RSET
RAJAGIRI SCHOOL OF ENGINEERING & TECHNOLOGY

INFORMATION THEORY & CODING

MODULE III

LINEAR BLOCK CODES – ERROR CONTROL CODING

Anila Kuriakose,
Assistant Professor, Department of ECE, RSET

Contents

- Introduction to Algebraic structures : Rings, Groups, Fields, and Galois fields.
- Codes for error detection and correction – parity check coding
- Linear block codes
  - Error detecting and correcting capabilities
  - Generator and Parity Check matrices
  - Standard Array and Syndrome Decoding

Modular arithmetic

- Any integer 'a' divided by a positive integer 'n' gives quotient 'q' and remainder 'r'.
- $a = qn + r$
- r is also called the residue and is given by $r = a \ mod \ n$
- n is called the modulus.
- Eg: $11 \ mod \ 7 = 4$
- $-11 \ mod \ 7 = 3$
- 2 integers are said to be "congruent modulo n" if $\boldsymbol{a \ mod \ n = b \ mod \ n}$
- Denoted by $\boldsymbol{a \equiv b \ (mod \ n)}$
- Eg: $73 \equiv 4 \ (mod \ 23) \rightarrow 73 \bmod 23 = 4 \ mod \ 23 = 4$

  $21 \equiv -9 \ (mod \ 10) \rightarrow 21 \bmod 10 = -9 \ mod \ 10 = 1$

Algebraic Structures

1. Groups
2. Rings
3. Fields

Algebraic Structures

1. Group

A set G on which a binary operation • is defined is called a group if the following conditions are satisfied:

(i) **Closure property** : If a and b are elements of G then $c = a \bullet b$ is also an element of G

(ii) **Associativity Property**: If a, b and c are elements of G , then $(a \bullet b) \bullet c = a \bullet (b \bullet c)$

(iii) **Existence of identity element**: For all a in G, there exists an element e in G , called identity element such that $a \bullet e = e \bullet a = a$

(iv) **Existence of inverse**: For each a in G, there exists an element a' in G, called the inverse of a such that $a \bullet a' = a' \bullet a = e$

- **Commutative group (Abelian group)**: Group which satisfies the four properties along with the commutative property

  Commutativity: For all a and b in G, $a \bullet b = b \bullet a$

  Q) Is the set of integers with the addition operator , $G = \{Z, +\}$ a commutative group?

- The number of elements in a group is called as the order of the group.
- A group of finite order is called a finite group.

Q. Perform modular addition and modular multiplication on the set Z_6={0,1,2,3,4,5} and Verify the properties for Group separately.

Modulo 6 Addition

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Modulo 6 multiplication

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2. Rings

- A ring R is a set of elements with 2 binary operations given by

  R={(....), •, *}

- The first operation should satisfy all the five properties of a commutative group.

Properties of first operation

(i) **Closure property** : If a and b are elements of R then $c = a \bullet b$ is also an element of R

(ii) **Associativity:** If a, b and c are elements of R , then $(a \bullet b) \bullet c = a \bullet (b \bullet c)$

(iii) **Existence of identity element**: For all a in R, there exists an element e in R , called identity element such that $a \bullet e = e \bullet a = a$

(iv) **Existence of inverse**: For each a in R, there exists an element a' in R, called the inverse of a such that $a \bullet a' = a' \bullet a = e$

(v) **Commutativity**: For all a and b in R, $a \bullet b = b \bullet a$

Properties of second operation

(i) Closure property : If a and b are elements of R then $c = a*b$ is also an element of R

(ii) **Associativity**: If a, b and c are elements of R , then

$(a*b)*c = a*(b*c)$

(iii) **Distributivity**: $a * (b\bullet\ c) = (a * b)\bullet(a * c)$

- **Commutative ring:** Ring in which commutative property is satisfied for the second operation

Commutativity: For all a and b in R, $a * \mathrm{b} = \mathrm{b} * a$

Q) Is the set of integers with addition and multiplication operators ,

R= $\{Z, +, \times\}$ a commutative ring?

3.Fields

- A field is a set of elements with 2 binary operations denoted by F = {(....), •, * }
- It is a commutative ring in which the second operation follows 2 more axioms except that the identity element of the first operation has no inverse in the second operation .

Properties of first operation

1) **Closure property** : If a and b are elements of F then $c = a \bullet b$ is also an element of F
2) **Associativity**: If a, b and c are elements of F , then $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
3) **Existence of identity element:** For all a in F, there exists an element e in F, called identity element such that $a \bullet e = e \bullet a = a$
4) **Existence of inverse:** For each a in F, there exists an element a′, called the inverse of a in F such that $a \bullet a' = a' \bullet a = e$
5) **Commutativity:** For all a and b in F, $a \bullet b = b \bullet a$

Properties of second operation

(i) Closure property : If a and b are elements of F then $c = a*b$ is also an element of F

(ii) **Associativity**: If a, b and c are elements of F , then $(a*b)*c = a*(b*c)$

(iii) **Existence of identity element:** For all a in F, there exists an element e in F , called identity element such that $a * e = e * a = a$

(iv) **Existence of inverse:** For each a in F, there exists an element a' in F called the inverse of a such that $a * a' = a' * a = e$

(v) **Commutativity:** For all a and b in F, $a * b = b * a$

(vi) **Distributivity:** $a * (b \bullet c) = (a * b) \bullet (a * c)$

Q. Perform modular addition and multiplication on the set Z_6={0,1,2,3,4,5} and Z_5={0,1,2,3,4}.Verify the properties for field under addition & multiplication.

Modulo 6 Addition

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Modulo 6 multiplication

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Galois Fields

- Finite field has finite no. of elements.
- For a field to be finite, the no. of elements should be p^n, where p is a prime number and n is a positive integer.
- Finite field with p^n elements, where p is a prime number and n is a positive integer is called a Galois field.
- Denoted by GF(p^n)
- GF(2^n) is commonly used
- When n=1, GF(2^n) = GF(2)
- GF(2) = {0,1}

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

w	$-w$	w^{-1}
0	0	—
1	1	1

Polynomials

- In GF(2^n), there are 2^n elements, hence n bits are required to represent each elements.
- It is easier to work with polynomials of degree (n-1) for n bits.
- $\boldsymbol{f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0x^0}$
- Coefficients of the terms are either 1 or 0

Eg: Polynomial representation of 8 bit word 10011001 : $\boldsymbol{x^7 + x^4 + x^3 + 1}$
8 bit word related to $\boldsymbol{x^5 + x^2 + x}$ is 00100110

Primitive Polynomial

- A polynomial f(x) over a field F is called **irreducible** if and only if f(x) cannot be expressed as a product of two polynomials of degree lower than that of f(x).

Degree	Irreducible Polynomial
1	x+1 , x
2	$x^2 + x + 1$
3	$x^3 + x^2 + 1$, $x^3 + x + 1$
4	$x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$
5	$x^5 + x^4 + x^3 + x + 1$, $x^5 + x^4 + x^2 + x + 1$, $x^5 + x + 1$

List of Primitive Polynomials

m	
3	$1+X+X^3$
4	$1+X+X^4$
5	$1+X^2+X^5$
6	$1+X+X^6$
7	$1+X^3+X^7$
8	$1+X^2+X^3+X^4+X^8$
9	$1+X^4+X^9$
10	$1+X^3+X^{10}$
11	$1+X^2+X^{11}$
12	$1+X+X^4+X^6+X^{12}$
13	$1+X+X^3+X^4+X^{13}$

m	
14	$1+X+X^6+X^{10}+X^{14}$
15	$1+X+X^{15}$
16	$1+X+X^3+X^{12}+X^{16}$
17	$1+X^3+X^{17}$
18	$1+X^7+X^{18}$
19	$1+X+X^2+X^5+X^{19}$
20	$1+X^3+X^{20}$
21	$1+X^2+X^{21}$
22	$1+X+X^{22}$
23	$1+X^5+X^{23}$
24	$1+X+X^2+X^7+X^{24}$

n	irreducible polynomials
1	$1+x, x$
2	$1+x+x^2$
3	$1+x+x^3, 1+x^2+x^3$
4	$1+x+x^4, 1+x+x^2+x^3+x^4, 1+x^3+x^4$
5	$1+x^2+x^5, 1+x+x^2+x^3+x^5, 1+x^3+x^5, 1+x+x^3+x^4+x^5, 1+x^2+x^3+x^4+x^5,$ $1+x+x^2+x^4+x^5$

n	primitive polynomials
1	$1+x$
2	$1+x+x^2$
3	$1+x+x^3, 1+x^2+x^3$
4	$1+x+x^4, 1+x^3+x^4$
5	$1+x^2+x^5, 1+x+x^2+x^3+x^5, 1+x^3+x^5, 1+x+x^3+x^4+x^5, 1+x^2+x^3+x^4+x^5,$ $1+x+x^2+x^4+x^5$

Construction of Galois Field

Q. Construct a Galois field GF(2^3) using the irreducible polynomial $f(x) = x^3 + x + 1$

Soln:

The elements of GF(2^3) are given as {0,1,g, g^2, g^3, ... , g^6}

To find the elements of the relation f(g) = 0 can be used

$$\mathbf{f(g) = g^3 + g + 1 = 0}$$

$$\boldsymbol{g^3 = -g - 1 = g + 1}$$

$$\boldsymbol{g^4 = g(g^3) = g^2 + g}$$

$$\boldsymbol{g^5 = g(g^4) = g^3 + g^2 = g^2 + g + 1}$$

$$\boldsymbol{g^6 = g(g^5) = g^3 + g^2 + g = g + 1 + g^2 + g = g^2 + 1}$$

Elements	Polynomial Representation	n tuple Representation
0	0	000
1	1	001
$\boldsymbol{g}$	$\boldsymbol{g}$	010
$\boldsymbol{g^2}$	$\boldsymbol{g^2}$	100
$\boldsymbol{g^3}$	$\boldsymbol{g+1}$	011
$\boldsymbol{g^4}$	$\boldsymbol{g^2+g}$	110
$\boldsymbol{g^5}$	$\boldsymbol{g^2+g+1}$	111
$\boldsymbol{g^6}$	$\boldsymbol{g^2+1}$	101

