Page No.
Date

Mod-3

3.1 Introduction, Types of code,
- ✓ Types of Error,
- ✓ Error control strategies,
- ✓ Modular arithmetic,
- * use of Galois field & primitive root for generator polynomial,

3.2 Linear Block codes - Introduction,
- ✓ Generator matrices,
- ✓ Parity check matrices,

3.3 ~~Error~~ Syndrome,
- ✓ ~~Error~~ detection,

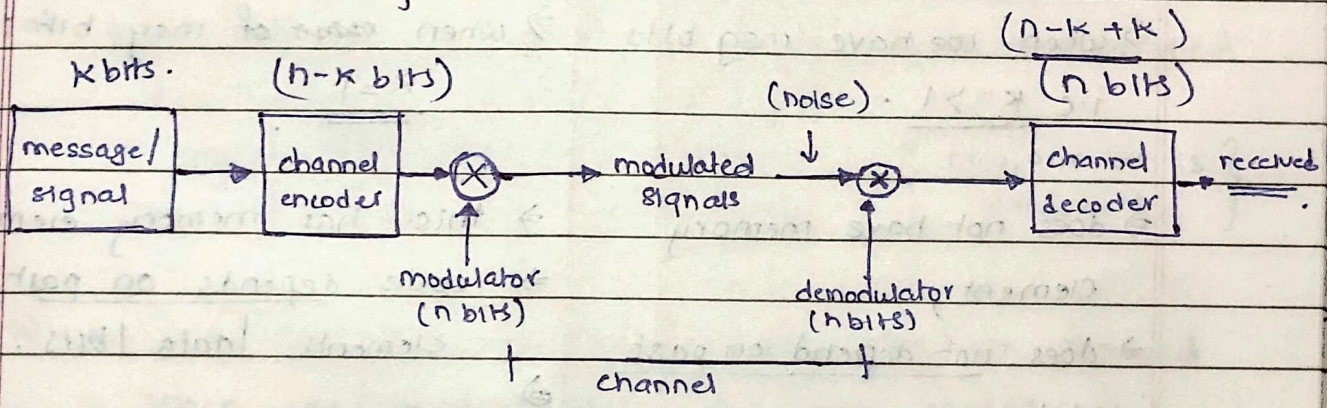
Error detecting and error correction capabilities.

3.4 ~~Standard~~ array and syndrome
- ✓ ~~Decoding~~

Hamming code.

Types of Error :

⇒ Most of the error occurs in the channel, when transmitter sends the signal / data, most of the error is in channel (noise), to prevent this channel encoder ~~transmitter~~ sends some redundant bits, & also we have channel decoder to remove redundant bits, thus avoiding noise.



⇒ message signal goes to channel encoder that adds (n bits) (k bits)

to maintain redundancy [redundant bits = n-k]

⇒ now this signal goes through the channel & decoder, removes the redundancy i.e. remove (n-k) bits.

* Types (2) ⇒ dependent on how channel decoder is connecting to the channel i.e. either retransmit data or ~~sends the data back~~.

⇒ i) Retransmit the data
↳ problem is time delay.

ii) forward action error correction
↳ solve the error, with the available redundant bits the code have.

Page No.
Date

* Type of error detection & correction coding:

Block code	convolution code.
a) Hamming	a) Turbo code
b) BCH	b) Trellis code.
c) cyclic	
d) RS	

⇒ when we have msg bits i.e $k > 1$.

⇒ when ~~none~~ of msg bit i.e. k $(k = 1)$.

⇒ does not have memory element,

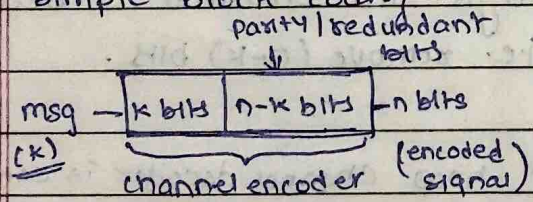
⇒ does not depend on past data

⇒ only works on present data (msg bit)

⇒ this has memory elements,

⇒ code depends on past elements / data / bits.

→ simple block coding.



⇒ n-k ⇒ parity bits

k ⇒ msg bits

(received)

** ⇒ code length (n) ⇒ Total number of bits in the encoded signal.

** ⇒ code efficiency ⇒ $\boxed{k/n = \eta}$. $0 < \eta < 1$

** code weight ⇒ total no. of non-zero bits in the code

eg: 10101 ⇒ 3

Page No.
Date

* Error detection & correction :

* Types of error :

a) single bit
b) Multiple bits
c) Burst error

a) single bits ⇒ only one bit of the data transmitted is changed from 0 to 1 or 1 to 0.

eg: 1 0 0 1 ⇒ 0 0 0 1 { only one bit is changed }
sent received.

b) Multiple bits error ⇒ Two or more bits are changed when received, and the bits should not be ~~consecutive~~ consecutive.

eg: 1 0 0 1 0 1 ⇒ 1 1 0 0 0 1

c) Burst error ⇒ 2 or more consecutive bits are changed when the data is received.

→ The length of burst error is measured from first incorrect bit to last corrupted bit.

→ But some bits in betⁿ may not be corrupted but are considered as corrupted.

eg: 1 0 0 1 0 1 ⇒ 1 1 0 0 0 1

eg: 1 1 1 1 1 1 ⇒ 1 0 0 0 0 1

total part is considered as error.

Page No.
Date

* Parity ⇒ extra bit which is added when data is transmitted.

⇒ even parity ⇒ total no. of 1's in o/p data is even.
odd parity ⇒ total no of 1's in o/p signal / data is odd.

∴ when we have any data to be transmitted (eg: 01101) and we want to make this as even parity and send, we'll add extra 1 to the end ⇒ (011011) to make this even parity.

⇒ 011011 —transmission→ 001011
(Sent) (received)

∴ now we see, we dont have even parity, thus error is present.
Thus we can ask for retransmission.

∴ similarly for odd parity, we'll add '0' to our code. eg: (01101) ⇒ 011010, to make odd parity.

* disadvantage ⇒ it cannot tell if 2 errors are made, then it cannot distinguish between if error is done or not.
eg: 011011 ⇒ 01100 } even parity both cases.

* Types of parity check:

a) Vertical b) longitudinal

a) vertical parity check ⇒ detect only 1 error & correct

⇒ we can use even odd parity check.

b) longitudinal parity check ⇒ can detect 2 errors, & correct 1

⇒ in x & y axis the data is set and then parity is calc. for both rows & columns, & matched.

⇒ more efficient to find the error.

Hamming distance: weight of $(C_1 \oplus C_2)$ (XOR)

C_1	C_2	$C_1 \oplus C_2$
0	0	0
0	1	1
1	0	1
1	1	0

∴ eg:

```
  0 1 1 0 1 0   ⇒ C1
⊕ 0 0 1 0 1 1   ⇒ C2
-----------------
  0 1 0 0 0 1   ⇒ 2 weight (total no. of 1's)
```

but another way is

```
0 1 1 0 1 0
0 0 1 0 1 1
```

⇒ 2 diff. ⇒ hamming dist = 2

Minimum hamming distance: $[c_1, c_2, c_3]$

$d\{c_1, c_3\}$ ⇒

0	(1)	1	(0)	1	(0)	⇒ c_1	⇒ 2
0	(1)	1	(1)	1	(1)	⇒ c_2	
0	(0)	1	(0)	1	(0)	⇒ c_3	⇒ 3

$d\{c_1, c_2\} = 2$
$d\{c_2, c_3\} = 3$
$d\{c_1, c_3\} = 1.$
} min. hamm. dist = 1

Hamming Vector: (all values in range of code)

c_1	c_2	c_3	c_1	c_2	c_3
0	0	0	1	1	1

⇒ 3 bit code from (0,0,0) to (1,1,1)

∴ hamming vector ⇒ (0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1).

Hamming sphere ⇒

possibility of transmitting 000 & 111

∴ when 000 is passed into channel, error can occur as (001 or 010 or 100)

similarly if error occurs in (111) it will turn into (110 or 101 or 011)

∴ when we represent all these points on graph, they form a sphere.

$p = n-k$

$d(min) \geq t+1$

Page No. Date

Hamming Bound:

(n, k) code can correct upto t errors.

∴ then hamming bound is $2^{n-k} \geq \sum_{i=0}^{t} {}^{n}C_i$ | $p = n-k$

eg: (7,4) LBC has t=1, find if it is hamming code or not.

$n=7, \quad k=4, \quad n-k=3, \quad t=1.$

$2^3 \geq {}^{7}C_0 + {}^{7}C_1$

$8 \geq 1+7$

$8 \geq 8$ true.

eg: $k=10, \quad p=?, \quad t=1$

$p = n-k \qquad 2^p \geq \sum_{i=0}^{1} {}^{n}C_i$

$2^p \geq n+1 \qquad (n = k+p)$

$2^p \geq 11+p.$

sub. values 1, 2 ... for p.

∴ $p=4$.

Error detection & correction capability:

$d(min) \geq t+1$ [t = detected error]

min hamm. dist.

