DISCRETE MATHAMETICS

(DMCA108)

(MCA)

ACHARYA NAGARJUNA UNIVERSITY

CENTRE FOR DISTANCE EDUCATION

NAGARJUNA NAGAR,

GUNTUR

ANDHRA PRADESH

Lesson 1

Sets and Operations

Objectives

At the end of the Lesson the student must be able to:

(i) Understand the fundamental idea of certain mathematical concepts.
(ii) Learn the various operations on sets.
(iii)Constructions of different equivalence relations on a set
(iv)Learn the basic notion of algebraic systems and algorithms

Structure

1.1 Introduction

The theory of sets was originated in the year 1895 by the German mathematician G. Cantor who defined a set as a collection or aggregate of definite and distinguishable objects selected by means of some rules or description. It is one of the principal foundation of mathematics, and nearly every mathematical object of interest is a set of some kind. Our aim of this lesson is to develop the techniques for logical constructions.

1.2 Sets

A set is considered as a primitive term and thus formally undefined but we have an idea of what constitutes a set.

1.2.1 Definition: A **set** is a well defined collection of objects in which we can say whether a given object is in the collection. The fact that a is a member of a set A is denoted by $a \in A$ and we call it as 'a belongs to A'. The members of a set are called **elements**.

For example: S = {2, 4, 6, 8, 10} is a set.

A set is usually specified either by listing all of its elements inside a pair of braces or by stating the property that determines whether or not an object x belongs to the set. We might write $S = \{x_1, x_2, \dots, x_n\}$.

1.2.2 Example: If E is the set of even positive integers, we describe E by writing either $E = \{2, 4, 6, \dots\}$ or $E = \{x \mid x$ is an even integer and $x > 0\}$.
We write $2 \in E$ when we want to say that 2 is in the set E, and $-3 \notin E$ to say that -3 is not in the set E.

1.2. 3 Notations: Some of the more important set notations are given below:

$\mathbb{N}$: The set of all natural numbers = {n | n is a natural number} = {1, 2, 3, …};

$\mathbb{Z}$: The set of all integers = {x | x is an integer} = {…, -1, 0, 1, 2, …};

$\mathbb{Q}$: The set of all rational numbers = $\{p/q \mid p, q \in \mathbb{Z}$ where $q \neq 0\}$;

$\mathbb{R}$: The set of all real numbers = {x | x is a real number};

$\mathbb{C}$: The set of all complex numbers = {z | z is a complex number}.

1.2.4 Definitions: If x is not an element of A then we write $x \notin A$. Suppose A and B are two sets. We say that A is a **subset** of B (written as $A \subseteq B$) if every element of A is also an element of B. Two sets A and B are said to be **equal** (denoted by A = B) if A is a subset of B, and B is a subset of A. A set B is a proper subset of A if $B \subset A$ (that is, B is a subset of A, but not equal to A). Trivially, every set is a subset of it self. A set which contains no elements at all is called the **Null set** (denoted by Φ).

For example, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

1.2.5 Example: Consider the sets A = {x | x is an even positive integer} and B = { x | x is a positive integer}. Then $A \subseteq B$.

1.2.6 Definition: Let *A* be a set. Then the set of all subsets of *A*, is called the **power set** of *A*. It is denoted by $\wp(A)$.

1.2.7 Example: Let A = {1, 2, 3}. Then $\wp(A) = \{\Phi, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\} , A\}$

1.2.8 Problem: If the set *A* has *n* elements, then the number of elements in $\wp(A)$ is 2^n.

Solution: Suppose *A* has *n* elements. Let *m* be an integer such that $0 \le m \le n$. We can select *m* elements from the given set *A* in ${}^nC_m$ ways. So *A* contains ${}^nC_m$ distinct subsets containing *m* elements. Therefore the number of elements in

$\wp(A)$ = number of subsets containing 0 number of elements

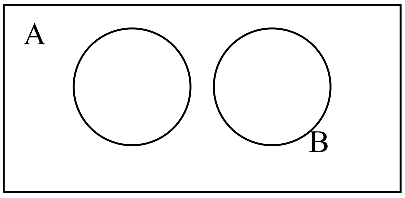
+ number of subsets containing only 1 element

+ … + number of subsets containing n elements

$$= {}^nC_0 + {}^nC_1 + {}^nC_2 + ... + {}^nC_n$$

$= 2^n$.

1.2.9 Definition: A Venn diagram is a pictorial representation of sets in which the universal set U is represented by a rectangle and the sets within U by circles.



1.2.10 Definition: A set A is called finite if it contains only finite number of elements. If A contains n distinct elements we write by $|A| = n$. A set which is not finite is called infinite.

1.2.11 Examples:

Finite sets:

(i) Set of months in a year

(ii) The set of vowels in English alphabets,

(iii) The set of students in a class.

Infinite Sets:

(i) Set of integers

(ii) Set of real numbers

(iii) $\{1, 1/3, 1/9, 1/27, \ldots\}$

Self Assessments Question 1:

List all the elements of the following sets

(i) $\{x / x \in \mathbb{Z}, x^2 < 12\}$

(ii) $\{x / x \in \mathbb{N}, \text{x is prime and } x < 20 \}$

(iii) $\{x / x \in \mathbb{N}, \text{x is even and } 10 < x < 20\}$

Self Assessment Question 2: Let A = {x, y, z}. Which of the following are subsets of A? which are proper subsets of A ?

(i) {x}; (ii) {y, z, x}; (iii) {a, x, y}.

Self Assessment Question 3: If S = {0, 1}, then write $\wp$(S).

Self Assessment Question 4: Write the elements in the following sets.

(i) A = {x / x is a multiple of 2 and x is odd};

(ii) B = {x / x is the number shows on the die, x > 6}.

1.3 Operations on Sets

In this section we will discuss several operations that will combine gives sets to yield new sets. These operations, which are analogous to the familiar operations on the real numbers, play a key role in many applications.

1.3.1 Definitions: (i) If A and B are two sets, then the set $\{x \ / \ x \in A \text{ or } x \in B\}$ is denoted by $A \cup B$ and we call it as the **union** of A and B.

(ii) The set $\{x \ / \ x \in A \text{ and } x \in B\}$ is denoted by $A \cap B$ and we call it as the **intersection** of A and B.

(iii) If A and B are two sets, then the set $\{x \in B \ / \ x \notin A\}$ is denoted by $B - A$ (or $B \setminus A$) and it is called as the **complement** A in B.

(iv) The set that contains no members is called the **empty set** and it is denoted by ϕ. Empty set is a subset of every set.

1.3.2 Example: (i) Suppose $A = \{a, b, c\}$ and $B = \{a, b, c, 3, 4\}$. Then A is a subset of B. If $X = \{c, b, a\}$, then $A = X$.

If $D = \{a, b, 2, 4\}$, then $A \cap D = \{a, b\}$ and $A \cup D = \{a, b, c, 2, 4\}$.

1.3.3 Example: Let $\mathbb{R}$ be the universal set and suppose that $A = \{x \in \mathbb{R} \mid 0 < x \leq 3\}$ and $B = \{x \in \mathbb{R} \mid 2 \leq x < 4\}$. Then

$$A \cap B = \{x \in \mathbb{R} \mid 2 \leq x \leq 3\};$$

$$A \cup B = \{x \in \mathbb{R} \mid 0 < x < 4\};$$

$$A \setminus B = \{x \in \mathbb{R} \mid 0 < x < 2\};$$

$$A' = \{x \in \mathbb{R} \mid x \leq 0 \text{ or } x > 3\}.$$

1.3.4 Note: The operations of union and intersection can be defined for three or more sets in the similar way.

$A \cup B \cup C = \{x / x \in A \text{ or } x \in B \text{ or } x \in C\}$ and $A \cap B \cap C = \{x / x \in A, x \in B, x \in C\}$

In general, let A_i be a collection of sets – one for each element i belongs to I, where I is some set (I may be the set of all positive integers). We define

$\bigcap_{i \in I} A_i = \{a / a \in A_i$ for all $i \in I\}$, and

$\bigcup_{i \in I} A_i = \{a / a \in A_i$ for some $i \in I\}$.

A collection $\{A_i\}_{i \in I}$ of sets is said to be **mutually disjoint** if $A_i \cap A_j = \phi$ for all $i \in I, j \in I$ such that $i \neq j$.

1.3.5 Example: (i) Write $A_i = \{i, i+1, i+2, ...\}$ for each $i \in N,$ the set of natural numbers. Then it is easy to observe that $\bigcup\limits_{i \in N} A_i = N$ and $\bigcap\limits_{i \in I} A_i = \phi$.

(ii) If $B_i = \{2i, 2i+1\}$ for all $i \in N$, then $\{B_i\}_{i \in N}$ is a collection of mutually disjoint sets.

1.3.6 Definition: Let A and B are two sets. We define their **symmetric difference** as the set A Δ B = (A - B) ∪ (B - A). Sometimes it is denoted by A ⊕ B.

1.3.7 Example: If A = {1, 2, 3, 4} and B = {1, 2, 5, 7}, then A ⊕ B = {3, 4, 5, 7}.

Self Assessment Question 5: Let A = {a, b, c, d, e, f}, B = {b, c, g} and C = {a, c, e}. Compute (i) A ∪ B ∪ C, (ii) A ∩ B ∩ C ; (iii) A – B ; (iv) B ⊕ C.

1.3.8 Theorem: The set operations satisfy the following properties.

1. A ∪ B = B ∪ A; A ∩ B = B ∩ A (commutative properties)
2. A ∪ (B ∪ C) = (A ∪ B) ∪ C; A ∩ (B ∩ C) = (A ∩ B) ∩ C (Associative)
3. A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C); A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ C) (Distributive)
4. A ∪ A = A; A ∩ A = A (Idempotent)
5. $(A')' = A$
6. A ∪ A′ = U
7. A ∩ A′ = Φ
8. Φ′ = U
9. U′ = Φ
10. (A ∪ B)′ = A′ ∩ B′ ; (A ∩ B)′ = A′ ∪ B′ (D' Morgan laws)
11. A ∪ Φ = A; A ∩ Φ = Φ; A ∪ U = U ; A ∩ U = A (Universal)

1.3.9 Note: For any two sets *P* and *Q*, we have

(i). $|P \cup Q| \leq |P| + |Q|$ where |A| denote the number of elements in A.

(ii). $|P \cap Q| \leq \min(|P|, |Q|)$

(iii). $|P \oplus Q| = |P| + |Q| - 2|P \cap Q|$ where $\oplus$ is the symmetric difference.

1. 3.10 Theorem: Let A_1 and A_2 be two sets. Then $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

This can be extended to any finite number of sets, which is known as principle of inclusion and exclusion, given following.

1.3.11 Theorem: If A_1, A_2, …, A_n are finite sets, then $|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i|$ $- \sum_{1 \leq i \leq j \leq n} |A_i \bigcap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{n-1} |A_1 \cap A_2 \cap \ldots \cap A_n|$.

1.3.12 Example: Thirty cars were assembled in a factory. The options available were a radio, an air conditioner, and white wall-tires. It is known that 15 of the cars have radios, 8 of them have air conditioners, and 6 of them have white wall-tires. Moreover, 3 of them have all three options. Find out "at least how many cars do not have any options at all".

Solution: Let A_1, A_2 and A_3 denote the sets of cars with the given options respectively.

$|A_1| = 15$, $|A_2| = 8$, $|A_3| = 6$, $|A_1 \cap A_2 \cap A_3| = 3$.

Now by the principle of inclusion and exclusion,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= 15 + 8 + 6 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + 3 \\ &= 32 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &\leq 32 - 3 - 3 - 3 \\ &= 23. \end{aligned}$$

(here we used the fact : $|A_i \cap A_j \cap A_k| \leq |A_i \cap A_j|$ for any i, j, k)

Therefore there are at most 23 cars have one or more options.

This means there are at least 7 cars that do not have any options.

Self Assessment Question 6: A sample of 80 people have revealed that 24 like cinema and 62 like television programmes. Find the number of people who like both cinema and television programmes.

1.3.13 Problem: Determine the number of integers between 1 to 250 that are divisible by any of the integers 2, 3, 5 and 7.

Solution: Write $A_1 = \{x \in \mathbb{Z}^+ / x \leq 250 \text{ and } x \text{ is divisible by } 2\}$

Similarly A_2, A_3, A_4 are set of integers ≤ 250 that are divisible by 3, 5 and 7 respectively.

$|A_1| = \left\lfloor \frac{250}{2} \right\rfloor = 125$ where $\lfloor x \rfloor$ denotes the integer smaller than or equal to x.

$|A_2| = \left\lfloor \frac{250}{3} \right\rfloor = 83$, $|A_3| = \left\lfloor \frac{250}{5} \right\rfloor = 50$, $|A_4| = \left\lfloor \frac{250}{7} \right\rfloor = 35$,

$|A_1 \cap A_2| = \left\lfloor \frac{250}{2\times 3} \right\rfloor = 41$, $|A_1 \cap A_3| = \left\lfloor \frac{250}{2\times 5} \right\rfloor = 25$, $|A_1 \cap A_4| = 17$, $|A_2 \cap A_3| = 16$, $|A_2 \cap A_4| = 11$, $|A_3 \cap A_4| = 7$, $|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{250}{2\times 3\times 5} \right\rfloor = 8$,

$|A_1 \cap A_2 \cap A_4| = 5$, $|A_1 \cap A_3 \cap A_4| = 3$, $|A_2 \cap A_3 \cap A_4| = 2$, $|A_1 \cap A_2 \cap A_3 \cap A_4| = 1$.

Therefore $|A_1 \cup A_2 \cup A_3 \cup A_4| = | 25 + 83 + 50 + 35 - 41 - 25 - 17 - 16 - 11 - 7 + 8 + 5 + 3 + 2 - 1 = 193$.

1.3.14 Definition: (i) If S and T are two sets, then the set {(s, t) / s ∈ S and t ∈ T} is called the **Cartesian product** of S and T (here (a, b) = (s, t) ⇔ a = s and b = t). The Cartesian product of S and T is denoted by S × T. Thus

$$S \times T = \{(s, t) \ / \ s \in S \text{ and } t \in T\}.$$

Note that if S and T are two sets, then S × T and T × S may not be equal.

(ii) If $S_1, S_2, .., S_n$ are n sets, then the **Cartesian product** is defined as $S_1 \times S_2 \times \ldots \times S_n = \{(s_1, s_2, \ldots, s_n) \ / \ s_i \in S_i \text{ for } 1 \leq i \leq n\}$.

Here the elements of $S_1 \times S_2 \times \ldots \times S_n$ are called **ordered n-tuples**. For any two n-tuples, we have $(s_1, s_2, \ldots, s_n) = (t_1, t_2, \ldots, t_n) \Leftrightarrow s_i = t_i, \quad 1 \le i \le n$.

1.3.15 Examples: (i) If $X = \{a, b\}$ and $Y = \{x, y\}$, then $X \times Y = \{(a, x), (a, y), (b, x), (b, y)\}$ and $Y \times X = \{(x, a) (x, b), (y, a), (y, b)\}$. Note that $X \times Y \neq Y \times X$.

(ii) If $A = \{a, b\}$, $B = \{2\}$, $C = \{x\}$, then $A \times B \times C = \{(a, 2, x), (b, 2, x))\}$.

1.3.16 Example: List the elements of $S \times T$, $T \times S$ when $T = \{a, b, c, d\}$ and $S = \{1, 2, 4\}$. Observe that the intersection of $S \times T$ and $T \times S$ is empty.

1.4 Computer Representation of Sets

One method to represent sets using computer is to store the elements of the set in an unordered fashion. In this method, the operations like union, intersection or difference of two sets would be time consuming since large amount of time will be required for searching of elements. A method using an arbitrary ordering of the elements of the universal set to store the elements can overcome this problem.

A set can be represented in a computer using characteristic function, defined as follows.

1.4.1 Definition: Let A be a subset of the Universal set $U = \{x_1, x_2, \ldots, x_n\}$. The **characteristic function** of A is defined as a function from U to {0, 1} by the following:

$$f_A(x_i) = \begin{cases} 1 \text{ if } x_i \in A \\ 0 \text{ if } x_i \notin A \end{cases}.$$

1.4.2 Example: Take A = {2, 3, 7} and U = {1, 2, …, 10}, then $f_A(1) = 0$, $f_A(2) = 1$, $f_A(3) = 1$, $f_A(7) = 1$. and $f_A(11)$ is undefined. It can be verified that f_A is everywhere defined and onto, but not one one.

1.4.3 Theorem: Characteristic functions of subsets satisfy the following properties:

(i) $f_{A \cap B} = f_A f_B$

(ii) $f_{A \cup B} = f_A + f_B - f_A f_B$.

Proof: (i) By definition, $f_{A \cap B}(x) = \begin{cases} 1, & \text{if } x \in A \cap B \\ 0, & \text{if } x \notin A \cap B \end{cases}$.

Now $f_A(x)f_B(x) = 1 \Leftrightarrow f_A(x) = 1$ and $f_B(x) = 1 \Leftrightarrow x \in A \cap B$ and $f_A(x)f_B(x) = 0 \Leftrightarrow x \notin A \cap B$. Therefore $f_{A \cap B} = f_A f_B$.

(ii) Now $x \in A \Rightarrow f_A(x) + f_B(x) – f_A(x)f_B(x) = 1 + f_B(x) – f_B(x) = 1$.

Similarly, $x \in B \Rightarrow f_A(x) + f_B(x) – f_A(x)f_B(x) = f_A(x) + 1 – f_A(x) = 1$.

If $x \notin A$ and $x \notin B$, then $f_A(x) + f_B(x) – f_A(x)f_B(x) = 0$, since $f_A(x) = 0 = f_B(x)$.

Therefore $f_A(x) + f_B(x) – f_A(x)f_B(x) = \begin{cases} 1, & \text{if } x \in A \cap B \\ 0, & \text{if } x \notin A \cap B \end{cases}$. Hence $f_{A \cup B} = f_A + f_B - f_A f_B$.

1.4.4 Note: A sequence is a list of objects arranged in order, such as first element, second element, third element and so on. Let U = {$x_1, x_2, …, x_n$} be the universal set and A be subset of U. List the elements of A in some order (the order we choose is of no importance). Then the characteristic function f_A defined as $f_A(x_i) = \begin{cases} 1 \text{ if } x_i \in A \\ 0 \text{ if } x_i \notin A \end{cases}$. Thus f_A can be represented by a sequence of 0's and 1's of length n.

1.5 Answers to Self Assessment Questions

SAQ 1:

(i) {-3, -2, -1, 0, 1, 2, 3}

(ii) {2, 3, 5, 7, 11, 13, 17, 19}

(iii) {12, 14, 16, 18}

SAQ 2:

(i), (ii) are the subsets of A, (iii) is not a subset of A; Moreover (i) is a proper subset of A.

SAQ 3:

$\wp$(S) = {Φ, {0}, {1}, S}.

SAQ 4:

(i), (ii): Empty sets

SAQ 5:

(i) {a, b, c, d, e, f, g}; (ii) {c}; (iii) {a, d, e, f}; (iv) {a, b, e, g}.

SAQ 6:

Let A = set of people who like cinema, B = set of people who like TV. Then $|A| = 24$, $|B| = 62$. By the principle of inclusion and exclusion, we get $|A \cup B| = |A| + |B| - |A \cap \mathrm{B}|$ $\Rightarrow 80 = 24 + 62 - |A \cap \mathrm{B}|$. Therefore $|A \cap \mathrm{B}| = 6$.

1.6 Summary

In this lesson we introduced the basic concept related to sets and the different ways of representing them. Some properties common to operations on sets were discussed. Cartesian product of sets was studied. Lastly we discussed the principle of inclusion and exclusion, characteristic functions and properties.

1.7 Technical Terms

Set	Well defined collection of objects.
Subset (written as $A \subseteq B$)	Every element of A is also an element of B
Null set	Set contains no elements (denoted by Φ).
Power set of A	The set of all subsets of A (denoted by $\wp(A)$).
Union	$A \cup B = \{x \ / \ x \in A \text{ or } x \in B\}$.
Intersection	$A \cap B = \{x \ / \ x \in A \text{ and } x \in B\}$.
Complement	$\{x \in B / x \notin A\}$ (the complement A in B).
Symmetric difference	$A \Delta B = (A-B) \cup (B-A)$.
Cartesian Product	$S \times T = \{(s, t) \ / \ s \in S \text{ and } t \in T\}$.
Characteristic function	$f_A(x_i) = \begin{cases} 1 \text{ if } x_i \in A \\ 0 \text{ if } x_i \notin A \end{cases}$.

1.8 Model Questions

1. Draw Venn diagram and verify the following properties

(i). $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (Distributive)

(ii). $A \cup A = A$; $A \cap A = A$ (Idempotent)

(iii). $(A')' = A$

2. State Principle of Inclusion and Exclusion.

3. How many arrangements of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 contain at least one of the patterns 289, 234 or 487 ?

4. A Computer company must hire 20 programmers to handle system programming jobs and 30 programmers for applications programming. Of those hired, 5 are expected to perform jobs of both types. How many programmers must be hired ?

5. Let A = {2, 4}. Which of the following sets are equal to A ?

(a) B = {4, 2} (b) C = $\{x / x^2 - 6x + 8 = 0\}$

(c) D = $\{x / x \in \mathbb{N}$, x is even and $1 < x < 5\}$ (d) E = $\{x / x - 4 = 0$ and $x + 2 = 0\}$

1.9 References

1. Akerkar Rajendra and Akerkar Rupali "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, "Discrete Mathematical Structures" PHI, New Delhi, 1999.

3. Fraleigh J.B. **"**A First Course in Abstract Algebra", Narosa Publ. House, New Delhi, 1992

4. Hari Kishan and Shivraj Pundir "Discrete Mathematics", Pragati Prakashan, Meerut, 2005.

5. Herstein I. N. "Topics in Algebra", Blaisdell, New York, 1964.

6. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. "Quantitative Methods", Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

7. Satyanarayana Bhavanari "Partially Ordered Sets and Finite Machines", Satyasri Maths Study Centre, Guntur, (0863- 2232138) 2002.

8. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

Name of the Lesson Writer: **Dr Bhavanari Satyanarayana**
Professor

Lesson 2

Mathematical Induction and Matrices

Objectives

At the end of the Lesson the student must be able to:

(i) To know the principle of mathematical induction
(ii) To find the nth term of the series
(iii)To apply the mathematical induction to write the proofs.
(iv)Properties of matrices.
(v) Know the different types of matrices.

Structure

2.1 Introduction

In this lesson we discussed the principle of Mathematical induction has a very special place in mathematics because of its simplicity and vast amount of applications. This lesson acts as foundations on which all mathematical knowledge is built. The theory of matrices, introduced by French mathematician Cayley. A matrix is a powerful tool in the study of branches of Mathematics, Engineering and Technology and business applications. The concept was initially developed for solving equations.

2.2 Mathematical Induction

2.2.1 Definition: A function f: N → R (where N is the set of natural numbers and R the set of real numbers) is called a sequence of real numbers denoted by $\{f(n)\} = \{f(1), f(2) ...., f(n), ... \}$ where $f(n)$ is called the n^{th} term of the sequence. A sequence may also be denoted by (a_n) or (u_n) where a_n or u_n is the n^{th} term of the sequence.

2.2.2 Definition: If (u_n) is a sequence, then $\sum u_n = u_1 + u_2 + \dots + u_n + \dots$ is called a series which may be finite or infinite according as the number of terms in it is finite or infinite.

2.2.3 Definition: A sequence of the form $a,\ a+d,\ a+2d, ...a+\overline{n-1}\ d, ...$ is called an Arithmetic Progression (A.P.) whose first term is a, common difference is d and n^{th} term denoted by $t_n = a+\overline{n-1}\ d$.

If S_n denotes the sum of the first n terms of the above A. P , then

$$S_n = a+(a+d) + ...+ \left(a + \overline{n-1}\ d\right)$$

$$= \frac{n}{2}\left[2a + \overline{n-1}d\right] \text{ or } \frac{n}{2}(a+l), \text{where } l = \text{ the last term } = a + \overline{n-1}d = t_n$$

Observations:

(i) $d = t_n - t_{n-1}$ is independent of n, a constant.

(ii) If each term of an A. P is multiplied or added by a constant the resulting sequence is also in A. P

(iii)If the corresponding terms of two A. P 's are added, the resulting sequence is also in A. P .

(iv)If a, A, b are in A. P , then *A* is called the arithmetic mean between the extremes *a and b* is given by $A = \frac{a + b}{2}$

(v) If $a, x_1, x_2, ...x_n, b$ are in A. P, then $x_1, x_2, ...x_n$ are the n AM 's between *a and b*, and their sum $S_n = \frac{n}{2}(a+b)$

Self Assessment Question 1: Find the n^{th} term of the following series

(a) 1 + 3 + 5 + 7 +.....

(b) 7 + 3 – 1 – 5 + ……..

(c) $1 + \frac{3}{2} + 2 + \frac{5}{2} + \ldots\ldots...$

(d) 1 + 3 + 9 + 27 + ……..

2.2.4 Definition: A sequence of the form $a, ar, ar^2 ....ar^{n-1}, ...$ is called a geometric progression (G.P.), whose first term is a, common ratio is r and the n^{th} term $t_n = ar^{n-1}$. If S_n denotes the sum of the first n terms of the above G. P , then

$$S_n = a + ar + ... + ar^{n-1}$$

$$= \frac{a\left(1-r^n\right)}{1-r} \quad \text{or} \quad \frac{a\left(r^n - 1\right)}{r - 1}, \quad r \neq 1$$

or $S_n = na$ if $r = 1$.

Also $S_n = \frac{a - lr}{1-r} = \frac{lr - a}{r - 1}$ $(r \neq 1)$ where $l =$ the last term $= t_n = ar^{n-1}$

If $|r| < 1$ and $n \to \infty$, then the sum S of infinite $G.\ P$ is $S = \frac{a}{1-r}$ $\left(\text{Since } r^n \to 0\right)$

Observations:

(i) $r = \frac{t_n}{t_{n-1}}$ = a term independent of $n = a$ constant ratio

(ii) If each term of a $G.\ P$ is multiplied by a constant, the resulting sequence is also in $G.\ P$

(iii)If a, G, b are in $G.\ P$, the G is called the geometric mean between the extremes a and b and is given by $G = \pm\sqrt{ab}$.

(iv)If $a,\ x_1,\ x_2 \ldots\ldots x_n,\ b$ are in $G.\ P$, then $x_1,\ x_2 \ldots\ldots x_n$ are the n $G.\ M$'s between a and b and the k^{th} $G.M = a\left(\frac{b}{a}\right)^{\frac{k}{k+1}}$

(v) Also product of the n $G.M\,s = (ab)^{\frac{n}{2}}$

2.2.5 Definition: A sequence of the form $\frac{1}{a}, \frac{1}{a+d}, \frac{1}{a+2d}, \ldots, \frac{1}{a+\overline{n-1}\,d}, \ldots$ is a harmonic progression whose n^{th} term $t_n = \frac{1}{a+(n-1)\,d}$

Observations:

i) There is no formula to find the sum of the first n terms of the H. P

ii) If $a,\ H,\ b$ are in H. P., then H is the harmonic mean between the extremes a and b and is given by $H = \frac{2ab}{a+b}$

iii) Problems on H. P. are solved by dealing with the corresponding A. P.

2.2.6 Principle of Mathematical Induction

Mathematical induction is the process of proving a general theorem or formula involving the positive integer n from particular cases.

A proof by mathematical induction consists of the following two steps.

(i) Show by actual substitution that the theorem is true for $n = 1$

(ii) Assuming the theorem to be true for $n = m$, prove that it is also true for $n = m + 1$

Note that here m is a particular value of n. From (i) the theorem is true for $n = 1$ and from (ii) it is true for $n = 1 + 1 = 2$; since it is true for $n = 2$ it follows from (iii) that it is also true for $n = 2 + 1 = 3$ and so on. Hence theorem is true for all positive integral values of n.

Second Principle of Mathematical Induction: Let S(n) be a statement about integers for $n \in N$ (set of natural numbers) and suppose $S(n_0)$ is true for some integer n_0. If $S(n_0)$, $S(n_0+1)$, …, $S(k)$ imply that $S(k+1)$ for $k \geq n_0$, then the statement S(n) is true for all integers n greater than n_0.

2.2.7 Example: Prove by mathematical induction that the sum of the first n natural numbers is $\frac{n(n+1)}{2}$.

Solution: That is to prove that $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$

Step (i): For $n = 1$, left side = 1, right side = $\frac{1(1+1)}{2} = 1$. Hence the result is true for $n = 1$.

Step (ii): <u>Induction Hypothesis</u>: Assume that the result to be true for n = m. Then $1 + 2 + 3 + \ldots m = \frac{m\ (m+1)}{2}$

Step (iii): We now show that the above result is true for $n = m + 1$. Adding the $(m + 1)^{th}$ term viz., $m + 1$ to both sides we obtain.

$$1+2+3+\ldots+ m + (m+1) = \frac{m(m+1)}{2} + (m+1)$$

$$= (m+1)\left[\frac{m}{2}+1\right] = \frac{(m+1)(m+2)}{2}$$

$$= \frac{(m+1)(\overline{m+1}+1)}{2}$$

Which is the same as the given result for $n = m+1$

Hence by mathematical induction, the result is true for all + ve integral values of n.

2.2.8 Example: Prove by mathematical induction that

$$1^2 + 2^2 + 3^2 + \ldots.+ n^2 = \frac{n(n+1)(2n+1)}{6}$$

Solution: Step(i): If $n=1$, left side $= 1^2 = 1$ and the right side $= \frac{1(1+1)(2.1+1)}{6} = \frac{1.2.3}{6} = 1$. Hence the result is true for n = 1.

Step(ii): Induction Hypothesis: Now assume that the result to be true for n = m.

Then $1^2 + 2^2 + 3^2 + \ldots.+ m^2 = \frac{m(m+1)(2m+1)}{6}$.

Adding the $(m+1)^{th}$ term i.e. $(m+1)^2$ to both sides of the above equation, we get,

$$1^2 + 2^2 + \ldots+ m^2 + (m+1)^2 = \frac{m(m+1)(2m+1)}{6} + (m+1)^2$$

$$= \frac{(m+1)}{6}\{m(2m+1) + 6(m+1)\}$$

$$= \frac{(m+1)}{6}(2m^2 + 7m + 6)$$

$$= \frac{(m+1)(m+2)(2m+3)}{6}$$

$$= \frac{(m+1)\left(\overline{m+1}+1\right)\left(2(m+1)+1\right)}{6}$$

Therefore the result is true for $n = m + 1$. Hence by mathematical induction the given result is true for all positive integers n.

2.2.9 Example: Prove that $1^3 + 2^3 + 3^3 + \ldots\ldots + n^3 = \frac{n^2\,(n+1)^2}{4}$, by mathematical induction.

Solution: (i) For $n = 1$, left side $= 1^3 = 1$ and right side $= \frac{1^2\,(1+1)^2}{4} = \frac{1\,.\,4}{4} = 1$

Hence it is true for $n = 1$

(ii) Induction Hypothesis: Assume the result is true for $n = m$. Then $1^3 + 2^3 + 3^3 + \ldots + m^3 = \frac{m^2\,(m+1)^2}{4}$.

Adding the $(m+1)^{th}$ term viz.,$(m+1)^3$ to both sides ,

$$1^3 + 2^3 + \ldots + m^3 + (m+1)^3 = \frac{m^2\,(m+1)^2}{4} + (m+1)^3$$

$$= \frac{(m+1)^2}{4}\left(m^2 + 4m + 4\right) = \frac{(m+1)^2\,(m+2)^2}{4} = \frac{(m+1)^2\,(m+1+1)^2}{4}$$

Therefore the result is true for $n = m + 1$. Hence by mathematical induction the given result is established for all positive integers.

2.2.10 Problem: Prove by mathematical induction

$$\frac{1}{2.5} + \frac{1}{5\,.\,8} + \frac{1}{8\,.\,11} + \ldots. + \frac{1}{(3n-1)\,(3n+2)} = \frac{n}{6n+4}$$

Solution:

(i) If $n = 1$, left side $= \frac{1}{2.5} = \frac{1}{10}$, right side $= \frac{1}{6.1+4} = \frac{1}{10}$. Therefore the result is true for $n = 1$

(ii) Induction Hypothesis: Assume the result to be true for $n = m$.

$$\frac{1}{2.5} + \frac{1}{5.8} + \frac{1}{8.11} + \ldots.. + \frac{1}{(3m-1)(3m+2)} = \frac{m}{6m+4}$$

Adding the $(m+1)^{th}$ term, $\frac{1}{(3m+2)(3m+5)}$ to both sides.

We have, $\frac{1}{2.5} + \frac{1}{5.8} + \ldots. + \frac{1}{(3m+2)(3m+5)}$

$$= \frac{m}{6m+4} + \frac{1}{(3m+2)(3m+5)} = \frac{m(3m+5)+2}{2(3m+2)(3m+5)} = \frac{m+1}{6m+10}$$

This is the value of $\frac{n}{6n+4}$ when $m+1$ is substituted for n. Therefore the proposition is true for all positive integral values of n.

2.2.11 Problem: Prove by mathematical induction that $2^n > n$ for all positive integer n.

Solution: Let $P(n)$ be the given proposition. Now $P(1)$ implies $2 > 1$ which is true. Hence $P(1)$ is true

Induction hypothesis: Let us assume that $P(m)$ is true. That is $2^m > m$ Now $2^{m+1} = 2 \cdot 2^m > 2m$. We know that $2m = m + m \geq m + 1$ for all $m \in N$. Therefore $2^{m+1} > m + 1$. Hence $P(m+1)$ is true.

Therefore by induction $P(n)$ is true for all n.

2.2.12Example: Show by induction that $n(n+1)(2n+1)$ is divisible by 6.

Solution: Let $P(n) = n(n+1)(2n+1)$

Now $P(1) = 1 \, . \, (1+1)(2+1) = 6$, this is divisible by 6.

Assume that $P(m)$ is divisible by 6.

That is, $m(m+1)(2m+1)$ is divisible by 6.

Therefore $m(m+1)(2m+1) = 6k$ for some integer k.

Now

$$\begin{aligned} P(m+1) &= (m+1)\,[(m+1)+1]\,[2\,(m+1)+1] \\ &= (m+1)(m+2)(2m+3) \\ &= (m+1)(m+2)\left(\overline{2m+1}+2\right) \\ &= (m+1)(m+2)(2m+1) + 2(m+1)(m+2) \\ &= m(m+1)(2m+1) + 2(m+1)(2m+1) + 2(m+1)(m+2) \\ &= 6k + 2(m+1)(3m+3) \qquad \text{by induction hypothesis} \\ &= 6k + 6(m+1)^2 \end{aligned}$$

Since each term on the R.H.S is divisible by 6 their sum is also divisible by 6.

Hence $P(m+1)$ is divisible by 6. Therefore by induction $P(n)$ is divisible by 6 for all $n \in N$

2.3 Matrices and Operations

2.3.1 Definition: A **matrix** A is a rectangular array of numbers arranged as m horizontal rows, n vertical columns. It is written as $A = \begin{bmatrix} a_{11} & a_{12}\ldots\ldots & a_{1n} \\ a_{21} & a_{22} & a_{2n} \\ \vdots & & \\ a_{m1} & \ldots\ldots\ldots & a_{mn} \end{bmatrix}$

The element in the ith row and jth column is a_{ij}. So A is also written as $\left[a_{ij}\right]_{\substack{1\le i\le m \\ 1\le j\le n}}$ or simply $[a_{ij}]$. A is called an m × n matrix. We also write the (i, j)th entry as $(A)_{ij}$. When m = n, then A is called a square matrix (also called n – square matrix A).

2.3.2 Example: A = $\begin{bmatrix} 2 & -5 & 4 & -1 \\ 1 & 0 & 6 & 5 \\ 4 & -6 & 8 & -6 \end{bmatrix}$, $B=\begin{bmatrix}2 & 1 & 5\end{bmatrix}$, $C=\begin{bmatrix}5\\-4\\-8\\-1\end{bmatrix}$, $D=\begin{bmatrix}0 & 0 & 2\\4 & 1 & -4\\5 & 0 & -6\end{bmatrix}$ are respectively, 3 × 4 , 1 × 3, 4 ×1and 3 × 3 matrices respectively.

2.3.3 Definition: Two matrices $A=\left[a_{ij}\right]$ and $B=\left[b_{ij}\right]$ are said to be **equal** if (i) the number of rows and columns of A and B are the same, (ii) $a_{ij} = b_{ij}$ for all i, j.

Self Assessment Question 2: How many entries are there in an m × n matrix ?

2.3.4 Definition: Let $A=\left[a_{ij}\right]$ and $B=\left[b_{ij}\right]$ be two m × n matrices. Then the sum A + B is defined as an m × n matrix as follows:

$$A+B=\left[a_{ij}+b_{ij}\right]_{\substack{1\le i\le m\\ 1\le j\le n}}$$

Observation: To get the sum of A and B, we add to an entry in A, the entry in B in the same place. We can add only two matrices of the same size.

2.3.5 Definition: Let $A=\left[a_{ij}\right]$ and $B=\left[b_{ij}\right]$ be two m × n matrices then A – B is defined as an m x n matrix as follows: $A-B=\left[a_{ij}-b_{ij}\right]_{\substack{1\le i\le m\\ 1\le j\le n}}$

2.3.6 Definition: Let $A=\left[a_{ij}\right]$ and k be a scalar (any real number). Then kA is defined as $kA=\left[ka_{ij}\right]_{\substack{1\le i\le n\\ 1\le j\le n}}$

Self Assessment Question 3: If $A=\begin{bmatrix}2 & 3 & 4\\ 5 & 6 & 7\end{bmatrix}$ and $B=\begin{bmatrix}7 & 8 & 9\\ 1 & 2 & 3\end{bmatrix}$, find A + B, A – B, 2A.

2.3.7 Definition: (i) The matrix that all its entries zero, that is $\begin{bmatrix}0 & 0 & \cdots & 0\\ \vdots & & & \\ 0 & 0 & \cdots & 0\end{bmatrix}$, is called the **zero matrix**. We denote as O.

(ii) The matrix of type $\begin{bmatrix}1 & 0 & \ldots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & & & \\ 0 & 0 & \ldots & 1\end{bmatrix}$ is called the **n–square unit matrix**. The number of rows is equal to the number of columns in the unit matrix. It is denoted by I_n.

(iii) A square matrix is a **diagonal matrix** if only the entries on the diagonal are nonzero and other entries are 0's. For example, $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix}$.

2.3.8 Definition: If $A = \left[a_{ij}\right]$ is an m × n matrix then the transpose of A denoted by A^T is defined as $A^T = \left[a_{ji}\right]_{\substack{1 \le j \le n \\ 1 \le i \le m}}$. The transpose of an m × n matrix is an n × m matrix.

The following theorem lists properties of addition of matrices.

2.3.9 Properties: If A, B, C are m × n matrices and k and l are scalars,

a) $A + (B + C) = (A + B) + C$

b) $A + 0 = 0 + A$ where 0 is the m × n zero matrix.

c) $A + (-A) = (-A) + A = 0$ (Here $-A$ denotes $(-1)\,A$)

d) $A + B = B + A$

e) $k(A+B) = kA + kB$

f) $(k+l)\,A = kA + lA$

g) $(kl)\,A = k\,(lA) = l(kA)$

h) $lA = A$

i) $(A+B)^T = A^T + B^T$

j) $\left(A^T\right)^T = A$

k) $(I_n)^T = I_n$

2.3.10 Definition: If A is an m × n matrix and B is an n × p matrix, then the **product** of A and B, denoted by AB, is an m × p matrix and is defined by $(AB)_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots + a_{in}b_{nk}$, for $1 \le i \le m$, $1 \le k \le p$. The matrix $(AB)_{ik}$ can be understood as follows.

$\begin{bmatrix} a_{i1}, & a_{i2}, & \ldots. & a_{in} \end{bmatrix}$ is the i^{th} row of A, $\begin{bmatrix} b_{1k} \\ b_{2k} \\ \vdots \\ b_{nk} \end{bmatrix}$ is the k^{th} column of B and both these have n elements. For calculating $(AB)_{ik}$, multiply the respective elements of i^{th} row of A and k^{th} column of B and add them. The resulting number is $(AB)_{ik}$. We can define the product of three matrices A, B, C when the number of columns of A = Number of rows of B; and Number of columns of B = Number of rows of C.

Let A, B, C be three matrices. Then the following hold well whenever the sums and products of matrices appearing below are defined.

a) (AB) C = A (BC) (Associative law)

b) A (B+C) = AB + AC (Left distributive law)

c) (B+C) A = BA + CA (Right distributive law).

2.3.12 Example: Let $A = \begin{bmatrix} 2 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 2 \\ 4 & 6 \\ 0 & 1 \end{bmatrix}$. Now A is a 2 × 3 matrix and B is a 3 × 2 matrix. So AB is a 2 × 2 matrix, given by

$$AB = \begin{bmatrix} 2(1)+0(4)+1(0) & 2(2)+0(6)+1(1) \\ -1(1)+0(4)+1(0) & -1(2)+0(6)+1(1) \end{bmatrix} = \begin{bmatrix} 2 & 5 \\ -1 & -1 \end{bmatrix}.$$

Self Assessment Question 4: Find BA for matrices A and B given in Example 2.3.11.

2.3.13 Note: We have seen that A + B = B + A when A and B are matrices of the same size. But

AB ≠ BA in general. It can happen that one of the products is defined whereas the other product is not defined. Consider the following example.

2.3.14 Problem: Give two matrices A and B such that

a) AB is defined but BA is not.

b) BA is defined but AB is not.

c) Both are defined but AB ≠ BA

d) Both are defined and AB = BA

Solution: a) Assume $A = \begin{bmatrix} 1 & 2 & 3 \\ -2 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -4 & 2 & -1 \\ 3 & 5 & 0 \\ 0 & 1 & -2 \end{bmatrix}$. Then AB is defined as the number of columns of A = 3 = number of rows of B. Number of columns of B = 3 ≠ number of rows of A. Hence BA is not defined.

b) If $A = \begin{bmatrix} -4 \\ 3 \\ 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 2 & 3 \\ -2 & 0 & 1 \end{bmatrix}$ then BA is defined, as number of columns of B = 3 = number of rows of A. Number of columns of A = 1 ≠ number of rows of rows of B. Hence AB is not defined.

c) Assume $A = \begin{bmatrix} 1 & 2 & 3 \\ -2 & 0 & 1 \end{bmatrix}_{2x3}$ and $B = \begin{bmatrix} -4 & 2 \\ 3 & 5 \\ 0 & 1 \end{bmatrix}_{3x2}$

Then $AB = \begin{bmatrix} 2 & 15 \\ 8 & -3 \end{bmatrix}$ and $BA = \begin{bmatrix} -8 & -8 & -10 \\ -7 & 6 & 14 \\ -2 & 0 & 1 \end{bmatrix}$. Hence $AB \neq BA$

d) Consider $A=\begin{bmatrix} 0 & 1 & 2 \\ 2 & -1 & 3 \\ 3 & 4 & 0 \end{bmatrix}$ and $B=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Then $AB=\begin{bmatrix} 0 & 1 & 2 \\ 2 & -1 & 3 \\ 3 & 4 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}=\begin{bmatrix} 0 & 1 & 2 \\ 2 & -1 & 3 \\ 3 & 4 & 0 \end{bmatrix}$ and

$$BA=\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 & 2 \\ 2 & -1 & 3 \\ 3 & 4 & 0 \end{bmatrix}=\begin{bmatrix} 0 & 1 & 2 \\ 2 & -1 & 3 \\ 3 & 4 & 0 \end{bmatrix}$$

Thus AB = BA.

Now we list the properties of multiplication.

2.3.15 Properties: If A is an m × n matrix and B is an n × p matrix and k is any scalar, then

a) $(AB)^T = B^TA^T$

b) $AI_n = A$ and $I_m A = A$

c) k (AB) = (kA)B = A(kB)

d) OA = O, BO = O where the four zero matrices are k × m, k × n, p × t and n × t matrices respectively (for some k and t).

2.4 Types of Matrices

2.4.1 Definition: A matrix $A=\left[a_{ij}\right]$ is called **symmetric** if $A = A^T$. That is, A is symmetric if and only if $a_{ij} = a_{ji}$ for $1 \le i \le m$, $1 \le j \le n$. If $A = -A^T$ then A is called **skew symmetric**. In a Skew-symmetric matrix, all the diagonal elements are zero.

2.4.2 Example: $A = \begin{bmatrix} a & h & g \\ h & b & f \\ g & f & c \end{bmatrix}$ is a symmetric matrix, since $A^T = A$.

$A = \begin{bmatrix} 0 & -h & g \\ h & 0 & -f \\ -g & f & 0 \end{bmatrix}$ is a Skew-symmetric matrix.

2.4.3 Properties: (i) $A + A^T$ is a Symmetric matrix

(ii) $A - A^T$ is a Skew-symmetric matrix

(iii) $A = \frac{1}{2}(A + A^T) + \frac{1}{2}(A - A^T)$.

2.4.4 Definition: A square matrix A is called an **orthogonal matrix** if the product of the matrix A and its transpose matrix A^T is an identity matrix.
That is, $AA^T = I = A^TA$.

2.4.5 Definition: A **Boolean matrix** is an m × n matrix whose entries are either 0 or 1.

We define three operations of Boolean matrices which have useful application: Boolean join, meet and product of matrices.

Let $A = \left[a_{ij}\right]$ and $B = \left[b_{ij}\right]$ be two m × n Boolean matrices. We define $A \vee B = C = \left[c_{ij}\right]$, the join of A and B by $c_{ij} = \begin{cases} 1 \text{ if } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 0 \text{ if both } a_{ij} \text{ or } b_{ij} \text{ are } 0 \end{cases}$

The meet of A and B, denoted by $A \wedge B = D = \left[d_{ij}\right]$, is defined as

$$d_{ij} = \begin{cases} 1 \text{ if } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 0 \text{ otherwise} \end{cases}$$

2.4.6 Example: Consider two matrices $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$.

Then $A \vee B = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ and $A \wedge B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$.

2.4.7 Properties: If A, B and C be three matrices of order m × n, then

1. $A \vee A = A$
2. $A \wedge A = A$
3. $A \vee B = B \vee A$
4. $A \wedge B = B \wedge A$
5. $A \vee (B \vee C) = (A \vee B) \vee C$
6. $A \wedge (B \wedge C) = (A \wedge B) \wedge C$
7. $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$
8. $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$

2.4.8 Definition: Let $A = \left[a_{ij}\right]$ be an m × p Boolean matrix and B = $\left[b_{ij}\right]$ be an p × n Boolean matrix. Then the Boolean product of A and B denoted by A ⊙ B is m × n Boolean matrix $C = \left[c_{ij}\right]$ defined by $c_{ij} = \begin{cases} 1 \text{ if } a_{ik} = 1 \text{ or } b_{kj} = 1, \text{for some } k, 1 \le k \le p \\ 0 \text{ otherwise} \end{cases}$

The (i, j)th element of C can be computed as follows:

(i) Select ith row of A and jth column of B ans arrange them side by side.

(ii) Compare the corresponding entries. If even a single pair of corresponding entries consists of two 1's, then $c_{ij} = 1$. Otherwise $c_{ij} = 0$.

2.4.9 Example: Let A = $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ and B = $\begin{pmatrix} 0101 \\ 1001 \\ 1110 \end{pmatrix}$. Now A ⊙ B = $\begin{pmatrix} 1101 \\ 1111 \\ 1101 \\ 1001 \end{pmatrix}$.

2.4.10 Note: The Boolean product is associative.

2.5 Answers to Self Assessment Questions

SAQ 1:

(a) Forms an A.P. in which $a = 1, \quad d = 2$ and $t_n = 1 + (n-1)2 = 2n - 1$.

(b) Forms an A.P. in which $a = 7, \ d = -4, \ t_n = 7 + (n-1)(-4) = 11 - 4n$

(c) Forms an A.P. in which $a = 1, \ d = \frac{1}{2}, \ t_n = 1 + (n-1)\frac{1}{2} = \frac{1}{2}(n+1)$.

(d) Forms a G.P. in which $a = 1, r = 3, t_n = 1 . 3^{n-1} = 3^{n-1}$

SAQ 2:

mn entries

SAQ3:

$$A+B = \begin{bmatrix} 9 & 11 & 13 \\ 6 & 8 & 10 \end{bmatrix},\ \text{A-B} = \begin{bmatrix} -5 & -5 & -5 \\ 4 & 4 & 4 \end{bmatrix},\ 2A = \begin{bmatrix} 4 & 6 & 8 \\ 10 & 12 & 14 \end{bmatrix}.$$

SAQ 4:

$$\begin{bmatrix} 0 & 0 & 3 \\ 2 & 0 & 10 \\ -1 & 0 & 1 \end{bmatrix}$$

2.6 Summary

In this lesson we studied the different types progressions like A.P., G. P. and H. P. The Principle of Mathematical induction is a useful tool in proving mathematical statements. We have also discussed the concept of matrices. The different types matrices is defined, and operations on matrices with illustrations given. The Boolean matrix is useful in digital computing analysis.

2.6 Technical Terms

Mathematical induction: Consists of the following two steps.

(i) Show by actual substitution that the theorem is true for $n = 1$

(ii) Assuming the theorem to be true for $n = m$, prove that it is also true for $n = m + 1$

Sum of the first n natural numbers: $1 + 2 + 3 + \ldots + n = \dfrac{n(n+1)}{2}$

Sum of squares of first n natural numbers: $1^2 + 2^2 + 3^2 + \ldots. + n^2 = \dfrac{n(n+1)(2n+1)}{6}$

Sum of cubes of first n natural numbers: $1^3 + 2^3 + 3^3 + \ldots.. + n^3 = \dfrac{n^2 (n+1)^2}{4}$,

Addition: Let $A = \left[a_{ij}\right]_{m \times n}$ and $B = \left[b_{ij}\right]_{m \times n}$.

$$A + B = \left[a_{ij} + b_{ij}\right]_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

Subtraction: Let $A = \left[a_{ij}\right]_{m \times n}$ and $B = \left[b_{ij}\right]_{m \times n}$.

$$A - B = \left[a_{ij} - b_{ij}\right]_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

Multiplication by a scalar: Let $A = \left[a_{ij}\right]$ and k be a scalar (any real number). Then

$$kA = \left[ka_{ij}\right]_{\substack{1 \le i \le n \\ 1 \le j \le n}}$$

Transpose matrix: If $A = \left[a_{ij}\right]$ is an m × n matrix then the transpose of A denoted by A^T is defined as $A^T = \left[a_{ji}\right]_{\substack{1 \le j \le n \\ 1 \le i \le m}}$. The transpose of an m × n matrix is an n × m matrix.

Product of matrices: If A is an m × n matrix and B is an n × p matrix then the product of A and B, denoted by AB, is an m × p matrix and is defined by $(AB)_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \ldots\ldots. + a_{in}b_{nk}$, for $1 \le i \le m$, $1 \le k \le p$.

Symmetric matrix: $A = A^T$.

Skew Symmetric matrix: $A = -A^T$

Orthogonal matrix: The product of the matrix A and its transpose matrix A^T is an identity matrix. That is, $AA^T = I = A^TA$.

2.8 Model Questions

1. Find the sum of first n natural numbers by the principle of mathematical induction.
2. Find the sum of the squares of first n natural numbers by the principle of mathematical induction
3. Find the sum of the cubes of first n natural numbers by the principle of mathematical induction.
4. Show by induction that $n(n+1)(2n+1)$ is divisible by 6.
5. Find the values of x, y, z and t satisfying the matrix relationship.

$$\begin{bmatrix} x+3 & z+4 & t-2 \\ 2y+5 & 4x+5 & 3t+1 \end{bmatrix} = \begin{bmatrix} 1 & -4 & 2t+5 \\ -5 & 2x+1 & -20 \end{bmatrix}$$

6. Find the values for x, y, z that satisfy the matrix relationship

$$3\begin{bmatrix} 2 & x \\ y & z \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ -1 & 2z \end{bmatrix} + \begin{bmatrix} 4 & x+2 \\ y+z & 3 \end{bmatrix}$$

7. If $A = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & -1 \end{bmatrix}$ and $C = \begin{bmatrix} 1 & 2 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$. Show that AB = AC. (Cancellation laws donot hold for matrices)
8. If $A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$, show that $A^2 - 2A - 5I = 0$.
9. If $A = \begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix}$ find AA^T and A^TA

10. If $A = \begin{bmatrix} 1 & 2 \\ 4 & -3 \end{bmatrix}$ evaluate A^2 and A^3.

2.9 References

1. Akerkar Rajendra and Akerkar Rupali "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, "Discrete Mathematical Structures" PHI, New Delhi, 1999.

3. Liu.C.L., "Elements of Discrete Mathematics", Mc Hill.

4. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. "Quantitative Methods", Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

5. Shanker Rao, G., "Discrete Mathematical Structures", New Age International Publishers, New Delhi, 2002.

6. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

Name of the Lesson Writer: **Dr Bhavanari Satyanarayana**
Professor

Lesson 3

Normal Forms and Logical Inference

Objectives

At the end of the Lesson the student must be able to:

(i) Understand the propositions.
(ii) Learn the validity of the arguments and tautologies.
(iii)Learn the disjunctive and conjunctive normal forms.
(iv)Understand the equivalence forms and inference rules.

Structure

3.1 Introduction

Logic means reasoning. The main aim of logic is to provide rules by which one can determine the validity of any particular argument or reasoning. The rules are called *rules of inference.* These rules should be independent of any particular argument or discipline or particular language used in the argument. We need an objective language to frame the rules or theory. The basic unit of our objective language is called a primary statement (variable). We assume that these statements cannot be further broken down or analyzed into simpler statements.

The basic unit of our objective language is called a *prime statement* (variable) (or *declarative sentence* or *Proposition*). We assume that these primary statements cannot be broken down further or analyzed into simpler statements. These primary statements have only one of the two possible values TRUE (T) or FALSE (F). These values T or F are referred as truth value of the primary statement. We often denote the truth value TRUTH (T) by ‘1’ and the truth value FALSE (F) by ‘0’.

Consider the following Examples:

(i) Moscow is the capital city of Italy.

(ii) $2 + 3 = 5$.

(iii)Hyderabad is the capital city of Andhra Pradesh.

(iv)New Delhi is the capital city of HUNGARY.

(v) Open the door

(vi)$1 + 2 = 3$

The statement (v) is not a primary statement because it has neither the truth value ‘T’ nor ‘F’. The remaining five statements are primary statements. Statements (ii), (iii) and (vi) have the truth value ‘T’ (or 1), and the statements (i) and (iv) have the truth value ‘F’ (or 0).

3.1.1 Example: Consider the case of a Researcher in Mathematics who has arrived at a reasonable conjecture. To verify this conjecture the Mathematician tries to construct a proof that will show that the statement of the conjecture follows logically from the accepted Mathematical statements. If he succeeds in this endeavor, he considers that he has proved his conjecture accepted Mathematical statement. Another Mathematician will accept this new statement only if he agrees that the proof is correct, or if he can construct a proof of his own. It appears that there lie some general rules and procedures for constructing proofs.

We shall mean, by formal logic, a system of rules and procedures used to decide whether or not a statement follows from some given set of statements. A familiar example from Aristotelian logic is:

(i). All men are mortal
(ii). Socrates is a man
Therefore (iii). Socrates is mortal.

According to the logic, if any three statements have the following form

(i) All M are P
(ii) S is M
Therefore (iii) S is P

then (iii) follows from (i) and (ii). The argument is correct, no matter whether the meanings of statements (i), (ii), and (iii) are correct. All that required is that they have the forms (i), (ii), and (iii). In Aristotelian logic, an argument of this type is called **syllogism**.

The formulation of the syllogism is contained in Aristotle's organon. It had a great fascination for medieval logicians, for almost all their work centered about ascertaining its valid moods. The three characteristic properties of a syllogism are as follows:

(i). It consists of three statements. The first two statements are called as **premises**, and the third statement is called as **conclusion**. The third one (**conclusion**) being a logical consequence of the first two (the **premises**).

(ii). Each of the three sentences has one of the four forms given in the Table

Classification	Examples
Universal and affirmative judgment	All *X* is *Y* All monkeys are tree climbers All integers are real numbers All men are mortal
Universal and negative judgment	No *X* is *Y* No man is mortal No monkey is a tree climber No negative number is a positive number
Particular and affirmative judgment	Some *X* is *Y* Some men are mortal Some monkeys are tree climbers Some real numbers are integers
Particular and negative judgment	Some *X* is not *Y* Some men are not mortal Some monkeys are not tree climbers Some real numbers are not integers

So a **syllogism** is an argument consisting of two propositions called **premises** and a third proposition called the **conclusion**.

3.2 Statements, Propositions and Tautologies

3.2.1 Definition: A **Proposition** is a statement that is either true or false, but not both.

3.2.2 Example: (i) "$x > 3$" is a statement. This statement is neither true nor false because the value of the variable x is not specified. Therefore "$x > 3$" is not a proposition.

(ii). "10 > 3" is a statement. This statement is true. Therefore "10 > 3" is a proposition.

(iii). "10 < 3" is a statement. This statement is false (or not true). Therefore "10 < 3" is a proposition.

3.2.3 Examples: (i). "$x + y + 4 = 7$" is a statement but it is not a proposition.

(ii). "$x \geq 3$" and "$x \geq 5$" are statements but not propositions (iii). "$x \geq 3$ for all x such that $x \geq 5$" is a statement. This statement is true. Therefore it is a proposition.

3.2.4 Examples: (i) "Hyderabad is the capital of Andhra Pradesh" is a statement. This is a true statement. Therefore it is a proposition.

(ii) "Guntur is the capital of Andhra Pradesh" is a statement which is false. Therefore it is a proposition.

(iii) "What is the time now ?". This is not a statement. So this is not a proposition.

(iv) "Read this carefully" is not a statement. So this is not a proposition.

Self Assessment Question 1: Verify whether or not the following are propositions.

(i) $1 + 1 = 2$, (ii). $2 + 2 = 3$, (iii) $x + y = 5 \Rightarrow x + y - 1 = 4$, (iv). $x = 2 \Rightarrow x^2 = 4$.

3.2.5 Negation: The negation of a statement is formed by means of the word "not". If "p" is a statement, then the negation of p is "$\sim p$". "$\sim p$" is read as "not-p". The symbol "~" is called "curl" or "twiddle" or "tilde". The notation "$\sim p$" is that of asserting the falsity of "p". If "p" considered to be false, then "$\sim p$" will be considered to be true.

3.2.6 Example: Let p be the statement "New York is a city". Now $\sim p$ is the statement "Not, New York is a city" (equivalently, "New York is not a city").

3.2.7 Definition: Let p be a statement. The statement "it is not the case that p" is another statement, called the negation of p.

3.2.8 Examples: (i). Let Q be the statement "All integers are real numbers", then the negation of this statement is $\sim Q$: Not, all integers are real numbers or

$\sim Q$: All integers are not real numbers.

(ii). Consider the statement given below

S: All angles can be trisected using straightedge and compass alone.

~S: There exists atleast one angle that cannot be trisected by using straightedge and compass alone.

(iii). Consider the statement given below

U: No angle can be trisected by suing straightedge and compass alone.

~U: Some angles can be trisected by using straightedge and compass alone.

The truth Table for the negation of a statement

P	***~P***
T	F
F	T

Here T stands for "True" and F stands for "False".

3.2.9 Definition: Let *P* and *Q* be statements. The statement "*P* and *Q*" (denoted by $P \wedge Q$) is true when both *P* and *Q* are true; and is false otherwise. $P \wedge Q$ is called the conjunction of *P* and *Q*.

3.2.10 Example: Consider the statement

P: "The number twelve is rational and positive",

A translation of *P* into symbols is not possible, since the word "positive" is not a statement. If the statement *P* is changed to form:

The number twelve is rational and the number twelve is positive.

Then a direct translation is "*A* & *B*", where "*A*" and "*B*" are translations given below.

A: the number twelve is rational, *B*: The number twelve is positive.

Truth Table for conjunction

P	***Q***	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

3.2.11 Example: Let P be the statement that "Today is a Friday" and Q be the statement "It is raining today". Then $P \wedge Q$ is the statement "Today is a Friday and it is raining today".

3.2.12 Example: (i) He will succeed or die in the attempt.

(ii). A simple closed curve in the plane divides it into two regions such that any point not on the curve is either inside or outside the curve.

3.2.13 Definition: The disjunction "or" is used to connect two classes (or sentences) to form a larger sentence. The meaning of this connection seems generally to be dependent on the meanings of the parts connected. If "P" and "Q" are statements, the "$P \vee Q$" is a statement that is true either when "P" is true or "Q" is true or both are true. "$P \vee Q$" is false only when both "P" and "Q" are false.

Truth Table for disjunction

P	Q	$P \vee Q$
T	T	T
F	T	T
T	F	T
F	F	F

3.2.14 Example: Let P be the statement that "Today is a Friday" and q be the statement that "It is raining to day". The $P \vee Q$ is the statement "Today is a Friday or it is raining today".

3.2.15 The Conditional (or Implication): The Conditional sentences are of type "if ………….., then………."

3.2.16 Example: Suppose x and y represent certain angles (see the following figure). Consider the following statements

A: x and y have their sides parallel

B: $x = y$

The above two statements may be combined as:

"If *x* and *y* have their sides parallel, then $x = y$" or "*x* and *y* having their sides parallel implies that $x = y$".

For this, consider the following diagram:

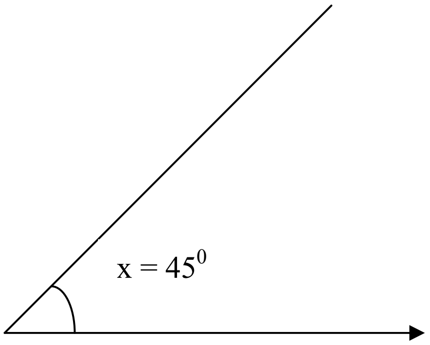


Fig. 3.2.16 (i)

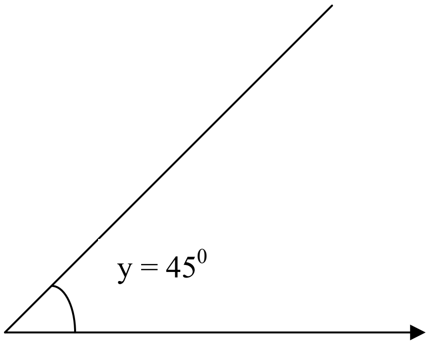


Fig.. 3.2.16 (ii)

This figure represents two angles of 45^0 with their sides parallel. Therefore $x = y$.