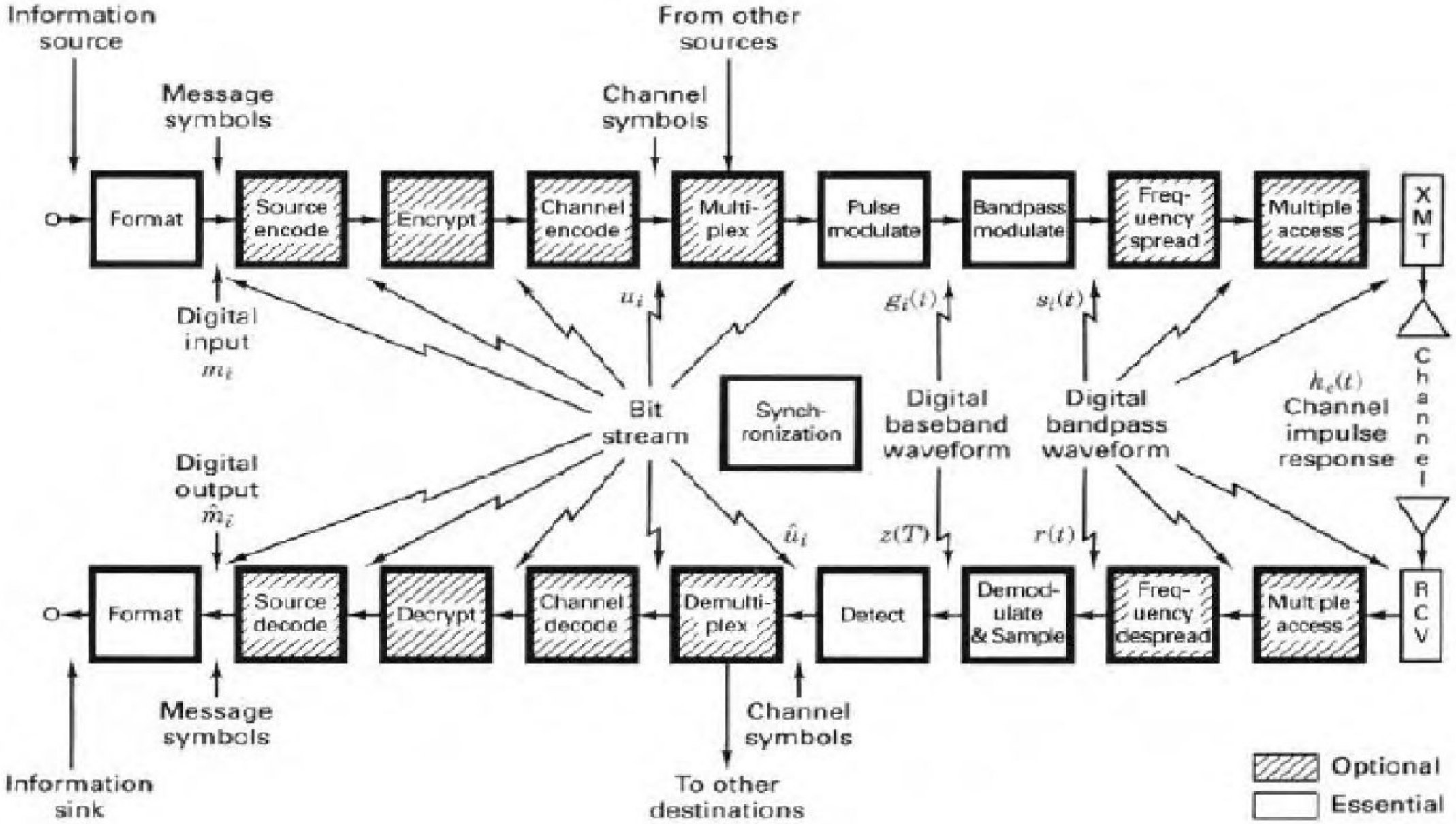
Q. Construct a Galois field GF(2^4) using the irreducible polynomial $f(x) = x^4 + x + 1$

Element	Polynomial	n tuple
0	0	0000
1	1	0001
g	**g**	0010
g^2	g^2	0100
g^3	g^3	1000
g^4	$g + 1$	0011
g^5	$g^2 + g$	0110
g^6	$g^3 + g^2$	1100

Element	Polynomial	n tuple
g^7	$g^3 + g + 1$	1011
g^8	$g^2 + 1$	0101
g^9	$g^3 + g$	1010
g^{10}	$g^2 + g + 1$	0111
g^{11}	$g^3 + g^2 + g$	1110
g^{12}	$g^3 + g^2 + g + 1$	1111
g^{13}	$g^3 + g^2 + 1$	1101
g^{14}	$g^3 + 1$	1001

Error Control Coding

Block Diagram of a Digital Communication System



Error Control Coding

- Redundant bits (bits which carry no information) are used to detect and correct errors.
- channel encoder and decoder are used for error control coding
- Disadvantages are

(i) Increased Bandwidth

(ii) System becomes more complex due to channel encoder & decoder.

Parity Check Codes and Repetition Codes

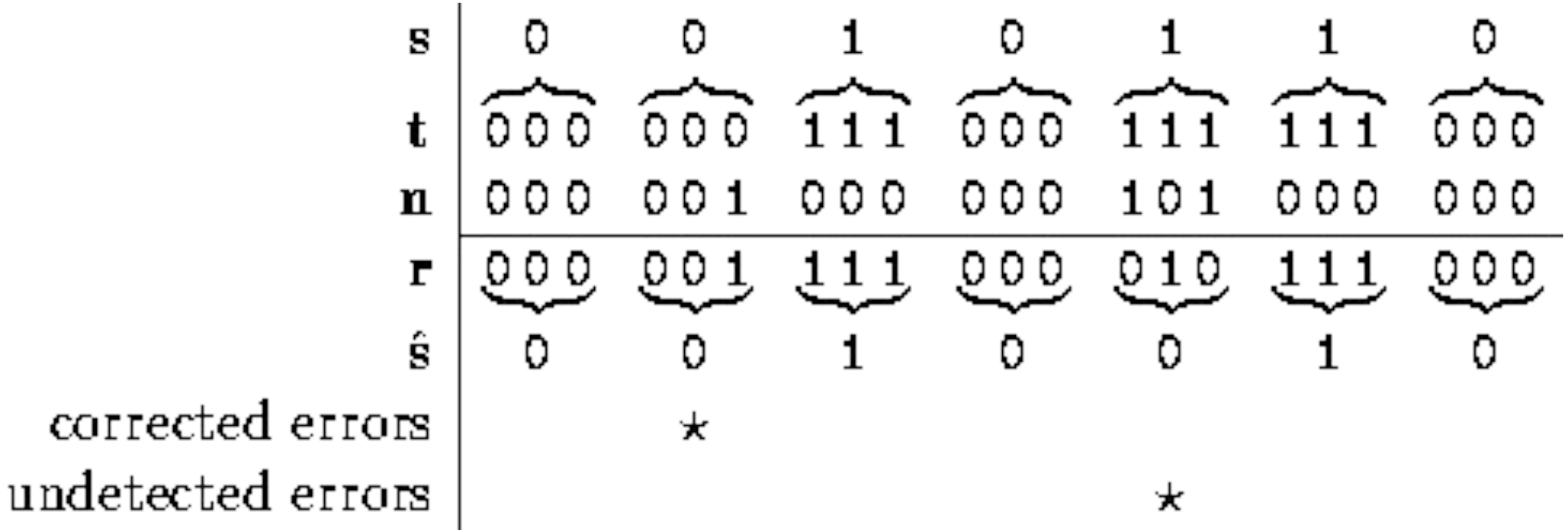
Codes for Error Detection & Correction

Parity Check Codes

- Parity check adds a redundant bit to a bit stream.
- Even parity: A parity bit 1 is added if the data has odd number of 1s. Otherwise bit 0 is added making the total number of 1s in the frame even.
- Odd parity: A parity bit 1 is added if the data has even number of 1s . Otherwise bit 0 is added making the total number of 1s in the frame odd.
- At the receiver, decoding consists of testing the mod 2 sum of the received codeword.(0 for even parity and 1 for odd parity)
- If there are even number of errors, it can not be detected.
- Also it can not detect which bit is in error (the parity bit also can be in error)
- This scheme has one bit error detection capability but no error correction capability.

Repetition codes

- Among the simplest error control codes are ***repetition codes***, where each codeword consists of a single symbol repeated several times.
- Consider a binary repetition code of length 3. The user wants to transmit the information bits **101.** Then the encoding maps each bit either to the all ones or all zeros code word, so we get the **111 000 111**, which will be transmitted.
- Decoding is usually done by a simple majority decision for each code word.
- That lead us to 100 as the decoded information bits, because in the first and second code word occurred less than two errors, so majority of the bits are correct. But in the third code word two bits are corrupted, which results in an erroneous information bit, since two errors lie above the error correcting capacity.


s 0 0 1 0 1 1 0
t 000 000 111 000 111 111 000
n 000 001 000 000 101 000 000
r 000 001 111 000 010 111 000
ŝ 0 0 1 0 0 1 0
corrected errors ⋆
undetected errors ⋆

Linear Block Codes

Linear Block Codes

- k bit messages are encoded into n bits by adding (n-k) number of check bits.
- 2^k messages are possible and hence 2^k codewords are generated.
- n should be greater than k
- Linear block codes are also called as (n, k) block code.
- (n,k) block code is said to be (n,k) linear block code if the modulo 2 addition of any 2 code words will produce another code word in the (n,k) block code.
- (n,k) block code is said to be systematic if k message bits appear either at the beginning or at the end of the code word.

Matrix Description of linear block codes

- Let the k bit message be represented as a row matrix

$$\boldsymbol{U = [u_1 \ u_2 \ldots\ldots u_k]_{1\times k}}$$

- The encoder adds (n-k) check bits to form (n,k) block code
- The code vector is

$$\boldsymbol{V = [v_1 \ v_2 \ldots\ldots v_n]_{1\times n}}$$

- The k message bits are placed at the beginning of the block code

$\therefore \boldsymbol{v_i = u_i}$ for all i=1,2,…k.

$$\therefore \boldsymbol{V = [\underbrace{v_1 \ v_2 \ldots\ldots v_k}_{\text{k message bits}} \ \underbrace{v_{k+1} \ v_{k+2} \ldots\ldots v_n}_{\text{(n-k) check bits}}]}$$

- The code vector $[V]_{1\times n} = [U]_{1\times k} \times [G]_{k\times n}$

  [G] is called the generator matrix of size (k× n)

- $[G] = [I_k \mid P]_{k\times n}$

  k linearly independent code vectors constitute G

$$[G] = \left[\begin{array}{ccccc|ccc} 1 & 0 & 0 & \dots & 0 & p_{11} & \dots & p_{1(n-k)} \\ 0 & 1 & 0 & \dots & 0 & p_{21} & \dots & p_{2(n-k)} \\ 0 & 0 & 1 & \dots & 0 & p_{31} & \dots & p_{3(n-k)} \\ . & . & & & & . & & \\ . & . & & & & . & & \\ 0 & 0 & 0 & \dots & 1 & p_{k1} & \dots & p_{k(n-k)} \end{array}\right]$$

Note

If $[G] = [P \mid I_k]_{k\times n}$ is used, then the message bits will be placed after the check bits in [C]