∴ corrected error $t = \frac{d(min-1)}{2}$ (odd dmin)

$t = \frac{d(min-2)}{2}$ (even d(min))

$a \equiv b \pmod m \Rightarrow a/m = rem = b$

Page No.
Date

Modular arithmetic

$$a \equiv b \pmod m$$

↳ When a is divided by m, remainder is b.

= ~~a/m ≡ b~~ $a/m = rem = b$

eg: $15/4 = rem = 3 \rightarrow 15 \equiv 3 \pmod 4$

$$\Rightarrow a + k \equiv b + k \pmod m$$

eg: $15 + 3 = 3 + 3 \pmod 4$

$18 = 6 \pmod 4$ $\quad 6 \bmod 4 = 2$

$\Rightarrow 18/4 = 2$ (N) ?

$$\Rightarrow a - k \equiv b - k \pmod m$$

$15 - 2 \equiv 3 - 2 \pmod 4$

$13 \equiv 1 \pmod 4$

$\therefore 13/4 = 1$

$$\Rightarrow ak = bk \pmod m$$

$15 \times 2 = 3 \times 2 \pmod 4$

$30 = 6 \pmod 4$

$30 = 2 \pmod 4 \Rightarrow 2$ ~~6~~ Y.4.

$\therefore 30/4 = 2$

* $$a^k = b^k \pmod m$$

$2^3 = 1 \pmod 7$

eg: 2^{100} / 7

eg: $15 \equiv 3 \pmod{12}$

divide by 3

$15/3 = 3/3 \pmod{12}$

$5 \equiv 1 \pmod{12}$

now, $5/12$ is not 1 as rem.

because, 15 & 3 both are not co-primes,

∴ we need to calc. HCF (15,3) = 3.

now divide all values by 3.

⇒ $5 \equiv 1 \pmod{4}$

now $5/4 = 1$

---

① $x \equiv y \pmod{n}$

If both x and y have same remainder when divided by n.

⇒ $x/n = \text{rem} = y$ ⇒ $x/n = \text{rem} = y$ or y/n

eg: $36 \equiv 24 \pmod{2}$ ⇒ $36/12 \neq 24/12 = 0$

eg: $20 = 3 \pmod{17}$

⇒ $x/n = 20/17 = 3 = y$

② If $x \equiv y \pmod{n}$ and $a \equiv b \pmod{n}$ then.

$$(x+a) = (y+b) \mod n$$

eg: $17 \equiv 4 \mod 13$ $\quad$ $42 = 3 \mod 13$

$17/8 = 4$ $\quad$ $42/13 = 3$

⇒ $(x+a) = (y+b) \mod n$.

$59 \equiv 7 \mod (13)$

$= 59/13 = 7$.

$x \to a \quad y \to b$.

$x \equiv y \pmod n \quad a \equiv b \pmod n$

Page No.
Date

(3) If $x \equiv y \bmod n$ and $a \equiv b \bmod n$,
then $(x-a) \equiv (y-b) \bmod n$.

eg: $42 \equiv 3 \bmod (13)$ & $14 \equiv 1 \bmod (13)$

$\Rightarrow (42 - 14) \equiv (3 - 1) \bmod (13)$

$= 28 \equiv 2 \bmod (13)$

$28/13 = 2$

(4) If $x \equiv y \bmod n$ and $a \equiv b \bmod n$,
then $(xa) \equiv (yb) \bmod n$

eg: $6 \equiv 1 \bmod (5)$ & $7 \equiv 2 \bmod (5)$

$\Rightarrow 6/5 = 1 \qquad 7/2 = 5$.

$\therefore (6 \times 7) \equiv (2 \times 1) \bmod 5$

$42 = 2 \bmod 5$

$42/5 = 2$.

(5) If $x \equiv (y \times z) \bmod n$, then.

$x \equiv (y \bmod (n) \times z \bmod (n)) \bmod n$

eg: $7 \equiv (12 \times 11) \bmod 5$

$7 \equiv (12 \bmod 5) \times 11 \bmod 5) \bmod 5$

$7 \equiv (2 \times 1) \bmod 5$

$\therefore 7 \equiv 2 \bmod 5$

$\therefore 7/5 = 2$

Page No.
Date

⑥ If $x \equiv (y+z) \bmod n$, then.

$x \equiv (y \bmod n + z \bmod n) \bmod n$.

eg. $8 = (11+12) \bmod 5$

$8 = [(11 \bmod 5) + (12 \bmod 5)] \bmod 5$

$8 = (1+2) \bmod 5$

$8 \equiv 3 \bmod 5$

$8/5 = 3$

Fermat's little Theorem

when P is a prime no.

$$a^{p-1} \equiv 1 \bmod (p)$$

Eulers Tohent theorem:

when, $\phi(N)$ = no. of coprime no. less than given no.

$$a^{\phi(N)} \equiv 1 \bmod (N)$$, when N is composite no.

Willsons theorem: (For Factorials)

$$(p-1)! + 1 \equiv 0 \pmod p$$

eg: $p=5$

$4! + 1 \equiv 0 \pmod 5$

$25 = 0 \pmod 5$

$\Rightarrow 25/5 = 0$

(GCD of 2 no = 1 they are coprime)

Page No.
Date

Euler's totient function : $\phi(N)$ $N \geq 1$

$\phi(N)$ = no. that are less than N and are coprime to N.

$\phi(5) = \{1, 2, 3, 4\}$ all are coprime.

$\phi(6) = \{1, 5\}$ 2, 3 ke table me 6 atay, 4 is divisible by 2 also, GCD = 2.

* When $\phi(N)$, N = prime

$\boxed{\phi(N) = N-1}$, $\phi(23) = 22$

* $\phi(a * b) = \phi(a) * a(b)$ [a & b are coprime] (a & b = prime)

$\phi(35) = \phi(7) \times \phi(5)$ 7 & 5 are coprime.

$= 6 \times 4$ GCD (7, 5) = 1

$= 24$.

* $\boxed{x^{\phi(N)} \equiv 1 \mod (N)}$ ⇒ eulers theorem.

eg: $x = 4$, $n = 165$

gcd (4, 165) = 1.

$\phi(165) = \phi(15) \times \phi(11)$

$= \phi(3) * \phi(5) * \phi(11)$

$= 2 \times 4 \times 10$

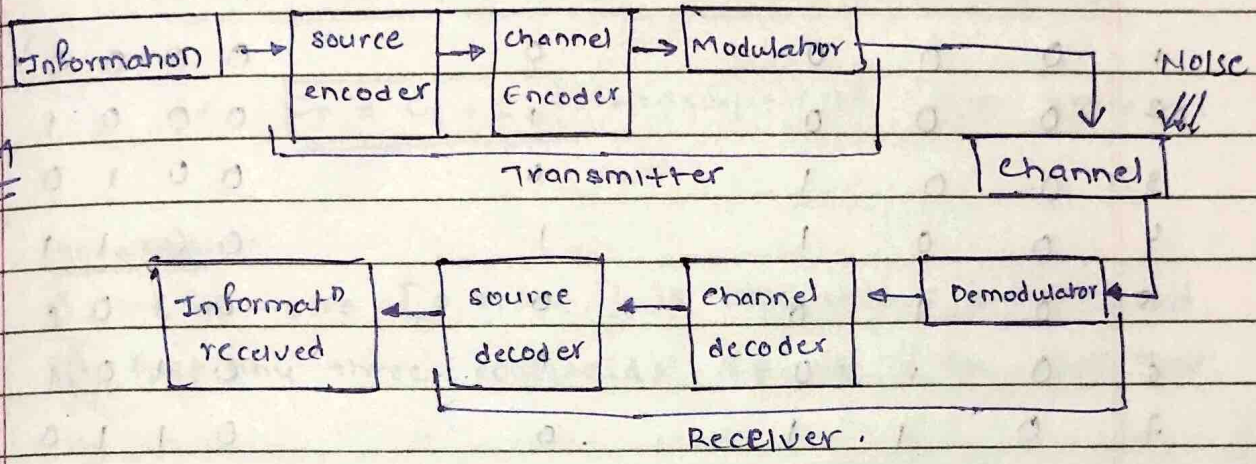
$= 80$

$(4)^{80} = 1 \mod (165)$

* we use block code, to correct error when data is received.

Page No. | Date

* A block code is a set of words that has well defined mathematical property structure + where each word is a sequence of fixed no. of bits.



S-C-M

⇒ at channel encoder, we add block code to solve error.

⇒ at source Encoder, we reduce redundancy to improve bandwidth utilization.

∴ information bits = K

Parity/Redundancy = r

∴ total bits = n = K + r

∴ (n, K) is block code representation.

* Systematic code word ⇒ where information bits & parity bits [$i_1, i_2, i_3 \dots, P_1, P_2, P_3 \dots$] are kept together.

* Asystematic ⇒ info & bits are not kept together.

[$i_1, P_1, i_3, P_4, i_5, i_6 \dots$]

* Block code (n, K)

a) total code words required as per n block codes = 2^n

b) K information = 2^K

c) total redundant code word as per parity bits = $2^n - 2^K$

d) code Rate, $R = K/n$ | n = total no of bits in block code.

⇒ $(n, k) \equiv (4, 3)$, parity $= n - k = 1$ $\quad n=4, k=3$.

