Algebraic Structures

SY Odd 2021-22

Syllabus

Algebraic Structures 11 CO4

7.1 Algebraic structures with one binary operation: semigroup, monoids and groups

7.2 Cyclic groups, Normal subgroups

7.3 Hamming Code ,Minimum Distance

7.4 Group codes ,encoding-decoding techniques

7.5 Parity check Matrix ,Maximum Likelihood

7.6 **Mathematics of Cryptography** - Modular Arithmetic, Matrices, Linear Congruence, GF Fields, Primes and Related Congruence Equations- Primes, Primality Testing, Factorization, Quadratics Congruence, Chinese reminder theorem, Exponentiation and Logarithm.

Algebraic systems

- **N = {1,2,3,4,…..∝ } = Set of all natural numbers.**

  Z = { 0, ± 1, ± 2, ± 3, ± 4 , ….. ∝} = Set of all integers.

  Q = Set of all rational numbers, R = Set of all real numbers.

- **Binary Operation:** The binary operator * is said to be a binary operation (closed operation) on a non empty set A, if

  $a * b \in A$ for all $a, b \in A$ (Closure property).

  Ex: The set N is closed with respect to addition and multiplication

  but not w.r.t subtraction and division.

- **Algebraic System:** A set 'A' with one or more binary(closed) operations defined on it is called an algebraic system.

  Ex: (N, +), (Z, +, –), (R, +, . , –) are algebraic systems.

Properties

- **Commutative:** Let * be a binary operation on a set A.

  The operation * is said to be commutative in A if

  a * b= b * a for all a, b in A

- **Associativity:** Let * be a binary operation on a set A.

  The operation * is said to be associative in A if

  (a * b) * c = a *(b * c) for all a, b, c in A

- **Idempotent :** Let * be a binary operation on a set A.

  The operation * is said to be idempotent in A if

  a * a = a

Semi group

Semi Group: An algebraic system (A, *) is said to be a semi group if

1. * is closed operation on A.

2. * is an associative operation, for all a, b, c in A.

- Ex. (N, +) is a semi group.
- Ex. (N, .) is a semi group.

The semigroup (A, ∗) is said to be commutative if ∗ is a commutative operation.

- The set P(S) where S is a set, together with the operation of union is a commutative semigroup.
- The set Z with the binary operation of subtraction is not a semigroup, since subtraction is not associative.

- The set P(S) where S is a set, together with the operation of union is a commutative semigroup
- S={1,2}
- P(S)={nullset, {1},{2},{1,2}}
- (p(s),union)=closed? Yes

  Associative? Yes ---Semigroup

  for any a,b belonging to P(S)

  a union b =b union a

  Commutative semigroup

Left Identity

- Let (A, ∗) be an algebraic system where ∗ is a binary operation on A. An element in A, e, is said to be a **left identity** if for all x in A, e ∗ x = x. For example for the algebraic system shown in Fig. both β and δ are left identifies.

$$\beta * \alpha = \alpha \qquad \delta * \alpha = \alpha$$
$$\beta * \beta = \beta \qquad \delta * \beta = \beta$$
$$\beta * \gamma = \gamma \qquad \delta * \gamma = \gamma$$
$$\beta * \delta = \delta \qquad \delta * \delta = \delta$$

*	α	β	γ	δ
α	δ	α	β	γ
β	α	β	γ	δ
γ	α	β	γ	γ
δ	α	β	γ	δ

Right Identity

An element in A, e is said to a **right identity** if for all x in A. $x * e = x$. For example, for the algebraic system shown in Fig. α is a right identity.

$*$	α	β	γ	δ
α	α	β	δ	γ
β	β	α	γ	δ
γ	γ	δ	α	β
δ	δ	δ	β	γ

Identity

An element is said to be an **identity** if it is both a left identity and a right identity.

Let W={0,1,2,3,4,……}

Then (W, +) is an algebraic system.

Clearly 0 is the identity of the algebraic system.

Monoid

Monoid: An algebraic system (A, *) is said to be a **monoid** if the following conditions are satisfied.

1) *** is a closed operation in A.**
2) *** is an associative operation in A.**
3) **There is an identity in A.**

Monoid

- Ex. Show that the set 'N' is a monoid with respect to multiplication.

Solution: Here, N = {1,2,3,4,……}

1. Closure property : We know that product of two natural numbers is again a natural number.

i.e., $a.b \in N$ for all $a,b \in N$

$\therefore$ Multiplication is a closed operation.

2. Associativity : Multiplication of natural numbers is associative.

i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in N$

3. Identity : We have, $1 \in N$ such that

$a.1 = 1.a = a$ for all $a \in N$.

$\therefore$ Identity element exists, and 1 is the identity element.

Hence, N is a monoid with respect to multiplication.

Monoid

Example: Is (p(s),U) a monoid?