- I_k is the identity matrix of order k
- $[P]$ is the parity matrix of order k×(n-k)

$$[v_1, v_2, \ldots\ldots, v_n] = [u_1, u_2, \ldots\ldots, u_k] \times \begin{bmatrix} 1 & 0 & 0 \ldots\ldots 0 & p_{11} & p_{12} & \ldots\ldots & p_{1(n-k)} \\ 0 & 1 & 0 \ldots\ldots 0 & p_{21} & p_{22} & \ldots\ldots & p_{2(n-k)} \\ 0 & 0 & 1 \ldots\ldots 0 & p_{31} & p_{32} & \ldots\ldots & p_{3(n-k)} \\ . & . & & & . & & \\ . & . & & & . & & \\ 0 & 0 & 0 \ldots\ldots 1 & p_{k1} & p_{k2} & \ldots\ldots & p_{k(n-k)} \end{bmatrix}$$

$$v_1 = u_1$$

$$v_2 = u_2$$

$$v_k = u_k$$

$$v_{k+1} = u_1 p_{11} + u_2 p_{21} + \cdots\cdots + u_k p_{k1}$$

$$v_n = u_1 p_{1(n-k)} + u_2 p_{2(n-k)} + \cdots\cdots + u_k p_{k(n-k)}$$

- I_k retains the message bits (u_k)
- P adds redundant bits

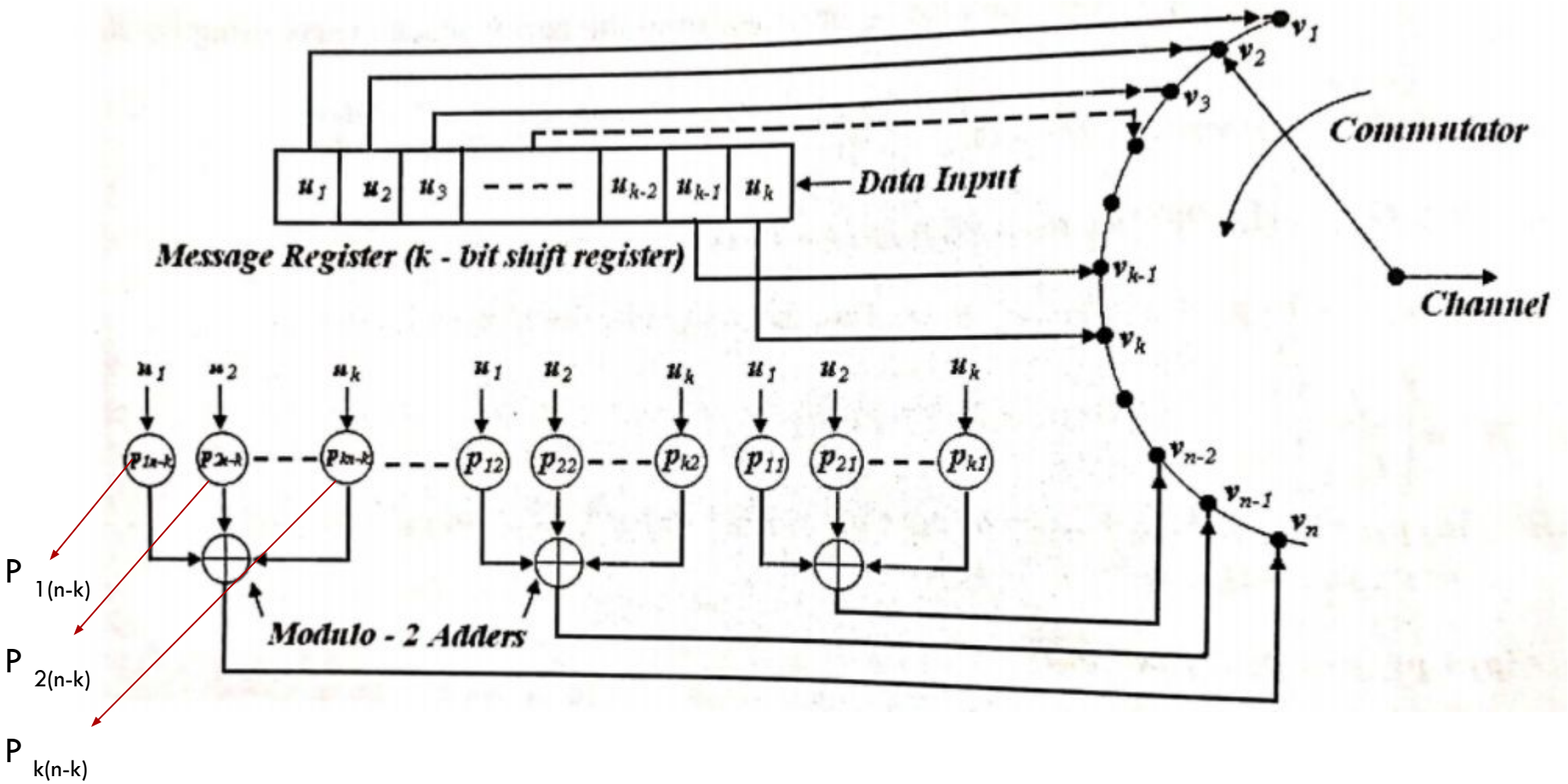
- If $G=\begin{bmatrix}1&0&0&0&1&1\\0&1&0&1&0&1\\0&0&1&1&1&0\end{bmatrix}$ find the codeword corresponding to U=[0 1 1]

- For every generator matrix $[G]_{k\times n}$ there exists $[H]_{(n-k)\times n}$ with n-k linearly independent rows such that all rows of G are orthogonal to all rows of H.
- H → Parity check matrix
- So V is a codeword generated by G if and only if $V.H^T=0$.
- $[\boldsymbol{H}] = [\boldsymbol{P^T} \mid \boldsymbol{I_{(n-k)}}]_{(n-k)\times n}$

- If G= $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$ find H and codeword corresponding to U=[0 1 1]

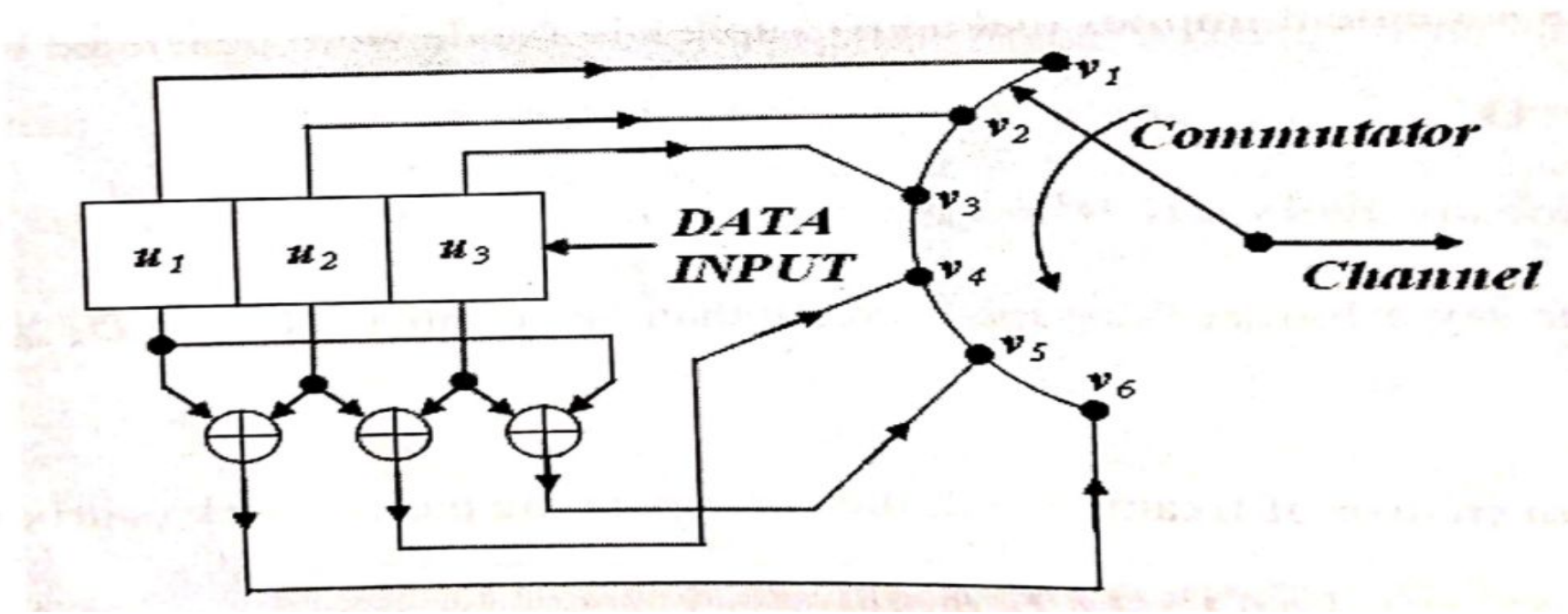
H= $\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ V=U.G=[0 1 1 0 1 1]

Encoding Circuit for (n,k) linear block codes



- P_{ij} = 1 or 0 , P_{ij} indicates a connection if P_{ij} is 1, else no connection.
- The message $\boldsymbol{U = [u_1\ u_2 \ldots\ldots\ldots u_k]}$ to be encoded is shifted into the message register and also into the channel via the commutator.
- Once the entire message enters into the register parity check digits are formed at the output of mod-2 adders and shifted into the channel.

- Draw the encoding circuit for the previous problem.



$$v_1 = u_1$$

$$v_2 = u_2$$

$$v_3 = u_3$$

$$v_4 = u_2 + u_3$$

$$v_5 = u_1 + u_3$$

$$v_6 = u_1 + u_2$$

Q. For a systematic (6,3) linear block code, find all possible codewords

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

Soln:

Codeword length n=6 , Message length k=3 , No. of check bits (n-k)=3

Since k=3, $\boldsymbol{2^k = 2^3 = 8}$ possible messages given by

(000), (001), (010), (011), (100), (101), (110), (111)

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

$$[V] = [U] \times [G]$$

$$[G] = \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}_{I_3} \underbrace{\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}}_{P_{3\times 3}}$$

$$[V] = [u_1 \quad u_2 \quad u_3] \times \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$[V] = [u_1 \quad u_2 \quad u_3 \quad (u_1+u_3) \quad (u_2+u_3) \quad (u_1+u_2)]$$

If [U]= (011), [V]=[011101]

(6,3) linear block code	Message vector	Code vector
	000	000000
	001	001110
	010	010011
	011	011101
	100	100101
	101	101011
	110	110110
	111	111000

Syndrome and Error Detection

- Let $\boldsymbol{V} = [\boldsymbol{v_1}\ \boldsymbol{v_2}. \ldots \ldots \boldsymbol{v_n}]$ be a codeword transmitted over a noisy channel.
- $\boldsymbol{R} = [\boldsymbol{r_1}\ \boldsymbol{r_2}. \ldots \ldots \boldsymbol{r_n}]$ be the received codeword.
- The error vector $\boldsymbol{E}$ is defined as $\boldsymbol{R} = \boldsymbol{V} + \boldsymbol{E}$ where
- $\boldsymbol{E} = \boldsymbol{R} - \boldsymbol{V} = \boldsymbol{R} + \boldsymbol{V} = [\boldsymbol{e_1}\ \boldsymbol{e_2}. \ldots \ldots \boldsymbol{e_n}]$
- $\boldsymbol{e_i} = 1$ if $\boldsymbol{r_i} \neq \boldsymbol{v_i}$ and $\boldsymbol{e_i} = 0$ if $\boldsymbol{r_i} = \boldsymbol{v_i}$

eg.