	Information bits (n) (i)			Parity (P)	code word
1	0	0	0	0	0 0 0 0
2	0	0	0	1	0 0 0 1
3	0	0	1	0	0 0 1 0
4	0	0	1	1	0 0 1 1
5	0	1	0	0	0 1 0 0
6	0	1	0	1	0 1 0 1
7	0	1	1	0	0 1 1 0
8	0	1	1	1	0 1 1 1
9	1	0	0	0	1 0 0 0
10	1	0	0	1	1 0 0 1
11	1	0	1	0	1 0 1 0
12	1	0	1	1	1 0 1 1
13	1	1	0	0	1 1 0 0
14	1	1	0	1	1 1 0 1
15	1	1	1	0	1 1 1 0
16	1	1	1	1	1 1 1 1

∴ For even parity check → 1, 4, 6, 7, 10, 11, 13, 16.

* codeword $= C = [I, P] = [i_1, i_2, i_3 \cdots, P_1, P_2, P_3 \cdots]$

* Error code word, $e = [e_1, e_2, \cdots]$

where $e_j = 1$ means error

$e_j = 0$ means no error.

∴ error codeword + received codeword = valid data

Page No.
Date

Linear Block code:

⇒ A block code is said to be linear block code if, sum of two code words is another codeword

i.e. $C_p = C_i + C_k$ → addition of 2 c.w = 3rd c.w.

Properties

i) The all-zero [0,0,0...] is also always a codeword

ii) Give any three codewords C_p, C_i & C_k such that

$C_p = C_i + C_k$, then minimum hamming dist.

$d(min)[C_i, C_k] = w[C_p]$

= weight of c_p.

⇒ $C_p = C_i + C_k$.

$d_{min}[C_i, C_k] = w[C_p]$

iii) min. distance of code = weight.

$d_{min} = w_{min}$.

eg: (7,4) hamming code,

$C_1 = 0\ 0\ 0\ 1\ 0\ 1\ 1$

$C_{10} = 1\ 0\ 1\ 0\ 0\ 1\ 1$

$C_p = C_1 + C_{10}$

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

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

$1\ 0\ 1\ 1\ 0\ 0\ 0 = C_{11}$ [according to hamming code table]

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

$C_0 = [0\ 0\ 0\ 0\ 0\ 0\ 0]$.

b) C_p, C_i, C_k

$w(C_p) \geq d_{min}(C_i, C_k)$

$w(C_1) = 3$ ∴ min hamm. dist = 3. $d(C_1, C_{10}) = 3$

$w(C_{10}) = 4$

∴ $w(C_{11}) = d_{min}(C_1, C_{10})$

$11 = 11$

c) $d_{min} = w_{min}$:

$C_{15} = [1, 1, 1, 1, 1, 1, 1]$

$w = 7$, other than C_{15}, codes are having wt. of 3 & 4.

∴ $d_{min} = w_{min}$

eg: Show that (4,3) even parity code is linear code.

⇒ (4,3) even parity.

∴ data bit = 3 ; even parity

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

take any 2 code.

a) $C_1 + C_2 =$ 0 0 1 1

→ 0 1 0 1

0 1 1 0

∴ $= C_3$

b) $w(C_1) = 2$, $w(C_2) = 2$

$d_{min} = 2$

$w(C_3) = 2$

$w(C_3) = d(min(C_1, C_2))$

$G = [I_k : P]$

↑ identity matrix ↑ parity matrix

Page No.
Date

Systematic Generator matrix in LBC

⇒ A generator matrix $[G] = [I_k : P]$, it is said to be in systematic form, only if it generates the systematic codewords.

$[C] = [i][G] = [m, P]$ (message & then parity)

Here, $[I_k] = k \times k$ matrix.

$[P] = k \times (n-k)$ matrix

$[G] = k \times n$ matrix.

Generator matrix: (to generate code words) in LBC.

⇒ using a matrix to generate codeword is a better approach.

$[C] = [i][g]$

c ⇒ code word

i ⇒ information words

g ⇒ generator matrix.

$[G] = [I : P]$

⇒ The generator matrix of an (n, k) linear code has (n-columns) & (k-rows)

eg: generator matrix (G) for (7, 4) ⇒ 7 col, 4 rows.

$[G = I : P]$

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

identity matrix. (I_k) k no. of rows & cols

parity matrix.

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

$[C]$ ← codeword, $[i]$ ← info matrix, $[G]$ ← generator

Page No. Date

∴ code word $[C]$ = $[i]$ msg × $[G]$ generator matrix.

eg codeword generate, i = (1110) with (7,4) generator matrix

⇒ ∴ ~~7 row~~ 7 cols 4 rows

$[G] = [i][P]$

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

∴ code word = information matrix $[i]$ × $[G]$

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

row · col

$= [\text{row}_1 \times \text{col}_1 \quad \text{row}_1 \times \text{col}_2 \quad \ldots\ldots]$

$= [1\cdot1+1\cdot0+1\cdot0+0\cdot0 \quad 1\cdot0+1\cdot1+1\cdot0+0\cdot0 \quad 1\cdot0+1\cdot0+1\cdot1+0\cdot0 \quad 1\cdot0+1\cdot0+1\cdot0+0\cdot1 \quad \ldots$

continuation to same row.

$\ldots \quad 1\cdot1+1\cdot1+1\cdot1+0\cdot0 \quad 1\cdot0+1\cdot1+1\cdot1+0\cdot1 \quad 1\cdot1+1\cdot1+1\cdot0+0\cdot1]$

$1+1+1=1 \qquad 1+1=0 \qquad 1+1=0$

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

codeword

$G = I : P$ $\quad [C] = [m : P]$

$c = [i][G]$

Page No. Date

eg: determine. generate codeword for (6,3) code. $n=6,\ k=3,\ p = n-k = 3$.

msg bit = 3 = n.

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

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

(possible combinations)

	m_0	m_1	m_2
c_0	0	0	0
c_1	0	0	1
c_2	0	1	0
c_3	0	1	1
c_4	1	0	0
c_5	1	0	1
c_6	1	1	0
c_7	1	1	1

$\therefore c_0 = [i][G]$

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

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

$c_1 = [i][G]$

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

row × col.

$c_1 = [0\ 0\ 1\ 1\ 1\ 0]$

∴ calculate for all

c_0	0	0	0	0	0	0
c_1	0	0	1	1	1	0

→ parity bits (verified from ques).

* codeword $[C] = [m, P]$

$[P_c] = [m] \times [P]$ → parity matrix.

$[G] = [I : P]$ $\quad [C] = [i][G]$

5 7 6 3

Page No.
Date

* **Systematic Generator matrix in LBC.**

A Generator matrix $[G] = [I : P]$ ~~is said to~~ generates only systematic codewords

↳ $[m, P] = c$

$$[C] = [i][G] = [m : P]$$

here: I ⇒ identity matrix = $k \times k$
P ⇒ parity = $k \times (n-k)$
[G] ⇒ Generator $(k \times n)$ } size

⇒ in systematic matrix info bits are together.

⇒ codeword $[C] = [i][G]$

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

i_1 i_2 i_3 i_4 P_1 P_2 P_3

∴ codeword $= [i_1, i_2, i_3, i_4, P_1, P_2, P_3]$ } Systematic code matrix.

$P_1 = i_1 \oplus i_2 \oplus i_3$
$P_2 = i_2 \oplus i_3 \oplus i_4$
$P_3 = i_1 \oplus i_2 \oplus i_4$ } Parity bits values

Page No.
Date

Q (5,3) LBC has generator matrix.

a) determine systematic form of G.

b) Generate c.w. from i = (0 1 1)

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

I_k not present

∴ no systematic G. matrix

$$\Rightarrow [G] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix} \quad (\times, \checkmark, \times)$$

∴ if we add 2nd & 3rd row, 3rd row will get correct

(add R_2 to R_3)

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

now if we add R_3 & R_1 we get desired I matrix.

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

now $[G] = [I : P]$

∴ generate a code (i = 011) with non-systematic [G]

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

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

(row × col)

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

transpose → row ko col / col ko row.

Page No.
Date

for systematic [G] c.w →

(i = 011)

$$[c] = [i]\,[G]$$

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

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

∴ for systematic [G] ⇒ [c] = [0 1 1 | 1 0]
[i] | P

Parity check matrix in LBC [H]

⇒ From Generator matrix, we get identity & parity matrix

$$[G] = [I : P]$$

⇒ by taking (transpose) P^T, we can make parity check matrix. [H]

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

⇒ Parity check matrix is used at Receiver to decode data

eg: Generate parity check matrix.

$$[G] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \quad P^T = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

$G \cdot H^T = 0$

$G \cdot H^T = 0$

Page No.
Date

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

$I_{7-4} = I_3$ identity matrix.

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

g] Prove that GH^T and $GH^T = 0$

$G \cdot H^T = [G] = [I_k : P] \times [H]^T = [P^T : I_{n-k}]^T$

divide.

$= [I_k \mid P] \times [P \mid (I_{n-k})^T]$

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

$= P + P$

∴ $P = 0$ OR $P = 1$

∴ $G \cdot H^T = 0$

H = Parity check matrix.
S = error syndrome

Page No.
Date

Error Syndrome in (LBC) :

⇒ means solving error in received data.