Sub-semigroup & sub-monoid

Subsemigroup : Let (S, *) be a semigroup and let **T be a subset of S.**

If T is closed under operation * , then (T, *) is called a subsemigroup of (S, *).

Ex: (N, .) is semigroup and T is set of multiples of positive integer m then (T,.) is a sub semigroup.

N={1,2,3,4,5,……..},(N,*) semigroup

T={2,4,6,8,10,12,14,……..} (T,*) sub-semigroup

Submonoid : Let (S, *) be a monoid with identity e, and let T be a non-empty subset of S. If T is closed under the operation * and e $\in$ T, then (T, *) is called a submonoid of (S, *).

(P(S),Union)-Monoid, T={null,{a},{b},{a,b}} sub-monoid

Inverse

- Let (A, *) be an algebraic system with an identity e. Let a be an element in A. An element b is said to be a **left inverse** of a if b * a = e. An element b is said to be a **right inverse** of a if a * b = e. For example for the algebraic system shown in Fig. a is an identity. So b is a left inverse of g, and d is a right inverse g

*	a	b	g	d
a	a	b	g	d
b	b	d	a	g
g	g	b	b	a
d	d	a	g	d

An element b is said to be an inverse of a, if it is both a left and a right inverse of a. Clearly if b is an inverse of a, a is also an inverse of b.

Group

- **Group:** An algebraic system (G, *) is said to be a **group** if the following conditions are satisfied.

  1) * is a closed operation.

  2) * is an associative operation.

  3) There is an identity in G.

  4) Every element in G has inverse in G.

- **Abelian group (Commutative group):** A group (G, *) is said to be ***abelian*** (or ***commutative)*** if

  $a * b = b * a$ for all a, b belongs to G.

Group

- A group (A, *) is said to be **finite group,** if A is a finite set and **infinite group**, if A is an infinite set. The size of A is often referred to as the order of the group.
- E.g. (i) The group (Z, +) is of infinite order. (ii) The group (Zm, +) is of finite order viz m.

Theorems –Self Study

- **In a Group (G, *) the following properties hold good**

1. Identity element is unique.

2. Inverse of an element is unique.

3. Cancellation laws hold good

$a * b = a * c \Rightarrow b = c$ (left cancellation law)

$a * c = b * c \Rightarrow a = b$ (Right cancellation law)

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

- In a group, the identity element is its own inverse.

Ex. Show that, the set of all integers is an abelian group with respect to **addition**.

Solution: Let Z = set of all integers. Let a, b, c are any three elements of Z.

1. **Closure property** : We know that, Sum of two integers is again an integer.

   i.e., $a + b \in Z$ for all $a,b \in Z$

2. **Associativity**: We know that addition of integers is associative.

   i.e., $(a+b)+c = a+(b+c)$ for all $a,b,c \in Z$.

3. **Identity** : We have $0 \in Z$ and $a + 0 = a$ for all $a \in Z$.

   $\therefore$ Identity element exists, and '0' is the identity element.

4. **Inverse**: To each $a \in Z$, we have $-a \in Z$ such that

   $a + (-a) = 0$ Each element in Z has an inverse

5. **Commutativity:** We know that addition of integers is commutative.

   i.e., $a + b = b + a$ for all $a,b \in Z$.

Hence, (Z , +) is an abelian group.

Ex. Show that set of all non zero real numbers is a group with respect to multiplication .

Solution: Let R^* = set of all non zero real numbers.

Let a, b, c are any three elements of R^* .

1. Closure property : We know that, product of two nonzero real numbers is again a nonzero real number .

   i.e., $a \cdot b \in R^*$ for all $a,b \in R^*$.

2. Associativity: We know that multiplication of real numbers is associative.

   i.e., $(a.b).c = a.(b.c)$ for all $a,b,c \in R^*$.

3. Identity : We have $1 \in R^*$ and $a \cdot 1 = a$ for all $a \in R^*$.

   $\therefore$ Identity element exists, and '1' is the identity element.

4. Inverse: To each $a \in R^*$, we have $1/a \in R^*$ such that

   $a \cdot (1/a) = 1$ i.e., Each element in R^* has an inverse.

5. Commutativity: We know that multiplication of real numbers is commutative.

   i.e., $a \cdot b = b \cdot a$ for all $a,b \in R^*$.

Hence, (R^* , .) is an abelian group.

Ex. Determine whether the set Z together with the binary operation a*b where a * b = a + b – ab is a semigroup, a monoid or neither. Also determine if it is commutative.

(c) Get set Z is set of integers

(i) For any $a, b \in Z, a * b \in Z$,

So set Z is closed under binary operation *.