3.2.17 Definition: Let P and Q be propositions. The **implication** (denoted by $P \rightarrow Q$ or $P \Rightarrow Q$) is the proposition that is false when P is true and Q is false; and true otherwise. In this implication P is called the hypothesis (or antecedent or premise) and Q is called the conclusion (or consequence).

Truth Table for "Implication" is given below

P	***Q***	**P** $\rightarrow$ ***Q***
T	T	T
T	F	F
F	T	T
F	F	T

3.2.18 Examples: (i). "If $x > 10$, then $x > 2$" (or "$x > 10 \Rightarrow x > 2$") is a true statement (because if "$x > 10$" is true, then "$x > 2$" is also true)

(ii) If "today is a Sunday, then tomorrow is a Monday" (or today is a Sunday ⇒ tomorrow is a Monday) is true.

(iii). If "today is a Sunday, then tomorrow is a Saturday" is not true.

3.2.19 Note: "$P \to Q$" can be read in any one of the following ways

(i). P implies Q

(ii). Q is a (logical) consequence of P

(iii). P is a sufficient condition for Q

(iv). Q is a necessary condition for P

(v). If P then Q

(vi). If P, Q

(vii). P only if Q

(viii).Q if P

(ix). Q whenever P.

3.2.20 Example: If "$x = 5$", then "$2x = 10$" is a true statement.

3.2.21 Bi conditional (or imply and implied by or iff): Let P and Q be propositions. The bi-conditional P $\leftrightarrow$ Q is the proposition that is true when P and Q have the same truth values and is false otherwise.

P	Q	$\mathbf{P} \rightleftharpoons Q$
T	T	T
T	F	F
F	T	F
F	F	T

3.2.22 Note: (i). $p \leftrightarrow q$ may be read as "p is and only if q"

(ii). $p \leftrightarrow q$ means "$p \to q$ and $q \to p$"

(iii). It is clear that $p \leftrightarrow q$ is true precisely when both $p \to q$ and $q \to p$ are true.

3.2.23 Definition: A **tautology** is an expression which has truth value T for all possible values of the statement variables involved in that expression. A **contradiction** is an expression which has truth value F for all possible values of the statement variables involved in that expression. For example, P $\vee$ ~P is a tautology and P$\wedge$ ~P is a contradiction

3.2.24 Example: Construct the truth table for $((p \wedge \sim q) \to r) \to (p \to (q \vee r))$

Solution: Let E denote the expression as in the following table.

p	q	r	$p \wedge \sim q$	$(p \wedge \sim q) \to r$	$p \to (q \vee r)$	E
T	T	T	F	T	T	T
T	T	F	F	T	T	T
T	F	T	T	T	T	T
T	F	F	T	F	F	T
F	T	T	F	T	T	T
F	T	F	F	T	T	T
F	F	T	F	T	T	T
F	F	F	F	T	T	T

3.2.25 Example: (In this example, we denote the truth value T by '1' and the truth value F by '0'). Consider the statement $(p \vee q) \wedge \bar{r}$ where p, q and r are three propositions.

Truth table for $(p \vee q) \wedge \bar{r}$

p	q	r	$p \vee q$	$\bar{r}$	$(p \vee q) \wedge \bar{r}$
0	0	0	0	1	0
0	0	1	0	0	0
0	1	0	1	1	1
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	0	0

Self Assessment Question 2: Construct the truth table for $\bar{p} \wedge \bar{q}$

3.2.26 Problem: Show that $[p \wedge (p \vee q)] \wedge \bar{p}$ is a contradiction.

Solution: Now we write down the truth table

p	q	$p \vee q$	$p \wedge (p \vee q)$	$\bar{\text{p}}$	$[p \wedge (p \vee q)] \wedge \bar{\text{p}}$
0	0	0	0	1	0
0	1	1	0	1	0
1	0	1	1	0	0
1	1	1	1	0	0

Observing the table, we can conclude that $[p \wedge (p \vee q)] \wedge \bar{\text{p}}$ is always false. Hence $[p \wedge (p \vee q)] \wedge \bar{\text{p}}$ is a contradiction.

3.3 Equivalence of formulas

3.3.1 Definition: Let A and B be two statements involving the variables P_1, P_2. ..., P_n. We say that A and B are **equivalent** if the truth value of A is equal to the truth value of B for every 2^n-possible sets of truth values assigned to P_1, P_2, ..., P_n and is denoted by A $\Leftrightarrow$ B. In other words A $\Leftrightarrow$ B is a tautology.

3.3.2 Example: Prove that $(p \rightarrow q) \Leftrightarrow \sim p \vee q$.

Solution:

p	q	$p \rightarrow q$	$\sim p \vee q$
T	T	T	T
T	F	F	F
F	F	T	T
F	F	T	T

Therefore $(p \rightarrow q) \Leftrightarrow \sim p \vee q$.

3.3.3 Example: Prove that $\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$

Solution:

p	q	$\sim (p \vee q)$	$\sim p \wedge \sim q$
T	T	F	F
T	F	F	F
F	T	F	F
F	F	T	T

Hence $\sim(p \vee q) \Leftrightarrow \sim p \wedge \sim q$.

Self Assessment Question 3: Prove that $\sim(P \wedge Q) \rightarrow (\sim P \vee (\sim P \vee Q)) \Leftrightarrow \sim P \vee Q$.

3.4 Normal Forms

3.4.1 Definition: Let $P_1, P_2, ..., P_n$ be n statement variables. The expression $P_1^* \wedge P_2^* \wedge ... \wedge P_n^*$ where P_i^* is either P_i or $\sim P_i$ is called a **minterm**. There are 2^n such minterms.

The expression $P_1^* \vee P_2^* \vee ... \vee P_n^*$, where P_i^* is either P_i or $\sim P_i$ is called a **maxterm**. There are 2^n such maxterms.

3.4.2 Example: Let P. Q, R be the three variables.

Then the minterms are: $P \wedge Q \wedge R$, $P \wedge Q \wedge \sim R$, $P \wedge \sim Q \wedge R$, $P \wedge \sim \wedge \sim R$, $\sim P \wedge Q \wedge R$, $\sim P \wedge Q \wedge \sim R$, $\sim P \wedge \sim Q \wedge R$, $\sim P \wedge \sim Q \wedge \sim R$.

3.4.3 Definition: (i) For a given formula, an equivalent formula consisting of disjunction's of minterms only is known as its **disjunctive normal form** (DNF) or sum of products canonical form.

(ii) For a given formula, an equivalent formula consisting of conjunction of maxterms only is known as its **conjunctive normal form** (CNF) or product of sums canonical form.

3.4.4 Note: (i) DNF can be computed either by truth table or by direct computation.

(ii) If the DNF for a formula F is known then disjunction of the minterms which do not appear in the DNF of F is the DNF of $\sim F$.

(ii) Since $F \Leftrightarrow \sim(\sim F)$, we can compute CNF of F using D'Morgan's law.

3.4.5 Example: Obtain the DNF and CNF of the following formula:

$$(\sim P \vee \sim Q) \rightarrow (P \rightleftharpoons \sim Q)$$

Solution: Let E be the expression that $(\sim P \vee \sim Q) \rightarrow (P \rightleftharpoons \sim Q)$.

$E \Leftrightarrow (\sim P \vee \sim Q) \rightarrow ((P \rightarrow \sim Q) \wedge (\sim Q \rightarrow P))$

$\Leftrightarrow (\sim P \vee \sim Q) \rightarrow ((\sim P \rightarrow \sim Q) \wedge (Q \vee P))$

$\Leftrightarrow \sim (\sim P \vee \sim Q) \vee ((\sim P \vee \sim Q) \wedge (Q \vee P))$

$\Leftrightarrow (P \wedge Q) \vee ((\sim P \wedge Q) \vee (\sim P \wedge P)) \vee (\sim Q \wedge Q) \vee (Q \wedge P)$

$\Leftrightarrow (P \wedge Q) \vee (\sim P \wedge Q) \vee (P \wedge Q)$

$\Leftrightarrow (P \wedge Q) \vee (\sim P \wedge Q)$, which is in disjunctive normal form.

Now $\sim E \Leftrightarrow (P \wedge \sim Q) \vee (\sim P \wedge \sim Q)$ or

$E \Leftrightarrow \sim (\sim E) \Leftrightarrow (\sim P \vee Q) \wedge (P \vee Q)$, which is the CNF.

Using Truth Tables: Consider the following table.

P	Q	E
T	T	T
T	F	F
F	T	T
F	F	F

The DNF of E is the disjunction of the minterms with truth values T. Therefore

$E \Leftrightarrow (P \wedge Q) \vee (\sim P \wedge Q)$.

3.4.6 Example: Obtain the DNF and CNF for

$$(P \rightarrow (Q \wedge R)) \wedge (\sim P \rightarrow (\sim Q \wedge \sim R))$$

Solution: Let the expression E be $(P \rightarrow (Q \wedge R)) \wedge (\sim P \rightarrow (\sim Q \wedge \sim R))$

Now $E \Leftrightarrow (\sim P \vee (Q \wedge R)) \wedge (P \vee (\sim Q \wedge \sim R))$

$\Leftrightarrow (\sim P \vee Q) \wedge (\sim P \vee R) \wedge (P \vee \sim Q) (P \vee \sim R)$

$\Leftrightarrow (\sim P \vee Q \vee R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee \sim Q \vee R)$

$\Leftrightarrow (P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee \sim R) \wedge (P \vee Q \vee \sim R)$

$\Leftrightarrow (\sim P \vee Q \vee R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee \sim R) \wedge (P \vee Q \vee \sim R)$.

This is the CNF for E. Now

$\sim E \Leftrightarrow (\sim P \vee \sim Q \vee \sim R) \wedge (P \vee Q \vee R)$.

Therefore $E \Leftrightarrow \sim (\sim E) \Leftrightarrow (P \wedge Q \wedge R) \vee (\sim P \wedge \sim Q \wedge \sim R)$, which is the DNF of E.

Self Assessment Question 4: Write the following in the DNF and the CNF.

(a) $\sim P \vee Q$

(b) $(P \wedge Q) \vee (\sim P \wedge R) \vee (Q \wedge R)$.

(c) $P \rightarrow ((P \rightarrow Q) \wedge \sim (\sim Q \vee \sim P))$

3.5 Logical Inferences

The main function of logic is to provide rules of inference or principles of reasoning.

3.5.1 Definition: Any conclusion which is arrived at by following the rules is called a **valid conclusion** and argument is called a **valid argument**.

Let A and B be two statement formulas. We say that "B logically follows from A" or "B is a valid conclusion of A", if and only if A —b B is a tautology, that is, $A \Rightarrow B$.

3.5.2 Validity using truth table

Let $P_1, P_2, \ldots, P_n$ be the variables appearing in the premises $H_1, H_2, ..., H_m$ and the conclusion C. Let all possible combinations of truth values are assigned to $P_1, P_2, \ldots, P_n$ and let the truth values of $H_1, H_2, ..., H_m$ and C are entered in the table. We say that C follows logically from premises

$H_1, H_2, ..., H_m$ if and only if $H_1 \wedge H_2 \wedge \dots H_m \Rightarrow C$. This can be checked from the truth table using the following procedure:

I. Look at the rows in which C has the value F.

2. In every such row if at least one of the values of $H_1, H_2, ..., H_m$ is F then the conclusion is valid.

3.5.3 Example: Show that the conclusion C: ~ P follows from the premises H_1: ~ P ∨ Q, H_2: ~ (Q ∧ ~ R) and H_3: ~ R.

Solution: Given that C: ~ P, H_1: ~ P ∨ Q, H_2: ~ (Q ∧ ~ R) and H_3: ~ R.

P	Q	R	H_1	H_2	H_3	C
T	T	T	T	T	F	F
T	T	F	T	F	T	F
T	F	T	F	T	F	F
T	F	F	F	T	T	F
F	T	T	T	T	F	T
F	T	F	T	F	T	T
F	F	T	T	T	F	T
F	F	F	T	T	T	T

The rows in which C has the truth values F at least one of H_1, H_2, H_3 has truth value F. Thus C logically follows form H_1, H_2, and H_3.

3.5.4 Validity using rules of Inference:

We now describe the process of derivation by which one demonstrates that a particular formula is a valid consequence of a given set of premises. The following are the three rules of inference.

Rule P: A premise may be introduced at any point in the derivation.

Rule T: A formula S may be introduced in a derivation If Sis tautologically implied by any one or more of the preceding formulas in the derivation.

Rule CP: If we can derive S from R and a set of premises then we can derive R → S from the set of premises alone.

Before we proceed with the actual process of derivation, we flat some important implications and equivalences that will be referred to frequently. Not all the implications and equivalences listed in tables respectively are independent of one another. One could start with only a minimum number of them and derive the others by using the above rules of inference.

3.5.5 Example: Show that the conclusion C: ~ P follows from the premises

H_1: ~ P ∨ Q, H_2: ~ (Q ∧ ~ R) and H_3: ~ R.

Solution: We get

(1) ~ R Rule P (assumed premise)

(2) ~ (Q ∧ ~ R) Rule P

{2} (3) ~ Q ∨ R Rule T

{3} (4) R ∧ ~ Q Rule T

{4} (5) ~ R → ~ Q Rule T

{1, 5} (6) ~ Q Rule T

(7) ~ P ∨ Q Rule P

{7} (8) ~ Q → ~ P Rule T

{6, 8} (9) ~ P Rule T

Hence C logically follows from H_1, H_2, and H_3.

3.5.6 Example: Show that S ∨ R is tautologically implied by (P∨Q)∧(P → R) ∧(Q → S).

Solution: We have

(1) P ∨ Q Rule P

{1} (2) ~ P → Q Rule T

(3) Q → S Rule P

{2, 3}	(4) $\sim P \rightarrow S$	Rule T
	(5) $\sim S \rightarrow P$	Rule T (as $P \rightarrow Q \Leftrightarrow \sim Q \rightarrow \sim P$)
	(6) $P \rightarrow R$	Rule P
{5, 6}	(7) $\sim S \rightarrow R$	Rule T
{7}	(8) $S \vee R$	Rule T

3.5.7 Example: Show that $R \rightarrow S$ can be derived from the premises $P \rightarrow (Q \rightarrow S)$, $\sim R \vee P$ and Q.

Solution: We get

	(1) R	Rule P
	(2) $\sim R \vee P$	Rule P
{2}	(3) $R \rightarrow S$	Rule T
{1, 3}	(4) P	Rule T
	(5) $P \rightarrow (Q \rightarrow S)$	Rule P
{4, 5}	(6) $Q \rightarrow S$	Rule T
	(7) Q	Rule P
{7, 6}	(8) S	Rule T
	(9) $R \rightarrow S$	Rule CP

3.5.8 Validity by Indirect Method:

In order to show that a conclusion C follows logically from the premises $H_1, H_2, ..., H_m$ we assume that C is FALSE and consider ~C as an additional premise. If $H_1 \wedge H_2 \wedge ... \wedge H_m \wedge \sim C$ is a contradiction, then C follows logically from $H_1, H_2, ..., H_m$.

3.5.9 Example: Show that $\sim (P \wedge Q)$ follows from $\sim P \wedge \sim Q$.

Solution: Assume $\sim (\sim (P \wedge Q))$ as an additional premise. Then

	(1) $\sim(\sim(P \wedge Q))$	Rule P
{1}	(2) $P \wedge Q$	Rule T
	(3) P	Rule T
	(4) $\sim P \wedge \sim Q$	Rule P
{4}	(5) $\sim P$	Rule T
{3, 5}	(6) $P \wedge \sim P$	Rule T

Therefore $P \wedge \sim P$ is a contradiction. Hence by the indirect method of proof $\sim(P \wedge Q)$ follows from $\sim P \wedge \sim Q$.

3.6 Answers to Self Assessment Questions:

SAQ 1.

(i) "1 + 1 = 2" is a true statement and hence it is a proposition.

(ii). "2 + 2 = 3" is a statement which is false. Therefore it is a proposition.

(iii). "$x + y = 5 \Rightarrow x + y - 1 = 4$" is a true statement. Therefore it is a proposition.

(iv). "$x = 2 \Rightarrow x^2 = 4$" is a true statement. Therefore it is a proposition.

SAQ 2.

Truth table for $\bar{p} \wedge \bar{q}$ is given below

p	q	$\bar{p}$	$\bar{q}$	$\bar{p} \wedge \bar{q}$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	0	0	0

SAQ 3

SAQ 4.

(a) CNF: $(\sim P \vee Q)$

DNF: $(\sim P \wedge \sim Q) \vee (\sim P \wedge Q) \vee (P \wedge Q)$

(b) DNF: $(P \wedge Q) \vee (\sim P \wedge R) \vee (Q \wedge R)$

CNF: $(\sim P \vee Q \vee \sim R) \wedge (\sim P \vee Q \vee R) \wedge (P \vee \sim Q \vee R) \wedge (P \vee Q \vee R)$.

(c) DNF: $(\sim P \wedge Q) \vee (\sim P \wedge \sim Q) \vee (P \wedge Q)$

CNF: $(\sim P \vee Q)$.

3.7 Summary

Logic was discussed by its ancient founder Aristotle (384 BC – 322 BC) from two quite different points of view. On one hand he regarded logic as an instrument or organ for appraising the correctness or strength of the reasoning; On the other hand, he treated the principles and methods of logic as interesting and important topics of the study. The study of logic will provide the reader certain techniques for testing the validity of a given arguments. Logic provided the theoretical basis for many areas of computer science such as digital logic design, automata theory and computability, and artificial intelligence. In this lesson we have discussed the truth tables, validity of arguments using the rules of inference. Further, we studied the various normal forms and logical equivalences using the rules.

3.8 Technical Terms

Proposition: A Proposition is a statement that is either true or false, but not both.

Implication: Let P and Q be propositions. The implication (denoted by $P \to Q$ or $P \Rightarrow Q$) is the proposition that is false when P is true and Q is false; and true otherwise.

Bi conditional: Let P and Q be propositions. The bi-conditional $P \leftrightarrow Q$ is the proposition that is true when P and Q have the same truth values and is false otherwise.

Tautology: A *tautology* is an expression which has truth value T for all possible values of the statement variables involved in that expression.

Contradiction: is an expression which has truth value F for all possible values of the statement variables involved in that expression.

Equivalent forms: $A \Leftrightarrow B$ is a tautology.

DNF: For a given formula, an equivalent formula consisting of disjunction's of minterms or sum of products canonical form.

CNF: For a given formula, an equivalent formula consisting of conjunction of maxterms or product of sums canonical form.

Rule P: A premise may be introduced at any point in the derivation.

Rule T: A formula S may be introduced in a derivation If Sis tautologically implied by any one or more of the preceding formulas in the derivation.

Rule CP: If we can derive S from R and a set of premises then we can derive $R \rightarrow S$ from the set of premises alone.

3.9 Model Questions

1. Prove that the equivalence $\sim (p \wedge q) \Leftrightarrow \sim p \vee \sim q$.

2. Show the validity of the following argument for which premises are given in the left and conclusion on the right:

(a) $P \to Q, Q \to R$	$P \to R$
(b) $\sim Q, P \to Q$	$\sim P$
(c) $\sim (P \wedge \sim Q), \sim Q \vee R, \sim R$	$\sim P$
(d) $(P \wedge Q) \to R, \sim R \vee S, \sim S$	$\sim P \vee \sim Q$.

3. Prove the following using the Rule CP if necessary:

(a) $P \to Q \Rightarrow P \to (P \wedge Q)$

(b) $P, P \to (Q \to (R \wedge S)) \Rightarrow Q \to S$

(c) $P \to (Q \to R), Q \to (R \to S) \Rightarrow P \to (Q \to S)$.

4. Show that the following statements constitute a valid argument “If A works hard then either B or C enjoys himself. If B enjoys himself then A will not work hard. If D enjoys himself then C will not. Therefore, if A works hard D will not enjoy himself.”

5. “If there was a meeting then catching the bus was difficult. If they arrived on time catching the bus was not difficult. They arrived on time. Therefore there was no meeting”. Show that the statement constitutes a valid argument.

6. Show that $R \to S$ can be derived from the premises $P \to (Q \to S), \sim R \vee P$ and Q.

3.10 References

1. Akerkar Rajendra and Akerkar Rupali “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, “Discrete Mathematical Structures” PHI, New Delhi, 1999.

3. Hari Kishan and Shivraj Pundir “Discrete Mathematics”, Pragati Prakashan, Meerut, 2005.

4. Liu.C.L., “Elements of Discrete Mathematics”, Mc Hill.

5. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

6. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Bhavanari Satyanarayana**
Professor

Lesson 4

Predicate Logic

Objectives

At the end of the Lesson the student must be able to:

(i) Understand the fundamental idea of logical statements.
(ii) Learn the symbolic representation of statements.
(iii)Learn the predicate formulas
(iv)Understand the logical quantifiers.

Structure

4.1 Introduction

Let us first consider the two statements:

John is a bachelor

Smith is a bachelor.

Obviously, if we express these statements by symbols, we req two different symbols to denote them. Such symbols do not reveal the features of these two statements; viz., both are statements about two different individuals who are bachelors. If we introduce some symbol to denote “is a bachelor” and a method to join it with symbols denoting the names of individuals, then we will have a symbolism to denote statements about any individual’s, being a bachelor. Now we introduce the predicates.

4.2 Predicates

The part “is a bachelor” is called a *predicate*. Another so which led to some similar device for the representation of statements is by the following argument.

All human beings are
John is a human being.
Therefore, John is a mortal.

We shall symbolize a predicate by a capital letter and individuals or objects in general by small letters. We shall soon see letters to symbolize statements as well as predicates will not confusion. Every predicate describes something about one or more objects.

We again consider the statements

1. John is a bachelor.
2. Smith is a bachelor.

Denote the predicate “is a bachelor” symbolically by the predicate letter B, “John” by j, and “Smith” by s. Then statements (1) and (2) can be written as B(j) and B(s) respectively. In general, any statement of the type “p is Q” where Q is a predicate and p is the subject can be denoted by Q(p).

A predicate requiring m (m >0) names is called an m-place predicate. For example, B in (1) and (2) is a 1-place predicate. Another example is that "L: is less than" is a 2-place predicate. In order to extend our definition to m = 0, we shall call a statement a 0-place predicate because no names are associated with a statement.

4.2.1 Example: Consider, now, statements involving the names of two objects, such as
Jack is taller than Jill. --------(1)
Canada is to the north of the United States. --------(2)

The predicate "is taller than" and "is to the north of" are 2-place predicates names of two objects are needed to complete a statement involving these predicates.
If the letter G symbolizes "is taller than," j_1 denotes "Jack," j_2 denotes "Jill," then statement (1) can be translated as G (j_1, j_2). Note that the order in which the names appear in the statement as well as in the predicate is important.

Similarly, if N denotes the predicate "is to the north of," c: Canada, and s: United States, then (2) is symbolized as N(c, s). Obviously, N(s, c) is the statement "The United States is to the north of Canada."

4.2.2 Examples: 3-place predicate: Susan sits between Ralph and Bill.
4-place predicate: Green and Miller played bridge against Johnston and Smith.

4.2.3 Note: An n-place predicate requires n names of objects to be inserted in fixed positions in order to obtain a statement.

4.2.4 Definition: A **simple statement function** of one variable is defined to be an expression consisting of a predicate symbol and an individual variable. Such a statement function becomes a statement when the variable is replaced by the name of any object.

4.2.5 Example: Let H be a predicate 'is beautiful', s be the name 'Senthil' and m be the name 'Mythily'. Then H(x) is a simple statement function.

If we replace x by s or m, then H(x) becomes a statement, x is used as a place holder.

4.2.6 Note: Statement functions are obtained from combining one or more simple statement functions and the logical connectives. Statement functions of two or more variables can be defined in a similar manner.

4.2.7 Example: In the statement function G(x, y): x is richer than y if x and y are replaced by names 'Raja' and 'Kutti' then we have the statements:

G(r, k): Raja is richer than Kutti.

G(k, r): Kutti is richer than Raja.

There is another way for obtaining statements. In this regard we introduce the notion of quantifiers such as 'all' and 'some'.

Self Assessment Question 1: Give some examples of first order predicates.

4.3 Quantifiers

4.3.1 Definition: The word 'all' is called the **universal quantifier** and is denoted by (x) or for all x. This symbol is placed before the statement function.

4.3.2 Example: For example, consider the statement functions:

M(x): is a mathematician.

I(x): x is intelligent.

Then (x) $(M(x) \rightarrow I(x))$ denotes the statement "for all x, if x is a mathematician then x is intelligent".

4.3.3 Note: The statements (x) $(M(x) \rightarrow I(x))$ and (y) $(M(y) \rightarrow I(y))$ are equivalent.

4.3.4 Example: Let G(x, y): x is richer than y. Then
$(x)(y)\ (G(x, y) \rightarrow \sim G(y, x))$ denotes the statements "For any x and any y, if x is richer than y then y is not richer than x".

4.3.5 Definition: The word 'some' is called the **existential quantifier** and is denoted by $\exists x$. This also means 'for some', 'there is at least one' or 'there exists some'. The symbol $\exists!\ x$ is read "there is a unique x such that".

4.3.6 Example: Let
M(x): x is a man
C(x): x is clever
I(x): x is an integer
E(x): x is even
P(x): x is prime.
Then
$\exists\ x\ M(x)$ symbolizes "There exists a man"
$\exists\ x\ (M(x) \wedge C(x))$ symbolizes "There are some men who are clever".
$\exists\ x\ (I(x) \wedge E(x))$ symbolizes "Some integers are even" or "There are some integers which are even".
$\exists!\ x\ (E(x) \wedge P(x))$ symbolizes "There exists unique even prime".

Self Assessment Question 2: Translate each of the statement into symbols, using quantifiers, variables and predicate symbols.

Let P(x): x can speak Telugu and Q(x): x knows the language C^{++}

(a) There is a student who can speak Telugu and who knows C^{++}

(b) There is a student who can speak Telugu but does not know C^{++}

(c) Every student either can speak Telugu or knows C^{++}

(d) No student can speak Telugu or knows C^{++}.

4.3.7 Definition: Variables which are quantified stand for only those objects which are members of a particular set or class. Such a set is called the **universe of discourse** or the **domain** or **simply universe**.

4.3.8 Note: The universe may be, the class of human beings, or numbers (real, complex, and rational) or some other objects. The truth value of a statement depends upon the universe.

4.3.9 Example: consider the predicate Q(x): x is less than 10 and the statements (x) Q(x) and ∃ x Q(x).

Now, consider the following universes:

U_1: {—1, 0, 1, 2, 4, 6, 8}

U_2: {3, —2, 12, 14, 10}

U_3: {l0, 20, 30, 40}

The statement (x) Q (x) is true in U_1 and false in U_2 and U_3.

The statement ∃ x Q(x) is true in U_1 and U_2 and false in U_3.

4.3.10 Example: Let the universe of discourse be the set of integers. Determine the truth values of the following sentences:

1. $(x)\ (x^2 \geq 0)$
2. $(x)\ (x^2-5x+6 = 0)$
3. $\exists(x)\ (x^2-5x+6 = 0)$
4. $(y)(\exists\ x\ (x^2 = y))$

Solution: 1. True, 2. False, 3. True, 4. Flase.

Self Assessment Question 3: Symbolize the statement "All men are giants."

4.3.11 Example: Consider the statement "Given any positive integer, there is a greater positive integer." Symbolize this statement with and without using the set of positive integers as the universe of discourse.

Solution: With Universe of discourse:

Let the variables x and y be restricted to the set of positive integers.

Then the above statement can be paraphrased as follows: For all x, there exists a y such that y is greater than x. If G(x, y) is "x is greater than y" then the given statement is

$(x)\ (\exists y)\ (G(y, x).$

With out universe of discourse: Let P(x) stands for x is a positive integer. Then we can symbolize the given statement as $(x)\ (P(x) \rightarrow (\exists y)\ (P(y) \wedge G(y, x)))$.

4.4 Free and Bound Occurrences

4.4.1 Definition: The expression $P(x_1, x_2, \ldots, x_n)$ where $x_1, x_2, \ldots, x_n$ are individual variables and P is an n-place predicate, is called an **atomic formula**.

For example: R, Q(x), P(x, y), A(x, y, z), P(a, y) …. etc.

4.4.2 Definition: A well-formed formula (wff) of predicate calculus is obtained by using the following rules.

a) An atomic formula is a wff.

b) If A is a wff, then $\sim A$ is a wff.

c) If A and B are wff, then $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ and $(A \rightleftharpoons B)$ are also wff.

d) If A is a wff and x is any variable, then (x)A and $(\exists x)$ A are wff.

e) Only those formulas obtained by using rules (1) to (4) are wff.

4.4.3 Definition: In a formula a part of the form (x) p(x) or $\exists$ x p(x) is called an x-**bound part**. Any occurrence of x in an x-bound part is called a **bound occurrence** of x while any occurrence of x or of any variable that is not a bound occurrence is called a **free occurrence**. The formula p(x) either in (x) p(x) or $\exists$ x p(x) is called the *scope* of the quantifier. In a statement every occurrence of a variable must be bound and no variable should have a free occurrence.

4.4.4 Example: Consider the following formulas:

$(x)P(x, y)$ --(1)

$(x)(P(x) \to Q(x))$ ----------------------------------- (2)

$(x)\,(P(x) \to (\exists y)R(x, y))$ ----------------------------(3)

$(x)(P(x) \to R(x)) \vee (x)(P(x)\text{—.}Q(x))$ --------------(4)

$(\exists x)(P(x) \wedge Q(x))$ ---------------- (5)

$(\exists x)P(x) \wedge Q(x)$ ----------------------(6)

In (1), P(x, y) is the scope of the quantifier, and both occurrences of a are bound occurrences, while the occurrence of y is a free occurrence.

In (2), the scope of the universal quantifier is $P(x) \to Q(x)$, and all occurrences of x are bound.

In (3), the scope of (x) is $P(x) \to (\exists y)\ R(x,y)$, while the scope of $(\exists y)$ is R(x, y). All occurrences of both x and y are bound occurrences.

In (4), the scope of the first quantifier is $P(x) \to R(x)$, and the scope of the second is $P(x) \to Q(x)$. All occurrences of x are bound occurrences.

In (5), the scope of $(\exists x)$ is $P(x) \wedge Q(x)$.

In (6), the scope of $(\exists x)$ is P(x), and the last occurrence of x in Q(X) is free.

4.4.5 Example: Symbolize the following:

1. All birds can fly.

2. All babies are innocent.

3. There is an integer such that it is odd and prime.

4. Not all birds can fly.

Solution: We get

1. Denote $B(x)$: x is a bird; $F(x)$: x can fly.

Then the symbolic form of "All birds can fly" is $(x)\ (B(x) \text{ — } F(x))$

2. Denote $B(x)$: x is a baby; $I(x)$: x is innocent.

Then the symbolic form of "All babies are innocent" is $(x)\ (B(x) \rightarrow I(x))$

3. Denote $O(x)$: x is odd; $P(x)$: x is prime.

Then the symbolic form of "There is an integer such that it is odd and prime" is

$\exists\, x\ (O(x) \wedge P(x))$.

4. $B(x)$: x is a bird; $F(x)$: x can fly.

Then the symbolic form of "Not all birds can fly" is

$\sim [(x)(B(x) \rightarrow F(x))]$ or $\exists\, x\ (B(x) \wedge \sim F(x))$.

Self Assessment Question 4: Symbolize the expression "All the world respect selfless Leaders".

4.4.6 Example: Let

$P(x)$: x is a person

$F(x, y)$: x is the father of y

$M(x, y)$: x is the mother of y.

Write the predicate " x is the father of the mother of y"

Solution: In order to symbolize the predicate we name a person called z as the mother of y. Obviously, we want to say that x is the father of z and z mother of y.

It is assumed that such a person z exists. We symbolize the predicate

$$(\exists z)\ (P(z) \wedge F(x, z) \wedge M(z, y))$$

4.4.7 Example: Symbolize the expression "All the world loves a lover."

Solution: First note that the quotation really means that everybody loves a lover.
Now let P(x): x is a person; L(x): x is a lover; R(x, y): x loves y.
The required expression is
$(x)\ (P(x) \rightarrow (y)(P(y) \wedge L(y) \rightarrow R(x, y)))$.

Self Assessment Question 5: Write the negation of the following.
(a). For each integer x, if x is even then $x^2 + x$ is even.
(b). There is an integer x such that $x^2 = 9$.

4.5 Rules of Inference

4.5.1 Definitions: (a) **Universal specification (US)**: If (x) P(x) is assumed to be true then the universal quantifier can be dropped to obtain P(c) is true, where c is an arbitrary object in the universe.
(b) **Universal generalization (UG)**: If P(c) is true for all c in the universe then the universal quantifier may be prefixed to obtain (x) P(x).
(c) **Existential specification (ES)**: If $\exists$ x P(x) is assumed to be true then P(c) is true for some element c in the universe.
(d) ***Existential generalization (EG)***: If P(c) is true for some element c in the universe then $\exists$ x P(x) is true.

4.5.2 Example: Consider the following statements:
All men are selfish.
All kings are men.
Prove that all kings are selfish.

Solution: Let

M(x): x is a man.

K(x): x is a king.

S(x): x is selfish.

The above arguments are symbolized as,

(1)	$(x)M(x) \to S(x))$	P
(2)	$M(c) \to S(c)$	US, (1)
(3)	$(x)(K(x) \to M(x))$	P
(4)	$K(c) \to M(c)$	US, (3)
(5)	$K(c) \to S(c)$	(2), (4) and inference rule
(6)	$(x)(K(x) \to S(x))$	UG

4.5.3 Example: Show that $(x)(P(x) \to Q(x)) \wedge (x)(Q(x) \to R(x)) \Rightarrow (x)(P(x) \to R(x))$

Solution: The given statement is symbolized as

(1)	$(x)(P(x) \to Q(x))$	P
(2)	$P(y) \to Q(y)$	US (1)
(3)	$(x)(Q(x) \to R(x))$	P
(4)	$Q(y) \to R(y)$	US (3)
(5)	$P(y) \to R(y)$	(2), (4), and Inference Rule
(6)	$(x)(P(x) \to R(x))$	UG, (5).

4.5.4 Example: Show that $\exists x(P(x) \wedge Q(x)) \Rightarrow (\exists xP(x)) \wedge (\exists x Q(x))$.

Solution: The given statement can be symbolized as

(1)	$\exists x(P(x) \wedge Q(x))$	P
(2)	$P(y) \wedge Q(y)$	ES, (1), y fixed
(3)	$P(y)$	T
(4)	$Q(y)$	T

(5)	$\exists$ x P(x)	EG, (3)
(6)	$\exists$x Q(x)	EG, (4)
(7)	$\exists$xP(x) $\wedge$ $\exists$ xQ(x)	T

4.5.5 Formulas with more than one quantifiers: Consider the case in which the quantifiers occur in combinations.

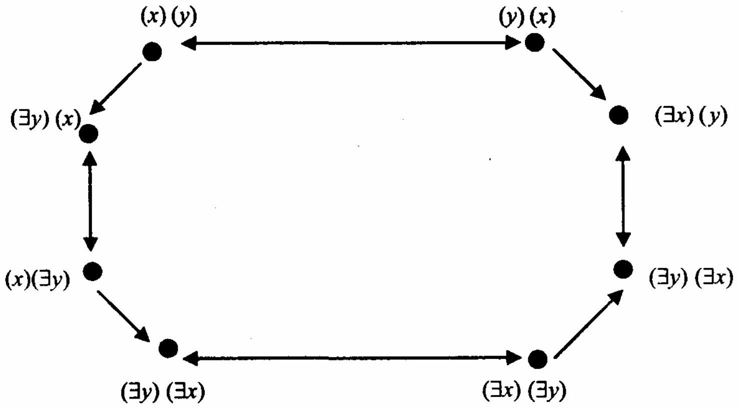
If P(x, y) is a 2-place predicate formula, then the following possibilities exist.

(x)(y)P(x, y); (x)($\exists$y)P(x, y); ($\exists$x)(y)P(x, y)

($\exists$x)($\exists$y)P(x, y); (y)(x)P(x, y); ($\exists$y)(x)P(x, y)

(y)($\exists$x)P(x, y); ($\exists$y)($\exists$x)P(x, y)

There is logical relationship among sentences with two quantifiers if the same predicate is involved in each sentence.



4.5.6 Example: Show that ~ P(a, b) follows logically from (x) (y) P(x, y) → W(x, y) and ~ W(a, b).

Solution: We get

(1) (x)(y) P(x, y) $\rightarrow$ W(x, y)	P
(2) (y) P(a, y) $\rightarrow$ W(a, y)	US, (1)
(3) P(a, b) $\rightarrow$ W(a, b)	US, (2)

(4) $\sim W(a, b)$	P
(5) $\sim P(a, b)$	T, (3), (4)

4.6 Answers to Self Assessment Questions

SAQ1.

(i) All men are mortal

(ii). Given any thing in the Universe, it is mortal

(iii). California is human

(iv). Aristotle is human

(v). there exists a thing in the Universe which is mortal

(vi). there exists atleast one human who is mortal

SAQ2.

(a) $\exists x\, (P(x) \wedge Q(x))$

(b) $\exists x\, (P(x) \wedge \sim Q(x))$

(c) $\forall x\, (P(x) \vee Q(x))$

(d) $\forall\, x \sim (P(x) \vee Q(x))$

SAQ3.

Let G(x): x is a giant; M(x): x is a man.

Without universe of discourse: (x) (M(x) — G(x)).

With universe of discourse as “class of men”: (x)G(x).

SAQ4.

We can write

P(x): x is a person.

S(x): x is a selfless leader.

R(x, y): x respects y.

Then the given expression is $(x)\ (P(x) \rightarrow (y)\ (P(y) \wedge S(y) \rightarrow R\ (x, y))$.

SAQ5.

(a). The given expression is $(x)\ (E(x) \rightarrow S(x))$, where E(x): x is even, S(x) : $x^2 + x$ is even. Therefore the Negation is $\exists x\ (E(x) \rightarrow \sim S(x))$.

(b). The given expression is $\exists\ x\ P(x)$ where P(x): $x^2 = 9$. Therefore the Negation is $(x)\ (\sim P(x))$.

4.7 Summary

In this lesson we discussed the n-place predicates, formulas with more than one quantifiers and writing the symbolic form of the predicate statements. The role of free and the bound occurrences in proving the mathematical theorems are very useful. The universal and existential quantifiers are defined. With the help of the rules of inference, we have derived the logical implications and the equivalences.

4.8 Technical Terms

Quantifiers:	Existential quantifier, denoted by $\exists x$ and universal quantifier, is denoted by (x) or $\forall x$.
Atomic Formula:	The expression $P(x_1, x_2, \ldots, x_n)$ where $x_1, x_2, \ldots, x_n$ are individual variables and P is an n-place predicate.
Free and Bound Occurrence:	(x) p(x) or $\exists$ x p(x)
Universal specification (US):	If (x) P(x) is assumed to be true then the universal quantifier can be dropped to obtain P(c) is true, where c is an arbitrary object in the universe.

Universal generalization (UG): If P(c) is true for all c in the universe then the universal quantifier may be prefixed to obtain (x) P(x).

Existential specification (ES): If ∃ x P(x) is assumed to be true then P(c) is true for some element c in the universe.

Existential generalization (EG): If P(c) is true for some element c in the universe then ∃ x P(x) is true.

4.9 Model Questions

1. Symbolize the following:

(a) Not all birds can fly.

(b) Some men are giants.

(c) Not all men are giants.

(d) All flowers are beautiful.

(e) Not every graph is planar.

2. Let U be the set of integers. Determine the truth values of the following:

(a) $(x)(x^2 - x - 1 \neq 0)$

(b) $\exists\, x(x^2 - 3 = 0)$

(c) $(x)(\exists\, y(x^2 = y))$

(d) $(x)(x^2 - l0x + 21 = 0)$.

3. Write the negations of the following expressions:

(a) There is an integer x such that x is even and x is prime.

(b) Not all graphs are planar.

(c) All men are bad.

(d) Every graph is not connected.

4. Show that $P(x) \wedge (x)Q(x) \Rightarrow \exists\, x(P(x) \wedge Q(x))$.

5. Show that P(a) logically follows from $(x)(\sim P(x) \rightarrow Q(x))$, $(x)\,(\sim Q(x))$.

6. Check the validity of the following arguments:

a) All men are mortal. Socrates is a man. Therefore, Socrates mortal.

b) Lions are dangerous animals. There are lions. Therefore, there are dangerous animals.

c) Some rational numbers are powers of 3. All integers are rati numbers. Therefore, some integers are powers of 3.

4.10 References

1. Akerkar Rajendra and Akerkar Rupali "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Hari Kishan and Shivraj Pundir "Discrete Mathematics", Pragati Prakashan, Meerut, 2005.

3. Liu.C.L., "Elements of Discrete Mathematics", Mc Hill.

4. Shanker Rao, G., "Discrete Mathematical Structures", New Age International Publishers, New Delhi, 2002.

5. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

Name of the Lesson Writer: **Dr Bhavanari Satyanarayana**
Professor

Lesson 5

Relations

Objectives

At the end of the Lesson the student must be able to:

(i) Learn the relation between two sets.
(ii) Understand the properties of relations.
(iii)Learn to draw a digraph for a given relation.
(iv)Know the matrix representation of a relation.
(v) Apply the concept to different types of relations

Structure

5.1 Introduction

A relation may involve equality or inequality. A mathematical concept of a relation deals with the way the variables are related or paired. A relation may signify a family tie between such as "is the son of", "is the father of" etc. In mathematics the expressions like "is less than", "is greater than", "is perpendicular", "is parallel to", are relations. In this lesson we shall consider the relations, called binary relations.

5.2 Relations

5.2.1 Definition: A **relation** R from a set A to another set B is a subset of A × B. That is, $R \subseteq A \times B$.

5.2.2 Note: (i) If $(a, b) \in R$, then we say that a related to b by R and we write aRb.

(ii) If a is not related to b by R, we write a $\not{R}$ b.

(iii)If B = A, then $R \subseteq A \times A$ is a relation on A.

5.2.3 Example: Take A = {1, 2, 3, 4, 5}. Define a relation 'R' on A as $aRb \Leftrightarrow a > b$

Then R ={ (5,1), (5,2), (5, 3), (5,4), (4,3),(4,2),(4,1), (3,2), (3,1), (2,1)} is a relation on A.

5.2.4 Example: Take Z^+, the set of positive integers.

Define $aRb \Leftrightarrow$ a divides b

Then clearly 4R12, since 4 divides 12, but not 5R16.

5.2.5 Example: Let R denote the set of real numbers.

Define a relation $S = \{(a, b) \mid 4a^2 + 25b^2 \leq 100\}$. Then S is a relation on R.

5.2.6 Definition: Let R be a relation from A to B .

The domain of R is defined as Dom R = $\{x \in A \mid (x, y) \in R$ for some $y \in B\}$

and the range of R is defined as Ran R = $\{ y \in B \mid (,x\ y) \in R$ for some $x \in A\}$.

5.2.7 Notation: For any $x \in A$, we denote,

$R(x) = \{y \in B \mid (x, y) \in R\}$

$R(A_1) = \{y \in B \mid (x, y) \in R$ for some $x \in A_1\}$where A_1 is a subset of A.

5.2.8 Definition: Let R be a relation on a set S. We define the inverse of the relation R as the relation R^{-1}, where $b\, R^{-1} a \Leftrightarrow a\, R\, b$. The complement relation $\overline{R}$ is a relation such that $a\, \overline{R}\, b \Leftrightarrow a \not{R}\, b$.

5.2.9 Example: Take A = {Set of all living people}. Define B = {(x, y) | x is parent of y} and C = {(y, x) | y is child of x}. Then each of B and C is the inverse of other.

5.2.10 Example: Take $A = \{1, 2, 3\}$. Define $R = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$.
Then $\overline{R} = \{(1, 1), (2, 1), (3, 1), (3, 2), (3, 3)\}$.

Self Assessment Question 1: Take $A = \{ 2, 3, 5\}$, $B = \{ 6, 8, 10 \}$. Define R from A to B as follows: $(a, b) \in R \Leftrightarrow$ a divides b
The write the relations R and R^{-1}. Also write Dom (R) and Dom (R^{-1}).

5.2.11 Definition: A relation R on a set A is said to be **identity relation**, denoted by I_A, if $I_A = \{(x, x) \mid x \in A\}$

5.2.12 Example: Take $A = \{1, 2, 3\}$, then $I_A = \{(1, 1), (2, 2), (3, 3)\}$

5.2.13 Definition: A relation R on a set A is said to be a **universal relation** if $R = A\times A$.

5.2.14 Example: Take $A = \{(a, b)\}$. Define $R = \{(a, a), (a, b), (b, a), (b, b)\}$, which is a universal relation.

5.2.15 Definition: A relation R on a set A is

(i) **reflexive** if $a \, R \, a$ for all $a \in A$.

(ii) **irreflexive** if $a \not{R} a$ for every $a \in A$.

(iii) **symmetric** if $a \, R \in \Rightarrow b \, R \, a$

(iv) **anti– symmetric** if $a \, R \, b$, $b \, R \, a \Rightarrow a = b$

(v) **asymmetric** if $a \, R \, b$ implies $b \not{R} a$.

(vi) **transitive** if $a \, R \, b$ and $b \, R \, c \Rightarrow aRc$

5.2.16 Example: (i) Take $T = \{(a, b) \mid a, b \in a, \quad a = b\}$. Since $a = a$ for all $a \in A$ and so $(a, a) \in R$ for all $a \in A$. Therefore R is reflexive.

Suppose $(a, b) \in R$. Then $a = b$, which is same as $b = a$. Therefore $(b, a) \in R$. So R is symmetric.

Suppose $(a, b) \in R$, $(b, c) \in R$. Then $a = b$, $b = c$

This means $a = c$ and so $(a, c) \in R$.

Therefore R is transitive.

R is not irreflexive

R is antisymmetric.

(ii) Take $A = Z^+$, the set of positive integers.

Define $R = \{(a, b) \mid a < b\}$

R is not reflexive, since a □ a.

R is irreflexive, since $(a, a) \notin R$ for every $a \in A$.

R is not symmetric, since if $a < b$, but not $b < a$.

R is transitive, since $a < b$, $b < c \Rightarrow a < c$

R is asymmetric

(iii) Take $A = Z^+$ and define $R = (a, b) \mid b = a^2\}$

Then R is not reflexive

R is not symmetric

R is asymmetric

R is not asymmetric

R is not transitive, since (2, 4), (4, 16) $\in$ R but (2, 16) $\notin$ R.

5.2.17 Example: Take A = {1, 2, 3, 4} and define R = {(1, 2), (2, 3), (1, 3), (3, 4)} Then R is not reflexive, since (1, 1) $\notin$ R

R is not symmetric, since (2, 3) $\in$ R but (3, 2) $\notin$ R

R is not transitive, since (2, 3) $\in$ R, (3, 4)$\in$ R, but (2, 4) $\notin$ R.

R is irreflexive

R is asymmetric

R is antisymmetric

5.2.18 Problem: Let A = { 1, 2, 3, 4}. Define R_1, R_2, R_3 as follows

R_1 = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)}

R_2 = {(1, 1), (2, 2), (3, 3)}

R_3 = {(1, 1), (1, 3), (3, 1), (1, 2), (3, 3), (4, 4)}

Determine whether there are reflexive, symmetric, anti – symmetric or transitive.

Solution: R_1: Reflexive, symmetric, transitive not anti-symmetric (since $1R_12$, $2R_11$ but $1 \neq 2$)

R_2: Symmetric, not reflexive (since (4,4) $\notin R_2$) transitive, antisymmetric

R_3: Not reflexive (since (2,2) $\notin R_3$)

Not symmetric (since (1,2) $\in R_3$, (2,1) $\notin R_3$

Not transitive (since (3, 1), (1, 2) $\in R_3$, but (3, 2) $\notin R_3$.

Not antisymmetric (since (1,3), (3,1) $\in R_3$ but $1 \neq 3$)

5.3 Matrix Representation

5.3.1 Definition: Let A = $\{a_1, a_2, \ldots, a_n\}$ and B = $\{b_1, b_2, \ldots , b_n\}$. If R is relation from A to B, then R can be represented by matrix $M_R = (M_{ij})_{m\times n}$, defined $\left(M_{ij}\right)_{m\times n} = \begin{cases} 1 \text{ if } & (a_i, a_j) \in R \\ 0 \text{ if } & (a_i, a_j) \notin R \end{cases}$, where M_{ij} is the element in the i^{th} row and j^{th} column. M_R can be first obtained by first constituting a table, whose columns are preceded by a column consisting of successive elements of A and where rows are headed by row consisting of successive elements of B. If $(a_i, b_j) \in R$, then we enter 1 in the i^{th} row and j^{th} column.

5.3.2 Example: Let A = {1, 2, 3} and = {(x, y) | x < y}. Write M_R.

Solution: R = {(1, 2), (1, 3), (2, 3)}. Since (1, 2) ∈ R, we have $m_{12} = 1$; (1, 3)∈ R, we have $m_{12} = 1$; also $m_{23} = 1$.

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

5.3.3 Example: Let A = { 1, 2, 3, 4}. Define a R b ⇔ a < b. Then $M_R = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

5.3.4 Example: Write the relation for the relation matrix $M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$

Solution: Since M is a 3× 3 matrix, take A = $\{a_1, a_2, a_3\}$ and B = $\{b_1, b_2, b_3\}$

Then R = $\{(a_1, b_1), (a_2, b_2), (a_2, b_3), (a_3, b_1)\}$

Self Assessment Question 2: Given the relation R = {(1, 4), (1, 5), (4, 1), (4, 4) (5, 5)} on A = {1, 4, 5}. Find M_R

5.3.5 Definition: A relation R is **transitive** if and only if $M_R = [m_{ij}]$ has the property: $m_{ij} = 1$ and $m_{ik} = 1 \Rightarrow m_{ik} = 1$

5.3.6 Example: Define a relation R represented by a matrix $M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

Here, $m_{22} = 1, m_{23} = 1 \Rightarrow m_{23} = 1$

$m_{23} = 1, m_{32} = 1 \Rightarrow m_{22} = 1$

$m_{33} = 1, m_{32} = 1 \Rightarrow m_{32} =1$

Therefore the relation R is transitive.

5.4 Digraph Representation and properties

A relation can be represented pictorially by drawing its graph.

5.4.1 Definition: Let R be a relation on a set A (finite). Denote each element of A by small circles, called **vertices**. Draw an arrow, called an **edge** from a_i to a_j if and only a_i R a_j. The diagram so obtained is called the **directed graph** or **digraph** of the relation R.

5.4.2 Definition: If R is a relation on A and if a ∈ A, then the **indegree** of A is the number of elements b ∈ A such (b, a) ∈ R and **out degree** of a is the number of elements b ∈ A of element b ∈ A such that (a, b) ∈ R.

5.4.3 Example: Let A = { 1, 2, 3, 4} and R = { (1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (3, 4), (4,1)}.

The corresponding digraph of R is

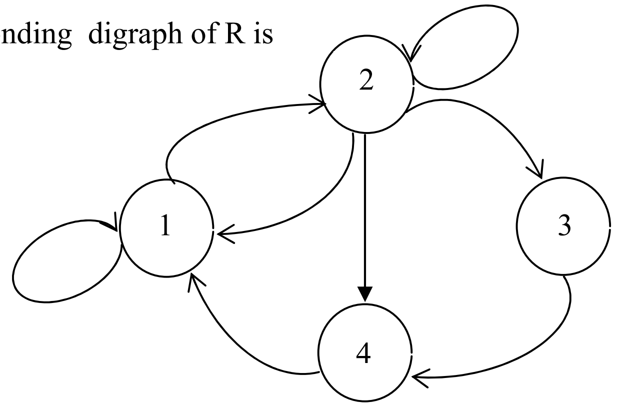


Fig. 5.4.3

In this graph

Indegree of 1 = 3, outdegree of 1 = 1

Indegree of 2 = 2, outdegree 2 = 3

5.4.4 Problem: Let A = { 1,2, 3, 4) and $M_R = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. Write the relation and construct the digraph.

Solution: The relation $(a_j, a_j) \in R \Leftrightarrow a_{ij} = 1$

Therefore R is { (1, 1), (1, 2), (1, 4), (2, 2), (2, 3), (3, 3), (3, 4), (4, 1)}

The digraph is

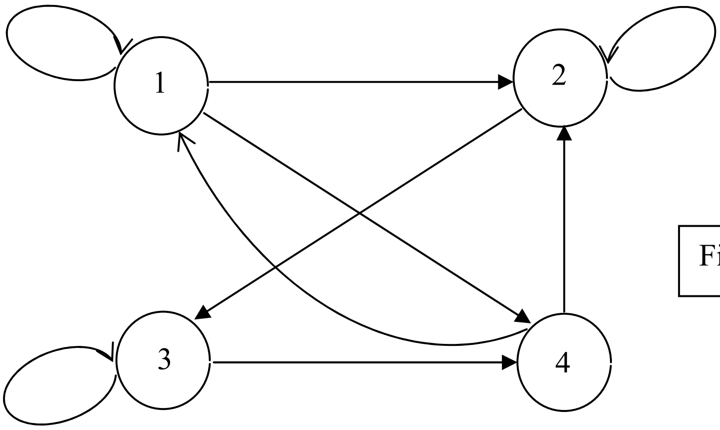


Fig. 5.4.4

Self Assessment Question 3: Let A = {a, b, c, d} and R = {(a, a), (b, b), (c, d), (c, b), (c, c), (d, b), (d, d)}. Draw the diagraph of R.

5.4.5 Problem: Write the relation as a set of ordered pairs from the digraph shown below:

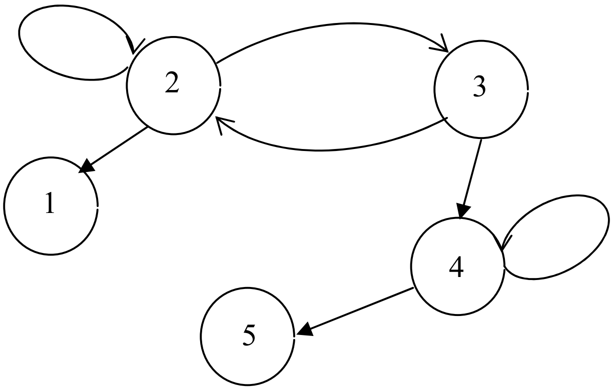


Fig. 5.4.5

Solution: Since (2, 2) is an edge, (2, 2) ∈ R

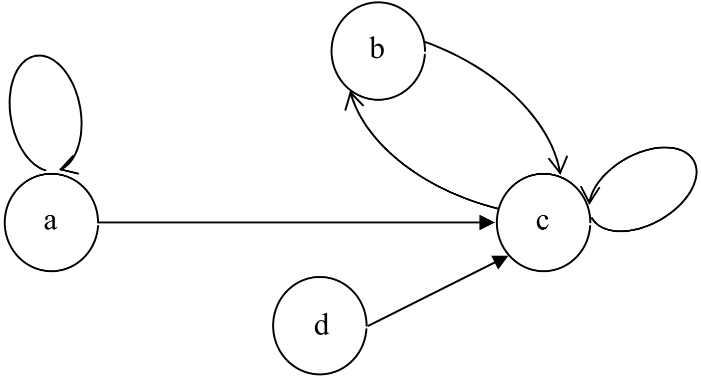
Since (2, 1) is an edge, (2,1) ∈ R

Since (2, 3) is an edge, (2,3) ∈ R

Since (4, 5) is an edge, (4,5) ∈ R, ….

Therefore the relation R = {(2, 1), (2, 2), (2, 3), (3, 2), (3, 4),(4, 4), (4, 5)}.

Self Assessment Question 4: Find the relation determined by the digraph.



5.4.6 Definition: Let R be a relation on the set A. A path of length n in R from a to b is a finite sequence P = $a_1, x_1, x_2, \ldots, x_{n-1}$, b beginning with a and ending with b such that a R x_1 , x_1 Rx_2 , …x_{n-1} Rb.

5.4.7 Note: A path of length n involves n + 1 elements of A, not necessarily distinct.

5.4.8 Definition: A path beginning and ending at the same vertex is called a cycle.

5.4.9 Example: Consider the following digraph of the relation R on A = {1, 2, 3, 4, 5}. The Paths in this digraph are:

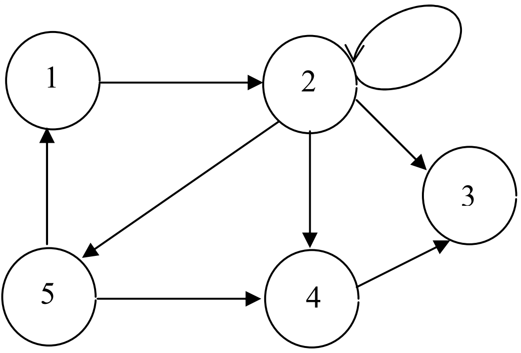


Fig. 5.4.9

P_1: 1, 2, 5, 4, 3 is a path from vertex 1 to vertex 3, of length 4.

P_2: 1, 2, 5, 1 is a path of length 3 from 1 to 1 (Cycle)

P_3: 1, 2, 3 is a path from 1 to 3, if length 2.

P_4: 2, 2 is a path of length one from 2 to 2.

5.4.10 Definition: Let P_1 = ax_1 x_2, …. , x_{r-1} b be a path of length r from a to b, and P_2: by_1y_2, …, y_{s-1} c be a path from b to c. Then the path P: ax_1x_2 ,… x_{r-1} by_1y_2, .., y_{s-1}c is a path from a to c of length (r + s) in R. This path P is called the **composition** of two paths P_1 and P_2 in R.

5.4.11 Example: Take A = { a, b, c, d, e} and R = (a, a), (a, b), (b, c), (c, e), (c, d), (d, e)}. Compute R^2.

Solution: Since (a, a) ∈ R and (a, a) ∈ R, we have (a, a) ∈ R^2.

Since (a, a) $\in$ R and (a, b) $\in$ R, we have (a, b) $\in R^2$

Since (a, b) $\in$ R and (b, c) $\in$ R, we have (a, c) $\in R^2$

Since (b, c) $\in$ R and (c, e) $\in$ R, we have (b, e) $\in R^2$

Since (b, c) $\in$ R and (c, d) $\in$ R, we have (b, d) $\in R^2$

Since (c, d) $\in$ R and (d, e) $\in$ R, we have (c, e) $\in R^2$

Therefore the diagraph is:

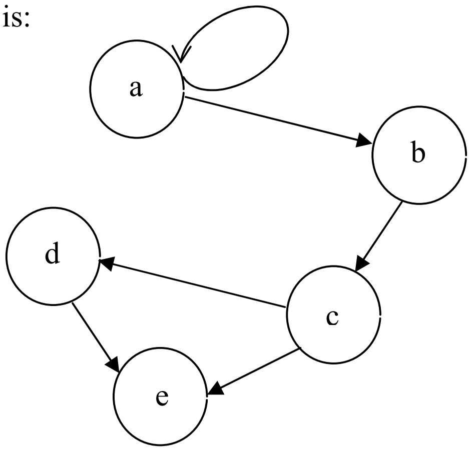


Fig. 5.4.11

R^2 = {(a, a), (a, b), (a, c), (b, e), (b, d) (c, e)}

5.4.12 Notation: $(a_i, a_j) \in R^\infty \Leftrightarrow$ there is some path in R from a_i to a_j.

5.4.13 Example: Compute R^∞ for the above example.

Solution: There is a path from a to a, we have (a, a)$\in R^\infty$. There is a path form a to b, we have (a, b) $\in R^{\infty.}$

Therefore R^∞ = {(a, a), (a, b), (b, c), (a, d), (a, e), (b, c), (b, d), (b, e), (c, d), (c, d), (d, e)}.

5.4.14 Example: Let A = {1, 2, 3}, B = {p, q, r}, C = {x, y, z}:

and let R = { 1, p), (1, r), (2, q), (2, r)} and S = { (p, q), (q, x), (q, y), (r, z)}

Now we compute RoS.

(1, p) $\in$ R and (p y) $\in$ S $\Rightarrow$ (1, y) $\in$ RoS

$(1, r) \in R, (r, z) \in S \Rightarrow (1, z) \in RoS$

$(2, q) \in R, (q, x) \in S \Rightarrow (2, x) \in RoS$

$(2, r) \in R, (r, z) \in S \Rightarrow (2, z) \in RoS$

Therefore RoS = {(1, y), (1, z), (2, x), (2, z)}

Self Assessment Question 5: Let R = (1, 1), (2, 1), (3, 2)}. Compute R^2.

5.4.15 Some Properties:

1. If R_1 and R_2 are relation form A to B, R_3 and R_4 are relations form B to C, then
   - (i) If $R_1 \subseteq R_2$ and $R_3 \subseteq R_4$, then $R_1oR_3 \subseteq R_2 \subseteq R_4$.
   - (ii) $(R_1 \cup R_2) \cup R_3 = (R_1oR_3) \cup (R_2oR_3)$
2. If R: A → B, S: B → C, T: C→D then (RoS)oT = Ro(SoT)
3. $(RoS)^{-1} = S^{-1}o\, R^{-1}$.

5.4.16 Definition: The matrix for the composite of relations can be found using the Boolean product of the matrices. Suppose R is a relation form A to B and S is a relation form B to C. Suppose that A, B and C and m, b and p elements respectively. Let $M_R = [r_{ij}]_{m\times n}$, $M_S = [s_{ij}]_{n\times p}$ and $M_{RoS} = [t_{ij}]_{m\times p}$. $t_{ij} = 1 \Leftrightarrow r_{ik} = 1 = s_{kj}$ for some k.

