ECT306 INFORMATION THEORY AND CODING

Module 3

Module 3 – Introduction to Linear Block Codes

- Overview of Groups, Rings, Finite Fields, Construction of Finite Fields from Polynomial rings, Vector spaces.
- Block codes and parameters. Error detecting and correcting capability. Linear block codes. Two simple examples -- Repetition code and single parity-check code. Generator and parity-check matrix. Systematic form.
- Maximum likelihood decoding of linear block codes. Bounded distance decoding. Syndrome. Standard array decoding.

Introduction

- Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra, or modern algebra.
- In abstract algebra, we are concerned with sets on whose elements we can operate algebraically.
- That is, we can combine two elements of the set, perhaps in several ways, to obtain a third element of the set.

Modulo Operations

Modulo-m Addition

- Let m be a positive integer and Z={0,1,2,…,m-1}
- For any two integers i & j ϵ Z, , where *r* is the remainder resulting from dividing *i*+*j* by *m*.

Composition Table

- A binary operation in a finite set can completely be described by means of a table.
- This table is known as a composition table.
- The composition table helps us to verify most of the properties satisfied by the binary operations.

Modulo-2 addition

Z={0,1}

m=2

Composition Table for Modulo-2 addition

⊕	0	1
0	0	1
1	1	0

Modulo – 5 Addition

Z={0,1,2,3,4}

M=5

Composition Table for Modulo-5 addition

⊕	0	1	2	3	4
0	0	1	2	2	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Additive Identity Element

- Let (*Z*, +) be a set equipped with a binary operation +. Then an element *e* of *Z is called the* ***identity element*** *if* ***e + a = a*** *for all a in Z, and if* ***a + e = a*** *for all a in Z.*
- For which value the elements in the set is vertically repeating in the same order, then that value will be the identity element.

Additive Inverse Element

- Let (Z, +) be a set equipped with a binary operation +. Then any element a in Z , there exists another element a' *in* Z such that

  a + a'= a'+ a= e

  The element a' is called additive inverse of a.

- We can find the additive inverse element as follows.
  - Find all the identity elements repeating in the table.
  - Then the intersection of identity elements in horizontal and vertical directions are the inverses.

Modulo-2 addition

Identity element is 0

Additive Inverses

Element a	Inverse a'
0	0
1	1

⊕	0	1
0	0	1
1	1	0

Modulo – 5 Addition

Identity element is 0

Additive Inverses

Element a	Inverse a'
0	0
1	4
2	3
3	2
4	1

⊕	0	1	2	3	4
0	0	1	2	2	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- Write the composition table for Modulo-8 Addition. Find the additive identity element and additive inverses.

Composition Table

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Identity Element is 0

Inverse elements are

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

Modulo-m Multiplication

- Let m be a positive integer and $Z=\{0,1,2,\ldots,m-1\}$
- For any two integers i , $j \epsilon Z_m$, $i \otimes j = r$, where r is the remainder resulting from dividing i x j by m.

Modulo-2 multiplication

Z={0,1}

m=2

Composition Table for Modulo-2 multiplication

⊗	0	1
0	0	0
1	0	1

Modulo – 5 Multiplication

Z={0,1,2,3,4}

M=5

Composition Table for Modulo-2 multiplication

⊗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplicative Identity Element

- Let (*Z*, x) be a set equipped with a binary operation x. Then an element *e* of *Z is called the* ***identity element*** *if* ***e x a = a*** *and* ***a x e = a*** *for all a in Z.*
- For which value the elements in the set is vertically repeating in the same order, then that value will be the identity element.

Multiplicative Inverse Element

- Let (Z, x) be a set equipped with a binary operation x. Then any element a in Z , there exists another element a' *in* Z such that

  $a \times a' = a' \times a = e$

  The element a^{-1} is called multiplicative inverse of a.

- We can find the multiplicative inverse element as follows.
  - Find all the identity elements repeating in the table.
  - Then the intersection of identity elements in horizontal and vertical directions are the inverses.

Modulo-2 multiplication

⊗	0	1
0	0	0
1	0	1

Identity element

Identity element is 1

Inverse Elements

Element a	Inverse a'
0	No inverse
1	1

Modulo – 5 Multiplication

Identity Element

Identity element is 1

⊗	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Inverse Elements

Element a	Inverse a'
0	No inverse
1	1
2	3
3	2
4	4

- Write the composition table for Modulo-8 Multiplication. Find the multiplicative identity element and multiplicative inverses.

Composition Table

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

Modulo –8 Multiplication

Identity Element

Identity element is 1

Inverse Elements

a	a'
0	No inverse
1	1
2	No inverse
3	3
4	No inverse
5	5
6	No inverse
7	7

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

Groups

- A group G, sometimes denoted by {G, *} is a set of elements together with a binary operation, denoted by *, such that the following axioms are obeyed:

(A1) Closure: If a and b belong to G, then a*b is also in G.

(A2) Associative: a * (b * c) = (a * b) * c for all a, b, c in G.

(A3) Identity element: There is an element e in G such that a * e = e * a = a for all a in G.

(A4) Inverse element: For each a in G there is an element a' in G such that a * a' = a' * a = e.

- If a group has a finite number of elements, it is referred to as a finite group, and the order of the group is equal to the number of elements in the group. Otherwise, the group is an infinite group.
- A group is said to be **abelian if it satisfies the following additional condition:**

(A5) Commutative: a * b = b * a for all a, b in G.

- *The set of integers (positive, negative, and 0) under addition is an abelian group. The set of nonzero real numbers under multiplication is an abelian group.*

• Check whether the set G={0, 1, 2, 3, 4} is a group under

i)modulo-5 addition

ii) modulo-5 multiplication

Solution

i) **Closure property**

The sum of any two elements in the set is also an element in the set.

Associative property

a + (b + c) = (a + b) + c

1+(2+3)=(1+2)+3

1+0=3+3

1=1

Identity element

Existing identity element which 0

Existence of inverse

Inverse element also existing for all elements in the set

The set G={0, 1, 2, 3, 4} is a group under modulo-5 addition.

ii) **Closure property**

The product of any two elements in the set is also an element in the set.

Associative property

a x (b x c) = (a x b) x c

1x(2x3)=(1x2)x3

1x1=2x3

1=1

Identity element

Existing identity element which is 1

Existence of inverse

Inverse element is not existing for the element 0.

The set G={0, 1, 2, 3, 4} is not a group under modulo-5 multiplication

Field

- A field F, sometimes denoted by {F, +, x}, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in F the following axioms are obeyed:

(A1) Closure: If a and b belong to F, then a +b is also in F.

(A2) Associative: a + (b +c) = (a +b) + c for all a, b, c in F.

(A3) Identity element: There is an element e in F such that a +e = e + a = a for all a in F.

(A4) Inverse element: For each a in F there is an element a' in F such that a + a' = a' + a = e.

(A5) Commutative: a + b = b + a for all a, b in F.

- **(M1) Closure under multiplication:** If a and b belong to F, then axb is also in F.
- **(M2) Associativity of multiplication:** ax(bxc) = (axb)x c for all a, b, c in F.
- **(M3) Distributive laws:** ax(b + c) = axb + axc for all a, b, c in F.

  (a + b)x c = a x c + b x c for all a, b, c in F.
- **(M4) Commutativity of multiplication:** axb = bxa for all a, b in F.
- **(M5) Multiplicative identity:** There is an element 1 in F such that ax1 = 1xa = a for all a in F.

- **(M6) No zero divisors:** If a, b in F and axb = 0, then either a = 0 or b = 0.
- **(M7) Multiplicative inverse:** For each a in F, except 0, there is an element a^{-1} in F such that $axa^{-1} = (a^{-1}) \times a = 1$.

- A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set.
- Division is defined with the following rule:

$$a/b = a(b^{-1}).$$

Q. Check whether the following set of integers can form a field.

Z={0,1,2,3,4}

Solution:

(A1) Closure property

The sum of any two elements in the set is also an element in the set.

(A2) Associative property

a + (b + c) = (a + b) + c

1+(2+3)=(1+2)+3

1+0=3+3

1=1

(A3) Identity element

Existing identity element which is 0

(A4) Existence of inverse

Inverse element also existing for all elements in the set

(A5) Commutative: a * b = b * a for all a, b in F.

2+3=3+2

0=0

(M1) Closure property

The product of any two elements in the set is also an element in the set.

(M2) Associative property

a x (b x c) = (a x b) x c

1x(2x3)=(1x2)x3

1x1=2x3

1=1

(M3) Distributive laws: ax(b + c) = axb + axc

1x(2+3)=1x2+1x3

1x0=2+3

0=0

(M4) Commutativity of multiplication: axb = bxa

2x3=3x2

1=1

(M5) Identity element

Existing identity element which is 1

(M6) No zero divisors

(M7) Multiplicative inverse:

Inverse element is existing for all elements except 0.

The given set Z={0,1,2,3,4} is obeying all axioms for the existence of a field. So the given set Z={0,1,2,3,4} is a field.

- Similarly we can see the set Z={0,1} will also a field.
- It is known as Binary field.
- If we consider the set Z={0,1,2,3,4,5,6,7}, it wont satisfy the axiom **(M7) Multiplicative inverse:.**
- Inverse element is not existing for all non zero elements.
- So the set Z={0,1,2,3,4,5,6,7} is not a field.

Q. Check whether the following set of integers can form a field.

$Z=\{0,1,2,3,4,5,6,7,8\}$

Composition table for Modulo-9 addition

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Inverse pairs are --------→

a	a^{-1}
0	0
1	8
2	7
3	6
4	5
5	4
6	3
7	2
8	1

Composition table for Modulo-9 multiplication

x	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

- Identity element is 1
- Inverse pairs are---------→

a	a^{-1}
0	No inverse
1	1
2	5
3	No inverse
4	7
5	2
6	No inverse
7	4
8	8

- Inverse element is not existing for all non zero elements.
- So the set Z={0,1,2,3,4,5,6,7,8} is not a field.

How we can generalize?

Z={0,1}, m=2 Field

Z={0,1,2,3,4}, m=5 Field

Z={0,1,2,3,4,5,6,7}, m=8 Not a Field

Z={0,1,2,3,4,5,6,7,8}, m=9 Not a Field

- Let p be a prime number, then the set Z={1,2,3,…..p-1} will form a Field.
- It is also called Prime Field.
- If a prime field is finite, then it is called Galois Field. It is represented by GF(p).
- The number of elements of a finite field is called its *order* or its *size*.

Z={0,1}, m=2 Field →GF(2)

Z={0,1,2,3,4}, m=5 Field →GF(5)

Z={0,1,2,3,4,5,6,7}, m=8 Field → $GF(2^3)$

Z={0,1,2,3,4,5,6,7,8}, m=9 Field → $GF(3^2)$

- A finite field of order *m* exists if and only if the order *m* is a prime power p^k (where *p* is a prime number and *k* is a positive integer).

Ring

- A ring R, sometimes denoted by {R, +, x}, is a set of elements with two binary operations, called addition and multiplication, such that for all a, b, c in R the following axioms are obeyed:

(A1) Closure: If a and b belong to R, then a +b is also in R.

(A2) Associative: a + (b +c) = (a +b) + c for all a, b, c in R.

(A3) Identity element: There is an element e in R such that
a +e = e + a = a for all a in R.

(A4) Inverse element: For each a in R there is an element a'
in G such that a + a' = a' + a = e.

(A5) Commutative: a + b = b + a for all a, b in R.

- **(M1) Closure under multiplication:** If a and b belong to R, then axb is also in R.
- **(M2) Associativity of multiplication:** ax(bxc) = (axb)x c for all a, b, c in R.
- **(M3) Distributive laws:** ax(b + c) = axb + axc for all a, b, c in R.

  (a + b)x c = a x c + b x c for all a, b, c in R.
- **(M4) Commutativity of multiplication:** axb = bxa for all a, b in R.
- **(M5) Multiplicative identity:** There is an element 1 in R such that ax1 = 1xa = a for all a in R.

- Solve the equation

2X+3Y=1 ----→(1)

X+2Y=2 ----→(2) using Modulo-5

Solution:

Multiply eqn(2) by 3

3X+Y=1 ----→(3)

(3)+(1)--→ (3+2)X+(1+3)Y=1+1

0+4Y=2

Y=2/4=2*4=3

X=2-2Y=2-2*3=2-1=2+4=1

X=1 and Y=3

Construction of Finite Fields from Polynomial rings

Finite (Galois) Fields: GF(p)

Order of Finite Field must be a power of prime number $GF(p^n)$

When $n = 1$ we get $GF(p)$ The structure is different then that of $GF(p^n)$

Else $n > 1$ $GF(p^n)$

- $GF(p) :=$ set of Z_p integers $\{0,1,2 \ \ldots \ p-1\}$
- Eg: $GF(2) :=$ $F = < Z_p, +, * >$ $:= GF(2^1)$

+	0	1
0	0	1
1	1	0

XOR

*	0	1
0	0	0
1	0	1

AND

a	$-a$	a^{-1}
0	0	-
1	1	1

Inverse

The identity of additive inverse does not have multiplicative inverse

Finite (Galois) Fields: GF(p)

- Eg: $GF(7) := Z_7$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

a	$-a$	a^{-1}
0	0	-
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Modulo 8 domain Z_8

Integer	1	2	3	4	5	6	7
Frequency	4	8	4	12	4	8	4

Frequency of elements is evenly distributed in Addition

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

Frequency of elements is not evenly distributed in Multiplication

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

a	$-a$	a^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-
7	1	7

Justification for Galois Field

Better Solution
$GF(2^n)$

- We need to perform +,-,* and ÷. So we need something that qualifies for a field.
- Z_p qualifies to be a field.
- Problems:
  - But if we have 3 bits representation then the we are dealing with Z_8 domain.
  - For 8 bits representation we have Z_{256}
  - All of theses are even integer domains and none of them, except Z_2, are in Z_p
  - Z_{256}, Z_8 etc are Commutative Rings
- Solution: Not Good
  - We can opt for largest prime number in the given Z_n domain.
  - 3 bits can have Z_7 and 8 bits can have Z_{251}. But this leads to inefficiency.