(ii) Now check for associativity

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

$(a + b – ab) * c = a * (b + c – bc)$

$a + b – ab + c – (a + b – ab)\, c = a + b + c – bc – a\,(b + c – bc)$

$a + b – ab + c – (ac + bc – abc) = a + b + c – bc – (ab + ac – abc)$

$a + b – ab + c – ac – bc + abc = a + b + c – bc – ab - ac + abc$

* is associative operation

∴ Algebraic system (Z, *) is semigroup

(iii) Now check for identity

$$a * 0 = a + 0 - a * 0$$

$$= a$$

$\therefore$ '0' is identity element

$\therefore$ Algebraic system $(Z, *)$ is monoid

(iv) and $a * b = a + b - ab$

$b * a = b + a - ba$

$\therefore\ a * b = b * a$

$\therefore$ It is commutative operation.

Modulo systems

Addition modulo m ($+_m$)

let m be a positive integer. For any two positive integers a and b

$a +_m b = a + b$ if $a + b < m$

$a +_m b = r$ if $a + b \geq m$ where r is the remainder obtained by dividing (a+b) with m.

Ex. $14 +_6 8 = 22 \% 6 = 4$

Ex. $9 +_{12} 3 = 12 \% 12 = 0$

Multiplication modulo p ($\times_p$)

let p be a positive integer. For any two positive integers a and b

$a \times_p b = a\,b$ if $a\,b < p$

$a \times_p b = r$ if $a\,b \geq p$ where r is the remainder obtained by dividing (ab) with p.

Ex. $3 \times_5 4 = 2$, $5 \times_5 4 = 0$, $2 \times_5 2 = 4$

Ex. : Show that the set G = {0,1,2,3,4,5} is a group with respect to addition modulo 6.

Solution: The composition table of G is

$+_6$	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

1. **Closure property**: Since all the entries of the composition table are the elements of the given set, the set G is closed under $+_6$.

Contd.,

$+_6$	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

2. Associativity: The binary operation $+_6$ is associative in

for ex. $(2 +_6 3) +_6 4 = 5 +_6 4 = 3$ and

$2 +_6 (3 +_6 4) = 2 +_6 1 = 3$

3. Identity : 0 is the identity element.

4. . Inverse: From the composition table, we see that the inverse elements of

0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively.

5. Commutativity: The corresponding rows and columns of the table are

identical. Therefore the binary operation $+_6$ is commutative.

Hence, $(G, +_6)$ is an abelian group.

Ex. : Show that the set G = {1,2,3,4,5,6} is a group with respect to multiplication modulo 7.

Solution: The composition table of G is

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1. Closure property: Since all the entries of the composition table are the elements of the given set, the set G is closed under $\times_7$.

Contd.,

2. Associativity: The binary operation $\times_7$ is associative in G.

for ex. $(2 \times_7 3) \times_7 4 = 6 \times_7 4 = 3$ and

$2 \times_7 (3 \times_7 4) = 2 \times_7 5 = 3$

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

3. Identity : 1 is the identity element.

4. . Inverse: From the composition table, we see that the inverse elements of 1, 2, 3, 4. 5 ,6 are 1, 4, 5, 2, 3, 6 respectively.

5. Commutativity: The corresponding rows and columns of the table are identical. Therefore the binary operation $\times_7$ is commutative.

Hence, $(G, \times_7)$ is an abelian group.

Ex. : Let Z4 i.e. G = {0, 1, 2, 3}
(i)Prepare its composition table with respect to 'x4'
(ii) Is it a group ?

Let G = { 0, 1, 2, 3,}

(i) Composition table with respect to 'X4'

X4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) (a) The set G is closed under the operation X4 because all elements belongs to composition table are belong to set G.

(b) Now check for associativity for any a, b, c ∈ G

$(a \times_4 b) \times_4 C = a \times_4 (b \times_4 C)$

Let a = 1, b = 2, c = 3

$(1 \times_4 2) \times_4 3 = 1 \times_4 (2 \times_4 3)$

$2 \times_4 3 = 1 \times_4 2$

$2 = 2$

'X4' is an associative operation.

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(c) For any element a in set A

$1 \times_4 a = a \times_4 1 = a$ that is

$0 \times_4 1 = 1 \times_4 0 = 0$

$1 \times_4 1 = 1 \times_4 1 = 1$

$2 \times_4 1 = 1 \times_4 2 = 2$

$3 \times_4 1 = 1 \times_4 3 = 3$

∴ '1' is identity element.

- Inverse of 1 is 1
- Inverse of 3 is 3
- 0 and 2 do not have inverse.

X_4	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- SO, (G, ×4) is not a group.

Cyclic group

- A **cyclic group** is a group that can be generated by a single element.
- Every element of a cyclic group is a power of some specific element which is called a **generator**.
- A cyclic group can be generated by a generator ‘g’, such that every other element of the group can be written as a power of the generator ‘g’.

Subgroup

Let (A, *) be a group and B be a subset of A, (B, *) is said to be a **subgroup** of A if (B, *) is also a group by itself. Suppose we want to check whether (B, *) is a subgroup for a given subset B of A. We note that

1. We should test whether * is a closed operation on B.
2. * is known to be an associative operation.
3. The identity of (A, *) must be in B as the identity of (B, *)
4. Since the inverse of every element in A is unique for every element b in B, we must check that its inverse is also in B.

