rightarrow D_3\ D_6\ D_7$
$P_4 \rightarrow D_5\ D_6\ D_7$

Generation Hamming Code.

- 5 bit data (01101) is given, Represent given data in Hamming code.

→ $K = 5$ bits

→ Identify parity bits

$\Rightarrow 2^P \geq P+K+1$

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

For $P=1$, $P=2$, $P=3$, $P=4$

$2^1 \geq 7$ ✗, $2^2 \geq 8$ ✗, $2^3 \geq 9$ ✗, $2^4 \geq 10$ ✓

$\therefore P = 4$,

So for $P=4$, $K=5$, $n=9$

→ This is (9, 5) Hamming code.

9	8	7	6	5	4	3	2	1
0 D_9	P_8	1 D_7	1 D_6	0 D_5	P_4	1 D_3	P_2	P_1

Position of parity bits	Val. of parity bits.
$P_1 = 2^0 = 1$	$P_1 \to D_3\ D_5\ D_7\ D_9$
$P_2 = 2^1 = 2$	$P_2 \to D_3\ D_6\ D_7$
$P_4 = 2^2 = 4$	$P_4 \to D_5\ D_6\ D_7$
$P_8 = 2^3 = 8$	$P_8 \to D_9$

$P_1 = 1 + 0 + 1 + 0 = 0$

$P_2 = 1 + 1 + 1 = 1$

$P_4 = 0 + 1 + 1 = 0$

$P_8 = D_9 = 0$

$\therefore$ code $= \boxed{001100110}$

for 5 bit data

Haming code Error detection & correction

If Recieved Hamy code is 1110101 with even parity
then detect & correct error

In 7 bit Hamy code

7	6	5	4	3	2	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	1	1	0	1	0	1

$P_1 = D_3 + D_5 + D_7 = 1 \oplus 1 + 1 + 1 \Rightarrow P_1 = 0$ ✓

$P_2 = D_3 + D_6 + D_7 = 0 = 1 + 1 + 1 \quad P_2 = 1$ ✗

$P_4 = D_7 + D_6 + D_5 = 0 = 1 + 1 + 1 \quad P_4 = 1$ ✗

$P_4 P_2 P_1 = 110 = 6$

$\therefore$ On 6th bit there is error

Error syndrome : E =

0	1	0	0	0	0	0

Recieve R =

1	1	1	0	1	0	1

Corrected data = $R \oplus E$

=

1	0	1	0	1	0	1

Linear codes basics & property with example.

Definition - A block code is said to be linear code if its codewords satisfy the condition that the sum of any two codewords gives another codeword. i.e. $C_p = C_i + C_K$

Property i) The all-zero words $[0, 0, 0 \cdots 0]$ is always a code word.

ii) Given any three codewords C_i, C_j and C_K such that
$C_p = C_i + C_K$, then $d(C_i, C_j) = W(C_p)$

iii) minimum distance of the code
$d_{min} = W_{min}$

eg: (7,4) Hamming code

			weight
C_1	=	0 0 0 1 0 1 1	$\boxed{3}$
C_{10}	=	1 0 1 0 0 1 1	$\boxed{4}$
C_{11}	=	1 0 1 1 0 0 0	$\boxed{3}$

$C_{11} = C_1 + C_{10}$

→ $C_0 = [0 0 0 0 0 0 0]$

$d(C_1, C_{10}) = 3$ | $d(C_1, C_{10}) = 3 = W(C_{11})$

$W(C_{11}) = 3$

→ $C_{15} = [1 1 1 1 1 1 1]$, $w = 7$

other than C_{15} codes are having weight 3 & 4

$d_{min} = W_{min}$

Show that (4,3) Even parity code is a linear and (4,3) odd parity is not linear

→ (4,3) even parity code

C	d_1	d_2	d_3	P
C_0	0	0	0	0
C_1	0	0	1	1
C_2	0	1	0	1
C_3	0	1	1	0
C_4	1	0	0	1
C_5	1	0	1	0
C_6	1	1	0	0
C_7	1	1	1	1

→ 0 0 1 1 C_1

→ 0 1 0 1 $+C_2$

0 1 1 0 C_3

$d_{min}(C_1, C_2) = 2$

$W(C_3) = 2$

$- d_{min} = W$

→ odd parity (4,3) code

C	d_1	d_2	d_3	P
C_0	0	0	0	1
C_1	0	0	1	0
C_2	0	1	0	0
C_3	0	1	1	1
C_4	1	0	0	0
C_5	1	0	1	1
C_6	1	1	0	1
C_7	1	1	1	0

0 0 1 0 C_1

0 1 0 0 C_2

0 1 1 0

→ $C_1 + C_2$ is not present in odd parity (4,3) code.