$GF(2^3)$

$GF(2^n) \equiv GF(p^n)$

Integer	1	2	3	4	5	6	7
Frequency	7	7	7	7	7	7	7

Frequency of elements is evenly distributed in Addition

+	000	001	010	011	100	101	110	111
000	0	1	2	3	4	5	6	7
001	1	0	3	2	5	4	7	6
010	2	3	0	1	6	7	4	5
011	3	2	1	0	7	6	5	4
100	4	5	6	7	0	1	2	3
101	5	4	7	6	1	0	3	2
110	6	7	4	5	2	3	0	1
111	7	6	5	4	3	2	1	0

Frequency of elements is not evenly distributed in Multiplication

*	000	001	010	011	100	101	110	111
000	0	0	0	0	0	0	0	0
001	0	1	2	3	4	5	6	7
010	0	2	4	6	3	1	7	5
011	0	3	6	5	7	4	1	2
100	0	4	3	7	6	2	5	1
101	0	5	1	4	2	7	3	6
110	0	6	7	1	5	3	2	4
111	0	7	5	2	1	6	4	3

Multiplicative Inverse of all elements does exist

$-a = a$

a	$-a$	a^{-1}
0	0	-
1	1	1
2	2	5
3	3	6
4	4	7
5	5	2
6	6	3
7	7	4

Modular Polynomial Arithmetic

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

$$x^7 + x^4 + x^2 + x^0$$

$$x^7 + x^4 + x^2 + 1$$

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

$$x^6 + x^5 + x^3 + x^1$$

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

Example of $GF(2^3)$

000	0
001	1
010	x
011	$x + 1$
100	x^2
101	$x^2 + 1$
110	$x^2 + x$
111	$x^2 + x + 1$

For $GF(2^n)$ order of polynomial will never exceed $n - 1$

If, after some operation, the order exceeds $n - 1$ then perform mod order n **Irreducible Polynomial**

Irreducible Polynomial of order 3 is $x^3 + x + 1$

Operation on Mod Poly. Arth.

Example in $GF(2^3)$

$f(x) = x^2 + x + 1$ (1 1 1 = 7)

$g(x) = x^2 + 1$ (1 0 1 = 5)

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

Addition:

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

(0 1 0 = 2)

$$\begin{array}{r} x+1 \\ x^3+x+1 \;\overline{)\; x^4+x^3+\quad x+1} \\ x^4+\quad x^2+x \\ \hline x^3+x^2\quad +1 \\ x^3\quad +x+1 \\ \hline x^2+x \end{array}$$

Multiplication:

$$= f(x) * g(x)$$
$$= (x^2 + x + 1) * (x^2 + 1)$$
$$= (x^4 + x^3 + x^2) + (x^2 + x + 1)$$
$$= (x^4 + x^3 + x^2) + (x^2 + x + 1)$$
$$= x^4 + x^3 + x + 1$$

$$= f(x) * g(x) \bmod m(x)$$
$$= (x^4 + x^3 + x + 1) \bmod (x^3 + x + 1)$$
$$= x^2 + x$$

(1 1 0 = 6)

Concept of Vectors

► The set $\mathbf{R}^n$ with operations of componentwise addition and scalar multiplication is an example of a **vector space,** and its elements are called **vectors.**

We shall Henceforth interpret R^n *to be a vector space.*

(We say that $\mathbf{R}^n$ is **closed** under addition and scalar multiplication).

► In general, if **u** and **v** are vectors in the same vector space, then **u** + **v** is the diagonal of the **parallelogram** defined by **u** and **v**.

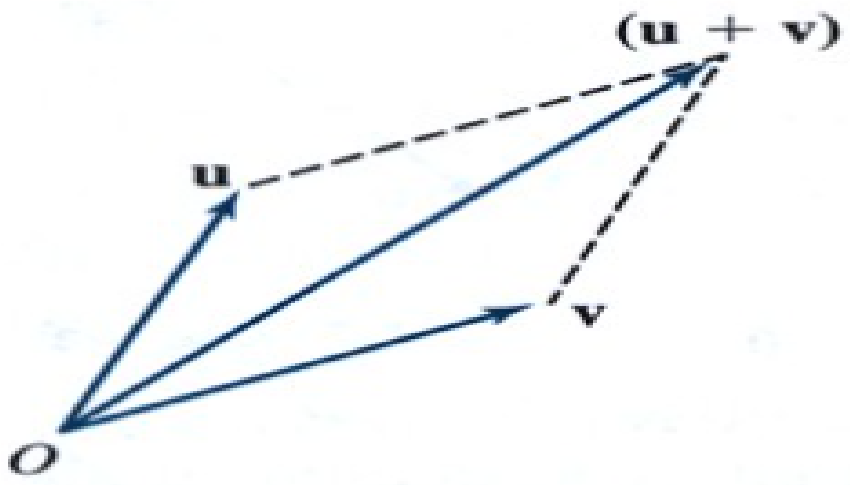


Figure 4.2

Example 2

Let $\mathbf{u} = (-1, 4, 3)$ and $\mathbf{v} = (-2, -3, 1)$ be elements of $\mathbf{R}^3$.
Find $\mathbf{u} + \mathbf{v}$ and $3\mathbf{u}$.

Solution: $\mathbf{u} + \mathbf{v} = (-1, 4, 3) + (-2, -3, 1) = (-3, 1, 4)$

$3\mathbf{u} = 3(-1, 4, 3) = (-3, 12, 9)$

Example 3

In R^2, consider the two elements (4, 1) and (2, 3).
Find their sum and give a geometrical interpretation of this sum.

we get (4, 1) + (2, 3) = (6, 4).

The vector (6, 4), the sum, is the diagonal of the parallelogram.

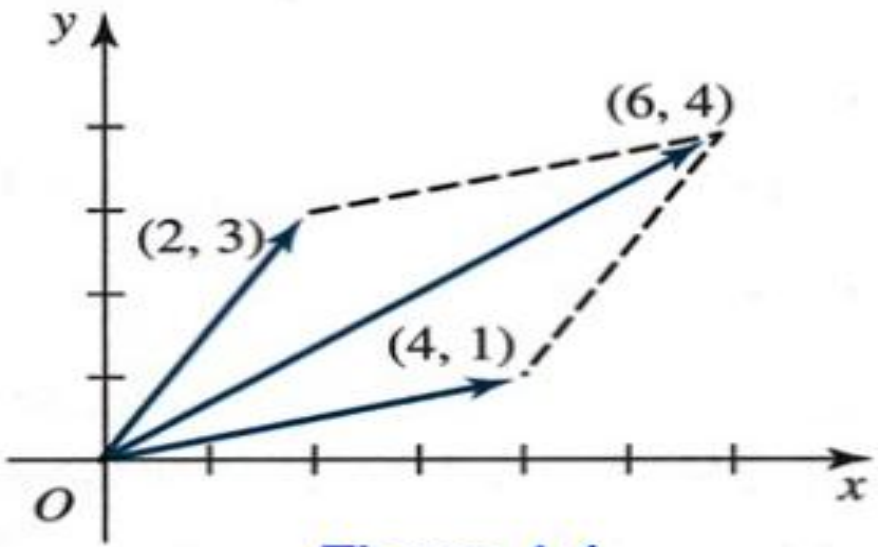
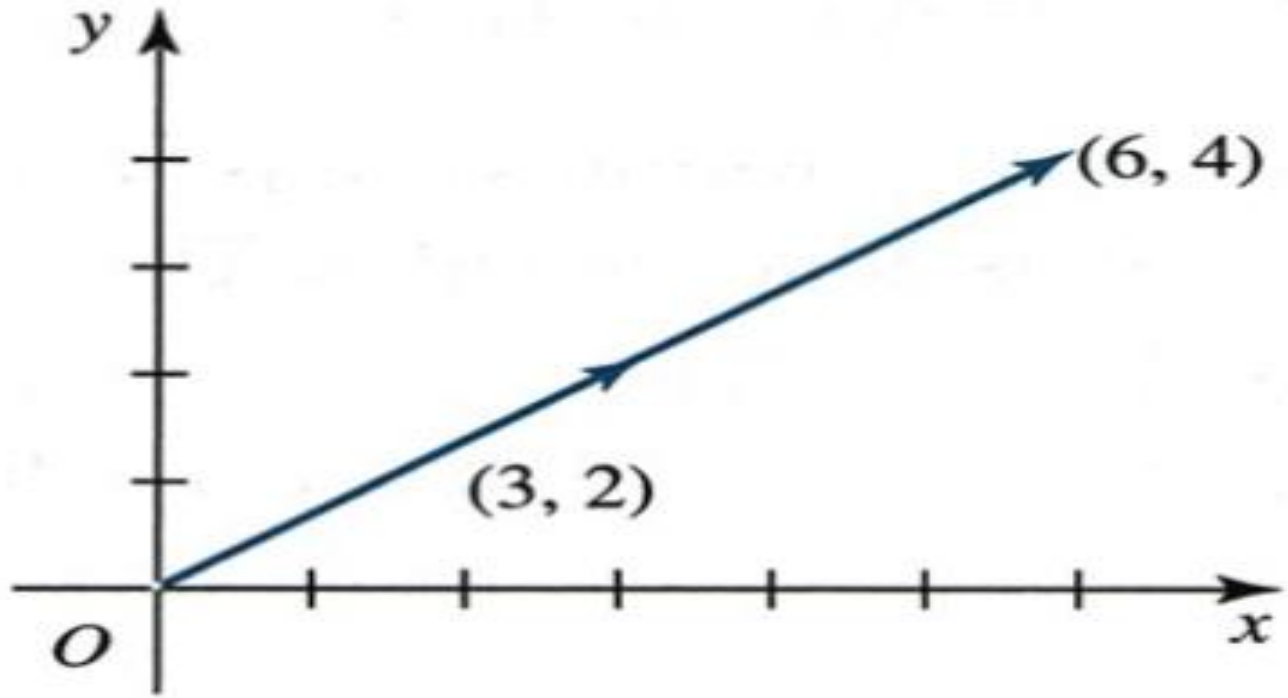


Figure 4.1

Consider the scalar multiple of the vector (3, 2) by 2, we get

$$2(3, 2) = (6, 4)$$

Observe in Figure 4.3 that (6, 4) is a vector in the same direction as (3, 2), and 2 times it in length.

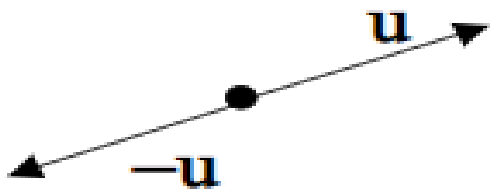


Zero Vector

The vector $(0, 0, \ldots, 0)$, having n zero components, is called the **zero vector** of $\mathbf{R}^n$ and is denoted $\mathbf{0}$.

Negative Vector

The vector $(-1)\mathbf{u}$ is writing $-\mathbf{u}$ and is called **the negative of u** . It is a vector having the same length (or magnitude) as $\mathbf{u}$, but lies in the opposite direction to $\mathbf{u}$.



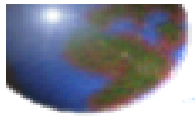
Subtraction

Subtraction is performed on element of $\mathbf{R}^n$ by subtracting corresponding components.

Let $\mathbf{u} = (2, 5, -3)$, $\mathbf{v} = (-4, 1, 9)$, $\mathbf{w} = (4, 0, 2)$ in the vector space R^3. Determine the vector $2\mathbf{u} - 3\mathbf{v} + \mathbf{w}$.

Solution

$$
\begin{aligned}
2\mathbf{u} - 3\mathbf{v} + \mathbf{w} &= 2(2, 5, -3) - 3(-4, 1, 9) + (4, 0, 2) \\
&= (4, 10, -6) - (-12, 3, 27) + (4, 0, 2) \\
&= (4 + 12 + 4, 10 - 3 + 0, -6 - 27 + 2) \\
&= (20, 7, -31)
\end{aligned}
$$



Column Vectors

Row vector: $\mathbf{u} = (u_1, u_2, \ldots, u_n)$

Column vector: $\begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}$

We defined addition and scalar multiplication of column vectors in $\mathbf{R}^n$ in a componentwise manner:

$$\begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} + \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{bmatrix} \quad \text{and} \quad c\begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} cu_1 \\ \vdots \\ cu_n \end{bmatrix}$$

4.2 Dot Product, Norm, Angle, and Distance

Definition

Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ be two vectors in $\mathbf{R}^n$. The dot product of $\mathbf{u}$ and $\mathbf{v}$ is denoted $\mathbf{u}.\mathbf{v}$ and is defined by

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \cdots + u_n v_n$$

The dot product assigns a real number to each pair of vectors.

Example 1

Find the dot product of

$$\mathbf{u} = (1, -2, 4) \text{ and } \mathbf{v} = (3, 0, 2)$$

Solution

$$\begin{aligned} \mathbf{u} \cdot \mathbf{v} &= (1 \times 3) + (-2 \times 0) + (4 \times 2) \\ &= 3 + 0 + 8 \\ &= 11 \end{aligned}$$

Properties of the Dot Product

Let $\mathbf{u}$, $\mathbf{v}$, and $\mathbf{w}$ be vectors in $\mathbf{R}^n$ and let c be a scalar. Then

1. $\mathbf{u}.\mathbf{v} = \mathbf{v}.\mathbf{u}$
2. $(\mathbf{u} + \mathbf{v}).\mathbf{w} = \mathbf{u}.\mathbf{w} + \mathbf{v}.\mathbf{w}$
3. $c\mathbf{u}.\mathbf{v} = c(\mathbf{u}.\mathbf{v}) = \mathbf{u}.c\mathbf{v}$
4. $\mathbf{u}.\mathbf{u} \geq 0$, and $\mathbf{u}.\mathbf{u} = 0$ if and only if $\mathbf{u} = \mathbf{0}$

Proof

1. Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$. We get

$$\begin{aligned}\mathbf{u} \cdot \mathbf{v} &= u_1 v_1 + \cdots + u_n v_n \\ &= v_1 u_1 + \cdots + v_n u_n \quad \text{by the commutative property of real numbers} \\ &= \mathbf{v} \cdot \mathbf{u}\end{aligned}$$

4. $\mathbf{u} \cdot \mathbf{u} = u_1 u_1 + \cdots + u_n u_n = (u_1)^2 + \cdots + (u_n)^2$

$(u_1)^2 + \cdots + (u_n)^2 \geq 0$, thus $\mathbf{u} \cdot \mathbf{u} \geq 0$.