5.4.17 Note: $M_{RoS} = M_R \cdot M_S$.

5.4.18 Theorem: Let R be a relation on A = $\{a_1, a_2, \ldots, a_n\}$. Then $M_R{}^n = M_R \varepsilon\, M_R \varepsilon \ldots \varepsilon\, M_R$ (n factors) $= (M_R)^n = M_R{}^n$, where ε is an operator representing the Boolean multiplication of matrices.

Proof: By induction on n:

Step 1: n = 2.

Let $M_R = M_{ij}$ and $M_R{}^2 = n_{ij}$

(i, j)th element of $M_R^2 = 1$.

$\Leftrightarrow$ ith row of M_R and jth column of M_R have a 1 in the same relative position say k

$\Leftrightarrow$ $m_{ik} = 1$ and $m_{kj} = 1$ for $1 \le k \le n$

$\Leftrightarrow$ $a_i R a_k$ and $a_k R a_j$

$\Leftrightarrow$ $a_i R^2 a_j$

Thus (i,j)th element of $M_R \varepsilon M_R = 1 \Leftrightarrow n_{ij} = 1$

Hence $M_R^2 = M_R \varepsilon M_R$

Therefore the theorem is true for $n = 2$.

Step 2: Induction Hypo: Assume the result is true for $n = k$

Step 3: Let $M_R^k = [y_{ij}]$ and $M_R^{k+1} = [x_{ij}]$ and $M_R = [m_{ij}]$

If $x_{ij} = 1$, then there is a path of length (k +1) from a_i to a_j.

Let a_s be the vertex that this path reaches just before the last vertex a_j.

Then there is a path of length k from a_i to a_s and a path of length 1 from a_s to a_j

Therefore $y_{is} = 1$ and $m_{sj} = 1$

This mean $M_R^k \varepsilon M_R$ has a 1 in the (i, j)th position.

Similarly, we can prove that $M_R^k \varepsilon M_R$ has a 1 in the (i, j)th position, then $x_{ij} = 1$

Now $M_R^k = \varepsilon \ldots \varepsilon M_R$ (k factors) (by indu. Hypothesis)

So $M_R^{k+1} = M_R^k \varepsilon M_R$

$= \{M_R \varepsilon M_R \varepsilon \ldots \varepsilon M_R\} \varepsilon M_R$

$= M_R \varepsilon \ldots \varepsilon M_R$ (k + 1 factors)

Therefore the result is true for all n.

5.4.19 Example: Let M_R and M_S respectively denote the matrices of the relations R and S.

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \; M_S = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{Then } M_{RoS} = M_R \,\square\, MS = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \square \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

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

5.4.20 Definition: (i) Let R and S two relations on a set A. Then we define $R \cup S$ as follows: $x(R \cup S)y \Leftrightarrow xRy$ or xSy. Note that $M_{R \cup S} = M_R \vee M_S$, where $\vee$ denotes the Boolean addition.

(ii) Define $R \cap S$ as $x(R \cap S)y \Leftrightarrow xRy$ and xSy. Note that $M_{R \cap S} = M_R \wedge M_S$

5.3.21 Example: Consider a relation R defined on A = {1, 2, 3} whose matrix representation is $M_R = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$. Compute R^{-1} and the complement R^1

Solution: We have $M_R^{-1} = (M_R^1) =$ the transpose of M_R.

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

$R^{-1} = \{(1, 1), (1, 2), (2, 2), (3, 2), (3, 3)\}$

Also M_R^1 can be obtained by changing 0 to 1 and 1 to 0 in M_R.

Therefore $M_R{}^1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$. That is R^1 = {(1, 2), (1, 3), (3, 1) (3, 2)}.

5.4.22 Definition: Define $xR^*y \Leftrightarrow x = y$ or R^∞ y.

Then $M_R{}^* = I \vee M_R \vee (M_R)^2 \vee (M_R)^3 \vee \ldots$, where I is the unit matrix.

5.4.23 Problem: Let R be the relation on A = { 1, 2, 3, 4, 5, 6} such that R = { (1, 2), (1,6), (2,3), (3,3), (3,4), (4,1), (4,3), (4,5) (6,4)}

Find (i) R^2 (ii) $M_R{}^2$ (iii) $M_R{}^\infty$ (iv) a cycle starting at 2 (v) a cycle starting at 6.

Solution: (i) R^2 = {(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4), (3, 5), (4, 2), (4, 3), (4, 4), (4, 6), (6, 1), (6, 3)}.

(i) $$M_R^2 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

(ii) $$M_R^\infty = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 11 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

(iii) Cycle staring at 2: 2 → 3→ 4→ 1→ 2

(iv) Cycle staring at 6: 6→ 4→ 1→ 6.

5.5 Answers to Self Assessment Questions

SAQ1.

{(2, 8) (2, 10), (3, 6), (5, 10)}

R^{-1} = {(8, 2), (10, 2), (6, 3), (10, 5)}

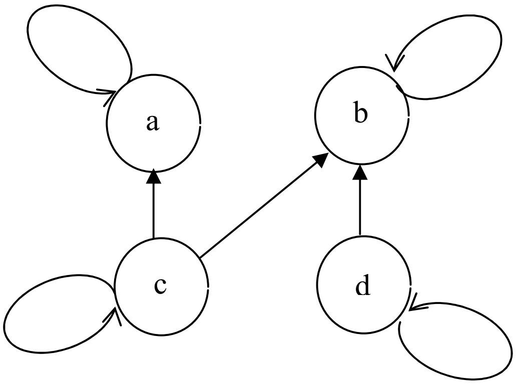
Dom (R) = {2, 3, 5} = Ran R^{-1}

Dom (R^{-1}) = {8, 10, 6} = Rang. R.

SAQ 2.

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

SAQ 3.



SAQ4.

The relation R = {(a, a), (a, c), (b, c), (c, d), (c, c), (d, c)}

SAQ 5.

R^2 = {(1, 1), (2, 1), (3, 1)}

5.6 Summary

In this lesson some basic concepts of relations and their pictorial representations were discussed. Sufficient number of illustrations provided to understand the concepts. Also the matrix array representation of relations was discussed. For a given relation, the matrix relation was given and vice versa.

5.6. Technical Terms

Relation:	$R \subseteq A\times B$
Domain of a relation:	Dom r = $\{ x \in A \mid (x, y)\in R$ for some $y \in b\}$
Range of a relation:	Range R = $\{ y \in B \mid (x, y) \in R$ for some $x \in A\}$
Matrix Relation:	$\left(m_{ij}\right)_{m\times n} = \begin{cases} 1 \text{ if } (a_i, a_j) \in R \\ 0 \text{ if } (a_i, a_j) \notin R \end{cases}$
Digraph:	Edge a_i to $a_j \Leftrightarrow a_i$ R a_j and $(a_i , a_j)\in R^{\infty}$: There is a path in R from a_i to a_j.
Boolean product:	Let $M_R = [r_{ij}]_{m\times n}$, $M_S = [s_{ij}]_{n\times p}$ and $M_{RoS} = [t_{ij}]_{m\times p}$ $T_{ij} = 1 \Leftrightarrow r_{ik} = 1 = s_{kj}$ for some k.
Union of two relations:	$x\ (R\cup S)\ y \Leftrightarrow x$ R y or x S y
Intersection of two relations:	$x\ (R \cap S)\ y \Leftrightarrow x$ R y and x S y.

5. 7 Model Questions

1. Define a relation and give example.

2. Let A = {1, 2, 3,4, 6} and R be a relation on A such that a R b $\Leftrightarrow$ a is a multiple of b. Find the domain, range, matrix and digraph of R.

3. Let A = { 1, 2, 3} , R and S be two relations defined on A as R = { (1,1), (1, 3), (2,1), (2,2), (2,3), (3, 2)} and S = { (1,1), (2,2), (2,3), (3,1), (3,3) }. Determine SoR.

4. Determine the domain and range of relation R, on set of integers, R = {(x, y) | x is a multiple of 3 and y is a multiple of 5}.

5. Let R = {(1,2), (3,4), (2,2)} and S = {(4,2), (2,5), (3,1), (1,3)}. Find RoS, SoR, RoRoR, SoS.

6. Describe the relation if A = {1, 2, 3, 4} and B = {1, 4, 6, 8, 9} and a R b $\Leftrightarrow$ $b = a^2$. Also find the domain and range of R.

7. Determine whether the relation R on the set of all integers Z, is reflexive, symmetric, antisymmetric and / or transitive.

(i) $(x, y) \in R \Leftrightarrow x \neq y$

(ii) $(x, y) \in R \Leftrightarrow$ x is a multiple of y

(iii) $(x, y) \in R \Leftrightarrow | x + y | = z$

8. Give an example of a relation on the set of positive integers which is

(i) symmetric, reflexive but not transitive

(ii) reflexive, transitive but not symmetric

(iii) symmetric, transitive, but not reflexive

(iv) reflexive but neither symmetric nor transitive

(v) neither symmetric nor antisymmetric

5.9 References

1. Akerkar Rajendra and Akerkar Rupali "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, "Discrete Mathematical Structures" PHI, New Delhi, 1999.

3. Hari Kishan and Shivraj Pundir "Discrete Mathematics", Pragati Prakashan, Meerut, 2005.

4. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. "Quantitative Methods", Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

5. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

6. Trembly, J.P., and Manohar, R. "Discrete Mathematical Structures with Applications to Computer Science", Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 6

Equivalence Relations

Objectives

At the end of the Lesson the student must be able to:

(i) Learn various properties of relations.
(ii) Understand equivalence relations.
(iii) Know the closure of relation and apply this to find reflexive, symmetrical transitive closure relations.
(iv) Know the matrix representation of closure relations.
(v) Learn graphical representation of closure relations.
(vi) Apply Warshall's algorithm to find the transitive closure.

Structure

6.1 Introduction

In this lesson we deal a particular type of relation called equivalence relation. We discuss the various representations of these relations such as graphical and matrix forms. We also define closure relations on a set, obtain different properties these and apply Warshall algorithm to find the transitive closure of relations.

6.2 Equivalence Relations

6.2.1 Definition: A relation R on a set A is called an **equivalence relation** if R is reflexive, symmetric and transitive.

6.2.2 Example:

(i) Take A = {1, 2, 3, 4}. Define
R = {(1, 1), (1, 2), (2, 1), (2, 2) (3, 3) (3, 4), (4, 3), (4, 4). Then R is a reflexive, symmetric and transitive. Therefore R is an equivalence relation.

(ii) Take A = Z, the set of integers. Define: R = {(a, b) | $a \leq b$}. Now $a \leq a$ for all $a \in Z$, R is reflexive. $a \leq b \Rightarrow b$ □ a, R is not symmetric
$a \leq b$, $a \leq c \Rightarrow a \leq c$, R is transitive. Therefore R is not an equivalence relation.

(iii) Take A = Z, the set of integers.
Define: R = {(a, b} | $a \equiv r \pmod 2$, $b = r \pmod 2$}. That is $(a, b) \in R \Leftrightarrow$ a and b give the same remainder r when divided by 2. R is an equivalence relation.

6.2.3 Problem: Let R be a relation on A. Then

(i) If R is reflexive, then R^{-1} is also reflexive.

(ii) R is symmetric $\Leftrightarrow$ $R = R^{-1}$.

(iii) R is antisymmetric $\Leftrightarrow R \cap R^{-1} \subseteq I_A$.

Solution: (i) $(a, a) \in R$ for all $a \in A \Rightarrow (a, a) \in R^{-1}$ for all $a \in A$. Therefore R^{-1} is reflexive.

(ii) Take $(a, b) \in R^{-1} \Rightarrow (b, a) \in R \Rightarrow (a, b) \in R$ (since R is symmetric).

Therefore $R^{-1} \subseteq R$, Similarly we can show that $R \subseteq R^{-1}$.

Converse: Suppose $R = R^{-1}$. Let $(a, b) \in R$. Then $(a, b) \in R^{-1}$ and so $(b, a) \in R$.

Hence R is symmetric.

(iii) Suppose R is antisymmetric. Let $(a, b) \in R \cap R^{-1} \Rightarrow (a, b) \in R$ and $(a, b) \in R^{-1}$

Since $(a, b) \in R^{-1}$, we have $(b, a) \in R$. Now $(a, b) \in R$ and $(b, a) \in R$. Since R is antisymetric, we have $a = b$. This is true for all $(a, b) \in R \cap R^{-1}$. Hence every element of $R \cap R^{-1}$ is the form (a, a) where $a \in A$. Therefore $R \cap R^{-1} \subseteq I_A$.

6.2.4 Note: Suppose R and S are relations on a set A. Then

(i) If R and S are reflexive, then $R \cup S$ and $R \cap S$ are reflexive.

(ii) If R and S re symmetric, then $R \cup S$ and $R \cap S$ are symmetric.

(iii) If R and S are transitive, then $R \cup S$ and $R \cap S$ are transitive.

6.2.5 Remark: If R and S are transitive, then $R \cup S$ need not be transitive.

Proof: Take A = {1, 2, 3} and define transitive relations. R = { (1, 1) (2, 2), (1, 2), (2,1) }, and S = { (2,2), (3,3), (2,3) (3, 2)} on A.

Therefore $R \cup S$ = {(1, 1) (2, 2), (1, 2), (2,1), (3,3), (2,3) (3, 2)}. Now $(1, 2) \in R \cup S$ and $(2, 3) \in R \cup S$, but $(1, 3) \notin R \cup S$. Therefore $R \cup S$ is not transitive.

6.2.6 Result: If R and S are equivalence relations on the set A, then

(i) R^{-1} is an equivalence relation

(ii) $R \cap S$ is an equivalence relation.

Proof: Reflexive: $(a, a) \in R^{-1}$, since $(a, a) \in R$ for all $a \in A$.

Symmetric: $(a, b) \in R^{-1}$

$\Rightarrow (b, a) \in R$

$\Rightarrow (a, b) \in R$ (since R is symmetric)

$\Rightarrow (b, a) \in R^{-1}$

Transitive: $(a, b), (b, c) \in R^{-1}$

$\Rightarrow (b, a), (c, d) \in R$

$\Rightarrow (c, b), (b, a) \in R$

$\Rightarrow$ (c, a) $\in$ R (since R is transitive)

$\Rightarrow$ (a, c) $\in$ R^{-1}

Therefore R^{-1} is an equivalence relation.

Self Assessment Question 1: Verify R $\cap$ S is an equivalence relation on A if R and S are equivalence relations on A

6.2.7 Problem: Let R = Set of real numbers. Define

(i) $(a,b) \in R \Leftrightarrow |a|=|b|$

(ii) $(a,b) \in R \Leftrightarrow a \geq b$

(iii) $(a,b) \in R \Leftrightarrow |a| > |b|$

Which of these are equivalence relations?

Solution:

(i) Equivalence relation

(ii) Not Symmetric and so it is not an equivalence relation

(iii) Not Symmetric and so not equivalence relation.

6.2.8 Definition: Let S be a non empty set. A class $\{A_i\}_{i\in I}$ is said to be a partition for S if it satisfies

(i) $A_i \cap A_j = \phi$ for all $i \neq j$

(ii) $\bigcup_{i\in I} A_i = S$

6.2.9 Theorem: Let P be a partition of the Set A. Define a relation R on R as a R b $\Leftrightarrow$ a and b are the numbers of the same block. Then R is an equivalence relation on A.

Proof: Reflexive: a and b are in the same block for the a$\in$A and so a R a.

Symmetric: a R b $\Rightarrow$ a and b are in the same block

$\Rightarrow$ b and a are in the same block

$\Rightarrow$ b R a

Transitive**:** a R b, b R c $\Rightarrow$ a, b, c are in the same block $\Rightarrow$ a R C.

Therefore R is equivalence relation.

6.2.10 Properties of Equivalence Relations:

Let R be an equivalence relation defined by A. Let a, b $\in$ A be arbitrary elements. Then

(i) $a \in [a]$

(ii) $b \in [a] \Rightarrow [a] = [b]$

(iii) $[a] = [b] \Leftrightarrow (a, b) \in R$

(iv) $[a] = [b]$ or $[a] \cap [b] = \phi$

Proof: Proofs of (i), (ii) and (iii) are trivial.

Now we will prove (iv)

Consider $[a] = \{x \mid x \in A \text{ and } x\,R\,a\}$ Assume that $[a] \cap [b] \neq \phi$

$\Rightarrow$ $\exists\, x \in A$ such that $x \in [a] \cap [b]$

$\Rightarrow$ $x \in [a]$ and $x \in [b]$

$\Rightarrow$ x R a and x R b

$\Rightarrow$ a R x and x R b (since R is symmetric)

$\Rightarrow$ a R b (since R is transitive)

$\Rightarrow$ $[a] = [b]$ (by (iii))

This completes the proof.

6.2.11 Theorem: Let R be an equivalence relation defined on A. Then R induces a partition on A.

Proof: Let a $\in$ A. Write $R(a) = \{x \in A \mid a\,R\,x\}$.

Since R is reflexive, we have a R a and so a $\in$ R(a).

Therefore R(a) is non empty. Also every element of A is some R(x).

Next we show that any two sets R(a) and R (b) for some a and b, are either identical or disjoint.

Suppose $R(a)\cap R(b)\neq\phi$ then

$c\in R(a)\cap R(b)$ for some $c\in A$.

$\Rightarrow$ $c\in R(a)$ amd $c\in R(b)$
$\Rightarrow$ aRc and bRc
$\Rightarrow$ aRc and cRb (since R is symmetric)
$\Rightarrow$ aRb (since R is transitive)
$\Rightarrow$ $b\in R(a)$
$\Rightarrow$ $a\in R(b)$ (since R is symmetric)

Also $x\in R(b)\Rightarrow$ bRx $\Rightarrow$ bRx $\Rightarrow$ xRb $\Rightarrow$ xRa, (since bRa) $\Rightarrow$ aRx (since R is symmetric) $\Rightarrow x\in R(a)$. Therefore $R(b)\subseteq R(a)$. In a similar way we can verify that $R(a)\subseteq R(b)$ and hence R(a) = R(b) . Thus R induces a partition P of A by the subsets r (a) as:

(i) every element of A is in one of the elements of P.

(ii) $R(a)\cap R(b)\neq\phi\Rightarrow R(a) = R(b)$.

The sets R(a) are called equivalence classes of R, denoted by [a].

6.2.12 Notation: The partition P is denoted by A/R. The element of A/R are called quotient sets of A with respect to R.

6.2.13 Example: Let A = {1, 2, 3, 4} and P = {{1, 2, 3}, {4}} be a partition of A. Find the equivalence relation determined by P.

Solution: Each element in the block is related to every other element in the same block and only to those elements.

Therefore R = { (1,1), (1, 2), (1, 3), (2, 2), (3, 3), (2, 3), (3,1), (3, 2), (2,1), (4, 4) }

6.2.14 Example: Let R = {(1, 1), (1, 2) (2, 1), (2, 2) (3, 4), (4, 3), (3,3), (4, 4)} be an equivalence relation on A = { 1,2,3,4}. Write the set A/ R.

Solution: R (1) = {1, 2}; R (2) = {1, 2}; R (3) = {3, 4}; R (4) = {3, 4}.

The partition is $\{\{1, 2\}, \{3, 4\}\}$. Therefore $A/ R = \{[1], [3]\}$.

6.2.15 Problem: Write the procedure for construction of A / R.

Solution:

Step (1): Choose $a \in A$ and find $R (a) = \{ x \in A \mid a R x \}$.

Step (2): Verify whether $R(a) = A$ or not. If $R (a) \neq A$, choose $b \in A$ and $b \notin R(a)$ and find $R(b)$.

Step (3): If $R (a) \cup R(b) \neq A$, choose $c \in A$ such that $c \notin R(a) \cup R(b)$, and find $R(c)$.

Step (4): Repeat step (3) until all the elements of A are included in the computed equivalence classes.

6.2.16 Example: Take Z, the set of integers. Define $R = \{(a, b) \mid (b - a)$ is divisible by $3\}$

Reflexive: $0 = a - a$ is divisible by 3, so $(a, a) \in R$.

Symmetric: $(a, b) \in R \Leftrightarrow a - b$ is divisible by 3

$\Leftrightarrow -(a - b)$ is divisible by 3

$\Leftrightarrow b - a$ is divisible by 3

$\Leftrightarrow (b, a) \in R$.

Transitive: $(a, b) \in R$ and $(b, c) \in R \Rightarrow a - b$ and $b - c$ divisible by $3 \Rightarrow a - b + b - c$ is divisible by $3 \Rightarrow a - c$ is divisible by $3 \Rightarrow (a, c) \in R$. Therefore R is an equivalence relation.

$[a] = \{ x \in Z \mid xRa\} = \{ x \in Z \mid x - a$ is divisible by $3\} = \{x \in Z \mid x = 3k + a$ for some integer $k\}$

In particular

$[0] = \{x \in Z \mid x = 3k + 0$ for some integer $k\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

$[1] = \{ x \in Z \mid x = 3k + 1$ for some integer $k\} = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\}$

$[2] = \{ x \in Z \mid x = 3k + 2$ for some integer $k\} = \{ \ldots, -7, -4, -1, 2\ 5,8, 11, \ldots\}$

Clearly $[0] \cup [1] \cup [2] = Z$. Also these classes are pair wise disjoint.

Therefore $Z / R = \{[0], [1], [2]\}$.

Self Assessment Question 2

Show that the relation (x, y) R (a, b) $\Leftrightarrow x^2 + y^2 = a^2 + b^2$ is an equivalence relation.

6.2.17 Problem: If {(a, b, c), (b, d, f)} is partition pf the set A= {a, b, c, d, e, f}; determine the corresponding equivalence relation R.

Solution: R = {(a, a), (a, c), (a, e), (c, e), (c, c), (e, e), (e, c), (e, a), (b, b), (d, d),(f, f), (b, d), (b, f), (d, f), (f, d), (d, b), (c, a)}.

6.3 Closure Relations

6.3.1 Definition: Let R be a relation on a set A. R may or may not have some property P, such as reflexivity, symmetry or transitivity. If there is a relation S with property P containing R such that S is a subset of every relation with P containing R, the S is called the **closure** of R with respect to P.

6.3.2 Definition: Let R be a relation on a set S. The **reflexive closure** of R is the smallest reflexive relation R_1which contains R.

6.3.3 Note: $R_1 = R \cup \Delta$, where Δ is the diagonal relation on S, i.e., $\Delta = \{ (a, a) \mid a \in S\}$.

6.3.4 Definition: The symmetric closure of R is the smallest symmetric relation containing R. That is $R \cup R^{-1}$ is symmetric closure R, where R^{-1} is the inverse of the relation R. It is denoted by $R^{(s)}$.

6.3.5 Definition: Transitive closure of a relation R is the smallest transitive relation containing R.

6.3.6 Example: Consider the set S = {1, 2, 3, 4}

(i) The relation R = { (1,2), (2, 1), (1, 1), (2, 2)} is not reflexive, since (3, ,3) $\notin$ S.

Consider Δ = { (1,1,), (2, 2), (3, 3), (4, 4)}.

Now the reflexive closure $R_1 = R \cup \Delta = \{(1, 2), (2, 1), (1, 1), (2, 2), (3, 3), (4, 4)\}$.

Observe that R_1 (the reflexive closure of R, sometimes we denote as $R^{(r)}$ is obtained by supplementing with exactly essential (non more, no less) in order to get a reflexive relation containing R.

(ii) Consider the relation $K = \{ (1,2), (4, 3), (2, 2), (2, 1), (3, 1)\}$, which is not symmetric on S. Now $K^{-1} = \{(2, 1), (3, 4), (2, 2)\ (1, 2), (1, 3)\}$. The symmetric closure $K^{(s)}$ of K is given by $K^{(s)} = K \cup K^{-1} = \{ (1, 2), (2, 1), (4, 3), (3, 4), (3, 1), (1, 3)\}$.

6.3.7 Note: Given a relation R on a set A. To make a relation R transitive, add all pairs of R^2, all pairs of R^3, …,all pairs of R^m (assume that $|A| = m$), unless these pairs are already in R.

Then the transitive closure of R, denoted by R^∞ or $R^{(T)}$

$R^{(T)} = R \cup R^2 \cup \ \dots \cup R^m$.

6.3.8 Properties of Transitive closure:

(i) $R^{(T)}$ is transitive

(ii) $R \in R^{(T)}$

(iii) If S is any other transitive relation that contains R, then $R^{(T)} \in S$.

6.4 Matrix Representation of Closure Relations

6.4.1 Definition: Let M be the relation matrix of the relation R. Then

(i) the symmetric closure of R, denoted by M_S, defined as $M_S = M \vee M'$ where M' is the transpose of M.

(ii) The reflexive closure of R, denoted by M_R, defined as $M_R = M \vee I_n$ where n is the cardinality of the set of for which the relation defined and I_n is the identity matrix of size n.

(iii) The transitive closure of R, denoted by M_T or M_{R^∞} defined as $M_T = M \vee M^2 \vee M^3 \vee \dots\vee M^n$.

6.4.2 Example: Take A = {1, 2, 3} and R = {(1, 2), (2, 3), (3, 1)}. Find the reflexive, symmetric and transitive closure of R, using composition of matrix relation of R.

Solution: Let M be the matrix relation R then $M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

(i) The Reflexive closure of R, $M_R = M \vee I_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

One can write the reflexive closure $R^{(r)}$, using the above matrix as $R^{(r)}$ = {(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 3)}.

(ii) The symmetric closure of R, is $M_S = M \vee M' = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \vee \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$.

One can write the symmetric closure $R^{(S)}$, using the above matrix as
$R^{(S)}$ = {(1, 2), (1,3), (2,1), (2,3), (3,1), (3,2)}

(iii) To find the transitive closure of R, we first find M^2 and M^3 (since the cardinality of the set A = 3).

$$M^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad \text{and}$$

$$M^3 = M^2. M = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Therefore the transitive closure of R, $M_T = M \vee M^2 \vee M^3$

$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \vee \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \vee \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$. One can write the transitive closure of R,
R^T = { (1,10), (1,2), (1,3), (2,1), (2,1), (2,2), (2,3), (3,1), (3,2) (3,3)}.

Self Assessment Question 3: Consider the relation R = { (0,1), (1,2), (2,3) } on A = { 0, 1, 2, 3. Write the reflexive, symmetric and transitive closures of R, using (i) composition of relation and (ii) composition of matrix relation.

6.5 Composition of Relations

6.5.1 Definition: Let R be a relation from A to B, S be a relation from B to C. Then the relation **SoR** from A to C is defined by a (SoR) c ⇔ a R b and b S c for some b ∈ B for all a ∈ A and c ∈ C.

6.5.2 Example: Take A = {1, 2, 3, 4}

Define R = {(1, 1), (1, 2) (2, 3), (2, 4), (3,4), (4,1), (4,2)} and

S = {(3,1), (4, 4), (2,3), (2,4), (1,1), (1, 4)}

Then since (1,1) ∈ R, (1,1)∈ S we have (1,1) ∈ SoR

since (1,2) ∈ R, (2,3)∈ S we have (1, 3)∈ SoR

since (2,3) ∈ R, (3,1)∈ S we have (2, 1)∈ SoR

Continuing this way we set

SoR = { (1,1), (1,4), (1,3), (2,1), (2,4), (3,4), (4,1), (4,4), (4,3)}

Similarly,

RoR = { (1,1), (1,2), (1,3), (1,4), (2,4), (2,1), (2,2), (3,1), (3,2), (4,1), (4,2), (4,3), (4,4)}

Self Assessment Question 4: Take A = { 1,2,3,4,5} . Define R = { (1,2), (3,4), (2,2) } and S = { (4, 2), (2,5), (3,1), (1,3) }. Write (i) RoS (ii) SoR (iii) Ro (SoR) (iv) (RoS)oR, (v) SoS

6.5.3 Problem: If R_1 and R_2 are relations from A to B, R and R_4 are relations from B to C, then (i) If $R_1 \subseteq R_2$ and $R_3 \subseteq R_4$, then R_1 o $R_3 \subseteq R_2$ o R_4.

(ii) $(R_1 \cup R_2)$ o $R_3 = R_1$ o $R_3 \cup R_2$ o R_3.

Solution: (i) Take $(x, y) \in R_1$ o R_3. By def; $(x, y) \in R_1$ and $(y, z) \in R_3$ for some $y \in B$

Now $(x,y) \in R_1 \subseteq R_2 \Rightarrow (x, y) R_2$

$(y, z) \in R_3 \subseteq R_4 \Rightarrow (y, z) \in R_4$

Therefore $(x, z) \in R_2$ o R_4. Hence R_1 o $R_3 \subseteq R_2$ o R_4.

(ii)Since $R_1 \subseteq R_1$o R_2 , we have R_1o$R_3 \subseteq (R_1 \cup R_2)$ o R_3 (by (i))

Similar way, R_2 o $R_3 \in (R_1 \cup R_2)$oR_3

Therefore R_1 o $R_3 \cup R_2$ o $R_3 \subseteq (R_1 \cup R_2)$ o R_3

On the other hand, take $(x, z) \in (R_1 \cup R_3)$ o R_3

$\Rightarrow \exists\, y \in B$ such that $(x, y) \in R_1 \cup R_2$ and $(y, z) \in R_3$.

If $(x, y) \in R_1$, then $(x, z) \in R_1$o R_3

If $(x, y) \in R_2$ then $(x, z) \in R_2$ o R_3

Therefore $(x, z) \in R_1$ o $R_3 \cup R_2$ o R_3. Thus $(R_1 \cup R_2)$ o $R_3 = R_1$ o $R_3 \cup R_2$ o R_3.

6.5.4 Problem: If R is a relation from A to B, S is a relation form B to C, and T is a relation from C to D, then (RoS)o T = Ro(SoT)

Solution: We show that $(x, v) \in$ (R oS) oT $\Leftrightarrow \exists\, y \in B, Z \in C$ such that $(x, y) \in R$, $(y, z) \in S$ and $(x,v) \in T$ ------- (say condition (A))

Take $(x, v) \in$ (RoS)oT $\Rightarrow$ there exists $z \in C$ such that $(z, z) \in$ RoS and $(z, v) \in T$. Since $(x,z) \in$ RoS, there exists $y \in B$ such that $(x, y) \in R$ and $(y,z) \in S$.

Thus condition (A) holds. In a similar way, one can verify that (x, v) $\in$ Ro(SoT) $\Leftrightarrow$ $\exists$ y $\in$ B and z $\in$ C such that (, y) $\in$ R, (y, z) $\in$ S and (x, v) $\in$ T. Thus we can conclude that (RoS)oT = Ro(SoT).

6.5.5 Problem: If R is a relation from A to B and S is a relation from B to C, then $(RoS)^{-1} = S^{-1}o\ R^{-1}$

Solution: Since R is a relation from A to B we have R^{-1} is a relation from B to A. Similar way, S^{-1} is a relation from C to B. Therefore $S^{-1}oR^{-1}$ is a relation from C to B.

If (x, y) $\in$ R, (y,z) $\in$ S, then (x, z) $\in$ R o S $\Rightarrow$ (z, x) $\in$ (R o S^{-1})

But (z, y) $\in$ S^{-1} and (y, x) $\in$ R^{-1}, we have (z, x) $\in$ S^{-1} o R^{-1}.

This is true for any x $\in$ A and z $\in$ C. Hence $(RoS)^{-1} = S^{-1}$ o R^{-1}

6.5.6 Problem: If R is a relation on a set A, then R is transitive $\Leftrightarrow$ $R^2 \subseteq R$.

Solution: Suppose R is transitive, take (x, y) $\in$ R^2 $\Rightarrow$ $\exists$ z $\in$ A such that (x, z) $\in$ R, (z, y) $\in$ R. Since R is transitive, we have (x, y) $\in$ R Thus $R^2 \subseteq R$

Converse: Suppose $R^2 \subseteq R$. Take (x, y) $\in$ R, and (y, z) $\in$ R. Then (x, z) $\in$ RoR = $R^2 \subseteq R$. Thus R is transitive.

6.5.7 Theorem: Let A, b, C be finite sets. Let R be a relation from A to B and S be a relation from B to C. Then $M_{RoS} = M_R \cdot M_S$ where M_R and M_S represents relation matrices of R and S respectively.

Proof: Let A = $\{a_1, a_2, \ldots, a_m\}$, B = $\{ b_1, b_2, \ldots, b_n\}$, and C = $\{ c_1, c_2, \ldots, c_p\}$

Suppose $M_R = [a_{ij}]$, $M_S = [b_{ij}]$, $M_{RoS} = [d_{ij}]$

Then $d_{ij} = 1 \Leftrightarrow (a_i, c_j) \in RoS$

$\Leftrightarrow (a_i, b_k) \in R$ and $(b_k, c_j) \in S$ for some $b_k \in B$

$\Leftrightarrow a_{ik} = 1 = b_{kj}$ for some k $1 \le k \le n$.

If $d_{ij} = 0$, then $(a_i, a_k) \notin R$ or $(a_k, a_j) \notin S$. This condition is identical to the condition needed for M_R . M_S to have 1or 0 in position I, j and thus $M_{RoS} = M_R \cdot M_S$.

6.5.8 Theorem: Let R be a relation on a set A. Then R^∞ is the transitive closure of R.

Proof: Clearly $\subseteq R^\infty$. For a, b $\in$ A,

a R^∞ b $\Leftrightarrow$ there is a path in R from a to b. Now a R^∞b and b R^∞c $\Rightarrow$ there is a path from a to b in R, and a path from b to c in R $\Rightarrow$ there is a path from a to c in R. This path is the composition of paths from a to b and b to c.

Next we verify that R^∞ is the smallest transitive relation containing R.

Let S be any transitive relation such that R $\subseteq$ S to show that $R^\infty \subseteq$ S.

Since S is transitive, we have $S^n \subseteq$ S for all n that is, if a and b are connected by a path of length n, then aSb and $.S^\infty = \bigcup_{n=1}^{\infty} \subseteq S$

Since $R \subseteq S$, $R^\infty = \bigcup_{n=1}^{\infty} R_n \subseteq R \subseteq S$. Thus R^∞ is the transitive closure of R.

6.6 Graphical Representation of Closure relation

6.6.1 Definition: Consider the relation R on a set A (finite set). We add all missing arrows (edges) from points themselves in the digraph of the relation R, we get the reflexive closure of R. If we add missing reverses of all arrows in the digraph of R we get the symmetric closure of R. If we add an arrow connecting a point x to y whenever some sequence of arrows in the diagraph of R connected to x and y and there was not an arrow from x to y already.

6.6.2 Example: Let R = { (1,2), (2, 3), (3,1)} on the set A = { 1,2,3}. Find the reflexive, symmetric and transitive closure of R, using the graphical representation of R.

Solution: Consider the graphical representation of R

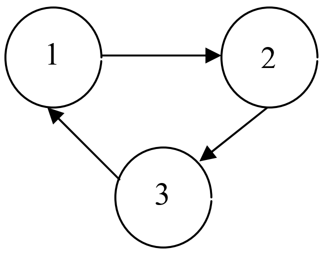


Fig. 6.6.2 (a)

(i) To get the reflexive closure, we add all the arrows to themselves shown below.

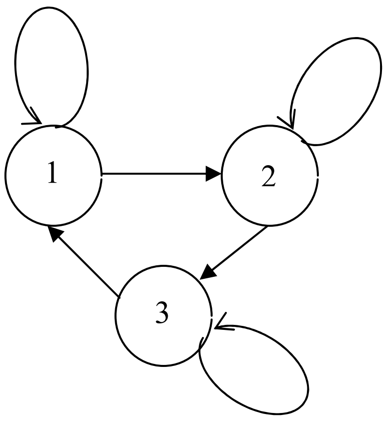


Fig. 6.6.2 (b)

(ii) To find the symmetric closure of R, add missing reverses of all the arrows in graphical representation of R.

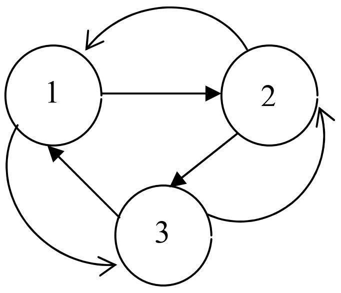


Fig. 6.6.2 (c)

(iii) To find the 2 transitive closure;

since 1 → 2 → 3 → 1 , we add arrow 1 to 1

since 2 → 3→ 1→ 2, we add arrow 2 to 2

since 3 → 1 → 2 → 3 , we add arrow 3 to 3

since 1 → 2 → 3, we add 1 to 3

since 2 → 3 → 1 , we add 2 to 1

since 3 → 1 → 2, we add 3 to w

Finally we get

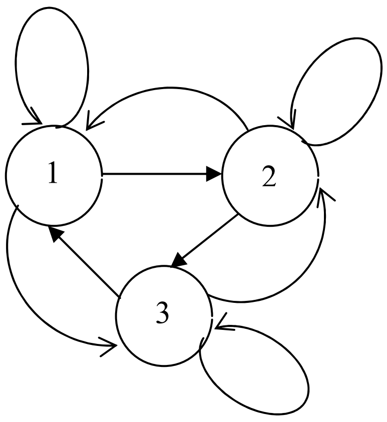


Fig. 6.6.2 (d)

Self Assessment Question 5: Let R = { (1,2), (2,3), (3,4), (2,1)} be a relation on A = {1,2,3,4}. Find the transitive closure of R^{∞} using digraph.

6.6.3 Warshall's Algorithm: Graphical representation and matrix representation methods are not suitable for large sets and relations. Warshall's algorithm is more efficient method for computing the transitive closure of a relation.

Procedure:

Let R be a relation on a set A = { a_1, a_2 …, a_n} we generate a sequence of matrices P^0, P^1, P^2,…P^k,…,P^n for a graph on n vertices with P^n = P (the path matrix)

Initially P^0 = A (the adjacency matrix)

Iteration (1):

The existence of paths from any vertex to any vertex either directly via an edge or indirectly through the intermediate or pivot vertex say a_1.Let p^1 denotes the resulting matrix with its general element $P_{ij}^{(1)}$ obtained as follows:

$$P_{ij}^{(1)} \begin{cases} 1, & \text{if there exists an edge from } a_i \text{ to } a_j \text{ or there is a path (of length 2)} \\ & \text{from } a_i, \text{ to } a_1 \text{ and } a_1 \text{ to } a_j. \\ 0, & \text{otherwise} \end{cases}$$

Iteration (2):

In this iteration, explore any paths from any vertex to any other vertex with $a_1$and a_2 or both as pivots. We compute P^2 and consider its general element $P_{ij}^{(2)}$ as follows:

$$P_{ij}^{(2)} = \begin{cases} 1, & \begin{array}{l}\text{if there exists an edge from } a_i \text{ to } a_j \text{ or a path from } a_i \text{ to } a_j \text{ using only pivots} \\ \text{(intermediate vertices from } \{a_1, a_2\}\end{array} \\ 0, & \text{otherwise} \end{cases}$$

Continuing this way, in general

k

k^{th} iteration:

$$P_{ij}^{(k)} = \begin{cases} 1, & \begin{array}{l}\text{if there exists an edge from } a_i \text{ to } a_j \text{ or} \\ \text{a path from } a_i \text{ to } a_j \text{ using only pivots from } \{a_1, a_2, \ldots a_k\}\end{array} \\ 0. & \text{otherwise} \end{cases}$$

We can compute $P_{ij}^{(k)}$ from the previous iteration $P_{ij}^{(k-1)}$ as follows

$P_{ij}^{(k)} = P_{ij}^{(k-1)} \vee (P_{ik}^{(k-1)} \wedge P_{kj}^{(k-1)})$

In other words :

$P_{ij}^{(k)} = 1$ if $P_{ij}^{(k-1)} = 1$

or both $P_{ij}^{(k-1)} = 1$ and $P_{kj}^{(k-1)} = 1$

The only way that the value of $P_{ij}^{(k)}$ can change 0 is to find a path through a_k, that is, there is a path from a_i to a_k and a path from a_k to a_j.

Algorithm:

M_R = n ×n non zero matrix

$P^{(0)} = M_R$

For k = 1 to n

```
begin
 for i = 1 to n
begin
for j = 1 to n
$P_{ij}^{(k)} = P_{ij}^{(k-1)} \vee ( P_{ik}^{(k-1)} \wedge P_{kj}^{(k-1)})$
end
end { $P_{ij}^{(n)}$ }
```

6.6.4 Example: Find the matrix of transitive closure of R using Warshall algorithm for the relation given by the digraph.

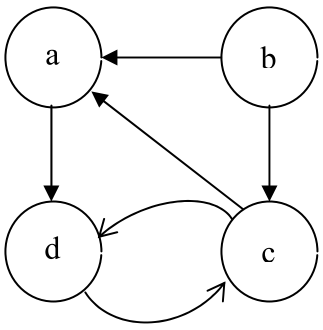


Fig. 6.6.4

Solution: Relation matrix $M_R = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = P^{(0)}$

Observe that $P_{14}^{(0)} = P_{21}^{(0)} = P_{23}^{(0)} = P_{31}^{(0)} = P_{34}^{(0)} = P_{43}^{(0)} = 1$

Therefore $P^{(1)}$ also have 1 in the corresponding places

Since $P_{21}^{(0)} = 1 = P_{14}^{(0)}$, where $P_{24}^{(1)} = 1$

Therefore $P^{(1)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = P^{(0)}$

Observe that $P_{14}^{(1)} = P_{21}^{(1)} = P_{23}^{(1)} = P_{31}^{(1)} = P_{34}^{(1)} = P_{34}^{(1)} = 1$

Since there is no 1 and 2nd column of P(1), there is no edges that have b as terminal vertex.

So no new path is obtained when we permit b as terminal vertex, and therefore, no new 1's are inserted in $P^{(1)}$.

Thus $P^{(2)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Since $P_{43}^{(2)} = 1$ and $P_{34}^{(2)}$ and we have $P_{44}^{(3)} = 1$ and since $P_{43}^{(2)} = 1$, $P_{31}^{(2)}$, we have $P_{41}^{(3)} = 1$

Therefore $P^{(3)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

Finally , $P^{(4)}$ has 1 as its (i, j)th entry if there is a path from v_i to v_j that has only v_1 = a, v_2 = b, v_3 = c and / or v_4 = d as intermediate vertices.

$P_{14}^{(3)} = 1$ and $P_{41}^{(3)} = 1$, we have $P_{11}^{(4)} = 1$

Now $P_{14}^{(3)} = 1$ and $P_{43}^{(3)} = 1$, we have $P_{13}^{(4)} = 1$

$P_{34}^{(3)} = 1$ and $P_{43}^{(3)} = 1$, we have $P_{33}^{(4)} = 1$

Thus $P^{(4)} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ is the matrix of transitive closure.

6.7 Answer to Self Assessment Questions

SAQ1.

(i) Symmetric

(ii) Reflexive, transitive

(iii) Symmetric

SAQ2.

Verification of equivalence relation is straight forward. For any point (x, y) the sum $x^2 + y^2$ is the square of its distance from the origin. The equivalence classes are, the sets of points in the plane which have the same distance from the origin.

SAQ3.

$R^{(r)}$ = { (0,1), (1,), (2,2), (3,3), (0,1) (1,2) (2,3)}

$R^{(S)}$ = { (0,1), (1,0), (1,2), (2,1), (2,3), (3,2)}

$R^{(T)}$ = { (0,1), (0,2), (0,3), (1,2), (1,3), (2,3)}

SAQ 4.

(i) RoS = {(1,5), (3,2),(2,5)}

(ii) SoR = {(4,2), (3,2), (1,4)}

(iii)Ro(SoR) = { (3,2)}

(iv)(RoS)oR ={(3,2)}

(v) SoS = {(4,5), (3,3), (1,1)}

SAQ 5.

R^{∞} = { (1,1), (1,2), (1,3),(1,4), (2,1), (2,2), (2,3), (2,4), (3,4)}

6.8 Summary

In this lesson we studied the special types of relations called equivalence relations. Properties of equivalence relations and equivalence classes were studied. The various like graphical and matrix representations of these equivalence relations were studied. The algorithms for closure relations and applications were given.

6.9 Technical terms

Equivalence Relation:	Reflexive, symmetric, transitive
Partition:	Pair wise disjoint close of subsets whose union is the given set.
Reflexive closure ($R^{(r)}$):	Smallest reflexive relation which contains the relation R.
Symmetric closure ($R^{(s)}$):	Smallest symmetric relation containing the relation R.
Transitive closure ($R^{(\infty)}$):	Smallest transitive relation containing the relation R.
Warshall's Algorithm**:**	Computing the transitive closure of a given relation for longer number of sets.

6.10 Model Questions

1.Determine whether the relation R represented by the matrix $M^R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ is an equivalence relation. (Ans : Yes)

2.Find the transitive closure of the given relation using Warshall's algorithm

(i) $R = \{ (1,2), (2,3), (3,4), (2,1)\}$ on $A = \{ 1,2,3,4\}$

(ii) $M^R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ on $A = \{ 1, 2, 3, 4\}$

(Ans : (i) $R^{(\infty)} = \{ (1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4), (3,4)\}$

(ii) $R^{(\infty)}) = \{(1,1), (1,2), (2,1), (2,2), (4,4)\} \}$

3.Let A = { 1,2,3,4} and R = { (1,1), (1,4), (2,1) (2,2),(3,3), (4,4)}. Find the transitive closure of R.

(Ans: { (1,1), (,4), (2,1), (2,2), (2,4), (3,3), (4,4)})

4.Define the relation R on $Z^+ \times Z^+$ as (a, b) R (c, d) ⇔ a+ d = b + c . show that R is an equivalence ration. What is [(1,2)]?

(Ans: [(1, 2)] = {(1, 4), (2, 5), (3, 6), (4, 7)…})

5.Define a relation ρ on the set IR × IR of all ordered pairs on the complex plane.

For (a, b), (c, d) ∈ IR × IR, define (a, b) ρ (c, d) ⇔ a = c.

(i) Show that ρ is an equivalence relation

(ii) Describe the distinct equivalence class of ρ.

(Ans: [a] = {(x, y) | x= a} for each real number a.

Geometrically : The equivalence classes are all vertical lines in the Cartesian plane).

6.Let R be a relation with the following diagraph. Using Warshall's algorithm, find the matrix of transitive closure of R.

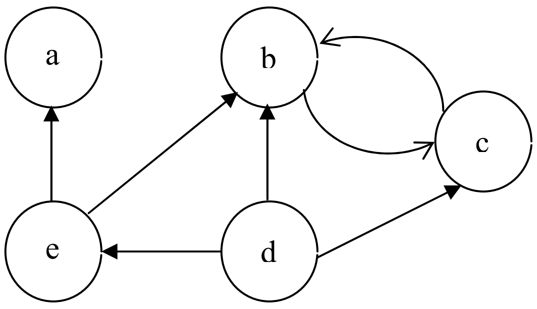


Fig. 6.10.6

$$(\text{Ans : } M_{R^\infty} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix})$$

6.10 References

1. Akerkar Rajendra and Akerkar Rupali “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Herstein I. N. “Topics in Algebra”, Blaisdell, New York, 1964.

3. Liu.C.L., “Elements of Discrete Mathematics”, Mc Hill.

4. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. “Quantitative Methods”, Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

5. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

6. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 7

Functions

Objectives

At the end of the Lesson the student must be able to:

(i) Understand the definition of function.
(ii) Distinguish the types of functions.
(iii)Learn the composition of relations and floor, ceiling functions
(iv)Illustrations on different types of functions.

Structure

7.1 Introduction

In this lesson, we study a particular class of relations called function. Functions play an important role in Mathematics, computer science and many applications. First we consider the discrete functions which transform a finite set into another finite set. Computer output can be considered as a function of the input. Functions can also be used for counting and for establishing the cardinality of sets. We also discuss the different types of functions and some of their applications.

7.2 Functions

A function is a special case of relation. Let A, B be two non-empty sets and R be a relation from A to B, then R may not relate an element of A to an element of B or it may relate an element of A to more than one element of B. But a function relates each element of A to unique element of B.

7.2.1 Definition: Let S and T be sets. A **function** f from S to T is a subset f of $S \times T$ such that

(i) for $s \in S$, there exists $t \in T$ with $(s, t) \in f$;

(ii) $(s, u) \in f$ and $(s, t) \in f \Rightarrow t = u$.

If $(s, t) \in f$, then we write $(s, f(s))$ or $f(s) = t$.
Here t is called the **image** of s; and s is called the **preimage** of t.
The set S is called the **domain** of f and T is called the **codomain**.
The set $\{f(s) / s \in S\}$ is a subset of T and it is called the **image** of S under f (or image of f).
We denote the fact: 'f is a function from S to T' by "$f: S \rightarrow T$".

7.2.2 Example: Let X = {a, b, c} and Y = {0, 1}. Then observe the following.

(i) f = {(a, 0), (b, 1), (c, 0)} is function. Hence f(a) = 0, f(b) = 1, f(c) = 0.

(ii) g = {(a, 0), (a, 1), (b, 0), (c, 1)} is not a function as a is related to 0 and 1.

(iii) h = {(a, 0), (b, 1)} is not a function as c is not related to any element in Y.

(iv) k = {(a, 0), (b, 0), (c, 0)} is a function. Domain of k is = {a, b, c} and the range of k is = {0}.

We can write function by some rule.

7.2.3 Example: Let R be the set of real numbers. Define f(x) = x^2 for every x $\in$ R. This represents a function f = $\{(x, x^2) \mid x \in R\}$.

7.2.4 Example: Let f: N $\rightarrow$ N be a function such that

$$f(x) = \begin{cases} 1, & \text{if x is odd} \\ 0, & \text{if x is even} \end{cases}.$$

Then the domain and the range of f respectively are N and {0, 1}.

7.2.5 Example: Let f: N $\rightarrow$ N be a function such that f(x) = x (mod 3). That is f(x) is the remainder obtained when x is divided by 3. Then the domain of f is N and the range of f is {0, 1, 2}.

Self Assessment Question 1: Let A = {a, b, c, d} and B = {1, 2, 3}. Verify f = {(a, 1), (b, 2), (c, 1), (d, 2)} is a function or not ?. If it is a function specify its range.

7.3 Types of Functions

7.3.1 Definition: $f: S \rightarrow T$ is said to be **one-one function** (or **injective function**) if it satisfies the following condition: $f(s_1) = f(s_2) \Rightarrow s_1 = s_2$.

7.3.2 Definition: $f: S \rightarrow T$ is said to be **onto function** (or **surjective function**) if it satisfies the following condition: $t \in T \Rightarrow$ there corresponds an element s in S such that $f(s) = t$.

7.3.3 Definition: A function is said to be a **bijection** if it is both one-one and onto.

7.3.4 Examples: (i) f: R → R such that f(x) = 3x+2 is an one-to-one and onto function.

(ii) f: N → {0, 1} such that $f(x) = \begin{cases} 1, \text{ if x is odd} \\ 0, \text{ if x is even} \end{cases}$ is an onto function but not an one-one function.

(iii) f: N → N defined by $f(x) = x^2 + 2$. It is an one-one function not an onto function, since there is no x ∈ N such that f(x) = 1.

(iv) f: R → R be such that f(x) = | x | where | x | is the absolute value of x. Then f is neither one-one nor onto.

7.3.5 Theorem: Let X and Y be two finite set with same number of elements. A function f: X → Y is one-to-one if and may is it is onto.

Proof: Let $X = \{x_1, x_2, \ldots, x_n\}$ and $Y = \{y_1, y_2, \ldots, y_n\}$. If f is one-to-one then $\{f(x_1), f(x_2), \ldots, f(x_n)\}$ is a set of n distinct elements of Y and hence f is onto.

If f is onto then $\{f(x_1), f(x_2), \ldots, f(x_n)\}$ form the entire set Y, so must all be different. Hence f is one-to-one.

Observation: From the above theorem, if we want a bijection between two finite sets, it is a must that the two sets have same number of elements.

7.3.6 Example: The function $\sigma : Z^+ \to Z^+$ such that σ (x) = x + 1 is called the Peano's successor function. Here σ (1) = 2, σ (2) = 3, …. The range of σ is the set {2, 3, 4, …}.

7.3.7 Definition: For any real number *x*, we define the floor of *x* as

$\lfloor x \rfloor$ = the greatest integer less than or equal to $x = \max \{n \,/\, n \le x, n \text{ is an integer}\}$

7.3.8 Example: Take $x = 2.52$, then

$\lfloor x \rfloor$ = max $\{n \,/\, n \leq x$, n is an integer$\}$ = max $\{1, 2\}$ = 2.

7.3.9 Definition: For any real number x, we define the ceiling of x as

$\lceil x \rceil$ = the least integer greater than or equal to x = min $\{n \,/\, n \geq x$, n is an integer$\}$.

7.3.10 Example: Take $x = 3.732$, then

$\lceil x \rceil$ = min $\{n \,/\, n \geq x$, n is an integer$\}$ = min $\{4, 5, 6, 7\ldots\}$ = 4.

Self Assessment Question 2: Specify the types of the following function:

(i). $X = \mathbb{R}$, $Y = \{x \,/\, x \in \mathbb{R}$ and $x > 0\}$ and $f(x) = |x|$

(ii). $f: \mathbb{N} \to \mathbb{N}$ and $f(j) = j \pmod 4$.

7.3.11 Geometric Interpretation: Floor and Ceiling functions may be understood from their graphical (or geometrical) representation consider the line $f(x) = x$, the diagonal on I, III coordinates, take $x = e = 2.71828\ldots$. we describe floor and ceiling of e as follows:

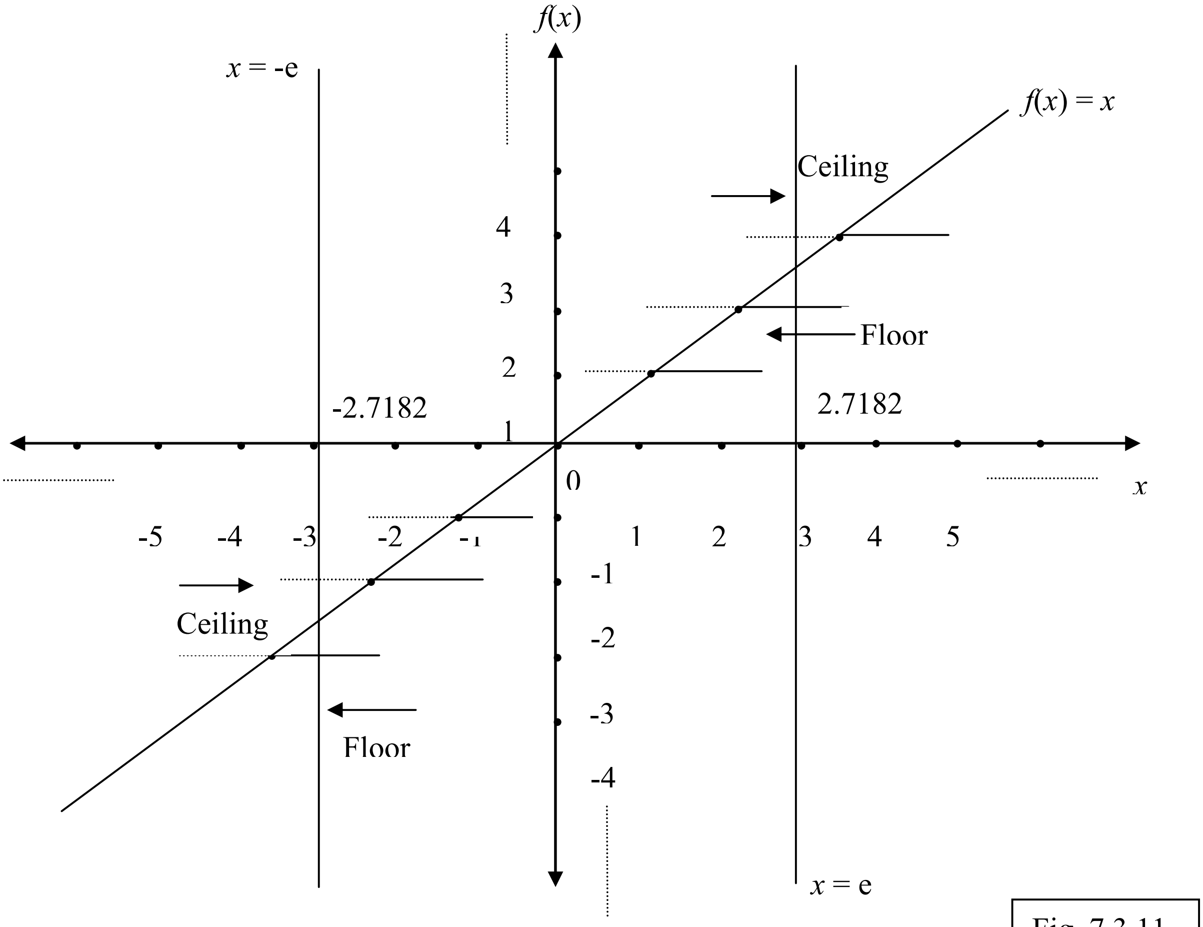


Fig. 7.3.11

From the graph, $\lfloor e \rfloor = 2$ $\lceil x \rceil = \ldots\ldots\ldots..$

$\lceil e \rceil = 3$ $\lfloor x \rfloor =$ _____

$\lfloor -e \rfloor = -3$, $\lceil -e \rceil = -2$

7.3.12 Properties:

(i) From the above graph, it can be observed that, the two functions $\lceil x \rceil$ and $\lfloor x \rfloor$ are equal at integer points. That is, $\lfloor x \rfloor = x \Leftrightarrow x$ is an integer $\Leftrightarrow \lceil x \rceil = x$.

(ii) $\lceil x \rceil - x = [\, x$ is not an integer]

That is, $\lceil x \rceil - \lfloor x \rfloor = \begin{cases} 1, & \text{if } x \text{ is not an integer} \\ 0, & \text{otherwise} \end{cases}$

(iii) $x - 1 < \lfloor x \rfloor$ and $x + 1 > \lceil x \rceil \Rightarrow x - 1 < \lfloor x \rfloor \le x \le \lceil x \rceil < x + 1$

(iv) $\lfloor -x \rfloor = -\lceil x \rceil$ and $\lceil -x \rceil = -\lfloor x \rfloor$.

(v) For any real number x, $\lfloor x \rfloor \le x$ and $\lceil x \rceil \ge x$.

7.3.13 Some Rules on floor and ceiling functions:

In all the following cases, x is real and n is an integer.

1. $\lfloor x \rfloor = n \Leftrightarrow n \le x < n + 1$
2. $\lfloor x \rfloor = n \Leftrightarrow x - 1 < n \le x$
3. $\lceil x \rceil = n \Leftrightarrow n - 1 < x \le n$
4. $\lceil x \rceil = n \Leftrightarrow x \le n < x + 1$.

7.3.14 Example: The above rules can be illustrated, by taking $x = 4.5$.

$\lfloor 4.5 \rfloor = 4 \Leftrightarrow 4 \le 4.5 < 5$

$\lfloor 4.5 \rfloor = 4 \Leftrightarrow 3.5 < 4 \le 4.5$

$\lceil 4.5 \rceil = 5 \Leftrightarrow 4 < 4.5 \le 5$

$\lceil 4.5 \rceil = 5 \Leftrightarrow 4.5 \le 5 < 5.5$

7.3.15 Example: Let X be the set of all statements in logic and Y denotes the set {T, F} where T and F are truth values. The assignment of truth values to each statement in X can be considered as a function from X to Y.

7.3.16 Example: (i) Compiler transforms a program written in a high level language into a machine language.

(ii) The output from a computer is a function of its input.

7.3.17 Definition: Let f: X → Y be a function and let $A \subseteq X$. $f_A: A \to Y$ is called the restriction of f to A if $f_A(x) = f(x)$ for any $x \in A$. If g is the restriction of f then f is called the extension of g.

7.3.18 Example: Let f: R → R be such that $f(x) = x^2$. Then f_N: N → R is such that $f(n) = n^2$ is the restriction of f to N.

7.3.19 Problem: Let X = {a, b, c} and Y = {0, 1}. List all the functions from X to Y.

Solution: The set X × Y = {(a, 0), (a, 1), (b, 0), (b, 1), (c, 0), (c, 1)} contains 6 elements. Hence there are 2^6 of subsets of X × Y. Out of these subsets only the following $2^3 = 8$ subsets are functions.

f_0 = {(a, 0), (b, 0), (c, 0)}
f_1 = {(a, 0), (b, 0), (c, 1)}
f_2 = {(a, 0), (b, 1), (c, 0)}
f_3 = {(a, 0), (b, 1), (c, 1)}
f_4 = {(a, 1), (b, 0), (c, 0)}
f_5 = {(a, 1), (b, 0), (c, 1)}
f_6 = {(a, 1), (b, 1), (c, 0)}
f_7 = {(a, 1), (b, 1), (c, 1)}

We can observe that, in general, if X has m elements and Y has n elements then there will be n^m function from X to Y.

7.3.20 Example: For each positive integer n, we define a function f_n: Z^+ → N such that $f_n(x) = r$, where x = r (mod n), $0 < r < n$. That is, r is the remainder obtained when x is divided by n.

7.3.21 Example: (Factorial function): f: N → Z^+ such that f(n) = n! for n > 0 and f(0) is defined by f(0) = 1.

7.3.22 Example: (Hashing function): To determine to which list a particular record should be assigned, we create a hashing function from the set of keys to the set of list numbers. A unique identifier for a record is called a key.

For example, suppose 10, 000 customer account records are to be stored and processed. The computer is capable of searching 100 items at a particular time. We create 101 linked lists for storage. We define a hashing function from the set of 7-digit account numbers to the set {0, 1, 2, …, 100} as h(n) = n (mod 101). Thus
h(2473871) = 2473871 (mod 101) = 78.
This means the record with account number 2473871 be assigned to list 78. Range of h is {0, 1, 2, …, 100}.

Self Assessment Question 3: Show that f: $\mathbb{R} \to \mathbb{R}$ such that f(x) = 3x + 2 is an one to one and onto function.

7.4 Composition of Functions

7.4.1 Definition: Let *g: S → T* and *f : T → U.* The **composition** of *f* and *g* is a function *fog : S → U* defined by *(fog)(s) = f(g(s))* for all *s* in *S*.
That is, fog = {(s, u) | s ∈ S, u ∈ U and ∃ t ∈ T and t = g(s) and u = f(t)}.