→ It is not linear block code

Generator matrix to generate code words in linear code.

→ Using generator matrix to generate code words is a better approach

$[c] = [i][G]$

$[c]$ = Code word

$[i]$ = Information words

$[G]$ = Generator matrix

$[G] = [I : P]$

$[c] = [m : P_c]$ // incase of systematic

$[P_c] = [m][P]$

→ The Generator matrix of an (n, k) linear code has 'k' rows and 'n' columns.

→ Generator matrix for (7,4) code is given by

$[G] = [I : P]$

$$= \left[\underbrace{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}}_{\substack{\text{Identity} \\ \text{matrix } I_k}} \middle| \underbrace{\begin{matrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{matrix}}_{\substack{\text{Parity} \\ \text{matrix}}}\right]$$

→ $[C] = [i][G]$

Example: Generate code word for i = (1110) with (7,4) generator matrix code.

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

message $[i] = [1\ 1\ 1\ 0]$

$c = [i][G]$

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

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

Example: Determine the set of codewords for the (6,3) code with generator matrix.

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

$n = 6,\ K = 3$

message bits = 3

Possible combinations of message bits

m_0	m_1	m_2
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

$\rightarrow C = [i][G]$

$\rightarrow C_0 = [0\ 0\ 0]\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$

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

$\rightarrow C_1 = [0\ 0\ 1]\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$

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

$[C] = [m : P_c]$

$[P_c] = [m][P]$

	m_0	m_1	m_2	P_0	P_1	P_2
C_0	0	0	0	0	0	0
C_1	0	0	1	1	1	0
C_2	0	1	0	1	0	1
C_3	0	1	1	0	1	1
C_4	1	0	0	0	1	1
C_5	1	0	1	1	0	1
C_6	1	1	0	1	1	0
C_7	1	1	1	0	0	0

$C = [m, P]$

Systematic generator matrix in linear block codes

- A generator matrix $[G] = [I_k : P]$ is said to be in a systematic form if it generates the systematic codewords. $[C] = [i][G] = [m, P]$

→ Here, $[I_k] \rightarrow K \times K$ matrix

$[P] \rightarrow K \times (n-K)$ matrix

$[G] \rightarrow K \times n$ matrix

- In these matrix information bits are placed together

- Codeword

$$[C] = [i][G]$$

$$= [i_1, i_2, i_3, i_4] \begin{array}{c} \begin{array}{cccccccc} i_1 & i_2 & i_3 & i_4 & & P_1 & P_2 & P_3 \end{array} \\ \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \end{array}$$

→ So when you get codeword

$$C = (i_1, i_2, i_3, i_4, P_1, P_2, P_3)$$

→ Identity matrix keeps information together

→ Parity matrix generates parity bits.

$$P_1 = i_1 + i_2 + i_3$$

$$P_2 = i_2 + i_3 + i_4$$

$$P_3 = i_1 + i_2 + i_4$$

The (5,3) linear code has the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} = [I_K : P]$$

→ Determine systematic form of G

→ Generate codeword for information (011) with systematic G and Non-systematic G

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

$$[G] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad [R_3 = R_2 + R_3]$$

$$[G] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad [R_1 = R_1 + R_3]$$

$$\underbrace{}_{I} \; \underbrace{}_{P}$$

$$G = [I_K : P]$$

→ For non systematic [G]

$$c = [i][G]$$

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

$$= [0\ 0\ \underbrace{1\ 1\ 1}]$$

→ Info is somewhere between, Hence called non systematic

→ For systematic [G]

$$c = [i][G]$$

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

$$= [\underbrace{0\ 1\ 1}_{\text{Info}}\ \underbrace{1\ 0}_{\text{Parity}}]$$

Parity check Matrices in Linear block codes with examples.

→ From generator matrix $[G] = [I_k | P]$ we can identify parity matrix.

→ By taking P^T we can make parity check Matrix $[H]$

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

→ Parity check matrix is used at R_x to decode data.

Example – Generate Parity check matrix for (7,4) code

$$[G] = \left[\underbrace{\begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix}}_{\text{Identity matrix } I} \; \underbrace{\begin{matrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{matrix}}_{\text{Parity matrix } P}\right]$$

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

$$\Rightarrow I_{n-k} = I_{7-4} = I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

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

(a) Prove that GH^T and $CH^T = 0$

→ $GH^T = [I_k | P] [P^T | I_{n-k}]^T$

$= [I_k | P] \left[\frac{P}{I_{n-k}} \right]$

$= I_k P + P I_{n-k}$

$= P + P$

$P \rightarrow 0, 1$ For mod-2 add, $0+0 = 0$, $1+1 = 0$

$\therefore GH^T = 0$

$CH^T = [i][G][H^T]$

$= [i] 0$

$\therefore CH^T = 0$

Error Syndromes in Linear block codes with Examples.