$(u_1)^2 + \cdots + (u_n)^2 = 0$, if and only if $u_1 = 0, \cdots, u_n = 0$.

Thus $\mathbf{u} \cdot \mathbf{u} = 0$ if and only if $\mathbf{u} = \mathbf{0}$.

Norm of a Vector in R^n

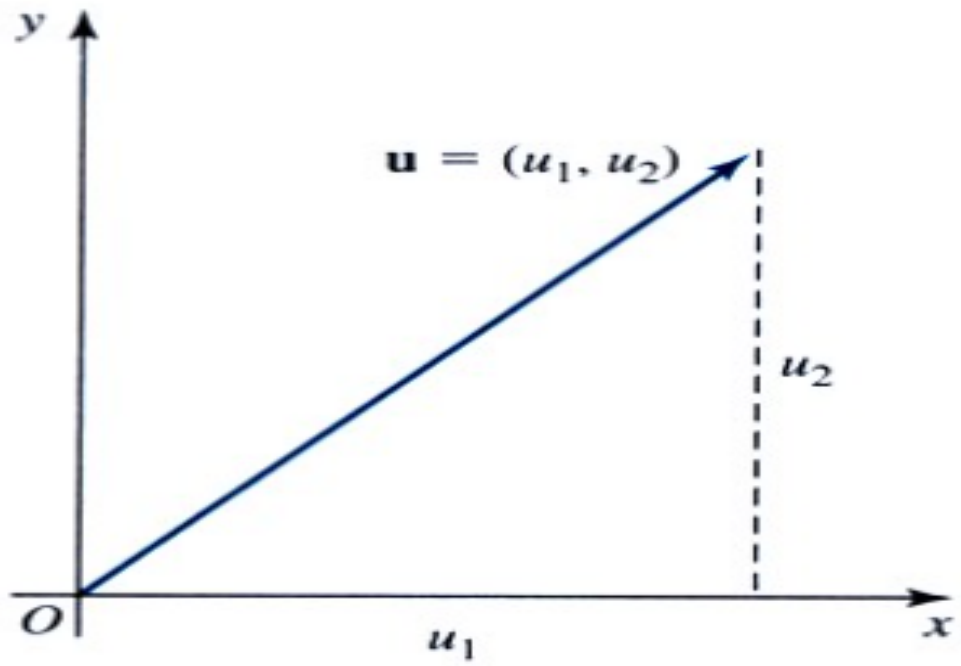


Figure 4.5 length of **u**

Definition

The **norm** (**length** or **magnitude**) of a vector $\mathbf{u} = (u_1, \ldots, u_n)$ in $\mathbf{R}^n$ is denoted $\|\mathbf{u}\|$ and defined by

$$\|\mathbf{u}\| = \sqrt{(u_1)^2 + \cdots + (u_n)^2}$$

Note:
The norm of a vector can also be written in terms of the dot product $\|\mathbf{u}\| = \sqrt{\mathbf{u} \cdot \mathbf{u}}$

Example 2

Find the norm of each of the vectors $\mathbf{u} = (1, 3, 5)$ of $\mathbf{R}^3$ and $\mathbf{v} = (3, 0, 1, 4)$ of $\mathbf{R}^4$.

Solution

$$\|\mathbf{u}\| = \sqrt{(1)^2 + (3)^2 + (5)^2} = \sqrt{1+9+25} = \sqrt{35}$$

$$\|\mathbf{v}\| = \sqrt{(3)^2 + (0)^2 + (1)^2 + (4)^2} = \sqrt{9+0+1+16} = \sqrt{26}$$

Definition

A **unit vector** is a vector whose norm is 1.

If $\mathbf{v}$ is a nonzero vector, then the vector

is a unit vector in the direction of $\mathbf{v}$.

This procedure of constructing a unit vector in the same direction as a given vector is called **normalizing** the vector.

Example 3

(a) Show that the vector (1, 0) is a unit vector.

(b) Find the norm of the vector (2, −1, 3). Normalize this vector.

Solution

(a) $\|(1, 0)\| = \sqrt{1^2 + 0^2} = 1$. Thus (1, 0) is a unit vector. It can be similarly shown that (0, 1) is a unit vector in $\mathbf{R}^2$.

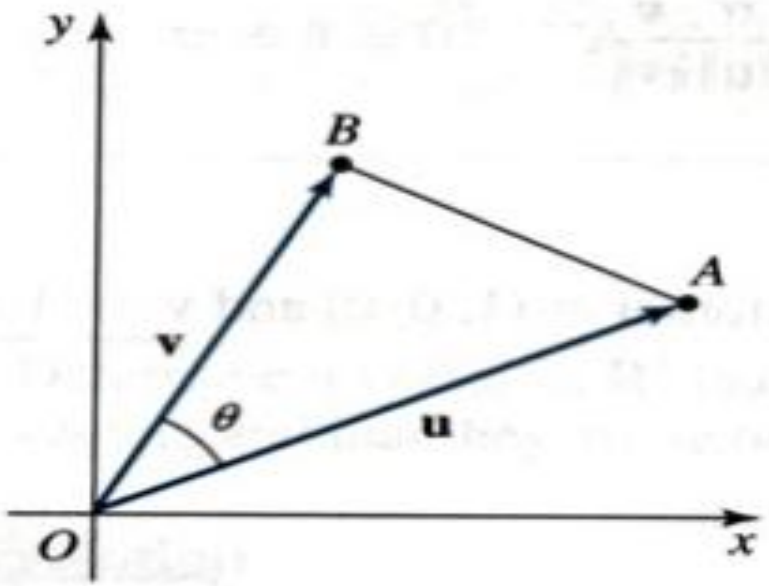
(b) $\|(2, -1, 3)\| = \sqrt{2^2 + (-1)^2 + 3^2} = \sqrt{14}$. The norm of (2, −1, 3) is $\sqrt{14}$. The normalized vector is

$$\frac{1}{\sqrt{14}}(2, -1, 3)$$

The vector may also be written $\left(\frac{2}{\sqrt{14}}, \frac{-1}{\sqrt{14}}, \frac{3}{\sqrt{14}}\right)$.

This vector is a unit vector in the direction of (2, −1, 3).

Angle between Vectors (in R^2)



The law of cosines gives:

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|}$$

← Figure 4.6

Definition

Let **u** and **v** be two nonzero vectors in $\mathbf{R}^n$.

The **cosine of the angle** θ between these vectors is

$$\cos\theta = \frac{\mathbf{u}\cdot\mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|} \qquad 0 \le \theta \le \pi$$

Example 4

Determine the angle between the vectors $\mathbf{u} = (1, 0, 0)$ and $\mathbf{v} = (1, 0, 1)$ in $\mathbf{R}^3$.

Solution $\mathbf{u} \cdot \mathbf{v} = (1, 0, 0) \cdot (1, 0, 1) = 1$

$$\|\mathbf{u}\| = \sqrt{1^2 + 0^2 + 0^2} = 1 \qquad \mathbf{v} = \sqrt{1^2 + 0^2 + 1^2} = \sqrt{2}$$

Thus $\cos\theta = \dfrac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{u}\|\|\mathbf{v}\|} = \dfrac{1}{\sqrt{2}}$, the angle between $\mathbf{u}$ and $\mathbf{v}$ is $45°$.

Orthogonal Vectors

Definition

Two nonzero vectors are **orthogonal** if the angle between them is a right angle .

Theorem 4.2

Two nonzero vectors $\mathbf{u}$ and $\mathbf{v}$ are orthogonal *if and only if* $\mathbf{u}.\mathbf{v} = \mathbf{0}$.

Example 5

Show that the following pairs of vectors are orthogonal.

(a) (1, 0) and (0, 1).

(b) (2, –3, 1) and (1, 2, 4).

Solution

(a) $(1, 0).(0, 1) = (1 \times 0) + (0 \times 1) = 0.$

The vectors are orthogonal.

(b) $(2, -3, 1).(1, 2, 4) = (2 \times 1) + (-3 \times 2) + (1 \times 4) = 2 - 6 + 4 = 0.$

The vectors are orthogonal.

- (1, 0), (0,1) are orthogonal unit vectors in $\mathbf{R}^2$.
- (1, 0, 0), (0, 1, 0), (0, 0, 1) are orthogonal unit vectors in $\mathbf{R}^3$.
- (1, 0, …, 0), (0, 1, 0, …, 0), …, (0, …, 0, 1) are orthogonal unit vectors in $\mathbf{R}^n$.

Orthonormal Vectors

The vectors u_1, u_2, u_3 in R^n are called orthonormal if they are all unit vectors and orthogonal to each other

For two orthonormal vectors

$$u_i \cdot u_j = \begin{cases} 1 \text{ if } i=j \\ 0 \text{ if } i \neq j \end{cases}$$

Vector Space Definition

Our aim in this section will be to focus on the algebraic properties of $\mathbf{R}^n$.

Definition

A **vector space** is a set V of elements called **vectors**, having operations of ***addition*** and ***scalar multiplication*** defined on it that satisfy the following conditions.

Let u, v, and w be arbitrary elements of V, and c and d are scalars.

- **Closure Axioms**

1. The sum $\mathbf{u} + \mathbf{v}$ exists and is an element of V. (V is closed under addition.)
2. $c\mathbf{u}$ is an element of V. (V is closed under scalar multiplication.)

- **Addition Axioms**

3. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ (commutative property)
4. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ (associative property)
5. There exists an element of V, called the **zero vector**, denoted $\mathbf{0}$, such that $\mathbf{u} + \mathbf{0} = \mathbf{u}$. (additive identity)
6. For every element $\mathbf{u}$ of V there exists an element called the **negative** of $\mathbf{u}$, denoted $-\mathbf{u}$, such that $\mathbf{u} + (-\mathbf{u}) = \mathbf{0}$. (additive inverse)

- **Scalar Multiplication Axioms**

7. $c(\mathbf{u} + \mathbf{v}) = c\mathbf{u} + c\mathbf{v}$
8. $(c + d)\mathbf{u} = c\mathbf{u} + d\mathbf{u}$

(distributive properties)

9. $c(d\mathbf{u}) = (cd)\mathbf{u}$
10. $1\mathbf{u} = \mathbf{u}$ (multiplicative inverse)

Let $W = \{a(1,0,1) \mid a \in \boldsymbol{R}\}$. Prove that W is a vector space.

Proof

Let $\mathbf{u} = a(1,0,1)$ and $\mathbf{v} = b(1,0,1) \in W$, for some a, $b \in \mathbf{R}$.

Axiom 1: $\mathbf{u} + \mathbf{v} = a(1,0,1) + b(1,0,1) = (a+b)(1,0,1)$

$\therefore \mathbf{u} + \mathbf{v} \in W$. Thus W is closed under addition.

Axiom 2: $c\mathbf{u} = ca(1,0,1) \in W$.

Thus W is closed under scalar multiplication.

Axiom 5: Let $\mathbf{0} = (0, 0, 0) = 0(1,0,1)$,
then $\mathbf{0} \in W$ and $\mathbf{0}+\mathbf{u} = \mathbf{u}+\mathbf{0} = \mathbf{u}$ for any $\mathbf{u} \in W$.

Axiom 6: For any $\mathbf{u} = a(1,0,1) \in W$. Let $-\mathbf{u} = -a(1,0,1)$,
then $-\mathbf{u} \in W$ and $(-\mathbf{u})+\mathbf{u} = \mathbf{0}$.

Subspaces

Vector spaces may be formed from subsets of other vectors spaces. These are called *subspaces*.

Subspaces

A **subspace** of a vector space V is a subset H of V that has three properties:

a. The zero vector of V is in H.

b. For each $\mathbf{u}$ and $\mathbf{v}$ are in H, $\mathbf{u} + \mathbf{v}$ is in H. (In this case we say H is closed under vector addition.)

c. For each $\mathbf{u}$ in H and each scalar c, $c\mathbf{u}$ is in H. (In this case we say H is closed under scalar multiplication.)

If the subset H satisfies these three properties, then H itself is a vector space.

Error Control Coding

- To detect and control errors
- It rely on the systematic addition of *redundant* symbols.
- At transmitter-Channel encoder
- At receiver-Channel decoder
- Also called *channel coding*.
- Improves data quality and reduce *Eb/N* for a fixed bit error rate.
- Reduces the transmitter power and hence the hardware cost.

Error Control Coding

- Additional digits are called *redundant digits-no information*
- The process is called *redundancy.*
- *Probability of error* is reduced.
- Disadvantages are,
  - Increased bandwidth
  - System become more complex

Types of Error control codes

(i)Block Codes

- Consist of (n-k) number of check bits or redundant bits
- Which is added to k number of information bits.
- Forms ‘n’ bit code word.
- (n-k) number of check bits are derived from k information bits.
- At receiver check bits are used to detect and correct errors.

Types of Error control codes

(ii)Convolutional Codes

- Check bits are continuously interleaved with information bits.
- These check bits are used to correct errors in any block.

(iii) Linear codes and non-linear codes

- In a linear code word, any two code words added using modulo-2 arithmetic produces a third code word in that code set.
- Non-linear code word, doesn't hold this condition.

Linear Block Codes

- K message bits or information bits
- (n-k) check bits
- N-code word length or block length
- Let C_1 and C_2 be any two code words belongs to a set of (n,k) block code. If $C_1 \oplus C_2$ is also a n-bit code word belongs to the same set of (n,k) block code, then such code is called (n,k) linear block code.
- A (n,k) linear block code is said to be systematic if the k-message bits appear either at the beginning of the code word or at the end of the code word.