Generation of Subgroups

Let (G, *) be a group and let S be a non-empty subset of G. Then the subgroup generated by S, denoted by $< S >$ is defined as

(i)If x is an element of S, then x is also an element of $< S >$.

(ii) (a)if x is in $< S >$, then x^{-1} is also in $< S >$

(b)if x and y are in $< S >$ then $x * y$ is also in $< S >$

(iii) Only elements obtained by a finite number of iterations of (a) and (b) are in $< S >$.

Step (i) : Guarantees that the set S is contained in $< S >$

Step (ii) : Guarantees that $< S >$ is a subgroup of G.

Ex. : Generate subgroup by 2 in (Z, +). For set (Z, +) identity element is '0'.

Soln. :

Set	S	=	{2}
Since	2	$\in$	S, $2 \in < S >$
	2	$\in$	$< S >$
$\therefore$	Inverse of 2	=	$-2 \in < S >$
	2 + 2	=	$4 \in < S >$
	– 2 + –2	=	$-4 \in < S >$
	4 + 4	=	$8 \in < S >$
	– 4 + –4	=	$-8 \in < S >$
	2 + 4	=	$6 \in < S >$
	– 2 + –4	=	$-6 \in < S >$

This subgroup is denoted by $< 2 >$ and it contains even integers

$\therefore \quad < 2 > = \quad < \ldots -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots >$

Ex. :Find the subgroup generated by [2] in Z_5

- The elements are Z5 are

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

Indentity Element is 0

The inverse of [2] in Z5 is [3]. It must be in $< [2] >$

Also $2 + 3 = 0$,

$2 + 2 = 4$,

$3 + 3 =$ 1 must be in $< 2 >$

Thus all the elements of Z5 are in $< [2] >$.

$\therefore \quad < [2] > = < 0, 1, 2, 3, 4 >$

Ex. : Consider the set A = {1, 2, 3, 4, 5, 6} under the multiplication modulo 7.

(a)Find the multiplication table for the above

(b)Find the inverses of 2, 3 and 5, 6

(c)Prove that it is a cyclic group

(d)Find the orders and the subgroups generated by {3, 4} and {2, 3}

Solution:

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

Identity element :1

2 and 4 are inverse of each other.
3 and 5 are inverse of each other.
Inverse of 6 is 6

Multiplication modulo 7 table for set A is :

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

$2^2 = 2^1 \times_7 2 = 4$

$2^3 = 2^2 \times_7 2 = 4 \times_7 2 = 1$

$2^4 = 2^3 \times_7 2 = 1 \times_7 2 = 2$

$\therefore$ Hence $|2| = 3$

$\therefore$ 2 is not generator of this group

We have $3^1 = 3$

$3^2 = 3 \times_7 3 = 2$

$3^3 = 3^2 \times_7 3 = 2 \times_7 3 = 6$

$3^4 = 3^3 \times_7 3 = 6 \times_7 3 = 4$

$3^5 = 3^4 \times_7 3 = 4 \times_7 3 = 5$

$3^6 = 3^5 \times_7 3 = 5 \times_7 3 = 1$

Hence $|3| = 6$

$\therefore$ 3 is generator of this group and this group is cyclic.

$\times 7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(d) Subgroup generated by $\{3, 4\}$ is denoted by $< \{3, 4\} >$ since 3, 4 are elements of this set they have to be there in $< \{3, 4\} >$

Inverse of 3 is 5, inverse of 4 is 2

$\therefore$ $3, 4, 5, 2, \in < \{3, 4\} >$

$3 \times_7 4 = 5$ $\quad$ $5 \times_7 4 = 6$

$3 \times_7 3 = 2$ $\quad$ $6 \times_7 6 = 1$

$3 \times_7 5 = 1$ $\quad$ $5 \times_7 1 = 5$

$4 \times_7 4 = 2$ $\quad$ $1 \times_7 1 = 1$

$3 \times_7 2 = 6$ $\quad$ $5 \times_7 2 = 3$

$5 \times_7 5 = 4$ $\quad$ $3 \times_7 6 = 4$

$5 \times_7 6 = 2$ $\quad$ $2 \times_7 2 = 4$

$\therefore$ $< \{3, 4\} > = < 1, 2, 3, 4, 5, 6 >$

$\therefore$ Subgroup generated by $\{3, 4\}$ is the set A itself whose order is 6.

Subgroup generated by $\{2, 3\}$ is denoted by $< \{2, 3\} >$.

Since 2, 3 are elements of this set they have to be there in $< \{2, 3\} >$.

Inverse of 2 is 4.