→ If received codeword is $[Y]$

→ Then error syndromes

$[S] = [Y][H^T]$

Tx $\square \rightarrow [C]$ ↑ Channel noise → $[Y]$ $\square$ Rx $= [C] + [e]$

here, Received codeword $[Y]$

$[Y] = [C] + [e]$

where, $[C]$ = Codeword

$[e]$ = error

→ If error $[e] = 0$, $[Y] = [C]$

So, $[S] = [C][H^T] = 0$

(1) Find the error syndromes of $V_1 = (1101101)$. for $H^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

where v is recieved codeword, also calculate errored bit.

→ Recieved codeword $= V_1 = (1101101)$

→ $[S] = [V_1][H^T]$

$$= [1101101] \begin{array}{c} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array} \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ \\ \\ \end{array}$$

$= [1\ 0\ 0]$ ∴ error bit is at 5th position.

$Y = [1101101]$

$e = [0000100]$

$X = Y + e$

$= [1101001]$

Error detection and correction capacity of linear block code

Step 1 – Identify dmin [minimum Hamming distance]

Error detection capacity of linear block code

⇒ $d_{min} \geq s + 1$

→ where, s = error ~~det~~ detection capacity

Error correction capacity of linear block code

⇒ $d_{min} \geq 2t + 1$

→ where, t = error correction capacity

Q If minimum hamming dist of linear block code is 3. Find Linear block code error correction & detection capability.

→ $d_{min} = 3$

→ for error detection

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

$\Rightarrow 3 \geq s+1$

$\Rightarrow 2 \geq s$

$\Rightarrow s \leq 2$

→ This code can detect 2 bit ~~leo~~ error

For error correction,

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

$\Rightarrow 3 \geq 2t+1$

$\Rightarrow 2 \geq 2t$

$\Rightarrow t \leq 1$

This code can correct 1 bit error

Linear block codes complete examples

— For a (6, 3) code, the generator matrix G is

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

Find (a) All corresponding code vectors.

(b) minimum Hamming dist d_{min}

(c) Error detection & Error correction capability

(d) Parity check matrix

(e) Find error if received code is (100011)

→ $G = [I_k : P]$

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

→ $[C] = [i][G]$

$= [m : P_c]$

→ $[P_c] = [i_m][P]$

$$[P_0\ P_1\ P_2] = [i_0\ i_1\ i_2] \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

$P_0 = (i_0 \oplus i_2)$

$P_1 = (i_1 \oplus i_2)$

$\cancel{P_2} = (i_0 \oplus i_1)$

codewords:

C	i_0	i_1	i_2	P_0	P_1	P_2	W
C_1	0	0	0	0	0	0	—
C_2	0	0	1	1	1	0	3
C_3	0	1	0	0	1	1	3
C_4	0	1	1	1	0	1	4
C_5	1	0	0	1	0	1	3
C_6	1	0	1	0	1	1	4
C_7	1	1	0	1	1	0	4
C_8	1	1	1	0	0	0	3

$d_{min} = 3$

$d_{min} = 3$

Error detection capability $S \Rightarrow$ $d_{min} \geq S+1$

$\Rightarrow 3 \geq S+1$

$\Rightarrow S \leq 2$

It can detect 2bit error collection

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

$3 \geq 2t+1$

$\Rightarrow t \leq 1$ $\therefore$ It can correct 1 bit error

(i) Parity check matrix.

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

$\Rightarrow P^T = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ $I_{6-3} = I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

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

$\Rightarrow [S] = [Y][H^T]$

$\Rightarrow [Y] = [1\ 0\ 0\ 0\ 1\ 1]$

$S = YH^T$

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

$\therefore$ error is at 3rd position

$e = [0\,0\,1\,0\,0\,0]$

$Y = [1\,0\,0\,0\,1\,1]$

$\Rightarrow X = e + Y$

$= [1\,0\,1\,0\,1\,1] \longrightarrow$ Actual Transmitted signal.

Cyclic codes basics & Properties with example.

- Cyclic codes are ~~support~~ subpart of linear block codes.
- It follows following properties.