7.4.2 Example: Let X = {1, 2, 3}, Y = {a, b} and Z = {p, q, r}. Let f: X → Y defined by f = {(1, a), (2, b), (3, a)} and g: Y → Z defined by g = {(a, r), (b, q)}. Then gof = {(1, q), (2, q), (3, r)}.

7.4.3 Problem: Let f: R → R and g: R → R where R is the set of real numbers. If f(x) = x^2-2 and g(x) = x + 4. Find gof and fog

Solution: (gof)(x) = g(f(x)) = g(x^2-2) = (x^2-2) + 4 = x^2 + 2; and
(fog)(x) = f(g(x)) = f(x + 4) = $(x + 4)^2 - 2$ = x^2 + 8x +14.

7.4.4 Definition: Let f: X → Y, g: Y → Z and h: Z → W are functions. Then the compositions are fog: X → Z and hog: Y → W can be formed. We can also form the compositions ho(gof) and (hog)of which ae functions from X → W.

Observation: Composition of functions is associative: ho(gof) = (hog)of.

7.4.5 Example: Let f(x) = x + 3, g(x) = x – 4 and h(x) = 5x are functions from R → R where R is the set of real numbers. Find fo(goh) and (fog)oh.

Solution: Now fo(goh) (x) = f(goh)(x)

= f[g(h(x))]

= f[g(5x)]

= f(5x-4)

= 5x -4 +3

= 5x – 1.

Also, (fog)oh (x) = (fog)(h(x))

= (fog)(5x)

= f(g(5x))

= f(5x-4)

= 5x-4+3

= 5x-1.

Therefore fo(goh) = (fog)oh.

7.4.6 Problem: Show that if $g : S \to T$ and $f : T \to U$ are one-one functions, then fog is also one-one.

Solution: Suppose that $(fog)(s) = (fog)(t)$ *for* $s, t \in S$. By the definition of composition of maps, we have $f(g(s)) = f(g(t))$. Since f is one-one, we get $g(s) = g(t)$. Since g is one-one, we get $s = t$. Therefore fog is one-one.

7.4.7 Problem: If $g : S \to T$ and $f : T \to U$ are onto, then so is fog.

Solution: Let $u \in U$. To show that fog is onto, we have to find an element s in S such that $(fog)(s) = u$. Since f is onto, there exists t in T such that $f(t) = u$. Now since g is onto there exists s in S such that $g(s) = t$. It is clear that $(fog)(s) = f(g(s)) = f(t) = u$. Hence fog is an onto function.

7.4.8 Theorem: If f: X → Y and g: Y → Z are bijections then gof: X → Z is also a bijection.

Proof: Combination of the above two problems.

7.4.9 Definition: A function $f : S \to T$ is said to have an **inverse** if there exists a function g from T to S such that $(gof)(s) = s$ for all s in S and $(fog)(t) = t$ for all t in T. We call the function 'g' the **inverse** of f. A function $f : S \to S$ is said to be an **identity function** if $f(s) = s$ for all s in S. The identity function on S is denoted by either I or I_S. Inverse of a function f, if it exists, is denoted by f^{-1}. Two functions $f : A \to B$ and $g : C \to D$ are said to be **equal** if $A = C$, $B = D$ and $f(a) = g(a)$ for all elements a in $A = C$. If two functions f and g are equal, then we write $f = g$.

7.4.10 Theorem: Let f: X → Y be a function and I_x is the identity function of X, then $foI_x = I_xof = f$.

Proof: Now $foI_x(x) = f(I_x(x)) = f(x)$. Similarly we get $I_xof(x) = f(x)$.

Observation: The identity function is one-one and onto.

A function g is inverse of $f \Leftrightarrow fog$ and gof are identity functions.

7.4.11 Problem: Find out two functions f and g defined from R to R, where R is the set of all real numbers such that $fog \neq gof$.

Solution: Define $f(x) = 2x$ and $g(x) = x + 5$ for all x in R.

Then $(fog)(1) = f(g(1)) = f(1 + 5) = f(6) = 12$.

$(gof)(1) = g(f(1)) = g(2) = 2 + 5 = 7$.

This shows that the two functions are not equal at 1.

7.4.12 Problem: Prove that a function f has an inverse $\Leftrightarrow$ f is one-one and onto.

Solution: Suppose the inverse of $f : S \rightarrow T$ is $g : T \rightarrow S$.

By definition, $gof(s) = s$ for all s in S and $fog\,(t) = t$ for all t in T.

To show f is one-one, suppose $a, b \in S$ such that $f(a) = f(b)$.

By applying the function g on both sides, we get $gof(a) = gof(b)$.

Since gof is identity, we get $a = gof(a) = gof(b) = b$.

Hence f is one-one. To show f is onto, let t be an element of T. Write $x = g(t)$. Then x is in S and $f(x) = f(g(t)) = fog(t) = t$. Hence f is onto.

Converse: Suppose f is one-one and onto.

Define $g : T \rightarrow S$ as $g(t) = s$ where $f(s) = t$. To verify that g is a function, suppose $g(t) = a$ and $g(t) = b$. Then $f(a) = t$, $f(b) = t$.

So $f(a) = f(b)$ which implies $a = b$ (since f is one-one). Therefore g is a function.

For all s in S, we have that $gof(s) = g(f(s)) = g(t) = s$ (where $t = f(s)$).

Also for all t in T, we have $fog(t) = f(g(t)) = f(s) = t$. Hence g is an inverse of f.

7.4.13 Note: Inverse of a function is unique. Identity function on a set is unique. Identity element in a set with respect to a binary operation is unique.

7.4.14 Notation: If S is a non-empty set, then we write $A(S) = \{f \,/\, f : S \rightarrow S$ is a bijection$\}$.

7.4.15 Theorem: For $f \in A(S)$, there corresponds an element f^{-1} in $A(S)$ such that $fof^{-1} = I = f^{-1}of$.

Proof: Define $f^{-1}: S \to S$ by $f^{-1}(y) = x$, if $f(x) = y$.

Then f^{-1} is a function and $(f^{-1}of)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I(x)$.

So $f^{-1}of = I$. Similarly $(fof^{-1})(y) = f(f^{-1}(y)) = f(x) = y = I(y)$.

This implies $fof^{-1} = I$. Therefore $fof^{-1} = I = f^{-1}of$.

7.4.16 Theorem: Let f: X → Y and g: Y → X. Then $g = f^{-1}$ if and only if $gof = I_x$ and $fog = I_y$.

Proof: Let $gof = I_x$ and $fog = I_y$.

Then $g(f(x)) = x$ and $f(g(y)) = y$ for all $x \in X$ and $y \in Y$.

This means range of f = Y and the range of g = X.

Hence both f and g are onto. Now to show f is one one.

Suppose $f(x_1) = f(x_2) \Rightarrow x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Therefore f is one-to-one. Similarly g is one-to-one.

Hence both f and g are one-to-one and onto functions and so are invertible. Now

$f^{-1}(y) = f^{-1}(f(g(y))) = (f^{-1}of)(g(y))) = I_x(g(y)) = g(y)$.

Hence $f^{-1} = g$. Similarly we can prove that $g^{-1} = f$.

7.4.17 Theorem: Let f: X → Y and g: Y → Z are invertible functions. Then (i) $(f^{-1})^{-1} = f$, (ii) $(gof)^{-1} = f^{-1}og^{-1}$.

Proof: (i) To show that f^{-1} is one one and onto.

Now $f^{-1}(y_1) = f^{-1}(y_2) \Rightarrow x_1 = x_2$ where $f(x_1) = y_1$ and $f(x_2) = y_2$, since f is onto.

$\Rightarrow f(x_1) = f(x_2)$ (since f is one one)

$\Rightarrow y_1 = y_2$.

Therefore f^{-1} is one one.

Also, take $x \in X$. Then there exist a unique $y \in Y$ such that $f(x) = y$. That is there exists $y \in Y$ such that $f^{-1}(y) = x$. Hence f^{-1} is onto. Since f^{-1} is the inverse relation of f and vice versa, we get that $(f^{-1})^{-1} = f$.

(ii) Since f, g are one one and onto, we have that (gof) is one one and onto. Hence (gof) is invertible. Also f, g are invertible. Hence $(gof)^{-1}$, f^{-1}, g^{-1} and $f^{-1}og^{-1}$ exist. Now $(gof)^{-1}$ and $f^{-1}og^{-1}$ are functions from Z to X.

Now for any $x \in X$, let $y = f(x)$ and $z = g(y)$.

Then $(gof)(x) = z$ and $(gof)^{-1}(z) = x$ for all $x \in X$, $y \in Y$, $z \in Z$.

Also $x = f^{-1}(y)$ and $y = g^{-1}(z)$ so that

$(f^{-1}og^{-1})(z) = f^{-1}(g^{-1}(z)) = f^{-1}(y) = x$, for all $x \in X$, $y \in Y$, $z \in Z$.

Hence $(gof)^{-1}(z) = f^{-1}og^{-1}(z)$ for all $z \in Z$. Thus $(gof)^{-1} = f^{-1}og^{-1}$.

7.4.18 Example: Let X = {1, 2, 3, 4} and Y = {a, b, c, d}.

(i) For the function f = {(1, a), (2, a), (3, b), (4, d)}, the inverse relation f^{-1} = {(a, 1), (a, 2), (b, 3), (d, 4)} is not a function since c has no relative and a has two relatives. Hence f is not invertible.

(ii) For the function g = {(1, d), (2, c), (3, b), (4, a)}, the inverse relation g^{-1} = {(a, 4), (b, 3), (c, 2), (d, 1)} is a function. Hence g is invertible.

Self Assessment Question 4: Let A = {1, 2, 3, 4} and B = {a, b, c, d}, and let f = {(1,a), (2, a), (3, d), (4,c)}. Verify that f is a function but f^{-1} is not a function.

7.4.19 Example: Let f: R → R, where R is the set of real numbers, be defined by $f(x) = \frac{2x-1}{3}$.

Then $f^{-1}(y) = \frac{3y+1}{2}$.

7.4.20 Example: Let f: R → R and g: R → R be defined as $f(x) = 2x + 1$ and $g(y) = \frac{y}{3}$. Verify whether or not $(gof)^{-1} = f^{-1}og^{-1}$.

Solution: Now consider

(gof)(x) = g(f(x)) = g(2x+1) = $\frac{2x+1}{3}$ and (gof)$^{-1}$ (z) = $\frac{3z-1}{2}$.

Now f^{-1}(y) = $\frac{y-1}{2}$ and g^{-1}(z) = 3z.

Then (f^{-1}og^{-1}) (z) = f^{-1}(g^{-1}(z)) = f^{-1}(3z) = $\frac{3z-1}{2}$.

7.4.21 Problem: Show that the mapping f: R → R defined by f(x) = ax + b where a, b, x ∈ R, a ≠ 0 is invertible. Define its inverse.

Solution: Take x_1, x_2 ∈ R. Now f(x_1) = f(x_2) ⇒ ax_1+ b = ax_2 + b ⇒ ax_1 = ax_2 ⇒ x_1 = x_2. Therefore f is one one.

Take y ∈ R. Now y = f(x) ⇒ y = ax + b ⇒ x = $\frac{(y-b)}{a}$. Therefore for y ∈ R, there exists $\frac{(y-b)}{a}$ ∈ R such that f($\frac{(y-b)}{a}$) = a ($\frac{(y-b)}{a}$) + b = y – b + b = y.

This shows that f^{1} exists and it is defined by f^{-1}(y) = $\frac{(y-b)}{a}$.

Self Assessment Question 5: Let f: X → Y and g: Y → Z are functions such that (gof) is onto. Prove that 'g' is onto.

7.4.22 Problem: If *S* contains more than two elements, then there exists *f, g* ∈ *A(S)* such that *fog ≠ gof.*

Solution: Since *S* contains more than two elements, we have $|S| > 2 \Rightarrow |S| \geq 3$. Let *a, b, c* ∈ *S* be three distinct elements. Define *f : S → S* by *f(a) = b, f(b) = c*, *f(c) = a* and *f(x) = x* for all *x* ∈ *S* \ *{a, b, c}*. Define *g : S → S* by *g(a) = b*, g(b) = a, and g(x) = x for all x ∈ S \ {a, b}. Then f, g are bijections and hence *f, g* ∈ *A(S)*. Now *(gof)(a) = g(f(a)) =*

$g(b) = a$ and $(f.g)(a) = f(g(a)) = f(b) = c$. Therefore $(gof)(a) = a \neq c = (fog)(a)$. This shows that $gof \neq fog$.

7.4.23 Problem: If S is a non-empty set with $|S| \leq 2$, then for any two elements $f, g \in A(S)$, we have $fog = gof$.

Solution: If $|S| = 1$, then $S = \{x\}$. Now there exists only one bijection $f : S \to S$ defined by $f(x) = x$. So in this case, the result is clear. Now suppose that the set S contains two elements x and y. Define $f : S \to S$ and $g: S \to S$ by $f(x) = x$, $f(y) = y$, $g(x) = y$, $g(y) = x$. Clearly f, g are bijections and $A(S) = \{f, g\}$.

Since f is identity mapping on S, we have $fog = Iog = g = goI = gof$. This completes the solution.

7.4.24 Problem: If $|S| = n$, then show that $|A(S)| = n!$.

Solution: Suppose $S = \{x_i \,/\, 1 \leq i \leq n\}$. If $f \in A(S)$, then f is a bijection.

To define $f : S \to S$, we have to define $f(x_i)$ as an element of S for each $1 \leq i \leq n$.

To define $f(x_1)$ there are n possible ways (because $f(x_1) \in \{x_1, x_2, ..., x_n\}$).

Since f is one-one, we have that $f(x_1) \neq f(x_2)$.

So after defining $f(x_1)$, to define $f(x_2)$ there are $(n\text{-}1)$ ways, because $f(x_2) \in \{x_1, x_2, \ldots, x_n\} \setminus \{f(x_1)\}$. Thus $f(x_1)$ and $f(x_2)$ both can be defined in $n(n\text{-}1)$ ways. Now for $f(x_3)$ there are $(n\text{-}2)$ ways and so on. Hence $f(x_1), f(x_2), \ldots, f(x_n)$ can be defined in $n(n\text{-}1)(n\text{-}2) \ldots 2\times1 = n!$ ways. Therefore $n!$ number of bijections can be defined from S to S. This means $A(S) = n!$.

7.5 Classification of Functions

Functions can be classified mainly into two ways.

(a) Algebraic function, (b) Transcendental function.

7.5.1 Definition: A function which consists of a finite number of terms involving powers and roots of the independent variable x and the four fundamental operations of addition, subtraction, multiplication and division is called **algebraic function**.

7.5.2 Example: (i) Polynomial function: A function of the form $a_0x^n + a_1x^{n-1}+ \ldots + a_n$ where n is a positive integer and $a_0, a_1, \ldots, a_n$ are real constants and $a_0 \neq 0$, is called a polynomial of x in degree n. (for example, $f(x) = 5x^3 + 4x^2 + 7x + 9 = 0$ is a polynomial of degree 3).

(ii) Rational function: A function of the form $\frac{f(x)}{g(x)}$ where f(x) and g(x) are polynomials in x and $g(x) \neq 0$, is called a rational function. (for example, $\frac{x^2+x+1}{x+3}$).

(iii) Irrational function: The functions involving radicals are called irrational functions (for example, $f(x) = \sqrt[3]{x} + 5$ is an irrational function.

7.5.3 Definition: A function which is not algebraic is called Transcendental function.

7.5.4 Example: (i) Trigonometric functions and Inverse Trigonometric functions: the functions like sin x, cos x, tan x, sec x, cosec x, cot x; and $\sin^{-1}x$, $\cos^{-1}x$, $\tan^{-1}x$, $\sec^{-1}x$, $\text{cosec}^{-1}x$, $\cot^{-1}x$ where the angle x is measured in radians.

(ii) Exponential and logarithmic functions: A function $f(x) = a^x$ $(a > 0)$ satisfying the law $a^1 = a$ and $a^x.a^y = a^{x+y}$ is called the exponential function. The inverse of the exponential function is called the logarithmic function. If $y = a^x$ then $x = \log_a y$ is a logarithmic function.

7.6 Answers to Self Assessment Questions

SAQ 1.

Yes, 'f' is a function. Range = {1, 2}

SAQ 2.

(i) onto (ii) Neither one-one nor onto.

7.7 Summary

In this lesson we studied the special kind of relations called functions. We have discussed the properties of function and illustrations. Some types of functions like one one and onto functions and intern bisection functions discussed; related results concern to the composition of functions were obtained. The special case of discrete functions like floor and ceiling were introduced and interpreted these geometrically. Sufficient number of examples and results were provided.

7.8 Technical Terms

Function: $f \subseteq S \times T$ such that (i) for $s \in S$, there exists $t \in T$ with $(s, t) \in f$; (ii) $(s, u) \in f$ and $(s, t) \in f \Rightarrow t = u$.

One-one function (or injective function): $f(s_1) = f(s_2) \Rightarrow s_1 = s_2$.

Onto function (or surjective function): $t \in Codomain$ implies that there corresponds an element s in S such that $f(s) = t$.

Bijection: Both one one and onto.

The floor function: $\lfloor x \rfloor$ = the greatest integer less than or equal to x = max $\{n / n \leq x, n$ is an integer$\}$

The ceiling function: $\lceil x \rceil$ = the least integer greater than or equal to x = min $\{n \,/\, n \geq x, n$ is an integer$\}$.

Restriction: Let f: X → Y be a function and let $A \subseteq X$. f_A: A → Y is called the restriction of f to A if $f_A(x) = f(x)$ for any $x \in A$

Composition of *f* and *g*: fog = $\{(s, u) \mid s \in S, u \in U$ and $\exists\, t \in T$ and $t = g(s)$ and $u = f(t)\}$.

Inverse function: A function $f : S \to T$ is said to have an **inverse** if there exists a function g from T to S such that $(gof)(s) = s$ for all s in S and $(fog)(t) = t$ for all t in T. We call the function '*g*' the **inverse** of *f*.

Equality: Two functions $f : A \to B$ and $g : C \to D$ are said to be **equal** if $A = C$, $B = D$ and $f(a) = g(a)$ for all elements a in $A = C$. If two functions f and g are equal, then we write $f = g$.

Algebraic function: A function which consists of a finite number of terms involving powers and roots of the independent variable x and the four fundamental operations of addition, subtraction, multiplication and division is called algebraic function.

Transcendental function: A function which is not algebraic is called Transcendental function.

7.9 Model Questions

1. Define the terms (i) Function, (ii) One one function, (iii) Onto function, (iv) Identity function.

2. State whether true or false

(i) the relation {(3, 1), (2, 2), (3, 0), (1, 1), (1, 3)}

(ii) the relation $\{(x, y) \mid x^2 = y \text{ for all } x, y \in Z^+\}$ is a function

(iii)the relation $\{(x, y) \mid$ x and y are natural numbers and $x < y\}$.

3. Show that the function f: R → R defined by $f(x) = x^2+1$ is one one and onto. Find f^{-1}.

4. A function f is defined on the set of integers as follows:

$$f(x) = \begin{cases} x \text{ if } & 0 \le x < 1 \\ x+2 \text{ if } & 1 \le x < 3 \\ 4x-5 \text{ if } & 3 \le x < 5 \end{cases}$$

. Find (i) the domain of the function, (ii) the range of the function, (iii) state whether f is one one or not.

5. Determine which of the following functions f: R → R are one to one and which are onto.

(i) $f(x) = x + 1$

(ii) $f(x) = x^3$

(iii)$f(x) = |x| + x$ for all $x \in R$.

6. Let A = {-1, 0, 2, 5, 6, 11}. If f: A → B is defined by $f(x) = x^2-x-2$ for all $x \in A$. Find the range of f if f is onto.

7. Let X = Y = Z = R (the set of real numbers). Define f: X → Y, g: Y → Z are defined by $f(x) = x + 1$, $g(y) = y^2+2$. Find gof, fof, gog, fog.

8. Let R be the set of real numbers. Define $f(x) = x +2$, $g(x) = x-2$, and $h(x) = 3x$ for all $x \in R$. Find gof, fog, fof, gog, hog, hof, fogoh.

9. Let A = R-{3} and let f: A → B be defined by f(x) = $\frac{x-2}{x-3}$. Show that f is one one and onto. Find f^{-1}.

10. Let X and Y be two finite sets with same number of elements. Prove that a function f: X → Y is one-to-one if and only if it is onto.

11. Let f: R → R be defined by f(x) = $x^2 - 2$. Find f^{-1}.

12. Compute the floor and ceiling of the values

(i) 5, (ii) 6.01, (iii) -4.8, (iv) 0.5, (v) 8.2.

7.10 References

1. Akerkar Rajendra and Akerkar Rupali "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, "Discrete Mathematical Structures" PHI, New Delhi, 1999.

3. Fraleigh J.B. "A First Course in Abstract Algebra", Narosa Publ. House, New Delhi, 1992

4. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. "Quantitative Methods", Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

5. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

6. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 8

Permutation Functions and Recursions

Objectives

At the end of the lesson the student must be able to:

(i) Understand the notion of permutation function.
(ii) Distinguish the types of permutation.
(iii)Learn to express the given permutation into transpositions.
(iv)Applications of recursion to find gcd.

Structure

8.1 Introduction

In this lesson we consider a permutation function of a set. A special type of permutation called cyclic permutation was discussed. We observe that a permutation can be expressed as a product (usual composition of mappings) of disjoint cycles (or transpositions). Further we discussed the concept of recursion, which is a very elegant and powerful tool that can often be used to describe rather complex process in a very understandable way. We also give the computation of the greatest common divisor using the recursion.

8.2 Permutation Functions

8.2.1 Definition: Let A = $\{x_1, x_2, x_3, \ldots, x_n\}$ be a set with n elements. A bijection (one to one and onto map) from A to A is called a permutation of A. Function values of a permutation p on A namely $p(x_1), p(x_2), \ldots, p(x_n)$ are given in the following form

$$p = \begin{pmatrix} x_1 & x_2 & \ldots. & x_n \\ p(x_1) & p(x_2) & \ldots. & p(x_n) \end{pmatrix}$$

8.2.2 Note: A permutation is just a rearrangement of elements of A.

8.2.3 Example: Consider the set A = {1, 2, 3}. There are 3! = 6 permutations. These are

$$I_A = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Observation: In the above example, the inverse of p_4 is p_3 and the inverse of p_2 is p_2.

8.2.4 Definition: If the set *S* contains *n* elements, then the group

$$A(S) = \{f : S \to S \,/\, f \text{ is a bijection}\}$$

has n! elements. Since S has n elements we denote $A(S)$ by S_n and this $A(S) = S_n$ is called the *symmetric group* of degree n. If $\phi \in A(S) = S_n$, then ϕ is a one to one mapping of S onto itself.

8.2.5 Example: If $S = \{x_1, x_2, x_3, x_4\}$ and $\phi \in A(S)$ by $\phi(x_1) = x_2$, $\phi(x_2) = x_4$, $\phi(x_3) = x_1$, $\phi(x_4) = x_3$ is denoted by $\phi = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_4 & x_1 & x_3 \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$. If $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ then $\psi\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ (verify). Here we use $\psi\theta(x) = \psi(\theta(x))$ (the usual composition of mapping) for all $x \in S$.

8.2.6 Example: Permutation multiplication is not usually commutative. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$. Then $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ but $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

8.3 Cyclic Permutations

8.3.1 Definition: A permutation $\sigma \in S_n$ is a *cycle* of length k if there exists elements $a_1, a_2, \ldots, a_k \in S$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_k) = a_1$ and $\sigma(x) = x$ for all other elements $x \in S$. We will write $(a_1, a_2, \ldots, a_k)$ to denote the cycle σ. Cycles are the building blocks of the permutations.

8.3.2 Example: Let P be a cyclic permutation of length 4 defined as

$$P = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{bmatrix} = (1 \quad 3 \quad 4 \quad 5)$$

P can also be written as $(3 \quad 4 \quad 5 \quad 1)$ or $(4 \quad 5 \quad 1 \quad 3)$ or $(5 \quad 1 \quad 3 \quad 4)$

8.3.3 Example: Let A = {1, 2, 3, 4, 5, 6}. Compute $\begin{pmatrix}2 & 1 & 3 & 5\end{pmatrix}\circ\begin{pmatrix}1 & 6 & 2\end{pmatrix}$

Solution: We have

$$\begin{pmatrix}2 & 1 & 3 & 5\end{pmatrix}\circ\begin{pmatrix}1 & 6 & 2\end{pmatrix}=\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 5 & 4 & 2 & 6\end{bmatrix}\circ\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 1 & 3 & 4 & 5 & 2\end{bmatrix}=\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 3 & 5 & 4 & 2 & 1\end{bmatrix}$$

The composition is not cyclic.

Now $\begin{pmatrix}1 & 6 & 2\end{pmatrix}\circ\begin{pmatrix}2 & 1 & 3 & 5\end{pmatrix}=\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 6 & 5 & 4 & 1 & 2\end{bmatrix}$. This is also not a cyclic.

Further $\begin{pmatrix}2 & 1 & 3 & 5\end{pmatrix}\circ\begin{pmatrix}1 & 6 & 2\end{pmatrix}\neq\begin{pmatrix}1 & 6 & 2\end{pmatrix}\circ\begin{pmatrix}2 & 1 & 3 & 5\end{pmatrix}$.

8.3.4 Example: The permutation $\sigma=\begin{pmatrix}1\ 2\ 3\ 4\ 5\ 6\ 7\\ 6\ 3\ 5\ 1\ 4\ 2\ 7\end{pmatrix}$ = (1 6 2 3 5 4) is a cycle of length 6, whereas $\tau=\begin{pmatrix}1\ 2\ 3\ 4\ 5\ 6\\ 1\ 4\ 2\ 3\ 5\ 6\end{pmatrix}$ = (2 4 3) is a cycle of length 3. Also, not, every permutation is a cycle. Consider the permutation $\begin{pmatrix}1\ 2\ 3\ 4\ 5\ 6\\ 2\ 4\ 1\ 3\ 6\ 5\end{pmatrix}$ = (1 2 4 3)(5 6).

8.3.5 Example: Compute the product of cycles σ = (1 3 5 2), τ = (2 5 6).

Solution: στ = (1 3 5 6).

8.3.6 Note: Two cycle ($a_1, a_2, \ldots, a_k$) and ($b_1, b_2, \ldots, b_k$) are said to be disjoint if $a_i \neq b_j$ for all i and j.

For instance, the cycles (1 3 5) and (2 7) are disjoint; however, the cycles (1 3 5) and (3 4 7) are not. Calculating their products, we get that

$$(1\ 3\ 5)(2\ 7) = (1\ 3\ 5)(2\ 7)$$

$$(1\ 3\ 5)\ (3\ 4\ 7) = (1\ 3\ 4\ 7\ 5).$$

8.3.7 Theorem: A permutation of a finite set that is not the identity or a cycle can be written as a product (composition) of disjoint cycles of length greater than or equal to 2.

Proof: Let θ (non identity with length ≥ 2) be a permutation.

The its cycles are of the form $(s, s\theta, \ldots, s\theta^{i-1})$. Write

$$\psi = \text{the product of distinct cycles of } \theta.$$

Since each cycle forms an equivalence class, if we take two cycles, they are either equal or disjoint. Therefore any two distinct cycles are disjoint.

Suppose $\psi = c_1 \cdot c_2 \cdot \ldots \cdot c_n$ where $c_1, c_2, \ldots, c_n$ are disjoint cycles. Let $s^1 \in s$. Now since $c_1, c_2, \ldots, c_n$ is a collection of disjoint cycles, we have that s^1 occurs in c_k for some $1 \leq k \leq n$. (clearly s^1 is not any other cycle, since any distinct cycles are disjoint). Also $s^1c_k = s^1\theta$. If $i \neq k$, $s^1c_i = s^1$ (since s^1 is not in c_i). Hence $s^1(\psi) = s^1(c_1 \cdot c_2 \cdot \ldots \cdot c_{k-1} \cdot c_k \cdot c_{k+1} \cdot \ldots \cdot c_n) = s^1(c_1 \cdot c_2 \cdot \ldots \cdot c_{k-1}) \cdot (c_{k+1} \cdot \ldots \cdot c_n) = s^1c_k(c_{k+1} \cdot \ldots \cdot c_n) = s^1\theta$ (since $s^1 \sim s^1\theta$, we have that $s^1\theta$ is also not in c_i for $i \geq k + 1$). Therefore $s^1\psi = s^1\theta$ for all $s^1 \in S$. Hence $\psi = \theta$.

8.3.8 Example: Write $p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 5 & 1 & 8 & 7 & 6 \end{bmatrix}$ as a product of disjoint cycles.

Solution: Take A = {1, 2, 3, 4, 5, 6, 7, 8}. Start with element 1.

Now p(1) = 4, p(4) = 5, p(5) = 1, we get a cycle $(1 \quad 4 \quad 5)$.

Next we choose x such that $x \in A$ and x is not appeared in the cycle.

Choose 2. Now p(2) = 3, p(3) = 2.

Thus we get a cycle $(2 \quad 3)$.

Next choose 6, we get the cycle $(6 \quad 8)$ and p(7) = 7.

Thus $p = (6 \quad 8) \circ (2 \quad 3) \circ (1 \quad 4 \quad 5)$.

8.3.9 Note: The product is unique except for the order of the cycles.

The simplest permutation is a cycle of length 2. Such cycles are called *transpositions*.

8.3.10 Theorem: Every cycle can be written as a product of transpositions.

Proof: Take a cycle (a_1 a_2 … a_n).

Now (a_1 a_2 … a_n) $=(a_1 \quad a_n)\circ(a_1 \quad a_{n-1}) \ldots\circ(a_1 \quad a_3)\circ(a_1 \quad a_2)$.

Therefore any cycle can be written as the product of transpositions.

8.3.11 Example: $(1 \quad 4 \quad 2 \quad 3 \quad 5) = (1 \quad 5)\circ(1 \quad 3)\circ(1 \quad 2)\circ(1 \quad 4)$.

8.3.12 Theorem: Every permutations of a finite set with at least two elements can be expressed as a product of transpositions.

8.3.13 Definition: (i) *A* permutation is said to be an **odd permutation** if is the product of an odd number of transpositions (or 2- cycles).

(ii) *A* permutation is said to be an **even permutation** if is the product of an even number of transpositions (or 2 – cycles).

8.3.14 Example: (i) Consider the permutation (1 6)(2 5 3) = (1 6)(2 3)(2 5) = (1 6)(4 5)(2 3)(4 5)(2 5). There is no unique way to represent permutation as the product of transpositions.

For instance, we can write the identity permutation as (1 2)(2 1), as (1 3)(2 4)(1 3)(2 4), and in many other ways.

(ii) No permutation can be written as the product of both an even number of transpositions and an odd number of transpositions.

For instance, we could represent the permutations (1 6) by (2 3)(1 6)(2 3) or by (3 5)(1 6)(1 3)(1 6)(1 3)(3 5)(5 6) but (1 6) will always be the product of an odd number of transpositions.

8.3.15 Note: (i) The product of two even permutations is an even permutation.

(ii) The product of an even permutation and an odd one is odd (like wise for the product of an odd and even permutation).

(iii) The product of two odd permutations is an even permutation.

8.3.16 Theorem: Let A = {a_1, $a_{2, \ldots,}$ a_n} be a finite set with n elements and n > 2. Then there are $\frac{n!}{2}$ odd permutations.

Proof: Let A_n be the set of all even permutations and B_n be the set of all odd permutations. Define f: $A_n \to B_n$ by

f(p) = $q_o \circ p$ for p ∈ A_n and q_0 be a particular transposition.

<u>f is one-to-one</u>:

For p_1, $p_2 \in A_n$,

$$\begin{aligned}
& \Rightarrow q_0 \circ p_1 = q_0 \circ p_2 \\
& \Rightarrow q_0 \circ (q_0 \circ p_1) = q_0 \circ (q_0 \circ p_2) \\
f(p_1) = f(p_2) \Rightarrow \quad & \Rightarrow (q_0 \circ q_0) \circ p_1 = (q_0 \circ q_0) \circ p_2 \\
& \Rightarrow I_A \circ p_1 = I_A \circ p_2 \quad \text{since} \quad q_0 \circ q_0 = I_A \\
& \Rightarrow p_1 = p_2
\end{aligned}$$

Therefore f is one-to-one.

<u>f is onto</u>: Let q ∈ B_n. Then $q_0 \circ q \in A_n$ and f($q_0 \circ q$)

$$\begin{aligned}
&= q_0 \circ (q_0 \circ q) \\
&= (q_0 \circ q_0) \circ q \\
&= I_A \circ q \\
&= q.
\end{aligned}$$

Therefore f is onto.

Thus f is an one-to-one and onto function from a finite set A_n to a finite set B_n. Hence A_n and B_n have same number of elements.

We have $A_n \cap B_n = \phi$ and $A_n \cup B_n = n!$.

Thus n ! = $|A_n \cup B_n| = |A_n| + |B_n| - |A_n \cap B_n| = 2|A_n| = 2|B_n|$.

Therefore $|A_n| = \frac{n!}{2} = |B_n|$.

Self Assessment Question 1: Let A = {1, 2}. Write all the permutations on A.

Self Assessment Question 2: Let A = {1, 2, 3, 4, 5, 6}

and $p_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{bmatrix}, p_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 5 \end{bmatrix}, p_3 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 4 & 1 \end{bmatrix}$

Find $(i) p_1^{-1}, (ii) p_3 \circ p_1, (iii) p_1 \circ (p_3 \circ p_2^{-1})$.

Self Assessment Question 3: Express the following permutations into a product of transpositions and check whether they are even or odd.

(i) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 7 & 8 & 4 & 3 & 2 & 1 \end{bmatrix}$,

(ii) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 6 & 7 & 8 & 5 \end{bmatrix}$,

(iii) $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 5 & 2 & 1 & 8 & 7 \end{bmatrix}$.

8.4 Recursion

In computer programming, recursion plays an important role. It is an important facility in many programming languages.

Recursion is the technique of defining a function, a set or an algorithm in terms of itself. That is, the definition will be in terms of previous values.

8.4.1 Definition: A function f: N → N, where N is the set of non-negative integers is defined **recursively** if the value of f at 0 is given and for each positive integer n, the value of f at n is defined in terms of the values of f at k, where $0 \leq k < n$.

Observation: f defined (above) may not be a function. Hence, when a function is defined recursively it is necessary to verify that the function is well defined.

8.4.2 Example: The sequence 1, 4, 16, 64, ... , can be defined explicitly by the formula
$f(n) = 4^n$ for all integers $n \geq 0$.
The same function can also be defined recursively as follows:

$$f(0) = 1,\ f(n + 1) = 4f(n), \text{ for } n > 0$$

To prove that the function is well defined we have to prove existence and uniqueness of such function. In this case, existence is clear as $f(n) = 4^n$.

8.4.3 Theorem (Recursion Theorem): Let F be a given function from a set S into S. Let s_0 be fixed element of S. The there exists a unique function f: N → N where N is the set of non-negative integers satisfying

(i) $f(0) = s_0$

(ii) $f(n + 1) = F(f(n))$ for all integers $n \in N$.

(Here the condition (i) is called initial condition and (ii) is called the recurrence relation).

8.4.4 Example: Define n! recursively and compute 5! recursively.

Solution: We have f: N → N. Then

(i) $f(0) = 1$

(ii) $f(n + 1) = (n + 1)f(n)$ for all $n \geq 0$.

Clearly $f(n) = n!$.

Now we compute 5! recursively as follows:

$$\begin{aligned} 5! &= 5.\ 4! \\ &= 5.\ 4.\ 3! \\ &= 5.\ 4.\ 3.\ 2! \\ &= 5.\ 4.\ 3.\ 2.\ 1! \\ &= 5.\ 4.\ 3.\ 2.\ 1.\ 0! \\ &= 5.\ 4.\ 3.\ 2.\ 1.\ 1 \\ &= 120. \end{aligned}$$

8.4.5 Note: Any sequence in arithmetic progression or geometric progression can be defined recursively. Consider the sequence a, a + d, a + 2d, …. Then

A(0) = a, A(n + 1) = A(n) + d.

Consider another sequence a, ar, ar^2, …. Then

G(0) = a, G(n +1) = r G(n).

8.4.6 Definition: The *Fibonacci sequence* can be defined recursively as

(i) $F_0 = 1 = F_1$

(ii) $F_{n+1} = F_n + F_{n-1}$ for n > 1.

Then

$$F_2 = F_1 + F_0 = 2$$
$$F_3 = F_2 + F_1 = 3$$
$$F_4 = F_3 + F_2 = 5$$
$$\ldots..$$

Here, there are two initial conditions.

8.4.7 Example: Define $f(x) = \begin{cases} \dfrac{x}{2} & \text{when x is even} \\ \dfrac{x-1}{2} & \text{when x is odd} \end{cases}$.

Solution: Define f: N → N such that f(0) = 0 and f(x + 1) = x – f(x).

Then f(6) = 5 – f(5) = 5 – [4- f(4)]

= 5 - 4 + [3-(3)]

= 5- 4 + 3 -2 + [1 – f(1)]

= 5 – 4 + 3 -2 +1 - [0 – f(0)]

= 3.

and f(5) = 4 – f(4)

= 4 – [3 - f(3)]

= 4 – 3 + 2 - [1-f(1)]

= f – 3 + 2 -1 + [0 – f(0)]

= 2.

8.4.8 Example: Using recursion theorem, verify that the object defined by the recursive definition is a function. That is.,

(i) g(0) = 1

(ii) $g(n + 1) = 3[g(n)]^2 + 7$ for all n > 0

Solution: We obtain (i) $s_0 = 1$

(ii) $f(k) = 3k^2 + 7$, where f: N → N

Then $g(0) = s_0$. And g(n +1) f(g(n)). Thus g is a well-defined function.

8.4.9 Definition: If m and n are two non-negative integers then the (greatest common divisor) g.c.d. (m, n) is defined as the largest positive integer d such that d divides both m and n. Euclidean algorithm computes the greatest common divisor (g.c.d.) of two non-negative integers. We can find g.c.d. (m, n) recursively as follows:

$$g.c.d.\ (\mathrm{m, n}) = \begin{cases} \mathrm{g.c.d.\,(n, m)} & \text{if n > m} \\ \mathrm{m} & \text{if n = 0} \\ \mathrm{g.c.d.\,(n, mod\,(m, n))} & \text{Otherwise} \end{cases}$$

where mod (m, n) is the remainder obtained when m is divided by n.

Observation:

a) The first part interchanges the order of m and n if n > m.

b) Second part is the initial condition.

c) Third part is the recursive part mod (m, n) will become 0 in a finite number of steps.

8.4.10 Example: Calculate the g.c.d. (20, 6).

Solution: g.c.d. (20, 6) = g.c.d. (6, mod (20, 6)) (since 20 = 6• 3 + 2)

= g.c.d. (6, 2)

= (2, mod (6, 2))

= g.c.d. (2, 0)

= 2.

8.4.11 Example: Calculate the g.c.d. (81, 36).

Solution: g.c.d. (81, 36) = g.c.d. (36, 9)

= g.c.d. (9, 0)

= 9.

8.4.12 Example: Calculate the g.c.d. (22, 8).

Solution: g.c.d. (22, 8) = g.c.d. (8, mod (22, 8))

= g.c.d. (8, 6)

= g.c.d. (6, mod (8, 6))

= g.c.d. (6, 2)

= g.c.d. (2, 0)

= 2.

Self Assessment Question 4: Calculate the g.c.d. (144, 118).

8.4.13 Note: The recursive definition can be extended to functions of more than one variable.

Consider the following example.

8.4.14 Example: Define f(x, y) = x + y recursively.

Solution: Here, we keep x fixed and use recursion on y. We define

(i) f(x, 0) = x

(ii) f(x, y + 1) = f(x, y) + 1.

Take x = 2, y = 3. Now f(2, 3) = f(2, 2) + 1

= f(2, 1) + 1 + 1

= f(2, 0) + 1 + 1 +1

= 2 + 1 + 1 +1

= 5.

8.4.15 Example: Define g(x, 0) = 0, g(x, y + 1) = g(x, y) + x. Take x = 3, y = 4. Then

g(3, 4) = g(3, 3) + 3

= g(3, 2) + 3 + 3

= g(3, 1) + 3 + 3 + 3

= g(3, 0) + 3 + 3 + 3 + 3 = 12 (since g(3, 0) = 0).

8.5 Answers to Self Assessment Questions

SAQ1.

$$p_1 = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}, p_2 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

SAQ 2.

$$(i) p_1^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{bmatrix}$$

$$(ii) p_3 \circ p_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 3 & 1 & 4 \end{bmatrix}$$

$$(iii) p_1 \circ (p_3 \circ p_2^{-1}) = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 2 & 6 & 3 \end{bmatrix}$$

SAQ3.

(i) Odd permutation: $(1 \quad 8) \circ (1 \quad 4) \circ (1 \quad 5) \circ (1 \quad 2) \circ (1 \quad 7) \circ (1 \quad 3) \circ (1 \quad 6)$.

(ii) Odd permutation: $(5 \quad 8) \circ (5 \quad 7) \circ (5 \quad 6) \circ (1 \quad 3) \circ (1 \quad 2)$.

(iii) Odd permutation: $(7 \quad 8) \circ (2 \quad 5) \circ (2 \quad 4) \circ (1 \quad 6) \circ (1 \quad 3)$.

SAQ4.

g.c.d. (144, 118) = 2.

8.6 Summary

In this lesson we introduced the notion permutation function. Various permutations defined on a given set; and a special type of permutation called cyclic permutation was discussed. It also observed that a permutation can be expressed as a product of transpositions. Further we discussed the concept of recursion, which is very useful in writing efficient algorithms and is an important facility in many programming languages. The computation of the greatest common divisor using the recursion illustrated.

8.7 Technical Terms

Permutation: Let A = $\{x_1, x_2, x_3, \ldots, x_n\}$ be a set with n elements. A bijection (one to one and onto map) from A to A is called a permutation of A.

Symmetric Group: If the set S contains n elements, then the group $A(S)$ = $\{f : S \rightarrow S \,/\, f$ is a bijection$\}$ has $n!$ elements. Since S has n elements we denote $A(S)$ by S_n and this $A(S) = S_n$ is called the *symmetric group* of degree n.

Cycle of length k: A permutation $\sigma \in S_n$ is a *cycle* of length k if there exists elements $a_1, a_2, \ldots, a_k \in S$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_k) = a_1$ and $\sigma(x) = x$ for all other elements $x \in S$. We will write $(a_1, a_2, \ldots, a_k)$ to denote the cycle σ.

Odd permutation: The product of an odd number of transpositions (or 2- cycles).

Even permutation: The product of an even number of transpositions (or 2-cycles).

Recursion Theorem: Let F be a given function from a set S into S. Let s_0 be fixed element of S. The there exists a unique function f: N → N where N is the set of non-negative integers satisfying (i) $f(0) = s_0$; (ii) $f(n + 1) = F(f(n))$ for all integers $n \in N$.

Fibonacci sequence: (i) $F_0 = 1 = F_1$; (ii) $F_{n+1} = F_n + F_{n-1}$ for $n > 1$.

Greatest Common Divisor: The gcd of two non-negative integers m and n is defined as the largest positive integer d such that d divides both m and n.

8.8 Model Questions

1. Let A = {1, 2, 3, 4, 5, 6, 7, 8}. Compute the products.

(i) $\begin{pmatrix}3 & 5 & 7 & 8\end{pmatrix}\circ\begin{pmatrix}1 & 3 & 2\end{pmatrix}$

(ii) $\begin{pmatrix}2 & 6\end{pmatrix}\circ\begin{pmatrix}3 & 5 & 7 & 8\end{pmatrix}\circ\begin{pmatrix}2 & 5 & 3 & 4\end{pmatrix}$.

2. Show that the recursive definitions

(i) h(0) = 9 and

(ii) h(b + 1) = 5h(n) + 24 for n > 0 defines a function.

3. Find the g.c.d. of 345 and 112.

4. Compute 8! Recursively.

5. Let A = {a_1, $a_{2, \ldots,}$ a_n} be a finite set with n elements and n > 2. Then prove that there are $\frac{n!}{2}$ odd permutations.

6. Show that a permutation of a finite set that is not the identity or a cycle can be written as a product (composition) of disjoint cycles of length greater than or equal to 2.

8.9 References

1. Akerkar Rajendra and Akerkar Rupali “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.
2. Bernard Kolman, Busby R.C., Sharon Ross, “Discrete Mathematical Structures” PHI, New Delhi, 1999.

3. Shanker Rao, G., “Discrete Mathematical Structures”, New Age International Publishers, New Delhi, 2002.

4. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

5. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 9

Permutations and Combinations

Objectives

At the end of the lesson the student must be able to:

(i) Learn the principles of counting with certain natural objects.
(ii) Apply the techniques of generating function to partitions and compositions.
(iii)Apply the principles of inclusion and exclusion to various models.

Structure

9.1 Introduction

Combinatorics is the study of arrangements of objects, is an important part of discrete mathematics. In this lesson, we shall study the permutations, combinations with some illustrations. An experiment means a physical process that has a number of observable outcomes. Simple examples are tossing of a coin which has two possible outcomes HEAD and TAIL, rolling a die which has six possible outcomes 1, 2, …, 6. We would like to know how many possible outcomes are there in selecting 10 student representatives from 3000 students. When we consider the outcomes of several experiments we shall follow the following rules.

9.2 Principle of Counting

9.2.1 Rules:

(i). **Rule of Sum**: If the object *A* may be chosen in '*m*' ways, and *B* in '*n*' ways, then "either *A* or *B*" (exactly one) may be chosen in $m + n$ ways. This can be generalized for any '*p*'objects.

(ii). **Rule of Product**: If the object *A* may be chosen in *m* ways and the object *B* in *n* ways, then both "*A* and B" may be chosen in this order in '*mn*' ways. This can be generalized for any '*p*' objects.

9.2.2 Example: If there are 42 ways to select a representation for class *A* and 50 ways to select a representative for the class *B*, then

(i). By the rule of product, there are 42×50 ways to select the representative for both the class *A* and class *B*;

(ii). By the rule of sum, there will be $42 + 50$ ways to select a representative for either class *A* or class *B*.

9.2.3 Example: Suppose a license plate contains 2 letters followed by four digits, with the first digit is not zero. How many different license plates can be printed ?.

Solution: Each letter can be printed in 26 different ways.

Since the first digit is other than zero, this can be selected in 9 ways.

Second, third and fourth digits in 10 ways.

Therefore by the rule of product, there are 26 × 26 × 9 × 10 × 10 ways.

Special case: All are distinct

First letter can be printed in 26 ways.

Second letter can be printed in 25 ways.

First digit can be printed in 9 ways (other than ‘0’).

Second digit can be printed in 9 ways (any one from 0 to 9 except choosen first digit)

Third digit can be printed in 8 ways

Fourth digit can be printed in 7 ways.

Therefore by the rule of product, there are 26 × 25 × 9 ×9 × 8 × 7 ways.

Self Assessment Question 1:

a) How many different binary bit strings of length 7 are there?

b) Suppose that a State’s license plates consist of three letters followed by 4 digits. How many different plates can be formed if repetitions are allowed?

c) A company produces combination locks. The combinations consist of three numbers from 0 to 9 inclusive. No number can occur more than once in the combination. How many different combinations for locks can be attained?

d) How many possible outcomes are there when 100 dice are rolled?

e) A new-born child can be given I or 2 names. In how many ways can a child be named if we can choose from 100 names?

9.3 Permutation of distinct things

Let us recollect that the first of the members of an r-permutation of n distinct things may be choosen in n ways. The second is choosen in $(n - 1)$ ways, …., the rth is choosen in $n - (n - 1)$ ways.

So by the repeated application of product rule, the number required is $n(n - 1)\ldots.(n - (r - 1))$ ways, $n \geq r$., it is denoted by $p(n, r)$.

If $r = n$, then $p(n, n) = n(n - 1) \ldots (n - n + 1) = n(n - 1) \ldots 2.1 = n!$.

$$\text{Therefore } p(n , r) = \frac{n(n-1)(n-2).....(n-(r-1))....2.1}{(n-r)....2.1}$$

$$= \frac{n!}{(n-r)!}$$

$$= \frac{p(n, n)}{p(n-r, n-r)}$$

or $p(n, n) = p(n, r). p(n -r, n - r)$.

9.3.1 Problem: Prove that $p(n, r) = p(n - 1, r) + r.p(n - 1, r - 1)$

Solution: Write $p(n, r) = n(n - 1) \ldots (n - (r- 1)) = (n - 1)(n - 2) \ldots.. n - (r - 1)[(n - r) + r]$
Which is equal to $p(n - 1, r) + r.p(n -1, r - 1)$, on multiplication.

9.3.2 Permutations with repetitions: The number of permutations of n objects taken 'r' at a time with unlimited repetition, which is same as the number of ways of filling r blank spaces with n objects.

After choosing the object in n ways, the next object can also be choosen in 'n' ways and so on.
Therefore, in this case there are $\underbrace{n \times n \times \ldots. \times n}_{\text{r times}} = n^r = U(n, r)$ ways.

9.3.3 Example: A bit is either 0 or 1: a byte is a sequence of 8 bits. Find (a) the number of bytes that can be formed (b) the number of bytes that begin with 11 and end with 11, (c) the number of bytes that begin with 11 and do not end with 11, and (d) the number of bytes that begin with 11 or end with 11.

Solution:(a) Since the bits 0 or 1 can repeat, the eight positions can be filled up either by 0 or 1 in 2^8 ways. Hence the number of bytes that can be formed is 256.

(b) Keeping two positions at the beginning by 11 and the two positions the end by 11, there are four open positions which can be filled up in 2^4 = 16 ways. Hence the required number is 16.

(c) Keeping two positions at the beginning by 11, the remaining six open positions can be filled up by 2^6 = 64 ways. Hence the required number is 64 -16 = 48.

(d) 64 bytes begin with 11, likewise, 64 bytes end with 11. In the sum of these numbers, 64 + 64 = 128, each byte that both begins and ends with 11 is counted twice. Hence the required number is l28-16 = ll2 bytes.

9.3.4 Example: A computer password consists of a letter of the alphabet followed by 3 or 4 digits. Find (a) the total number of passwords that can be formed, and (b) the number of passwords in which no digit repeats.

Solution: (a) Since there are 26 alphabets and 10 digits and the digits can be repeated, by product rules the number of 4-character password is 26.10.10.10. = 26000. Similarly the number of 5-character password is 26.10.10.10.10. = 260000. Hence the total number of passwords is 26000 + 260000 = 286000.

(b) Since the digits are not repeated, the first digit after alphabet can be taken from any one out of 10, the second digit from remaining 9 digits and so on. Thus the number of 4- character password is 26.10.9.8 = 18720 and the number of 5-character password is 26.10.9.8.7 = 131040 by the product rule. Hence, the total number of passwords is 149760.

9.3.5 Example: How many 6-digit telephone numbers have one or more repeated digits?

Solution: Six-digit numbers can be formed in 10^6 ways. There are P(10, 6), 6-digit numbers without repetitions. Hence there are 10^6-P(10, 6) numbers have one or more digits repeated.

Self Assessment Question 2: In how many ways can the letters of the word ‘SUNDAY’ be arranged? How many of them begin with S and end with Y? How many of them do not begin with S but end with?

9.3.6 Problem: Find the sum of all the four digit number that can be obtained by using the digits 1, 2, 3, 4 once in each.

Solution: The number of permutations (arrangements) can be made using 4 numbers (1, 2, 3, 4) taking 4 at a time is $p(4, 4) = \frac{4!}{0!} = 24$.

Each number occur 6 times in unit place, 6 times in 10th place, 6 times in 100th place, 6 times in 1000 place.

Therefore sum of the numbers in the unit place is = 6.1 + 6.2 + 6.3 + 6.4 = 60;

Total sum of the digits in the 10th place = 60×10

Total sum of the digits in the 100th place = 60×100

Total sum of the digits in the 1000th place = 60×1000

Therefore total sum of all 24 numbers = 66,660.

9.3.7 Example: In how many ways 4 examinations can be scheduled within a six-day period so that no two examinations are scheduled on the same day?

Solution: $P(6, 4) = 6 \times 5 \times 4$ as 4 examinations can be considered as distinct balls and 6 days as distinct boxes.

9.3.8 Example: Determine the number of 5-digit decimal numbers that contain no repeated digits and does not have a leading 0.

Solution: There are 10 digits 0, 1, 2, 3, 4, 5, 6 7, 8, 9. Here n = 10. We can form 5 digit numbers with no repeated digits in $P(10, 5) = 10 \times 9 \times 8 \times 7 \times 6 = 30240$ ways.

Among these 30240 numbers there are $9 \times 8 \times 7 \times 6 = 3024$ numbers with leading 0. Thus there are 30240 — 3024 = 27216, 5-digit numbers with no repetition and without leading zero.

9.3.9 Example: Suppose there are 6 boys and 5 girls.

(i) In how many ways can they sit in a row?

(ii) In how many ways can they sit in a row if the boys and girls are each to sit together?

(iii) In how many ways they can sit in a row if the girls are to sit together and the boys do not sit together?

(iv) How many seating arrangements are there with no two girls sitting together?

Solution: (i) There are 6 + 5 = 11 persons and they can sit in P(11, 11) = 11! ways.

(ii) The boys among themselves can sit in 6! ways and the girls among themselves can sit in 5! ways. They can be considered as 2-units and can be permuted in 2! ways. Thus the required seating arrangements can be in 2! 6! 5! ways.

(iii) The boys can sit in 6! ways and girls in 5! ways. Since girls have to sit together they are considered as one unit. Among the 6 boys either 0 or 1 or 2 or 3 or 4 or 5 or 6 have to sit to the left of the girls unit. Of these seven ways 0 and 6 cases have to be omitted as the boys do not sit together. Thus the required number of arrangements = 5 × 6! × 5!.

(iv) The boys can sit in 6! ways. There are seven places where the girls can be placed. Thus total arrangements are P(7, 5) × 6!.

9.3.10 Example: In how many ways can the letters of English alphabet be arranged so that there are exactly 5 letters between the letters a and b.

Solution: There are P(24, 5) ways of arranging 5 letters between a and b; 2 ways to place a and b; and 20! ways to arrange any 7-letter word treated as one unit with the remaining 19 letters. Thus there are P(24, 5) × 2 × 20! ways.

9.3.11 Example: Find the number of ways in which 5 boys and S girls can be seated in a row if the boys and girls are to have alternate seats.

Solution:

Case (i): Boys can be arranged among themselves in 5! ways.

_B_B_B_B_B

There are 6 places for girls. Hence there are P(6, 5) × 5! arrangements.

Case (ii) Girls can be arranged in 5! ways.

_G_G_G_G_G_

There are 6 places for boys. Hence there are P(6, 5) × 5! ways.

Hence taking the two cases into account there are 2 × P (6, 5) × 5! arrangements in total.

9.4 Combinations

The number of ways to select r objects from n distinct objects is called an r combinations of n objects and is denoted by C(n, r). Observe C(n, 1) = n, C(n, n) = 1 and C(n, 0) = 1. The other notations are $^{n}C_{r}$ and $\begin{pmatrix} n \\ r \end{pmatrix}$.

9.4.1 Theorem: The *r* objects of each *r*-combination can be permuted among *r*! different *r*-permutations, each of which corresponds to a single combination. If the number or *r*-combinations of n objects without repetition (denoted by C(*n*, *r*)). Then $C(n, r) = \dfrac{n!}{(n - r)!}$

Proof: Any r permutations of n objects without repetition can be obtained by selecting r objects and then arranging the r objects in all possible orders.

Selection can be made in C(n, r) ways and arrangements can be made in r! ways.

Thus P(n, r) = r! C(n, r).

This implies that $C(n, r) = \dfrac{n!}{(n - r)!\,r!} = \begin{pmatrix} n \\ r \end{pmatrix}$.

Note that $C(n – 1, r - 1) + C(n – 1, r) = C(n, r)$.

9.4.2 Problem: How many ways may one right and one left shoe be selected from six pairs of shoes without obtain a pair.

Solution: Any one of the left shoe can be selected in six ways. We have five choice for selecting a right shoe without obtaining a pair. Therefore the total number of ways selecting one left and one right shoe is = 6 × 5 = 30 ways.

9.4.3 Problem: A new national flag is to be designed with six vertical strips in yellow, green, blue, and red. In how many ways can this be done so that no two adjacent strips have the same colour.

Solution: The first strip can be selected in four different ways. Since no two adjacent strips have the same colour, the second strip can be selected in three different ways. In a similar way, 3rd , 4rth, 5th and 6th strips are selected in three different ways. Therefore the total number of ways selecting the different colours in the strips are $4 \times 3 \times 3 \times 3 \times 3 \times 3 = 4 \times 3^5 = 972$ ways.

9.4.4 Problem: (i). How many positive integers less than one million can be formed using 7's 8's and 9's only ?

(ii). How many using 0's, 8's and 9's only ?.

Solution: (i). We find the number of integers used from 1 to 9,99,999.

Number of single digits (less than 10) are 7, 8, 9.

Number of integers formed using two digits are $3 \times 3 = 3^2$.

Similarly, number of integers with 3 digits is $3 \times 3 \times 3 = 3^3$, …, the number of integers with 6 digits is 3^6.

Therefore the total number of positive integers less than 1 million can be formed using 7, 8, 9 only = $3 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 = 1092$.

(ii). Number of positive integers contuining one digit is 2 (zero is not considered); number of positive integers containing two digits = 2 × 3^1., and so on, number of positive integers containing six digits is 2 × 3^5.

Therefore the total number of integers containing 0, 8, 9 is = $2 + 2(3 + 3^2 +\ldots+ 3^5) = 728$.

9.4.5 Definition: The permutations considered so far are called linear permutations as the objects are being arranged in a row (line). Suppose we arrange them in a circle, see the fig.

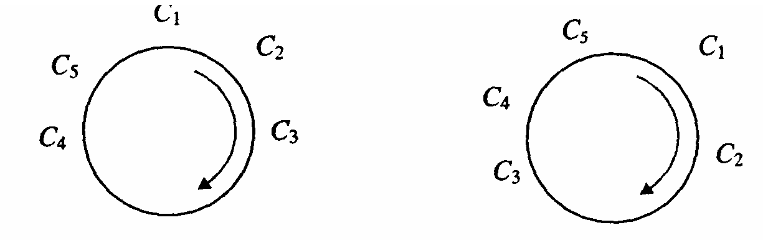


Figure: Circular permutation.

The arrangements are considered to be the same if the objects are in the same order clockwise. Therefore keeping c1 in a fixed position there are (n -1)! arrangements for the remaining objects. We have the following theorem.

9.4.6 Note: There are (n-1)! permutations of n distinct objects in a circle.

9.4.7 Example: How many ways are there to seat 10 boys and 10 girls around a circular table? If boys and girls sit alternate how many ways are there?

Solution: There are total 19! seating arrangements. 10 boys can be arranged in 10! ways. There are 9 gaps for girls and can be placed in 9! ways.

Thus, we have 10! × 9! ways.

9.4.8 Theorem: There are 2^r subsets of a set A with r elements.

Proof: Consider the problem of placing r elements of A in two boxes. Corresponding to each placement we can define a subset of A by taking the elements placed in box 1 and discarding the elements placed in box 2. Since there are 2^r ways to place r elements, there are 2^r subsets of A. That is P(A) contains 2^r elements.

9.4.9 Example: There are 2^r, r-digit binary sequences. Out of these 2^r sequences how many of them have even number of l's?

Solution: Pair off these binary sequences such that two sequences in a pair differ only in the r^{th} digit. Clearly one of the two sequences in a pair has even number of l's and other has odd number of l's. Hence there are $\frac{1}{2} \times 2^r = 2^{r-1}$, r-digit binary sequences that contain even number of l's.

9.4.10 Note: Consider n objects of which m_1 are first kind, m_2 are of second kind, …., m_k are of k^{th} kind, then $\sum_{i=1}^{k} m_i = n$.

9.4. 11 Theorem: The number of distinguishable permutations of n objects in which the first object appears in m_1 times, second object in m_2 ways, …. and so on, $\frac{n!}{m_1!m_2!....m_k!}$, where m_k is the k^{th} object appears in m_k times.

Proof: Let x be the number required. In permutation among x, make m_1 all distinct. Since m_1 objects can be permuted among themselves, one permutation will give rise to $m_1!$. Therefore x permutations give $x.m_1!$ permutations. Now make m_2 identical objects all distinct. Then we get $xm_1!\ m_2!$ Permutations of n objects in which m_3 are alike, … m_k are alike. Continuing this process we get $xm_1!\ m_2!\ \ldots\ m_k!$ as the number of permutations of n objects of which are all distinct and hence equal to $n!$.

Therefore $x = \frac{n!}{m_1!\,m_2!....m_k!}$.

9.4.12 Example: Find the number of different letter arrangements can be formed using “MATHEMATICS”.

Solution: Total number of letters n = 11 (with repetitions)

Number of M’s = 2

Number of T’s = 2

Number of A’s = 2.

And the letters H, C, S, E, each is 1.

Therefore the required number of permutations is $\frac{11!}{2!2!2!1!1!1!1!}$ = 6652800.

Self Assessment Questions 3:

a) Compute P(8, 5) and P(7, 4).

b) In how many ways can 10 people arrange themselves

   I. In a row of 10 chairs?

   II. In a row of 7 chairs?

   III. In a circle of 20 chairs?

c) In how many ways can 7 women and 3 men be seated in a row if the 3 men must always sit next to each other?

d) How many 5-digit even numbers can be formed using the figures 0, 1, 2, 3, 5, 7 and 8 without using a figure more than once?

9.4.13 Example: (a) In how many ways a committee of 3 be formed chosen from 10 people.

(b) How many committees of 3 or more can be chosen from 10 people?

Solution: (a) C(10, 3) ways

(b) C(l0, 3) + C(l0, 4) + C(10, 5) + ... + C(10, 10), which is also equal to 2^{10}-C(10, 1) C(l0, 2).

Self Assessment Question 4: Find the number of arrangements of the letters in the word: ACCOUNTANT.

9.4.14 Example: How many ways can 3 integers be selected from the integers 1, 2, 3, ..., 30 so that their sum is even.

Solution: There are 15 odd integers 1, 2, 5, ..., 29 and 15 even integers 2, 4, 6, ..., 30. Sum of 3 integers will be even only if

(i) All the 3 are even.