Steps for Find all the code words for a Linear Block Code

(*i*) Let us consider that the particular code vector consists of m_1, m_2, m_3, ... m_k message bits and c_1, c_2, c_3 ..... c_q check bits. Then this code vector may be written as under:

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

where $q = n - k$

(*ii*) This means that q are the number of redundant bits added by the encoder. The above code vector may also be written as,

$$X = (M \mid C)$$

where $M = k$-bit message vector and

and $C = q$-bit check vector

(*iii*) Here, the check bits play the role of error detection and correction. The function of the linear block code is to generate these 'check bits'. The code vector can be represented as,

$$X = MG$$

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

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

and G = Generator matrix of $k \times n$ size.

(*iv*) Hence, equation $X = MG$ represents matrix form *i.e.*,

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

(*v*) The generator matrix depends upon the linear block code used. Normally, it is represented as,

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

Here $I_k = k \times k$ identity matrix, and

$P = k \times q$ submatrix

(*vi*) Now, the check vector may be obtained as,

$$C = MP$$

Hence, in the expanded form, the above expression can be written as

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

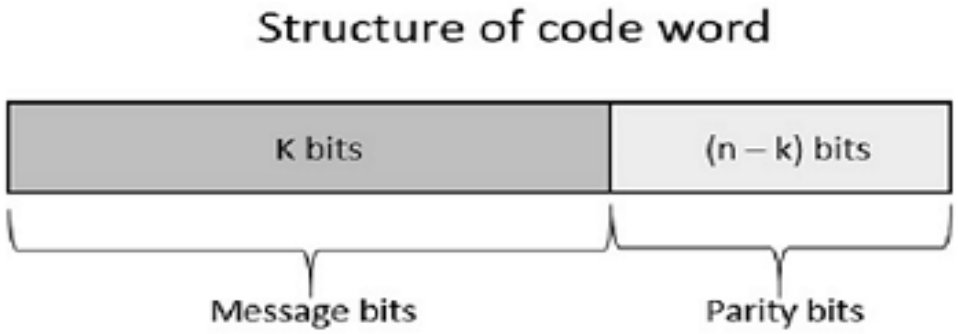
(*vii*) On solving the above matrix equation, check vector may be obtained as under:

$$\left.\begin{aligned} c_1 &= m_1 P_{11} \oplus m_2 P_{21} \oplus m_3 P_{31} \oplus \ldots. \oplus m_k P_{kl} \\ c_2 &= m_1 P_{12} \oplus m_2 P_{22} \oplus m_3 P_{32} \oplus \ldots. \oplus m_k P_{k2} \\ c_3 &= m_1 P_{13} \oplus m_2 P_{23} \oplus m_3 P_{33} \oplus \ldots. \oplus m_k P_{k3} \\ &\qquad\qquad\qquad\qquad\qquad\qquad \ldots.\text{and so on} \end{aligned}\right\}$$

Here, it may be noted that all the additions are mod-2 additions.

Linear Block Codes

- In the linear block codes, the parity bits and message bits have a linear combination, which means that the resultant code word is the linear combination of any two code words.
- Let us consider some blocks of data, which contains k bits in each block.
- The transmitter adds redundant bits which are n−k bits. The ratio k/n is the code rate. It is denoted by r and the value of r is $r < 1$.
- The n−k bits added here, are parity bits. Parity bits help in error detection and error correction, and also in locating the data.



Linear block Codes

- The information bit stream is divided into blocks of k bits.
- Each block is encoded to a larger block of n bits.
- The coded bits are modulated and sent over channel.
- The reverse procedure is done at the receiver.

Linear Block Codes

Definition: A code is said to be linear if any two code words in the code can be added in modulo 2 addition to produce a third code word in the code.

Code word length= n bits

k message bits (n-k) parity bits

(n,k) linear block code

Linear Block Codes

Properties

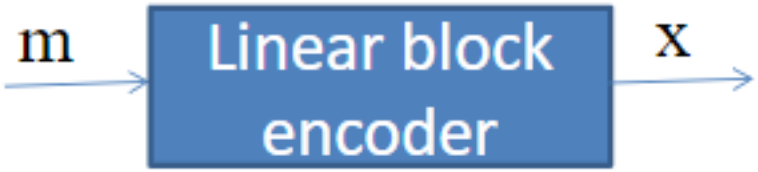
- Sum of two codewords belonging to a code is also a codeword.

  {0000, 0101, 1010, 1111}
  Eg: 0101 + 1111 = 1010

- All zero codewords is always a codeword.
- The minimum distance between 2 codewords
  of a linear code is equal to the minimum weight of the code.

Linear Block Codes-Encoding

- A vector notation is used for the message bits and parity bits
  - message bit m = $[m_0\ m_1 \ldots . m_{k-1}]$
  - Parity bit c = $[c_0\ c_1 \ldots \ldots . c_{n-k-1}]$



--The code vector can be mathematically represented by

X=[M:C]

M= k message vector

C= (n-k) parity vector

Linear Block Codes-Encoding

- A block code encoder generates the parity vector or parity bits required to be added to the message bits to generate the code word. The code vector x can also be represented as

$$[X]=[M][G]$$

X=code vector of (1×n) size

M=message vector of (1×k) size

G=generator matrix of (k×n) size

- The generator matrix depends on the type of linear block code used and is defined as

$$G = [\, I_k \mid P]$$

Where I_k = (k×k) identity matrix

P= k×(n-k) coefficient matrix

Linear Block Codes-Encoding

$$I_k = \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & 1 & . & . & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}_{k \times k}$$

$$P = \begin{bmatrix} p_{11} & p_{12} & \cdots\cdots & p_{1,n-k} \\ p_{21} & p_{22} & \cdots\cdots & p_{2,n-k} \\ \vdots & \vdots & \vdots & \vdots \\ p_{k1} & p_{k2} & \cdots\cdots & p_{k,n-k} \end{bmatrix}_{k \times n-k}$$

The parity vector can be obtained as

C=MP

$$\begin{bmatrix} c_1 & c_2 \ldots\ldots & c_{n-k} \end{bmatrix} = \begin{bmatrix} m_1 & m_2 & \ldots\ldots & m_k \end{bmatrix} \begin{bmatrix} p_{11} & p_{12} & \cdots\cdots & p_{1,n-k} \\ p_{21} & p_{22} & \cdots\cdots & p_{2,n-k} \\ \vdots & \vdots & \vdots & \vdots \\ p_{k1} & p_{k2} & \cdots\cdots & p_{k,n-k} \end{bmatrix}_{k \times n-k}$$

Linear Block Codes-Encoding

- On solving Matrix Equations, we get the check bits $c_1, c_2, c_3 \dots \dots c_{n-k}$

$$c_1 = m_1 p_{11} \oplus m_2 p_{21} \dots \dots \dots \oplus m_k p_{k1}$$

$$c_2 = m_1 p_{12} \oplus m_2 p_{22} \dots \dots \dots \oplus m_k p_{k2}$$

$$c_3 = m_1 p_{13} \oplus m_2 p_{23} \dots \dots \dots \oplus m_k p_{k3}$$

and so on

- By combining check bits along with message bits we get the complete code word.

Q) The generator matrix for a (6,3) block code is shown below. Obtain all codewords

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

Solution:

We know the generator matrix is given by

$$G = [I_k \ : \ P_{k \times q}]_{kxn} \quad (1)$$

Given Generator matrix is

$$G = \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right] \quad (2)$$

Comparing (1) with (2), we get

$$I_k = I_{3x3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{and } P_{kxq} = P_{3x3} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

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

This means the block size of the mesasage vector is 3 bits. Thus there will be total of 8 possible message vector.

Solution

The code vector or check vector can be obtained as,

$$C = MP$$

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

Thus, from the above matrix multiplication , we get

$C_1 = (0 \times m_1) \oplus m_2 \oplus m_3$ $\qquad$ $C_1 = m_2 \oplus m_3$

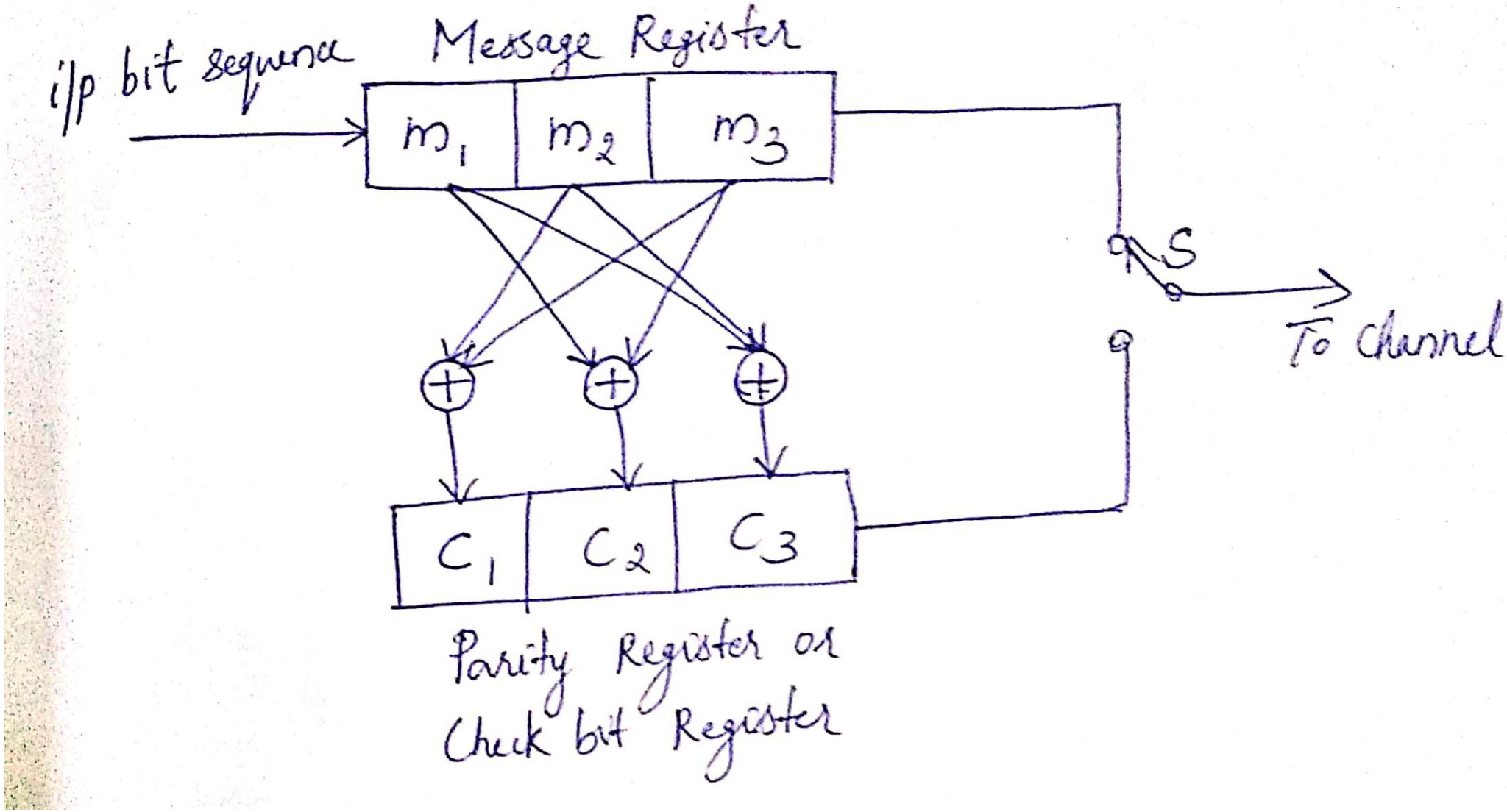
$C_2 = m_1 \oplus (0 \times m_2) \oplus m_3$ $\qquad$ $C_2 = m_1 \oplus m_3$

$C_3 = m_1 \oplus m_2 \oplus (0 \times m_3)$ $\qquad$ $C_3 = m_1 \oplus m_2$

Solution

	m_1	m_2	m_3	c_1 $m_2 \oplus m_3$	c_2 $m_1 \oplus m_3$	c_3 $m_1 \oplus m_2$	Complete codeword
1	0	0	0	0	0	0	000000
2	0	0	1	1	1	0	001110
3	0	1	0	1	0	1	010101
4	0	1	1	0	1	1	011011
5	1	0	0	0	1	1	100011
6	1	0	1	1	0	1	101101
7	1	1	0	1	1	0	110110
8	1	1	1	0	0	0	111000

Encoder Circuit



Hamming Weight, Hamming Distance, Minimum Distance

Definition 5.2 Hamming weight

The Hamming weight $w_H(c)$ of a codeword c is the number of nonzero components of c.

Definition 5.3 Hamming distance

The Hamming distance $d_H(c_1, c_2)$ between a codeword c_1 and a codeword c_2 is the number of elements in which they are different.

For a linear block code, the Hamming distance between any two codewords is the Hamming weight of the difference between any two codewords. It can be described as follows:

$$d_H(c_1, c_2) = w_H(c_1 - c_2) = w_H(c_3).$$

Hamming Weight, Hamming Distance,Minimum Distance

Example 5.3 Hamming weight and distance

Find the Hamming weight and distance of two codewords $\boldsymbol{c}_1 = [1011010]$ and $\boldsymbol{c}_2 = [1010001]$.