V=1 0 0 0 0 1

R=1 0 0 0 1 1

E=0 0 0 0 1 0

- The receiver does not know $\boldsymbol{V}$ or $\boldsymbol{E}$.
- When $\boldsymbol{R}$ is received the decoder computes the syndrome

$$\boldsymbol{S} = \boldsymbol{R}.\boldsymbol{H}^{\boldsymbol{T}} = [\boldsymbol{s_1}\ \boldsymbol{s_2}. \ldots \ldots \boldsymbol{s_{n-k}}]_{1\times(n-k)}$$

$\boldsymbol{S} = 0$ if $\boldsymbol{R}$ is a codeword and $\boldsymbol{S} \neq 0$ if $\boldsymbol{R}$ is not a codeword .

- If $\boldsymbol{E}$ is a nonzero codeword then $\boldsymbol{R} = \boldsymbol{V} + \boldsymbol{E}$ is a sum of 2 codewords and will be a codeword due to linearity property and the error is undetectable.

- This type of error patterns are called as undetectable error patterns.
- There are 2^k-1 nonzero codewords and hence 2^k-1 such error patterns.
- When such error pattern occurs, decoder makes an error at the receiver.
- $\boldsymbol{S} = \boldsymbol{R}.\boldsymbol{H}^{\boldsymbol{T}} = [\boldsymbol{s_1}\ \boldsymbol{s_2}.\ldots\ldots..\ \boldsymbol{s_{n-k}}]$

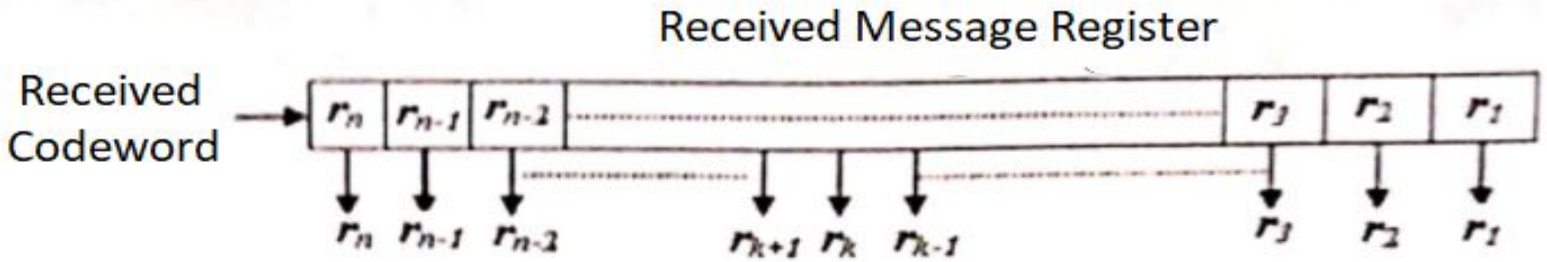
$$= [\boldsymbol{r_1}\ \boldsymbol{r_2}\ldots\ldots\boldsymbol{r_n}] \times \begin{bmatrix} \boldsymbol{p_{11}} & \boldsymbol{p_{12}} & \cdots\cdots & \boldsymbol{p_{1(n-k)}} \\ \boldsymbol{p_{21}} & \boldsymbol{p_{22}} & \cdots\cdots & \boldsymbol{p_{2(n-k)}} \\ & & \ldots\ldots.. & \\ \boldsymbol{p_{k1}} & \boldsymbol{p_{k2}} & \cdots\cdots & \boldsymbol{p_{k(n-k)}} \\ \boldsymbol{1} & \boldsymbol{0} & .. & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{1} & .. & \boldsymbol{0} \\ & & \ldots\ldots. & \\ \boldsymbol{0} & \boldsymbol{0} & .. & \boldsymbol{1} \end{bmatrix}$$

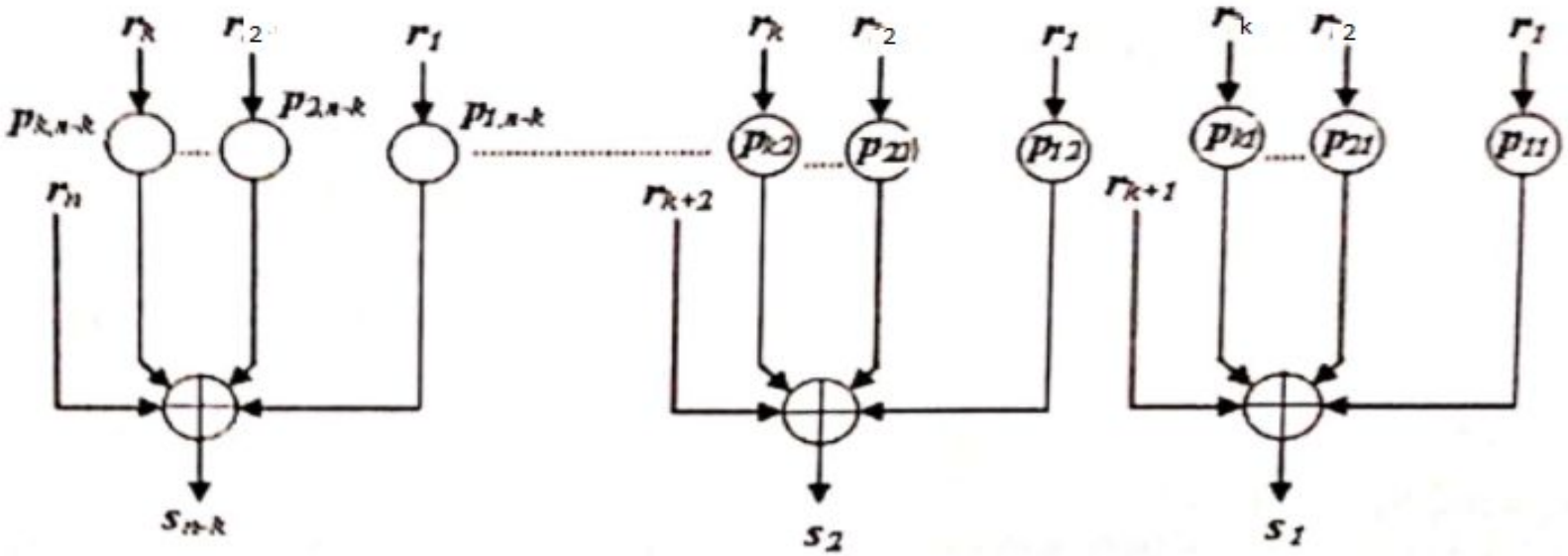
$$S_1 = r_1p_{11} + r_2p_{21} + \ldots + r_kp_{k1} + r_{k+1}$$

$$S_2 = r_1p_{12} + r_2p_{22} + \ldots + r_kp_{k2} + r_{k+2}$$

.....

$S_1 = r_n \quad + r_n \quad + \quad + r_n \quad + r$



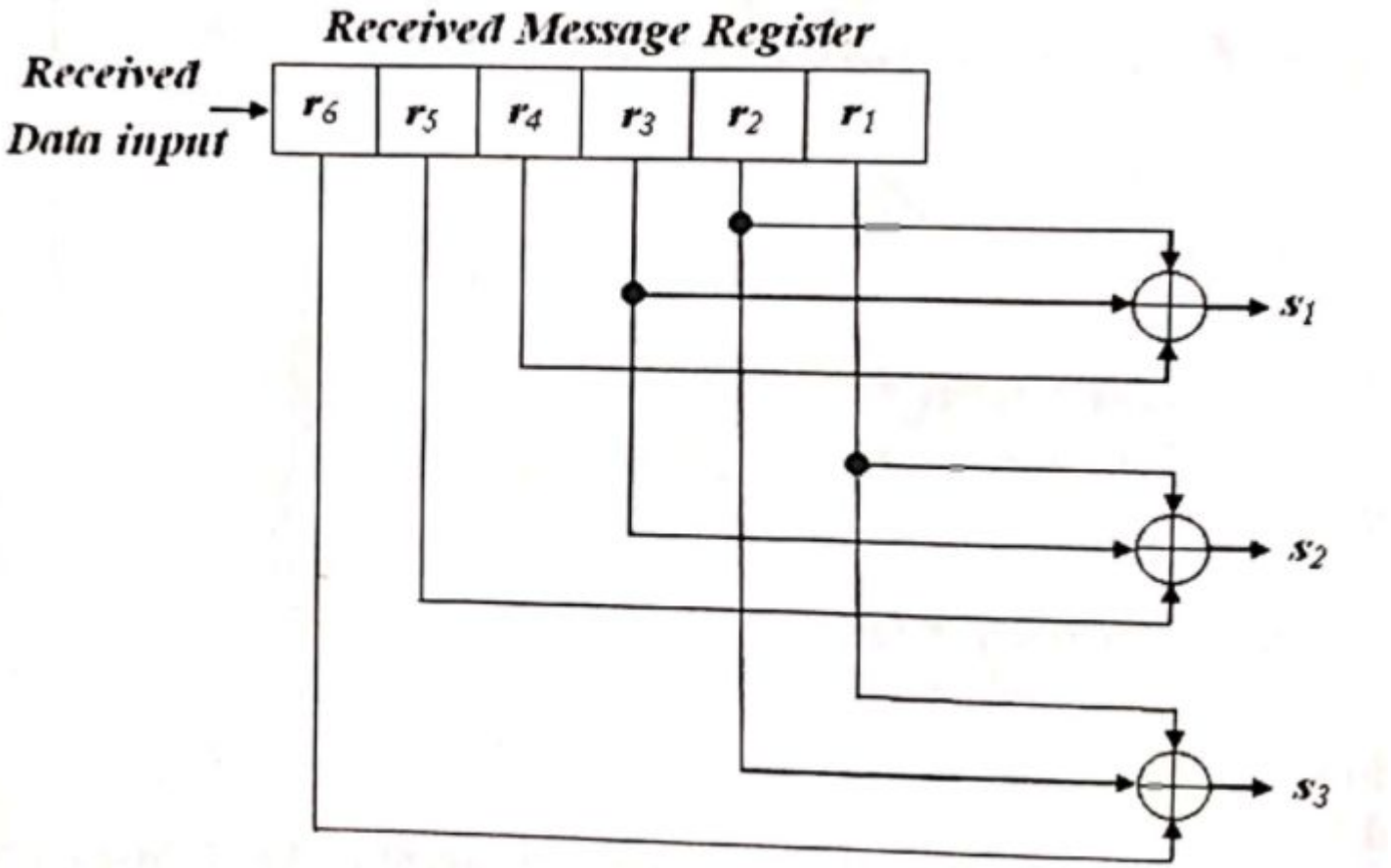


Q) Draw the circuit and compute syndrome for (6,3) code

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

$$s = (s_1, s_2, s_3) = (r_1, r_2, r_3, r_4, r_5, r_6) \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$s_1 = r_2 + r_3 + r_4$$
$$s_2 = r_1 + r_3 + r_5$$
$$s_3 = r_1 + r_2 + r_6$$


Received Message Register
Received
Data input
r_6
r_5
r_4
r_3
r_2
r_1
s_1
s_2
s_3

- $\boldsymbol{S = R.H^T = (V + E).H^T = V.H^T + E.H^T}$
- $\boldsymbol{S = E.H^T}$

- Syndrome depends only on error pattern

$S_1=e_1P_{11}+ e_2P_{21}+\ldots. +e_kP_{k1}+ e_{k+1}$

$S_2=e_1P_{12}+ e_2P_{22}+\ldots. +e_kP_{k2}+ e_{k+2}$

.....