(ii) Two of them odd and one even.

Hence the total number of ways to select 3 integers out of the given 30 integers is C(15, 3) + C(15, 2)C(15, 1) = 560 ways.

9.4.15 Problem: Find the number of subsets of a set with n elements, in a different way.

Solution: The number of subsets with $r \leq n$ elements is given by C(n, r). Hence altogether there are C(n, 0) + C(n, 1) + ... + C(n, n) subsets of A. But from binomial theorem, we have the number of subsets of a set with n elements as

$$C(n, 0) + C(n, 1) + \ldots + C(n, n) = 2^n$$

9.4.16 Example: A multiple choice test has 15 questions and 4 choices for each answer. How many ways can the 15 questions be answered so that,

(a) exactly 3 answers are correct? (b) at least 3 answers are correct?

Solution:

(a) Exactly 3 answers are correct is 3^{12} C(15, 3)

(b) At least 3 answers correct are 4^{15} - [3^{15} + 3^{14} C(15, 1) + 3^{13}C(15, 2)].

9.4.17 Example: A student is to answer 12 out of 15 questions in an examination. How many choices does the student have?

a) in all?

b) if he must answer the first two questions.

c) if he must answer the first or second question but not the both.

d) if he must answer exactly 3 of the first-five questions.

e) if he must answer at least 3 of the first-five questions.

Solution:

(a) C(15, 12) ways

(b) If the first-two questions are to be answered he has to select 10 questions out of remaining 13. Thus he has C(1 3, 10) choices.

(c) If he answers the first question he could not choose the second question. So he has to choose 11 questions from the remaining 13 questions. Hence he has C(13, 11) choices. Similarly, if he answers the second question he has C(13, 11) choices. Total number of choices = 2 × C(13, 11).

(d) To choose 3 from the first 5 he has C(5, 3) choices. Other 9 questions have to be chosen from the next 10 questions. He has C(l0, 9) choices. Thus in total he has C(5, 3)C(10, 9) choices.

(e) He can choose 3 from the first-five and 9 from the next 10 questions. Or, he can choose 4 from the first-five and 8 from the next 10 questions. Or, he can choose 5 from the first-five and 7 from the next 10 questions. Thus he has

$$C(5, 3)C(10, 9) + C(5, 4)C(10, 8) + C(5, 5)C(10, 7)$$

choices.

9.4.18 Note: (Combinations with repetitions) Suppose that r selections are to be made from n items without regard to the order and that unlimited repetitions are allowed, assuming at least *r*-copies of *n* items. The number of ways of these selection can be made is $C(n + r - 1, r) = \frac{(n+r-1)!}{r!(n-1)!}$.

9.4.19 Example: The number of ways to choose 3 out of 7 days (repetitions allowed) is C(7 + 3 -1, 3) C(9, 3) = 84.

9.4.20 Example: When 3 dice are rolled the number of different outcomes is C(6 + 3 -1, 3) = 56 as rolling 3 dice is same as selecting 3 (here r = 3) numbers from numbers 1, 2, 3, 4, 5, 6, (here n = 6) with repetitions allowed.

9.4.21 Example: Find the number of ways to seat 5 boys in a row of 12 chairs using permutations and using combinations.

Solution: (a) Using permutations:

The problem is to arrange 12 objects that are of 6 different kinds. The 6 different objects are 5 boys and 7 unoccupied chairs (these 7 considered as a single object). Thus the number of arrangements is $\dfrac{12!}{1!1!1!1!1!7!} = \dfrac{12!}{7!}$

(b) Using combinations: Five boys can be arranged in a row in 5! ways. Distribute the 7 unoccupied chairs arbitrarily in 6 places (in the gaps between any two boys or at the two ends). Then

Total number of ways = 5! × C(6 + 7 -1, 7) = 5! × C(12, 7) = 5! × $\dfrac{12!}{5!\times 7!} = \dfrac{12!}{7!}$.

9.4.22 Example: In how many ways can a lady wear five rings on the fingures (not the thumb) of her right hand ?

Solution: There are five rings and four fingures. Five rings can be permuted in *p*(5, 5) ways. The number of unrestricted combinations of 4 objects taken 5 at a time is $\binom{4+5-1}{5} = \binom{8}{5}$.

Therefore the total number of ways = 5! $\binom{8}{5}$ = 6720.

Self Assessment Question 5: How many different two digit positive integers can be formed from the digits:0, 1, 2, 3, 4, 5, 6, 7, 8, 9. (i) When repetition is not allowed, (ii) When repetition is allowed.

9.5 Answers to Self Assessment Questions

SAQ1.

a) 2^7

b) $26^3 \times 10^4$

c) $10 \times 9 \times 8 = 720$

d) 6^{100}

e) $100 + (100 \times 99)$

SAQ2.

The word SUNDAY consists of 6 letters, which can be arranged in P (6, 6) = 6! = 720 ways. If 'S' occupies first place and Y occupies last place, then other four letters U, *N*, D, A can be arranged in 4! = 24 ways. If S does not occupy the first place but Y occupies last place, the first place can be occupied in 4 ways by any one of U, *N*, D, A. For the second place, again 4 letters are available, including S. The 3rd, 4th and 5th places can be filled by 3, 2, 1 ways. Hence the required number of arrangements = $4 \times 4 \times 3 \times 2 \times 1 = 96$.

SAQ3.

a) 6720, 840

b) I) 10!, II) P(10, 7), III) 9!.

c) 3! 8!

d) 1080 (allowing leading zero).

SAQ4.

The number of arrangements $= \frac{10!}{2!2!2!2!1!} = 226800.$

5. (i) 90, (ii)100.

9.6 Summary

In this lesson we studied the basic principles of counting. Techniques for counting are important in computer science especially in probability theory and in the analysis of algorithms. Some illustration on permutations and combination with distinct objects are given. These are also useful in graph theoretical algorithm.

9.7 Technical Terms

$P(n\ , r)$ $= \frac{n(n-1)(n-2).....(n-(r-1))....2.1}{(n-r)....2.1} = \frac{n!}{(n-r)!}$

$C(n, r)$ $= \frac{n!}{r!(n-r)!}$

Combinations with repetitions: Suppose that r selections are to be made from n items without regard to the order and that unlimited repetitions are allowed, assuming at least r-copies of n items. The number of ways of these selection can be made is $C(n + r - 1, r) = \frac{(n+r-1)!}{r!(n-1)!}$.

9.8 Model Questions

1. How many numbers between 4000 and 6000 can be formed by using the integers 1, 2, 3, 4, 5, 6, 7 and 8 if any integer is not used more than once?

2. There are 6 books on mathematics, 3 on computer science, and 5 on electronics. In how many ways can these be placed on a shelf if books on the same subjects are to be together?

3. Six papers are set in an examination of which two are mathematics. In how many ways can the examination papers be arranged if the mathematics papers are not to be together?

4. Find the number of different arrangements that can be made out of the letters of the word 'TRIANGLE' if the vowels are to come together.

5. How many 4 – digit numbers can be formed by using 2, 4, 6, 8 when repetition of digits is allowed?

6. In how many ways can 4 prizes be distributed among 5 persons when
(i). No person gets more than 1 prize
(ii). A person may get any number of prizes.
(iii). A person gets all the prizes.

7. Out of 15 boys and 9 girls, how many different committees can be formed each
consisting of 6 boys and 4 girls?

8. How many cards must you pick up from a standard 52 card deck to be sure of getting at least one red card.

9. A dice are rolled thrice, find the numbers of different outcomes

10. A bag contains 5 red marbles and 6 white marbles. Find the number of ways of selecting 4 marbles such that 2 are red and 2 are white.

11. There are 12 points P_1, P_2, ..., P_{12} in the plane, no three of them on the same line.

(a) How many triangles can be formed?

(b) How many of the triangles contain the point P1 as a vertex?

12. How many diagonals are there in a regular polygon of n sides?

13. How many ways can 5 days be chosen from each of the 12 months of an ordinary year of 365 days?

9.9 References

1. Akerkar Rajendra and Akerkar Rupali. “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Liu.C.L., “Elements of Discrete Mathematics”, Mc Hill.

3. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. “Quantitative Methods”, Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

4. Shanker Rao, G., “Discrete Mathematical Structures”, New Age International Publishers, New Delhi, 2002.

5. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

6. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 10

Partitions and Binomial Coefficients

Objectives

At the end of the lesson the student must be able to:

(i) Learn the partitions of integers and sets.
(ii) Know the properties of binomial coefficients and combinatorial identities.
(iii)Application of multinomial theorem.
(iv)Convert the discrete numeric functions and generating function.

Structure

10.1 Introduction

In this lesson we start with the partition of integers and the sets. We present some basic identities involving binomial coefficients. In formulas arising from the analysis of algorithms in computer science, the binomial coefficients occur. We extended the notion of binomial to multinomial and obtained provided suitable illustrations. We end with the representations of discrete numeric functions and the corresponding generating functions.

10.2 Partitions

10.2.1 Definition: Let S be a set with n distinct elements, and let t be a positive integer. A **t-partition** of the set S is a set $\{A_1, A_2, ..., A_t\}$ of t subsets of S, such that

(i) $S=A_1 \cup A_2 \cup .... \cup A_t$

(ii) $A_i \cap A_j = \phi$ (empty set) $i \neq j$

The subsets A_i, are called **parts** or **cells** or **blocks** of S.

Note that (i) We will omit 't' and simply call partition.

(ii) An ordered partition of S is a partition with a specified order on the subsets.

10.2.2 Example: For S = {a, b, c, d}; A_1 = {a, b}, A_2 = {c}, A_3 = {d} form a 3-partition of S. Then (A_1, A_2, A_3), (A_1, A_3, A_2), (A_2, A_1, A_3), (A_2, A_3, A_1), (A_3, A_1, A_2) and (A_3, A_2, A_1) form 6 different ordered partitions of S using the subsets A_1, A_2, A_3.

10.2.3 Note: An ordered partition of S is of *type* $(q_1, q_2, ..., q_t)$ if $|A_i| = q_i$. That is., A_i contains q_i elements.

10.2.4 Example: For the set S = {a, b, c, d), write A_1 = {a), A_2 {b}, A_3 = {c, d}. Then (A_1, A_2, A_3) is a partition. This is of a type (1, 1, 2) partition.

The following theorem gives the number of ordered partitions of a set.

10.2.5 Theorem: The number of ordered partition of a set with n elements of type (q_1, q_2, ..., q_t) is P(n, q_1, q_2, ..., q_t) = $\frac{n!}{q_1!q_2!...q_t!}$.

Proof: q_1 elements of the first set can be chosen in C(n, q_1) ways and q_2 elements of the second set in C(n-q_1, q_2) ways etc.

Thus the number of ordered partitions of type (q_1, q_2, ..., q_t) is C(n, q_1), C(n-q_1, q_2) … C(n- q_1-q_2 …-q_{t-1}, q_t), which is equal to P(n, q_1, q_2, …, q_t).

10.2.6 Example: Let S = {a, b, c, d}. The number of ordered partition of type (1, 2, 1) is P(4, 1, 2, 1) = $\frac{4!}{1!2!1!}$ = 12.

10.2.7 Example: A store has 10 red flags, 5 white flags, 4 yellow flags and 6 blue flags. In how many ways can the flags be displayed?

Solution: Total number of flags n = 25. They are partitioned into (10, 5, 4, 6) type ordered partitions. The number of such ordered partitions is

$$\frac{25!}{10!5!4!6!}$$

10.2.8 Theorem (**unordered partitions**): Let S be a set with n elements and n = qt. Then the number of unordered partitions ‘of S of type (q_1, q_2, ..., q_t) is $\frac{1}{t!}\frac{n!}{(q!)^t}$

Proof: Each unordered t-partition gives rise to t! ordered partitions. Hence the theorem follows.

10.2.9 Example: In how many ways 12 of the 14 people will be distributed into 3 teams of 4 each?

Solution: The number of ways where 12 people can be chosen from 14 is C(14, 12). Hence there are

C(14, 12) $\frac{1}{3!}\frac{12!}{(4!)^3}$

unordered (4, 4, 4) type partitions.

10.2.10 Definition: Let $A_1, A_2, ..., A_n$ be subsets of S. Then a **minset generated** by $A_1, A_2, \ldots, A_n$ is of the form $B_1 \cap B_2 \cap ... \cap B_n$, where B_i, may be either A_i, or $A_i^{'}$ ($A_i^{'}$ = S – A_i).

10.2.11 Theorem: Let $A_1, A_2, ..., A_n$ are subsets of S. Then the non-empty minsets generated by $A_1, A_2, ..., A_n$ form a partition of S.

Proof: Let $A_1, A_2, ..., A_n$ are n subsets of S. Then there are k = 2^n minsets $M_1, M_2, \ldots, M_k$ (generated by $A_1, A_2, ..., A_n$). Further $\bigcup_{i=1}^{k} M_i \subseteq S.$ Now let x ∈ S. Then x ∈ A_i or $A_i^{'}$ for i = 1, 2, ..., n.

Thus x will be in one of the minsets. Hence S = $\bigcup_{i=1}^{k} M_i$.

Hence $M_1, M_2, ..., M_k$ form a partition of S.

10.2.12 Example: Let S = {1, 2, 3, ..., 9). Give a partition of S into minsets generated by A_1 = {1, 2, 5), A_2 = {5, 6, 8, 9) and A_3 = {2, 3, 4}.

Solution: We have

$A_1^{'}$ = {3, 4, 6, 7, 8, 9}

$A_2^{'}$ = {1, 2, 3, 4, 7}

$A_3^{'}$ = {1, 5, 6, 7, 8, 9}

$M_1 = A_1 \cap A_2 \cap A_3 = \phi$

$M_2 = A_1^{'} \cap A_2 \cap A_3 = \phi$

$M_3 = A_1 \cap A_2^{'} \cap A_3 = \{2\}$

$M_4 = A_1 \cap A_2 \cap A_3^{'} = \{5\}$

$M_5 = A_1^{'} \cap A_2^{'} \cap A_3 = \{3, 4\}$

$M_6 = A_1^{'} \cap A_2 \cap A_3^{'} = \{6, 7, 8\}$

$M_7 = A_1 \cap A_2^{'} \cap A_3^{'} = \{1\}$

$M_8 = A_1^{'} \cap A_2^{'} \cap A_3^{'} = \{7\}$

form partition of S.

Self Assessment Questions 1:

1. Let S = {1, 2, 3, 4, 5) and A_1 = {2, 3, 4) and A_2 = {3, 4, 5} are subsets of S. Find the partition of S into minsets generated by $A_1$and A_2.

2. Let S = {l, 2, 3, 4, 5, 6); A_1={2, 5, 6}, A_2={1, 2, 3}, A_3={1, 4, 6}. Find the partition of S into minsets generated by A_1, A_2 and A_3.

10.3 Binomial Coefficients

10.3.1 Definition: Let n is a positive integer, we have $(a + b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2!} a^{n-2}b^2 +$

$\ldots + \frac{n(n-1)(n-2)(n-r+1)}{2!} a^{n-r}b^r + \ldots + b^n.$

This is known as **binomial theorem**. The coefficients are C(n, 0), C(n, 1), ..., C(n, r), ..., C(n, n). These coefficients are called binomial coefficients, where $C(n,r) = \frac{n!}{r!(n-r)!}$

10.3.2 Properties of binomial coefficients (Combinatorial Identities):

An identity that results from some counting process is called a *combinatorial identity*. Some identities involving binomial coefficients are given below:

1. C(n, 0) + C(n, l) + … + C(n, n) = 2^n.

2.C(n, 1) + C(n, 3) + …. = C(n,0) + C(n,2) + …. = 2^{n-1}.

3. C(n, r)=C(n, n-r)

4. Newton's Identity: C(n, r).C(r, k)=C(n, k).C(n-k, r-k) for integers n ≥ r ≥ k ≥ 0.

5. Pascal Identity: C(n+ l, r) = C(n, r) + C(n, r-1)

6. Vandermonde's Identity:

C(n + m, r) = C(n, 0). C(m, r) + C(n, 1). C(m, r- l) + … + C(n, r). C(m,0)

$= \sum_{k=0}^{r} \text{C(m, r - k).C(n, k)}$ for integers n ≥ r ≥ 0 and m ≥ r ≥ 0.

The combinatorial proofs of (3), (4) and (6) are given below and the remaining identities left as exercises.

10.3.3 Problem: Prove the identity C (n, r) = C (n, n — r):

Proof (combinational version): If r objects are chosen from n objects there are n-r objects are left. Thus selection of r objects from n objects is the same as to pick out the n-r objects that are not to be selected. Hence to every r-combination automatically there is an associated (n-r) combination and conversely. This proves the identity.

10.3.4 Problem: Prove the Pascal Identity C(n+1, r) = C(n, r) + C(n, r-l) where n and r are positive integers with r ≥ n.

Proof (combinatorial version): A choice of r of the n +1 objects $x_1, x_2 , \ldots, x_n$ may or may not include x_{n+1}. If it does not, then r objects have to be chosen from $x_1, x_2 , \ldots, x_n$ and there are C(n, r) such choices.

If it does contain x_{n+1} then r-1 further objects have to be chosen from $x_1, x_2 , \ldots, x_n$ and there are C(n, r-1) such choices. So by the rule of sum, the total number of choices is C (n, r) + C(n, r-1) which must be equal to C (n + 1, r).

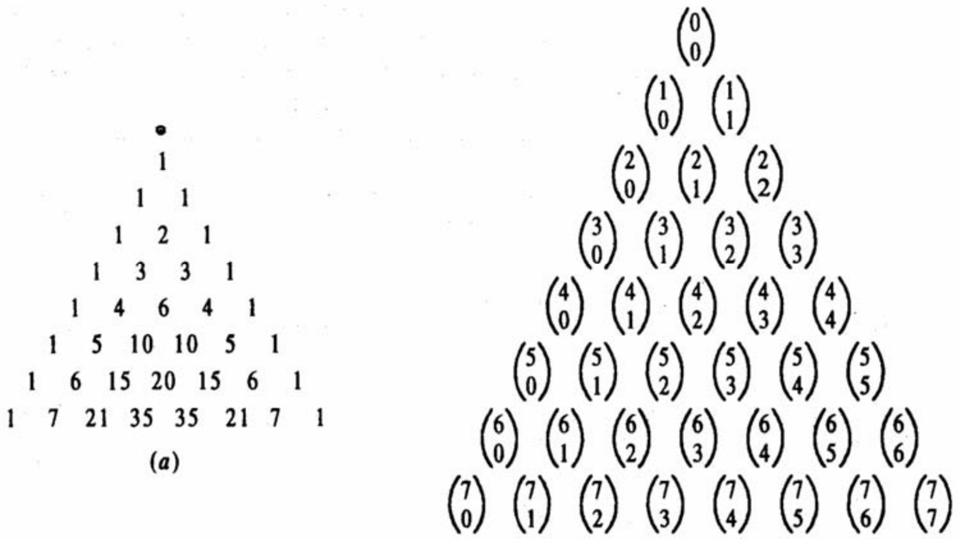
Hence C (n + 1, r) = C(n, r)+ C(n, r-1).

10.3.5 Pascal's formula: Pascal's formula gives a recurrence relation for the computation of Binomial coefficient, given the initial data C(n, 0) = C(n, n) = 1 for all n. Notice that no multiplication is needed for this computation. One can obtain the numbers by constructing a triangular array using very simple arithmetic. The triangular array is usually called *Pascal's triangle*. One can label the rows of the triangular array by n = 0, 1, 2 and the positions within the n^{th} row as k = 0, 1, 2, …, n. The zero row of the triangle is the single entry 1 and the first row be a pair of entries each equal to 1. This gives the first two rows, The n^{th} row of the triangle, which contains n + 1 numbers, can be formed from the preceding row by the following rules

(a) The first (k = 0) and the last (k = n) entries are both equal to 1.

(b) For $l \leq k \leq n\text{-}l$, the k^{th} entry in the n^{th} row is the sum of the $(k\text{-}1)^{th}$ and k^{th} entries in the (n -1) rows.

The first eight rows of Pascal's trinagle are shown in the following diagram.


1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
$\binom{0}{0}$
$\binom{1}{0}$ $\binom{1}{1}$
$\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$
$\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$
$\binom{4}{0}$ $\binom{4}{1}$ $\binom{4}{2}$ $\binom{4}{3}$ $\binom{4}{4}$
$\binom{5}{0}$ $\binom{5}{1}$ $\binom{5}{2}$ $\binom{5}{3}$ $\binom{5}{4}$ $\binom{5}{5}$
$\binom{6}{0}$ $\binom{6}{1}$ $\binom{6}{2}$ $\binom{6}{3}$ $\binom{6}{4}$ $\binom{6}{5}$ $\binom{6}{6}$
$\binom{7}{0}$ $\binom{7}{1}$ $\binom{7}{2}$ $\binom{7}{3}$ $\binom{7}{4}$ $\binom{7}{5}$ $\binom{7}{6}$ $\binom{7}{7}$

(*a*)

(*b*)

A basic property of binomial coefficients is illustrated by Pascal's triangle. If we evaluate th numbers, we can find that we obtain the same numbers as in the first six rows of Pascal's triangle. Each number in the triangle is the sum of the two numbers above it, i.e., the number just above i and to the right, and the number just above it and to the left.

For example, take n = 5 and k = 3, we have $\binom{5}{3}=\binom{4}{3}+\binom{4}{2}$, which is the particular case of Pascal's identity.

10.4 Multinomial Coefficients

The expression in the form $x_1 + x_2$ is a binomial, a multinomial is an expression of the form $x_1 + x_2 + \ldots + x_n$, with $n \geq 3$. Just as binomial coefficients appear in the expansion of powers of a binomial, multinomial coefficients appear when a power of a multinomial is expanded.

10.4.1 Multinomial Theorem: For real numbers a$_1$, …, a$_k$ and for n ∈ N, we have $(a_1 + ... + a_k)^n = \sum_{n_1+...+n_k} \begin{pmatrix} n \\ n_1...n_k \end{pmatrix} a_1^{n_1}...a_k^{n_k}$.

Here $\begin{pmatrix} n \\ n_1...n_k \end{pmatrix}$ stands for $\frac{n!}{n_1!n_2!...n_k!}$ is called the multinomial coefficient and the sum is over all possible ways to write n as n$_1$ + n$_2$ + … + n$_k$.

10.4.2 Example: Find the number of arrangement of the letters in the word ACCOUNTANT.

Solution: Total number of letters in the word ACCOUNTANT is 10. Out of which A occurs twice, C occurs twice, N occurs twice, T occurs twice and the rest are all different. Since some of the letters are repeated, we apply multinomial theorem.

Hence the number of arrangements is $\frac{10!}{2!2!2!2!} = 226800$.

10.4.3 Note: Like the term “binomial coefficient,” the term “multinomial coefficient” comes from considering algebraic expressions. Given real numbers a$_1$, a$_2$, …, a$_k$, consider the power (a$_1$ + ... + a$_k$)^n = (a$_1$ + ... + a$_k$) (a$_1$ + ... + a$_k$) ... (a$_1$ + ... + a$_k$).

After performing this product but before collecting like terms, a typical term in this product has the form $a_1^{n_1}...a_k^{n_k}$

The coefficient of $a_1^{n_1}...a_k^{n_k}$ after collecting like terms is equal to the number of ways of picking n$_1$ factors equal to a$_1$, and n$_2$ factors equal to a$_2$, and so on, as we multiply the n copies of a$_1$ + a$_2$ + ... + a$_k$. This is precisely the multinomial coefficient $\begin{pmatrix} n \\ n_1 n_2 ... n_k \end{pmatrix}$

10.4.4 Example: Find the coefficient of x^3 y^2 z^2 in $(x + y + z)^9$?

Solution: This is the same as how many ways one can choose x from three brackets, a y from 2 brackets and a z from two brackets in the expansion.

(x + y + z) (x + y + z) … (x + y + z) (9 times)

This can be done in $\begin{pmatrix} & 9 & \\ 3 & 2 & 2 \end{pmatrix} = \dfrac{9!}{3!2!2!} = 15120.$

10.5 Discrete Numeric Functions

The functions whose domain is the set of natural numbers and whose range is the set of real numbers are called sequences or discrete numeric functions or simply numeric functions. We encounter these functions very often in digital computation.

a_0, a_1, a_2, ..., a_{r}., ... denote the values of the function at 0, 1, 2, ..., r, …. We can specify a numeric function by exhaustively listing its values or by a representation.

10.5.1 Example:

(a) $\{2^0, 2^1, 2^2, ..., 2^r ...\}$ can be given the representation $a_r = 2^r$, $r \geq 0$.

(b) $a_r = 7r^3 + 1$, $r \geq 0$ represents {1, 8, 57, ...}.

(c) $b_r = \begin{cases} 2r, 0 \leq r \leq 11 \\ 3^{r-1}, r \geq 12 \end{cases}$

are some of the numeric functions.

10.5.2 Example: Suppose we deposit Rs 100 in a bank at an interest rate of 7% per year, compounded annually. The amounts at the end of the first, second, third, ... year are Rs 107, Rs 114.49, Rs. 122.50, respectively.

The amount at the end of each year is a numeric function (100, 107, 114.49, 122.50, ...).

That is $a_r = 100(1.07)^r$, $r \geq 0$.

10.5.3 Example: In a process control system a monitoring device measures the temperature inside a chemical reaction chamber once every 10 sec. Let a_r denote the rth reading in degree in centigrade. Determine an expression for a_r if it is known that the temperature rises from 100° to 125° at a constant rate in the first 100 seconds and stays at 125° afterward.

Solution: The uniform rate of rising the temperature = $\frac{125-100}{100}$ = 0.25.

The temperature at the first reading $a_1 = (100 + 0.25 \times 1)^{\circ}$

The temperature at the second reading $a_2 = (100 + 0.25 \times 2)^{\circ}$

Similarly the temperature at the rth reading $a_r = (100 + 0.25r)^{\circ}$

Thus the required numeric function $a_r = 100 + 0.25r$.

10.5.4 Definition: The **sum** of two numeric functions is a numeric function whose value at r is equal to the sum of the values of the two numeric functions at r. The **product** is defined as the numeric function whose value at r is equal to the product of values of the two numeric functions at r.

10.5.5 Example: Let

$$a_r = \begin{cases} 0, 0 \leq r \leq 2 \\ 2^{-r} + 5 \end{cases}, b_r = \begin{cases} 3 - 2^r, 0 \leq r \leq 1 \\ r + 2, r \geq 2 \end{cases}$$

Then $c_r = a_r + b_r = \begin{cases} 3 - 2^{\mathrm{r}}, 0 \le \mathrm{r} \le 1 \\ 4, \mathrm{r} = 2 \\ 2^{\mathrm{r-1}} + r + 7, r \ge 3 \end{cases}$

and $d_r = a_r b_r = \begin{cases} 0, 0 \le \mathrm{r} \le 2 \\ \mathrm{r}2^{\mathrm{-r}} + 2^{\mathrm{-r+1}} + 5\mathrm{r} + 10, \mathrm{r} \ge 3. \end{cases}$

Self Assessment Question 3: Let a and b be two numeric functions given by

$a_r = \begin{cases} 0, 0 \le \mathrm{r} \le 4 \\ 2^{\mathrm{-r}} + 3, \mathrm{r} \ge 5 \end{cases}, b_r = \begin{cases} 1 - 2^{\mathrm{r}}, 0 \le \mathrm{r} \le 2 \\ 2 + 2, \mathrm{r} \ge 2 \end{cases}$. Find a + b and a· b.

10.5.6 Definition: Let 'a' be a numeric function. Then **modulus** of 'a' denoted by $|a|$ is a numeric function defined as $|a| = \begin{cases} a_r \textit{ if } a_r \textit{ is non negative} \\ -a_r \textit{ if } a_r \textit{ is non negative} \end{cases}$

10.5.7 Note: Let a be a numeric function and α be a real number. Then αa is the numeric function whose value at r is α times the value of a at r. αa is called a *scaled version* of a of with *scaling factor* α. We use | a | to denote the numeric function whose value at r is equal to | a_r |.

10.5.8 Example: Let a be a numeric function with $a_r = (-1)^r \frac{2}{r^2}$, r ≥ 0 and if b = | a |, then $b_r = \frac{2}{r^2}$, r ≥ 0.

10.5.9 Generating Function: This is an alternative way to represent numeric functions. A numeric function a can also be represented as (a_0, a_1, …, a_r, …). The infinite series $a_0 + a_1z + a_2z^2 + \ldots + a_rz^r + \ldots$ is called the generating function of the numeric function a.

(a) The generating function for ($3^0, 3^1, 3^2, \ldots, 3^r, \ldots.$) is $3^0 + 3^1z + 3^2z^2 + \ldots + 3^rz^r + \ldots.$ The closed form of this series is $\frac{1}{1-3z}$.

(b) The generating function for the numeric function $a_r = 7 \times 3^r$, $r \geq 0$ is A(z) = $\frac{9}{1-3z}$.

10.5.10 Result: Let A(z) and B(z) are the generating functions of the numeric functions a = {a_r} and b = {b_r}. Then

(i) C(z) = A(z) + B(z) is the generating function f the numeric functions a + b.

(ii) D(z) = α A(z) is the generating function of αa.

10.5.11 Example: Find the generated function of 1, 1, 1, 1,1, 1, 1.

Solution: The generating function is given by

$$G(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = \frac{x^7 - 1}{x - 1}.$$

10.5.12 Example: Let $a_r = 2^r$ and $b_r = 3^r$ are two numeric functions. Then A(z) = $\frac{1}{1-2z}$ and B(z) = $\frac{1}{1-3z}$ are generating functions of a_r and b_r. Then the generating function of $c_r = 2^r + 3^r$ is

$$C(z) = A(z) + B(z) = \frac{1}{1-2z} + \frac{1}{1-3z}.$$

10.5.13 Example: Generating function for 2^r3^r (using partial fractions) is D(z) = $\frac{1}{1-2z}\ \frac{1}{1-3z}$

$=\frac{3}{1-3z}$ - $\frac{2}{1-2z}$.

Self Assessment Question 4: Obtain the generating function of the numeric function $a_r = 3^{r+2}$, $r \geq 0$.

10.5.14 Example: Obtain the numeric function corresponding to the generating function $\frac{x^5}{1-3x}$.

Solution: We that the numeric function a for the generating function $\frac{1}{1-3x}$ is given by $a_r = 3^r$.

Therefore the numeric function for the generating function $\frac{x^5}{1-3x}$ will be $x^5a = b$ such that

$$b_r = \begin{cases} 0, 0 \leq r \leq 4 \\ 3^{r-5}, r \geq 5 \end{cases}.$$

10.5.15 Example: Determine the numeric function corresponding to each of the following generating function.

(i) G(x) = $\frac{1}{5-6x+x^2}$

(ii) G(x) = $\frac{(1+x)^2}{(1-x)^4}$

Solution: (i) G(x) = $\frac{1}{5-6x+x^2}$ = $\frac{1}{(5-x)(1-x)}$

$$= \frac{1}{4}\left[\frac{1}{1-x} - \frac{1}{5-x}\right]$$

$$= \frac{1}{4}\frac{1}{1-x} - \frac{1}{4.5[1-\frac{1}{5}x]}.$$

Therefore $a_r = \frac{1}{4}.1 - \frac{1}{20}\left(\frac{1}{5}\right)^r = \frac{1}{4}\left[1 - \frac{1}{5^{r+1}}\right].$

(ii) $G(x) = \frac{(1+x)^2}{(1-x)^4} = (1 + x^2)(1-x)^{-4}$

$$= (1 + x^2)\left[1 + 4x + \frac{4.5}{2!}x^2 + \frac{4.5.6}{3!}x^3 + ...\right]$$

Therefore $a_r = \left[\frac{4.5.6...(r+3)}{r!} + \frac{4.5.6...(r+1)}{(r-2)!}\right] = \left[\frac{4.5.6...(r+1)}{(r-2)!}\right]\left[\frac{(r+2)(r+3)}{r(r-1)} + 1\right]$

$= \left[\frac{4.5.6...(r+1)}{(r-2)!}\right]x^r(2r^2 + 4r + 6) = \frac{(r+1)(r^3+2r+3)}{3}.$

Therefore the corresponding numeric function is $c_r = 3.3^r - 2.2^r = 3^{r+1} - 2^{r+1}$.

10.5.16 Accumulated sum of a numeric function: The accumulated sum of a numeric function a is a numeric function whose value at r is equal to $\sum_{i=0}^{r} a_i$. If A(z) is the generating function for a then the generating function for the accumulated sum is $\frac{1}{1-z}A(z)$.

10.5.17 Example: Let a be a numeric function given by $a_r = 100(1.05)^r$, $r \geq 0$. Obtain the accumulated sum of a.

Solution: Let b be the accumulated sum of a. Then

$b_r = \sum_{i=0}^{r} a_i = \sum_{i=0}^{r} 100(1.05)^r = \frac{100}{r+1}[(1.05)^{r+1} - 1], r \geq 0.$

10.6 Answers to Self Assessment Questions

SAQ1.

$M_1 = \{3, 4\}$, $M_2 = \{2\}$, $M_3 = \{5\}$, $M_4 = \{1\}$ form a partition into mun-sets.

SAQ2.

$M_1 = \{2\}$, $M_2 = \{6\}$, $M_3 = \{5\}$, $M_4 = \{1\}$, $M_5 = \{4\}$, $M_6 = \{3\}$ form a partition into mun-sets.

SAQ3.

$$c_r = a_r + b_r = \begin{cases} 1\text{-}2^{\mathrm{r}}, 0 \le \mathrm{r} \le 2 \\ 2^{\mathrm{r}} + 2, 3 \le \mathrm{r} \le 4 \\ 2^{\text{-r}} + r + 5, r \ge 5 \end{cases}$$

$$d_r = a_r b_r = \begin{cases} 0, 0 \le \mathrm{r} \le 4 \\ \mathrm{r}.2^{\text{-r}} + 2^{\text{-r+1}} + 3\mathrm{r} + 6, \mathrm{r} \ge 5. \end{cases}$$

SAQ4.

$$\mathrm{G(x)} = \mathrm{x}^{\text{-2}}\left(\frac{1}{1-3x} - 1 - 3x\right) = x^{-2}\left(\frac{9x^2}{1-3x}\right) = \frac{9}{1-3x}.$$

10.7 Summary

In this lesson we presented notions of partition of integers and sets and various useful results. In formulas arising from the analysis of algorithms in computer science, the binomial coefficients occur. For a given numeric function the corresponding generating function (vice versa) is obtained. Multinomial coefficients are the generalizations of binomial coefficients, are given with suitable examples.

10.8 Technical Terms

Partition: Let S be a set with n distinct elements, and let t be a positive integer. A t- of the set S is a set $\{A_1, A_2, ..., A_t\}$ of t subsets of S, such that (i) $S=A_1 \cup A_2 \cup .... \cup A_t$; (ii) $A_i \cap A_j = \phi$ (empty set) $i \neq j$. The subsets A_i, are called *parts* or *cells* or *blocks* of S.

Newton's Identity: C(n, r).C(r, k)=C(n, k).C(n-k, r-k) for integers $n \geq r \geq k \geq 0$.

Pascal Identity: C(n+ l, r) = C(n, r) + C(n, r-1)

Vandermonde's Identity: C(n + m, r) = C(n, 0). C(m, r) + C(n, 1). C(m, r- l) + … + C(n, r). C(m,0) = $\sum_{k=0}^{r} \mathrm{C(m, r-k).C(n,k)}$ for integers $n \geq r \geq 0$ and $m \geq r \geq 0$.

Multinomial Theorem: For real numbers $a_1, …, a_k$ and for $n \in N$, we have $(a_1 + ... + a_k)^n = \sum_{n_1+...+n_k} \binom{n}{n_1 ... n_k} a_1^{n_1} ... a_k^{n_k}$. Here $\binom{n}{n_1 ... n_k} = \frac{n!}{n_1!n_2!...n_k!}$ and $n = n_1 + n_2 + … + n_k$.

Sum and Product: The *sum* of two numeric functions is a numeric function whose value at r is equal to the sum of the values of the two numeric functions at r. The *product* is defined as the numeric function whose value at r is equal to the product of values of the two numeric functions at r.

Modulus: Let 'a' be a numeric function. $|a| = \begin{cases} a_r \text{ if } a_r \text{ is non negative} \\ \text{-}a_r \text{ if } a_r \text{ is non negative} \end{cases}$

Generating Function: The infinite series $a_0 + a_1z + a_2z^2 + \ldots + a_rz^r + \ldots$ corresponding the numeric function a = $(a_0, a_1, \ldots, a_r, \ldots)$

Accumulated sum of a numeric function: $\sum_{i=0}^{r} a_i$.

10.9 Model Questions

1. Prove that C(n, 1) + C(n, 3) + …. = C(n,0) + C(n,2) + …. = 2^{n-1}.

2. Prove that C(n, r)=C(n, n-r)

3. Prove that C(n, r).C(r, k)=C(n, k).C(n-k, r-k) for integers n ≥ r ≥ k ≥ 0.

4. Find the coefficient of x^3y^4 in the expansion of $(2x + y^2)^5$.

4. Let a and be two numeric functions given by $a_r = \begin{cases} 0, \text{r} = 0 \\ 2, \text{r} = 1 \\ 0, \text{r} \geq 2 \end{cases}, b_r = \begin{cases} 1, \text{r} = 0 \\ 0, \text{r} \geq 1 \end{cases}$

Determine (a + b) and a·b.

5. Determine the numeric functions corresponding to the generating functions:

(i) $\frac{1}{1-z^3}$

(ii) $(1 + z)^n + (1- z)^n$

(iii) $\dfrac{1}{z^2 - 6z + 5}$

(iv) $\dfrac{1}{(1-z)(1-z^2)(1-z^3)}$

10.10 References

1. Akerkar Rajendra and Akerkar Rupali. “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, “Discrete Mathematical Structures” PHI, New Delhi, 1999.

3. Hari Kishan and Shivraj Pundir “Discrete Mathematics”, Pragati Prakashan, Meerut, 2005.

4. Liu.C.L., “Elements of Discrete Mathematics”, Mc Hill.

5. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. “Quantitative Methods”, Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

6. Shanker Rao, G., “Discrete Mathematical Structures”, New Age International Publishers, New Delhi, 2002.

7. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

8. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 11

Recurrences Relations

Objectives

At the end of the Lesson the student must be able to:

(i) Learn the solving of recurrences.
(ii) Use of generating functions to solve the recurrence relations.
(iii)Know the applications of recurrence relations.

Structure

11.1 Introduction

A sequence can be defined by giving a general formula for its n^{th} term or by writing few of its terms. An alternative approach is to represent the sequence by finding a relationship among its terms. Such relations are referred as recurrences. Recurrence relations are used to model a wide variety of problems both in computer and non-computer sciences. In this unit we provide few applications of recurrences and a brief visit to the integer functions.

11.2 Recurrence Relation

A recurrence relation for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely $a_0, a_1, \ldots, a_{n-1}$ for all integers n with $n \geq n_0$, where n_0 is a non negative integer.

A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation.

11.2.1 Example: Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1}- a_{n-2}$ for $n = 2, 3, 4, \ldots$ and suppose that $a_0 = 3$ and $a_1 = 5$. What are a_2 and a_3 ?

Solution: From the recurrence relation $a_2 = a_1 - a_0 = 5 - 3 = 2$ and $a_3 = a_2 - a_1 = 2 - 5 = - 3$. In a similar way we can find a_4, a_5 and also each successive term.

11.2.2 Example: Determine whether the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = 2\, a_{n-1}- a_{n-2}$ for $n = 2, 3, 4, \ldots$ where (i). $a_n = 3n$ for every non negative integer n and (ii). $a_n = 2^n$.

Solution: (i). Suppose that $a_n = 3n$ for every non negative integer n. For $n \geq 2$, we have that $2a_{n-1} - a_{n-2} = 2[3(n - 1)] - 3(n - 2) = 3n = a_n$.
Therefore $\{a_n\}$, where $a_n = 3n$, is a solution of the recurrence relation.
(ii). Suppose $a_n = 2^n$ for every non negative integer n. Now $a_0 = 1$, $a_1 = 2$, $a_2 = 4$. Consider $2a_1 - a_0 = 2.2 - 1 = 3 \neq a_2$. Therefore $\{a_n\}$, where $a_n = 2^n$ is not a solution of the recurrence relation.

11.2.3 Definition: A recurrence relation of the form $C_0a_r + C_1a_{r-1} + C_2a_{r-2} + \ldots + C_ka_{r-k} = f(r)$, where C_i's are constants, is called a **linear recurrence relation with constant coefficients**. Here, if both C_0 and C_k are non-zero, then it is known as k^{th} order recurrence relation.

11.2.4 Example: $2a_r + 3a_{r-1} = 2^r$ is the first order linear recurrence, with constant coefficients.

11.2.5 Fibonacci sequence of numbers: The sequence of the form {1, 1, 2, 3, 5, 8, 13, …} is called the Fibonacci sequence. This sequence starts with the two numbers 1, 1 and contains numbers that are equal to the sum of their two immediate predecessors. The recurrence relation can be written as $a_r = a_{r-1} + a_{r-2}$, $r \geq 2$, with $a_0 = 1$ and $a_1 = 1$.

11.2.6 Note: $a_n = r^n$, where r is constant, is a solution of the recurrence relation $a_n = C_1a_{n-1} + C_2a_{n-2} + \ldots. + C_ka_{n-k}$ if and only if $r^n = C_1r^{n-1} + C_2r^{n-2} + \ldots + C_kr^{n-k}$. Dividing both sides by r^{n-k} and the right hand side is subtracted from the left, we obtain the equation $r^k - C_1r^{k-1} - C_2r^{k-2} - \ldots. - C_{k-1}r - C_k = 0$ …………(i).

Therefore the sequence $\{a_n\}$ with $a_n = r^n$ is a solution if and only if r is a solution of the equation (i). Equation (i) is called the characteristic equation of the recurrence relation.

11.2.7 Theorem: Let C_1 and C_2 be real numbers. Suppose that $r^2 - C_1r - C_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = C_1a_{n-1} + C_2a_{n-2}$ if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n = 0, 1, 2, \ldots$ where α_1 and α_2 are constants.

11.2.8 Example: Find the solution of the the recurrence relation $a_n = a_{n-1} + 2a_{n-2}$ with $a_0 = 2$ and $a_1 = 7$.

Solution: The characteristic equation of the recurrence relation is $r^2 - r - 2 = 0$. Its roots are $r = 2$ and $r = -1$. Therefore the sequence $\{a_n\}$ is a solution to the recurrence if and only if $a_n = \alpha_1 2^n + \alpha_2(-1)^n$, for some constants α_1 and α_2. Now $a_0 = 2 = \alpha_1 + \alpha_2$, $a_1 = 7 = \alpha_1 = 3$ and $\alpha_2 = -1$. Therefore the solution to the recurrence relation is $a_n = 3.2^n - (-1)^n$.

11.2.9 Theorem: Let C_1 and C_2 be real numbers with $C_2 \neq 0$. Suppose that $r^2 - C_1r - C_2 = 0$ has only one root r_0. A sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = C_1a_{n-1} + C_2a_{n-2}$ if and only if $a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$, for $n = 0, 1, 2, \ldots$, where α_1 and α_2 are constants.

11.2.10 Example: Find the solution of the recurrence relation $a_n = 6a_{n-1} - 9a_{n-2}$ with the initial conditions $a_0 = 1$ and $a_1 = 6$.

Solution: The characteristic equation $r^2 - 6r + 9 = 0$. The only root is $r = 3$. Therefore the solution to the recurrence relation is $a_n = \alpha_1 3^n + \alpha_2 n3^n$, for some constants α_1 and α_2. Using the initial conditions, we get $a_0 = 1 = \alpha_1$, $a_1 = 6 = \alpha_1.3 + \alpha_2.3$. Solving these simultaneous equations, we get $\alpha_1 = 1$ and $\alpha_2 = 1$. Therefore the solution to the recurrence relation is $a_n = 3^n + n3^n$.

11.2.11 Theorem: Let $C_1, C_2, \ldots, C_k$ be real numbers. Suppose that the characteristic equation $r^k - C_1r^{k-1} - \ldots - C_k = 0$ has k distinct roots $r_1, r_2, \ldots, r_k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = C_1a_{n-1} + C_2a_{n-2} + \ldots. + C_ka_{n-k}$ if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \ldots + \alpha_k r_k^n$, for $n = 0, 1, 2, \ldots$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are constants.

11.2.12 Example: Find the solution to the recurrence relation $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ with initial conditions: $a_0 = 2$, $a_1 = 5$ and $a_2 = 15$.

Solution: The characteristic equation of the given recurrence relation is $r^3 - 6r^2 + 11r - 6 = 0 \Rightarrow (r - 1)(r - 2)(r - 3) = 0$.

The roots of this equation $r = 1$, $r = 2$, $r = 3$.

Therefore the solutions to this recurrence relation are $a_n = \alpha_1.1^n + \alpha_2.2^n + \alpha_3.3^n$.

From the given initial condition, $a_0 = 2$, we get $a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3$.

Similarly, for $a_1 = 5 = \alpha_1 + \alpha_2.2 + \alpha_3.3$; $a_2 = 15 = \alpha_1 + \alpha_2.4 + \alpha_3.9$.

Solving the above three simultaneous equations we get $\alpha_1 = 1$, $\alpha_2 = -1$ and $\alpha_3 = 2$. Therefore the unique solution to this recurrence relation is $a_n = 1 - 2^n + 2.3^n$.

11.2.13 Theorem: Let $C_1, C_2, \ldots, C_k$ be real numbers. Suppose that the characteristic equation $r^k - C_1r^{k-1} - \ldots - C_k = 0$ has t-distinct roots $r_1, r_2, \ldots, r_t$ with multiplicities $m_1, m_2, \ldots, m_t$, respectively, so that $m_i \geq 1$, for i = 1, 2, …, t and $m_1 + m_2 + \ldots + m_t = k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = C_1a_{n-1} + C_2a_{n-2} + \ldots + C_ka_{n-k}$ if and only if $a_n = (\alpha_{1,0} + \alpha_{1,1}.n + \ldots. + \alpha_{1,m_1-1}n^{m_1-1})r_1^n + \ldots + (\alpha_{t,0} + \alpha_{t,1}n + \ldots + \alpha_{t,m_t-1}n^{m_t-1})r_t^n$, for $n = 0, 1, 2, \ldots$, where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_i - 1$.

11.2.14 Example: Find the solution to the recurrence relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with initial conditions $a_0 = 1$, $a_1 = -2$ and $a_2 = -1$.

Solution: The characteristic equation to the given recurrence is $r^3 + 3r^2 + 3r + 1 = 0 \Rightarrow (r + 1)^3 = 0$. Therefore $r = -1$ is a root of multiplicity 3. By Theorem …., the solutions are of the form $a_n = \alpha_{1,0}(-1)^n + \alpha_{1,1}.n(-1)^n + \alpha_{1,2}.n^2(-1)^n$. Use the given initial conditions, find the constants $\alpha_{1,0}, \alpha_{1,1}, \alpha_{1,2}$.

Now $a_0 = 1 = \alpha_{1,0}$; $a_1 = -2 = -\alpha_{1,0} - \alpha_{1,1} - \alpha_{1,2}$; $a_2 = -1 = \alpha_{1,0} + 2\alpha_{1,1} + 4\alpha_{1,2}$.

Solving these simultaneous equations, we get $\alpha_{1,0} = 1$, $\alpha_{1,1} = 3$, and $\alpha_{1,2} = -2$. Hence the unique solution to the given recurrence is $a_n = (1 + 3n - 2n^2)(-1)^n$.

11.3 Particular Solution

The particular solution depends on the form of f(r). The particular solution for some simple functions f(r) are given in the following table.

f(r)	Particular solution
Constant k	Constant P if k is not a root of the characteristic equation. If k is a root of multiplicity m then Pr^m.

Polynomial of degree t in r, $F_1r^t + F_2r^{t-1}+\ldots+ F_{t+1}\beta^r$	Polynomial of degree t in r, $P_1r^t + P_2r^{t-1} + \ldots + P_{t+1}P\beta^r$ if β is not a root of the characteristic equation. If β is a root of multiplicity of m, then $Pr^m\beta^r$.
$(F_1r^t + F_2r^{t-1}+\ldots+ F_{t+1})\beta^r$	$(P_1r^t + P_2r^{t-1} + \ldots + P_{t+1})\beta^r$ if β is not a root of the characteristic equation. $r^m(P_1r^t + P_2r^{t-1} + \ldots + P_{t+1})\beta^r$ if β is a root of multiplicity m.

11.3.1 Note: The total solution of a recurrence relation is the sum of the homogeneous solution and the particular solution. The arbitrary constants in the homogeneous solution can be determined using boundary conditions.

11.3.2 Example: Solve $a_n - 5a_{n-1} + 6a_{n-2} = 1$

Solution: The characteristic equation is $r^2 - 5r + 6 = 0$. The roots are 3, 2.
The homogeneous solution is $A_1(3)^n + A_2(2)^n$.
Particular solution of the form P, substituting in the given relation, we get

$P-5P + 6P = 1$ or $P = \frac{1}{2}$.

Therefore the total solution is $a_n = A_1(3)^n + A_2(2)^n + \frac{1}{2}$.

11.3.3 Example: Solve $a_n - 4a_{n-1} + 4a_{n-2} = (n+1)^2$ given $a_0 = 0$ and $a_1 = 1$.

Solution: The characteristic equation is $r^2 - 4r + 4 = 0$. The roots are 2, 2. Therefore the homogeneous solution is $(A_1n + A_2)2^n$.
Particular solution is of the form $P_1n^2 + P_2n + P_3$. Substituting in the given relation, we get $P_1n^2 + P_2n + P_3 - 4 P_1(n-1)^2 - 4P_2(n-1) - 4P_3 + 4P_1(n-2)^2 + 4P_2(n-2) + 4P_3 = n^2 + 2n + 1$.
That is.,

$P_1n^2 + (P_2 - 8P_1)n + (P_3 - 4P_2 + 12P_1) = n^2 + 2n + 1.$

Equating the coefficients, we obtain that

$P_1 = 1, P_2 - 8P_1 = 2, P_3 - 4P_2 + 12P_1 = 1.$

Hence $P_1 = 1, P_2 = 10, P_3 = 29.$

Therefore the total solution is

$a_n = (A_1n + A_2)2^n + n^2 + 10\,n + 29.$

Given that $a_0 = 0$ and $a_1 = 1$, we get

$0 = A_2 + 29 \Rightarrow A_2 = -29$ and

$1 = (A_1 + A_2)2 + 1 + 10 + 29 \Rightarrow A_1 = \frac{19}{2}.$

Therefore the total solution is

$a_n = (\frac{19}{2}n\text{-}29)2^n + n^2 + 10\,n + 29.$

11.3.4 Example: Solve $a_n - 3a_{n-1} - 4a_{n-2} = 3^n$ given $a_0 = 0$ and $a_1 = 2$.

Solution: The characteristic equation is $r^2 - 3r - 4 = 0$. The roots are -1, 4.

Therefore the homogeneous solution is $A_1(-1)^n + A_24^n$.

Particular solution is of the form $P3^n$. Also 3 is not a root of the characteristic equation. Hence substituting $a_n = P3^n$ in the given equation, we get

$P3^n - 3P3^{n-1} +- 4\,P3^{n-2} = 3^n.$

This implies that $P = -\frac{9}{4}$. Hence the total solution is $a_n = A_1(-1)^n + A_2(4)^n - \frac{9}{4}3^n$.

Further $a_0 = 1$ and $a_1 = 2$. Then

$1 = A_1 + A_2 - \frac{9}{4}; 2 = A_1 + 4A_2 - \frac{27}{4}.$

We get $A_1 = \frac{17}{20}$, $A_2 = \frac{12}{5}$. Therefore the total solution is

$a_n = \frac{17}{20}(-1)^n + \frac{12}{5}(4)^n - -\frac{9}{4}(3)^n.$

11.3.5 Example: Solve $a_n — 4a_{n-1} + 4a_{n-2} = 2^n$

Solution: Characteristic equation is $r^2 – 4r + 4 = 0$. The roots are 2, 2. Homogeneous solution is of the form $(A_1n + A_2)2^n$. Since 2 is a double root of the characteristic equation, the particular solution is of the form Pn^22^n. Substituting in the given relation, we get

$Pn^22^n - 4P(n- 1)^2 2^{n-1} + 4P(n-2)^22^{n-2} = 2^n$

That is., $2P2^n = 2^n$ which implies P = 1/2. Thus particular solution is $\frac{1}{2}$ $n^2 (2)^n = (2)^{n-1}$

Hence the total solution is $a_n = (A_1n + A_2)2^n + n^2 (2)^{n-1}$.

11.3.6 Example: Solve $a_n -2a_{n-1} = (n + 1)2^n$.

Solution: Characteristic equation is $r^2 – 2r = 0$. The roots are 0, 2. The homogeneous solution is $A(2)^n$. Since 2 is a root (multiplicity 1) of the characteristic equation, the particular solution is of the form $n(P_1n + P2)2^n$. Substituting,

That is.,

$n(P_1n + P_2)2^n - 2\{(n-1)[P_1(n -1) + P_2]\}2^{n-1} = (n +1)2^n$.

That is., $(2P_1n + P_2 – P_1)2^n = (n +1)2^n$

Equating the coefficients, we get

$P_1 = \frac{1}{2}$ and $P_2 = \frac{3}{2}$.

Thus particular solution is $n\left(\frac{1}{2}n+\frac{3}{2}\right)2^n$ and $P_2 = \frac{3}{2}$.

Hence the total solution is $A_n = A(2)^n + (n^2 + 3n)2^{n-1}$.

Self Assessment Questions:

1. Solve the recurrence relation $a_n = 5a_{n-1} – 6a_{n-2}$, $n \geq 2$, given $a_0 = 1$, $a_1 = 4$.

2. Solve the recurrence $a_n = 4a_{n-1} – 4a_{n-2}$, $n \geq 2$ with initial conditions $a_0 =1$, $a_1 = 4$.

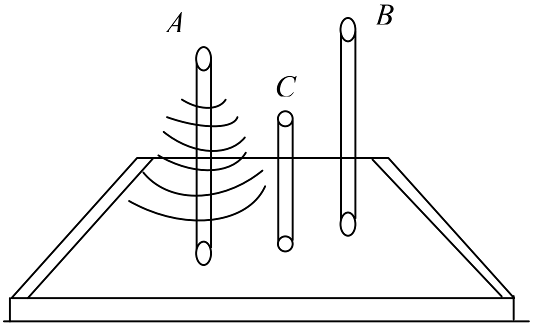
11.4 Applications of Recurrences

11.4.1 The Problem of tower of Hanoi

Given a tower of eight disks, initially stacked in decreasing size on one of the three pegs. The objective is to transfer the entire tower to one of the other pegs, moving only one disk at a time and never moving a larger on to smaller (these rules are called Lucas Rules) (This was invented by the French mathematician Edouard Lucas in 1883).

Let T_n be the minimum number of moves that will transfer n disks from one peg to another under Lucas rules. Then clearly $T_0 = 0$, since no moves are needed to transfer a tower of $n = 0$ disks.

By observation, $T_1 = 1$, $T_2 = 3$



Now transfer the top disks to the middle peg, then move the third, then bring the other two onto it. So we get $T_3 = 7 = 2.3 + 1 = 2\ T_2 + 1$.

Induction hypo: Assume for n-1 disks. That is., $T_{n-1} = 2.T_{n-2} + 1$.

Suppose that there are n-disks. We first transfer the (n-1) smallest disks to a different peg. It requires T_{n-1} moves.

Then move the largest (it requires one move), and finally transfer the (n-1) smallest disks back onto the largest (it requires another T_{n-1} moves).

Thus we can transfer n disks ($n > 0$) in at most 2 $T_{n-1} + 1$ moves.

Thus $T_n \leq 2\ T_n + 1$ for $n > 0$.

This shows that $2T_{n-1} + 1$ moves are suffices for our construction.

Next we prove that $2T_{n-1} + 1$ moves are necessary.

We must move the largest disk. When we do, the n-1 smallest disks must be on a single peg, and it has taken atleast T_{n-1} moves to put them there (we might move the largest disk more than once).

After moving the largest disk for the last time, we must transfer the n-1 smallest disks (which must be again on a single peg) back onto the largest; This requires T_{n-1} moves.

Hence $T_n \geq 2T_{n-1} + 1$ for $n > 0$.

Therefore $$\left.\begin{array}{l} T_0 = 0 \\ T_n = 2T_{n-1} + 1 \text{ for } n > 0 \end{array}\right\}$$

These set of equalities above is the recurrence for the Tower of Honai problem.

From this it is clear that $T_3 = 2.3 +1 = 7$, $T_4 = 2.7 +1 = 15$, and so on.

11.4.2 Remark: T_n can also be identified as $T_n = 2^n - 1$ for $n \geq 0$.

The proof of this remark makes use of the principle of mathematical induction.

11.5 Generating Functions

A generating function is a polynomial of the form $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$, which has infinitely many non-zero terms. There is a correspondence between generating functions and sequences. (That is, $a_0 + a_1x + a_2x^2 + \ldots \leftrightarrow a_0, a_1, a_2, \ldots$.).

11.5.1 Example: (i). The generating function of the sequence 1, 2, 3, … of natural numbers is $f(x) = 1 + 2x + 3x^2 + \ldots$.

(ii). The generating function of the arithmetic sequence 1, 4, 7, 10, … is $f(x) = 1 + 4x + 7x^2 + 10x^3 + \ldots$.

11.5.2 Note: Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots$ and $g(x) = b_0 + b_1x + b_2x^2 + \ldots$ be two generating sequences, then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$ and $f(x)g(x) = (a_0b_0) + (a_1b_0 + a_0b_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots$, the coefficient of x^n in the product $f(x)g(x)$ is the finite sum: $a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \ldots + a_nb_0$.

11.5.3 Example: If $f(x) = 1 + x + x^2 + \ldots + x^n + \ldots$ and $g(x) = 1 - x + x^2 - x^3 + \ldots + (-1)^n x^n + \ldots$, then $f(x) + g(x) = (1 + 1) + (1 - 1)x + (1 + 1)x^2 + \ldots + (1 + (-1)^n)x^n + \ldots$

$$= 2 + 2x^2 + 2x^4 + \ldots$$

$$f(x)g(x) = 1 + [1(-1) + 1(1)]x + [1(1) + 1(-1) + 1(1)]x^2 + \ldots$$

$$= 1 + x^2 + x^4 + x^6 + \ldots$$

11.5.4 Problem: Solve the recurrence relation $a_n = 3a_{n-1}$, $n \geq 1$, $a_0 = 1$ using generating function.

Solution: Consider the generating function $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$ of the sequence $a_0, a_1, a_2 \ldots$

$3x.f(x) = 3a_0x + 3a_1x^2 + \ldots + 3a_{n-1}x^n + \ldots$

$f(x) - 3x.f(x) = a_0 + (a_1 - 3a_0)x + (a_2 - 3a_1)x^2 + \ldots. + (a_n - 3a_{n-1})x^n + \ldots$

Since $a_0 = 1$, $a_1 = 3a_0$ and in general, $a_n = 3a_{n-1}$, we get $(1 - 3x) f(x) = 1$

$\Rightarrow f(x) = \frac{1}{1-3x} = (1 - 3x)^{-1} = 1 + 3x + (3x)^2 + \ldots + (3x)^n + \ldots$

Therefore a_n, which is the coefficient of x^n in $f(x)$, is equal to 3^n.

11.5.5 Problem: Solve the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$, $n \geq 2$, given $a_0 = 3$, $a_1 = -2$ using the generating function.

Solution: Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$

$$2x\text{f}(x) = \quad 2a_0x + 2a_1x^2 + \ldots + 2a_{n-1}x^n + \ldots$$

$$x^2\text{f}(x) = \quad a_0x^2 + \ldots + a_{n-2}x^n + \ldots$$

Therefore $f(x) - 2x\text{f}(x) + x^2\text{f}(x) = a_0 + (a_1 - 2a_0)x + (a_2 - 2a_1 + a_0)x^2 + \ldots$ $+ (a_n - 2a_{n-1} + a_{n-2})x^n + \ldots = 3 - 8x$ (since $a_0 = 3$, $a_1 = -2$ and $a_n - 2a_{n-1} + a_{n-2} = 0$ for $n \geq 2$).

On simplification, we get $f(x) = \dfrac{1}{(1-x)^2}(3 - 8x)$

$$= (1 + 2x + 3x^2 + \ldots + (n+1)x^n + \ldots)(3 - 8x)$$

$$= 3 - 2x - 7x^2 - 12x^3 + \ldots + (-5n + 3)x^n + \ldots.$$

Therefore the coefficient of x^n, that is.; $a_n = 3 - 5n$ is the solution.

Self Assessment Question 3:

If $f(x) = 1 + x + x^2 + \ldots, + x^n + \ldots$ and $g(x) = 1 - x + x^2 - x^3 + \ldots + (-1)^n x^n + \ldots$ Find $f(x) + g(x)$, and $f(x).g(x)$.

11.5.6 Table of some generating functions

Sequence	Generating Function
1	$\frac{1}{1-z}$
$(-1)^r$	$\frac{1}{1+z}$
a^r	$\frac{1}{1-az}$
$(-a)^r$	$\frac{1}{1+az}$
r + 1	$\frac{1}{1-(z)^2}$
R	$\frac{z}{(1-z)^2}$
r^2	$\frac{z(1+z)}{(1-z)^3}$
ra^r	$\frac{az}{(1-az)^2}$
$\frac{1}{n!}$	e^z
C(n, r)	$(1+z)^r$

11.5.7 Example: Solve the recurrence relation a_r -7a_{r-1} + l0a_{r-2} = 0 for n ≥ 2 given that a_0 = 10, a_1 = 41 using generating functions.