⇒ If code word transmitted is [C]
+ we receive [Y] codeword.
∴ channel adds noise, to codeword ⇒ [C] + [e]

then to solve error we need error syndrome.

$$[S] = [Y]\,[H^T]$$ Y = received CW

= [received code] × [H transpose]

∴ [Y] = [C] + [e]

if error [e] = 0

[Y] = [C] -- received = transmitted.

∴ $[S] = [C]\,[H^T]$ but $[C]\,[H^T] = 0$

$[S] = 0$.

Page No.
Date

Eg: Find error syndrome of $V_1 = (1101101)$, where V is received cw & also calc. errored bit.

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

$\therefore [S] = [V] \times [H^T]$

$= [1101101] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ 1, 2, 3, 4, (4).5, 6, 7

row x col.

$= [1\ 0\ 0]$

check at what pos is 100 present in H^T & count the position, at 5th pos

$y = [1101101]$, error at 5th pos.

$\therefore e = [0000100]$

$\therefore y \oplus e = [1101001]$ = correct o/p.

error detectn	$d_{min} \geq s+1$	s = err. dete. capacity
error correctn	$d_{min} \geq 2t+1$	t = error correctn capacity

Page No.
Date

Error detection & correction capability of LBC

⇒ step 1 → identify min hamming distance

* error detection capacity

⇒ $\boxed{d_{min} \geq s+1}$

where, s = error detection capacity

* error correction capacity

⇒ $\boxed{d_{min} \geq 2t+1}$

where t = error correction capacity

eg. If min hamming dist of LBC = 3, $d_{min} = 3$

Find LBC error correction & detection = ?

⇒ $d_{min} = 3$,

∴ error detection = $d_{min} \geq s+1$

$= 3 \geq s+1$

$2 \geq s$

$s \leq 2$

this code can detect 2 bit error.

∴ error correction = $d_{min} \geq 2t+1$

$= 3 \geq 2t+1$

$t \leq 1$

this code can correct 1 bit error.

2^K possible codewords.

Page No.
Date

Standard array

(n, k) LBC, k = no. of bits of info.

∴ 2^K possible msg sequences.

= 2^K possible codewords

∴ 2^n possible received vectors

∴ let r be any vector that is received, which is a part of 2^n possible vectors that can be received.

now, receiver has job of partitioning 2^n possible vectors into 2^K disjoint subsets in such a way that i^{th} subset D_i corresponds to codevector C_i

~~D_1, D_2 etc such that sub~~

~~* The 2^K subsets of possible codewords is the standard array of LBC~~

* The 2^K subsets of $D_1, D_2 \dots D_{2^K}$ such that subset D_i corresponds to codevector C_i is the standard array of LBC

* 2^K subsets such that $D_i \equiv C_i \Rightarrow$ standard array.

* Steps involved in constructing standard array.

⇒ the 2^K codewords are placed in a row, with all zero codeword as leftmost element.

let $C_0 \dots C_{2^K-1}$ be 2^K possible codewords, & C_0 = all zero.

be 1st row of standard array.

2^n elements are present in std. array, of these 2^n elements are partitioned into 2^k subsets (disjoints),

2^k cols | $2^n/2^k$ rows

(2) → An error pattern (e_1) is picked & placed under c_0 and a 2nd row is formed by adding e_{01} to each of remaining code vectors in first row.

c_0	c_1	c_2	... c_{2^k-1}	row 1
e_1	c_1+e_1	c_2+e_1	... $c_{2^k-1}+e_1$	row 2.

∴ we can say 1st row is formed by adding e_0 to all values where (e_0) = all zero.

(3) → Step 2 is repeated unnil all possible error pattern with distinct syndrome is selected.

c_0	c_1	c_2	...	c_{2^k-1}
e_1	e_1+c_1	e_1+c_2	...	$c_{2^k-1}+e_1$
e_2	e_2+c_1	e_2+c_2		$c_{2^k-1}+e_2$
e_3	e_3+c_1	e_3+c_2		$c_{2^k-1}+e_3$
⋮				
$e_{2^{n-k}-1}$	$e_1+e_{2^{n-k}-1}$	...		$c_{2^k-1}+e_{2^{n-k}-1}$

⇒ The 2^{n-k} rows of array represet coset of the code. and 1st element of each row = coset leader which gives locatn of error.

⇒ The top tuple is fixed code vector.

⇒ e_1, e_2 etc represent single bit error pattern.

* no. of rows 2^{n-k} = no. of syndrome

* each row of [G] = cw.

Page No.
Date

⇒ if $n < 2^{n-k}$, may list all double / triple error pattern until we have 2^{n-k} entries in 1st col.

q] [G] for (5,2) LBC,

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

a) all possible cw
b) find dmin
c) how many error it can correct.
d) construct std arry.
e) decode cw if received vector is 00110

⇒ n=5, k=2, p=3, n-k=3

∴ k=2 msg bits ∴ all possible, cw = $2^k = 2^2 = 4$.

m_0	m_1
0	0
0	1
1	0
1	1

(a) ∴ all possible cw.

1) 0 0 0 0 0
each row of [G] is cw.
2) 1 0 1 0 1
3) 0 1 1 1 0
add (2 & 3)
4) 1 1 0 1 1

(b) ∴ dmin of all (1-4) cw ⇒ 3.

(1,2) = 3 w(1) = 0
(1,3) = 3 w(2) = 3
(1,4) = 4. w(3) = 3
w(4) = 4.

(c) ∴ dmin ≥ 2t+1

3 ≥ 2t+1

$t \leq 1$

d) std array

① write cw as 1st row of std Array.

② $2^n = 2^5 = 32$ entries.

③ rows = $2^{n-k} = 2^3 = 8$

cols = 4 cw = 4 cols :

④ all possible single bit error patter = 1st col.

$2^3 = 8$ possibilities

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

$H = P^T I$

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

000
S_5 ← 001
S_4 ← 010
011
S_3 ← 100
S_1 ← 101
S_2 ← 110
111

} possibilities of syndrome.

$H^T = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ ← syndrome corresp. 1st bit error
2nd bit in error
3rd bit in error
4th
5th

∴ double error patter is at: 011, 111.

⇒ write all possible that act as 1st row. ① . Syndrome

$C_0 = e_0$	00000	10101	01110	11011	000
possible error patter ⇒	00001	⟶ $C_4 + e_1$			101
	00010 (e2)	⟶ $C_1 + C_2$			010
	00100				100
	01000				010
	10000				001
					111

Add 6 & 3.

Hamming code ⇒ used in detecting & correction

→ represented as (n, k) code.

n = total bits

k = info bits

p = parity bits = $n - k$. = p

= $2^p \geq p + k + 1$

∴ for $k = 4$,

$2^p \geq p + 4 + 1$

$2^p \geq p + 5$

for $p = 1$, $2^1 \geq 6$ ✗

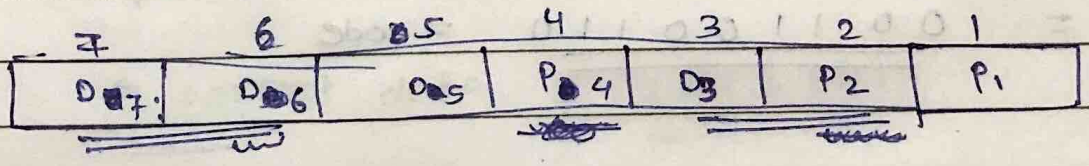
$p = 3$ $2^3 \geq 8$ ✓ ∴ 3 parity bits

∴ $n = 3 + 4 = 7$ bits

∴ (7, 4) hamming code with 3 parity bits.

∴ total bits $(n) = 7$, info = 4 bits = k.

$p = 3$,



∴ $(2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4)$ = position of parity bits

P_1 = take 1 skip 1 = $D_3 \oplus D_5 \oplus D_7 = P_1$

P_2 = take 2 skip 2 from $P_2 = D_3 \oplus D_6 \oplus D_7$

P_3 = take 3 skip 3 from $P_4 = D_5 \oplus D_6 \oplus D_7$.

* eg 5 bit data, n=5 (01101)

∴ no. of parity bits = $2^p \geq p+k+1$.

∴ $k = 5$

$= 2^p \geq p+6$

∴ $p = 4$ $\quad 2^4 \geq p+6$

$16 \geq 10$.

∴ ~~16 = 16~~ $p = 4$, $k = 5$ $\quad n = 9$ . . . (9,5)

9	8	7	6	5	4	3	2	1
D9	P8	D7	D6	D5	P4	D3	P2	P1

check first then skip → ek chod ke ek, 2 chod ke 2, 3 chod ke 3.

$2^0 = 1 = P_1 = D_3 \oplus D_5 \oplus D_7 \oplus D_9 = 0$

$2^1 = 2 = P_2 = D_3 \oplus D_6 \oplus D_7 = 1$

$2^2 = 4 = P_4 = D_5 \oplus D_6 \oplus D_7 = 0$

$2^3 = 8 = P_8 = D_9 = 0$

} odd parity

D9			D7	D6	D5			D3			
0	0	1	1	0	0	1	1	0			

= 0 0 1 1 0 0 1 1 0 = code

#

Page No.
Date

Q) * If say we receive 1110101 with even parity. then we need to detect & correct.

7	6	5	4	3	2	1
1	1	1	0	1	0	1

$P_1 = 1$, $P_2 = 0$, $P_4 = 0$.