$S_{n-k}=e_1P_{1(n-k)}+ e_2P_{2(n-k)}+\ldots. +e_kP_{k(n-k)}+ e_n$

- To recover the original codeword V=R+E

Minimum Distance

- Let $\alpha = (\alpha_1, \alpha_2 \ldots \alpha_n)$, $\beta = (\beta_1, \beta_2 \ldots \beta_n)$ be two code words.
- The **Hamming distance d(α,β)** between α and β is defined as the number of positions in which they differ.
- Alternatively, using Modulo-2 arithmetic

$$d(\alpha,\beta) \triangleq \sum_{j=1}^{n} (\alpha_j \oplus \beta_j)$$

- The **Hamming Weight ω(α)** of a code vector α is defined as the number of nonzero elements in the code vector.
- Hamming weight of a code vector is the distance between the code vector and the 'all zero code vector'.

E.g. α = (0 1 1 1 0 1), β = (1 0 1 0 1 1). Find their hamming weights and their hamming distance.

$$d(\alpha,\beta) = (0 \oplus 1) + (1 \oplus 0) + (1 \oplus 1) + (1 \oplus 0) + (0 \oplus 1) + (1 \oplus 1) = 4$$

- The Minimum distance of a linear block code is the smallest Hamming distance between any pair of code words in the code.

- The minimum distance of a linear block code is the smallest Hamming weight of the nonzero code vectors in the code because sum (difference) of 2 codewords is also a codeword.

- The Hamming distance is a metric function that satisfies the triangular inequality.
- Let α, β and δ be three code vectors of a linear block code.
- Then $d(\alpha,\beta) + d(\beta,\delta) \geq d(\alpha,\delta)$

$d(\alpha,\beta) = \omega(\alpha \oplus \beta)$

For a linear code V, $d_{min} = \text{Min}\ \{d(\alpha,\beta):\ \alpha,\beta \in V, \alpha \neq \beta\}$

$= \text{Min}\ \{\omega(\alpha \oplus \beta): \alpha,\beta \in V, \alpha \neq \beta\}$

$= \text{Min}\ \{\omega(u),\ u \in V, u \neq 0\} = \omega_{min}$

- ω_{min} is called the minimum weight of the linear code V.

- The minimum distance of a code d_{min} is related to the parity check matrix H.
- Suppose v is a code word.

$$0 = v.H^T$$

$$= v_1h_1 \oplus v_2h_2 \oplus \ldots \oplus v_nh_n$$

- Here $h_1, h_2 \ldots h_n$ represent the columns of the H matrix.
- If v is a code vector of Hamming weight *l*, then there exist *l* columns of H such that the vector sum of these columns is equal to the zero vector.
- If there are *l* columns of H matrix whose vector sum is the zero vector then there exists a code vector of Hamming weight *l*.

i) If no (d-1) or fewer columns of H add to 0, the code has a minimum weight of at least d.

ii) The minimum weight of a linear block code C, is the smallest number of columns of H that sum to 0.

Let C be an (n,k) linear block code with parity check matrix **H**. For each code word of Hamming weight l, there exists l columns of **H** such that the vector sum of these l columns is equal to the zero vector.

PROOF:

$H = [h_0 \quad h_1 \quad . \quad . \quad h_{n-1}]$, h_i is the i^{th} column

Let $v = (v_0 \quad v_1 \quad . \quad . \quad v_{n-1})$ be a codeword of weight l

By Definition:

$$vH^T = 0 \Rightarrow v_0 h_0 + v_1 h_1 + \ldots + v_{n-1} h_{n-1} = 0$$

Assume $v_{i_1}, v_{i_2}, \ldots, v_{i_l}$ are the l nonzero components of v

$$\therefore h_{i_1} + h_{i_2} + \ldots + h_{i_l} = 0$$

- Find minimum distance (weight)

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

- No two or fewer columns sum to zero vector. Hence the minimum weight of the code is 3.

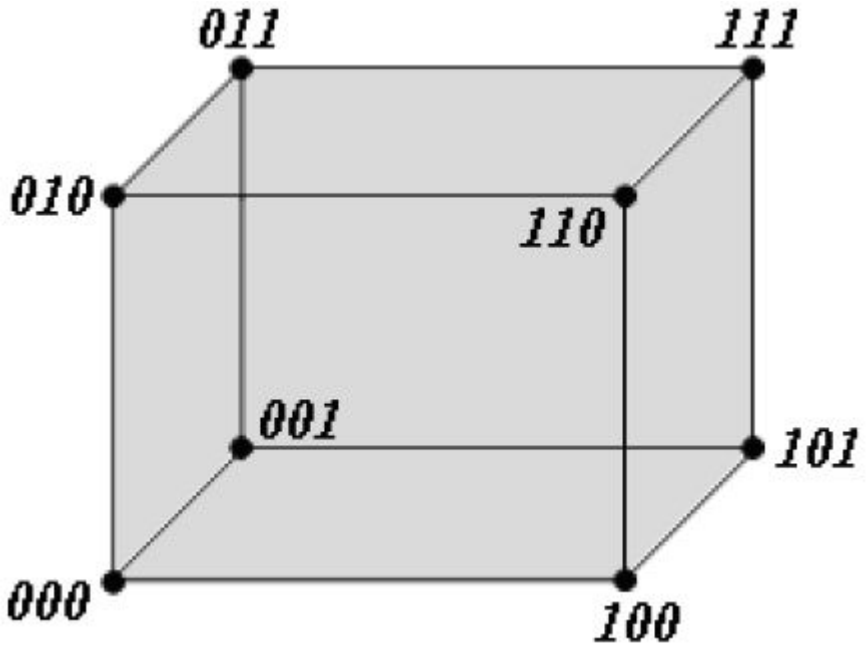
Error detecting and correcting capabilities of (n,k) LBC

- Thus an (n,k) block code with minimum distance d_{min} is capable of detecting all error patterns of d_{min} -1 or fewer errors.
- An (n,k) linear code is capable of detecting (2^n-2^k) error patterns.
- Error correcting capability (t)

$$t \leq \left\{\frac{1}{2}(d_{\min}-1)\right\}$$

Error Detecting and Error Correcting Capabilities

- The minimum distance, d_{min} determines the error correcting capability of the code.
- Suppose we consider ***3***-bit code words plotted at the vertices of the cube as shown.



- If the code words used are {000, 101, 110, 011}, $d_{min} = 2$.

Error Detecting and Error Correcting Capabilities

- Any error in the received word locates them on the vertices of the cube which are not code words and may be recognized as single errors.
- If the minimum distance of a linear block code is d_{min} then any 2 distinct codewords differ in atleast d_{min} places.
- So no error patterns of d_{min} -1 or fewer errors can change the codeword into another codeword.
- If the received vector is not a codeword, then error is detected.
- Thus an (n,k) block code with minimum distance d_{min} is capable of detecting all error patterns of d_{min} -1 or fewer errors.
- An (n,k) linear code is capable of detecting (2^n-2^k) error patterns.
- Out of (2^n-1) possible non-zero error patterns there are (2^k-1) error patterns identical to the codewords.
- Hence (2^k-1) undetectable error patterns (syndrome will be zero).

- If the error pattern is not a codeword, then the received vector is not a valid codeword and the syndrome will not be zero.

- Suppose an (n, k) linear block code has to detect and correct all error patterns whose Hamming weight, $\omega \leq t$.
- If we transmit a code vector α then received vector $\beta = \alpha \oplus e$
- The decoder output $\hat{\alpha} = \alpha$ if $\omega(e) \leq t$.
- The decoder picks the code vector nearest to the received vector β for which the Hamming distance is the smallest. {d (α,β) is minimum}.
- The decoder can detect and correct all error patterns of Hamming weight $\omega(e) \leq t$ provided that $d_{min} \geq (2t + 1)$
- Let t be a positive integer such that $2t + 1 \leq d_{min} \leq 2t + 2$
- Suppose δ be any other code word of the code.
- Hamming distances among α,β and δ satisfy the triangular inequality:
- $d(\alpha,\beta) + d(\beta,\delta) \geq d(\alpha,\delta)$

- Suppose an error pattern of t errors occurs during transmission of α.
- Then the received vector β differs from α in t places and hence $d(\alpha,\beta) = t'$.

- Since α and δ are code vectors, $d(\alpha,\delta) \geq d_{min} \geq 2t + 1$

$d(\alpha,\beta) = t'$

$d(\delta, \beta) \geq 2t + 1 - t'$

- If $t' \leq t$, then $d(\delta,\beta) > t$
- If an error pattern of t or fewer errors occurs, the received vector β is closer to the transmitted code vector α than to any other code vector δ of the code.
- For a BSC, this means $P(\beta|\alpha) > P(\beta|\delta)$ for $\alpha \neq \delta$ and β is decoded as α and thus the errors are corrected.
- The code is not capable of correcting error patterns of weight l > t.
- Suppose $d(\alpha,\delta) = d_{min}$, and let e_1 and e_2 be two error patterns such that:

i) $e_1 \oplus e_2 = \alpha \oplus \delta$

ii) e_1 and e_2 do not have nonzero components in common places.