① Linearity property:

- If we have two code words C_i & C_j then

$C_p = C_i + C_j$

where C_p should be a code word

② Cyclic shifting

Code word $= (C_1, C_2, C_3, \ldots C_n)$

- After shifting left or right by any no. of bits, resultant code should be a code word.

• If code words follow above two property then only that codes will be cyclic codes.

eg: {0000, 0110, 1001, 1111} Is it cyclic code?

→ Check property of linearity:

$$\begin{array}{r} 0110 \\ 1001 \\ \hline 1111 \end{array} \qquad \begin{array}{r} 0110 \\ 1111 \\ \hline 1001 \end{array} \qquad \begin{array}{r} 1001 \\ 1111 \\ \hline 0110 \end{array}$$

→ So it follows property of linearity

→ Check property of shifting

0 1 1 0

0 0 1 1 ← It is not ~~cyclic~~ a codeword

∴ It is not cy~~Hence~~clic code.

eg: {0000, 0101, 1010, 1111}, ~~is~~ is it a cyclic code

→ Check property of linearity

$$\begin{array}{r} 0101 \\ 1010 \\ \hline 1111 \end{array} \qquad \begin{array}{r} 0101 \\ 1111 \\ \hline 1010 \end{array} \qquad \begin{array}{r} 1010 \\ 1111 \\ \hline 0101 \end{array}$$

→ it follows ~~pro~~ property of linearity

→ Check shifting property

0 1 0 1   1 0 1 0

1 0 1 0 it is a codeword ← 0 1 0 1

It follows shifting property.

∴ Hence it is cyclic code.

Cyclic codes for non-systematic code word.

* Code word for non-systematic code word is given by

$c(x) = m(x) \cdot g(x)$

where, $c(x)$ = code word polynomial

$m(x)$ = message polynomial

$g(x)$ = generator polynomial

→ $\boxed{c = [\text{message, parity}] \text{ for systematic codeword.}}$

→ 1011

$x^3\ x^2\ x^1\ x^0$

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

$= x^3 + x + 1$

~~* Construct~~

* Construct Non systematic cyclic codes (7,4), using generator polynomial $g(x) = x^3 + x^2 + 1$, with message (1010)

$m = [1010]$

$x^3\ x^2\ x^1\ x^0$

→ $m(x) = x^3 + x$

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

→ $c(x) = m(x) g(x)$

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

$= x^6 + x^5 + \cancel{x^3} + x^4 + \cancel{x^3} + x$

$= x^6 + x^5 + x^4 + x$

$\therefore c = [1110010]$

Cyclic codes for systematic codeword

- Codeword for systematic codeword is given by

$$c(x) = x^{n-k}\, m(x) + p(x)$$

where, $$p(x) = \text{Rem}\left[\frac{x^{n-k}\, m(x)}{g(x)}\right]$$

$c(x)$: codeword polynomial

$m(x)$: message polynomial

$g(x)$: generator polynomial

$$\boxed{C = [\text{message, parity}]}$$

* Construct a ~~cyclic~~ systematic cyclic code (7,4), using generator polynomial $g(x) = x^3 + x^2 + 1$, with message (1010)

$n = 7,\ k = 4$

$m = (1\ 0\ 1\ 0) \Rightarrow m(x) = x^3 + x$

$\ \ \ \ \ \ \ \ x^3\ x^2\ x^1\ x^0$

$$c(x) = x^{n-k}\, m(x) + p(x)$$

$$p(x) = \text{Rem}\left[\frac{x^{n-k}\, m(x)}{g(x)}\right]$$

$$= \text{Rem}\left[\frac{x^3(x^3+x)}{x^3+x^2+1}\right] = \text{Rem}\left[\frac{x^6+x^4}{x^3+x^2+1}\right]$$

$$x^3+x^2+1 \overline{\big)\, x^6 + x^4 \,}\ \ (\text{quotient } x^3 + x^2 + 1)$$

$$\begin{array}{r} x^6 + x^4 \\ x^6 + x^5 + x^3 \\ \hline x^5 + x^4 + x^3 \\ x^5 + x^4 + x^2 \\ \hline x^3 + x^2 \\ x^3 + x^2 + 1 \\ \hline 1 \end{array}$$

$= 1$

$C(x) = x^{n-k} m(x) + P(x)$

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

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

$C = [\underbrace{1010}_{message}\underbrace{001}_{parity}]$

Generator matrix of cyclic code

→ Generator matrix

$[G] = [I : P]$

identity matrix — Parity matrix

→ If cyclic code is (n, k), then generator matrix G is having n columns of k rows.

→ Identity matrix is known by us.

→ So row of parity matrix based on generator polynomial $K(x)$ is given by.