$D_3 \oplus D_5 \oplus D_7$.

$\therefore P_1 = 1 \oplus 1 \oplus 1 = 1$ true

$P_2 = D_3 \oplus D_6 \oplus D_7 = 1$ = false = at 2nd pos we have 0.

$P_4 = D_5 \oplus D_6 \oplus D_7 = 1$ = ~~true~~ false = at 4th pos we have 0.

$P_2 \neq$ $P_4 \neq$.

P_4 P_2 P_1

1 1 0 $\Rightarrow$ 6th bit = error.

$\therefore$ error syndrome

E = | 0 | 1 | 0 | 0 | 0 | 0 | 0 |

↑ error.

$\oplus$

1	1	1	0	1	0	1

= correct data = 1010101 .

Page No.
Date

Mod-4

4.1 cyclic codes

- ✓ → Introduction
- ✓ → Generation
- ✓ → Syndrome Computation & error detection
- ✓ → Decoding

4.2 Hamming code ✓ → error syndrome

- ✓ → Error detection & correction
- → Extended Hamming code

Golay code

Error detection using Cyclic Redundancy check.

4.3. Convolution code – Intro

Tree and Trells codes.

4.4 Encoding

decoding

application.

Cyclic codes → linearity (c = a + b)
→ shifting properties 1001 → 1011

Cyclic codes ⇒

→ cyclic codes are subparts of LBC.

* Properties :

a) Linearity Property :

→ LBC follow property of linearity
∴ cyclic codes also follow
→ $C_p = C_i + C_j$
where all C_is are code words. | belong to eachother

b) Cyclic shifting property :

→ shifting bits left or right by any no. of bits, the resultant should be a codeword. | belonging to eachoth

⇒ If c.w. follows these both properties of linearity and cyclic shifting then they are cyclic.

eg : {0000, 0110, 1001, 1111}

→ check property of linearity.

0 1 1 0	1 0 0 1	0 1 1 0
+ 1 0 0 1	→ 1 1 1 1	1 1 1 1
1 1 1 1 ✓	0 1 1 0 ✓	1 0 0 1 ✓

thus they all belong to same grp thus, they follow property of linearity.

⇒ check property of shifting :

→ 0110 ⇒ 0011 X. nor a code word as it is not present in list.
shift

thus above codes are not cyclic

syndrome $S \times H^T = 0$ o/p has no error

Page No.
Date

* The minimum dist. betn 2 cyclic codeword.
= min. hamming wt
0 2 2 4. dmin.

eg: {0000, 1010, 0101, 1111}

$d_{min} = 2$ ∵ 0 is only a necessary condition.

↳ min hamming distance = 2
min hamming wt = 2

Types of generation and detection.

Generation	Detection
→ Non-systematic	→ syndrome detectn [error pattern]
→ systematic	→ Syndrome calc.
→ cyclic code generator	

⇒ Non-Systematic [don't know where Parity bit is placed].
⇒ Systematic [place of parity bit is known]
⇒ cyclic code generator ⇒ using registers & FF arrays.

* Non-systematic → multiplication
→ generator matrix

* Systematic → division
→ generator matrix.

Polynomial representation :

(n, K) cyclic code | n = no. of codeword bits | K = msg bits.

$m(p) = p^{K-1} \cdot m_K + p^{K-2} \cdot m_{K-1} + p^{K-3} \cdot m_{K-2} + \cdots p^2 m_3 + p^1 m_2 + p^0 m_1$

$(1101) = p^{4-1} \cdot 1 + p^{4-2} \cdot 1 + p^{4-3} \cdot 0 + p^{4-4} \cdot 1$

m_K = msb value, $K = 4$ m_K = value at corresponding digit from L→R.

$= p^3 + p^2 + p^0$ → 1101.

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

* generator polynomial ⇒ n-k parity bits.

$$g(p) = p^{n-k-1} g_{n-k} + p^{n-k-2} g + \cdots + p^1 g_2 + g_1$$

* codeword (c) = $c(p) = p^{n-1} c_n + p^{n-2} c_{n-1} + \cdots + p^2 c_3 + p c_2 + c_1$

Cyclic code for non systematic codewords:

- codeword = msg + parity bits.
- in ex non systematic msg & parity are jumbled / not in sequence.

* Polynomial for non systematic codeword:

$c(x) = m(x) \cdot g(x)$, where $m(x)$ = msg polynomial & $g(x)$ = generator polynomial.

∴ Polynomial = ?

eg: 1011 ⇒ 1 0 1 1

x^3 x^2 x^1 x^0

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

= $x^3 + x + 1$

} polynomial generation

* construct non-systematic cyclic code (7,4) code using generator polynomial $g(x) = x^3 + x^2 + 1$ with msg (1010).

⇒ msg = 1010, K = 4.

m(x) = msg polynomial = 1 0 1 0

x^3 x^2 x^1 x^0

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

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

∴ $c(x) = m(x) \cdot g(x)$

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

$= x^6 + x^5 + x^3 + x^4 + x^3 + x$ } mod 2 addtn // ⊕.

$c(x) = x^6 + x^5 + 2x^3 + x^4 + x$ // $= x^6 + x^5 + x^4 + x$

non systematic ⇒ $c(x) = m(x) \cdot g(x)$

systematic ⇒ $c(x) = x^{n-k}\ m(x) + p(x)$ $\quad p \neq$ parity

Page No. Date

$\therefore c(x) = 1\,x^6 + x^5 + x^4 + x$.

x^6	x^5	x^4	x^3	x^2	x^1	x^0
1	1	1	0	0	1	0

$= (1110010)$ = code

cyclic code for systematic codeword.

⇒ systematic ⇒ (msg : parity) sequence.

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

where $p(x) =$ Remainder of $\left[\dfrac{x^{n-k} \cdot m(x)}{g(x)}\right]$

$g(x)$ = generator polynomial.

eg: construct cyclic code (7,4) $g(x) = x^3 + x^2 + 1$.

msg = (1010), $K = 4$, $n = 7$.

⇒ $x^{n-k} = x^{7-4} = x^3$

$m(x) = 1\ 0\ 1\ 0$

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

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

$\therefore p(x) = \text{rem}\left[\dfrac{x^{n-k} \cdot m(x)}{g(x)}\right]$

$= \text{rem}\left[\dfrac{x^3 (x^3 + x)}{x^3 + x^2 + 1}\right]$

$= \text{rem}\left(\dfrac{x^6 + x^4}{x^3 + x^2 + 1}\right)$

$= 1$

$x^3 + x^2 + 1 \;\big|\; x^6 + x^4$ $\quad (x^3 + x^2 + 1)$

$\oplus\ x^6 + x^5 + x^3$

$0 + x^5 + x^4 + x^3$

$\oplus\ x^5 + x^4 + x^2$

$0 \quad 0 + x^2 + x^3$

$+\ x^2 + x^3$

1

generator matrix $g(x) = I : P$

$P = P_{i\,row} = rem\left[\frac{x^{n-i}}{g(x)}\right]$

$P(x) = 1 = x^0 = 1$

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

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

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

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

∴ check if code word is systematic or not;
compare C with msg in question.

Generator matrix of systematic cyclic codes

$[G] = [I : P]$

I = identity matrix. } n = columns
P = parity matrix } k = rows

→ Identity matrix is known to us

but for parity matrix

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

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

Kth row ⇒ $rem\left[\frac{x^{n-k}}{g(x)}\right]$ ← parity matrix value.

Generator matrix for non-systematic cyclic code:

$$\boxed{row_i = x^{k-i} \times g(x)} \Leftarrow \text{value at each row}$$

eg: (n,k) cyclic code, (7,4) cyclic code

$m = 0101 = x^2 + 1$ $\quad n = 7$

$g = 1011 = x^3 + x + 1$ $\quad k = 4$.

$$row_i = x^{k-i} \cdot g(x)$$

$row_1 = x^{4-1} \cdot (x^3 + x + 1)$

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

$= x^6 + x^4 + x^3$

$= (1011000)$

$row_2 = x^{4-2} (x^3 + x + 1)$

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

$= x^5 + x^3 + x^2$

$= (0101100)$

$row_3 = x^{4-3} \cdot (x^3 + x + 1)$

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

$= x^4 + x^2 + x$

$= (0010110)$

$row_4 = x^{4-4} (x^3 + x + 1)$

$= x^3 + x + 1$

$= (0001011)$

$$g(x) = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$ ⇐ generator matrix.

$[c] = [m] \times [g]$.