- $\omega(e_1) + \omega(e_2) = \omega(\alpha \oplus \delta) = d(\alpha, \delta) = d_{min}$
- Suppose, α is the transmitted code vector and is corrupted by the error pattern e_1.
- Then the received vector is:

$\beta = \alpha \oplus e_1$

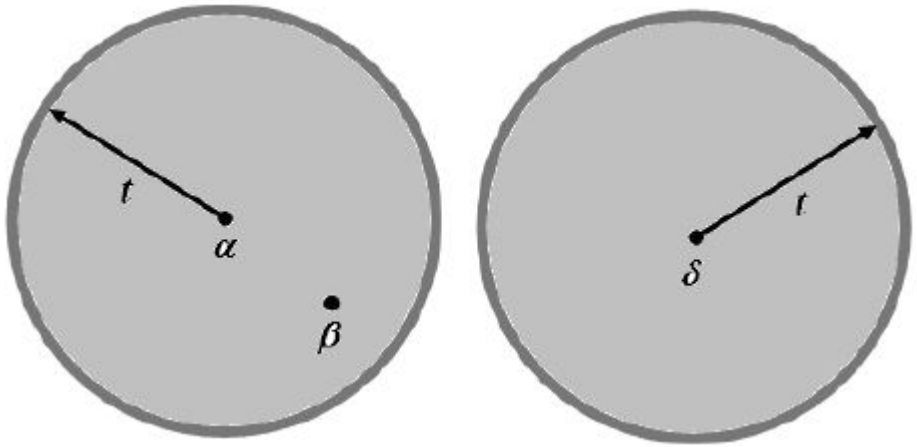
$d(\alpha, \beta) = \omega(\alpha \oplus \beta) = \omega(e_1)$

- $d(\delta, \beta) = \omega(\delta \oplus \beta) = \omega(\delta \oplus \alpha \oplus e_1) = \omega(e_2)$
- If e_1 contains more than t errors, $\omega(e_1) > t$, and since $2t + 1 \leq d_{min} \leq 2t + 2$,

$\omega(e_2) \leq t - 1$

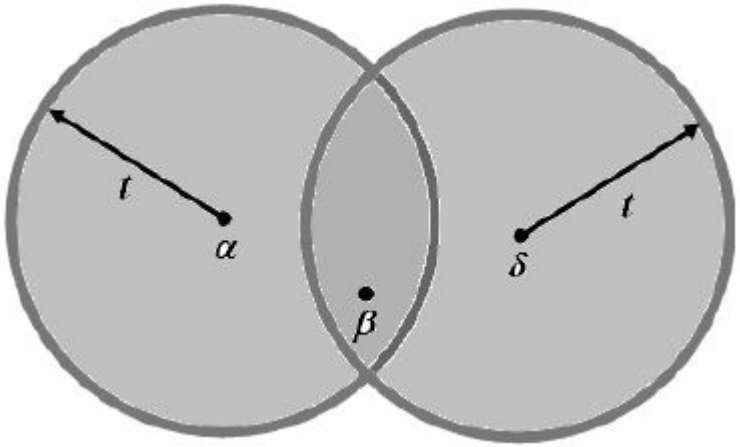
- $d(\alpha, \beta) \geq d(\delta, \beta)$
- The error pattern with $l > t$ errors results in a received vector closer to an incorrect code vector.

- The code vectors and the received vectors may be represented as points in an *n*- dimensional space.
- Construct 2 spheres of equal radii, *t* and locate code vectors α and δ at the centres.
- Let these two spheres be mutually exclusive i.e. $d(\alpha,\delta) \geq 2t + 1$ as shown.



- If $d(\alpha,\beta) \leq t$, the decoder will pick α as the transmitted vector.

- If d (α,δ) ≤ 2t, the two spheres intersect.

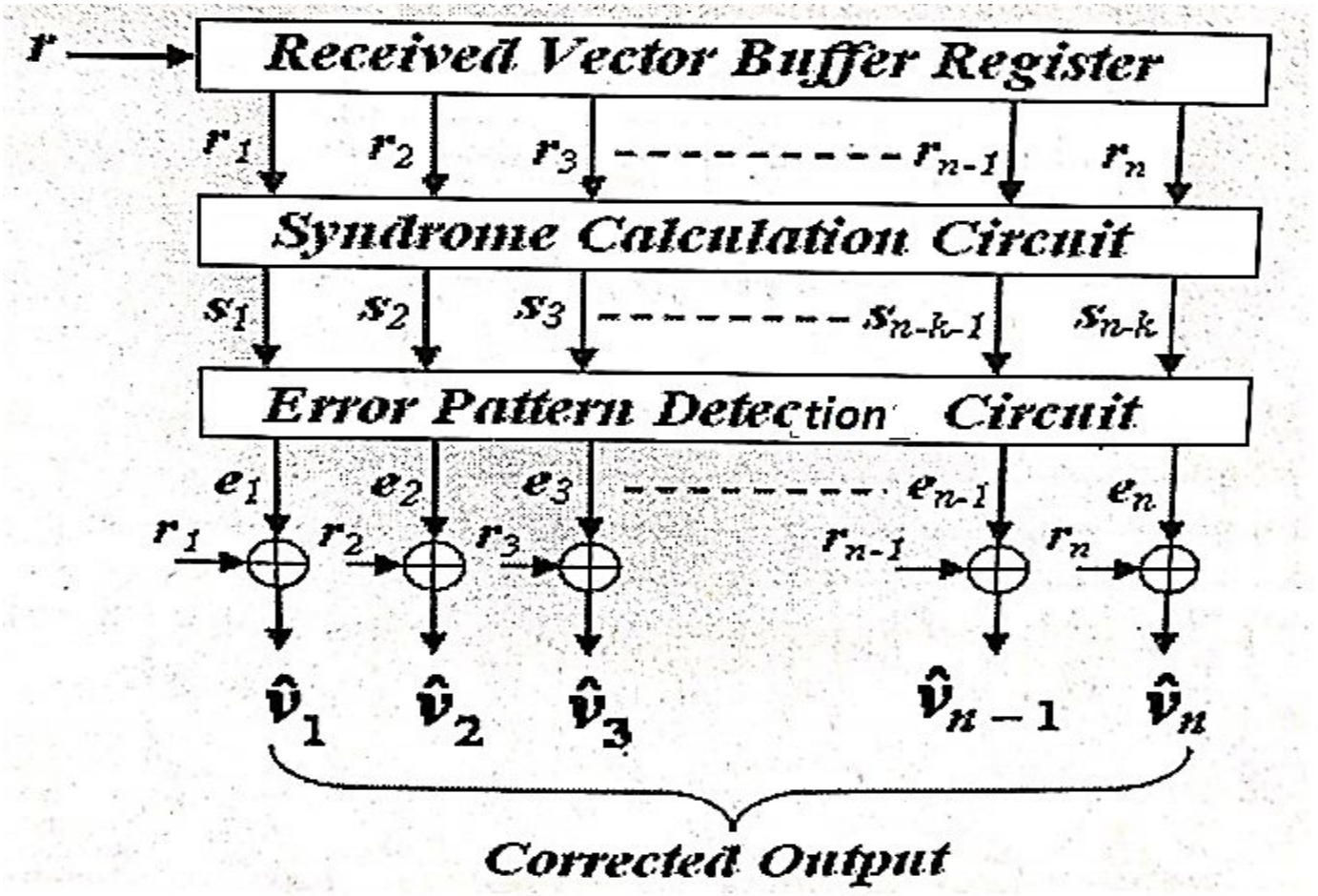


- Even if d(α,β)≤ t, β is close to δ as it is to α.
- The decoder picks δ as the transmitted vector which is wrong.
- An (n, k) linear block code can correct all error patterns of weight t or less if and only if d(α, δ) ≥ 2t + 1 for all α and δ.
- Hence $t \leq \left\{\frac{1}{2}(d_{min} - 1)\right\}$ $d(\alpha,\delta)_{min} = d_{min}$
- It is the largest integer not greater than ½ (d_{min} -1).
- t is called as the random-error-correcting capability of the code and the code is referred to as a “t-error correcting code”.

Syndrome Decoding

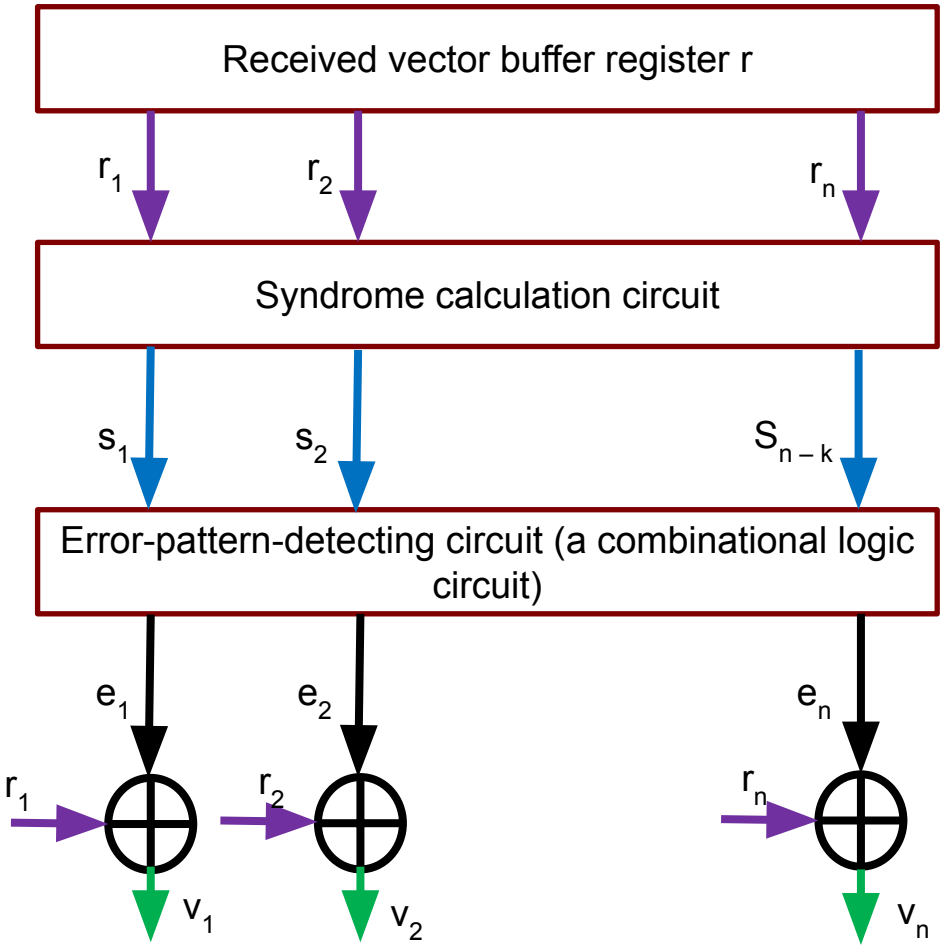
Decoding Circuit

- The error patterns can be expressed as functions of syndrome.
- $e_1 = f_1(s_1, s_2, \ldots, s_{n-k})$; $e_2 = f_2(s_1, s_2, \ldots, s_{n-k})$; …, $e_n = f_n(s_1, s_2, \ldots, s_{n-k})$



Syndrome Decoding

Decoding Circuit



- For the (6, 3) linear block code, $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$
- $G = [I_k \quad | \quad P_{k\times(n-k)}]$
- $H = [P^T \quad | \quad I_{(n-k)}]$
- $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$
- For standard array writing with Hamming weight '1' co-set leader is bit "1" from rightmost to left shift

Co-set leader
000 000
000 001
000 010
000 100
001 000
010 000
100 000
Hamming weight = 2

- $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$
- First error pattern is the all zero codeword.
- Next 6 co-set leaders are single error patterns.
- Write the syndrome.
- First one will be 000 and the remaining 6 syndromes are the **columns** of *H matrix* from the rightmost column in that order.
- Identify the one left, syndrome is 111.