Solution

From Definition 5.2, the Hamming weights are

$$w_H(c_1) = d_H([1\ 0\ 1\ 1\ 0\ 1\ 0]) = 4$$
$$w_H(c_2) = d_H([1\ 0\ 1\ 0\ 0\ 0\ 1]) = 3.$$

From Definition 5.3, the Hamming distance is

$$d_H(c_1, c_2) = d_H([1\ 0\ 1\ 1\ 0\ 1\ 0], [1\ 0\ 1\ 0\ 0\ 0\ 1]) = 3.$$

■

Hamming Weight, Hamming Distance,Minimum Distance

Definition 5.4 Minimum distance

Among the Hamming distances between all pairs of codewords in a block code $\boldsymbol{C}$, the smallest Hamming distance is the minimum distance $d_{\min}$. It is defined as follows:

$$d_{\min} = \min\left\{d_{\mathrm{H}}(c_1, c_2) : c_1, c_2 \in C, c_1 \neq c_2\right\}.$$

Theorem

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

	Message Vector m_1 m_2 m_3	c_1 $m_2 \oplus m_3$	c_2 $m_1 \oplus m_3$	c_3 $m_1 \oplus m_2$	Complete codeword	Hamming Weight
1	0 0 0	0	0	0	000000	0
2	0 0 1	1	1	0	001110	3
3	0 1 0	1	0	1	010101	3
4	0 1 1	0	1	1	011011	4
5	1 0 0	0	1	1	100011	3
6	1 0 1	1	0	1	101101	4
7	1 1 0	1	1	0	110110	4
8	1 1 1	0	0	0	111000	3

Minimum Distance $d_{min}=3$

Parity check matrix

- To check for errors in a (n,k) linear code, we use an (n-k)×n parity check matrix H of the code
- The parity check matrix H has an important property that

$$XH^T = 0$$

- There is another way of expressing the relationship between the message bits and the parity bits of a linear block codes. Let H denote an (n-k)×n matrix defined as

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

Where P^T = (n-k)×k matrix representing the transpose of the coefficient matrix P

I_{n-k} = (n-k)×(n-k) identity matrix

Parity Check Matrix

Parity Check matrix $H = [P^T : I_q]_{qxn}$

P^T is the transpose of P parity matrix where

$$P = \begin{bmatrix} P_{11} & P_{12} & P_{13} & \dots\dots P_{1q} \\ P_{21} & P_{22} & P_{23} & \dots\dots P_{2q} \\ & & \vdots & \\ P_{k1} & P_{k2} & P_{k3} & \dots\dots P_{kq} \end{bmatrix}$$

$$P^T = \begin{bmatrix} P_{11} & P_{21} & P_{23} & \dots\dots P_{k1} \\ P_{12} & P_{22} & P_{33} & \dots\dots P_{k2} \\ & & \vdots & \\ P_{1q} & P_{2q} & P_{3q} & \dots\dots P_{kq} \end{bmatrix}$$

Parity Check Matrix

$H = [P^T : I_q]$

$$\begin{bmatrix} P_{11} & P_{21} & P_{23} & \ldots\ldots P_{k1} : 1\ 0\ 0 \ldots\ldots 0 \\ P_{12} & P_{22} & P_{33} & \ldots\ldots P_{k2} : 0\ 1\ 0 \ldots\ldots 0 \\ & & & \vdots \\ P_{1q} & P_{2q} & P_{3q} & \ldots\ldots P_{kq} : 0\ 0\ 0 \ldots\ldots 1 \end{bmatrix}$$

If Generator matrix G is given, Parity check matrix H can be obtained and vice versa

Question

For a systematic (6,3) linear block code, the parity matrix P is given by

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

Find parity check matrix, generator matrix and all possible code words.
Draw the encoder circuit for the system

Solution

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

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

$I_{3x3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$,,

We Know $H = [P^T \mid I_{n-k}]$

Solution

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

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

$C = MP$

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

$c_1 = m_1 \oplus m_3$

$c_2 = m_2 \oplus m_3$

$c_3 = m_1 \oplus m_2$

	Message Vector			c_1	c_2	c_3	Complete codeword	Hamming Weight
	m_1	m_2	m_3	$m_1 \oplus m_3$	$m_2 \oplus m_3$	$m_1 \oplus m_2$		
1	0	0	0	0	0	0	000000	0
2	0	0	1	1	1	0	001110	3
3	0	1	0	0	1	1	010011	3
4	0	1	1	1	0	1	011101	4
5	1	0	0	1	0	1	100101	3
6	1	0	1	0	1	1	101011	4
7	1	1	0	1	1	0	110110	4
8	1	1	1	0	0	0	111000	3

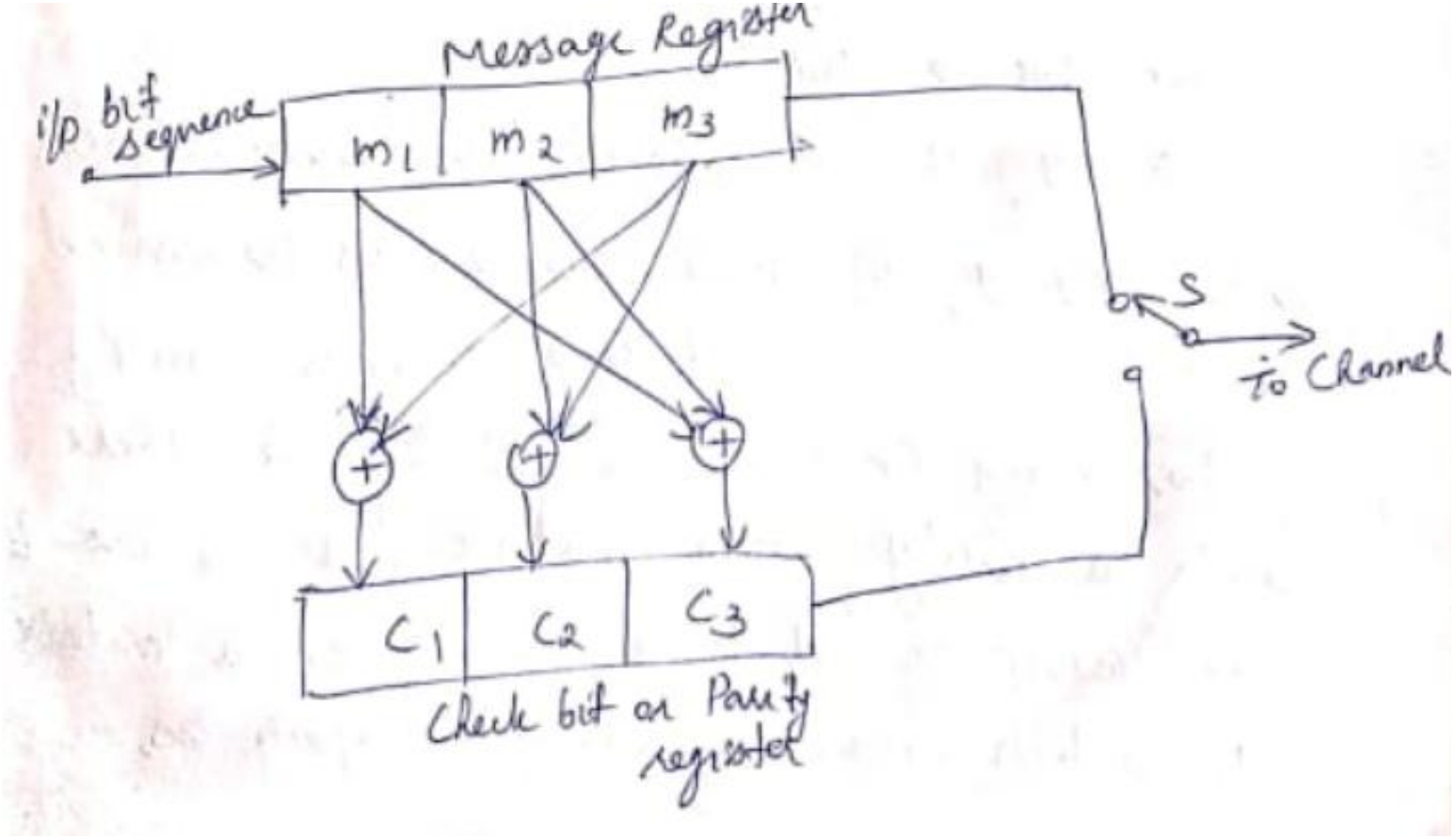
- Minimum Distance, $d_{min}=3$

Encoder Circuit

$c_1 = m_1 \oplus m_3$

$c_2 = m_2 \oplus m_3$

$c_3 = m_1 \oplus m_2$



Previous University Question

The parity bits of a (7,4) linear systematic block code are generated by

$c_5 = d_1+d_3+d_4$

$c_6=d_1+d_2+d_3$

$c_7=d_2+d_3+d_4$

(+ sign denotes modulo-2 addition)

where d_1, d_2, d_3 and d_4 are message bits and c_5, c_6, c_7 are parity bits. Find generator matrix G and parity check matrix H for this code. Draw the encoder circuit.

$$C_5 = d_1 + d_3 + d_4 \quad \text{——— (1)}$$

$$C_6 = d_1 + d_2 + d_3 \quad \text{——— (2)}$$

$$C_7 = d_2 + d_3 + d_4 \quad \text{——— (3)}$$

$C = M P$ ← Parity Matrix

↑ parity vector ↑ Message vector

$$\underset{1\times3}{\begin{bmatrix} C_5 & C_6 & C_7 \end{bmatrix}} = \underset{1\times4}{\begin{bmatrix} d_1 & d_2 & d_3 & d_4 \end{bmatrix}} \underset{4\times3}{\begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \\ P_{41} & P_{42} & P_{43} \end{bmatrix}}$$

$$C_5 = P_{11} d_1 + P_{21} d_2 + P_{31} d_3 + P_{41} d_4 \quad \text{——(4)}$$

$$C_6 = P_{12} d_1 + P_{22} d_2 + P_{32} d_3 + P_{42} d_4 \quad \text{——(5)}$$

$$C_7 = P_{13} d_1 + P_{23} d_2 + P_{33} d_3 + P_{43} d_4 \quad \text{——(6)}$$

- Compare Eqn (1) and (4)

$$P_{11} = 1, \; P_{21} = 0, \; P_{31} = 1, \; P_{41} = 1$$

- Compare Eqn (2) and (5)

$$P_{12} = 1, \; P_{22} = 1, \; P_{32} = 1, \; P_{42} = 0$$

- Compare Eqn (3) and (6)

$$P_{13} = 0, \; P_{23} = 1, \; P_{33} = 1, \; P_{43} = 1$$

- Parity Matrix

$$P = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}_{4\times 3}$$

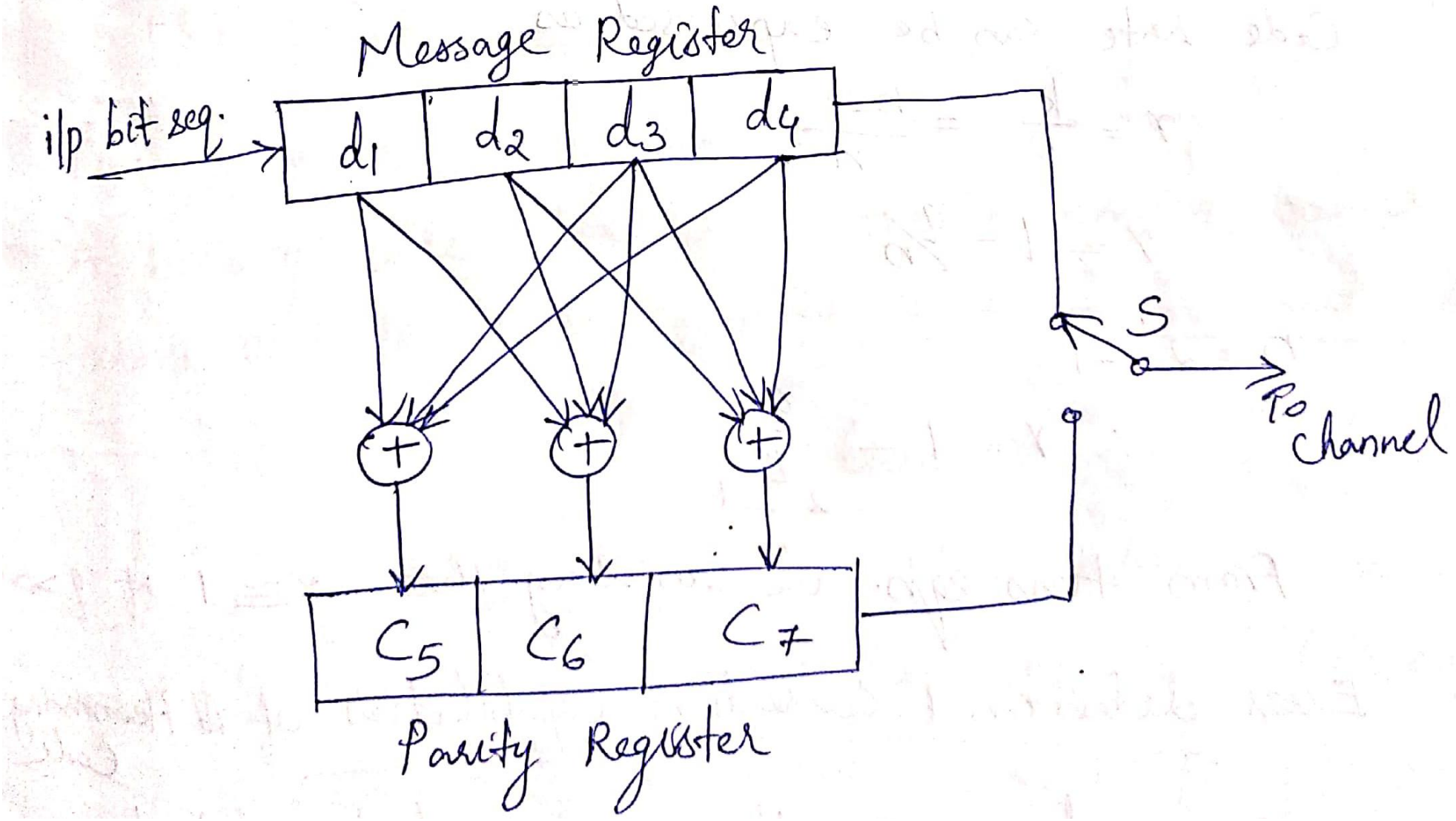
- Generator Matrix G=

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

- Parity Check Matrix

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

Encoder Circuit



Error Detecting and Correcting Capabilities of a Block Code

- For a code word with a minimum distance of d_{min} is capable of detecting all the error patterns of d_{min}-1 or fewer errors.
- A block code with minimum distance d_{min} guarantees correction of all the error patterns of $t=(d_{min}-1)/2$ or fewer errors.

Previous University Question

The parity matrix of a (6, 3) linear systematic block code is given below.

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

Find all the possible code vectors.

a) Find out the minimum distance of the code.

b) How many errors can be detected and corrected by this code?