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

$\therefore$ XOR 2 4 4th row

$= (0100111)$ code.

no. of FF = n-K

Page No. Date

K

Syndrome calc & error detection :

q] Design syndrome calc for (7,4) cyclic code where generator polynomial is $G(x) = x^3 + x + 1$. calculate syndrome for e.w = 1010

C = 1010011

⇒ $G(x) = x^3 + x + 1$

(G) = 1011

(received) R = 1110 011

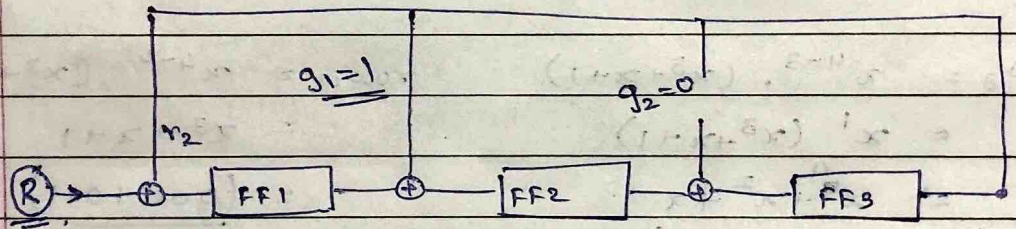
$g(x) = x^3 + g_2 x^2 + g_1 x^1 + 1 \dashrightarrow x^{n-K} + \sum_{i=1}^{n-K-1} g_i x^i + 1$

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

$g_2 = 0$ & $g_1 = 1$ $= x^3 + x + 1$ → (compare)

$= g_1 = 1 \quad g_2 = 0.$

∴ no. of FF = n-K = 7-4 = 3



= Syndrome calculator.

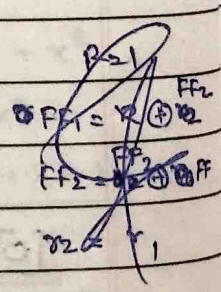
∴ FF1 = $R \oplus r_2$ $= R \oplus FF_3$

$FF_2 = r_2 \oplus r_0$ $= FF_3 \oplus FF_1$

$FF_3 = r_1$ $= FF_2$.

(Jitna bit utna shift)

no. of shift	R	register content FF1	FF2	FF3
		0	0	0
1	1	1	0	0
2	1	1	1	0
3	1	1	1	1
4	0	1	0	1
5	0	1	0	0
6	1	1	1	0
7	1	1	1	1



$c(x) = R(x) + e(x)$

Page No. Date

4.

general eqn for generator polynomial

$$g(p) = p^{n-k-1} g_{n-k} + p^{n-k-2} g_{n-k-1} + \cdots + p^1 g_2 + g_1$$

$$g(x) = x^{n-k} + \sum_{i=1}^{n-k-1} g_i x^i + 1$$

$g_0 = 1$

$g_{n-k} = 1$

* we need some flip flops to generate syndrome calculator.

$\therefore$ no. of FF $= n-k$

s [FF$_3$ FF$_2$ FF$_1$] = 1 1 1

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

$c(x) = R(x) + e(x)$

Error vector							e(x)	s(x) = rem $\left(\frac{e(x)}{g(x)}\right)$
6	5	4	3	2	1	0		
1	0	0	0	0	0	0	x^6	$x^2+1 \Rightarrow 101$
0	1	0	0	0	0	0	x^5	$x^2+x+1 \Rightarrow 111$
0	0	1	0	0	0	0	x^4	$x^2+x \Rightarrow 110$
0	0	0	1	0	0	0	x^3	$1 \Rightarrow 001$
0	0	0	0	1	0	0	x^2	$x^2 \quad 100$
0	0	0	0	0	1	0	x^1	$x \quad 010$
0	0	0	0	0	0	1	x^0	$1 \quad 001$

$e = 0100000$

$c = R + e$

$= 1110011$

0100000

1010011

$x^3+x+1 \;|\; x^5 \ldots$ quotient x^2+1

$x^5 + x^3 + x^2$

$x^3 + x^2$

$x^3 + x + 1$

$x^2 + x + 1$

$x^3+x+1 \;|\; x^4$ quotient x

$x^4 + x^2 + x$

$x^2 + x$

$m = 1010$

* 1st & last is always = 1

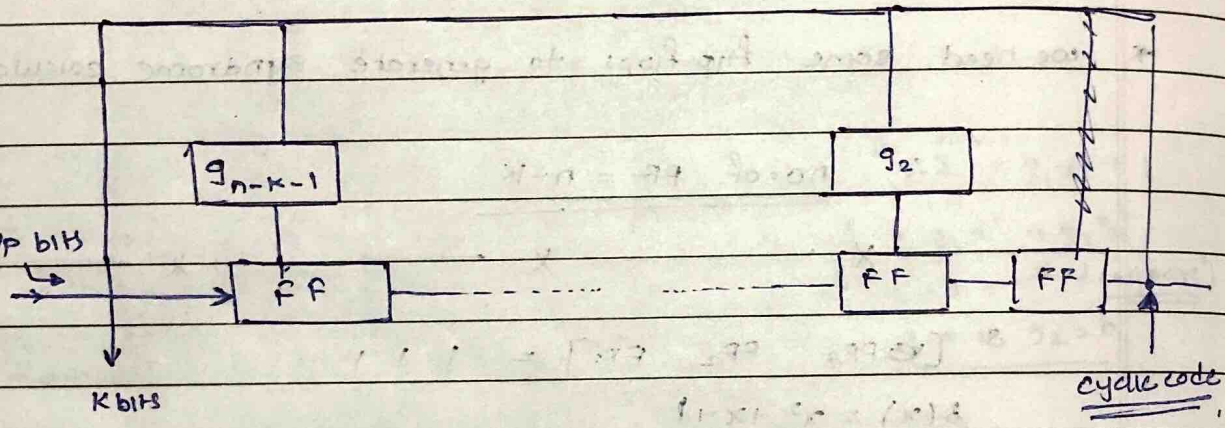
Page No. Date

Encoding using flip flops

$g(x) = x^{n-k-1} g_{n-k} + x^{n-k-2} g_{n-k-1} + \cdots + x^1 g_2 + g_1$

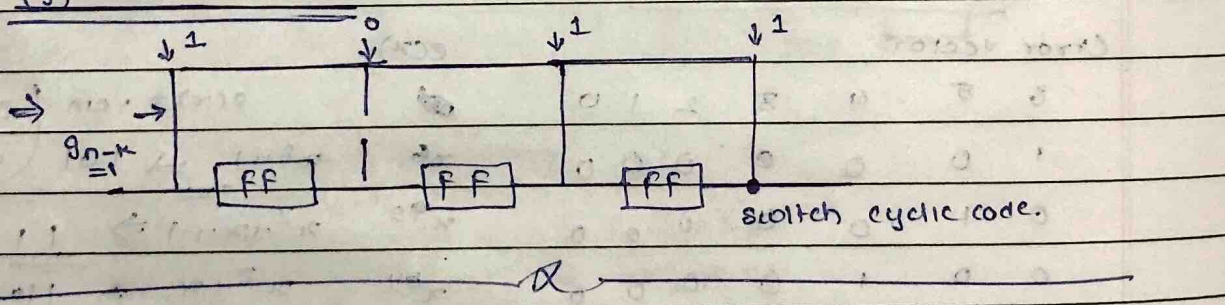
* Properties

a) $g_{n-k} \neq 0$ & $g_1 \neq 0$ → MSB ≠ 0 & LSB ≠ 0.



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

(g) = 1 0 1 1



* Syndrome calc^n.

① get generator poly eqn from $x^{n-k} + \sum_{i=1}^{n-k-1} g_i x^i + 1$ and compare this with given $g(x)$.

② get values of $g_0, g_1, g_2 \cdots$ according to comparision

③ $n-k$ = no. of FF betn each FF, we put $g_1, g_2 \cdots$ values. if $g=1$ closed circuit | $g=0$ open circuit.

④ get eqn of FFs: all. (from diagram)

⑤ get table → no. of shift = count of (no of bits received) | Y = received bits | FF_1 FF_2 FF_3 values according to eqn.

S [FF_3 FF_2 FF_1] last row of table

Syndrome calculation

Page No.
Date

9] For (7,4) generator poly = $g(x) = x^3 + x + 1$.

~~received seq = 1001001~~, find error, if R = correct or not

calculate syndrome for $Y = 1001101$ (received).

⇒ generator polynomial

$$g(x) = x^{n-k} + \sum_{i=1}^{n-k-1} g_i x^i + 1$$

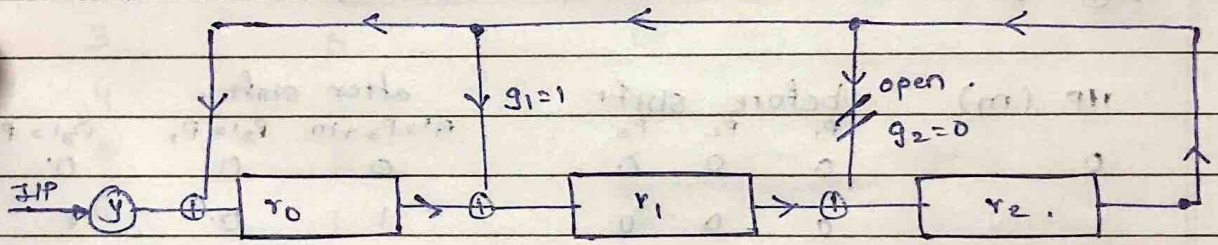
$(n,k) \equiv (7,4)$ $n=7$, $k=4$, no of FF = $n-k = 3$.

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

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

$\therefore g_1 = 1$ $g_2 = 0$ --- we dont have x^2 term.

now, 3 FFs.



* shift register

$r_0' = Y \oplus r_2$

$r_1' = r_0 \oplus r_2$

$r_2' = r_1$

} eqn of calc. syndrome [5]

$S = [r_2' \quad r_1' \quad r_0']$

no of shift = no of values in received cw.