Solution: Multiplying the given equation by z^r and summing from 2 to ∞, we get

$$\sum_{r=2}^{\infty} a_r z^r - 7\sum_{r=2}^{\infty} a_{r-1} z^r + 10\sum_{r=2}^{\infty} a_{r-2} z^r = 0$$

⇒ [A(z) – a_0 –a_1z] – 7z [A(z) – a_0] + 10 z^2 [A(z)] = 0

⇒ [A(z) - a_0 - a_1z] — 7z[A(z) - a_0] + 10z^2[A(z)] = 0

⇒ A(z) = $\dfrac{a_0 + (a_1 - 7a_0)z}{1-7z+10z^2} = \dfrac{a_0 + (a_1 - 7a_0)z}{(1-2z)(1-5z)}$

$$= \frac{C_1}{1-2z} + \frac{C_2}{1-5z}$$

$$= C_1\sum_{r=0}^{\infty} 2^r z^r + C_2\sum_{r=0}^{\infty} 5^r z^r$$

Thus a_r = $C_1 2^r$ + $C_2 5^r$, r ≥ 2. Given that a_0 = 10, a_1 = 41. Substituting, we get C_1 = 3, C_2 = 7. Thus a_r = 3.2^r + 7.5^r.

11.5.8 Example: Solve a_r -5a_{r-1} + 6a_{r-2} = 2^r + r, where r ≥ 2, with a_0 = 1, a_1=1.

Solution: Multiplying the given equation by z^r and summing from 2 to ∞, we get

$$\sum_{r=2}^{\infty} a_r z^r - 5\sum_{r=2}^{\infty} a_{r-1} z^r + 6\sum_{r=2}^{\infty} a_{r-2} z^r = \sum_{r=2}^{\infty} 2^r z^r + \sum_{r=2}^{\infty} r z^r$$

⇒ [A(z) – a_0 –a_1z] – 5z [A(z) – a_0] + 6z^2 [A(z)] = $\dfrac{4z^2}{1-2z} + z\left[\dfrac{1}{(1-z)^r} - 1\right]$

Therefore A(z) = $\dfrac{1-8z+27-35z^2+14z^4}{(1-z)^2(1-2z)^2(1-3z)}$.

By substituting a_0 = 1, a_1 = 1, we get

A(z) = $\frac{5/4}{1-z}+\frac{1/2}{(1-z)^2}-\frac{3}{1-2z}-\frac{2}{(1-2z)^2}+\frac{17/4}{(1-3z)}$

Thus, we have

$$a_r = \frac{5}{4}+\frac{1}{2}(r+1)-3\times 2^r-2(r+1)2^r+\frac{17}{4} = \frac{5}{4}+\frac{r}{2}-r2^{r+1}-5\times 2^r+\frac{17}{4}3^r$$

11.5.9 Example: Solve the recurrence relation corresponding to the Fibonacci sequence $a_n = a_{n-1} + a_{n-2}$, $n \geq 2$, $a_0 = 0$ and $a_1 = 1$.

Solution: We get $\sum_{r=2}^{\infty} a_r z^r - \sum_{r=2}^{\infty} a_{r-1} z^r + \sum_{r=2}^{\infty} a_{r-2} z^r = 0$.

$\Rightarrow$ [A(z)-a$_1$z-a$_0$]-z[A(z)-a$_0$]-z^{2}A(z) = 0

$\Rightarrow$ A(z)[1-z-z^2] = a$_0$ + (a$_1$-a$_0$)z = 0

Substituting a$_0$ = 1 and a$_1$ = 1, we obtain

A(z) = $\frac{1+(1-1)z}{1-z-z^2}=\frac{1}{1-z-z^2} = \frac{1}{\left(1-\frac{1+\sqrt{5}}{2}z\right)\left(1-\frac{1-\sqrt{5}}{2}z\right)} = \frac{C_1}{1+\frac{1+\sqrt{5}}{2}z}+\frac{C_2}{1-\frac{1-\sqrt{5}}{2}z}$.

Hence C$_1$ = $\frac{1}{\sqrt{5}}\frac{1+\sqrt{5}}{2}$, C$_2$ = $-\frac{1}{\sqrt{5}}\frac{1+\sqrt{5}}{2}$

Hence a$_r$ = $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{r+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{r+1}$.

11.6 Answers to Self Assessment Questions

SAQ1.

$a_n = -2^n + 2(3^n)$.

SAQ2.

$a_n = 2^n + n(2^n) = (n + 1).2^n$.

SAQ3.

$f(x) + g(x) = 2 + 2x^2 + 2x^4 + \dots.$

$f(x).g(x) = 1 + x^2 + x^4 + x^6 + \dots..$

11.7 Summary

The applications of recurrence relations were discussed. The reader will be able to solve the recurrences using the generating function techniques; also it gives the tool for practical problems involving the difference equations, and problems on analytical number theory.

11.8 Technical Terms

Recurrence Relation: The sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely $a_0, a_1, \dots, a_{n-1}$ for all integers n with $n \geq n_0$, where n_0 is a non negative integer.

Linear Recurrence: A recurrence relation of the form $C_0a_r + C_1a_{r-1} + C_2a_{r-2} + \dots + C_ka_{r-k} = f(r)$, where C_i's are constants, with constant coefficients. Here, if both C_0 and C_k are non-zero, then it is known as k^{th} order recurrence relation.

Fibonacci sequence of numbers: The sequence of the form {1, 1, 2, 3, 5, 8, 13, …} is called the Fibonacci sequence. This sequence starts with the two numbers 1, 1 and contains numbers that are equal to the sum of their two immediate predecessors. The recurrence relation can be written as $a_r = a_{r-1} + a_{r-2}$, $r \geq 2$, with $a_0 = 1$ and $a_1 = 1$.

Generating Functions: A polynomial of the form $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots$, which has infinitely many non-zero terms. There is a correspondence between generating functions and sequences. (That is, $a_0 + a_1x + a_2x^2 + \ldots \leftrightarrow a_0, a_1, a_2, \ldots.$).

11.9 Model Questions

1. Solve the recurrence relation $a_n = -3a_{n-1} + n$, $n \geq 1$, where $a_0 = 1$.

2. Solve $a_n = 2a_{n-1} + 3a_{n-2} + 5^n$, $n \geq 2$, given $a_0 = -2$, $a_1 = 1$.

3. Solve the recurrence relation $a_n = 3a_{n-1}$, $n \geq 1$ given $a_0 = 1$.

4. Solve the recurrence $a_n = -3a_{n-1} + 10a_{n-2}$, $n \geq 2$, given $a_0 = 1$, $a_1 = 4$.

5. Solve the recurrence relation $a_n = -a_{n-1} + 2\text{n} - 3$, $n \geq 1$, given $a_0 = 1$.

11.10 References

1. Akerkar Rajendra and Akerkar Rupali. “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, “Discrete Mathematical Structures” PHI, New Delhi, 1999.

3. Liu.C.L., “Elements of Discrete Mathematics”, Mc Hill.

4. Shanker Rao, G., “Discrete Mathematical Structures”, New Age International Publishers, New Delhi, 2002.

5. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

6. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 12

Semigroups and Monoids

Objectives

At the end of the Lessson the student must be able to:

(i) Understand the algebraic systems with one binary operation.
(ii) Generalize the structure of semigroup to a monoid.
(iii)Learn the results on homomorphism and isomorphisms.
(iv)Apply the results to codes in later lessons.

Structure

12.1 Introduction

We begin our study of algebraic structures by investigating sets associated with single operations that satisfy certain reasonable axioms; that is, we wish to define an operation on a set in a way that will generalize such familiar structures as the integers Z together with the single operations of addition, matrix multiplication. We consider some algebraic systems with one binary operation on the set. These systems have useful applications in the theory of finite state machines, coding theory, and sequential mechanics.

12.2 Semigroups

A *binary operation* on a set S where S is non-empty, is a function from $S \times S$ into S. An *n-ary operation* on a set S is a function from $S\times S \times \ldots \times S$ (n times) into S. A *unary operation* is a function from S into S. If f is a binary operation on S, then for any two elements a, b in S the image of (a, b) under f is denoted by afb.

A non empty set together with a number of operations (one or more m-ary) operations defined on the set is called an algebraic system. Generally the binary operations denoted by "*, o, □, +, **.**" etc.

12.2.1 Definition: Let S be a non empty set. Then the operation * on S is said to be associative if $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Consider the following example

(i). Take Z^+ = the set of positive integers. The binary operation '+' (usual) on Z^+ is an associative operation.

(ii). Define * on Z^+ as $a * b = a^2 + b$, where '+' is usual addition.

For any $2, 3, 4 \in Z^+$, $2 * 3 = 2^2 + 3 = 4 + 3 = 7$, $(2 * 3) * 4 = 7 * 4 = 49 + 4 = 53$.

Whereas $2 * (3 * 4) = 17$. Therefore '*' on Z^+ is not associative.

12.2.2 Example: (i). Take Z^+ = the set of positive integers. The binary operation '+' (usual) on Z^+ is an associative operation.

(ii). Define $\square$ on Z^+ as $a \square b = a^2 + b$, where '+' is usual addition.

For any 2, 3, 4 $\in Z^+$, $2 \square 3 = 2^2 + 3 = 4 + 3 = 7$, $(2 \square 3) \square 4 = 7 \square 4 = 49 + 4 = 53$.

Where $2 \square (3 \square 4) = 17$. Therefore '$\square$' on Z^+ is not associative.

12.2.3 Definition: Let (A, *) be an algebraic system where * is a binary operation on A. (A, *) is called a **semigroup** if the following conditions are satisfied:

(i) '*' is a closed operation. That is., $a * b \in A$ for all $a, b \in A$.

(ii) '*' is an associative operation. That is., $a * (b * c) = (a * b) * c$, for all $a, b, c \in A$.

12.2.4 Example: (i). Take $E = \{2, 4, 6, \ldots.\}$. Define '+' on E as usual addition. Then (E, +) is a semigroup.

(ii). Take $A = \{a_1, a_2, \ldots, a_n\}$ be a non empty set. Let A^* be the set of all finite sequences of elements of A. That is, A^* consists of all words that can be formed from the set A. Let α, β be elements of A^*. The operation catenation is a binary operation . on A^***.** For any two strings $\alpha = a_1a_2 \ldots a_n$ and $\beta = b_1\, b_2 \ldots b_k$, then $\alpha.\beta = a_1a_2 \ldots a_n\, b_1\, b_2 \ldots b_k$. It can be verified that for any α, β and ϒ of A^*, $\alpha.(\beta.\Upsilon) = (\alpha.\beta).\Upsilon)$. Therefore $(A^*,.)$ is a semi group.

(iii) Let S be any set and $P(S)$ the power set of S. Then $(P(S), \cup)$ is a semi group, where $\cup$ is the set union.

(iv) The set Z (the set of integers) with the binary operation subtraction is not a semigroup, since subtraction is not associative.

12.2.5 Example: The set ℕ, of natural numbers is a semigroup, under the operation *, where $x * y = \max\{x, y\}$.

Solution: $(x * y) * z = \max\{\max(x, y), z\} = \max\{x, y, z\} = \max\{x, \max(y, z)\} = x * (y * z)$. Therefore * is associative. Thus (ℕ, *) is a semigroup.

12.2.6 Example: Test whether the set $\mathbb{Z}$ (the set of integers), with binary operation * such that $x * y = x^y$ is a semigroup.

Solution: Consider $(2 * 2) * 3 = 2^2 * 3 = 4 * 3 = 4^3 = 64$ and $2 *(2 * 3) = 2 * 2^3 = 2 * 8 = 2^8 = 256$. Therefore $(\mathbb{Z}, *)$ is not a semigroup.

Self Assessment Question 1: Let $A = \{x, y\}$. Whether or not the following tables define a semigroup on A?

*	*x*	*y*
x	*x*	*y*
y	*x*	*x*

Self Assessment Question 2: Whether or not $(\mathbb{Z}^+,*)$ where $a*b = a$ is a semigroup?

Self Assessment Question 3: Let $S = \{a, b\}$. Write the operation table for the functions on semigroup S. Is the semigroup commutative?

Self Assessment Question 4: Let $A = \{a, b, c\}$ and consider the semigroup $(A^*, .)$ where '**.**' is the operation of catenation. If $\alpha = abac$, $\beta = cba$ and $\gamma = babc$, compute

(i). $(\alpha.\beta).\gamma$ (ii). $\gamma.(\alpha.\alpha)$ (iii). $(\gamma.\beta).\alpha$.

12.2.7 Definition: (i). Let $(S, *)$ be a semigroup and let T be a subset of S. If T is closed under the operation * (That is., $a * b \in T$ whenever a and b are elements of T), then $(T, *)$ is called a **subsemigroup** of $(S, *)$.

12.2.8 Definition: Let (S, *) be a semigroup. For $a \in S$, we define $a^1 = a$ and $a^n = a^{n-1}* a, n \geq 2$. For non-negative integers m, n we have $a^m * a^n = a^{m+n}$.

12.2.9 Example: (i) Let (S, *) be a semigroup and T = $\{a^i \mid a \in S \text{ and } i \in Z^+\}$. Then for $a^i, a^j \in$ T, we have $a^i * a^j = a^{i+j} \in$ T (since $a \in S$ and $i + j \in Z^+$). Therefore T is closed with respect to the operation *. Hence (T, *) is a subsemigroup of (S, *).

12.2.10 Definition: Let (S, *) be a semigroup. An element $a \in S$ is called a left-cancelable element if $a*x = a*y \Rightarrow x = y$, for all $x, y \in S$.

12.2.11 Problem: Show that if a and b are left-cancelable elements of a semigroup (S, *), then a*b is also a left cancelable element.

Solution: Take $x, y \in S$.

Now $(a * b)*x = (a * b)* y \Rightarrow a * (b * x) = a * (b * y)$ (by associative property)

$\Rightarrow b * x = b * y$ (since a is left cancelable)

$\Rightarrow x = y$ (since b is left cancelable)

Observation: We can define right cancelable element in a semigroup and the problem is true for right cancelable elements also.

12.3 Homomorphism and Isomorphism

12.3.1 Definition: Let (*S*, *) and (S^1, o) be two semigroups. *A* function *f*: $S \to S^1$ is called an **isomorphism** from (*S*, *) to (S^1, o) if

(i) *f* is one-to-one (that is, one-one and onto)

(ii) $f(a * b) = f(a) \circ f(b)$ for all $a, b \in S$ (homomorphism condition).

A homomorphism of a semigroup into itself is called a semigroup **endomorphism**.

12.3.2 Example: Consider (N, +) and (Z_m, $+_m$). Define g: $N \to Z_m$ by g(a) = [i] where i is the remainder obtained when a is divided by m, for $a \in N$.

For a, b ∈ N, let g(a) = [i] and g(b) = [j]. Then

g(a + b) = [(a + b) (mod m)] = [(i + j) (mod m)] = [i] $+_m$ [j] = g(a) $+_m$ g(b).

Hence g is a homomorphism. Further g(0) = [0]. Hence g preserves the identity.

12.3.3 Result: If f is an isomorphism from $(S, *)$ to (S^1, o), then f^1 is an isomorphism from (S^1, o) to $(S, *)$.

Proof: Let $a^1, b^1 \in S^1$. Since f is onto, there exist $a, b \in S$ such that $f(a) = a^1, f(b) = b^1$. Then

$f^{-1}(a^1 o b^1) = f^1(f(a) o f(b)) = f^1(f(a * b))$ (Since f is homomorphism)

$= (f^1 o f)(a * b)$

$= a * b$

$= f^1(a^1) * f^1(b^1)$.

Therefore f^1 is an isomorphism.

12.3.4 Problem: Show that the semigroups (Z, +) and (E, +) where E is the set of all even integers, are isomorphic.

Solution: Define f: Z→ E by $f(n) = 2n$.

f is one-one: Suppose $f(n_1) = f(n_2) \Rightarrow 2n_1 = 2n_2 \Rightarrow n_1 = n_2$.

f is onto: Suppose $b \in E$. Then b is an even integer. Write $a = \frac{b}{2} \in Z$

Now $f(a) = f\left(\frac{b}{2}\right) = 2\left(\frac{b}{2}\right) = b$. Therefore f is one-one and onto.

f is homomorphism: Let $m, n \in Z$.

$f(m + n) = 2(m + n) = 2m + 2n = f(m) + f(n)$.

Therefore f is a homomorphism and hence (Z, +) and (E, +) are isomorphic.

12.3.5 Definition: An equivalence relation 'R' on the semigroup $(S, *)$ is called a **congruence relation** if $aR\,a^1$ and bRb^1 imply $(a * b)\,R\,(a^1 * b^1)$.

Observation: $a \equiv b \pmod{n} \Rightarrow a = qn + r$ and $b = \text{tn} + r$ for some $q, t, r \in \mathbb{Z} \Rightarrow a - b$ is a multiple of n. That is., $n | a - b$.

12.3.6 Example: Semigroup $(\mathbb{Z}, +)$ and the equivalence relation R on $\mathbb{Z}$ defined by aRb if and only if $a \equiv b \pmod{2}$. If $a \equiv b \pmod{2}$, then $2| a - b$.

Now $a \equiv b \pmod{2}$ and $c \equiv d \pmod{2} \Rightarrow 2| a - b$ ad $2 | c - d$.

$\Rightarrow a - b = 2\text{m},\ c - d = 2\text{n}$, where $m, n \in \mathbb{Z}$

Adding $(a - b) + (c - d) = 2(m + n) \Rightarrow (a + c) - (b + d) = 2(m + n)$.

Therefore $(\text{a} + \text{c}) \equiv (\text{b} + \text{d}) \pmod{2}$.

This shows that the relation is a congruence relation.

12.3.7 Example: Consider the semigroup $(\mathbb{Z}, +)$ where '+' is the ordinary addition. Let $f(x) = \text{x}^2 - x - 2$. Define a relation R on $\mathbb{Z}$ by $a\ R\ b \Leftrightarrow f(a) = f(b)$.

Clearly aRa (reflexive);

$aRb \Leftrightarrow f(a) = f(b) \Leftrightarrow bRa$ (symmetric);

aRb and $bRc \Leftrightarrow f(a) = f(b)$ and $f(b) = f(c)$

$\Leftrightarrow f(a) = f(c) \Leftrightarrow aRc$ (transitive)

Therefore 'R' is an equivalence relation.

To verify R is a congruence relation. But R is not a congruence relation;

$f(-1) = f(2) = 0 \Rightarrow -1R2$; $f(-2) = f(3) = 4 \Rightarrow -2R3$, but $(-1 + (-2))$ is not 'R' related to $(2 + 3)$ since $f(-3) = 10$ and $f(5) = 8$.

12.3.8 Definition: If $(S, *)$ and (T, o) are semigroups, then $(S \times T, \Delta)$ is a semigroup, where Δ defined by $(s_1, t_1)\ \Delta\ (s_2, t_2) = (s_1 * s_2, t_1 \text{ o } t_2)$. This will become a semigroup, called **product semigroup**. If e_S and e_T are the identities of S and T then $(\text{e}_\text{S}, \text{e}_\text{T})$ is the identity element in S × T.

12.3.9 Definition: An equivalence relation R on a semigroup (S, *) is called a **congruence relation** if aRa^1 and bRb^1 imply $(a*b)$ R (a^1*b^1).

12.3.10 Example: Consider the semigroup (Z, +) and the equivalence relation R on Z defined by aRb if and only if $a \equiv b \pmod 2$. That is aRb $\Leftrightarrow$ a-b is divisible by 2. Clearly R is an equivalence relation on Z.

To verify that R congruence relation. Suppose aRb and cRd.

Then $a \equiv b \pmod 2$ and $c \equiv d \pmod 2$ $\Rightarrow$ a-b = 2m and c- d = 2n, where m and n are integers. Adding we get (a-b) + (c-d) = 2m+2n. That is (a + c) – (b +d) = 2(m+n). This means that $(a + c) \equiv (b + d) \pmod 2$.

12.3.11 Note: Let (*S*, *) be a semigroup and *R* is an equivalence relation on *S*. Then *R* determines a partition of *S*. Let $[a] = R(a)$ be the equivalence class containing *a*. Denote $S/R = \{[a] / a \in S\}$.

12.3.12 Theorem: Let *R* be a congruence relation on the semigroup (*S*, *). Consider the relation $\otimes$ from $S/R \times S/R$ to S/R in which the ordered pair ([*a*], [*b*]) is for *a* and *b* in *S*, related to $[a * b]$.

(i). $\otimes$ is a function from $S/R \times S/R$ to S/R.

$$\otimes([a], [b]) = [a] \otimes [b] = [a \otimes b].$$

(ii). $(S/R, \otimes)$ is a semigroup.

Proof: (i). To verify that $\otimes$ is a function: Suppose $([a], [b]) = ([a^1], [b^1])$.

Then aRa^1 and bRb^1. Since *R* is a congruence relation on *S*, we have $a*bRa^1*b^1$

$\Rightarrow [a*b] = [a^1*b^1]$

$\Rightarrow [a] \otimes [b] = [a^1] \otimes [b^1]$.

That is., $\otimes([a], [b]) = \otimes([a^1], [b^1])$.

This shows that $\otimes$ is *a* binary operation on *S*/*R*.

Next we verify that $\otimes$ is associative.

Now $[a] \otimes ([b] \otimes [c]) = [a] \otimes [b*c]$

$= [a*(b*c)] = [(a*b)*c]$ (by associativity of *)

$= [a * b] \otimes [c] = ([a] \otimes [b]) \otimes [c]$.

Therefore ⊗ satisfies associative property. Hence S/R is a semigroup.

12.3.13 Definition: The semigroup S/R verified above is called the **quotient semigroup** or **factor semigroup**.

12.3.14 Example: Take a semigroup (Z, +). Define a relation 'R' on Z a*s* follows: Let n be a positive integer, $aRb \Leftrightarrow a \equiv b \pmod{n}$.

We verify that 'R' is an equivalence relation.

Clearly $a \equiv a \pmod{n}$ and so aRa. Suppose aRb, then $a \equiv b \pmod{n}$

$\Leftrightarrow n|\ a - b$

$\Leftrightarrow n|\ -(a - b)$

$\Leftrightarrow n|\ b - a$

$\Leftrightarrow b \equiv a \pmod{n}$. Therefore $aRb \Rightarrow bRa$.

Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

Then $n|\ a - b$ and $n|\ b - c \Rightarrow n|\ (a - b) + (b - c) \Rightarrow n|\ a - c$.

Therefore $a \equiv c \pmod{n}$.

Therefore aRb, $bRc \Rightarrow aRc$. So R is an equivalence relation.

Take $n = 4$. The equivalence classes determined by the congruence relation ≡ (mod 4) on Z. (It is denoted by Z_4).

$[0] = \{\ldots\ldots -8, -4, 0, 4, 8, 12, \ldots\ldots\} = [4] = [8] = \ldots\ldots\ldots$

$[1] = \{\ldots\ldots -7, -3, 1, 5, 9, 13, \ldots\ldots\} = [5] = [9] = \ldots\ldots\ldots$

$[2] = \{\ldots\ldots -6, -2, 2, 6, 10, 14, \ldots\} = [6] = [10] = \ldots\ldots$

$[3] = \{\ldots\ldots -5, -1, 3, 7, 11, 15, \ldots\} = [7] = [11] = \ldots\ldots\ldots$

Define ⊕ on Z_4 as follows:

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

In general, $[a] \oplus [b] = [a + b]$. Thus Z_n has the 'n' equivalence classes [0], [1], [2], ….,$[n - 1]$ and that $[a] \oplus [b] = [r]$, where r is the remainder when $a + b$ is divided by n. The following theorem establishes a relation between the structure of a semigroup $(S, *)$ and the quotient semigroup $(S/R, \oplus)$, where R is a congruence relation on $(S, *)$.

12.3.15 Theorem: Let R be congruence relation on a semigroup $(S, *)$ and let $(S/R, \otimes)$ be the corresponding quotient semigroup. Then the function f_R: $S \to S/R$ defined by $f_R(a) = [a]$ is an onto homomorphism.

Proof: Take $[a] \in S/R$. Then $f_R(a) = [a]$, so f_R is an onto function. Let $a, b \in S$, then $f_R(a * b) = [a * b] = [a] \otimes [b] = f_R(a) \otimes f_R(b)$. Therefore f_R is a homomorphism.

The proof of the following theorem follows from 12.3.12 and 12.3.15

12.3.16 Fundamental Theorem of homomorphism: Let f: $S \to T$ be a homomorphism of the semigroup $(S, *)$ onto the semigroup (T, o). Let R be the relation on S defined by $a \, R \, b \Leftrightarrow f(a) = f(b)$ for a and b in S. Then (i) R is a congruence relation; (ii). (T, o) and the quotient semigroup $(S/R, \otimes)$ are isomorphic.

12.3.17 Theorem: Let f: S $\to$ T be a homomorphism of the semigroup $(S, \cdot)$ onto the semigroup $(T, *)$. Let R be a relation defined on S by $aRb \Leftrightarrow f(a) = f(b)$ for all $a, b \in S$. Then

(i) R is a congruence relation

(ii) (S/R, Θ) is isomorphic to (T, *)

Proof: (i) Reflexive: Since f(a) = f(a), we have that aRa.

Symmetric: aRb ⇒ f(a) = f(b) ⇒ f(b) = f(a) ⇒ bRa.

Transitive: aRb and bRc ⇒ f(a) = f(b) = f(c) ⇒ aRc.

Therefore R is an equivalence relation.

To verify that R is congruence, let aRa^1 and bRb^1.

This means that $f(a) = f(a^1)$ and $f(b) = f(b^1)$. This implies that $f(a) * f(b) = f(a^1) * f(b^1)$. That is, $f(a{\cdot}b) = f(a^1{\cdot}b^1)$.

Therefore $(a{\cdot}b)R(a^1{\cdot}b^1)$. Hence R is a congruence relation.

(ii) Consider the quotient semigroup (S/R, Θ). Define h: S/R → T as

h([a]) = f(a).

To show h is well defined: Suppose [a] = [b]. Then aRb. This implies that f(a) = f(b).

Take b ∈ T. Since f is onto there exists a ∈ S such that f(a) = b. This means that

h([a]) = f(a) = b.

To show that h is one one, suppose h([a]) = h([b]) ⇒ f(a) = f(b) ⇒ aRb ⇒ [a] = [b].

Also h([a] Θ[b]) = h([a·b]) = f(a·b) = f(a)*f(b). Therefore h is a homomorphism and hence an isomorphism.

12.4 Monoids

12.4.1 Definition: Let $(A, *)$ be an algebraic system where * is a binary operation on A. An element e in A is said to be a left identity (respectively, right identity) if for all $x \in A$, $e * x = x$ (respectively, $x * e = x$) holds.

12.4.2 Example: (i). Define '*' on $A = \{a, b, c, d\}$ as follows:

*	*a*	*b*	*c*	*d*
a	*d*	*a*	*b*	*c*
b	*a*	*b*	*c*	*d*
c	*a*	*b*	*c*	*c*
d	*a*	*b*	*c*	*d*

Here both *b* and *d* are left identities.

(ii). Define 'o' on $A = \{a, b, c, d\}$ as follows:

o	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*a*	*c*	*d*
c	*c*	*d*	*a*	*b*
d	*d*	*d*	*b*	*c*

Here *a* is a right identity.

12.4.3 Definition: An element in an algebraic system is said to be an **identity** if it is both a left identity and a right identity. It can be observed that if *e* is a left identity, then either *e* is also a right identity or there is no right identity at all.

12.4.4 Note: Observe that if *e* is a left identity, then either *e* is also a right identity or there is no right identity at all.

12.4.5 Definition: Let $(M, *)$ be an algebraic system, where * is a binary operation on *A*. $(M, *)$ is called a **monoid** if the following conditions are satisfied:

(i) * is a closed operation

(ii) * is an associative operation

(iii) existance of identity.

Self Assessment Question 5: Let $A = \{x, y\}$. Verify whether or not the following tables define a monoid on A?

$*$	x	y
x	x	y
y	y	y

Self Assessment Question 6: Verify $(\mathbb{Z}^+, *)$ where $a*b = \max\{a, b\}$, a semigroup or monoid?

12.4.6 Theorem: For any binary operation * on a set M if identity element exists then it is unique.

Proof: Suppose e_1, e_2 are two identity elements in M.

Then $e_1 = e_1*e_2$ (since e_2 is an identity)

$= e_2$ (since e_1 is an identity).

Hence the identity element if it exists is unique.

12.4.7 Example: Let X be a non empty set. Write $X^X = \{f\,/\,f: X \to X\}$.

Let 'o' denotes the operation of composition of mappings.

That is., $(fog)(x) = f(g(x))$ for all $f, g \in X^X$ and $x \in X$.

Now 'o' is a binary operation on X^X.

Also $f(x) = x$ for all $x \in X$ is the identity, as $(gof)(x) = g(f(x)) = g(x) = f(g(x)) = (fog)(x)$ for all $g \in X^X$. Therefore (X^X, o) is a monoid.

12.4.8 Problem: Show that the set N of natural numbers is a semigroup under the operation *, where $x * y = \max\{x, y\}$. Is it a moniod ?

Solution: Now

$(x*y)*z = \max\{\max\{x, y\}, z\} = \max\{x, y, z\}$

x*(y*z) = max {x, max{y, z}} = max {x, y, z}. Hence * is associative. Thus (N, *) is a semigroup. Also x*0 = max{x, 0} = max {0, x} = 0*x = x. Therefore (N, *) is a monoid.

12.4.9 Example: (i). For any set S, ($\wp(S)$, ∪) where $\wp(S)$ is a power set of S, is a commutative semigroup. It is also a monoid with the empty set ϕ a*s* the identity element.

(ii) The set ($\mathbb{Z}$, +) is a monoid with identity 0.

(iii) Let (M, *) be a monoid with identity 'e' and let T be a non empty subset of M. If T is closed under the operation '*' and $e \in T$, then (T, *) is called submonoid of (S, *).

Observation: (i). The associative property holds in any subset of a semigroup so that a subsemigroup (T, *) of a semigroup (S, *) is itself a semigroup. (ii). A submonoid of a monoid is itself a monoid.

12.4.10 Example: Let T be the set of even integers. Then (T, **.**) is a subsemigroup of the monoid (Z, **.**) where "**.**" is usual multiplication. But (T, **.**) is not a submonoid, since the identity $1 \notin T$.

12.4.11 Example: (i). Suppose (S, *) is a semigroup, and let $a \in S$. For any $n \in Z^+$, we define the integral powers of a^n recursively a*s* follows:

$a^1 = a$, $a^n = a^{n-1} * a$, $n \geq 2$. Write $T = \{a^n / n \in \mathbb{Z}^+\}$.

Then (T, *) is a subsemigroup of (S, *).

(ii). Let (S, *) be a monoid and $a \in S$.

Define $a^0 = e$, $a^1 = a$, $a^n = a^{n-1} * a$, $n \geq 2$ (a*s* in (i))

Write $T^1 = \{a^n / n \in Z^+, \cup \{0\}\}$. Then ($T^1$, *) is a submonoid of ($S$, *).

12.4.12 Definition: Let (M, *) be a monoid. An element $a \in M$ is called an **idempotent** element if $a^2 = a$.

12.4.13 Theorem: For any commutative monoid (M, *), show that the set of idempotent elements of M forms a sub-monoid.

Proof: Let (M, *) be any commutative monoid with identity e.

Write $T = \{x \mid x$ is an idempotent elements of M $\}$. Now e * e = e and so $e \in T$. Therefore T is non-empty.

Take $x, y \in T$.

Now (x * y) * (x * y) = (x * y) * (y * x) (since M is commutative)

= x * (y * y) * x (since M is associative)

= x * (y * x) (since $y \in T$ is an idempotent)

= x * (x * y) (since M is commutative)

= (x * x) * y (since M is associative)

= x * y (since $x \in T$ is an idempotent).

Therefore $x * y \in T$. Hence (T, *) is a sub-monoid of (M, *).

12.4.14 Theorem: Let (S, ·) and (T, *) be two monoids with identities e and e^1 respectively and f: S → T be an isomorphism. Then $f(e) = e^1$.

Proof: Let $b \in T$. Since f is onto, there exists $a \in S$ such that f(a) = b.

Now b = f(a) = f(a · e) = f(a) * f(e) = b * f(e).

Similarly, b = f(e) * b. Hence f(e) is an identity in T. Since identity is unique, we have $f(e) = e^1$.

12.5 Answers to Self Assessment Questions

SAQ 1.

Semigroup.

SAQ 2.

Yes

SAQ 3.

Let $f_1(a) = a, f_1(b) = a, f_2(a) = a, f_2(b) = b, f_3(a) = b, f_3(b) = a, f_4(a) = b, f_4(b) = b$. These are the only functions on S. It is not commutative.

o	f_1	f_2	f_3	f_4
f_1	f_1	f_1	f_4	f_4
f_2	f_1	f_2	f_3	f_4
f_3	f_1	f_3	f_2	f_1
f_4	f_1	f_4	f_4	f_4

SAQ 4.

(i). *abaccbababc,* (ii). *babcabacabac,* (iii). *babccbaabac*

SAQ 5.

Monoid.

SAQ 6.

Monoid: (identity exists).

12.6 Summary

The algebraic structures with one binary operation were discussed. Some important characterizations of the algebraic systems Semigroups and Monoid were given. The homomorphism between two semigroups (and monoids) were discussed and we established the fundamental theorem. The algebraic structures semigroups and monoids have many application in the finite automata and to perform efficient codes.

12.7 Technical Terms

Associative Operation: $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Semigroup: Closed and associative operation.

Subsemigroup: $(T, *)$ is a *subsemigroup* of $(S, *)$ if T is closed under the operation * (That is., $a * b \in T$ whenever a and b are elements of T).

Semigroup Isomorphism: A function f: $S \rightarrow S^1$ is called an *isomorphism* from $(S, *)$ to (S^1, o) if (i) f is one-to-one (that is, one-one and onto), (ii) $f(a * b) = f(a)$ o $f(b)$ for all $a, b \in S$ (homomorphism condition).

Congruence Relation: An equivalence relation 'R' on the semigroup $(S, *)$ with $aR\, a^1$ and bRb^1 imply $(a * b)\, R\, (a^1 * b^1)$.

Left (right) identity: An element x in A where $(A, *)$ is an algebraic system, is a left identity (respectively, right identity) if for all $x \in A$, $e * x = x$ (respectively, $x * e = x$) for all x.

Monoid: Algebraic system which is closed, associative, and existance of identity with respect to the defined operation.

Idempotent element: An element a in a monoid satisfies the condition: $a^2 = a$.

12.8 Model Questions

1. Define the terms semigroup and monoid. Give one example of each.

2. Let S = {a, b}. Write the operation tables for (P(S), $\cup$) and (P(S), $\cap$). Verify these are semigroups.

3. Prove that the intersection of two subsemigroups of a semigroup is also a subsemigroup of it.

4. Prove that the intersection of two submonoids of a monoid (S, *) is a submonoid of (S, *).

5. Prove that for any commutative monoid (M, *), show that the set of idempotent elements of M forms a sub-monoid.

6. State and prove fundamental theorem of homomorphism of semigroups.

7. Define an isomorphism between two semigroups. Prove that the semigroups (Z, +) and (*E*, +) where *E* is the set of all even integers, are isomorphic.

8. Consider the semigroup (Z, +). Let R be the relation on Z such that aRb ⇔ a+b is even. Prove that R is a congruence relation on.

12.9 References

1. Akerkar Rajendra and Akerkar Rupali. “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Fraleigh J.B. “A First Course in Abstract Algebra”, Narosa Publ. House, New Delhi, 1992

3. Hari Kishan and Shivraj Pundir “Discrete Mathematics”, Pragati Prakashan, Meerut, 2005.

4. Herstein I. N. “Topics in Algebra”, Blaisdell, New York, 1964.

5. Satyanarayana Bhavanari, Syam Prasad Kuncham, Pradeep Kumar T. V., Srinivasa Rao M “Algebra for Beginners”, Bhavanari Ramakotaiah & Co., Madugula, Guntur (Dt), AP, (0863 – 2232138) 1991.

6. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

7. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 13

Group Theory

Objectives

At the end of the Lesson the student must be able to:

(i) Understand the algebraic systems with one binary operation.
(ii) Generalize the structure of semigroup to a monoid.
(iii)Know the axioms of a group and its substructures.
(iv)Learn the normal subgroups properties.
(v) Get the idea of fundamental theorem of homomorphism.

Structure

13.1 Introduction

We begin our study of algebraic structures by investigating sets associated with single operations that satisfy certain reasonable axioms; that is, we wish to define an operation on a set in a way that will generalize such familiar structures as the integers Z together with the single operations of addition, matrix multiplication. We study the important algebraic object known as group which serve as one of the fundamental building blocks for the abstract algebra. In fact group theory has several applications in every area where symmetry occurs. Applications of groups also can be found in physics, chemistry. Some of exciting applications of group theory have arisen in fields such as particle physics, and binary codes.

13.2 Groups

13.2.1 Definition: We recollect that for *a* non empty set *G*, *a* **binary operation** on *G* is mapping from $G \times G$ to *G*. In general, binary operations are denoted by *, **.** , o etc.

13.2.2 Definition: *A* non empty set *G* together with a binary operation * is called a **group** if the algebraic system (*G*, *) satisfies the following four axioms:

(i) Closure: *a*, *b* are elements of *G*, implies *a*b* is an element of *G*.

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

(iii) Identity: there exists an element 'e' in *G* such that *a*e* = *e*a* = *a* for all $a \in G$.

(iv) Inverse: For any element *a* in *G* there corresponds an element *b* in *G* such that *a*b* = *e* = *b*a*.

13.2.3 Note: The element *e* of *G* (given in identity axiom) is called an *identity element*. The element *b* (given in the inverse axiom) is called an *inverse of a* in *G*.

13.2.4 Definition: Let (*G*, *) be a group. Then (*G*, *) is said to be a **commutative group** (or **Abelian group**) if it satisfies the commutative property: *a*b* = *b*a* for all *a*, *b* in *G*.

13.2.5 Example: Take G = {-1, 1}. Then (G, **.**) is a commutative group *w. r. t.* the usual multiplication of numbers.

•	-1	+1
-1	1	-1
1	-1	1

Closure: Clearly, $a.b$ is in G for all a, b in G.

Associative: Since 1, -1 are real numbers, this axiom holds.

Identity axiom: 1**.** $a = a = a$**.**1 for all elements $a \in G$.

Hence 1 is the identity element.

Inverse: The element 1 is the inverse of 1 and -1 is the inverse of -1

Commutative: (-1).1 = 1. (-1). Therefore commutative law holds in (G, **.**).

Hence (G, **.**) is a commutative group.

13.2.6 Example: (i) (Z, +) where Z is the set of all integers is an abelian group. 0 is the identity element and –a is the inverse of a.

(ii) The set of all n×n matrices under matrix addition is an abelian group with **0** matrix (null matrix) as the identity element and –A is the inverse of A.

(iii) (N, +) where N is the set of natural numbers, is not a group. Since no element has an inverse in N with respect to addition.

(for example, 3 ∈ N but the additive inverse of 3 = -3 ∉ N).

(iv) The set of all non-singular n×n matrices forms a group under matrix multiplication with I_n, the identity matrix of order n, as the identity element and A^{-1} as the inverse of the matrix A. Since for any two matrices A and B we have AB ≠ BA, we can conclude that this is not an abelian group.

Self Assessment Question 1: Let S = {0, 1}. Define the operation + on S as follows:

0+0 = 0, 0+1 = 1, 1+0 = 1 and 1+1 = 0. Verify that (S, +) is a group. What is the identity element and write the inverses of each element in S.

13.2.7 Problem: Let Z_m be the set of all equivalence classes for the relation congruent modulo m and $+_m$ is the modulo m addition. Take m = 5 and verify that (Z_5, $+_5$) is an abelian group.

Solution: We give the table of values with respect to the operation $+_5$ on Z_5.

Clearly Z_5 = {[0], [1], [2], [3], [4]}.

$+_5$	[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]

From the table we can conclude that (Z_5, $+_5$) is an abelian group.

Self Assessment Question 2: Define the operation * on the set of all integers as follows: a * b = a + b – ab. Verify whether (Z, *) forms a group.

13.2.8 Problem: Let p be a prime number. Consider the set (Z_p-{[0]}, $\times_p$) where $\times_p$ is multiplication modulo p. Verify that for p =5, Z_5 forms a commutative group with respect to multiplication modulo 5. Write the inverses of each element.

Solution: The multiplication table for (Z_5-{[0]}, $\times_5$) is given below.

Clearly Z_5 -{[0]} = {[1], [2], [3], [4]}.

$\times_5$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

From the table, the identity element is [1]; the inverse of [2] is [3], the inverse of [3] is [2], the inverse of [4] is [4].

Self Assessment Question 3: Give an example of abelian group o*f* 2 × 2 matrices over relas with respect to Multiplication.

13.2.9 Theorem: Given a, b in a group G. Then (i) The equations a.x = b and y.a = b have unique solutions for x and y in G.

(ii) The cancellation laws: a.u = a.w ⇒ u = w; and u.a = w.a ⇒ u = w for all u, w in G hold.

Proof: (i) Let a, b in G.

Since G is a group, we have a^{-1} is in $G \Rightarrow a^{-1}.b$, $b.a^{-1}$ are in G (by closure property). Write $x = a^{-1}.b$ and $y = b.a^{-1}$.

Consider $a.x = a.(a^{-1}.b) = (a.a^{-1}).b = e.b = b$. Similarly $y.a = b$.

Therefore $x = a^{-1}.b$ and $y = b.a^{-1}$ are required solutions.

Next we show that these solutions are unique.

Suppose x_1, x_2 are two solutions of $a.x = b$.

Then $a.x_1 = b$ and $a.x_2 = b$. So $a.x_1 = b = a.x_2$.

Now $x_1 = e.x_1 = (a^{-1}.a)x_1 = a^{-1}.(a.x_1) = a^{-1}.(a.x_2) = (a^{-1}.a).x_2 = e.x_2 = x_2$.Therefore $x_1 = x_2$. Hence $a.x = b$ has unique solution. Similarly we show that $y.a = b$ has unique solution.

(ii) Now we will prove that the cancellation laws holds good in G.

Suppose $a.u = a.w$. Consider u.

Now $u = e.u = (a^{-1}.a).u = a^{-1}.(a.u) = a^{-1}.(a.w) = (a^{-1}.a).w = e.w = w$.

Now suppose $u.a = w.a$. Consider u.

Now $u = u.e = u.(a.a^{-1}) = (u.a).a^{-1} = (w.a).a^{-1} = w.(a.a^{-1}) = w.e = w$.

Hence both the left and right cancellation laws hold in G.

13.2.10 Result: Let G be a non-empty set and '**.**' be a binary operation on G which is associative. If for all a ∈ G there exists e ∈ G such that e.a = a and for all a ∈ G, there exists b ∈ G such that b.a = e then (i) a.m = a.n ⇒ m = n (ii) for all a ∈ G, a.e = a (e is right identity) (iii) for all a ∈ G there exists b ∈ G such that a.b = e.

Proof: (i) Suppose $a.m = a.n$. Consider $m = e.m$ $(b.a)m = b(a\ m) = b(a\ n) = (ba)n =$ en $= n$. Therefore $m = n$

(ii) Given that $e.a = a$ for all $a \in G$. Now $e.e = e \Rightarrow (ba).e = ba$ (since $ba = e$) $\Rightarrow b$(ae) $= ba \Rightarrow$ ae $= a$ (by (i)).

(iii) Let $a \in G$. By our assumption $ba = e$. Consider $b(ab) = (ba)b =$ eb $= b =$ be (by (ii)) $\Rightarrow$ $b(ab) =$ be $\Rightarrow ab = e$.

This completes the proof.

13.2.11 Theorem: If G is a group, then

(i) The identity element of G is unique.

(ii) Every element in G has unique inverse in G.

(iii) For any a in G, we have $(a^{-1})^{-1} = a$.

(iv) For all a, b in G, we have $(a.b)^{-1} = b^{-1}.a^{-1}$.

Proof: (i) Let e, f be two identity elements in G. Since e is the identity we have $e.f = f$. Since f is the identity we have $e.f = e$. Therefore $e = e.f = f$. Hence the identity element is unique.

(ii) Let a be in G and a_1, a_2 are two inverses of a in G.

Now $a_1 = a_1.e$ (since e is the identity)

$= a_1.(a.a_2)$ (since a_2 is the inverse of a)

$= (a_1.a).a_2$ (by associativity)

$= e.a_2$ (since a_1 is the inverse of a)

$= a_2$.

Hence the inverse of an element in G is unique.

(iii) Let $a \in G$. Since $a.a^{-1} = e = a^{-1}.a$, we have that a is the inverse of a^{-1}.

Hence $(a^{-1})^{-1} = a$.

(iv) Let $a, b \in G$. Consider $(b^{-1}.a^{-1})(a.b) = b^{-1}.(a^{-1}.a).b = b^{-1}.e.\ b = b^{-1}.b = e$.

Similarly e $= (a.b).(b^{-1}.a^{-1})$. This shows that $(a.b)^{-1} = b^{-1}.a^{-1}$.

13.2.12 Definition: Let (G, o) be a group. *A* non-empty subset H of G is said to be a **subgroup** of G if H itself forms a group under the product in G.

13.2.13 Theorem: A non-empty subset H of a group G is a subgroup of G if and only if (i) a, b $\in$ H $\Rightarrow$ ab $\in$ H and (ii) a $\in$ H $\Rightarrow$ $a^{-1} \in$ H.

Proof: Suppose that H is *a* subgroup of G

$\Rightarrow$ H itself is a group under the product in G. Therefore (i), (ii) holds.

Converse: Suppose H satisfies (i) and (ii). By (i), H satisfies the closure property.

For any $a, b, c \in H$, we have that $a, b, c \in G$ implies that $a(bc) = (ab)c$.

Therefore (H, **.**) is a subgroup of (G, **.**).

13.2.14 Problem: If H is a non-empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.

Proof: Suppose H is a non-empty finite subset of a group G and H is closed under multiplication. Now we have to show that H is a subgroup of G.

It is enough to show that $a \in H \Rightarrow a^{-1} \in H$

Since H is a non-empty, there exists $a \in H$. Now $a, a \in H \Rightarrow a^2 \in H$.

Similarly $a^3 \in H, \ldots, a^m \in H, \ldots$.

Therefore $H \supseteq \{a, a^2, \ldots\}$. Since H is finite, we have that there must be repetitions in $a, a^2, \ldots$.

Therefore there exists integers r, s with $r > s > 0$ such that $a^r = a^s$

$\Rightarrow a^r . a^{-s} = a^0$

$\Rightarrow a^{r-s} = e \Rightarrow e \in H$ (since r-s > 0 and $a \in H \Rightarrow a^{r-s} \in H$).

Since r-s-1 $\geq$ 0, we have $a^{r-s-1} \in H$ and $a.\ a^{r-s-1} = a^{r-s} = e \in H$.

Hence a^{r-s-1} acts as the inverse of a in H. Hence H is a subgroup.

13.2.15 Example: (i) The set of even integers with respect to addition (E, +) is a subgroup of the group (Z, +).

(ii) If k is a positive integer then (kZ, +) is a subgroup of (Z, +).

13.2.16 Example: Consider G = Z, the group of integers with respect to addition. Write $H = \{5x / x \in G\}$. Suppose $a, b \in H \Rightarrow a = 5x$, $b = 5y$ for some $x, y \in G$

$\Rightarrow a + b = 5x + 5y = 5(x + y) \in H$. Also $-a = -5x = 5(-x) \in H$.

Therefore H is a subgroup of G.

13.2.17 Example: Let (G, ·) be a group. Let $H = \{x \mid x \in G \text{ and } x \cdot y = y \cdot x \text{ for all } y \in G\}$. Prove that H is a subgroup of G.

Solution: Since $e \cdot y = y \cdot e$ for all $y \in G$, we have $e \in H$.

Take $x_1, x_2 \in H$. Then $x_1 \cdot y = y \cdot x_1$ and $x_2 \cdot y = y \cdot x_2$ for all $y \in G$.

$$\begin{aligned} \text{Now } (x_1 \cdot x_2) \cdot y &= x_1 \cdot (x_2 \cdot y) \\ &= x_1 \cdot (y \cdot x_2) \\ &= (x_1 \cdot y) \cdot x_2 \\ &= (y \cdot x_1) \cdot x_2 \\ &= y \cdot (x_1 \cdot x_2). \end{aligned}$$

Therefore $x_1 \cdot x_2 \in H$.

Take $x \in H$. Now $x \cdot y = y \cdot x$ for all $y \in G$.

Now $x^{-1} \cdot y = (y^{-1} \cdot x)^{-1} = (x \cdot y^{-1})^{-1}$ (since $x \in H \Rightarrow x \cdot y^{-1} = y^{-1} \cdot x$) $= y \cdot x^{-1}$ for any $y \in G$.

This shows that $x^{-1} \in H$. Hence (H, ·) is a subgroup of (G, ·).

13.2.18 Theorem: Let (G, *) be a group. He be any non-empty subset of G. Then H is a subgroup of G if and only if $a * b^{-1} \in H$ whenever $a, b \in H$.

13.2.19 Definition: Let G be a group. If G contains only a finite number of elements then G is called a **finite group**. If G contains infinite number of elements then G is called an **infinite group**. If G is a finite group then the *Order of G* is the number of elements in G. If G is infinite group, then we say that order of G is infinite. The Order of G is denoted by O(G). If G is a group and $a \in G$, then the **order** of 'a' is defined as the least positive integer m such that $a^m = e$. If there is no positive integer n such that $a^n = e$ then 'a' is said to be of **infinite order**.

13.2.20 Example: (i) Let G be the set of all integers and + be the usual addition of numbers. Then $(G, +)$ is an Abelian group. Here '0' is the additive identity and $-x$ is the additive inverse of x, for any x in G. This $(G, +)$ is an infinite group and so O(G) is infinite.

(ii) Consider Q, the set of rational numbers, and R the set of all real numbers. Clearly these two are infinite Abelian groups *w. r. t.* usual addition.

(iii) From the above, it is clear that the set G consisting of -1 and 1 is a group *w. r. t.* usual multiplication. This group is a finite group and O(G) = 2.

13.2.21 Problem: Let G be a group, $a \in G$. Then $(a) = \{a^i / i = 0, \pm 1, \ldots\}$ is a subgroup of G.

Solution: Let $x, y \in (a) \Rightarrow x = a^i$ and $y = a^j$ for some $i, j \in Z$. Now $x. y = a^i. a^j = a^{i+j} \in (a)$ (since $i + j \in Z$).

Also $x^{-1} = (a^i)^{-1} = a^{-i} \in (a)$ (since $a^i. a^{-i} = a^{i-i} = a^0 = e \Rightarrow (a^i)^{-1} = a^{-i}$).

Therefore $x, y \in (a) \Rightarrow x. y \in (a)$ and $x^{-1} \in (a)$. Hence (a) is a subgroup of G.

13.2.22 Definition: (i) Let G be a group and $a \in G$. Then $(a) = \{a^i / i = 0, \pm 1, \ldots\}$ is called the **cyclic subgroup** generated by the element $a \in G$. In other words, G is said to be a **cyclic group** if there exists an element $a \in G$ such that $G = (a)$.

13.2.23 Examples: (i) The set of integers with respect to addition, (Z, +), is a cyclic group with generator 1.

(ii) The multiplicative group, the cube roots of unity, $\{1, \omega, \omega^2\}$ is a cyclic group with generators ω and ω^2.

(**Verification**: $\omega^0 = 1, \omega^1 = \omega, \omega^2 = \omega^2, \omega^3 = 1$ and $(\omega^2)^0 = 1, (\omega^2)^{\ 1} = \omega^2, (\omega^2)^2 = \omega^4 = \omega$).

Self Assessment Question 4: Write, if cyclic, the generators of the group {1, -1, i, -i} with respect to multiplication.

13.2.24 Theorem: Every cyclic group is abelian.

Proof: Let G be a cyclic group and let a be a generator of G.

Now G = (a) = $\{a^n \mid n \in Z\}$. Take $g_1, g_2 \in G$. Then there exists integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Therefore $g_1 \cdot g_2 = a^r \cdot a^s = a^{r+s} = a^{s+r} = a^s \cdot a^r = g_2 \cdot g_1$. Hence G is abelian.

13.2.25 Note: If a cyclic group G is generated by an element a of order n, then a^m is a generator of G if and only if the greatest common divisor of m and n is 1.

13.2.26 Example: Consider the cyclic group of order 8, generated by a. That is, $\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$. Since gcd (7, 8) = 1, we have a^7 is the generator; since gcd (5, 8) = 1, we have a^5 is the generator; since gcd (3, 8) = 1, we have a^3 is the generator. Therefore the set of generators are $\{a, a^3, a^5, a^7\}$.

13.2.27 Note: Let Z be the integers and let $n > 1$ be a fixed integer. By an example 2.25 of equivalence relation, where we defined $a \equiv b \pmod{n}$ (a is congruent to b mod n) if $n \mid (a - b)$. The class of a, $[a]$, consists of all a + nk, where k runs through all the integers. We call it the **congruence class** of a.

13.2.28 Theorem: Z_n forms a cyclic group under the addition $[a] + [b] = [a + b]$.

Proof: Consider $Z_n = \{[0], [1], ..., [n - 1]\}$. We define the operation + in Z_n as $[a] + [b] = [a + b]$. Suppose that $[a] = [a^1]$ then $n \mid (a - a^1)$. Also from $[b] = [b^1]$, $n \mid (b - b^1)$. Hence $n|((a - a^1) + (b - b^1)) \Rightarrow n \mid ((a + b) - (a^1 + b^1))$. Therefore $(a + b) \equiv (a^1 + b^1) \pmod{n}$. Therefore $[a + b] = [a^1 + b^1]$. Hence + is well defined in Z_n.

The element [0] acts as the identity element and [-*a*] acts as –[*a*], the inverse of [*a*].It can be verified that Z_n is a group under +. Also it is a cyclic group of order *n* generated by [1].

13.3 Cosets and Lagranges Theorem

13.3.1 Notation: If ~ is an equivalence relation on *S*, then [*a*], **the class of a**, is defined by [*a*] = $\{b \in S / b \sim a\}$.

13.3.2 Definition: Let *G* be a group, *H* be a subgroup of *G*, *a*, *b* ∈ *G*. We say that **a is congruent to b** (mod *H*), written as $a \equiv b$ (mod *H*) if $a\,b^{-1} \in H$.

13.3.3 Theorem: The relation a ≡ b (mod H) is an equivalence relation.

Proof: (i) Reflexive: Since *H* is *a* subgroup of *G*, we have that $aa^{-1} = e \in H$ for $a \in G \Rightarrow a \equiv a$ (mod *H*).

(ii) Symmetric: Suppose $a \equiv b$ (mod *H*) $\Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H$ (since *H* is *a* subgroup of *G*) $\Rightarrow (b^{-1})^{-1}\, a^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow b \equiv a$ (mod *H*).

(iii) Transitive: Suppose $a \equiv b$(mod *H*), $b \equiv c$ (mod *H*) $\Rightarrow ab^{-1} \in H$, $bc^{-1} \in H$

$\Rightarrow (ab^{-1})\,(bc^{-1}) \in H$ (since *H* is *a* subgroup of *G*)$\Rightarrow a(b^{-1}\mathrm{b})c^{-1} \in H \Rightarrow aec^{-1} \in H \Rightarrow ac^{-1} \in H \Rightarrow a \equiv c$ (mod *H*).

Therefore the relation $a \equiv b$ (mod *H*) satisfies (i) reflexive, (ii) symmetric, (iii) transitive properties. Thus the relation is an equivalence relation.

13.3.4 Definition: If *H* is a subgroup of *G* and $a \in G$, then write $Ha = \{ha / h \in H\}$ is called the **right coset** of *H* in *G*. aH = {ah / *h* ∈ *H*} is called the **left coset** (or **the left coset of H determined by H**).

13.3.5 Note: (i) We denote the set of left cosets of H in G by G/H is the quotient set with respect to the equivalence relation ≡ (mod H).

It clear that if H is a normal subgroup, then the coset relation is a congruence relation.

Verification: Let a ≡ p (mod H) and b ≡ q (mod H). Then by definition, $p^{-1}a \in H$ and $q^{-1}b \in H$. Let $p^{-1}a = h_1$ and $q^{-1}b = h_2$ for some $h_1, h_2 \in H$.

Now $(pq)^{-1}(ab) = (q^{-1}p^{-1})(ab) = q^{-1}(p^{-1}a)\,b = q^{-1}(h_1\,b) = q^{-1}(b\,h_3)$ (since bH = Hb)

$= (q^{-1}b)h_3 = h_2h_3 \in H$. Therefore (ab) ≡ (pq) (mod H). Thus ≡ (mod H) is a congruent relation on G.

(ii) Consider the quotient set G/H. Define the operations on G/H as aH*bH = (ab)H. Then (G/H, *) is a group. We call this as the quotient group.

13.3.6 Example: Consider the group (Z_4, $+_4$) given in the following table.

Clearly Z_4 = {[0], [1], [2], [3]}.

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Then H = {[0], [2]} is a subgroup of G. Now we will list the left cosets determined by the elements of Z_5 as follows.

Left coset determined by [0] is {[0], [2]}.

Left coset determined by [1] is {[1], [3]}.

Left coset determined by [2] is {[0], [2]}.

Left coset determined by [3] is {[1], [3]}.

These are the only two distinct left cosets of H in G.

Observation: (i) If a ∈ H, then aH = H.

(ii) Right coset can be defined in the same manner.

Self Assessment Question 5: Write the left cosets of H = {0, 3} in the group Z_6.

13.3.7 Lemma: For all a ∈ G, Ha = {x ∈ G / a ≡ x (mod H)} = [a].

Proof: Consider $[a] = \{x \in G \,/\, a \equiv x \text{ (mod } H)\}$, the equivalence class under the equivalence relation defined as $a \equiv b$ (mod H) if $a\, b^{-1} \in H.$ Let $x \in$ Ha $\Rightarrow x =$ ha for some $h \in H$. Since $h \in H$ we have that $a\, x^{-1} = a(\text{ha})^{-1} = a\, a^{-1}\, h^{-1} = e\, h^{-1} = h^{-1} \in H \Rightarrow a\, x^{-1} \in H \Rightarrow a \equiv x$ (mod H) $\Rightarrow$ $x \in [a]$.

Converse: Suppose $x \in [a] \Rightarrow a \equiv x$ (mod H) $\Rightarrow a\, x^{-1} \in H \Rightarrow (a\, x^{-1})^{-1} \in H \Rightarrow x\, a^{-1} \in H \Rightarrow x\, a^{-1} = h$ for some $h \in H \Rightarrow x =$ ha ∈ Ha. Therefore $[a] =$ Ha

13.3.8 Problem: There is a one-to-one correspondence between any two right cosets of H in G.

Proof: Let H be a subgroup of G and Ha, Hb be two right cosets of H in G (for some $a, b \in G$).

Define ϕ: $Ha \rightarrow Hb$ by $\phi(ha) = hb$ for all $ha \in Ha.$

ϕ is one-one: Let $h_1a, h_2a \in Ha$ such that $\phi(h_1a) = \phi(h_2a)$

$\Rightarrow h_1b = h_2b$

$\Rightarrow h_1 = h_2$ (by cancellation Law)

$\Rightarrow h_1a = h_2a.$

Therefore ϕ is one-one.

ϕ is onto: Let $hb \in Hb \Rightarrow h \in H$. Now $ha \in Ha$ and $\phi(ha) = hb$. Therefore ϕ is onto.

13.3.9 Note: Since $H = He$ we have that H is also a right coset of H in G and by the Problem 13.3.7, any right coset of H in G have $O(H)$ elements.

13.3.10 Theorem (Lagranges): If G is a finite group and H is a sub group of G, then O(H) is a divisor of O(G).

Proof: Let G be a finite group and H is a subgroup of G with $O(G) = n$, $O(H) = m$, (since G is finite, H is also finite).

We know that any two right cosets are either disjoint or identical.

Now suppose $Ha_1, Ha_2, \ldots, Ha_k$ are only distinct right coset of H in G

$\Rightarrow G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_k$

$\Rightarrow O(G) = O(Ha_1) + O(Ha_2) + \ldots + O(Ha_k)$

$= O(H) + O(H) + \ldots + O(H)$ (k times) (since every right coset has $O(H)$ elements)

$\Rightarrow O(G) = k.\ O(H)$

$\Rightarrow n = k.m \Rightarrow (n/m) = k.$

Hence $O(H)$ divides $O(G)$.

Observation: Converse of the Lagranges theorem is not true: that is, "If G is a finite group and $k \mid O(G)$ then there exists a subgroup H of G such that $O(H) = k$" is not true.

13.3.11 Example: Consider the symmetric group S_4. We know that $S_4 = \{f : A \to A \,/\, f$ is a bijection and $A = \{1, 2, 3, 4\}\}$. Clearly $|S_4| = 24$ (= 4!). Now A_4 = the set of all even permutations in S_4. Then $|A_4| = 12$. It can be verified that any six elements of A_4 can not form a subgroup. Therefore $6 \mid O(A_4)$ but A_4 contains no subgroup of order 6. (refer the section: Permutation Groups).

13.3.12 Definitions: (i) If H is a subgroup of G, then the **index** of H in G is the number of distinct right cosets of H in G. It is denoted by $i(H)$ or we denote as $\lambda = |G| / |H|$.

13.3.13 Example: In the example $(Z_4, +_4)$, $H = \{[0], [2]\}$ is a subgroup. Z_4 partitioned into two left cosets $\{[0], [2]\}$ and $\{[1], [3]\}$. Then $|G| = 4$ and $|H| = 2$ and so the index of H in G is $\lambda = 2$.

13.3.14 Lemma: If G is a finite group and a $\in$ G, then O(a) | O(G).

Proof: Suppose G is a finite group and $a \in G$ and $O(G) = n$, $O(a) = m$.

Let $H = \{a, a^2, \ldots a^m = e\}$. Clearly H is a subgroup of G.

Now we have to show that $O(H) = m$.

Suppose $O(H) < m \Rightarrow a^i = a^j$ for some $0 \leq i, j \leq m \Rightarrow a^i. a^{-j} = a^j. a^{-j}$ (if $j < i$) $\Rightarrow a^{i-j} = a^0 = e$ where $0 < i - j < m$, which is a contradiction (since m is the least positive integer such that $a^m = e$).

Therefore $O(H) = m = O(a)$.

Now by Lagranges theorem we have that $O(H) \mid O(G) \Rightarrow O(a) \mid O(G)$.