Inverse of 3 is 5

$\therefore$ $2, 3, 4, 5 \in < \{2, 3\} >$

$2 \times_7 3 = 6$ $\quad$ $3 \times_7 4 = 5$

$4 \times_7 4 = 2$ $\quad$ $5 \times_7 5 = 4$

$2 \times_7 4 = 1$ $\quad$ $3 \times_7 5 = 1$

$4 \times_7 1 = 4$ $\quad$ $5 \times_7 6 = 2$

$2 \times_7 5 = 3$ $\quad$ $3 \times_7 6 = 4$

$4 \times_7 5 = 6$ $\quad$ $5 \times_7 1 = 5$

$2 \times_7 6 = 5$ $\quad$ $3 \times_7 1 = 3$

$6 \times_7 6 = 1$ $\quad$ $2 \times_7 1 = 2$

$3 \times_7 3 = 2$ $\quad$ $6 \times_7 1 = 6$

$2 \times_7 2 = 4$

$\therefore$ $< \{2, 3\} > = < 1, 2, 3, 4, 5, 6 >$

$\therefore$ Subgroup generated by $< \{2, 3\} >$ is the set A and is of order 6.

Coset

Let $(G, *)$ be a group and let H be a subgroup of G. For $a, b \in G$, we say a is congruent to b modulo H, written as $a \equiv b \bmod H$, if $a * b^{-1} \in H$. One can easily see that the congruence relation is an equivalence relation on G. It therefore partitions G into equivalent classes called as **cosets** of H. The set of these equivalence classes is also called as the **quotient** set of G by H.

Let H be a subgroup of a group $(G, *)$. For $a \in G$ define

$$Ha = \{h * a \mid h \in H\}$$

then Ha is called a **right coset** of H in G.

$$aH = \{a * h \mid h \in H\}$$

is called a **left coset** of H in G.

a is called as the representative element of the coset aH or Ha. If $a \in H$, then $Ha = aH = H$.

Hence the right cosets of H in G partition G into disjoint subsets. Likewise the left cosets of H in G yield a portion of G into disjoint subsets.

Normal Subgroup

A subgroup H of G is said to be a **normal subgroup** of G if for every $a \in G$, $aH = Ha$.

A subgroup of an Abelian group is normal.

Ex. 1 : Let $H = \{[0]_6, [3]_6\}$. Find the left and right cosets in group Z_6. Is H a normal subgroup of group Z_6.

Soln. : The addition modulo 6 group, table of Z_6 is

$+_6$	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

This is Abelian group since for all $a, b \in Z_6$,

$$a +_6 b = b +_6 a$$

Left coset of H with respect to a in the set is

$$aH = \{a * h \mid h \in H\}$$

$\therefore$
$$0H = \{0 +_6 0, 0 +_6 3\} = \{0, 3\}$$
$$1H = \{1 +_6 0, 1 +_6 3\} = \{1, 4\}$$
$$2H = \{2 +_6 0, 2 +_6 3\} = \{2, 5\}$$
$$3H = \{3 +_6 0, 3 +_6 3\} = \{3, 0\}$$
$$4H = \{4 +_6 0, 4 +_6 3\} = \{4, 1\}$$
$$5H = \{5 +_6 0, 5 +_6 3\} = \{5, 2\}$$

Right coset of H with respect to a in the set is

$$Ha = \{h * a \mid h \in H\}$$

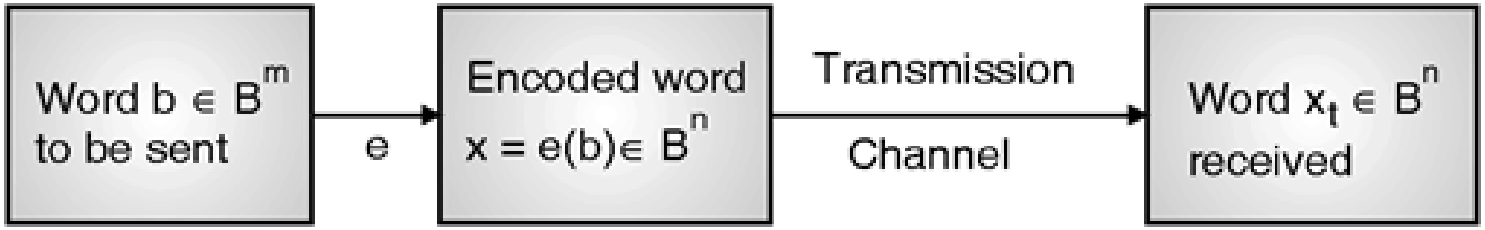
$\therefore$
$$H0 = \{0 +_6 0, 3 +_6 0\} = \{0, 3\}$$
$$H1 = \{0 +_6 1, 3 +_6 1\} = \{1, 4\}$$
$$H2 = \{0 +_6 2, 3 +_6 2\} = \{2, 5\}$$
$$H3 = \{0 +_6 3, 3 +_6 3\} = \{3, 0\}$$
$$H4 = \{0 +_6 4, 3 +_6 4\} = \{4, 1\}$$
$$H5 = \{0 +_6 5, 3 +_6 5\} = \{5, 2\}$$

Here $0H = H0$, $1H = H1$, $2H = H2$, $3H = H3$, $4H = H4$, $5H = H5$

$\therefore$ H is normal subgroup of Z_6.