∴ No of shift	Y	r_0'	r_1'	r_2'
		0	0	0 — initial state
1	1	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	0	1	0
5	1	1	0	1
6	0	1	0	0
7	1	1	1	0
		r_0	r_1	r_2

$S = [r_2 \; r_1 \; r_0] \equiv [0 \quad 1 \quad 1]$ //

$g(x) = x^{n-k} + \sum_{i=1}^{n-k-1} g_i x^i + 1$

Page No.
Date

8) (7,4) cyclic code $g(x) = 1 + x^2 + x^3$.

a) block diagram of cyclic encoder. m = 0110

b) block diagram of syndrome calc R = 1001011.

⇒ a) $g(x) = 1 + x^2 + x^3$.

$g(x) = x^{n-k} + \sum_{i=1}^{n-k-1} g_i x^i + 1$

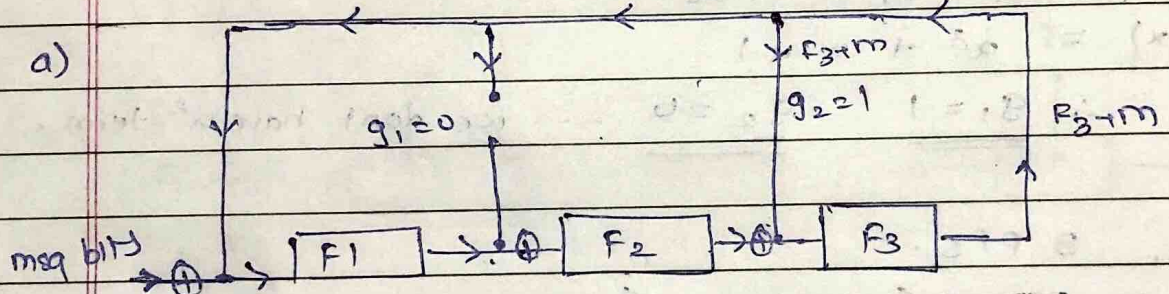
n-k = no. of FF

7-4 = 3

$= x^3 + g_1 x^1 + g_2 x^2$

$= g_1 = 0 \quad g_2 = 1$

a)



I/P (m)	before shift P_1	P_2	P_3	after shift $P_1' = P_3 + m$	$P_2' = P_1$	$P_3' = P_2 + P_3 + m$
0	0	0	0	0	0	0
1	0	0	0	1	0	1
1	1	0	1	0	1	0
0	0	1	0	0	0	1

↑ MSB LSB.

Parity = 001

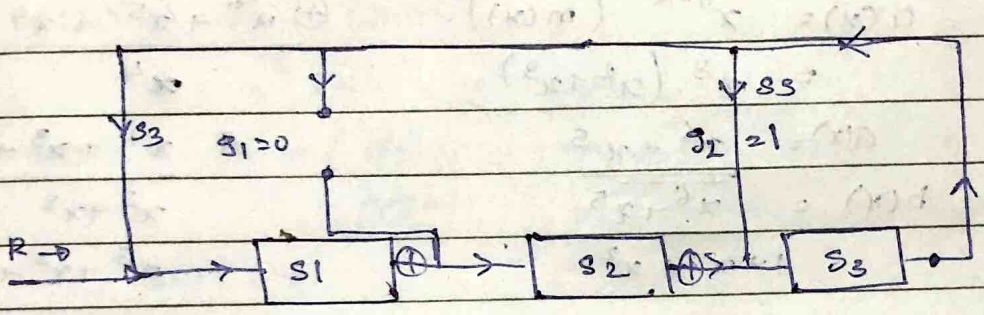
cw = 0110 001

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

$= x^{n-k} + \sum_{i=1}^{n-k-1} g_i x^i + 1$

$= x^3 + g_1 x^1 + g_2 x^2 + 1$

$g_1 = 0 \qquad g_2 = 1$



value	R	$S_1 = R + S_3$	$S_2 = S_1$	$S_3 = S_2 \oplus S_3$
		0	0	0
1	1	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	0	0	1
5	0	1	0	1
6	1	0	1	1
7	1	0	0	0

↑ MSB ↑ LSB.

$S[S_3 \; S_2 \; S_1] = 0\,0\,0$

encoding = $a(x) = x^{n-k}\, m(x)$

$b(x) = \text{rem}\left[a(x)/g(x)\right]$

$c(x) = a(x) + b(x)$

$s(x) = \text{rem}\left[R(x)/g(x)\right]$ decoding.

Page No. Date

Encoding of msg

Q] consider (7, 4) cyclic code, $g(x) = 1 + x + x^2$, m = 0011.

⇒ $g(x) = 1 + x^1 + x^2$

m = 0 0 1 1

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

encoding = $a(x) = x^{n-k}\,(m(x))$

$= x^3\,(x^2 + x^3)$

$a(x) = x^6 + x^5$

$b(x) = \dfrac{x^6 + x^5}{1 + x + x^2}$

$x^4 + x^2 + x$

$1 + x + x^2 \;\big|\; x^6 + x^5$

$\oplus\; x^6 + x^5 + x^4$

x^4

$\oplus\; x^4 + x^3 + x^2$

$x^3 + x^2$

$x^3 + x^2 + x$

x

$b(x) = x$

$c(x) = a(x) + b(x)$.

$c(x) = x^6 + x^5 + x$

$c(x) = x + x^5 + x^6$

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

decoding ⇒ syndrome decoding.

$s(x) = \text{rem}\left(\dfrac{R(x)}{g(x)}\right)$, $R = 0\,1\,0\,0\,0\,1\,1$

$R(x) = x^1 + x^5 + x^6$

$x^4 + x^2 + x$

$x^2 + x + 1 \;\big|\; x^6 + x^5 + x$

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

$x^4 + x$

$x^4 + x^3 + x^2$

$x^3 + x^2 + x$

$x^3 + x^2 + x$

rem = 0 ∴ no error

$$S(x) = \text{rem}\left[\frac{\text{error poly}}{g(x)}\right]$$

Page No. Date

* error detection & correction.

Q] $(7,4)$, $g(x) = 1+x+x^2$, $m = 0100$, $R = 0110011$.

→ • $g(x) = 1+x+x^2$

$m = 0\ 1\ 0\ 0$ (x^0 … x^3)

$m(x) = x$

$a(x) = x^{n-k}\,(m(x))$

$= x^3(x) = x^4 = a(x)$

$b(x) = \text{rem}\left(\frac{a(x)}{g(x)}\right) = \text{rem}\left(\frac{x^4}{1+x+x^2}\right)$

x^2+x | x^2+x+1 | x^4

$x^4+x^3+x^2$

x^3+x^2

x^3+x^2+x

x

$b(x) = x$

$c(x) = a(x) + b(x) = x^4+x$.

$c = 0100100$

$c = x+x^4$.

x^4+x^2+x+1 | x^2+x+1 | $x^6+x^5+x^2+x$

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

x^4+x^2+x

$x^4+x^3+x^2$

x^3+x

x^3+x^2+x

x^2+x

x^2+x+1

rem $x+1$

$R = 0110011$ $\quad R(x) = x+x^2+x^5+x^6$

$\therefore S(x) = \text{rem}\left(R(x)/g(x)\right)$

$= \text{rem} = x+1$

∴ some error is there in received $R = 0110011$

using error pattern table.

error pattern.	error poly	syndrome poly.
0 0 0 0 0 0 1	x^6	1
0 0 0 0 0 1 0	x^5	$x+1$
0 0 0 0 1 0 0	x^4	x
0 0 0 1 0 0 0	x^3	1
0 0 1 0 0 0 0	x^2	$x+1$
0 1 0 0 0 0 0	x	x
1 0 0 0 0 0 0	$1 = x^0$	1

error poly = syndrome poly

$C(x) = P(x) + e(x) = S(x) = rem\left(\frac{R(x)}{g(x)}\right)$

Page No.
Date

$$x^2+x+1 \;\big|\; x^6+x^5+x^4+x^3+x+1$$

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

x^5+x^4

$x^5+x^4+x^3$

x^3

$+\ x^3+x^2+x$

x^2+x

x^2+x+1

1

same for $x^5 \ldots x$.

$\therefore rem = 1$.

~~now chose biggest terms i.e. $x+1$~~

now check if any term = ans to the syndrom = $x+1$.

$\therefore x^5 \;\&\; x^2$, we get 2 terms with $x+1$

$\therefore$ which to select

$g(x) < n-k = g(x) \Rightarrow x^2$

$\therefore$ we can only detect error & cannot correct.

If degree of $g(x) < n-k$.

we can only detect & cannot correct

Syndrome $S(x) = \text{rem}\left(e(x)/g(x)\right)$ $C = R + e$ e=error vector

$S(x) = \text{rem}\left(\frac{C(x) \oplus e(x)}{g(x)}\right)$ $S(x) = 0$ no error

error table ⇒ error vector & e(x) & S(x)

q] calc. correct codeword for (7,4) $g(x) = x^3 + x^2 + 1$

$R = 1010011$.