Solution:

a)

$$[C_1 \quad C_2 \quad C_3] = [m_1 \quad m_2 \quad m_3] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$C_1 = m_1 \oplus m_2$$

$$C_2 = m_2 \oplus m_3$$

$$C_3 = m_1 \oplus m_3$$

m_1	m_2	m_3	c_1	c_2	c_3	Code word	Weight
0	0	0	0	0	0	000000	0
0	0	1	0	1	1	001011	3
0	1	0	1	1	0	010110	3
0	1	1	1	0	1	011101	4
1	0	0	1	0	1	100101	3
1	0	1	1	1	0	101110	4
1	1	0	0	1	1	110011	4
1	1	1	0	0	0	111000	3

b)

Minimum distance, d_{min} =3

No of errors can be detected= d_{min} -1 = 3-1=2

No.of errors can be corrected=(d_{min} -1)/2 = (3-1)/2 =1

Example 3. Consider the $(5, 2)$ block code with codewords $(1, 1, 0, 0, 1)$, $(1, 0, 1, 1, 1)$, $(0, 1, 1, 1, 0)$, and $(0, 0, 0, 0, 0)$.

1. Is the code linear?

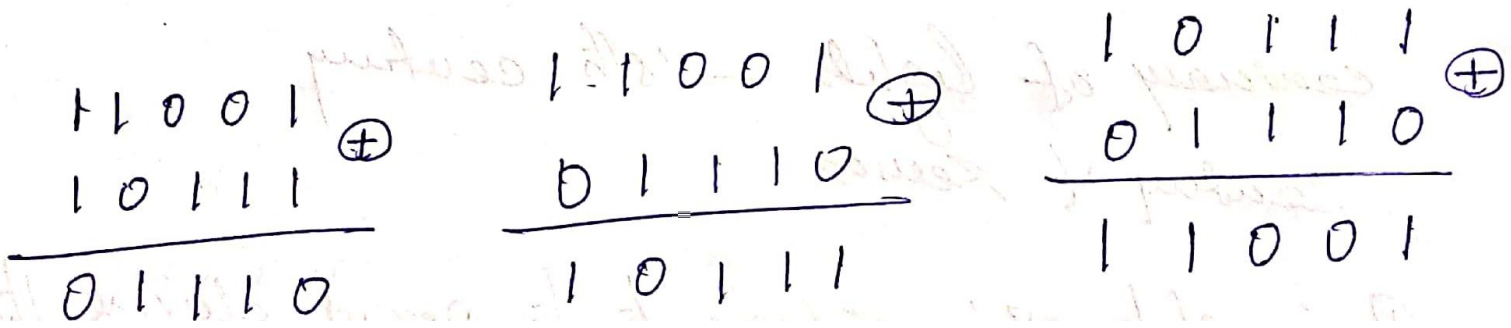
2. What is the rate of the code?

3. What is the minimum distance of the code, $d_{\min}$?

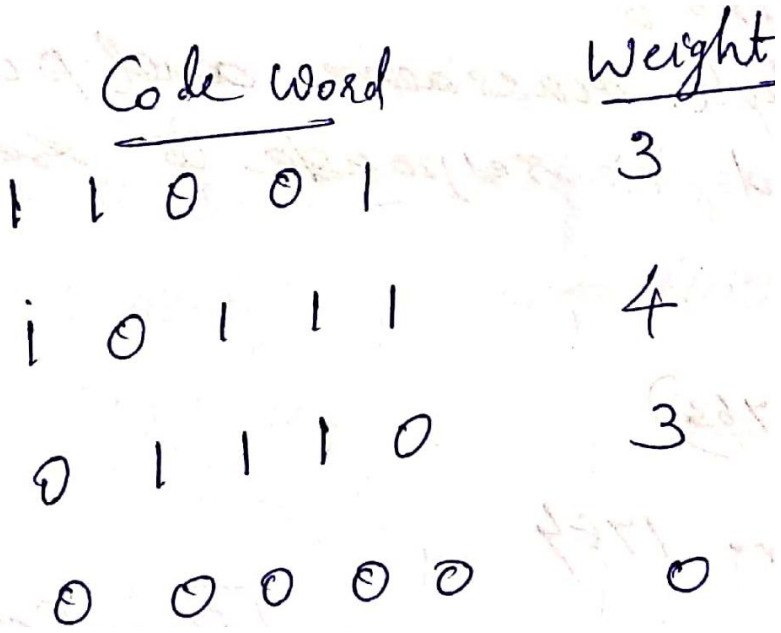
4. Find a generator matrix for the code.

Solution:

1. Code is linear



2. Rate of the code, r=k/n=2/5
3. d_{min} =3



4)

Code word	m_1	m_2	c_1	c_2	c_3
1 1 0 0 1	1	1	0	0	1
1 0 1 1 1	1	0	1	1	1
0 1 1 1 0	0	1	1	1	0
0 0 0 0 0	0	0	0	0	0

$$[X]_{1\times n} = [M]_{1\times k}[G]_{k\times n} = [M]\begin{bmatrix} 1 & 0 & P_{11} & P_{12} & P_{13} \\ 0 & 1 & P_{21} & P_{22} & P_{23} \end{bmatrix}_{2\times 5}$$

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & P_{11} & P_{12} & P_{13} \\ 0 & 1 & P_{21} & P_{22} & P_{23} \end{bmatrix}$$

$$
\left.\begin{aligned}
0 &= P_{11} \oplus P_{21} \\
0 &= P_{12} \oplus P_{22} \\
1 &= P_{13} \oplus P_{23}
\end{aligned}\right\} \longrightarrow (1)
$$

$$
\begin{bmatrix} 1 & 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & P_{11} & P_{12} & P_{13} \\ 0 & 1 & P_{21} & P_{22} & P_{23} \end{bmatrix}
$$

$$
\begin{aligned}
1 &= P_{11} \oplus 0 \cdot P_{21} \\
1 &= P_{12} \oplus 0 \cdot P_{22} \\
1 &= P_{13} \oplus 0 \cdot P_{23}
\end{aligned}
\qquad
\begin{aligned}
1 &= P_{11} \oplus 0 \\
1 &= P_{12} \oplus 0 \\
1 &= P_{13} \oplus 0
\end{aligned}
\qquad \Longrightarrow
\left.\begin{aligned}
P_{11} &= 1 \\
P_{12} &= 1 \\
P_{13} &= 1
\end{aligned}\right\} \longrightarrow (2)
$$

Substitute (2) in (1)

$$0 = 1 \oplus P_{21} \Rightarrow P_{21} = 1$$

$$0 = 1 \oplus P_{22} \Rightarrow P_{22} = 1$$

$$1 = 1 \oplus P_{23} \Rightarrow P_{23} = 0$$

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

Linear Block Codes-Decoding

Syndrome Decoding : Method to correct errors

- Let the transmitted code vector be ‘X’
- Corresponding received code vector be ‘Y’
- X=Y, if there is no transmission error
- X≠Y, if there are errors produced during transmission
- For every (n,k) linear block code, the parity check matrix has the property

$$XH^T = (0,0,0.....,0)$$

- Here X belongs to the valid code vector at the transmitter end.
- At the received end the received code vector is Y.

Linear Block Codes-Decoding

- $YH^T = (0,0,0.....,0)$, If X=Y, ie, no errors or Y is a valid code vector
- $YH^T = nonzero$, if X≠Y, ie, there is some errors.
- The non zero output of the product YH^T is called **Syndrome**.
- Syndrome is used to detect errors in Y.
- It is represented by S and $S = YH^T$
- The Syndrome depends on error pattern only.

$$\boldsymbol{Y = X \oplus E} \qquad \boldsymbol{S = (X \oplus E)H^T}$$

$$\boldsymbol{X = Y \oplus E} \qquad \boldsymbol{S = XH^T \oplus EH^T}$$

$$\boldsymbol{S = YH^T} \qquad \boldsymbol{S = EH^T}$$

Linear Block Codes-Decoding

Error Correction Using Syndrome Vector

- Let the transmitted code vector be X=(1 0 0 1 1 1 0)
- Let there be an error in the third bit of received code vector Y.
- Then Y will be , Y =(1 0 1 1 1 1 0)
- At the receiver, the syndrome decoder calculate the syndrome S of each received code vector using the relation

$$S = YH^T$$

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

We get, S=[1 1 0]

Linear Block Codes-Decoding

- On comparing this syndrome S with H^T we observe that S=(1 1 0) is the third row of H^T
- This shows that there is an error in the third bit of Y.
- The syndrome decoder will correct this error by adding error vector E with the received vector Y.

$$\boldsymbol{X = Y \oplus E}$$

- The syndrome decoder will select the error vector from a look up table.

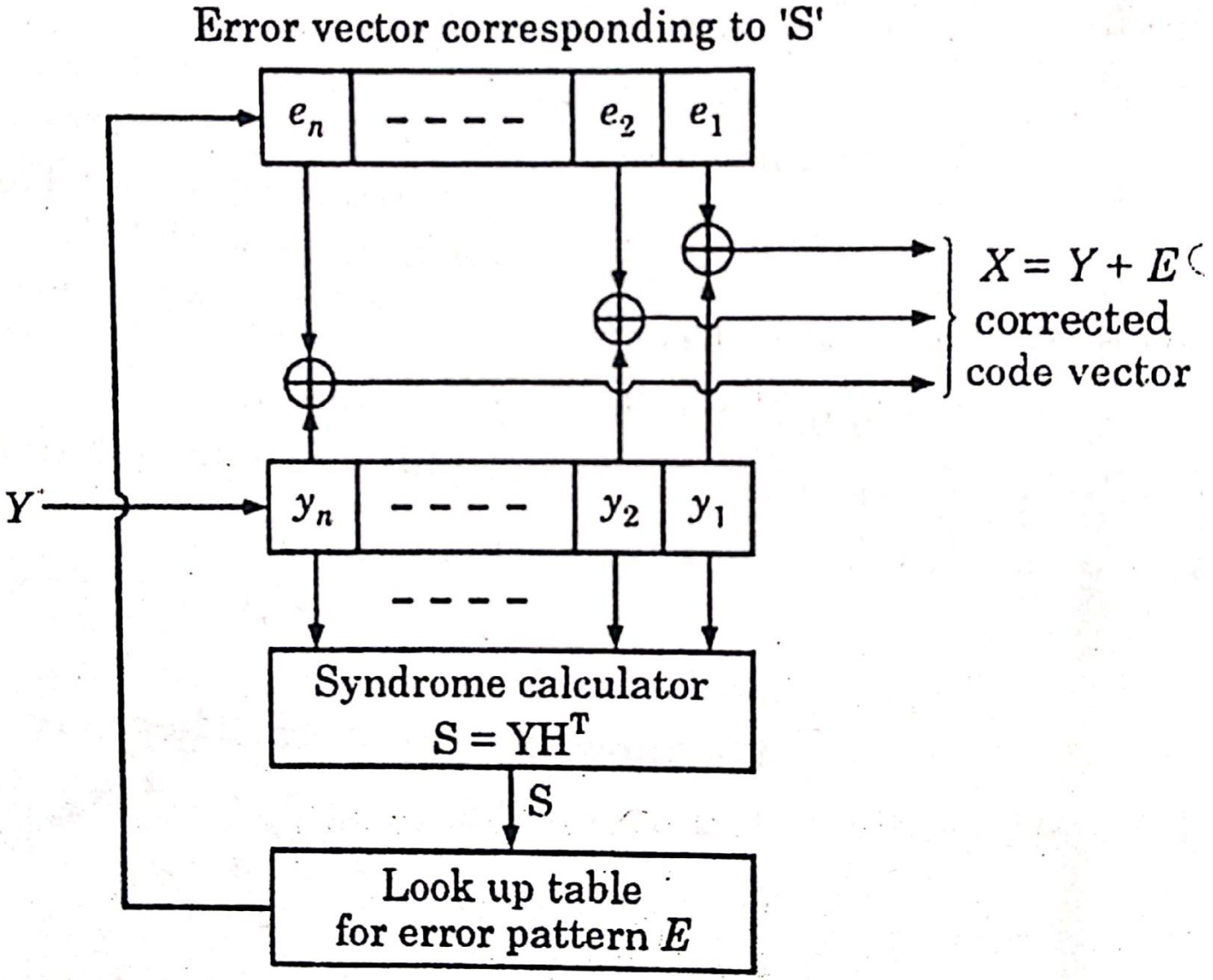
So the corrected vector is

$$\begin{array}{r} 1\,0\,1\,1\,1\,1\,0 \\ \oplus\ 0\,0\,1\,0\,0\,0\,0 \\ \hline 1\,0\,0\,1\,1\,1\,0 \end{array}$$

Single bit error pattern of 7-bit error vector

Bit in Error	Error Vector (E) - Single Bit						
1	1	0	0	0	0	0	0
2	0	1	0	0	0	0	0
3	0	0	1	0	0	0	0
4	0	0	0	1	0	0	0
5	0	0	0	0	1	0	0
6	0	0	0	0	0	1	0
7	0	0	0	0	0	0	1

Syndrome Decoder for Linear Block Code (Table look up decoding)



Previous University Question

The parity matrix for a (7,4) linear block code is given below:

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

i) Find generator and parity check matrices

ii) Draw the encoder circuit.

iii) Sketch the syndrome calculation circuit

iv) Illustrate the decoding of the received vector corresponding to the message vector 1001, if it is received with 5th bit in error.