13.3.15 Corollary: If G is a finite group and a $\in$ G, then $a^{O(G)} = e$.

Proof: By the above Corollary 2.40, we have that $O(a) \mid O(G)$

$\Rightarrow$ there exists m such that $O(G) = m..O(a)$. Now $a^{O(G)} = a^{m.O(a)} = [a^{O(a)}]^m = e^m = e$.

13.4 Normal Subgroups and Homomorphisms

13.4.1 Definition: *A* subgroup N of G is said to be a **normal subgroup** of G if for every $g \in G$ and $n \in N$ such that $gng^{-1} \in N$. It is clear that a subgroup N is a normal subgroup of G if and only if $gNg^{-1} \subseteq N$ for all $g \in G$.

13.4.2 Definition: (i) *A* mapping $\phi: G \rightarrow G^1$ where G, G^1 are groups, is said to be a **homomorphism** if for all $a, b \in G$ we have that $\phi(ab) = \phi(a). \phi(b)$.

(ii) If ϕ is a homomorphism of G into G^1, then the **kernal of** ϕ (denoted by ker ϕ) is defined by ker $\phi = \{x \in G / \phi(x) = e^1$, where e^1 is the identity in $G^1\}$. Further if ϕ is one one and onto then we call it as an isomorphism.

Self Assessment Question 6: Let G be a group of real numbers under addition and let G^1 be the group of non-zero real numbers with the ordinary multiplication. Define ϕ: $G \to G^1$ by $\phi(a) = 2^a$. Verify ϕ is a homomorphism.

Self Assessment Question 7: Define f: $(R, +) \to (R^+, \cdot)$ by $f(x) = e^x$. Verify that f is an isomorphism.

13.4.4 Problem: If ϕ is a homomorphism of G into G^1, then
(i) $\phi(e) = e^1$ where e^1 is the identity element of G^1. (ii) $\phi(x^{-1}) = [\phi(x)]^{-1}$ for all x in G.

Proof: (i) Let $x \in G \Rightarrow \phi(x) \in G^1$.
Now $\phi(x) = \phi(x).e^1$ and $\phi(x) = \phi(xe) = \phi(x).\ \phi(e)$ (since ϕ is homo.).
Therefore $\phi(x).\ e^1 = \phi(x).\ \phi(e)$
$\Rightarrow e^1 = \phi(e)$ (by cancellation laws).
(ii) By (i), $e^1 = \phi(e) = \phi(xx^{-1}) = \phi(x).\ \phi(x^{-1})$
$\Rightarrow \phi(x^{-1})$ is the inverse of $\phi(x)$.
That is $\phi(x^{-1}) = [\phi(x)]^{-1}$. This is true for all $x \in G$.

13.4.5 Problem: If ϕ is a homomorphism of G into G^1 with kernal K, then K is a normal subgroup of G.

Proof: First we show that $K \neq \phi$. Since $\phi(e) = e^1$ where e^1 is the identity in G^1, we have that $e \in \ker \phi = K$. Therefore $K \neq \phi$. Now we show that K is closed under multiplication and every element in K has inverse in K.
Let $x, y \in K \Rightarrow \phi(x) = e^1$ and $\phi(y) = e^1$
$\Rightarrow \phi(xy) = \phi(x).\ \phi(y)$ (since ϕ is homomorphism)
$= e^1.\ e^1 = e^1$
$\Rightarrow xy \in K$. Therefore closure axiom holds.

Let $x \in K \Rightarrow \phi(x) = e^1$. Now $\phi(x^{-1}) = [\phi(x)]^{-1} = [e^1]^{-1} = e^1$.

Therefore $x^{-1} \in K$. Thus every element in K has its inverse in K. Hence K is a subgroup of G.

Next we show that K is a normal. Take $g \in G$, $k \in K$.

$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1})$

$= \phi(g).e^1.\phi(g^{-1})$ (since $k \in K \Rightarrow \phi(k) = e^1$)

$= \phi(g).\phi(g^{-1}) = \phi(g).[\phi(g)]^{-1} = e^1$

$\Rightarrow \phi\,(gkg^{-1}) = e^1 \Rightarrow gkg^{-1} \in K$. Hence K is a normal subgroup of G.

13.4.6 Theorem (Fundamental theorem of homomorphism): Let ϕ be a homomorphism of G on to G^1 with kernal K. Then $G/K \cong G^1$.

Proof: Since ϕ is an onto homomorphism from G to G^1, we have $\phi\,(G) = G^1$. That is G^1 is the homomorphic image of ϕ. Define f: $G/K \to G^1$ by $f(Ka) = \phi(a)$ for all $Ka \in G/K$.

f is well defined: Let $a, b \in G$ and $Ka = Kb$

$\Rightarrow ab^{-1} \in K$

$\Rightarrow \phi\,(ab^{-1}) = e^1$

$\Rightarrow \phi\,(a).\,[\phi\,(b)]^{-1} = e^1$

$\Rightarrow \phi\,(a) = \phi\,(b)$

$\Rightarrow f\,(Ka) = f\,(Kb)$.

f is 1-1: Suppose $f(Ka) = f(Kb)$

$\Rightarrow \phi\,(a) = \phi\,(b)$

$\Rightarrow \phi\,(a).\,[\phi\,(b)]^{-1} = e^1$

$\Rightarrow \phi\,(a).\,\phi\,(b^{-1}) = e^1$

$\Rightarrow \phi\,(ab^{-1}) = e^1$

$\Rightarrow ab^{-1} \in K$

$\Rightarrow Ka = Kb$.

Therefore f is 1-1.

f is onto : Let $y \in G^1$. Since ϕ: $G \to G^1$ is onto, we have that there exists $x \in G$ such that $\phi(x) = y$. Since $x \in G$, we have $Kx \in G/K$. Now $f(Kx) = \phi(x) = y$. Therefore f is onto.

f is homomorphism : Let $Ka, Kb \in G/K$.

$f(Ka.Kb) = f(Kab) = \phi(ab) = \phi(a).\phi(b)$ (since ϕ is homomorphism) $= f(Ka).f(Kb)$. Therefore f is a homomorphism.

Hence f: $G/K \to G^1$ is an isomorphism.

13.5 Permutation Groups

13.5.1 Definition: If the set S contains n elements, then the group $A(S) = \{f : S \to S \,/\, f \text{ is } a$ bijection $\}$ has $n!$ elements. Since S has n elements we denote $A(S)$ by S_n and this $A(S) = S_n$ is called the **symmetric group** of degree n. If $\phi \in A(S) = S_n$, then ϕ is a one to one mapping of S onto itself.

13.5.2 Example: If $S = \{x_1, x_2, x_3, x_4\}$ and $\phi \in A(S)$ by $\phi(x_1) = x_2$, $\phi(x_2) = x_4$, $\phi(x_3) = x_1$, $\phi(x_4) = x_3$ is denoted by $\phi = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_4 & x_1 & x_3 \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$. If $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ and $\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ then $\psi\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ (verify). Here we use $\psi\theta(x) = \psi(\theta(x))$ for all $x \in S$.

13.5.3 Example: Permutation multiplication is not usually commutative. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$. Then $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ but $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

13.5.4 Definition: A permutation $\sigma \in S_n$ is a **cycle** of length k if there exists elements $a_1, a_2, \ldots, a_k \in S$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_k) = a_1$ and $\sigma(x) = x$ for all other elements $x \in S$.

We will write $(a_1, a_2, \ldots, a_k)$ to denote the cycle σ. Cycles are the building blocks of the permutations.

13.5.5 Example: The permutation $\sigma = \begin{pmatrix} 1234567 \\ 6351427 \end{pmatrix}$ = (1 6 2 3 5 4) is a cycle of length 6, whereas $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$ = (2 4 3) is a cycle of length 3. Also, not, every permutation is a cycle. Consider the permutation $\begin{pmatrix} 123456 \\ 241365 \end{pmatrix}$ = (1 2 4 3)(5 6).

Self Assessment Question 8: Compute the product of cycles σ = (1 3 5 2), τ = (2 5 6).

13.5.6 Note: Two cycle $(a_1, a_2,\ldots, a_k)$ and $(b_1, b_2, \ldots, b_k)$ are said to be disjoint if $a_i \neq b_j$ for all i and j.

For instance, the cycles (1 3 5) and (2 7) are disjoint; however, the cycles (1 3 5) and (3 4 7) are not. Calculating their products, we find that

(1 3 5)(2 7) = (1 3 5)(2 7)

(1 3 5) (3 4 7) =(1 3 4 7 5).

It is observed that the product of two cycles that are not disjoint may reduce to something less complicated; the product of disjoint cycles cannot be simplified.

The simplest permutation is a cycle of length 2. Such cycles are called *transpositions*.

Since $(a_1, a_2,\ldots, a_n) = (a_1a_n)\ (a_1a_{n-1})\ldots\ (a_1a_3)\ (a_1a_2)$, any cycle can be written as the product of transpositions.

13.5.7 Definition: (i) *A* permutation is said to be an **odd permutation** if is the product of an odd number of transpositions (or 2- cycles).

(ii) *A* permutation is said to be an **even permutation** if is the product of an even number of transpositions (or 2 – cycles).

Self Assessment Questions 9: Determine which of the following permutations is even or odd

(i). (1 3 5); (ii) (1 3 5 6); (iii) $\begin{pmatrix} 1 2 3 4 \\ 2 1 4 3 \end{pmatrix}$; (iv). $\begin{pmatrix} 1 2 3 4 5 \\ 5 3 2 4 1 \end{pmatrix}$; (v). (1 3)(1 2 4)(1 5 3).

13.5.8 Example: Consider the permutation (1 6)(2 5 3) = (1 6)(2 3)(2 5) = (1 6)(4 5)(2 3)(4 5)(2 5). As we can see, there is no unique way to represent permutation as the product of transpositions. For instance, we can write the identity permutation as (1 2)(2 1), as (1 3)(2 4)(1 3)(2 4), and in many other ways. However, no permutation can be written as the product of both an even number of transpositions and an odd number of transpositions.
For instance, we could represent the permutations (1 6) by (2 3)(1 6)(2 3) or by (3 5)(1 6)(1 3)(1 6)(1 3)(3 5)(5 6) but (1 6) will always be the product of an odd number of transpositions

Self Assessment Question 10: Write the following whether even or odd.
(i) The product of two even permutations.
(ii) The product of an even permutation and an odd one. (like wise for the product of an odd and even permutation).
(iii) The product of two odd permutations.

13.6 Answers to Self Assessment Questions

SAQ1.
It forms a group. 0 is the identity and each element has its own inverse.

SAQ2.

It can be verified that * is closed and associative. 0 (zero element in the set of integers) acts as identity. For 3 $\in$ Z, there is no x $\in$ Z such that 3 + x -3x = 0, since 3 + x -3x = 0 $\Rightarrow$ x = $\frac{3}{2}$ $\notin$ Z. Hence Z is not a group with the defined operation *.

SAQ 3.

Take G = {A, B, C, D}, where $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ $C = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ D $= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$. A is the identity in G. Table of multiplication as follows:

.	*A*	*B*	*C*	D
A	*A*	*B*	*C*	D
B	*B*	*A*	D	*C*
C	*C*	D	*A*	*B*
D	D	*C*	*B*	*A*

SAQ 4.

It is a cyclic group with generators i and –i.

SAQ 5.

The left cosets are H = {0, 3}, 1+H = {1, 4}, 2+H = {2, 5}.

SAQ 6.

$\phi(a + b) = 2^{a+b} = 2^{a}. 2^{b} = \phi(a). \phi(b)$. Therefore ϕ is a homomorphism.

SAQ 7.

f is one one and homomorphism is clear. To show f is onto, take x $\in$ R^{+}. Then $\phi(\ln x) = e^{\ln x} = x$ where ln x $\in$ R. Therefore ϕ is onto.

SAQ 8.

The product is $\sigma\tau = (1356)$.

SAQ 9.

(i). even, (ii). odd, (iii). even, (iv). even, (v). odd.

SAQ 10.

(i) even, (ii) odd, (iii) even.

13.7 Summary

The algebraic structures with one binary operation were discussed. Some important characterizations of the algebraic system: Groups were given. Some fundamental results are obtained. Cyclic subgroups play a fundamental part in the classification of abelian groups. The special types of groups, referred as permutation groups are the tool to study the geometric symmetries and finding solutions of polynomial equations. We also discussed the Lagrange's theorem, which provides a powerful tool for analyzing finite groups.

13.8 Technical Terms

Binary operation: Mapping from $G \times G$ to *G*.

Group: The algebraic system (*G*, *) satisfies: Closure, associative, existence of identity, and the Inverse.

Commutative group (or Abelian group): $a*b = b*a$ for all *a*, *b* in *G*.

Subgroup: A subset *H* of *G* which itself forms a group under the same operation in *G*.

Order of an element: Least positive integer *m* such that $a^m = e$.

Cosets: *H* is a subgroup of *G* and $a \in G$, $Ha = \{ha \,/\, h \in H\}$ is the *right coset* and $aH = \{ah \,/\, h \in H\}$ is the *left coset..*

Lagranges Theorem: If G is a finite group and H is a sub group of G, then O(H) is a divisor of O(G).

Index of H in G: The number of distinct right cosets of *H* in *G*.

Normal subgroup: N is normal in G if $gNg^{-1} \subseteq N$ for all $g \in G$.

Homomorphism: $\phi: (G, +) \rightarrow (G^1, .)$ such that $\phi(ab) = \phi(a).\ \phi(b)$ for all a and b in G.

Kernal of ϕ (denoted by ker ϕ): $\ker \phi = \{x \in G \,/\, \phi(x) = e^1$, where e^1 is the identity in $G^1\}$.

Fundamental theorem of homomorphism: Let ϕ be a homomorphism of G on to G^1 with kernal K. Then $G/K \cong G^1$.

Cycle permutation: A permutation $\sigma \in S_n$ is a *cycle* of length k if there exists elements $a_1, a_2, \ldots, a_k \in S$ such that $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, …, $\sigma(a_k) = a_1$ and $\sigma(x) = x$ for all other elements $x \in S$.

Odd permutation: The product of an odd number of transpositions (or 2-cycles).

Even permutation: The product of an even number of transpositions (or 2 – cycles).

13.9 Model Questions

1. Consider the group $(\mathbb{Z}, +)$. Let $H = \{3n \,/\, n \in \mathbb{Z}\}$. Show that the set H is a subgroup of $\mathbb{Z}$.

2. Prove that $(G, +_6)$ is cyclic where $G = \{0, 1, 2, 3, 4, 5\}$.

3. If '*' is a binary operation in Q^+ defined by (i). $a * b = \frac{ab}{3}$

(ii). $a * b = \frac{ab}{2}$

where a, $b \in Q^+$ (set of all positive rationals). Show that $(Q^+, *)$ is are abelian groups.

4. Examine which o*f* the following are groups. For those which fail to be groups mention which group axoims do not hold.

(i). G = $\mathbb{R}$, the set of reals, with respect to '*' where $a * b = a$ for all $a \in \mathbb{R}$.

(ii). G = $\mathbb{Z}$, the integers, with $a * b = a + b + 1$, a, b, $\in \mathbb{Z}$.

5. Find the inverse of each of the following permutations

(i). $\begin{pmatrix} 1234 \\ 1342 \end{pmatrix}$, (ii). $\begin{pmatrix} 12345 \\ 23154 \end{pmatrix}$, (iii). $\begin{pmatrix} 1234 \\ 3412 \end{pmatrix}$.

6. Express each of the following as a product of transpositions and hence determine whether it is odd or even.

(i). $\begin{pmatrix} 123 \\ 213 \end{pmatrix}$, (ii). $\begin{pmatrix} 123 \\ 321 \end{pmatrix}$, (iii). $\begin{pmatrix} 1234 \\ 4321 \end{pmatrix}$.

7. If G is a group such that $(ab)^2 = a^2b^2$ for all $a,b \in G$, then show that G is abelian.

8. In the following, determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.

(*a*) The set of all integers. Operation: $a\text{o}b = a\text{-}b$.

(*b*) The set of all positive integers. Operation: $a\text{o}b = a.b$.

(*c*) $\{a_o, a_1, \dots, a_6\}$ where $a_i\text{o}a_j = a_{i+j}$ if $i + j < 7$ and $a_i\text{o}a_j = a_{i+j-7}$ (that is, if $i + j \geq 7$).

(d) The set of all rational numbers with odd denominators. Operation: $a\text{o}b = a + b$.

9. If a group *G* has only three elements, show that it must be abelian.

10. Let *G* be the set of all real 2 × 2 – matrices $\begin{bmatrix} a & b \\ o & d \end{bmatrix}$ where ad ≠ 0. Prove that *G* forms a group under matrix multiplication. Is *G* is abelian?

11. State and prove Lagrange's theorem.

12. State and prove fundamental theorem of homomorphism of groups.

13.10 References

1. Akerkar Rajendra and Akerkar Rupali. "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Fraleigh J.B. **"**A First Course in Abstract Algebra", Narosa Publ. House, New Delhi, 1992

3. Hari Kishan and Shivraj Pundir "Discrete Mathematics", Pragati Prakashan, Meerut, 2005.

4. Herstein I. N. "Topics in Algebra", Blaisdell, New York, 1964.

5. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. "Quantitative Methods", Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

6. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

7. Trembly, J.P., and Manohar, R. "Discrete Mathematical Structures with Applications to Computer Science", Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 14

Advanced Algebras and Group Codes

Objectives

At the end of the Lesson the student must be able to:

(i) Learn the algebraic systems with two binary operations.
(ii) Know the structures rings and integral domain.
(iii)Understand the fundamental idea of coding system.
(iv)Know the hamming distance between the code words.
(v) Learn the group codes, linear codes and parity check codes
(vi)Apply the concepts to real world problem in communication technology

Structure

14.1 Introduction

Groups were studied in the previous chapter and the definition of a group involves a single binary operation. We know that there are two binary operations: addition and multiplications on the number such as integers, rational, real or complex. With respect to addition they form a group. Also the non zero rational, real or complex numbers form a group under multiplication.

Many of the properties of numbers depend simultaneously on both operations of addition and multiplication. These two operations are interrelated and lead us to study the algebraic systems with two binary operations. One such system is a ring. Further Coding theory is an application of algebra that has become increasingly important over the last several decades. When we transmit data, we are concerned about sending a message over a channel that could be affected by *noise*. We wish to be able to encode and decode the information in a manner that will allow the detection, and possible the correction, of errors caused by noise. This situation arises in many areas of communications, including radio, telephone, television, computer communication. Probability, combinatorics, group theory, linear algebra play important roles in coding theory.

14.2 Rings and Integral domains

14.2.1 Definition: *A* non empty set R is said to be a **ring** (or an associative ring) if there exists two operations + and "."on R such that (i) $(R, +)$ is an abelian group (ii) $(R, .)$ is a semi-group and (iii) for any $a, b, c \in R$ we have $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

14.2.2 Definition: Let $(R, +, .)$ be a ring. If $1 \in R$ such that $a.1= 1.a = a$ for every $a \in R$, then we say that R is a **ring with identity** (or unit) element. If $a.b = b.a$ for all $a, b \in R$, then R is said to be a **commutative** ring.

14.2.3 Examples: (i) (Z (set of integers), +, .) is a commutative ring with identity.

(ii) (2Z(set of even integers), +, .) is a commutative ring with out identity.

(iii) (Q(set of rationals), +, .) is a commutative ring with identity.

(iv) (Z_n,(integers modulo n) +, .) is a commutative ring with identity.

14.2.4 Definition: (i) If R is a commutative ring then $0 \neq a \in R$ is said to be a **zero divisor** if there exits $0 \neq b \in R$ such that $ab = 0$.

(ii) A commutative ring is said to be an **integral domain** if it has no zero divisors.

(iii) A ring R is said to be a **Boolean ring** if $x^2 = x$ for all $x \in R$ (in other words, each element of R is an idempotent).

14.2.5 Example: Let R be the set of all formal square arrays $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are any real numbers.

Define $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix}$. It is easy to see that R forms an abelian group under addition with $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ as the zero element and $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ is the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We define the multiplication in R by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} . \begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{pmatrix}$.

The element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ acting as multplicative unit element. Clearly R is a ring .

Since $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, we have that R is not an integral domain.

Since $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} . \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, we have that R is not commutative.

Self Assessment Question 1: Prove that if a, b $\in$ R, then $(a+b)^2 = a^2 + ab + ba + b^2$.

Self Assessment Question 2: If R is a Boolean ring then R is a commutative ring.

14.2.6 Definition: *A* ring R is said to be a **division ring** if $(R^*,.)$ is a group (here $R^* = R - \{0\}$). *A* division ring is said to be a **field** if it is commutative (we will learn this concept in the next section).

14.2.7 Problem: If R is a ring then for all $a, b \in R$ we have

(i) $a0 = 0 = 0a$

(ii) $a(-b) = (-a)b = -ab$

(iii) $(-a)(-b) = ab$. If in addition if R has identity 1, then

(iv) $(-1)a = -a$, $(-1)(-1) = 1$.

Solution: (i) $a0 = a(0 + 0) = a0 + a0$. Now

$0 + a0 = a0 = a0 + a0 \Rightarrow a0 = 0$ (by right cancellation law).

Similarly, we can prove that $0 = 0a$.

(ii) $0 = a0 = a(b+(-b)) = ab + a(-b)$

$\Rightarrow -(ab) = a(-b)$ and $0 = 0b = (a+(-a))b = ab+(-a)b$

$\Rightarrow -(ab)=(-a)b$.

(iii) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

(iv) from (ii), $(-1)a = -(1a) = -a$.

(v) from (iii), $(-1)(-1) = 1.1 =1$.

14.2.8 Example: Consider the ring $(Z_m, +_m, \times_m)$ for all $m \in Z$. For $m = 6$, we have $[2] \times_m [3] = [0]$ but $[2] \neq [3]$. Also for $m = 7$, $(Z_m, +_m, \times_m)$ is an integral domain.

14.2.9 The Pigeon Hole Principle: If a objects are distributed over m places and if $a > m$, then some place receives at least two objects.

14.2.10 Theorem: A finite integral domain is a field.

Proof: We know that in an integral domain we have $ab = 0 \Rightarrow a = 0$ or $b = 0$. Now it suffices to show that every non-zero element has multiplicative inverse. Let D be an integral domain. Now we show

(i) there exists $1 \in D$ such that $a \,.\, 1 = a$ for all $a \in D$,

(ii) $0 \neq a \in D \Rightarrow$ there exists $b \in D$ such that $ab = 1$.

Let $D = \{x_1, x_2, \ldots, x_n\}$ and $0 \neq a \in D$. Now $x_1a, x_2a, \ldots, x_na$ are all distinct

(If $x_ia = x_ja$, then $(x_i - x_j)a = 0 \Rightarrow x_i - x_j = 0 \Rightarrow x_i = x_j$ (since $a \neq 0$)).

Therefore $D = \{x_1a, x_2a \ldots, x_na\}$. Since $a \in D$, $a = x_ka$ for some $1 \leq k \leq n$.

Again siince D is commutative, we have $x_ka = a = ax_k$.

We show x_k is the identity element. For this, let $y \in D$, then $y = x_ia$ for some i.

Now consider $y.x_k = (x_ia)\, x_k = x_i\, (ax_k) = x_ia = y$.

Thus $yx_k = y$ for all $y \in D$. Therefore x_k is the identity element.

For $x_k \in D = \{x_1a, x_2a, \ldots, x_na\} \Rightarrow x_k = x_ja$ for some $1 \leq j \leq n$.

Therefore x_j is the multiplicative inverse of a. Hence D is a field.

14.2.11 Definition: A subset T of a ring $(S, +, \cdot)$ is called a subring if $(T, +, \cdot)$ is itself a ring.

14.2.12 Example: The set of all even integers is a subring of $(Z, +, \cdot)$.

14.2.13 Definition: Let $(R, +, .)$, $(R^1, +, .)$ be two rings. *A* mapping $\phi : R \to R^1$ is said to be a **homomorphism** *(or* a **ring-homomorphism***)* if (i) $\phi(a + b) = \phi(a) + \phi(b)$, (ii) $\phi(ab) = \phi(a)\, \phi(b)$ for all $a, b \in R$.

Self Assessment Question 3: If $\phi: R \to R^1$ is a homomorphism, then verify that (i) $\phi(0) = 0$, (ii) $\phi(-a) = -\phi(a)$ for all $a \in R$.

14.2.14 Definition: (i) Let $\phi: R \to R^1$ be a homomorphism. Then the set $\{x \in R \,/\, \phi(x) = 0\}$ is called the **kernal of ϕ** and is denoted by $ker\phi$.

(ii) *A* homomorphism $\phi: R \to R^1$ is said to be an **isomorphism** if ϕ is one one and, onto.

(iii) R and R^1 are said to be **isomorphic**, if there exist an isomorphism $\phi: R \to R^1$.

14.2.15 Problem: Let $\phi: R \to R^1$ be a homomorphism.

Then (i) kerϕ = {0} $\Leftrightarrow$ ϕ is one one.

(ii) If ϕ is onto then ϕ is an isomorphism if and only if kerϕ = {0}, where 0 is the additive identity if R.

Solution: (i) Suppose ker ϕ = {0}. To show ϕ is 1-1.

Suppose $x, y \in R$ such that $\phi(x) = \phi(y)$. Then $\phi(x) - \phi(y) = 0$

$\Rightarrow \phi(x) + \phi(-y) = 0$

$\Rightarrow \phi(x - y) = 0 \Rightarrow x - y \in \ker \phi = \{0\}$

$\Rightarrow x - y = 0$

$\Rightarrow x = y$. Therefore ϕ is one one.

Converse: Suppose ϕ is one one. Since $\phi(0) = 0$, we have $0 \in \ker \phi$

$\Rightarrow \{0\} \subseteq \ker \phi$. Now let $y \in \ker \phi$

$\Rightarrow \phi(y) = 0 = \phi(0)$ (since $\phi(0) = 0$)

$\Rightarrow y = 0$ (since ϕ is one one)

$\Rightarrow \ker \phi \subseteq \{0\}$. Therefore $\ker \phi = \{0\}$.

(ii) Suppose ϕ is an isomorphism. Since ϕ is one one, we have ker ϕ = {0} (by (i)).

Converse: Suppose kerϕ = {0} $\Rightarrow$ ϕ is 1-1 (by (i)).

Since ϕ is onto, we have ϕ is a bijection. Hence ϕ is an isomorphism.

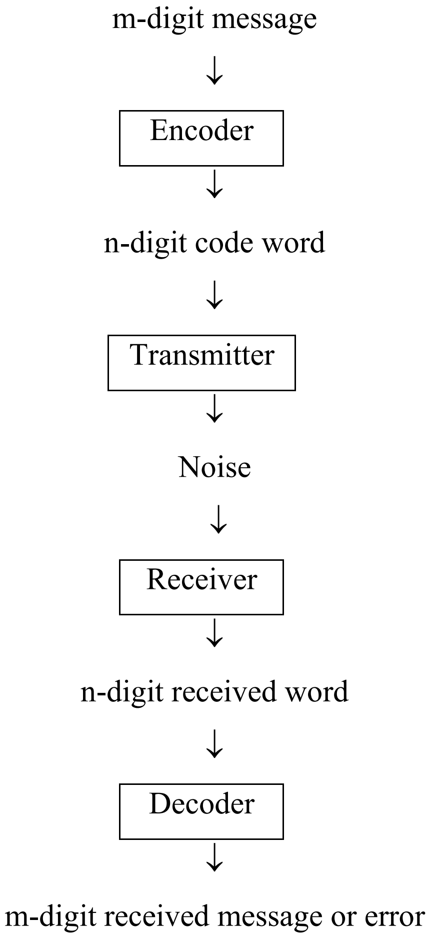
14.3 Codes

Let us examine a simple model of a communications system for transmitting and receiving coded messages. The model represented by at least three essential parts: Transmitter, Channel and Receiver.

The *channel* conveys the message sent by the transmitter to the receiver. But in practice, a communication channel is subjected to variety of disturbances. These disturbances distort the message being transmitted. Such disturbance is called *noise*. The main object of a communication system is to minimize the distortion due to noise and to recover the original message in some optimal manner.

Uncoded messages may be composed of letters or characters, but typically they consist of binary m-tuples. These messages are encoded into codewords, consisting of binary n-tuples, by a devise called an *encoder*. The message is transmitted and then decoded. We will consider the occurrences of errors during transmission. An error occurs if there is a change in one or more bits in the codeword. A decoding scheme is a method that either converts an arbitrarily received n-tuple into meaningful decoded message or gives an error message for that n-tuple.

Encoding and decoding messages:



m-digit message

Encoder

n-digit code word

Transmitter

Noise

Receiver

n-digit received word

Decoder

m-digit received message or error

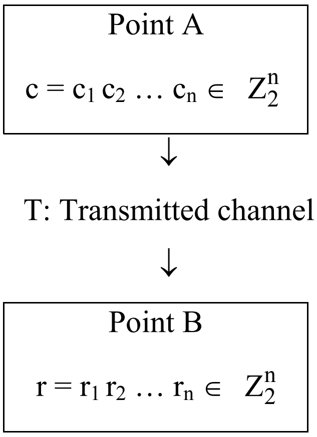
Consider the set Z_2 = {0, 1} and additive group (Z_2, +), where + denotes addition modulo 2. Then, for any positive integer n, we have

$Z_2^n = Z_2 \times Z_2 \times \ldots \times Z_2$ (n factors) = $\{(a_1, a_2, \ldots, a_n) / a_i \in Z_2$ for each i$\}$.

Thus, every element of Z_2^n is an n-tuple $(a_1, a_2, \ldots, a_n)$ in which every entry is either 0 or 1. Some times the n-tuple can be written as $a_1\ a_2 \ldots a_n$ called a *word* or a *string*. Each a_i (either 0 or 1) is called a bit.

14.3.1 Example: 11001 is a word in Z_2^5. That is $(1,1,0,0,1) \in Z_2^5$.

Suppose a string $c = c_1\, c_2 \ldots c_n \in Z_2^n$ is transmitted form a point A through a transmitted channel T. In normal situations, this word would be received at a point B with out any change. But in practice, transmission channel experience disturbances (which is referred as *noise*) that may cause a 0 to be received as a 1 (or vice versa). Therefore the word c transmitted from A is received as a different word $r \in Z_2^n$ at B. Let the word r will be of the form $r = r_1\, r_2 \ldots r_n$ where each r_i is either 0 or 1, $r_j \neq c_j$ for some j, $1 \leq j \leq n$.


Point A
$c = c_1\, c_2 \ldots c_n \in Z_2^n$
T: Transmitted channel
Point B
$r = r_1\, r_2 \ldots r_n \in Z_2^n$

If $r_i = c_i$ for all values of I except k values ($k < n$), we say that r differs from c in k places. The word r is denoted by T(c). Some times, it is convenient to write r as $r = c + E$ where $E \in Z_2^n$.

14.3.2 Binary Symmetric Channel: It is a model consists of a transmitter capable of sending a binary signal, either a 0 or a 1, together with a receiver. Let p be the probability that the signal is correctly received. Then $q = 1-p$ is the probability of an incorrect reception. If a 1 is sent, then the probability that a 1 is received is p and the probability that a 0 is received is q. The probability that no errors occur during the transmission of a binary codeword of length n is p^n. For example, if $p = 0.999$ and a message consisting of 10,000 bits is sent, then the probability of a perfect transmission is $(0.9999)^{10,000} \approx 0.00005$.

14.3.3 Note: Let $n > m$. We define a one-to-one function $E: B^m \rightarrow B^n$ where $B = \{0, 1\} = Z_2$. Sometimes we use E for the encoding function.

A code word is any element in the image of E. That is if $b \in B^m$ then $E(b) \in B^n$. We transmit the code word by means of a channel. Then each code word $x = E(b)$ is received as the work $x_1 \in B^n$. If the channel is noiseless then $x_1 = x$ for all $x \in B^n$. But in general, errors do occur.

14.3.4 Theorem: If a binary n-tuple $(x_1, x_2, \ldots, x_n)$ is transmitted across a binary symmetric channel with probability p that no error will occur in each coordinate, then the probability that there are errors in exactly k coordinates is $\begin{pmatrix} n \\ k \end{pmatrix} q^k p^{n-k}$

Proof: Fix k different coordinates. We first compute the probability that an error has occurred in this fixed set of coordinates. The probability of an error occurring in a particular one of these k coordinates is q; the probability that an error will not occur in any of the remaining n-k coordinates is p. The probability of each of these n independent events is $q^k p^{n-k}$.

The number of possible error patterns with exactly k errors occurring is equal to

$\binom{n}{k} = \frac{n!}{k!(n-k)!}$, the number of combinations of n things taken k at a time. Each of these error patterns has probability $q^k p^{n-k}$ of occurring; hence the probability of all these error patterns is $\binom{n}{k} q^k p^{n-k}$.

14.3.5 Example: Suppose that p = 0.995 and a 500-bit message is sent. The probability that the message was sent error-free is $p^n = (0.995)^{500} \approx 0.082$.

The probability of exactly one error occurring is

$$\binom{n}{1} q \; p^{n-1} = 500(0.005)(0.995)^{499} \approx 0.204.$$

The probability that exactly two errors is

$$\binom{n}{1} q^2 p^{n-2} = \frac{500 \cdot 499}{2}(0.005)^2(0.995)^{498} \approx 0.257.$$

The probability of more than two errors is approximately

$$1 - 0.082 - 0.204 - 0.257 = 0.457$$

Self Assessment Question 4: The word c = 1010110 is transmitted through a binary symmetric channel. If E = 0101101 is the error pattern, find the word r received.

Self Assessment Question 5: The word c = 1010110 is transmitted through a binary symmetric channel that c is received as r = 1011111. Determine the error pattern.

14.3.6 Definition: Let $D = [d_{ij}]$ be m×p and $E = [e_{ij}]$ be p×n Boolean matrices. We define the mod-2 Boolean product $D \otimes E$ as the m×n matrix $F = [f_{ij}]$, where $f_{ij} = d_{i1}e_{1j} + \ldots + d_{ip}e_{pj}$, $1 \leq i \leq m$, $1 \leq j \leq n$.

14.3.7 Example: The product of

$$\begin{pmatrix}1\ 1\ 0\\0\ 1\ 1\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\1 & 1\\0 & 1\end{pmatrix}=\begin{pmatrix}1\times1+1\times1+0\times0 & 1\times0+1\times1+0\times1\\0\times1+1\times1+1\times0 & 0\times0+1\times1+1\times1\end{pmatrix}=\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}.$$

Property: Let D and E be m×p Boolean matrix and F be a p×n Boolean matrix. Then (D + E)⊗ F = (D⊗F) + (E⊗F) (distributivity for + and ⊗).

14.3.8 Block Codes: If we are to develop efficient error-detecting and error-correcting codes, we will need more sophisticated mathematical tools. Group theory will allow faster methods of encoding and decoding messages. A code is an (n, m) block code if the information that is to be coded can be divided into blocks of m binary digits, each of which can be encoded into n binary digits.

14.3.9 Parity Check Code:

Define an encoding function E: $Z_2^m \to Z_2^{m+1}$ by E($e_1\ e_2\ \ldots\ e_m$) = $e_1\ e_2\ \ldots\ e_{m+1}$ where e_{m+1} = $\begin{cases}0 \text{ if e contains even number of 1s}\\1 \text{ if e contains odd number of 1s}\end{cases}$. Using the definition of E: $Z_2^3 \to Z_2^4$,

E(000) = 0000, E(001) = 0011, E(011) = 0110, …, E(111) = 1111

14.4 Hamming Distance:

14.4.1 Definition: Let x = (x_1, x_2, …,x_n) and y = (y_1, y_2, …,y_n) be binary n-tuples. The **hamming distance** or distance d(x,y), between x and y is the number of bits in which x and y differ.

14.4.2 Note: The distance between two codewords is the minimum number of transmission errors required to change one codeword into the other.

14.4.3 Definition: The **minimum distance of encoding function** E: $B^m \to B^n$ is the minimum distance between all pairs of code words.

That is, d_{min} = min. {d(x,y) | where x and y are distinct code words}.

14.4.4 Definition: The **weight** w(x) of a binary code word x is the number of 1's in x. It is also denoted by | x | . From the definition, it is clear that w(x) = d(x, 0) where 0 = (00…0).

14.4.5 Example: Find the weights of the following words in B^7 where B = Z_2.

(i) x = 0100101,

(ii) y = 1100101,

(iii) z = 1111101.

Solution: The weights are (i) w(x) = 3, (ii) w(y) = 4, (iii) w(z) = 6.

14.4.6 Example: Let x = (10101), y = (11010) and z = (00011) be all of the codewords in some code C. Then we have the following hamming distances.

$$d(x, y) = 4, d(x, z) = 3, d(y, z) = 3.$$

The minimum distance for this code is 3. Also we have the following weights.

$$w(x) = 3, w(y) = 3, w(z) = 2.$$

14.4.7 Problem: Let x and y be binary n-tuples. Then w(x + y) = d(x, y).

Solution: Suppose that x and y are binary n-tuples. Then the distance between x and y is exactly the number of places in which x and y differ. But x and y differ in a particular coordinate exactly when the sum in the coordinate is 1, since

1 + 1 = 0, 0 + 0 = 0, 1 + 0 = 1, 0 + 1 = 1. Consequently, the weight of the sum must be the distance between the two codewords.

14.4.8 Note: For all x, y $\in$ Z_2^m we have $w(x + y) \leq w(x) + w(y)$.

14.4.9 Problem: Let x, y, z $\in$ Z_2^n. Then

(i) $d(x, y) \geq 0$

(ii) $d(x, y) = 0$ exactly when $x = y$

(iii) $d(x, y) = d(y, x)$

(iv) $d(x, y) \leq d(x, z) + d(z, y)$.

Solution: (i) Since $w(x+y) \geq 0$, we have that $d(x, y) \geq 0$.

(ii) $d(x, y) = 0 \Leftrightarrow w(x + y) = 0 \Leftrightarrow x + y$ contains only 0's

$\Leftrightarrow$ x and y contains only 1's or only 0's $\Leftrightarrow x = y$.

(iii) $d(x, y) = w(x + y) = w(y + x) = d(y, x)$

(iv) $d(x, z) = w(x + z)$

$= w(x + y + y + z)$ (since $y + y = 0$ in Z_2)

$\leq w(x + y) + w(y + z)$ (by the above note)

$= d(x + y) + d(y + z)$

14.4.10 Note: (i) The function d satisfies the condition in the above problem is called a hamming metric and the pair (Z_2^n, d) is called a Hamming metric space.

(ii) For a specified word a $\in$ Z_2^n and a positive integer k, we define the sphere with center a and the radius k units is $S(a, k) = \{x \in Z_2^n / d(x, a) \leq k\}$.

14.4.11 Definition: Let $x_1, x_2, \ldots, x_n$ denote the codewords in a block code. The conditional probability $P(x_i | y)$ for i= 1, 2, …, n where $P(x_i | y)$ is the probability that x_i was the transmitted word given that y was the received word. If $P(x_k | y)$ is the largest of all conditional probabilities computed, then x_k was the transmitted word. Such a criterion for determining the transmitted word is known as the **maximum likelihood decoding criterion**.

14.4.12 Note: Suppose that x = (1101) and y = (1100) are codewords in some code. If we transmit (1100) and an error occurs in the rightmost bit, then (1100) will be received. Since (1100) is a codeword, the decoder will decode (1100) as the transmitted message. This code is clearly not very appropriate for error detection. The problem is that d(x, y) = 1. If x = (1100) and y = (1010) are codewords, then d(x, y) = 2. If x is transmitted and a single error occurs, then y can never be received. Consider the following table of distances of all 4-bit codewords in which the first three bits carry information and the fourth is an even parity check bit. We can see that the minimum distance is 2.

Distances between 4-bit codewords.

	0000	0011	0101	0110	1001	1010	1100	1111
0000	0	2	2	2	2	2	2	4
0011	2	0	2	2	2	2	4	2
0101	2	2	0	2	2	4	2	2
0110	2	2	2	0	4	2	2	2
1001	2	2	2	4	0	2	2	2
1010	2	2	4	2	2	0	2	2
1100	2	4	2	2	2	2	0	2
1111	4	2	2	2	2	2	2	0

14.4.13 Theorem: An (m, n) encoding function E: $B^m \rightarrow B^n$ can detect k or fewer errors if and only if its minimum distance is at least k +1.

Proof: Part 1: Suppose the minimum distance between any two code works is at least (k+1). Let $b \in B^m$ and $x = E(b) \in B^n$. Then x is transmitted and received as x_1. If x_1 were a code word different from x then $d(x, x_1) > k+1$. So x would be transmitted with (k+1) or more errors. Thus if x is transmitted with k or fewer errors then x_1 cannot be a code word.

This means that E can detect k or fewer errors.

Part 2: Suppose the minimum distance between the code words is $r < k$ and let x and y are code words with $d(x, y) = r$.

If $x_1 = y$, that is, if x is transmitted and received as y then $r < k$ errors have been committed and have not been detected. This it is not true that E can detect k or fewer errors. Hence the minimum distance is at least (k+1).

14.4.14 Example: Consider the following table of 5-bit codewords with the hamming distances for an error correcting code.

	00000	00111	11100	11011
00000	0	3	3	4
00111	3	0	4	3
11100	3	4	0	3
11011	4	3	3	0

The codeword $c_1 = (00000)$, $c_2 = (00111)$, $c_3 = (11100)$, $c_4 = (11011)$ determine a single error correcting code.

14.5 Linear Codes

14.5.1 Definition: Let E: $Z_2^m \to Z_2^n$, n > m be an encoding function and $C = \{E(w) | w \in Z_2^m\}$ be the set of codes. Then C is called a **group code** if C is a subgroup of Z_2^n.

14.5.2 Example: Consider the encoding function E: $Z_2^2 \to Z_2^6$ of the triple repetition code. For this code, we have

E(00) = 000000, E(10) = 101010, E(01) = 010101, E(11) = 111111 so that C = {000000, 101010, 010101, 111111}.

Also Z_2^6 is a finite group under the component wise addition modulo 2 and also C $\subseteq$ Z_2^6. (Further the reader can verify that it is an abelian group).

It can be easily verified that C is closed under component wise addition modulo 2. Therefore C is a subgroup. Hence C is a group code.

14.5.3 Problem: Let d_{min} be the minimum distance for a group code C. Then d_{min} is the minimum of all the nonzero weights of the nonzero codewords in C. That is,

$$d_{min} = \min \{w(x) \mid x \neq 0\}.$$

Solution: $d_{min} = \min \{d(x, y) \mid x \neq y\}$

$= \min \{d(x, y) \mid x + y \neq 0\}$

$= \min \{w(x + y) \mid x + y \neq 0\}$

$= \min \{w(z) \mid z \neq 0\}$.

14.5.4 Definition: The **inner product** of two binary n-tuples to be $x{\cdot}y = x_1y_1 + \ldots + x_ny_n$, where $x = (x_1, x_2, \ldots, x_n)^t$ and $y = (y_1, y_2, \ldots, y_n)^t$ are column vectors. We can also write an inner product as the product of a row matrix with a column matrix. That is, $x{\cdot}y = x^ty =$

$$(x_1\ x_2, \ldots x_n)\begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{pmatrix} = x_1y_1 + \ldots + x_ny_n.$$

For instance, if $x = (011001)^t$ and $y = (110101)^t$, then $x{\cdot}y = 0$.

14.5.5 Notation: $M_{m\times n}$ (Z_2) = the set of all m×n matrices with entries in Z_2. We adopt the usual matrix operations except that all addition and multiplication operations occur in Z_2.

14.5.6 Definition: The **null space of a matrix** $H \in M_{m\times n}(Z_2)$ defined to be the set of all binary n-tuples x such $H\otimes x = 0$. We denote the null space of a matrix H by Null (H).

14.5.7 Example: Suppose $H = \begin{pmatrix} 01010 \\ 11110 \\ 00111 \end{pmatrix}$. For a 5-tuple $x = (x_1, x_2, \ldots, x_5)^t$ to be in the null space of H, $H \otimes x = 0$.

Equivalently, the following system of equations must be satisfied:

$$x_1 + x_4 = 0$$

$$x_1 + x_2 + x_3 + x_4 = 0$$

$$x_3 + x_4 + x_5 = 0$$

The set of binary 5-tuples satisfying these equations is

(00000) (11110) (10101) (01011). This code is easily determined to be a group code.

14.5.8 Problem: Let $H \in M_{m\times n}(Z_2)$. Then prove that the null space of H is a group code.

Solution: Closure: Let $x, y \in$ Null(H) for some $H \in M_{m\times n}(Z_2)$.

Then $H\otimes x = 0$ and $H\otimes y = 0$. So $H\otimes(x + y) = H\otimes x + H\otimes y = 0 + 0 = 0$. Therefore x + y is in the null space of H and so must be a code word.

Inverse: Each element of Z_2^n is its own inverse.

Hence Null(H) is a code word.

14.5.9 Definition: A code is a **linear code** if it is determined by the null space of some matrix $H \in M_{m\times n}(Z_2)$.

14.5.10 Example: Let C be the code given by the matrix H = $\begin{pmatrix} 000111 \\ 011011 \\ 101001 \end{pmatrix}$. Suppose that the 7-tuple x = $(010011)^t$ is received. Now H⊗x = $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$. Therefore the received word is not a code word.

14.5.11 Theorem: Let m and n be non-negative integers with m < n, r = n-m, and let H be an n × r Boolean matrix. Then the function f_H: $B^m \rightarrow B^r$ defined by $f_H(x) = x \otimes H$, $x \in B^n$ is a homomorphism from the group B^n to the group B^r.

Proof: Take x, y ∈ B^n. Then $f_H(x + y) = (x + y)\otimes H$

$= (x\otimes H) + (y\otimes H)$ (by distributive law)

$= f_H(x) + f_H(y)$.

Hence f_H is a homomorphism from B^n to B^r.

14.5.12 Corollary: Let m, n, r ∈ H and f_H be $B^m \rightarrow B^r$ defined by $f_H(x) = x \otimes H$, $x \in B^n$ is a homomorphism from the group B^n to the group B^r. Then N = $\{x \in B^n \mid x \otimes H = \mathbf{0}\}$.

Proof: Since N is the kernel of the homomorphism, it follows that N is a normal subgroup.

14.6 Parity Check Matrix:

14.6.1 Definition: Let m < n and r = n –m. An n × r Boolean matrix:

$$\begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1r} \\ h_{21} & h_{22} & \cdots & h_{2r} \\ \vdots & & & \\ h_{m1} & h_{m2} & \cdots & h_{mr} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

is called a **parity check matrix**, whose last r rows form an r × r identity matrix.

14.6.2 Note: $N = \{x \in B^n \mid x \otimes H = \mathbf{0}\}$ where $\otimes$ is the Boolean matrix multiplication, is a normal subgroup of B^n. We use H to define an encoding function $e_H: B^m \rightarrow B^n$. If $b = b_1b_2\ldots b_m$, then we define

$x = e_H(b) = b_1b_2\ldots b_m\, x_1x_2\ldots x_r$ where

$x_1 = b_1h_{11} + b_2h_{21} + \ldots + b_mh_{m1}$,

$x_2 = b_1h_{12} + b_2h_{22} + \ldots + b_mh_{m2}$,

…

$x_r = b_1h_{1r} + b_2h_{2r} + \ldots + b_mh_{mr}$.

14.6.3 Theorem: Let $x = y_1y_2\ldots y_m\, x_1x_2\ldots x_r \in B^n$. Then $x \otimes H = \mathbf{0}$ (that is $x \in N$) if and only if $x = e_H(b)$ for some $b \in B^m$.

Proof: Suppose that $x \otimes H = \mathbf{0}$. Then

$y_1h_{11} + y_2h_{21} + \ldots + y_mh_{m1} + x_1 = 0$

$y_1h_{12} + y_2h_{22} + \ldots + y_mh_{m2} + x_2 = 0$

…

$y_1h_{1r} + y_2h_{2r} + \ldots + y_mh_{mr} + x_r = 0$.

The first equation is of the form $a + x_1 = 0$ where $a = y_1h_{11} + y_2h_{21} + \ldots + y_mh_{m1}$.

Adding a to both sides, we obtain

$a + (a + x_1) = a + 0 = a$

$\Rightarrow (a + a) + x_1 = a$

$\Rightarrow 0 + x_1 = a$, since $a + a = 0$

$\Rightarrow x_1 = a$.

This can be done for each row. Therefore $x_1 = \; y_1h_{1i} + \; y_2h_{2i} + \ldots + y_mh_{mi}$, $1 \le i \le r$.

Let $b_1 = y_1$, $b_2 = y_2$, …, $b_m = y_m$, we see that $x_1, x_2, \ldots, x_r$ satisfy the equations in the above note. Thus $b = b_1b_2\ldots b_m \in B^m$ and $x = e_H(b)$.

Converse: If $x = e_H(b)$ the equations in the above note can be rewritten by adding x_i to both sides of the i^{th} equation, $i = 1, 2, \ldots, n$, as

$b_1h_{11} + b_2h_{21} + \ldots + b_mh_{m1} + x_1 = 0$,

$b_1h_{12} + b_2h_{22} + \ldots + b_mh_{m2} + x_2 = 0$

…

$b_1h_{1r} + b_2h_{2r} + \ldots + b_mh_{mr} + x_r = 0$, which shows that $x \otimes H = \mathbf{0}$.

14.6.4 Corollary: The set $E_H(B^m) = \{E_H(b) \mid b \in B^m\}$ is a subgroup of B^n and is a group code.

14.6.5 Example: For the parity check matrix

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$ determine (2, 5) encoding function $E_H: B^2 \rightarrow B^5$.

Solution: We have $B^2 = \{00, 01, 10, 11\}$. Then $E_H(00) = 00\, x_1x_2x_3$, where

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

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

$x_3 = 0\cdot 1 + 0\cdot 1 = 0$. Therefore $E_H(00) = 00000$.

Now $E_H(01) = 01\, x_1x_2x_3$, where

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

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

$x_3 = 0\cdot 1 + 1\cdot 1 = 1$. Therefore $E_H(01) = 01011$.

Continue in this way we get that $E_H(10) = 10011$ and $E_H(11) = 11000$. Thus $E_H(B^2) = \{00000, 01011, 10011, 11000\}$.

14.6.6 Definition: Consider an (m, n) encoding function E: $B^m \to B^n$. Let x = E(b) for $b \in B^m$ is received as $x_1 \in B^n$. An onto function D: $B^n \to B^m$ is called an (n, m) decoding functrion associated with E if $D(x_e) = b^1 \in B^m$ is such tht when the transmission channel has no noise then $b^1 = b$. That is D o E = $I_B{}^m$ where $I_B{}^m$ is the identity function of B^m.

14.6.7 Note: The function D decodes properly received words correctly, but the decoding of improperly received words may or may not be correct.

14.6.8 Example: Consider the parity check code and the corresponding decoding function is D: $Z_2^{m+1} \to Z_2^m$ defined by $D(r_1 r_2 \dots r_m r_{m+1}) = r_1 r_2 \dots r_m$.

Using the definition of D: $Z_2^4 \to Z_2^3$,

D(0000) = 000, D(0001) = 000, …, D(1010) = 101, D(1100) = 110,…, D(1111) = 111.

14.6.9 Method: Given an (m, n) encoding function E: $B^m \to B^n$, we need to determine an (n, m) decoding function D: $B^n \to B^m$ associated with E. We adopt the maximum likelihood technique, for determining a decoding function D for a given E.

Since B^m has 2^m elements, there are 2^m code words in B^n. We first list the code words in a fixed order:

$x^{(1)}, x^{(2)}, \dots, x^{(2^m)}$. If the received word is x_t, we compute $d(x^{(i)}, x_t)$ for $1 \le i \le 2^m$ and choose the first code word, say it is $x^{(s)}$, such that

$$\min_{1\le i\le 2^m} \{d(x^i, x_t)\} = d(x^{(s)}, x_t).$$

That is, $x^{(s)}$ is a code word that is closest to x_t and the first in the list. If $x^{(s)} = E(b)$, we define the maximum likelihood decoding function · associated with E by $D(x_t) = b$. Observe that D depends on the particular order in which the code words in $E(B^n)$ are listed. If the code words are listed in a different order, we may obtain a different maximum likelihood decoding function D associated with E.

14.6.10 Theorem: Suppose that E is an (m, n) encoding function and D is a maximum likelihood decoding function associated with E. Then (E, D) can correct k or fewer errors if and only if the minimum distance of E is at least 2k+1.

Proof: Part (i): Assume that the minimum distance of E is at least 2k+1.
Let $b \in B^m$ and $x = E(b) \in B^n$. Suppose that x is transmitted with k or fewer errors and x_t is received. This means $d(x, x_t) \le k$. If z is any other code word, then
$2k+1 \le d(x, z) \le d(x, x_t) + d(x_t, z) \le k + d(x_t, z)$.
Thus $d(x_t, z) \ge 2k + 1 - k = k + 1$. This means that x is the unique code word that is closest to x_t, so $D(x_t) = b$. Hence (E, D) corrects k or fewer errors.

Part (ii): Assume that the minimum distance between code words is $r \le 2k$, and let $x = E(b)$ and $x^1 = E(b^1)$ be code words with $d(x, x^1) = r$. Suppose that x^1 precedes x in the list of code words used to define D.
Write $x = b_1b_2\ldots b_n$, $x^1 = b_1^1b_2^1\ldots b_n^1$. Then $b_i \ne b_i^1$ for exactly r integers i between 1 and n. Assume that $b_1 \ne b_1^1, \ldots, b_r \ne b_r^1$, but $b_i = b_i^1$ when $i > r$. Any other case handled in the similar way.

We now recollect the statement of Lagranges' theorem
(Statement: Let G be a finite group and let H a subgroup of G. Then O(G)/O(H) = [G:H] is the number of distinct left cosets of H in G). In particular, the number of elements in H must divide the number of elements in G.

14.6.11 Coset Decoding: A linear code C is a subgroup of Z_2^n. Coset or standard decoding uses the cosets of C in Z_2^n to implement maximum-likelihood decoding. Suppose that C is an (n, m) linear code. A coset C of Z_2^n is written in the form x + C, where x ∊ Z_2^n . By Lagranges theorem, there are 2^{n-m} distinct cosets of C in Z_2^n. An n-tuple of least weight in a coset is called a *coset leader*.

14.6.12 Example: Let C be the (5, 3) linear code given by the parity check matrix

$H = \begin{pmatrix} 01100 \\ 10010 \\ 11001 \end{pmatrix}$. The code consists of the codewords (00000) (01101) (10011) (11110). There are

$2^{5-2} = 2^3$ cosets of c in Z_2^5, each with order $2^2 = 4$. These cosets are listed in the following table.

	Cosets
C	(00000) (01101) (10011) (11110)
(10000) + C	(10000) (11101) (00011) (01110)
(01000) + C	(01000) (00101) (11011) (10110)
(00100) + C	(00100) (01001) (10111) (11010)
(00010) + C	(00010) (01111) (10001) (11100)
(00001) + C	(00001) (01100) (10010) (11111)
(10100) + C	(00111) (01010) (10100) (11001)
(00110) + C	(00110) (01011) (10101) (11000)

Self Assessment Question 6: Compute the hamming distances between the following pairs of n-tuples (i) (011010), (011100) (ii) (00110), (01111).

Self Assessment Question 7: Consider the encoding function E: $B^2 \to B^5$ defined by E(00) = 00000, E(01) = 01110, E(10) = 00111, E(11) = 11111. What is the minimum distance of the code words.

Self Assessment Question 8: Verify that the (3, 7) encoding function defined by E(000) = 0000000, E(001) = 0010110, E(010) = 0101000, E(011) = 0111110, E(100) = 1000101, E(101) = 1010011, E(110) = 1101101, E(111) = 1111011, is a group code.

Self Assessment Question 9: With doing any addition, explain why the following set of 4-tuples in Z_2^4 cannot be a group code.

(0110) (1001) (1010) (1100)

Self Assessment Question 10: Determine the (3, 6) encoding function corresponding to the parity-check matrix H = $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

14.7 Answers to Self Assessment Questions

SAQ 1.

Consider $(a+b)^2 = (a + b)\,(a + b) = a(a + b) + b(a + b) = a^2 + ab + ba + b^2$

SAQ2.

Let $a \in R$. Consider $a^2 + a^2 = a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2$.

Therefore $a^2 + a^2 = a^2 + a^2 + a^2 + a^2$

$\Rightarrow 0 = a^2 + a^2 = a + a$

$\Rightarrow a = -a$---- (1).

Now for any $a, b \in R$ consider

$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$

$\Rightarrow 0 = ab + ba$

$\Rightarrow ab = -ba = ba$ (by the condition (1)). Hence R is commutative.

SAQ 3.

(i) Consider $0 + \phi(0) = \phi(0) = \phi(0 + 0) = \phi(0) + \phi(0) \Rightarrow \phi (0) = 0$.

(ii) $0 = \phi(0) = \phi(a + (-a)) = \phi(a) + \phi(-a) \Rightarrow \phi(-a) = -\phi(a)$.

SAQ4.

Given c = 1010110 $\in Z_2^7$ and error pattern E = 0101101 $\in Z_2^7$.

Therefore the received word is r = c + E = 1010110 + 0101101 = 1111011

(where + is the addition in Z_2^7, that is addition is component wise,

1+1 = 0, 1+0 = 1, 0+1 = 1, 0+0 = 0).

It is clear that r differs from c in the second, fourth, fifth and seventh places (total 4 places).

SAQ 5.

The error pattern E is given by r = c + E, where + is the component wise addition in Z_2^7. Let E = $e_1 e_2 \ldots e_7$, we have r = c + $e_1 e_2 \ldots e_7$.

This implies 1011111 = 1010110 + $e_1 e_2 \ldots e_7$.

Since the addition is component wise in Z_2^7, we have $1 = 1 + e_1 \Rightarrow e_1 = 0$, $0 = 0 + e_2 \Rightarrow e_2 = 0$, $1 = 1 + e_3 \Rightarrow e_3 = 0$, $1 = 0 + e_4 \Rightarrow e_4 = 1$, $1 = 1 + e_5 \Rightarrow e_5 = 0$, $1 = 1 + e_6 \Rightarrow e_6 = 0$, $1 = 0 + e_7 \Rightarrow e_7 = 1$. Therefore E = 0001001.

SAQ6.

(i) 2, (ii) 2.

SAQ 7.

The minimum distance is 2.

SAQ 8.

The set $E(B^3)$ = {0000000, 0010110, 0101000, 0111110, 1000101,1010011, 1101101, 1111011} is closed, 0000000 is the identity element and each element is its own inverse. Therefore $E(B^3)$ is a subgroup of B^7 and hence a group code.

SAQ 9.

(0000) $\notin$ C.

SAQ10.

$E_H(000) = 000000$, $E_H(001) = 001111$, $E_H(010) = 010011$, $E_H(011) = 011100$, $E_H(100) = 100100$, $E_H(101) = 101011$, $E_H(110) = 110111$, $E_H(111) = 111000$.

14.8 Summary

This lesson provides the brief idea about the encoding and decoding the messages in a transmitted channel. This concept is an application of modern algebra. The student able to apply the concepts of semigroups, groups, cosets and several useful algebraic techniques in sending messages in terms of encoding and decoding functions. Parity check is useful in solving practical problems in communications systems.

14.8 Technical Terms

Ring: *A* non empty set *R* is said to be a *ring* (or an associative ring) if there exists two operations + and "."on *R* such that (i) (R, +) is an abelian group (ii) (R, .) is a semi-group and (iii) for any $a, b, c \in R$ we have $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

Division ring: Let (R^*,.) is a group (here $R^* = R - \{0\}$). *A* division ring is said to be a *field* if it is commutative (we will learn this concept in the next section).

The Pigeon Hole Principle: If *a* objects are distributed over *m* places and if $a > m$, then some place receives at least two objects.

Homomorphism: *A* mapping $\phi : R \to \mathrm{R}^1$ is said to be a *homomorphism (or* a *ring-homomorphism)* if (i) $\phi(a + b) = \phi(a) + \phi(b)$, (ii) $\phi(ab) = \phi(a)\,\phi(b)$ for all $a, b \in R$.

Hamming distance: or distance d(x,y), between x and y is the number of bits in which x and y differ.

The minimum distance: d_{min} = min. {d(x,y) | where x and y are distinct code words}.

The weight of the Code word: W(x) of a binary code word x is the number of 1's in x. It is also denoted by | x. It is clear that w(x) = d(x, 0) where 0 = (00…0).

Group Code: Let E: $Z_2^m \to Z_2^n$, n > m be an encoding function and C = {E(w)| w∈ Z_2^m} be the set of codes. Then C is called a *group code* if C is a subgroup of Z_2^n.

Null space: The matrix $H \in M_{m\times n}(Z_2)$ defined to be the set of all binary n-tuples x such $H\otimes x = 0$. We denote the null space of a matrix H by Null (H).

Linear Code: A code is a *linear code* if it is determined by the null space of some matrix $H \in M_{m\times n}(Z_2)$.

Parity Check Matrix: Let m < n and r = n –m. An n × r Boolean matrix:

$$\begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1r} \\ h_{21} & h_{22} & \cdots & h_{2r} \\ \vdots & & & \\ h_{m1} & h_{m2} & \cdots & h_{mr} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

is called a parity check matrix, whose last r rows form an r × r identity matrix.

14.10 Model Questions

1. Compute the weighs of the following n-tuples
(i) (011010), (ii) (01111).

2: In each of the following codes, what is the minimum distance (that is, d_{min})for the code
(i) (011010) (011100) (110111) (110000)
(ii) (000000) (011100) (110101) (110001)

3: An encoding function E: $Z_2^3 \to Z_2^4$ is defined by the generator matrix $G = \begin{pmatrix} 1001 \\ 0101 \\ 0011 \end{pmatrix}$

(i) Find the set of all code words assigned by E.

(ii) Determine the associated parity-check matrix.

4: For an encoding function $E: Z_2^4 \to Z_2^6$, the parity check matrix is given by H = $\begin{pmatrix} 101010 \\ 110101 \end{pmatrix}$.

Decode the received words: 010101, 111010, 111110.