$= S(x) = \text{rem}\left(\frac{R(x)}{g(x)}\right) = \text{rem}\left(\frac{x^6 + x^4 + x + 01}{x^3 + x^2 + 1}\right) = x$

error is present.

error vector	error poly	S(x)	S
1 0 0 0 0 0 0	x^6	$x^2 + x$	1100
0 1 0 0 0 0 0	x^5	$x + 1$	011
0 0 1 0 0 0 0	x^4	$x^2 + x + 1$	111
0 0 0 1 0 0 0	x^3	$x^2 + 1$	101
0 0 0 0 1 0 0	x^2	x^2	100
0 0 0 0 0 1 0	x^1	x	010
0 0 0 0 0 0 1	x^0	1	001

$x^3 + x^2$

$x^3 + x^2 + 1 \;|\; x^6 + x^5 + x + 1$

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

$x^5 + x^4 + x^3 + x + 1$

$x^3 + x^2 + x + 1$

x rem

$= e(x)$.

$S(x) = \left(\frac{e}{R(x)/g(x)}\right)$ rem

$x^3 + x^2 + 1 \;|\; x^6$

$x^3 + x^2 + x$

$x^6 + x^5 + x^3$

$x^5 + x^3$

$x^5 + x^4 + x^2$

$x^4 + x^3 + x^2$

$x^4 + x^3 + x$.

$x^2 + x$.

do the same for $x^5 - x^0$

$\therefore C(x) = R(x) + e(x)$

$R(x) = x^6 + x^4 + x + 01$ $e(x) = x$

$C(x) = x^6 + x^4 + x + 1 + x$

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

$= 1010001$

$$S(x) = \left(\frac{e(x)}{g(x)} \right) \text{rem}$$

Page No.
Date

Q] $g(x) = x^3 + x + 1$ | $R = 1010010$

$R(x) = x^6 + x^4 + x$

$S(x) = (R(x) / g(x)) \text{ rem}$

$S(x) = 1$

$S = [0\ 0\ 1]$

we know $c(x) = R(x) + e(x)$

$c = R + e$. e = error vector.

e.v.	e(x)	S(x)	S
1 0 0 0 0 0 0	x^6	x^2+1	101
0 1 0 0 0 0 0	x^5	x^2+x+1	111
0 0 1 0 0 0 0	x^4	x^2+x	110
0 0 0 1 0 0 0	x^3	$x+1$	011
0 0 0 0 1 0 0	x^2	x^2	100
0 0 0 0 0 1 0	x^1	x	010
0 0 0 0 0 0 1	1	1	001

matches our syndrom

$S(x) = \text{rem} \left(\frac{e(x)}{g(x)} \right)$

$e = 0000001$

$e(x) = 1 = c$.

$c = R + e$

$= 1010010 + 0000001$

$= 1010011$

Page No.
Date

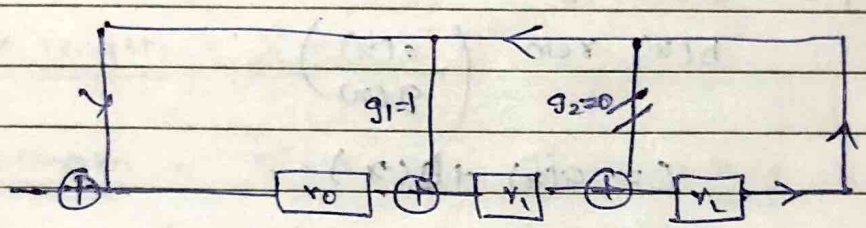
Q) (7,4) cyclic code.

$g(x) = x^3 + x + 1$ R = 1110011

$$g(x) = x^{n-k} + \sum_{i=1}^{n-k-1} x^i \cdot g_i + 1$$

$= x^3 + x^2 g_2 + x^1 g_1 + 1$

$g_1 = 1 \quad g_2 = 0$



$r_0 = R \oplus r_2$

$r_1 = r_2 \oplus r_0$

$r_2 = r_1$

no of shift	R	r_0	r_1	r_2
		0	0	0
1	1	1	0	0
2	1	1	1	0
3	1	1	1	1
4	0	1	0	1
5	0	1	0	0
6	1	1	1	0
7	1	1	1	1

$S[r_2\ r_1\ r_0] = 1\ 1\ 1$

$S(x) = x^2 + x + 1$ $\quad e(x) = R(x) + c(x)$

Syndrome table.

	e(x)	s(x) = rem[e(x)/g(x)]	
1 0 0 0 0 0 0	x^6	x^2+1	1 0 1
0 1 0 0 0 0 0	x^5	x^2+x+1	1 1 1
0 0 1 0 0 0 0	x^4	x^2+x	1 1 0
0 0 0 1 0 0 0	x^3	$x+1$	0 1 1
0 0 0 0 1 0 0	x^2	x^2	1 0 0
0 0 0 0 0 1 0	x^1	x	0 1 0
0 0 0 0 0 0 1	x^0	1	0 0 1

$C = R + e = 1110011 + 0100000$

$= 1010011$

Page No.
Date

* $C = R + e$

$c(x) = A(x) + e(x)$

$S(x) = \text{rem}\left(\frac{e(x)}{g(x)}\right) = \text{rem}\left(\frac{\text{error poly}}{g(x)}\right)$

$g(x) = x^{n-k} + \sum_{i=1}^{n-k-1} x^i g_i + 1$

* encoding = $a(x) = x^{n-k}\ m(x)$

$b(x) \text{ rem}\left(\frac{a(x)}{g(x)}\right)$

$C = a(x) + b(x)$

* no. of ff = $n-k$.

* Syndrom table | error table

= error vector | $e(x)$ | $S(x) = (e(x)/g(x))$ rem.

* shift | FR table.

no. of shifts: R r_0 r_1 r_2.

* $S(x) = \left(\frac{\text{received (poly)}(x)}{g(x)}\right) \text{rem}$

⇒ $1 + x^2 + x^3$ ⇒ $x^3 + x^2 + 1$

x^0 x^1 x^2 → $x \to 1$

(min distance = hamming bound)
⇓
wt .

Page No.
Date

Hamming codes → type of block code.

⇒ hamming codes are linear b.c. used for error correctn.
⇒ can detect upto 2 bits error & correct upto 1 bit error

* min distance = min no. of parity bits (= 3 = r)

* block length = $2^r - 1 = 2^3 - 1 = 7$. [c.w. length] (n)

* msg length = $2^r - r - 1 = 2^3 - 3 - 1 = 4$ (K)

d = min dist

$(n, K) \equiv (7, 4)$ $(n, K, d) \equiv (7, 4, 3)$

* Hamming bound = non zero elements in code. (minimum)

eg: (1011, 1101, 1111) = non zero element = (3, 3, 4)
= Hamming bound = 3

∴ (min distance = Hamming bound)

how to generate parity bits of hamming code.

$i = \{i_1, i_2, i_3, i_4\}$, $K = 4$

(7,4) $K = 4$, $n = 7$.

codeword
$= \{i_1, i_2, i_3, i_4, P_1, P_2, P_3\}$.
= block length
= msg length.

$P_1 = i_1 + i_2 + i_3$

$P_2 = i_2 + i_3 + i_4$

$P_3 = i_1 + i_2 + i_4$

eg: $\{0, 1, 1, 0\}$ $\{i_1, i_2, i_3, i_4\}$

$P_1 = i_1 + i_2 + i_3 = 0 + 1 + 1 = 0$

$P_2 = i_2 + i_3 + i_4 = 1 + 1 + 0 = 0$

$P_3 = i_1 + i_2 + i_4 = 0 + 1 + 0 = 1$

Syndrome

$P_1 = D_3 \oplus D_5 \oplus D_7 = 1$

$P_2 = D_3 \oplus D_6 \oplus D_7 = 1$

$P_3 = D_5 + D_6 + D_7 = 0$

P_7	D_6	D_5	P_4	D_3	P_2	P_1
0	1	1	0	0	1	1

Error correction

Error syndrome

code word = {0 1 1 1 0 0 0 1}

error syndrome table

Error vector	s_1	s_2	s_3	
0 0 0 0 0 0 0	0	0	0	0
0 0 0 0 0 0 1	0	0	1	1
0 0 0 0 0 1 0	0	1	0	2
0 0 0 0 1 0 0	1	0	0	4
0 0 0 1 0 0 0	0	1	1	3
0 0 1 0 0 0 0	1	1	0	6
0 1 0 0 0 0 0	1	1	1	7
1 0 0 0 0 0 0	1	0	1	5

received code = $V = (V_1, V_2, V_3, V_4, V_5, V_6, V_7)$

$S_1 = V_1 + V_2 + V_3 + V_5$

$S_2 = V_2 + V_3 + V_4 + V_6$

$S_3 = V_1 + V_2 + V_4 + V_7$

we got error syndrome value as (0 0 1) = parity

S_1	S_2	S_3
0	0	1

at pos: 1

with error pattern 0000001

$\therefore C = R + e$

$= 0\,1\,1\,1\,0\,0\,0\,1 + 0\,0\,0\,0\,0\,0\,0\,1$

$C = 0\,1\,1\,1\,0\,0\,0\,0$

0 0 0	no error
0 0 1	P_0
0 1 0	P_1
0 1 1	D_1
1 0 0	P_2
1 0 1	D_0
1 1 0	P_2
1 1 1	D_3