Solution:

Generator Matrix $G = [I_k : P_{k \times (n-k)}]_{k \times n}$

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{4 \times 7}$$

Parity check Matrix, $H = [P^T : I]_{q \times n}$

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

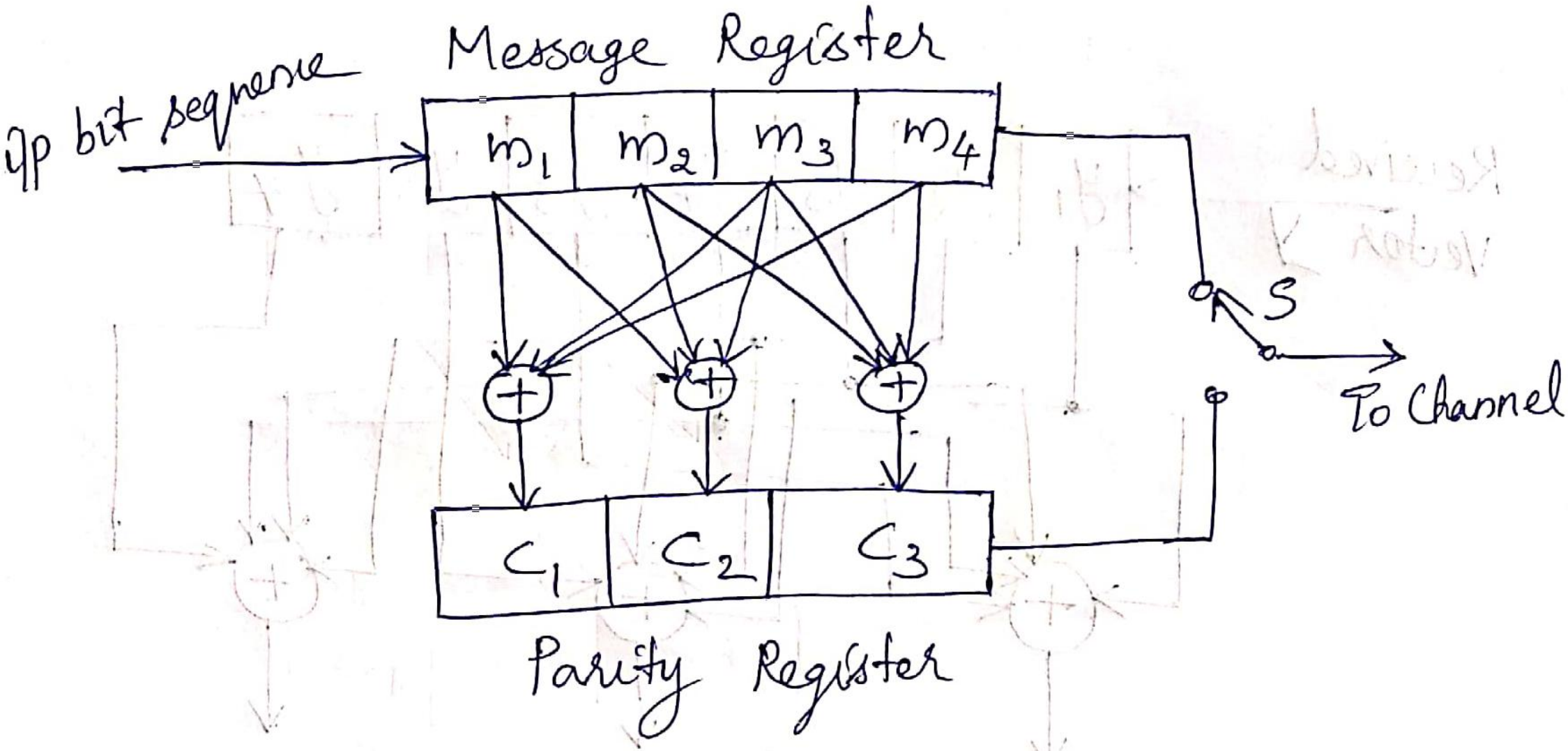
$$C = MP$$

$$\begin{bmatrix} c_1 & c_2 & c_3 \end{bmatrix} = \begin{bmatrix} m_1 & m_2 & m_3 & m_4 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$c_1 = m_1 \oplus m_3 \oplus m_4$$

$$c_2 = m_1 \oplus m_2 \oplus m_3$$

$$c_3 = m_2 \oplus m_3 \oplus m_4$$



Encoder Circuit

Syndrome, $S = YH^T$

In vector form $S = [S_1 \; S_2 \; \cdots \; S_{n-k}]$

$$Y = [y_1 \; y_2 \; \cdots \; y_n]$$

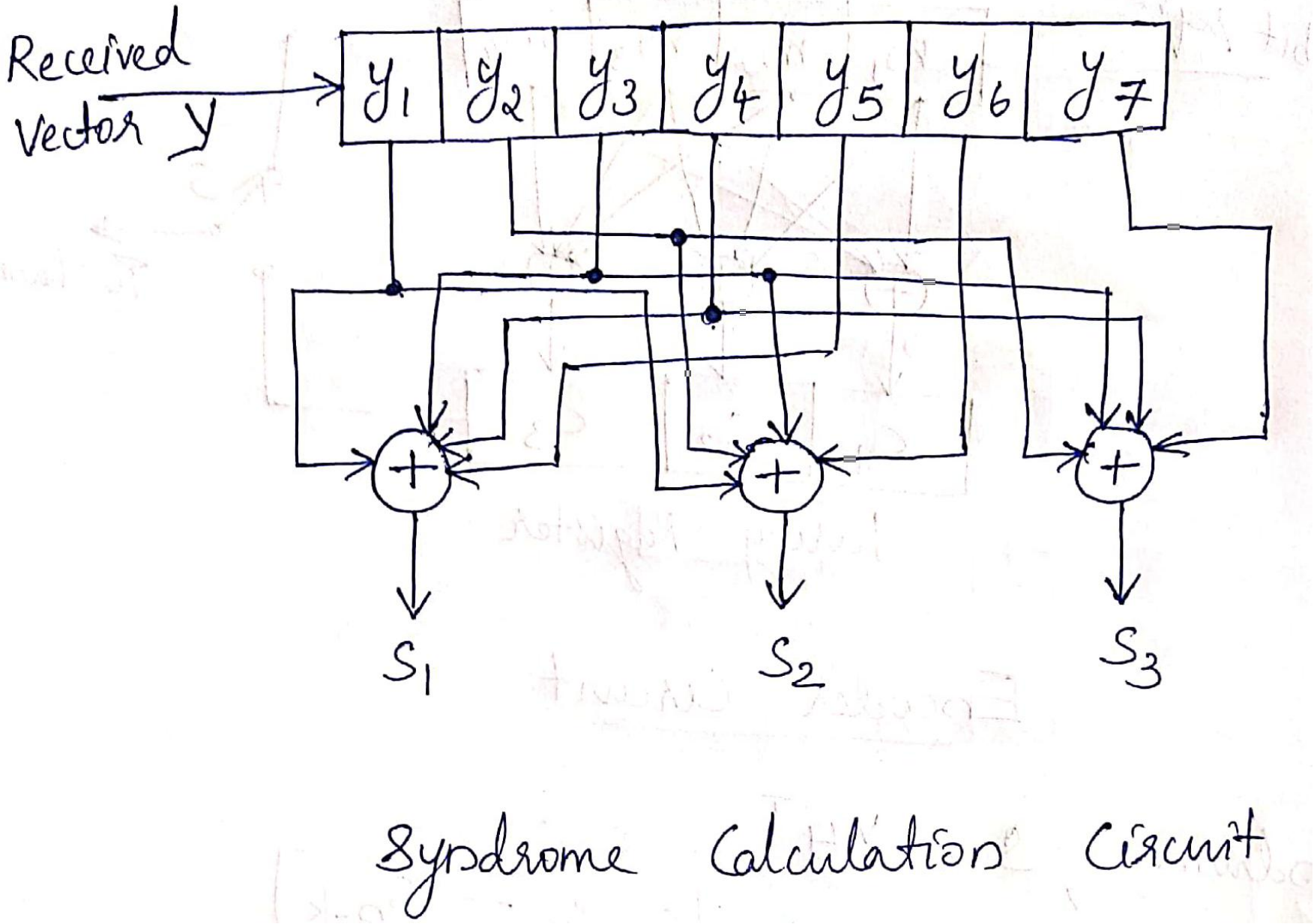
$$\therefore [S_1 \; S_2 \; \cdots \; S_{n-k}] = [y_1 \; y_2 \; \cdots \; y_n] H^T$$

$$[S_1 \; S_2 \; S_3] = [y_1 \; y_2 \; y_3 \; y_4 \; y_5 \; y_6 \; y_7] \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S_1 = y_1 \oplus y_3 \oplus y_4 \oplus y_5$$

$$S_2 = y_1 \oplus y_2 \oplus y_3 \oplus y_6$$

$$S_3 = y_2 \oplus y_3 \oplus y_4 \oplus y_7$$



Syndrome Calculation Circuit

Code vector $X = MG$

$$= \underbrace{\begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}}_{1\times 4} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}}_{4\times 7}$$

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

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

5^{th} bit error

Received vector

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

$$S = y H^T$$

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

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

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

When comparing syndrom vector with H^T we can observe that $S = [1\ 0\ 0]$ is the 5^{th} row of H^T. This shows that there is an error in the 5^{th} bit of Y.

So the corrected vector $X = Y \oplus E$

$$\begin{array}{r} 1\ 0\ 0\ 1\ 1\ 1\ 1 \\ 0\ 0\ 0\ 0\ 1\ 0\ 0 \\ \hline 1\ 0\ 0\ 1\ 0\ 1\ 1 \end{array} \quad \oplus$$

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

Table Look up Decoding(Syndrome Decoding) Using the Standard Array

- Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^k}$ be the code vector of C
- Any decoding scheme used at the receiver is a rule to partition the 2^n possible received vectors into 2^k disjoint subsets $D_1, D_2, \ldots, D_{2^k}$ such that the code vector $\mathbf{v}_i$ is contained in the subset D_i for $1 \leq i \leq 2^k$
- Each subset D_i is one-to-one correspondence to a code vector $\mathbf{v}_i$
- If the received vector $\mathbf{r}$ is found in the subset D_i, $\mathbf{r}$ is decoded into $\mathbf{v}_i$
- Correct decoding is made if and only if the received vector $\mathbf{r}$ is in the subset D_i that corresponds to the actual code vector transmitted

- The subset D_i is called the "CO-SET" of the code.
- A coset contains exactly 2^k elements that differ almost by a code vector.
- Thus we can conclude that for a (n,k) linear block code, there are 2^{n-k} co-sets.

Co-set Leader

- The vector having the minimum weight in a co-set is called the co-set leader.
- If there are more than one vector with the minimum weight, one of them is chosen at random and is declared the co-set leader.

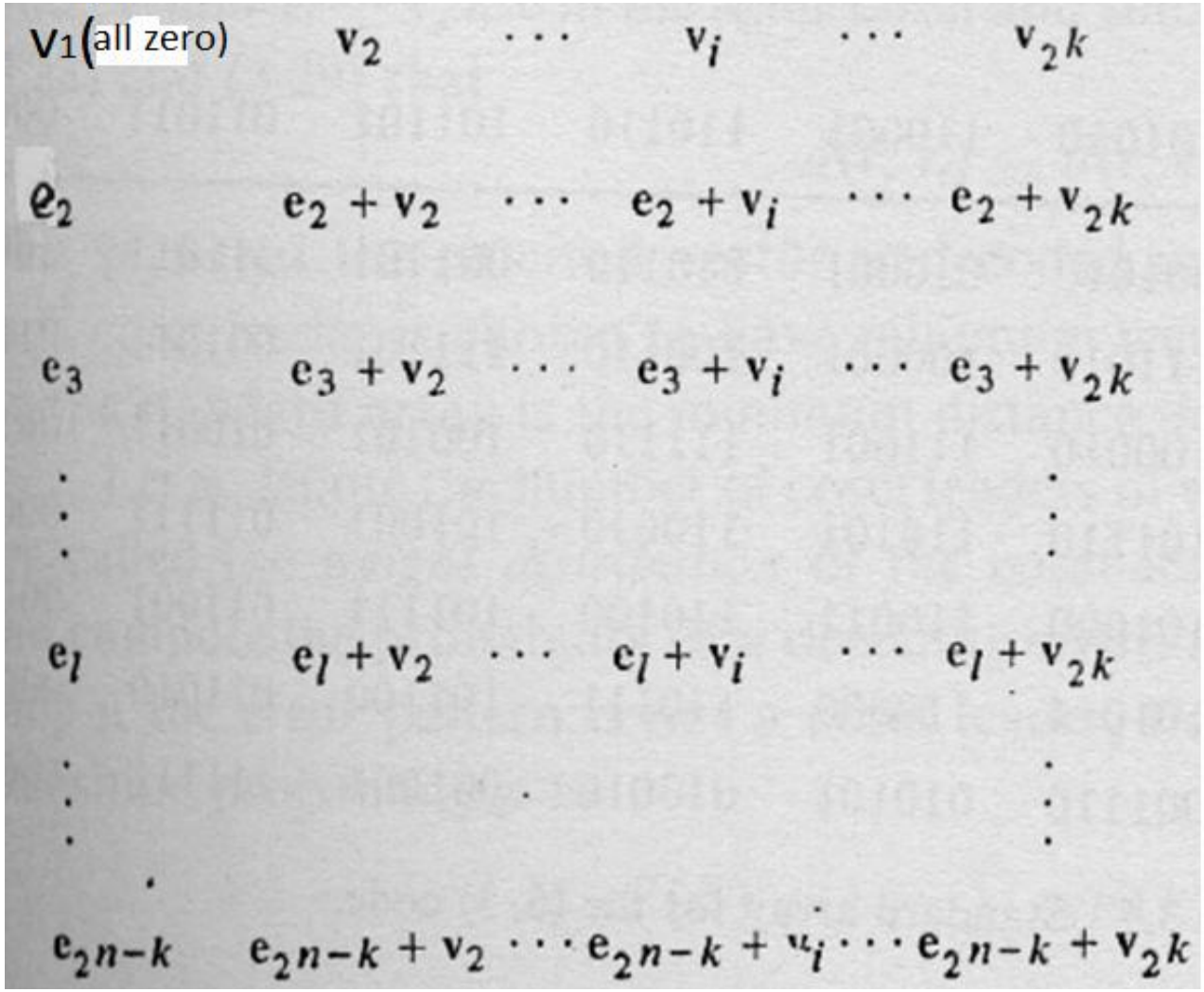
Standard Array

- Standard array for an (n,k) code C is a 2^{n-k} x 2^k array, in which
- The first row consists of the code C (with all zero code word on the extreme left) and
- The other rows are the co-sets e_i+C , each arranged in corresponding order, with the co-set leader on the left.