Groups and Coding

- We first choose an integer n > m and a one to one function e : Bm -> Bn. The function e is called as (m, n) **encoding function**, and we view it as a means of representing every word in Bm as a word in Bn. If b $\in$ Bm, then e (b) is called the **code word** representing b.



- We now transmit the code words by means of a transmission **channel**. Then each code word x = e(b) is received as the word xt in Bn.

Groups and Coding

- Encoding function e to be one to one so that different words in Bm will be assigned different code words.
- If the **transmission channel is noiseless**, then xt = x for all x in Bn. In this case x = e(b) is received for each b $\in$ Bm and since **e** is a known function, b may be identified.
- In general, errors in transmission do occur. We will say that the code word x = e(b) has been transmitted with k or fewer errors if x and xt differ in at least 1 but no more than k positions.

Weight

- If x $\in$ Bn, then the number of 1's in x is called the **weight** of x and is denoted by |X|.

Find the weight of each of the following words in B5:

(a) x = 01000 (b) x = 11100

(c) x = 00000 (d) x = 11111

Soln. :

(a) x = 1

(b) x = 3

(c) x = 0

(d) x = 5

Hamming Distance

Let x and y be words in Bm. The **hamming distance** d (x, y) between x and y is the weight, of $x \oplus y$. Thus the distance between x = x1 x2 … xm and y = y1 y2 … ym is the number of values of i such that $x_i \neq y_i$, that is, the number of positions in which x and y differ.

Ex. Find the distance between x and y.

(a) x = 110110, y = 000101

(b) x = 001100, y = 010110

(c) x = 1100010, y = 1010011

(d) x = 0100100, y = 0011010

Soln. : (a) $x \oplus y = 110011$ so $|x \oplus y| = 4$

(b) $x \oplus y = 011010$ so $|x \oplus y| = 3$

(c) $x \oplus y = 0110001$ so $|x \oplus y| = 3$

(d) $x \oplus y = 0111110$ so $|x \oplus y| = 5$

Minimum Distance

The **minimum distance** of an encoding function e : Bm $\rightarrow$ Bn is the minimum of the distances between all distinct pairs of code words that is,

$$min\{d(e(x), e(y)) | \, x, y \in B_m\}$$

Let x = (10001), y = (01000),

and z = (10101)

The distances are d (x, y) = 3, d (x, z) = 1, and d (y, z) = 4. Therefore, the minimum distance between the words x, y, z is 1.

Minimum distance is also called as '*Hamming distance*'.

With the help of weight and minimum distance as described above, a combination of errors can be detected and corrected.

Theorems

The minimum weight of all non zero words in a group code is equal to its minimum distance

A code can **detect** all combinations of k or fewer iff the minimum distance between any two code words is at least **k + 1**

A code can **correct** all combinations of k or fewer errors iff the minimum distance between any two code words is at least **2 k + 1**

Ex. 1 : Consider the (2, 4) encoding function. How many errors will e detect ?

e (00) = 0000 e (10) = 0110
e (01) = 1011 e (11) = 1100

Soln: We first find distances between pairs of code words

d (0000, 0110) = 2
d (0000, 1011) = 3
d (0000, 1100) = 2
d (0110, 1011) = 3
d (0110, 1100) = 2
d (1011, 1100) = 3

A code can **detect** all combinations of k or fewer iff the minimum distance between any two code words is at least **k + 1**

Minimum distance : 2

K+1=2, so k=1

The code will detect 1 or fewer errors.

Ex. 2 : Consider the encoding function e : B2 -> B6 defined as follows :

e (00) = 001000 e (01) = 010100

e (10) = 100010 e (11) = 110001

How many errors it can detect and correct.

Soln. : We first find the distances between pairs of code words.

d (001000, 010100) = 3

d (001000, 100010) = 3

d (001000, 110001) = 4

d (010100, 100010) = 4

d (010100, 110001) = 3

d (100010, 110001) = 3

The code will detect k or fewer errors if and only if its minimum distance is at least k + 1. Since the minimum distance is 3, we have $3 \geq k + 1$ or $k \leq 2$. The code will detect two or fewer errors.

The code will correct k or fewer errors if and only if its minimum distance is at least 2 k + 1. Since the minimum distance is 3 we have $3 \geq 2k + 1$ or $k \leq 1$. The code will correct 1 or fewer errors.

Group Codes

An (m,n) encoding function $e: B^m \rightarrow B^n$ is called a group code

if e(B^m) = {e(b)|b ∈ B^m}=Ran (e) is a subgroup of B^n

Recall from the definition of subgroup that N is a subgroup of B^n if ;

(a) the identity of B^n is in N.