Syndrome	Co-set leader
	000 000
	000 001
	000 010
	000 100
	001 000
	010 000
	100 000
	Hamming weight = 2

Syndrome Decoding

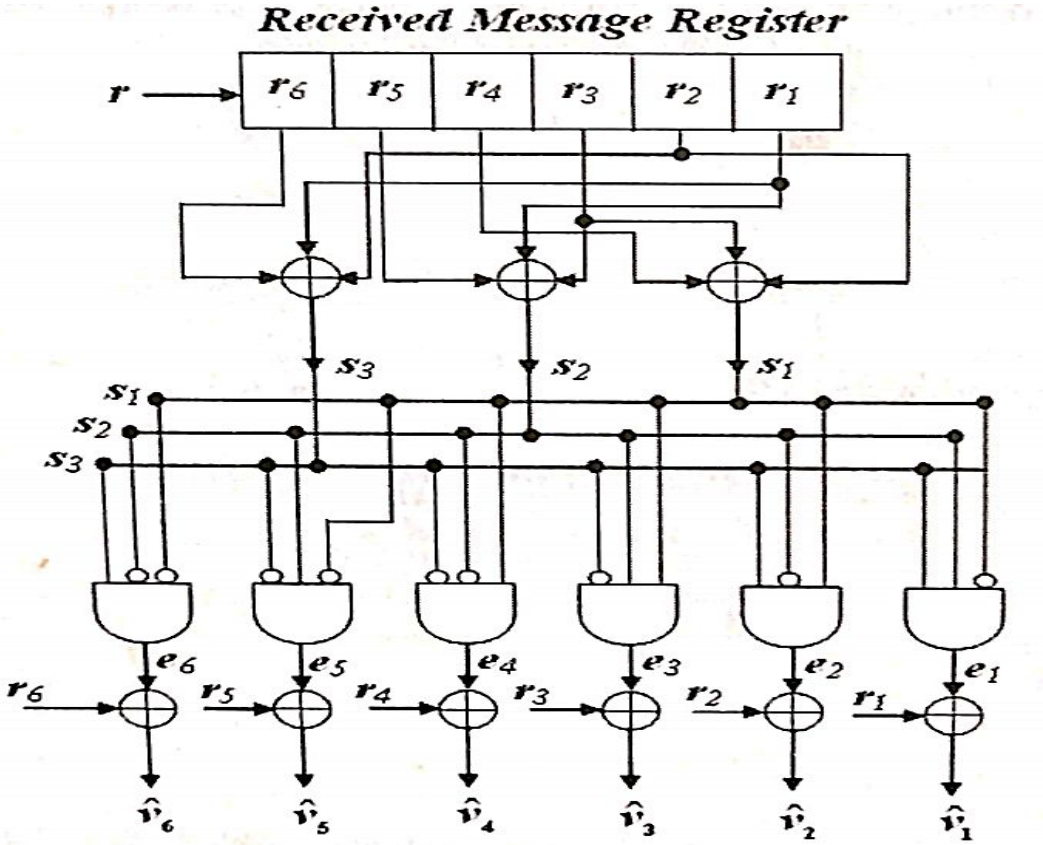
Decoding Circuit

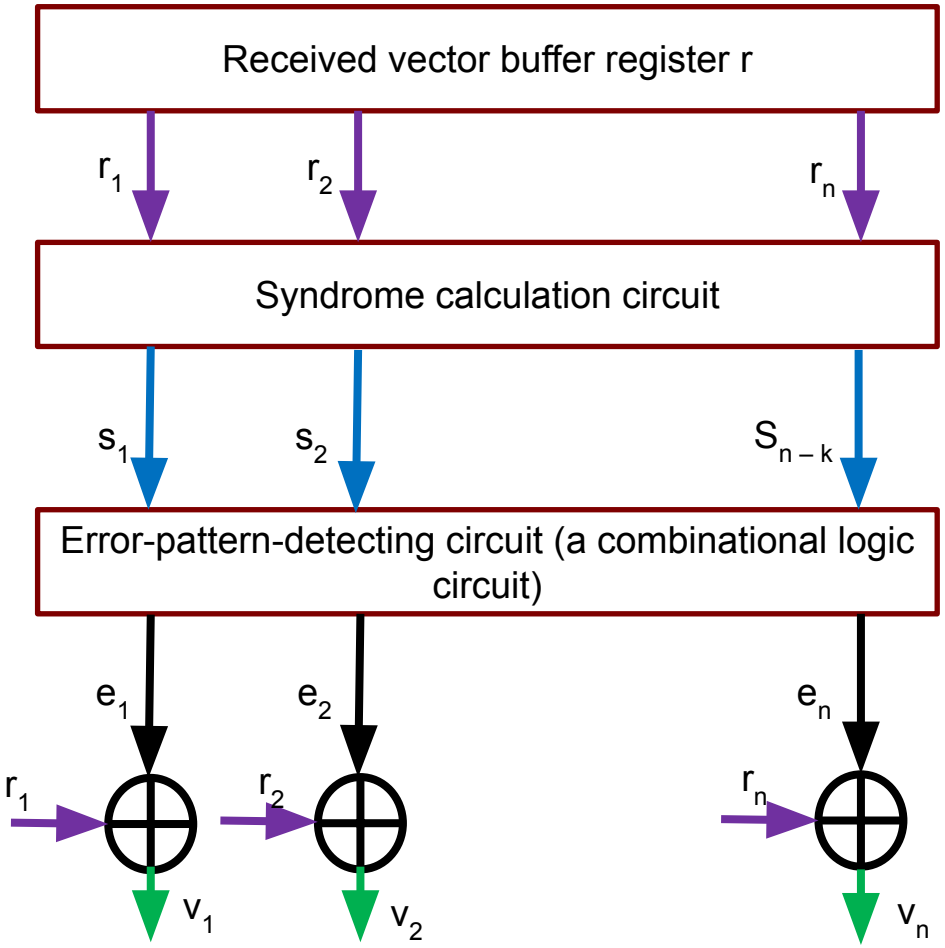
- For (6, 3) code obtain the decoder circuit.
- From the table we can write
  - $e_1 =$
  - $e_2 =$
  - $e_3 =$
  - $e_4 =$
  - $e_5 =$
  - $e_6 =$

Syndromes			Correctable error patterns (Co-set leaders)					
s_1	s_2	s_3	e_1	e_2	e_3	e_4	e_5	e_6
0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	1
0	1	0	0	0	0	0	1	0
1	0	0	0	0	0	1	0	0
1	1	0	0	0	1	0	0	0
1	0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0	0
1	1	1	0	0	1	0	0	1

Syndrome Decoding

Decoding Circuit





- For the (6, 3) linear block code, $G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$
- $G = [P_{k\times(n-k)} \mid I_k]$
- $H = [I_{(n-k)} \mid P^T]$
- $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$
- For standard array writing with Hamming weight '1' co-set leader is bit "1" from leftmost to right shift

Co-set leader
000 000
100 000
010 000
001 000
000 100
000 010
000 001
Hamming weight = 2

- $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$
- First error pattern is the all zero codeword.
- Next 6 co-set leaders are single error patterns.
- Write the syndrome.
- First one will be 000 and the remaining 6 syndromes are the **columns** of *H matrix* from the leftmost column in that order.
- Identify the one left, syndrome is 111.

Syndrome	Co-set leader
000	000 000
100	100 000
010	010 000
001	001 000
110	000 100
011	000 010
101	000 001
111	Hamming weight = 2

Syndrome Decoding

- For all correctable single error patterns the syndrome will be identical to a column of the H matrix and the received vector is in error corresponding to that column position.
- If the received vector is (010001), $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$
- $s = r.H^T$
- Then the syndrome is (100).

Syndrome Decoding

- If the received vector is (010001), then the syndrome is (100).
- $\hat{v} = r \oplus e$
- $\hat{v} = 010001 \oplus 000100$
- $\hat{v} = 010101$
- This is identical to the 4th column of the H-matrix and hence the 4th position of the received vector is in error.

Syndrome	Error Pattern	Error Location	Bit in Error
011	100 000	1	r_1
101	010 000	2	r_2
110	001 000	3	r_3
100	000 100	4	r_4
010	000 010	5	r_5
001	000 001	6	r_6
000	000 000	No erSror	