Steps form Standard Array

- A method to partition the 2^n possible received vectors into 2^k disjoint subsets such that each subset contains one and only one code vector is described here
  - First, the 2^k code vectors of C are placed in a row with the all-zero code vector $\mathbf{v}_1 = (0, 0, \ldots, 0)$ as the first (leftmost) element
  - From the remaining $2^n - 2^k$ n-tuple, an n-tuple $\mathbf{e}_2$ is chosen and is placed under the zero vector $\mathbf{v}_1$
  - Now, we form a second row by adding $\mathbf{e}_2$ to each code vector $\mathbf{v}_i$ in the first row and placing the sum $\mathbf{e}_2 + \mathbf{v}_i$ under $\mathbf{v}_i$
  - An unused n-tuple $\mathbf{e}_3$ is chosen from the remaining n-tuples and is placed under $\mathbf{e}_2$.
  - Then a third row is formed by adding $\mathbf{e}_3$ to each code vector $\mathbf{v}_i$ in the first row and placing $\mathbf{e}_3 + \mathbf{v}_i$ under $\mathbf{v}_i$.
  - we continue this process until all the n-tuples are used.

Standard Array for an (n,k) linear block code



Properties of Standard Array

- **Property 1:** Each element in the standard array is distinct and hence different columns of the array are disjoint.
- **Property 2:** The first n-tuple of each co-sets is called a co-set leader. If the error pattern caused by the channel coincides with a co-set leader, then the received vector is correctly decoded. If the error pattern, is not a co-set leader then an incorrect decoding will result. So co-set leaders are called correctable error patterns.
- **Property 3:**All the 2^k n-tuples of a co-set have the same syndrome and the syndromes of different co-sets are different.

➢ **If the received vector "r" is found in the i^{th} column, the v_i will be the corrected vector which lies on top of that column.**

Example:

Construct the standard array for the (6,3) linear block code. If the received vector r=000011, find the corrected vector.

Given that the code vectors are 000000, 001110, 010011, 011101, 100101, 101011, 110110, 111000

Standard Array

Co-set Leader							
000000	001110	010011	011101	100101	101011	110110	111000
100000	101110	110011	111101	000101	001011	010110	011000
010000	011110	000011	001101	110101	111011	100110	101000
001000	000110	011011	010101	101101	100011	111110	110000
000100	001010	010111	011001	100001	101111	110010	111100
000010	001100	010001	011111	100111	101001	110100	111010
000001	001111	010010	011100	100100	101010	110111	111001
100010	101100	110001	111111	000111	001001	010100	011010

The received vector 000011 is in third column, third row.

Therefore the corrected vector is 010011.

Previous University Question

The parity matrix of a (6,3) linearsystematic block code is given below.

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

Construct standard array.

If the received vector r=101010, find the corrected vector.

Standard Array

Coset leaders							
000000	001011	010110	011101	100101	**101110**	110011	111000
100000	101011	110110	111101	000101	001110	010011	011000
010000	011011	000110	001101	110101	111110	100011	101000
001000	000011	011110	010101	101101	100110	111011	110000
000100	001111	010010	011001	100001	**101010**	110111	111100
000010	001001	010100	011111	100011	101100	110001	111010
000001	001010	010111	011100	100100	101111	110010	111001
100010	101001	110100	111111	000111	001100	010001	011010

Corrected Vector

Received Vector

Previous University Question

Construct standard array for (6,3) systematic linear block code with generator matrix, $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$.

Check whether the received codeword, r = 010001 is erroneous? If yes, obtain the corrected codeword using standard array.

Standard Array

CorrectedVector

Co-set Leader							
000 000	001 110	010 101	011 011	100 011	101 101	110 110	111 000
000 001	001 111	010 100	011 010	100 010	101 100	110 111	111 001
000 010	001 100	010 111	011 001	100 001	101 111	110 100	111010
000 100	001 010	010 001	011 111	100 111	101 001	110 010	111 100
001 000	000 110	011 101	010 011	101 011	100 101	111 110	110 000
010 000	011 110	000 101	001 011	110 011	111 101	100 110	101 000
100 000	101 110	110 101	111 011	000 011	001 101	010 110	011 000
001 001	000 111	011 100	010 010	101 010	100 100	111 111	110 001

Previous University Question

The parity matrix for a (6,3) systematic linear block code is given by

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

(i) Find all code words. (ii) Find generator and parity check matrix. (iii) Draw encoding circuit. (iv) Draw syndrome circuit.

Previous University Question

The parity check matrix of (7,4) linear block code is given as

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

. Draw the encoder and decoder circuit of this code.

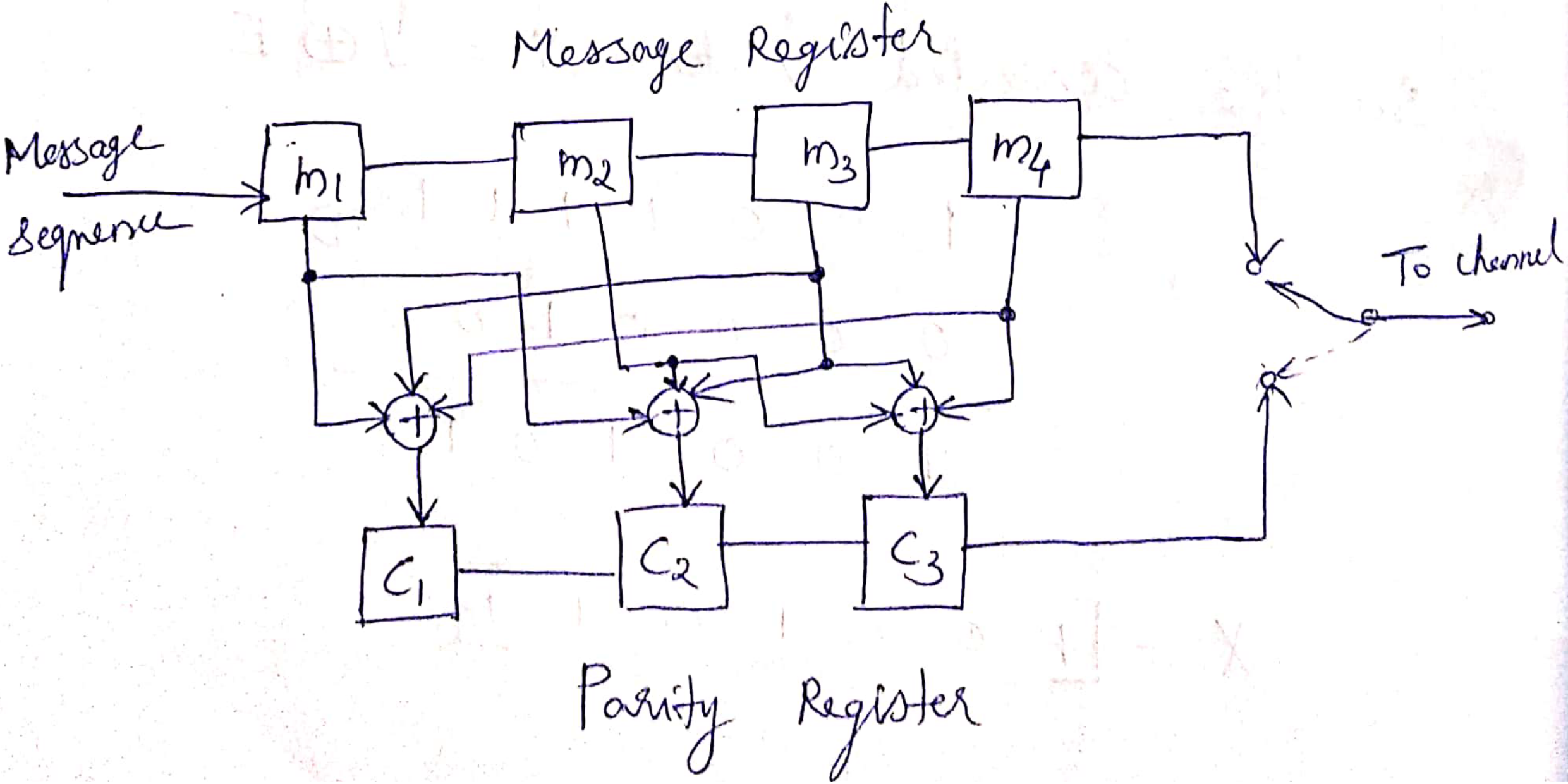
$$C = MP$$

$$[C_1 \; C_2 \; C_3] = [m_1 \; m_2 \; m_3 \; m_4] \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$C_1 = m_1 \oplus m_3 \oplus m_4$$

$$C_2 = m_1 \oplus m_2 \oplus m_3$$

$$C_3 = m_2 \oplus m_3 \oplus m_4$$


Message Register
Message Sequence
m_1
m_2
m_3
m_4
To channel
C_1
C_2
C_3
Parity Register

$$S = Y H^T$$

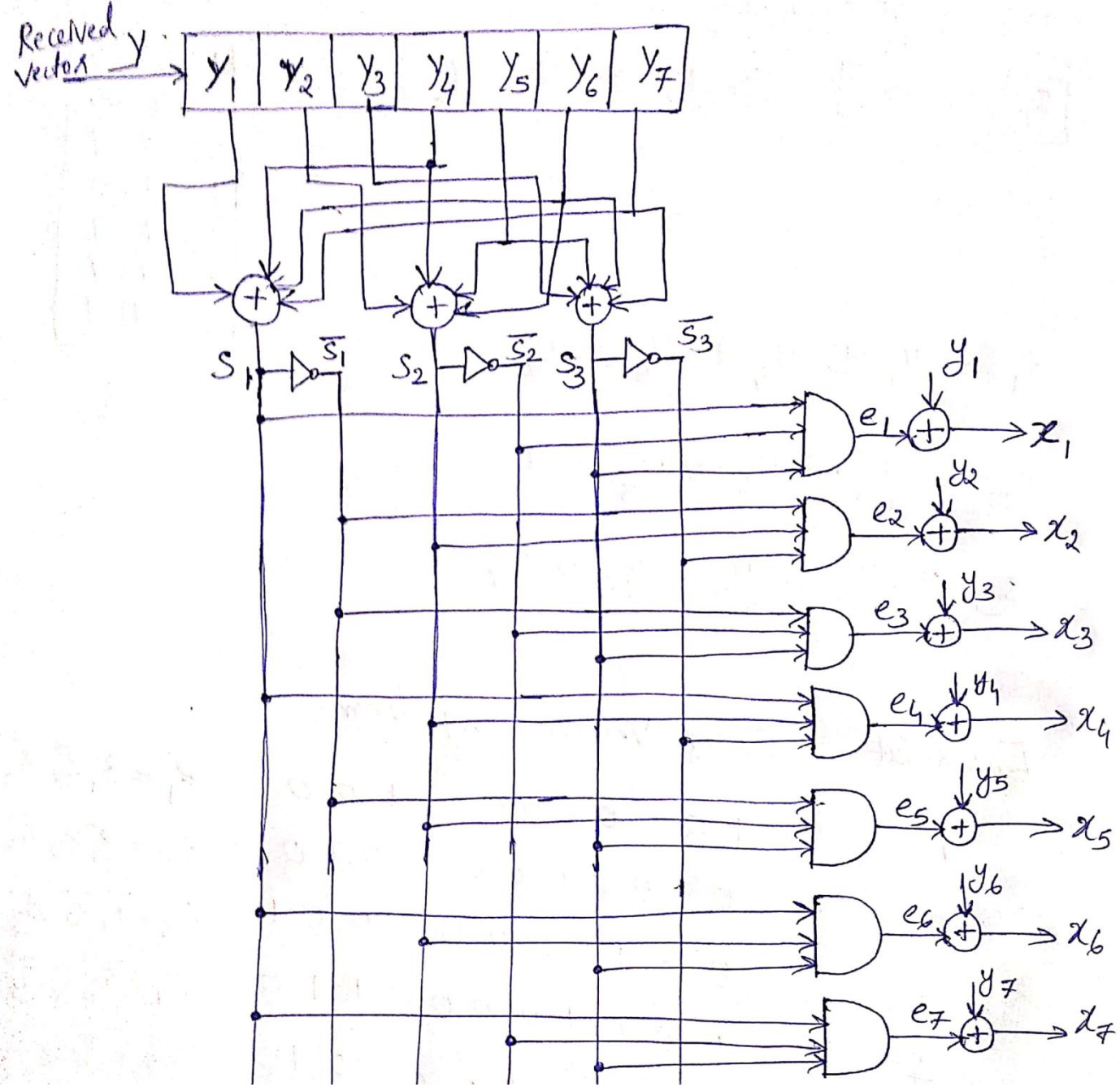
$$[S_1 \; S_2 \; S_3] = [y_1 \; y_2 \; y_3 \; y_4 \; y_5 \; y_6 \; y_7] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$S_1 = y_1 \oplus y_4 \oplus y_6 \oplus y_7$$

$$S_2 = y_2 \oplus y_4 \oplus y_5 \oplus y_6$$

$$S_3 = y_3 \oplus y_5 \oplus y_6 \oplus y_7$$

Error Bit	Error Vector	Syndrome	
1	1 0 0 0 0 0 0 0	1 0 0	$e_1 = S_1 \overline{S_2}\,\overline{S_3}$
2	0 1 0 0 0 0 0 0	0 1 0	$e_2 = \overline{S_1} S_2 \overline{S_3}$
3	0 0 1 0 0 0 0 0	0 0 1	$e_3 = \overline{S_1}\,\overline{S_2} S_3$
4	0 0 0 1 0 0 0	1 1 0	$e_4 = S_1 S_2 \overline{S_3}$
5	0 0 0 0 1 0 0	0 1 1	$e_5 = \overline{S_1} S_2 S_3$
6	0 0 0 0 0 1 0	1 1 1	$e_6 = S_1 S_2 S_3$
7	0 0 0 0 0 0 1	1 0 1	$e_7 = S_1 \overline{S_2} S_3$


Received vector y
y_1 y_2 y_3 y_4 y_5 y_6 y_7
s_1 $\bar{s}_1$ s_2 $\bar{s}_2$ s_3 $\bar{s}_3$
e_1 e_2 e_3 e_4 e_5 e_6 e_7
x_1 x_2 x_3 x_4 x_5 x_6 x_7