(b) if x and y belong to N, then x ⊕ y ∈ N and

(c) if x is in N, then its inverse is in N.

Property (c) need not be checked, since every element in B^n is its own inverse. Moreover, since B^n is Abelian, every subgroup of B^n is a normal subgroup.

Ex. 1 : Show that the (2, 5) encoding function e : B2 $\rightarrow$ B5 defined by e (00) = 00000 e (10) = 10101 e (01) = 01110 e (11) = 11011 is a group code.

Soln. :

Let $N = \{00000, 01110, 10101, 11011\}$ be the set of all code words.

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

(i) For a, b $\in$ N, a $\oplus$ b $\in$ N

$\therefore$ N is closed under $\oplus$ operation.

(ii) Identity element of B^5 i.e. 00000 $\in$ N.

Since, $00000 \oplus 00000 = 00000 \oplus 00000 = 00000$ $\quad$ $01110 \oplus 00000 = 00000 \oplus 01110 = 01110$

$10101 \oplus 00000 = 00000 \oplus 10101 = 10101$ $\quad$ $11011 \oplus 00000 = 00000 \oplus 11011 = 11011$

(iii) $\oplus$ is an associative operation

for e.g.

$$01110 \oplus (00000 \oplus 10101) = (01110 \oplus 00000) \oplus 10101$$

$$01110 \oplus 10101 = 01110 \oplus 10101$$

$$11011 = 11011$$

(iv) Every element is its own inverse.

$\therefore$ N is subgroup of B^5 and the given encoding function is a group code.

Example 2 : Consider (3, 6) encoding function 'e' as follows.

e (000) = 000000 e (001) = 000110 e (010) = 010010 e (011) = 010100

e (100) = 100101 e (101) = 100011 e (110) = 110111 e (111) = 110001

Show that the encoding function e is a group code.

Soln. : Let $N = \{000000, 000110, 010010, 010100, 100101, 100011, 110111, 110001\}$ be the set of all code words.

$\oplus$	000000	000110	010010	010100	100101	100011	110111	110001
000000	000000	000110	010010	010100	100101	100011	110111	110001
000110	000110	000000	010100	010010	100011	100101	110001	110111
010010	010010	010100	000000	000110	110111	110001	100101	100011
010100	010100	010010	0000110	000000	110001	110111	100011	100101
100101	100101	100011	110111	110001	000000	000110	010010	010100
100011	100011	100101	110001	110111	000110	000000	010100	010010
110111	110111	110001	100101	100011	010010	010100	000000	000110
110001	110001	110111	100011	100101	010100	010010	000110	000000

(i) For any $a, b \in N$, $a \oplus b \in N$.

$\therefore$ N is closed under $\oplus$ operation.

(ii) Identity element of B^6 i.e. $000000 \in N$.

(iii) $\oplus$ is associative operation

$$000000 \oplus (000110 \oplus 010010) = (000000 \oplus 000110) \oplus 010010$$

$$000000 \oplus (010100) = 000110 \oplus 010010$$

$$010100 = 010100$$

(iv) Every element of N is its own inverse.

$\therefore$ N is subgroup of B^6 and the given encoding function is a group code.

Ex. 3 : Show that the (2, 5) encoding function e : B2 ® B5 defined by

e (00) = 00000 e (01) = 01110 e (10) = 10101 e (11) = 11011

is a group code. How many errors will it detect and correct?

Soln. : Let N = {00000, 01110, 10101, 11011} be the set of all code words.

$\oplus$	00000	01110	10101	11011
00000	00000	01110	10101	11011
01110	01110	00000	11011	10101
10101	10101	11011	00000	01110
11011	11011	10101	01110	00000

(i) For any a, b ∈ N, a $\oplus$ b ∈ N

∴ Set N is closed under $\oplus$ operation.

(ii) Identity element of B^5 i.e. 00000 also belongs to N.

00000 $\oplus$ 00000 = 00000 $\oplus$ 00000 01110 $\oplus$ 00000 = 00000 $\oplus$ 01110

10101 $\oplus$ 00000 = 00000 $\oplus$ 10101 11011 $\oplus$ 00000 = 00000 $\oplus$ 11011

(iii) $\oplus$ is associative operation.

(iv) Each element of N is its own inverse.

00000 $\oplus$ 00000 = 00000 $\oplus$ 00000 = 00000 01110 $\oplus$ 01110 = 01110 $\oplus$ 01110 = 00000

10101 $\oplus$ 10101 = 10101 $\oplus$ 10101 = 00000 11011 $\oplus$ 11011 = 11011 $\oplus$ 11011 = 00000

∴ N is subgroup of B^5 and the given encoding function is a group code.

d (00000, 01110) = 3 d (00000, 10101) = 3

d (00000, 11011) = 4 d (01110, 10101) = 4

d (01110, 11011) = 3 d (10101, 11011) = 3

∴ Minimum distance is 3.