1^{st} row : $Rem\left[\frac{x^{n-1}}{g(x)}\right]$

2^{nd} row : $Rem\left[\frac{x^{n-2}}{g(x)}\right]$

⋮

k^{th} row : $Rem\left[\frac{x^{n-k}}{g(x)}\right]$

* If generator polynomial of cyclic code (7,4) is given by $g(x) = x^3 + x + 1$, then construct generator matrix.

→ (7,4) code

$\boxed{7 = n}$, $\boxed{k = 4}$

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

1st row of parity matrix

$$= \text{Rem}\left[\frac{x^{7-1}}{g(x)}\right] = \text{Rem}\left[\frac{x^6}{x^3+x+1}\right] = x^2+1 = [1\,0\,1]$$

2nd Row of parity matrix

$$= \text{Rem}\left[\frac{x^{7-2}}{g(x)}\right] = \text{Rem}\left[\frac{x^5}{x^3+x+1}\right] = x^2+x+1 = [1\,1\,1]$$

3rd Row of Parity matrix

$$= \text{Rem}\left[\frac{x^{7-3}}{g(x)}\right] = \text{Rem}\left[\frac{x^4}{x^3+x+1}\right] = x^2+1 = [1\,0\,1]$$

4th Row of parity Matrix

$$= \text{Rem}\left[\frac{x^{7-4}}{g(x)}\right] = \text{Rem}\left[\frac{x^3}{x^3+x+1}\right] = x+1 = [0\,1\,1]$$

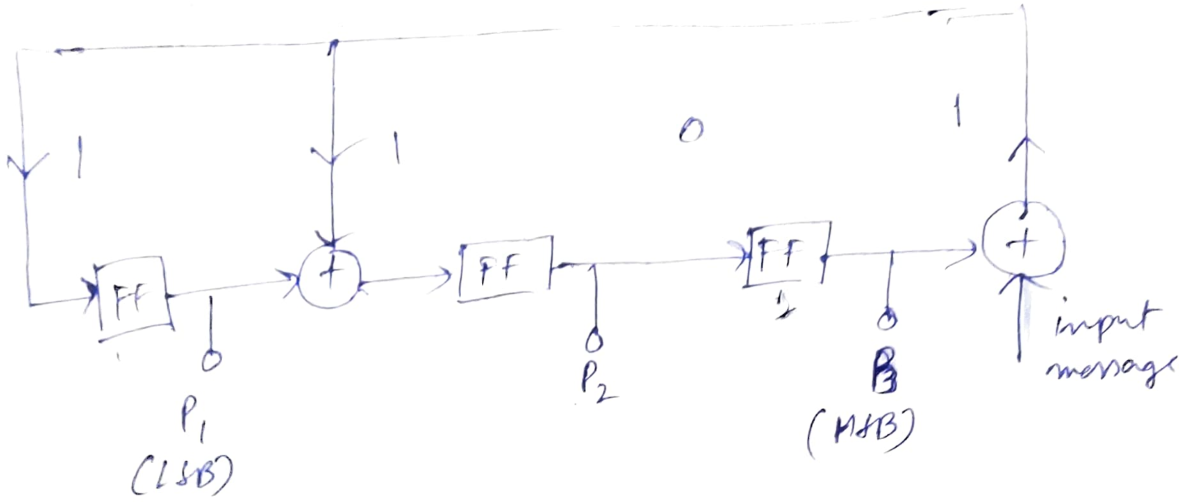
$$\begin{array}{r|l} & x^3+x+1 \\ x^3+x+1 & x^6 \\ & x^6+x^4+x^3 \\ \hline & x^4+x^3 \\ & x^4+x^2+x \\ \hline & x^3+x^2+x \\ & x^3+x+1 \\ \hline & x^2+1 \end{array} \qquad \begin{array}{r|l} & x^2+1 \\ x^3+x+1 & x^5 \\ & x^5+x^3+x^2 \\ \hline & x^3+x^2 \\ & x^3+x+1 \\ \hline & x^2+x+1 \end{array} \qquad \begin{array}{r|l} & x \\ x^3+x+1 & x^4 \\ & x^4+x^2+x \\ \hline & x^2+1 \end{array}$$

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

Cyclic encoder designing

- If generated polynomial is goes $= 1+x+x^3$
Calculate ① Cyclic encoder
② Codeword if message is (1110)

$$g(x) = 1 + x + x^3$$
$$= 1 + x + 0 \times x^2 + x^3$$



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

LSB MSB

∴ codeword = [message, parity]
= [1110, 100]

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

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