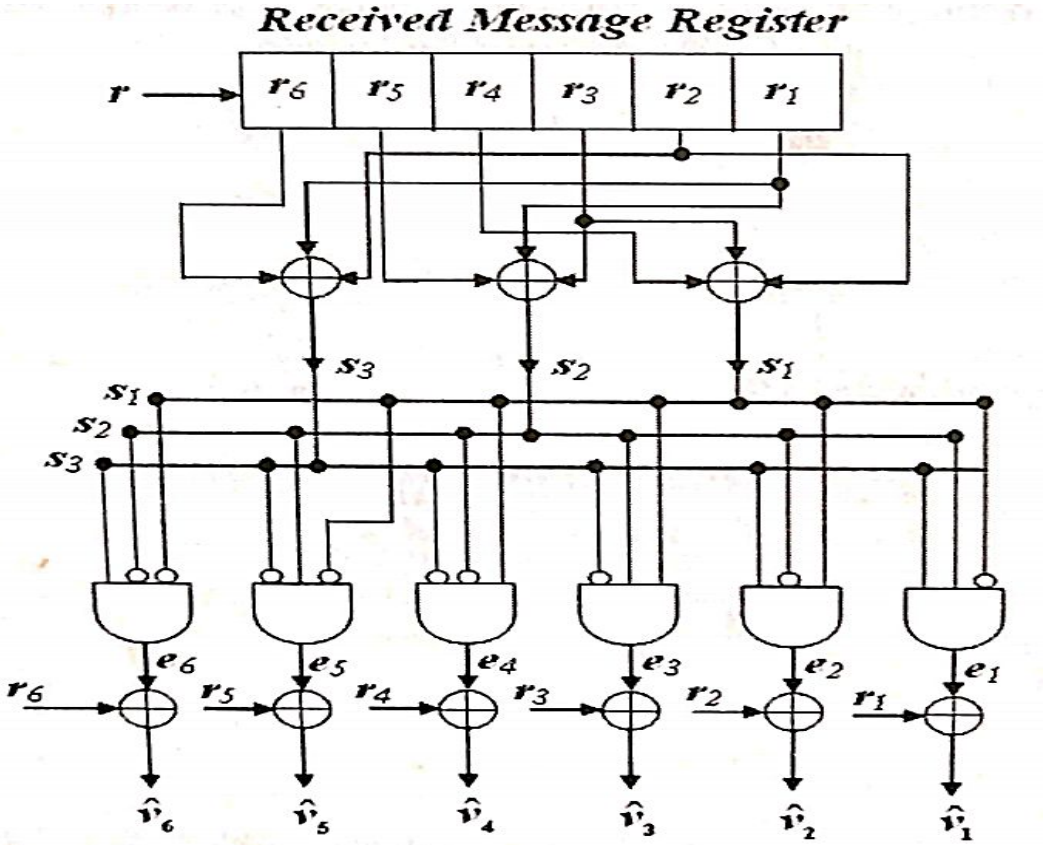
Syndrome Decoding

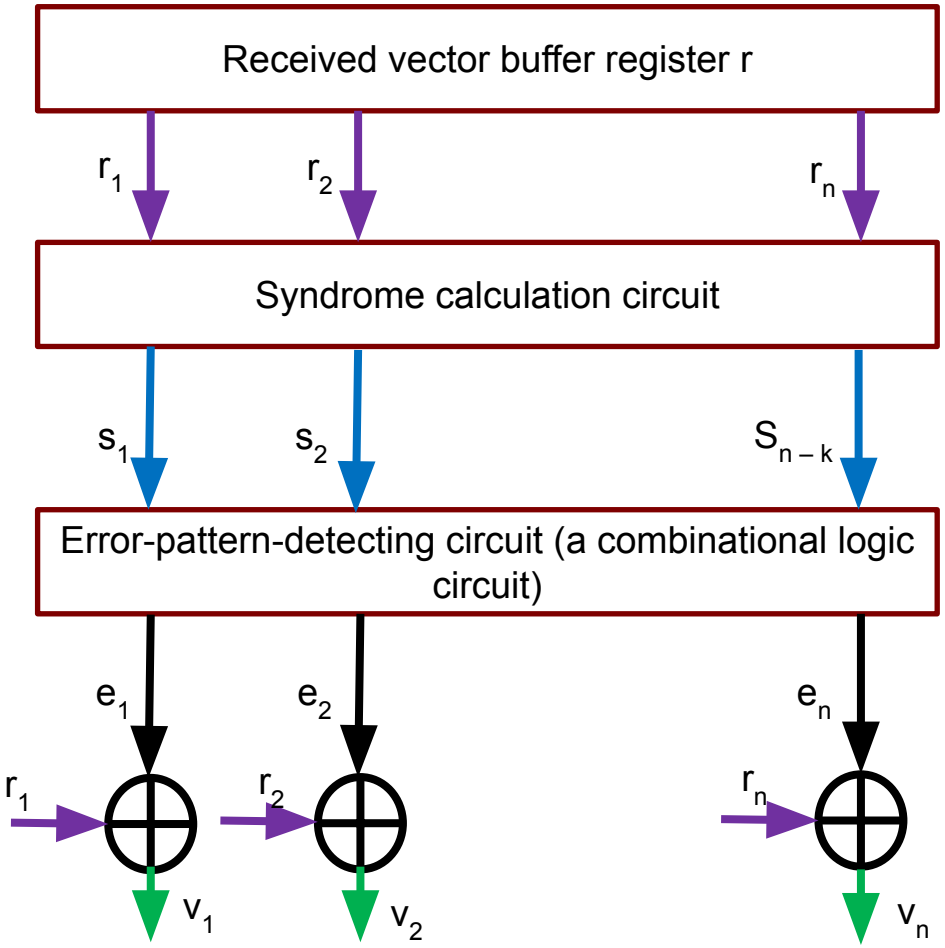
- Hence the corrected vector is 010101.
- A table can be prepared for error location and syndrome

Syndromes			Correctable error patterns (Co-set leaders)					
s_1	s_2	s_3	e_1	e_2	e_3	e_4	e_5	e_6
0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	1
0	1	0	0	0	0	0	1	0
1	0	0	0	0	0	1	0	0
1	1	0	0	0	1	0	0	0
1	0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0	0
1	1	1	0	0	1	0	0	1

Syndrome Decoding

Decoding Circuit





RSET
RAJAGIRI SCHOOL OF
ENGINEERING & TECHNOLOGY

Standard Array and Syndrome Decoding

Standard Array

- An important property of the syndrome.
- Let $\boldsymbol{v}_j$, j = 1, 2, …, 2^k be the 2^k distinct code vectors of an (n, k) linear block code.
- For any error pattern $\boldsymbol{e}$, 2^k distinct error vectors, e_j is

$$e_j = e \oplus v_j \,, j = 1, 2, \ldots, 2^k$$

- The set of vectors $e_j, j = 1, 2, \ldots, 2^k$ is called the "*co-set*" of the code.
- There are 2^{n-k} *co-sets* for an (n, k) *linear block code*.

$$e_j.H^T = e.\ H^T \oplus v_j.H^T = e.H^T$$

- *"All error patterns that differ at most by a code word have the same syndrome"*. Each co-set (row) has a unique syndrome.

Standard Array

- Since the received vector r can be any of the 2^n possible n-tuples, we can partition the received codewords into 2^k disjoint sets & identify the received vector using the "*Standard Array*".
- The steps involved are as below:
  1) **Step1**: Place the 2^k code vectors, with the all zero vector $v_1 = (0, 0, 0, \ldots, 0) = O$ as the first (left most) element.
  2) **Step 2**: From among the remaining $(2^n - 2^k)$-n–tuples, e_2 is chosen and placed below v_1. The second row is formed $(e_2 \oplus v_j)$, j = 2, 3, …, 2^k under every v_j.
  3) **Step 3**: Choose e_3 and complete the 3^{rd} *row* as in step 2.
  4) **Step 4**: Continue until all the n-tuples are used (Up to e_2^{n-k}).

Standard Array

			...	
			...	
			...	
			...	

Fig: Standard array for an (n, k) linear block code

- Since all the code vectors v_j are all distinct, the vectors in any row of the array are also distinct.
- "No two n-tuples in the same row of a standard array are identical".
- Every n-tuple appears in one and only one row.

Standard Array

- There are 2^{n-k} disjoint rows or co-sets in the *standard array* and each row or co-set consists of 2^k distinct entries.
- The first n-tuple of each co-set, (the entry in the first column) is called the *Co-set leader*.
- Suppose D_j^T is the j[th] column of the standard array. Then

$$D_j = \{v_j, e_2 \oplus v_j, e_3 \oplus v_j, \ldots, e_2^{n-k} \oplus v_j\}$$

$v_j \rightarrow$ code vector, $e_2, e_3, e_2^{n-k} \rightarrow$ co-set leaders.

Standard Array

- The 2^k disjoint columns $D_1^T, D_2^T, \ldots, D_{2^k}^T$ can be used for decoding the code.
- If $\boldsymbol{v}_j$ is transmitted code word over a noisy channel, the received vector $\boldsymbol{r}$ will be in D_j^T if the error pattern caused by the channel is a co-set leader and $\boldsymbol{r}$ will be decoded correctly as $\boldsymbol{v}_j$.
- If not an erroneous decoding will result for, error pattern $\hat{e}$ is not a co-set leader and let

$\hat{e} = e_i \oplus v_l$, then received vector is

$$r = v_j \oplus \hat{e} = v_j \oplus (e_i \oplus v_l) = e_i \oplus v_m$$

- Thus the received vector is in D_m^T and it will be decoded as v_m and a decoding error occurs

Standard Array and Syndrome Decoding

- *Correct decoding is possible iff the error pattern caused by the channel is a co-set leader*.
- Accordingly, the 2^{n-k} co-set leaders are called the *Correctable error patterns*, & it follows ***"Every (n, k) linear block code is capable of correcting 2^{n-k} error patterns"***.
- To minimize the probability of decoding error, ***"the most likely to occur"*** error patterns should be chosen as co-set leaders

Standard Array

- For a BSC an error pattern of smallest weight is most probable and hence error patterns of smallest weight should be chosen as co-set leaders.
- Then the decoding based on the standard array would be the *minimum distance decoding* (the maximum likelihood decoding).

Standard Array

- Suppose a received vector r is found in the j^{th} column and l^{th} row of the array, then r will be decoded as v_j.

$$d(r, v_j) = \omega(r \oplus v_j) = \omega(e_l \oplus v_j \oplus v_j) = \omega(e_l)$$

  - where v_j is the transmitted codeword.
- Let v_s be any other codeword, other than v_j.
- Then $d(r, v_s) = \omega(r \oplus v_s) = \omega(e_l \oplus v_j \oplus v_s) = \omega(e_l \oplus v_i)$
  - v_i is a code word

Standard Array

- Since e_l and $(e_l \oplus v_i)$ are in the same co-set and, e_l being the co-set leader has the smallest weight.
- $\omega(e_l) \leq \omega(e_l \oplus v_i)$ and hence $d(r, v_j) \leq d(r, v_s)$.
- *Thus the received vector is decoded into a closet code vector*.
- If each co-set leader has the minimum weight in its co-set, the standard array decoding results in the minimum distance decoding or maximum likelihood decoding.

Standard Array for an (n, k) linear code

$v_1 = 0$	v_2	$\cdots$	v_i	$\cdots$	v_{2^k}
e_2	$e_2 + v_2$	$\cdots$	$e_2 + v_i$	$\cdots$	$e_2 + v_{2^k}$
e_3	$e_3 + v_2$	$\cdots$	$e_3 + v_i$	$\cdots$	$e_3 + v_{2^k}$
$\vdots$					$\vdots$
e_l	$e_l + v_2$	$\cdots$	$e_l + v_i$	$\cdots$	$e_l + v_{2^k}$
$\vdots$					$\vdots$
$e_{2^{n-k}}$	$e_{2^{n-k}} + v_2$	$\cdots$	$e_{2^{n-k}} + v_i$	$\cdots$	$e_{2^{n-k}} + v_{2^k}$

Standard Array, e.g.

$$G = \begin{bmatrix} g_1 \\ g_2 \\ g_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

E.g.: For the (6, 3) code in Problem 4.4 construct standard array, along with the syndrome table

Syndrome	*Co-set Leader*							
000	*000 000*	*001 110*	*010 101*	*011 011*	*100 011*	*101 101*	*110 110*	*111 000*

Standard Array, e.g.

E.g.: For the (6, 3) $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$, $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

- First error pattern is the all zero codeword.
- Next 6 co-set leaders are single error patterns.
- They can be written down without any difficulty, uptill 7 rows in all & one more row has to be written.
- Write the syndrome.
- First one will be 000 and the remaining 6 syndromes are the columns of *H matrix* from the rightmost column in that order.

Standard Array, e.g.

E.g.: For the (6, 3) $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$, $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

- Identify the one left, syndrome is 111.
- This can be obtained by adding 1st & 4th or 2nd & 5th or 3rd & 6th columns of *H matrix*.
- So we get 3 possible double error patterns which can be used as a co-set leader. 100100 or 010010 or 001001
- Last one is used in the array.

Standard Array, e.g.

E.g.: For the (6, 3) $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$, $H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

- Identify the one left, syndrome is 111.

- To find the last error pattern of double error: Find the syndrome of all the error patterns.
- Now only one 3 *tuple* is left out, which is 111

Standard Array, e.g.

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

- For an *(n, k)* linear block code with minimum distance d_{min} all n-tuples of weight $t \leq \frac{1}{2}(d_{min} - 1)$ can be used as co-set leaders of a standard array.
- If all n-tuples of weight ≤ t are used as co-set leaders, there is atleast one n-tuple of weight (t+1) cannot be used as a co-set leader.