The code will detect k or fewer errors if and only if its minimum distance is atleast k + 1. Since the minimum distance is 3, we have 3 ≥ k + 1 or k ≤ 2. The code will detect 2 or fewer errors.

The code will correct k or fewer errors if and only if its minimum distance is atleast 2 k + 1. Since the minimum distance is 3 we have 3 ≥ 2 k + 1 or k ≤ 1. So the code will correct 1 or fewer errors.

Parity check matrix

Let m and n be non-negative integers with $m < n$ and $r = n - m$. An $n \times r$ Boolean matrix

$$\mathbf{H} = \begin{bmatrix} h_{21} & h_{22} & \dots & h_{2r} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \dots & h_{mr} \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} n - m = r \text{ rows}$$

Whose last r rows form the $r \times r$ identity matrix is called a **parity check matrix**.

We use **H** to define an encoding function.

$e_H : B^m \rightarrow B^n$.

If $b = b_1 b_2 \dots b_m$,

let $x = e_H(b) = b_1 b_2 \dots b_m x_1 x_2 \dots x_r$

where

$$x_1 = b_1 \cdot h_{11} + b_2 \cdot h_{21} + \dots + b_m \cdot h_{m1}$$

$$x_2 = b_1 \cdot h_{12} + b_2 \cdot h_{22} + \dots + b_m \cdot h_{m2}$$

$$\vdots$$

$$x_r = b_1 \cdot h_{1r} + b_2 \cdot h_{2r} + \dots + b_m \cdot h_{mr}$$

Consider the parity check matrix given by H;

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

Determine the group code $e_H : B^2 \rightarrow B^5$

Soln: $B^2 = \{00,01,10,11\}$

Then $e(00) = 00\ x_1\ x_2\ x_3 = B^5$

$x_1 = 0 \cdot 1 + 0 \cdot 0 = 0$

$x_2 = 0 \cdot 1 + 0 \cdot 1 = 0$

$X_3 = 0 \cdot 0 + 0 \cdot 1 = 0$

e (00) = 00000

Next $e(01) = 01\ x_1\ x_2\ x_3 = B^5$

$x_1 = 0 \cdot 1 + 1 \cdot 0 = 0$

$x_2 = 0 \cdot 1 + 1 \cdot 1 = 1$

$X_3 = 0 \cdot 0 + 1 \cdot 1 = 1$

e (01) = 01011

Next e(10) = 10 x_1 x_2 x_3 = B^5

x_1 = 1 . 1 + 0. 0 = 1

x_2 = 1 . 1 + 0. 1 = 1

X_3 = 1 . 0 + 0. 1 = 0

e (10) = 10 1 1 0

Next e(11) = 11 x_1 x_2 x_3 = B^5

x_1 = 1 . 1 + 1. 0 = 1

x_2 = 1 . 1 + 1. 1 = 0

X_3 = 1 . 0 + 1. 1 = 1

e (11) = 11 1 0 1

$e_H : B^2 \rightarrow B^5$ is as above for e (00) , e (01), e (10) ,e (11)

Problem 1

Consider the parity check matrix given by H;

H= 0 1 1

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

Determine the group code $e_H : B^2 \rightarrow B^5$

e (00) = 00000

e (01) = 01011

e (00) = 10011

e (00) = 11000

Problem 2

Consider the parity check matrix given by H;

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

Determine the group code $e_H : B^3 \rightarrow B^6$

e (000) = 000000

e (001) = 001111

e (010) = 010011

e (011) = 011100

e (100) = 100100

e (101) = 101011

e (110) = 110111

e (111) = 111000

MAXIMUM LIKELIHOOD DECODING TECHNIQUE

Consider the encoding function $B^2 \rightarrow B^4$ defined as follows

e (00)=0000 e (10)=1011

e (01)=0110 e (11)=1101

Decode the foll words relative to MLD function,

(i) 0101 (ii) 1010 (iii) 1101

Step 1: Construct Decoding Table

	e(00)	e(01)	e(10)	e(11)
	0000	0110	1011	1101
0000	0000	0110	1011	1101
0001	0001	0111	1010	1100
0010	0010	0100	1001	1111
1000	1000	1110	0011	0101

Step2: 0101 is decoded as 11

1010 is decoded as 10, 1101 is decoded as 11

Consider the encoding function $B^2 \rightarrow B^5$ defined as follows

e (00)=**00000** e (10)=**10101**

e (01)=**01110** e (11)=**11011**

Decode the following words relative to MLD function,

(i) 11110 (ii)10011(iii)10100

	e (00)	e (01)	e (10)	e (11)
	00000	**01110**	**10101**	**11011**
00000	00000	01110	10101	11011
00001	00001	01111	**10100**	11010
00010	00010	01100	10111	11001
00100	00100	01010	10001	11111
01000	01000	00110	11101	**10011**
10000	10000	**11110**	00101	01011

11110 is decoded as 01,
10100 is decoded as 10,
10011 is decoded as 11