5. Let $x = y_1y_2\ldots y_m\, x_1x_2\ldots x_r \in B^n$. Then $x \otimes H = \mathbf{0}$ (that is $x \in N$) if and only if $x = E_H(b)$ for some $b \in B^m$.

6. Suppose that E is an (m, n) encoding function and D is a maximum likelihood decoding function associated with E. Then (E, D) can correct k or fewer errors if and only if the minimum distance of E is at least 2k+1.

14.11 References

1. Akerkar Rajendra and Akerkar Rupali. “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Fraleigh J.B. “A First Course in Abstract Algebra”, Narosa Publ. House, New Delhi, 1992

3. Hari Kishan and Shivraj Pundir “Discrete Mathematics”, Pragati Prakashan, Meerut, 2005.

4. Herstein I. N. “Topics in Algebra”, Blaisdell, New York, 1964.

5. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. “Quantitative Methods”, Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

6. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

7. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr Kuncham Syam Prasad**

Lesson 15

Residue Arithmetic

Objectives

At the end of the Lesson the student must be able to:

(i) Know the basics of number theory.
(ii) Understand the prime factorization of integers.
(iii) Apply the Fermat's and Euler theorems.
(iv) Learn the residues and mixed-base system.

Structure

15.1 Introduction

The integers are the building blocks of mathematics. In this lesson we will study the properties of divisibility, prime factorizations. The applications of number theory are in the fields of efficient algorithms, cryptography and other computer related branches. We introduce the residue number system, which is an alternative to the fixed-base number systems, like decimal and binary number systems. The fixed-base number systems in digital computers have many advantages.

15.2 Divisibility

15.2.1 Definition: (**Principle of induction**) If Z is a set of integers such that

$a)$ $1 \in Z,$

$b)$ $n \in \mathrm{Z} \quad \Rightarrow \; n+1 \in Z,$

then all integers greater than equal to 1 belongs to Z.

15.2.2 Definition: (**The Well Ordering Principle)** If A is a non-empty set of positive integers, then A contains a smallest member.

15.2.3 Definition: For two integers d and n, we say that d *divides* n (we write $d \mid n$) if $n = cd$ for some integer c. In this case we also say that d is a *factor* of n. If d does not divide n, we write $d \nmid n$.

15.2.4 Properties of divisibility:

(i) $n \mid n$ (reflexive property)

(ii) $d \mid n$ and $n \mid m \Rightarrow d \mid m$ (transitive property)

(iii) $d \mid n$ and $d \mid m \Rightarrow d \mid an + bm$ for any two integers a and b (linearity)

(iv) $d \mid n \Rightarrow ad \mid am$ (multiplication property)

(v) $ad \mid an$ and $a \neq 0 \Rightarrow d \mid n$ (cancellation law)

(vi) $1 \mid n$ (1 divides every integer)

(vii) $n \mid 0$ (every integer divides zero)

(viii) $0 \mid n \Rightarrow n = 0$ (zero divides only zero)

(ix) $d \mid n$ and $n \neq 0 \Rightarrow |d| \leq |n|$ (comparison property)

(x) $d \mid n$ and $n \ |d \Rightarrow |d| = |n|$

(xi) $d \mid n$ and $d \neq 0 \Rightarrow (n / d) \mid n$.

15.2.5 Definition: (i) If $d \mid n$, then $\frac{n}{d}$ is called the **divisor conjugate to d**.

(ii) If d divides both a and b, then d is called a **common divisor** of a and b.

(iii) If $d \geq 0$, d is *a* divisor of a and b and c is a **divisor** of a and b, implies c divides d; then d is called the **greatest common divisor (gcd)** of a and b.

15.2.6 Definition: Every pair of integers a and b have *g.c.d.* If d is the greatest common divisor of a and b, then $d = ax + by$ for some integers x and y. The *g.c.d* of a, b is denoted by (a, b) or by $a\mathrm{D}b$. If $(a, b) = 1$, then *a* and *b* are said to be **relatively prime**.

15.2.7 Properties: (of greatest common divisor):

(i) $(a, b) = (b, a)$ or $a\mathrm{D}b = b\mathrm{D}a$ (commutative law)

(ii) $(a, (b, c)) = ((a, b), c)$ (associative law)

(iii) $(ac, bc) = |c|(a, b)$ (distributive law)

(iv) $(a, 1) = (1, a) = 1$ and $(a, 0) = (0, a) = |a|$.

15.2.8 Euclid's lemma: If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

15.2.9 Definition: (i) An integer n is said to be **prime** if $n > 1$ and if the only positive divisors of n are 1 and n.

(ii) If $n > 1$ and n is not prime, then n is called **composite number**.

15.2.10 Note: (i) (**Euclid**) There are infinite number of prime numbers.

(ii) If *a* prime p does not divide a, then $(p, a) = 1$.

(iii) If *a* prime p divides ab, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_{1.} a_2 \ldots a_n$, then $p \mid a_i$ for at least one i.

15.2.11 Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be written as a product of prime factors in only one way, apart from the order of the factors.

[*Example*: $3000 = 2 \times 2 \times 2 \times 5 \times 5 \times 5 \times 3 = 2^3.5^3.3^1$]

15.2.12 Note: (i) Let n be an integer. If the distinct prime factors of n are $p_1, p_2, \ldots p_r$ and if p_i occurs as a factor a_i times, then we write

$$n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_r^{a_r} \text{ or } n = \prod_{i=1}^{r} p_i^{a_i}$$

and is called the *factorization* of n into prime powers.

(ii) We can express 1 in this form by taking each exponent a_i to be zero.

(iii) If $n = \prod_{i=1}^{r} p_i^{a_i}$, then the set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^{r} p_i^{c_i}$, where $0 \le c_i \le a_i$ for $i = 1, 2, \ldots, r$.

(iv) If two positive integers a and b have the factorization $a = \prod_{i=1}^{r} p_i^{a_i}$, $b = \prod_{i=1}^{r} p_i^{b_i}$, then their *g.c.d.* has the factorization $(a, b) = \prod_{i=1}^{r} p_i^{c_i}$ where $c_i = \min\{a_i, b_i\}$

15.2.13 Division Algorithm: Given integers a and b with $b > 0$. Then there exists a unique pair of integers q and r such that $a = bq + r$, with $0 \le r < b$. Moreover, $r = 0 \Leftrightarrow b \mid a$.

Self Assessment Questions:

1. Find the *gcd* of 858 and 325.

2. If $a|c$ and $b|c$, then is it true that "$ab|c$"?

3. If gcd of $\{a, b\} = 1$, then what is the *gcd* of $a + b$ and $a - b$ is?

4. Are every two consecutive integers are co-prime?

15.2.14 Euclidean Algorithm: Given positive integers a and b, where $b \nmid a$. Let $r_0 = a$, $r_1 = b$ and apply the division algorithm repeatedly to obtain a set of remainders $r_2, r_3, \ldots, r_n, r_{n+1}$ defined successively by the relations

$r_0 = r_1q_1 + r_2$ $\quad 0 < r_2 < r_1$,

$r_1 = r_2q_2 + r_3$ $\quad 0 < r_3 < r_2$

……

$r_{n-2} = r_{n-1}q_{n-1} + r_n$ $\quad 0 < r_n < r_{n-1}$

$r_{n-1} = r_nq_n + r_{n+1}$ $\quad r_{n+1} = 0$

Then r_n, the last non zero remainder in this process, is the *g.c.d.* of a and b.

15.2.15 Definition: The greatest common divisor of three integers a, b, c is denoted by (a, b, c) and is defined as $(a, b, c) = (a, (b, c))$.

Note that from the properties of *g.c.d*, we have $(a, (b, c)) = ((a, b), c)$. So the *g.c.d.* depends only on a, b, c and not on the order in which they are written.

15.2.16 Definition: The *g.c.d.* of n integers $a_1, a_2, \ldots, a_n$ is defined inductively by the relation $(a_1, a_2, \ldots, a_n) = (a_1, (a_2, \ldots, a_n))$. Again this number is independent of the order in which the a_i appear.

15.2.17 Note: If $d = (a_1, a_2, \ldots, a_n)$, then d is a linear combination of the a_i. That is, there exist integers $x_1, x_2, \ldots, x_n$ such that $(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$.

(ii) If $d = 1$, then numbers are said to be *relatively prime*.

(iii) If $(a_i, a_j) = 1$ whenever $i \neq j$, then the numbers $a_1, a_2, \ldots, a_n$ are said to be *relatively prime in pairs*.

(iv) If $a_1, a_2, \ldots, a_n$ are relatively prime in pairs, then $(a_1, a_2, \ldots, a_n) = 1$.

15.2.18 Problem: If $p > 1$ and $2^p - 1$ is prime, then p is prime. Is the converse true? Justify.

Solution: If p is not prime, then $p = mn$, where $m, n > 1$.

Therefore $2^p - 1 = 2^{mn} - 1 = (2^m)^n - 1^n$. Take $2^m = a$.

Now $2^m = a = a^n - 1^n$ where $a = 2^m > 2$

$$= (a - 1)(a^{n-1} + a^{n-2} + \ldots + 1^{n-1})$$

Now each of the two factors on right hand side is greater than 1 and therefore $2^p - 1$ is composite, a contradiction.

Converse is not true: For example, take $p = 11$ is prime, but $2^{11} - 1$ is divisible by 23 and so it is not prime.

15.3 Residue Arithmetic

We introduce the residue number system. It is an alternative to the fixed-base number systems, like decimal and binary number systems. The fixed-base number systems in digital computers have many advantages. However these systems have speed restrictions in performing arithmetic operations. The residue number system does not have many advantages of fixed-base systems. However addition, subtraction and multiplication can be performed on a 'residue computer' in less time. But the residue number system has the following disadvantages, too.

1. Comparison of numbers is difficult.
2. It is difficult to determine overflow.
3. Division is complex.
4. Not convenient to represent fractions.

Now, let us introduce residue number system. Let m be a positive integer. From unique factorization theorem, we have $m = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} = m_1 m_2 \ldots m_r$

where p_i are prime numbers and n_i are positive integers for i = 1, 2, :.., r and $m_i = p_i^{n_i}$.

Clearly g.c.d. $(m_i, m_j) = 1$ for $i \neq j$. That is, $m_1 m_2 ... m_r$ are relatively prime.

15.3.1 Definition: Let x be any number in Z_m and let x_i = x mod m_i, for i = 1, 2, ..., r. Then the r-tuple $(x_1, x_2, ..., x_r)$ is called the residue or the modular representation of x.

Modular representation of any element $x \in Z_m$ is an r-tuple in $Z_m^* = Z_{m_1} \times Z_{m_2} \times ... \times Z_{m_n}$. There are m = $m_1 m_2 ... m_r$ elements in Z_m^*.

15.3.2 Theorem: (**Chinese remainder theorem**). There exists a one-to-one correspondence between Z_m and Z_m^*.

Proof: Let g: $Z_m \rightarrow Z_m^*$ be such that $g(x) = (x_1, x_2, \ldots, x_r)$

$= (x \bmod m_1, x \bmod m_2, ..., x \bmod m_r)$.

First, we prove g is one-to-one. If possible let $x \neq y$ and g(x) = g(y) for some x,y, $\in Z_m$. That is, x mod m_i = y mod m_i for i = 1,2, ..., r. This means (x-y) is divisible by m_i for each i or (x-y) is divisible by m since m_i^{-1}'s are pair-wise relatively prime. This is, a contradiction as (x - y) is not divisible by m. Therefore, g is one-to-one.

Since Z_m and Z_m^* have the same number of elements, g is onto. Hence the proof.

15.3.3 Note: From the above Theorem, it follows that the residue representation of any number in Z_m is unique and conversely.

15.3.4 Example: Let m = 15. Then m = 3 × 5 so that $m_1 = 3$ and $m_2 = 5$ and $Z_{15}^* = Z_3 \times Z_5$. The residue representation for the numbers in Z_{15} is given in Table.

x	3	5	x	3	5
0	0	0	8	2	3
1	1	1	9	0	4
2	2	2	10	1	0
3	0	3	11	2	1
4	1	4	12	0	2
5	2	0	13	1	3
6	0	1	14	2	4
7	1	2			

Now let us define addition and multiplication on Z_m^* in terms of the corresponding operations in Z_{m_i} for i = 1, 2, ..., r.

Let x, y $\in Z_m$ and $(x_1, x_2, ..., x_r)$ and $(y_1, y_2, ..., y_r)$ in Z_m^* be their residue representations. Then, we define

$(x_1, x_2, ..., x_r) \oplus_m (y_1, y_2, ..., y_r)) = (x_1 +_{m_1} y_1, x_2 +_{m_2} y_1, \dots, x_r +_{m_r} y_r)$

$(x_1, x_2, ..., x_r) \otimes_m (y_1, y_2, ..., y_r)) = (x_1 \times_{m_1} y_1, x_2 \times_{m_2} y_1, \dots, x_r \times_{m_r} y_r)$

In a similar manner, we can define subtraction.

Observation: $(Z_{m_i}, +_{m_1})$ are cyclic groups. Hence $(Z_m^*, \otimes_m)$ is also a cyclic group.

15.3.5 Theorem: The mapping g: $Z_m \to Z_m^*$ is an isomorphism.

The proof is out of the scope of the book.

15.3.6 Example: Let m = 15, x =6 and y = 11.

From the above table, we get g(x) = g(6) = (0, 1)

g(y) = g(11) = (2, 1)

Therefore $g(6) \oplus_{15} g(11) = (0 +_3 2, 1 +_5 1) = (2, 2) = g(2) = g(6 +_{15} 11)$.

Similarly, $g(6) \otimes_{15} g(11) = (0 \times_3 2, 1 \times_5 1) = (0, 1) = g(6) = g(6 \times_{15} 11)$.

Note that when m is large, it is difficult to construct the table of residue digits.

15.3.7 Theorem: (Cancellation law of multiplication): Let $c \in Z_m$ and g.c.d $(c, m) = 1$. Then for any two elements $a, b \in Z_m$, $(c\, a) \bmod m = (c\, b) \bmod m \Rightarrow a \bmod m = b \bmod m$.

Proof: Let $c\, a = pm + r_1$ and $cb = qm + r_2$. Then
$(c\, a) \bmod m = (c\, b) \bmod m \Rightarrow r_1 = r_2$
$\Rightarrow ca - pm = cb - qm$
$\Rightarrow c(a-b) = (p-q)m$.
Therefore c(a-b) is divisible by m.
Since gcd $(c, m) = 1$, it follows that (a-b) is divisible by m. That is,
$a \bmod m = b \bmod m$.

15.3.8 Corollary: If gcd $(a, m) = 1$, then the equation of the form $(a\, x) \bmod m = b \bmod m$ has a unique solution for x mod m.

15.3.9 Definition: For $0 \leq a < m$, if there exists a' such that $(a'a) \bmod m = 1$, then a^1 is called the multiplicative inverse of a.

15.3.10 Theorem: Multiplicative inverse a' exists and is unique if and only if gcd $(a, m) = 1$ and $a \neq 0$.

15.3.11 Example: The following table gives the inverses of elements in Z_5 and Z_8.

m = 5		**m = 8**	
A	a'	a	a'
1	1	1	1
2	3	2	none
3	2	3	3
4	4	4	none
		5	5
		6	none
		7	7

15.3.12 Theorem: (Fermat's Theorem): If a is an integer and m is a prime then a^m mod m = a mod m.

Proof: (By induction on a)

Case (i): a = 0. Then the theorem is clearly true.

Case (ii) Induction Hypo: Assume that the theorem is true for a = k.

That is k^m mod m = k mod m.

Now from Binomial theorem,

$(k + 1)^m = k^m + \frac{m}{1!}k^{m-1} + \frac{m(m-1)}{2!}k^{m-2} + \ldots + 1$

Since m is prime, each term except the first and last in the RHS is a multiple of m and it follows that

$(k + 1)^m$ mod m = $(k^m + 1)$ mod m.

Using induction hypothesis, we get

$(k +1)^m$ mod m = (k +1) mod m.

Hence from the principle of mathematical induction, the theorem is true for all non-negative integers. This can be extended to all integers.

15.3.13 Note: (i) Fermat's theorem can be proved using Lagrange's theorem for finite groups.

(ii) $a' = a^{m-2}$ mod m, when m is a prime.

15.3.14 Example: Let m = 7. We get $2' = 2^5$ mod 7 = 32 mod 7 = 4 and $3' = 3^5$ mod 7 = 243 mod 7 = 5.

15.3.15 Note: The above formula can be used only when m is a prime. We will generalize this formula to compute the inverse even, when m is not a prime.
We define f(p) = Number of elements in {1, 2, …, p-1}, which are relatively prime to p.
Thus f(2) = 1, f(3) = 2, f(4) = 2, ….
If p is a prime then f(p) = p -1. Also $f(p^n) = p^n - p^{n-1}$, where n is positive integer. Thus
$f(8) = f(2^3) = 2^3 - 2^2 = 4$.

Self Assessment Question 5: Compute the inverse of each element in Z_5 using Fermat's theorem.

15.3.16 Theorem: (Euler): Let a and m are positive integers which are relatively prime. Then $a^{f(m)}$ mod m = 1. Hence $a' = a^{f(n)-1}$mod m.

Proof: Let a and b are positive integers which are relatively prime to m. Then gcd (a, m) = gcd (b, m) = 1.
We will prove that gcd ((a b) mod m, m) = 1.
Suppose the converse is true. Let gcd ((a b) mod m, m) = ·, where d > 1.
That is, · divides both (a b) mod m and m.
d dividing (a b) mod m ⇒ either · divides a or d divides b ⇒ gcd (a, m) = d or gcd(b, m) = d.
This is a contradiction.
Therefore, (a b) mod m and m are relatively prime.

Now let $\{z_1, z_2, \ldots, z_{f(m)}\}$ be the set of distinct elements which are relatively prime to m. This set is same as $\{(a\ z_1) \bmod m, (a\ z_2) \bmod m, \ldots, (a\ z_{f(m)}) \bmod m\}$ in some order, where $0 < a < m$ and a is relatively prime to m.

This means the set $\{z_1, z_2, \ldots, z_{f(m)}\}$ is a group of order f(m) with respect to multiplication. By using Lagrange's theorem, it can be verified that every element a of this group satisfies, $a^{f(m)} \bmod m = 1$. Hence the theorem.

15.3.17 Note: The inverse can be computed using the formula,

$$a' = a^{f(m)-1} \bmod m.$$

15.3.18 Example: For m = 8 and a = 3, we have $3' = 3^{4-1} \bmod 8 = 27 \bmod 8 = 3$, since f(8) = 4.

Self Assessment Question 6: Compute the inverse of each element in Z_{12} using Euler's theorem.

15.3.19 Note: Fermat's theorem is a special case of Euler's theorem with f(m) = m – 1, when m is a prime.

Now, we will give an explicit procedure for determining the $z \in Z_m$, which corresponds to a given element in Z_m^*.

Let $\tilde{m}_i \in Z_m$ for i = 1, 2, …, r be such that their residue representation has 1 in the ith component and a 0 in all other components. That is,

$$\tilde{m}_i \bmod m_i = 1 \text{ and } \bmod \tilde{m}_i = 0 \text{ for } i \neq j.$$

Then for any number $(x_1, x_2, \ldots, x_r) \in Z_m^*$ we can write the corresponding number $x \in Z_m$ as

$$x = \left(\sum_{i=1}^{r} \tilde{m}_i x_i\right) \bmod m$$

15.3.20 Example: Let m = 30 so that $m_1 = 2$, $m_2 = 3$ and $m_3 = 5$.

$$\hat{m}_1 = \left(\frac{30}{2}\right)^{f(2)} \bmod 30 = 15$$

$$\hat{m}_2 = \left(\frac{30}{2}\right)^{f(3)} \bmod 30 = 10^2 \bmod 30 = 10$$

$$\hat{m}_3 = \left(\frac{30}{2}\right)^{f(5)} = 6^4 \bmod 30 = 6$$

Hence for $(x_1, x_2, x_3) \in Z_{30}^*$, $x = (15x_1 + 10x_2 + 6x_3) \bmod 30$.

For $(1, 1, 2) \in Z_{30}^*$, $x = (15 \times 1 + 10 \times 1 + 6 \times 2) \bmod 30 = 7$.

15.3.21 Definition: The above method involves operations modulo m which is not suitable for a computer which uses operation modulo m_i. So we give a new formulation called **mixed-base number system**.

15.4 Mixed-base number system

In this system, any number $x \in Z_m$ can be represented by $x = a_r \prod_{j=1}^{r-1} m_j + \ldots + a_3 m_1 m_2 + a_2 m_1 + a_1$

where $m = m_1 m_2 \ldots m_r$, each mixed-base digit a_i is in the interval $0 \le a_i < m_\cap$ and weight w_i of each a_i is given by

$$\prod_{j=1}^{r-1} m_j \text{ for i = 2, 3, …, r.}$$

Any positive integer in the interval $0 \le x < \prod_{i=1}^{r} m_i$ can be represented in this system uniquely.

15.4.1 Note: The system reduces to decimal number system when $m_i = 10$ for all i. The mixed-base digits $a_1, a_2, \ldots, a_r$ can be obtained sequentially in the following manner:

Let $(x_1, x_2, \ldots, x_r) \in Z_m^*$. Then $a_1 = x \bmod m_1 = x_1$

$a_2 = (x_2 - a_1)\, c_{12} \bmod m_2$

$a_3 = [(x_3 - a_1)c_{13} - a_2]\, c_{23} \bmod m_3$

$a_i = ((\ldots(x - a_1)c_{1i} - a_2)c_{2i} - \ldots a_{i-1})c_{i-1,\, i} \bmod m_i$ for $1 < i \le r$ where $c_{ij} = m_i^{f(m_i)-1} \bmod m_j$ for $1 \le i < j \le r$.

15.4.2 Example: Let m = 30 so that $m_1 = 2$, $m_2 = 3$, $m_3 = 5$. Also, let $x = (x_1, x_2, x_3) = (1, 1, 4)$. Then

$c_{12} = m_1^{f(m_2)-1} \bmod m_2 = 2^{f(3)-1} \bmod 3 = 2^{2-1} \bmod 3 = 2 \bmod 3.$

$c_{13} = m_1^{f(m_3)-1} \bmod m_3 = 2^{4-1} \bmod 5 = 3 \bmod 5.$

$c_{23} = m_2^{f(m_3)-1} \bmod m_3 = 3^{f(5)-1} \bmod 5 = 3^3 \bmod 5 = 2 \bmod 5.$

$a_1 = x_1 = 1$

$a_2 = (x_2 - a_2)\, c_{12} \bmod m_2 = (1-1)\, 2 \bmod 3 = 0$

$a_3 = [(x_3 - a_1)c_{13} - a_2]\, c_{23} \bmod m_3 = [(4-1)3 - 0]2 \bmod 5 = 3.$

Then for unique factorization theorem,

$$m = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} = m_1 m_2 \ldots m_r$$

Then $x = 6a_3 + 2a_2 + a_1 = 6 \times 3 + 2 \times 0 + 1 = 19.$

15.5 Answers to Self Assessment Questions

SAQ 1.

gcd of 858 and 325 is 13.

SAQ2.

If it is not true. For example, take $a = 3$, $b = 6$, $c = 12$. Now $3|12$ and $6|12$ but $3.6 \nmid 12$.

SAQ 3.

Either 1 or 2.

SAQ 4.

Yes, the *gcd* of $\{n, n+1\}$, $n \in \mathbb{Z}$ is equal to 1.

SAQ5.

The inverse of 1 = 1, the inverse of 2 = 3, the inverse of 3 = 2, the inverse of 4 = 4.

SAQ 6.

The inverse of 1 = 1, the inverse of 5 = 5, the inverse of 7 = 7, the inverse of 11 = 11.

15.6 Summary

In this lesson we have studied the basic number theory. We studied some important theorems like Fermat's and Euler's with suitable examples. Finding of inverse elements using these theorems were illustrated. Applications of Chinese remainder theorem in modular arithmetic has key role in cryptography and in analysis of algorithms. The mixed number system also introduced in this lesson.

15.7 Technical Terms

The Well Ordering Principle: If A is a non-empty set of positive integers, then A contains a smallest member.

Euclid's lemma: If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be written a*s* a product of prime factors in only one way, apart from the order of the f*ac*tors.

Division Algorithm: Given integers a and b with $b > 0$. Then there exists *a* unique pair of integers q and r such that $a = \mathrm{bq} + r$, with $0 \leq r < b$. Moreover, $r = 0 \Leftrightarrow b \mid a$.

Chinese remainder theorem: There exists a one-to-one correspondence between $\mathrm{Z_m}$ and Z_m^*.

Fermat's Theorem: If a is an integer and m is a prime then $\mathrm{a^m}$ mod m = a mod m.

Euler: Let a and m are positive integers which are relatively prime. Then $\mathrm{a^{f(m)}}$ mod m = 1. Hence $\mathrm{a' = a^{f(n) - 1}}$mod m.

Mixed based system: The method involves operations modulo m which is not suitable for a computer which uses operation modulo $\mathrm{m_i}$. So we give a new formulation called mixed-base number system.

15.8 Model Questions

1. State and Prove Fermat's theorem.

2. State and Prove Euler's theorem.

3. Give the residue representation of all integers in Z_{60} with $m_1 = 4$, $m_2 = 3$, and $m_3 = 5$.

4. Explain the mixed base number system.

15.9 References

1. Akerkar Rajendra and Akerkar Rupali. "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, "Discrete Mathematical Structures" PHI, New Delhi, 1999.

3. Shanker Rao, G., "Discrete Mathematical Structures", New Age International Publishers, New Delhi, 2002.

4. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

5. Trembly, J.P., and Manohar, R. "Discrete Mathematical Structures with Applications to Computer Science", Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Mr. T. V. Pradeep Kumar**

Lesson 16

Partially Ordered Sets and Lattices

Objectives

At the end of the Lesson the student must be able to:

(i) Know the order relations.
(ii) Diagram representation of partial ordered sets.
(iii) Know the properties of partial order relations

Structure

16.1 Introduction

There are various types of relations defined on a set. In this unit our interest is partially ordered relation which is defined on a set, referred as a partially ordered set. This would lead to the concepts of lattices and Boolean algebras. We discuss the different properties of partial order relations on a set, and representation of posets.

16.2 Partially Ordered Sets

16.2.1 Definition: A relation R on a set A is called a **partial order** if R is reflexive, anti-symmetric and transitive. The set S with a partial order R is called a **partially ordered set** or **Poset** and it is denoted by (A, R). In general, a partial order R on a set is denoted by $\leq$.

Note that if $(a, b) \in R$, then we write $a \geq b$. If $a \geq b$ and $a \neq b$, then we write $a > b$.

16.2.2 Example: Let A = Z^+ the set of all positive integers. Define R on A as aRb if and only if a $\leq$ b. Then (A, $\leq$) is a partially ordered set. It is clear that (A, <) is not a Poset, since it does not satisfy reflexive.

16.2.3 Example:

(i) The relations '$\leq$' and '$\geq$' are the partial orderings on the set of real numbers.

(ii) Let X be the power set of the set A. Then define R on X as S_1RS_2 if and only if $S_1 \subseteq S_2$ for $S_{1,} S_2 \in$ X. Then the relation inclusion '$\subseteq$' is a partial ordering on X.

16.2.4 Example: Let A be a non-empty set and $S = P(A)$, the power set of A.

Define a relation R on S as $R = \{(X, \mathrm{Y}) \ / \ X, \mathrm{Y}$ are in $P(A)$ such that X contains Y$\}$. Now we verify that the relation is reflexive.

For this take $X \in S$. Then X is a subset of A. Since X contains X, we have $(X, X) \in R$. Therefore R is reflexive. To verify the anti-symmetric condition, let $(X, \mathrm{Y}), (\mathrm{Y}, X) \in R$. Then X contains Y, and Y contains X, which imply $X =$ Y. Hence the relation is anti-symmetric. To verify the transitive condition, let $(X, \mathrm{Y}), (\mathrm{Y}, \mathrm{Z}) \in R$. Then X contains Y, and Y contains Z. So X contains Z, which implies $(X, \mathrm{Z}) \in R$. Hence R is transitive. Therefore S is a POset.

Self Assessment Question 1: Determine whether the relation R is a partial ordered on the$\mathbb{Z}$.

(i). a R $b \Leftrightarrow$ a = 2b

(ii). a R $b \Leftrightarrow b^2$ / a, where a, $b \in \mathbb{Z}$.

Self Assessment Question 2: Determine which of the following are equivalence relations and / or partial ordering relations for the given sets.

(i) S = {lines in the plane}; xRy $\Leftrightarrow$ x is parallel to y

(ii) N = {set of natural numbers}; xRy $\Leftrightarrow$ $|x - y| \leq 5$.

16.2.5 Definition: Let (A, $\leq$) be any Poset. Two elements a and b of A are **comparable** if either a $\leq$ b or b $\leq$ a. If every pair of elements is comparable then it is called a **linearly ordered set** or a **chain**. The Poset (Z^+, R) where R is defined on A as aRb if and only if a $\leq$ b is a chain.

16.2.6 Definition: Let $P_1, P_2, \ldots, P_k$ be POsets. The **lexicographic product** of $P_1, P_2, \ldots, P_k$ is defined to be the POset $P_1 \times P_2 \times \ldots \times P_k$ with $(a_1, a_2, \ldots, a_k) < (b_1, b_2, \ldots, b_k)$ if $a_1 < b_1$ or if $a_i = b_i$ for i = 1, …, m and $a_{m+1} < b_{m+1}$ for some $m < k$.

16.2.7 Problem: Prove that the lexicographic product of the POsets $P_1, \ldots, P_k$ is a partial order on $P_1 \times P_2 \times \ldots \times P_k$.

Proof: (i) Now we verify the reflexive property. Let $(a_1, \ldots, a_k) \in P_1 \times \ldots \times P_k$. Since $a_i \leq a_i$, for all $1 \leq i \leq k$, we have that $(a_1, \ldots, a_k) \leq (a_1, \ldots, a_k)$.

(ii) Now we verify the transitive property. Suppose $(a_1, \ldots, a_k) \leq (b_1, \ldots, b_k)$ and $(b_1, \ldots, b_k) \leq (c_1, \ldots, c_k)$.

Case-(i): Suppose $a_i = b_i$ for all $1 \leq i \leq k$.

Then clearly $(a_1, \ldots, a_k) = (b_1, \ldots, b_k) \leq (c_1, \ldots, c_k)$. If $b_i = c_i$, for all $1 \leq i \leq k$, then we have that $(a_1, \ldots, a_k) \leq (b_1, \ldots, b_k) = (c_1, \ldots, c_k)$.

Case-(ii): Suppose $a_1 < b_1$. If $b_1 < c_1$, then $a_1 < c_1$ and hence $(a_1 \ldots a_k) \leq (c_1 \ldots c_k)$.

Case-(iii): Suppose $a_\mathrm{i} = b_\mathrm{i}$ for $1 \le \mathrm{i} \le m$ and $a_{\mathrm{m+1}} < b_{\mathrm{m+1}}$ for $m < \mathrm{k}$.. If $b_1 < c_1$, then $a_1 = b_1 < c_1$ and so $(a_1 \ldots a_\mathrm{k}) \le (c_1 \ldots c_\mathrm{k})$. Otherwise, since $(b_1 \ldots b_\mathrm{k}) \le (c_1 \ldots c_\mathrm{k})$, there exists m^1 such that $b_\mathrm{i} = c_\mathrm{i}$, for all $1 \le \mathrm{i} \le m^1$ and $\mathrm{b}_{\mathrm{m}^1+1} < \mathrm{c}_{\mathrm{m}^1+1}$ for $m^1 < \mathrm{k}$.

If $m < m^1$, then $a_\mathrm{i} = b_\mathrm{i} = c_\mathrm{i}$ for all $1 \le \mathrm{i} \le m$ and $a_{\mathrm{m+1}} < b_{\mathrm{m+1}} \le c_{\mathrm{m+1}}$. If $m > m^1$, then $a_\mathrm{i} = b_\mathrm{i} = c_\mathrm{i}$ for all $1 \le \mathrm{i} \le m^1$ and $a_{\mathrm{m=1}} = \mathrm{b}_{\mathrm{m}^1+1} < \mathrm{c}_{\mathrm{m}^1+1}$.

Hence $(a_1, \ldots, a_\mathrm{k}) \le (c_1, \ldots, c_\mathrm{k})$.

(iii). Now we verify the anti-symmetric property. Suppose $(a_1, \ldots, a_\mathrm{k}) \le (b_1, \ldots, b_\mathrm{k})$ and $(b_1, \ldots, b_\mathrm{k}) \le (a_1, \ldots, a_\mathrm{k})$. If $(a_1, \ldots, a_\mathrm{k}) \ne (b_1, \ldots, b_\mathrm{k})$, then there exists $m <$ k such that $a_\mathrm{i} = b_\mathrm{i}$ for $1 \le \mathrm{i} \le m$ and $a_{\mathrm{m+1}} \ne b_{\mathrm{m+1}}$. If $(a_1, \ldots, a_\mathrm{k}) < (b_1, \ldots, b_\mathrm{k})$, then $a_{\mathrm{m+1}} < b_{\mathrm{m+1}}$. If $(b_1, \ldots, b_\mathrm{k}) < (a_1, \ldots, a_\mathrm{k})$, then $b_{\mathrm{m+1}} < a_{\mathrm{m+1}}$. This imply that $a_{\mathrm{m+1}} < b_{\mathrm{m+1}}$ and $b_{\mathrm{m+1}} < a_{\mathrm{m+1}}$, a contradiction (since $P_{\mathrm{m+1}}$ is a POset and $a_{\mathrm{m+1}}, b_{\mathrm{m+1}} \in P_{\mathrm{m+1}}$). This shows that the relation is

16.2.8 Definition: A finite POset can be diagrammed on the plane. If S is a POset and a, b are in S such that $a > b$ and there is no c in S such that $a > c$ and $c > b$, then we say that **a covers b**.

16.2.9 Example: If a covers b, then represent the point corresponding to a, above the point for b and join the points (This fact is illustrated in the following Fig-1).

Now consider the Fig - 2. In this, we can observe that:

D covers E; B covers C; F covers C; A covers F.

*A*lso note that B joined to E by a sequence of line segments all going downwards.

So we have B $\ge$ E.

Fig-1

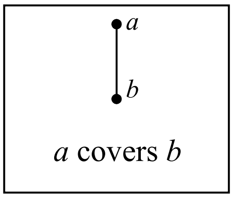
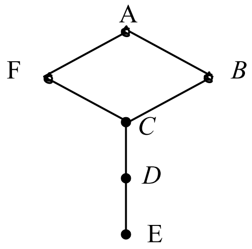


Fig-2



16.2.10 Definition: (i) An element x of a POset S is said to be a **minimal element** if it satisfies the following condition: $y \in S$ and $x \geq y \Rightarrow y = x$..
(ii) An element 'a' of S is said to be a **maximal element** if it satisfies the following condition: $b \in S$ and $b \geq a \Rightarrow b = a$.

16.2.11 Definition: A POset S is said to be a **totally ordered** (or **ordered**) set if for a, b in S exactly one of the conditions: $a > b$, $a = b$, or $b > a$ holds.

16.2.12 Problem: In a finite POset S, show that there is always atleast one maximal element and one minimal element.

Solution: **Part-I**: (For maximal element): In a contrary way, suppose S contains no maximal element. Let $x_1 \in S$. Since x_1 is not maximal, there exists x_2 in S such that $x_2 > x_1$. Since x_2 is not maximal, there exists x_3 in S such that $x_3 > x_2$. If we continue this process, we get an infinite sequence of distinct elements $x_1, x_2, x_3, \ldots$, such that $x_{i+1} > x_i$ for each i. This is a contradiction to the fact that S contains only a finite number of elements (since S is a finite POset). Hence we conclude that S contains a maximal element.
Part-II: This part of the proof is parallel to that of part-I.

16.2.13 Definition: (i) A **chain** in a POset is a sequence $a_0, a_1, \ldots, a_n$ of elements of the POset such that $a_i > a_{i+1}$. The length of this chain is said to be n.

16.2.14 Definition: Let $(P, \geq)$ be a POset and $A \subseteq P$. An element $x \in P$ is called a **lower bound** for A if $a \geq x$, for all $a \in A$. A lower bound x of A is called a **greatest lower bound** of A if $x \geq y$ for all lower bounds y of A.

An element $x \in P$ is called an **upper bound** for A if $x \geq a$, for all $a \in A$. An upper bound x is called a **least upper bound** of A if $b \geq a$ for all upper bounds b of A.

16.2.15 Note: Let R be the set of all real numbers, $\phi \neq A \subseteq R$. If A has a lower bound, then its greatest lower bound is called infimum and it is denoted by $\inf A$. If A has an upper bound, then its least upper bound is called its supremum and it is denoted by $\sup A$.
For any subset A of R (the set of all real numbers), we have that $\inf A = \min A$ and $\sup A = \max A$.

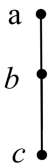
16.2.16 Zorn's Lemma: If P is a partially ordered set in which every chain has an upper bound, then P possesses a maximal element.

16.3 Diagram Representation of Posets

16.3.1 Definition: The **covering matrix** of a finite POset $P = \{p_i \,/\, 1 \leq i \leq n\}$ is the matrix $(b_{i_j})_{n \times n}$ where $b_{i_j} = 1$ if p_i covers p_j or $i = j$;

$= 0$ otherwise.

16.3.2 Example: The diagram of a POset was given on the right side. The covering matrix of this POset is given by $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$.



16.3.3 Note: (i) The chain $p_0 > p_1 > p_2 > \ldots > p_k$ is said to have **length** k.

(ii) An element p of a finite POset is on **level** k if there exists a sequence $p_0 > p_1 > \ldots > p_k = p$ and any other such sequence has length less than or equal to k.

(iii) Suppose p is on level k and $p_0 > p_1 > \ldots > p_k = p$. Then p_0 is a maximal element of the POset. (if p_0 is not maximal, then there exists p^1 such that $p^1 > p_0$.

Then $p^1 > p_0 > p_1 > \ldots > p_k$ is of length $(k + 1)$, a contradiction to the fact p is on level k).

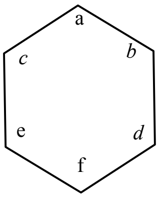
(iv) Fix j. An element p_j is maximal $\Leftrightarrow$ p_j has no cover $\Leftrightarrow$ $b_{i_j} = 0$ for all $i \neq j$ and $i = 1, 2, \ldots, n$. $\Leftrightarrow$ j^{th} column of (b_{i_j}) contains 1 in the j^{th} row and 0 else where.

$\Leftrightarrow$ The sum of the elements in the j^{th} column is 1.

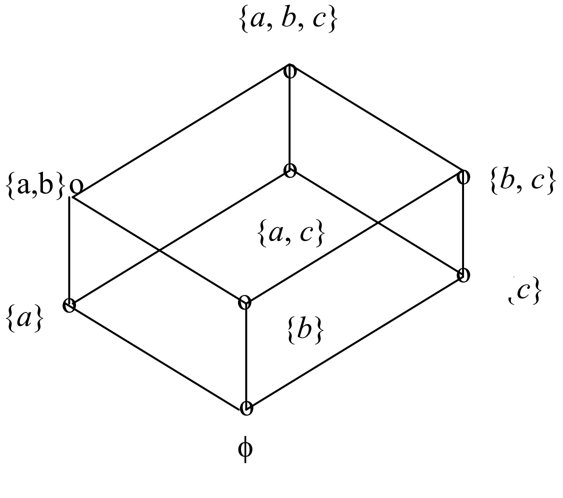
(v) If the sum of the elements of the j^{th} column of the covering matrix is "1", then the corresponding j^{th} element is a maximal element (that is, the element is of level 0).

16.3.4 Definition: A partial ordering $\leq$ on A poset, represented by a diagram called **Hasse diagram**. In a Hasse diagram, each element is represented by a small circle.

16.3.5 Example: Consider the POset with the diagram. Here a is of level 0; b is of level 1; c is of level 1; d is of level 2; e is of level 2; f is of level 3.

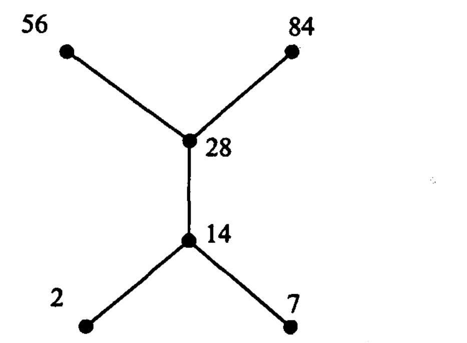


16.3.6 Example: Let $A = \{a, b, c\}$. Then $p(A) = \{ \phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$. Consider the poset $(p(A), \subseteq)$. Then Hasse diagram is shown below.



16.3.7 Example: Let A = {2, 7, 14, 28, 56, 84) and a $\leq b$ if and only if a divides b. Then Hasse diagram for the poset $(A, \leq)$ is

Since 2 divides 14, we join 2 and 14 with a line segment; 7 divides 14 so we join 7 and 14 by a line segment; and so on.

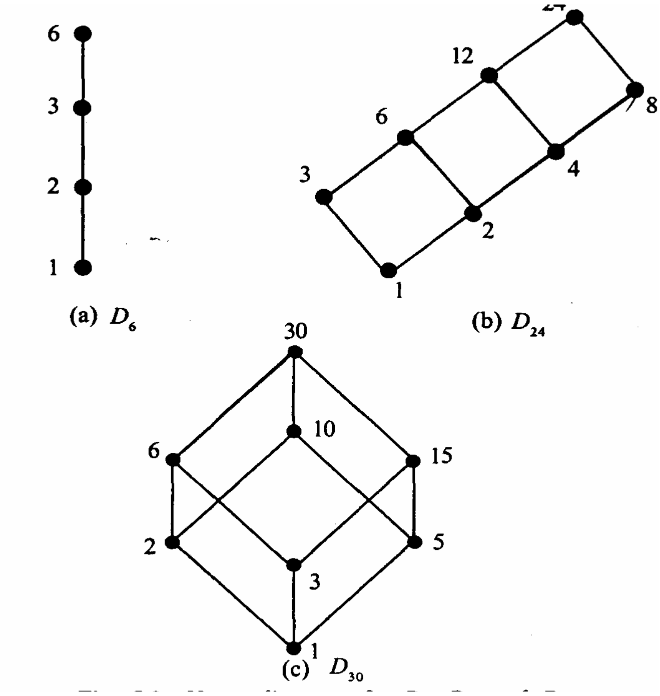


16.3.8 Example: Let n be a positive integer and D_n denotes the set of all divisors of n. Consider the partial order 'divides' in D_n. The Hasse diagrams for $D_{6,}$, D_{24} and D_{30} are given in the following figures.

D_6 = {l, 2, 3, 6},

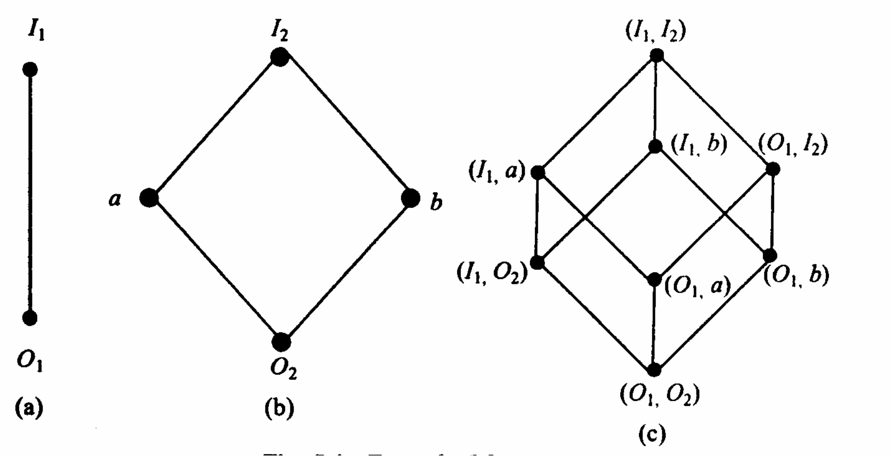
D_{24} = {1, 2, 3, 4, 6, 8, 12, 24}

D_{30} = {1, 2, 3, 5, 6, 10, 15, 30}.



(a) D_6 (b) D_{24} (c) D_{30}

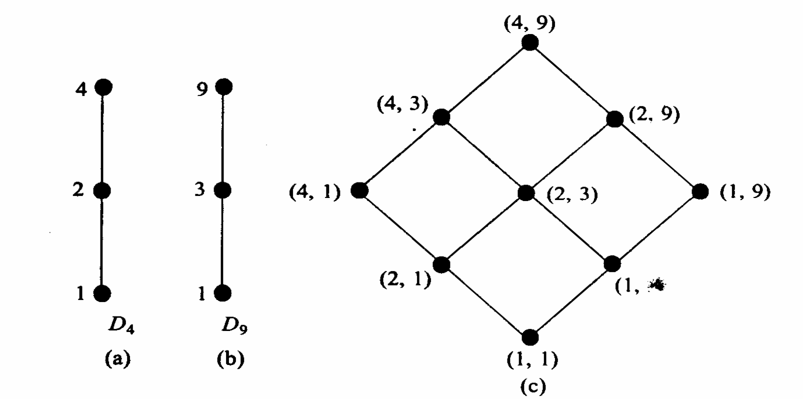
16.3.8 Example: Consider the Posets S and T represented in the following figures (a) and (b).



(a) (b) (c)

Then the Poset (S × T, ≤) is given in figure (c).

16.3.9 Example: Consider the Posets (D_4, ≤) and (D_9, ≤) given in (a) and (b). The Hasse diagram for L = $D_4 \times D_9$ under the partial order, is given by figure (c).



16.3.10 Observations: (i) The elements in level -1 are called *atoms.*

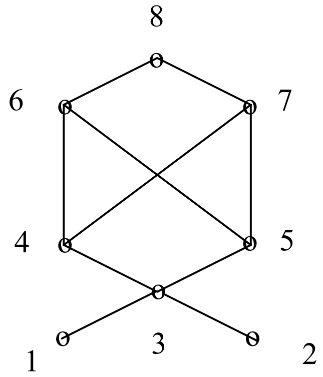
(ii) For a given Poset Hasse diagram need not be unique.

(iii) Hasse diagram for the dual Poset (A, ≥) can be obtained by rotating the Hasse diagram of the Poset (A, ≤) through 180^0.

Self Assessment Question 3: Let A = {1, 2, 3, 4, 5, 6}. The relation "|" (divides) is a partial order relation on *A*. Draw the Hasse diagram of (*A*, "|").

Self Assessment Question 4: Consider the partial ordered set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$ under the relation whose Hasse diagrams shown below. Consider the subsets $S_1 = \{1, 2\}$, $S_2 = \{3, 4, 5\}$ of *A*. Find (i). All the lower and upper bounds of S_1 and S_2

(ii). glb S_1, lub S_1, glb S_2, lub S_2.



16.4 Answers to Self Assessment Questions

SAQ 1.

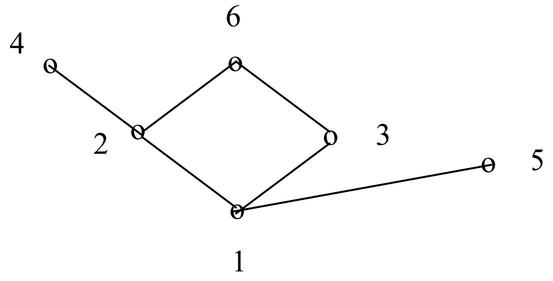
(i). No (ii). No

SAQ 2.

(i). It is an equivalance relation, but not partial ordering as R is not antisymmetric.

(ii). Not transitive and so it is neither.

SAQ 3.



SAQ 4.

Upperbounds of S_1 are 3, 4, 5, 6, 7 and 8

Lowerbounds of S_1 are none.

glb (S_1) : none

lub (S_1) : none

Upperbounds of S_2 are 6, 7 and 8

Lowerbounds of S_2 are 1, 2 and 3

glb (S_2) = 3

lub (S_2) = none.

16.5 Summary

The structures of partial ordered sets and lattices are useful in sorting and search procedures, and constructions of logical representations for computer circuits. The diagrammatic forms of lattices are useful in search, path procedures. We observed the interrelations between the algebraic structures POsets and Lattices and obtained some of their important equivalences. These concepts are base for the Boolean algebra and logical circuits.

16. 5 Technical Terms

Partial order: Reflexive, anti-symmetric and transitive.

Comparable: Let (A, $\leq$) be any Poset. Two elements a and b of A are if either $a \leq b$ or $b \leq a$.

Linearly ordered set or a chain: Every pair of elements is comparable.

Lexicographic product: Let $P_1, P_2, \ldots, P_k$ be POsets. The of $P_1, P_2, \ldots, P_k$ is defined to be the POset $P_1 \times P_2 \times \ldots \times P_k$ with $(a_1, a_2, \ldots, a_k) < (b_1, b_2, \ldots, b_k)$ if $a_1 < b_1$ or if $a_i = b_i$ for i = 1, …, m and $a_{m+1} < b_{m+1}$ for some $m < k$.

Minimal element: $y \in S$, a poset and $x \geq y \Rightarrow y = x$..

Maximal element: $b \in S$, a poset and $b \geq a \Rightarrow b = a$.

Totally ordered (or ordered): For a, b in S (a poset) exactly one of the conditions: $a > b$, $a = b$, or $b > a$ holds.

Greatest lower bound of A: A lower bound x of A is called a greatest lower bound of A if $x \geq y$ for all lower bounds y of A.

Zorn's Lemma: If P is a partially ordered set in which every chain has an upper bound, then P possesses a maximal element.

Covering matrix: Let $P = \{ p_{\text{i}} \ / \ 1 \le \text{i} \le n \}$ be a poset. Then the matrix $(b_{i_j})_{n \times n}$ where $b_{i_j} = 1$ if p_{i} covers p_{j} or i = j; and = 0 otherwise.

Hasse diagram: Representation of Poset by a diagram.

Atom: Elements in level zero

16.7 Model Questions

1. Determine which of the following are partial order?

(i). $\text{R}_1 = \{(\text{a}, b) \in \mathbb{Z} \times \mathbb{Z} \ / \ |\text{a} - b| \le 1\}$ on $\mathbb{Z}$

(ii). $\text{R}_2 = \{(\text{a}, b) \in \mathbb{Z} \times \mathbb{Z} \ / \ |\text{a}| \le |b| \}$ on $\mathbb{Z}$

(iii). $\text{R}_3 = \{(\text{a}, b) \in \mathbb{Z} \times \mathbb{Z} \ / \ \text{a divides } b \text{ in } \mathbb{Z} \}$ on $\mathbb{Z}$

(iv). $\text{R}_4 = \{(\text{a}, b) \in \mathbb{Z} \times \mathbb{Z} \ / \ \text{a-}b \le 0\}$

2. Define a relation R on $\mathbb{Z}$, the set of all integers as: aRb $\Leftrightarrow$ a + b is even for all a, $b \in \mathbb{Z}$. Is R a partial order relation on $\mathbb{Z}$?

3. Let A = {1, 2, 3, 4, 5, 6}. The relation "|" (divides) is a partial order relation on *A*. Draw the Hasse diagram of (*A*, "|").

16.8 References

1. Akerkar Rajendra and Akerkar Rupali. "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Fraleigh J.B. "A First Course in Abstract Algebra", Narosa Publ. House, New Delhi, 1992

3. Herstein I. N. "Topics in Algebra", Blaisdell, New York, 1964.

4. Satyanarayana Bhavanari "Partially Ordered Sets and Finite Machines", Satyasri Maths Study Centre, (0863 – 2232138) Guntur, 2002.

5. Satyanarayana Bhavanari "Lattices and Boolean Algebras", Satyasri Maths Study Centre, Guntur, (0863 – 2232138) 2002.

6. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

7. Trembly, J.P., and Manohar, R. "Discrete Mathematical Structures with Applications to Computer Science", Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Mr. T. V. Pradeep Kumar**

Lesson 17

Lattices

Objectives

At the end of the Lesson the student must be able to:

(i) Learn the structure of a lattice.
(ii) Know the properties of lattices.
(iii)Draw the lattice diagrams.
(iv)Learn bounded and complemented lattice.
(v) Learn distributive and modular lattice and its characterization.

Structure

17.1 Introduction

In this lesson we discussed the algebraic structure defined a lattice. Properties of lattices were discussed. Lattices with universal lower and universal upper bounds considered. Diagram representations of lattices are observed. Two equivalent form of lattice are defined. Some characterizations of complemented and distributive lattices are obtained. The concepts are play important role in logical circuits and Boolean algebras.

17.2 Definitions and Examples

17.2.1 Definition: Let $(P, \geq)$ be a POset and $A \subseteq P$. An element $x \in P$ is called a **lower bound** for A if $a \geq x$, for all $a \in A$. A lower bound x of A is called a **greatest lower bound** (infimum) of A if $x \geq y$ for all lower bounds y of A.

An element $x \in P$ is called an **upper bound** for A if $x \geq a$, for all $a \in A$. An upper bound x is called a **least upper bound** (supremum) of A if $b \geq a$ for all upper bounds b of A.

17.2.2 Example: Consider the Poset $(Z^+, \leq)$, where $\leq$ denotes divisibility. Let A = {1, 2, 3, 4, 6, 8, 12, 24} = D_{24}. Clearly A is a subset of Z^+. Now the upper bounds set of A = {24, 48, 72, …}. Here 24 is the least upper bound and 1 is the glb.

Note that for any subset A of R (the set of all real numbers), we have that $\inf A = \min A$ and $\sup A = \max A$.

17.2.3 Definition: A poset $(L, \leq)$ is said to be a **lattice** (or **lattice ordered**) if supremum of x and y; and infimum of x and y exist for every pair $x, y \in L$.

17.2.4 Note: (i) Every chain is lattice ordered

(ii) Let $(L, \leq)$ be a lattice ordered set; and $x, y \in L$. Then we have the following: $x \leq y \Leftrightarrow \sup(x, y) = y \Leftrightarrow \inf(x, y) = x$.

17.2.5 Definition: A **lattice** $(L, \wedge, \vee)$ is a set L with two binary operations $\wedge$ (called as **meet** or **product**) and $\vee$ (called as **join** or **sum**) which satisfy the following laws, for all $x, y, z \in L$:

$x \wedge y = y \wedge x$, and $x \vee y = y \vee x$ (Commutative laws).

$x \wedge (y \wedge z) = (x \wedge y) \wedge z$, and $x \vee (y \vee z) = (x \vee y) \vee z$ (Associative laws).

$x \wedge (x \vee y) = x$; and $x \vee (x \wedge y) = x$ (Absorption laws).

17.2.6 Examples: (i). Let Z^+ be the set of positive integers. Define a relation 'D' on Z^+ by $aDb \Leftrightarrow a$ divides b for any $a, b \in Z^+$. Then (Z^+, D) is a lattice, in which, $a \wedge b = \gcd \{a, b\}$ and $a \vee b = \text{lcm}\,\{a, b\}$.

Self Assessment Question 1: Verify whether the set $L = \{1, 2, 3, 4, 6, 12\}$, the factors of 12 under the relation 'divisibility' forms a lattice.

Let X be a non-empty set and consider $(P(X), \subseteq)$, the power set with the inclusion relation. Then for any A, B in $P(X)$, we have that $A \wedge B = A \cap B$ and $A \vee B = A \cup B$.

17.2.7 Definition: Let $(L, \geq)$ be a lattice. If every non-empty subset of L has greatest lower bound and least upper bound, then L is said to be a *complete lattice*.

17.2.8 Examples: (i) Let P be the set of all integers with usual ordering. Clearly it is a lattice. The set of all even integers is a subset of P and it has no upper bound or lower bound. Hence P is not a complete lattice.

(ii) If $P = \{ i \;/\; 1 \leq i \leq n \}$ and $\geq$ is the usual ordering of integers, then P is a complete lattice.

17.2.9 Definition: A subset S of a lattice L is called a **sublattice** of L if S is a lattice with respect to the restriction of $\wedge$ and $\vee$ from L to S. It is clear that a subset S of L is a sublattice of the lattice $L \Leftrightarrow$ S is "closed" with respect to $\wedge$ and $\vee$ (that is, $s_1, s_2 \in S \Rightarrow s_1 \wedge s_2 \in S$ and $s_1 \vee s_2 \in S$).

17.2.10 Example: Let (A, $\leq$) be a lattice and S be a non-empty subset of L. Then (S, $\leq$) is called a sublattice of (L, $\leq$) if a $\vee$ b $\in$ S and a $\wedge$ b be S for a, b $\in$ S.

17.2.11 Example: The lattice (D_n, $\leq$) is a sublattice of (Z^+, $\leq$) where $\leq$ is the divisibility relation.

17.2.12 Example: Consider the lattice A shown in fig (a) and the partially ordered subset S of L shown fig (b). Now (S, $\leq$) is not a sublattice, since b $\wedge$ c $\notin$ S. The partially ordered shown in fig(c).

17.2.13 Definition: Let (A, $\leq$) be a lattice. An element g $\in$ A is called the **greatest element** of A if a $\leq$ g for all a $\in$ A. Similarly, an element s $\in$ A is called the **smallest** (least) **element** of A if s $\leq$ a for all a $\in$ A.

17.2.14 Example: (i) Consider $\mathbb{N}$ = the set of all natural numbers. Define $a \leq b \Leftrightarrow a$ divides b, for all a, $b \in \mathbb{N}$. Then $(\mathbb{N}, \leq)$ is a POset. For any x, $y \in \mathbb{N}$, we write $x \wedge y$ = gcd $\{x, y\}$ and $x \vee y$ = lcm $\{x, y\}$. Then $(\mathbb{N}, \leq)$ is a lattice. Here 1 is the zero element. The greatest element does not exist.

(ii) Let A be a set. Consider $\wp(A)$ = the power set of A. $(\wp(A), \subseteq)$ is a POset (where $\subseteq$ is the set inclusion) For any X, $Y \in \wp(A)$, we write $X \wedge Y = X \cap Y$ and $X \vee Y = X \cup Y$. Then $(\wp(A), \subseteq)$ is a lattice. In this lattice, ϕ is the smallest element and A is the greatest element.

17.3 Properties of Lattices

17.3.1 Properties: Let $(L, \wedge, \vee)$ be an algebraic lattice and $x \in L$.

1. $x \wedge x = x, \; x \vee x = x$ (idempotent)

2. $x \vee y = y \vee x, x \wedge y = y \wedge x$ (commutative)

3. $x \vee (y \vee z) = (x \vee y) \vee z, x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (Associative)

4. $x \vee (x \wedge y) = x, \; x \wedge (x \vee y) = a$ (Absorption)

17.3.2 Theorem: Let $(L, \leq)$ be a lattice. For $a, b \in L$,

(i) $a \leq b \Leftrightarrow a \wedge b = a$

(ii) $a \leq b \Leftrightarrow a \vee b = b$

Proof: Assume that $a \leq b$.

Since $a \leq a$, we have that a is a lower bound of a and b. Therefore $a \leq a \wedge b$ and $a \wedge b$ is the glb of a and b.

By definition of $a \wedge b$, we have $a \wedge b \leq a$. Therefore by antisymmetric property, we have $a \wedge b = a$.

Conversely suppose that $a \wedge b = a$. Then by definition of $a \wedge b$, $a = a \wedge b \leq b$.

Thus we have $a \wedge b = a \Rightarrow a \leq b$.

In a similar way we can prove (ii).

17.3.3 Problem: Let a and b be two elements in a lattice $(L, \leq)$. Show that $a \wedge b = b$ if and only if $a \vee b = a$.

Solution: Part (i): Suppose $a \wedge b = b$. Now

$a = a \vee (a \wedge b)$ (by absorption law)

$= a \vee b$ (supposition).

Part (ii): Suppose $a \vee b = a$. Now

$b = b \wedge (b \vee a)$ (by absorption)

$= b \wedge (a \vee b)$ (by commutative)

$= b \wedge a$ (supposition)

$= a \wedge b$ (by commutative)

17.3.4 Theorem: Let $(L, \leq)$ be a lattice. Then for $a, b, c, d \in L$,

(i) $a \leq b \Rightarrow a \vee c \leq b \vee c$

(ii) $a \leq b \Rightarrow a \wedge c \leq b \wedge c$

(iii) $a \leq b$ and $c \leq d \Rightarrow a \vee c \leq b \vee d\cdot$

(iv) $a \leq b$ and $c \leq d \Rightarrow a \wedge c \leq b \wedge d$.

Proof: (i) From the above theorem 17.3.2, we have $a \leq b \Leftrightarrow a \vee b = b$.

Now $(a \vee c) \vee (b \vee c) = (a \vee c) \vee (c \vee b)$ (by commutative)

$= a \vee (c \vee c) \vee b$ (by associative)

$= a \vee (c \vee b)$ (by idempotent)

$= (a \vee b) \vee c$

$= b \vee c$.

By theorem 17.3.2, we have $a \vee c \leq b \vee c$.

(ii) Similar

(iii) From the theorem 17.3.2, $a \leq b \Leftrightarrow a \vee b = b$ and $c \leq d \Rightarrow c \vee d = d$.

Now $(a \vee c) \vee (b \vee d) = a \vee (c \vee b) \vee d$ (by associative)

$= a \vee (b \vee c) \vee d$ (commutative)

$= (a \vee b) \vee (c \vee d)$ (associative)

$= b \vee d$ (since $a \leq b$ and $c \leq d$)

Therefore $a \vee c \leq b \vee d$ (by theorem 17.3.2).

(iv) Similar.

17.3.5 Theorem: The following two conditions are equivalent.

(i) $(L, \leq)$ is a partially ordered set in which every pair of elements a, b in L, the *lub* $\{a, b\}$ and *glb* $\{a, b\}$ exist.

(ii) $(L, \wedge , \vee)$ be an algebraic system satisfying commutative, associative, absorption and idempotent laws with $a \leq b$ if and only if $a \wedge b = a$.

17.3.6 Theorem: (i) Let $(L, \leq)$ be a lattice ordered set. Define x $\wedge y = \inf (x, y)$, and $x \vee y = \sup (x, y)$. Then $(L, \wedge, \vee)$ is an algebraic lattice.

(ii) Let $(L, \wedge, \vee)$ be an algebraic lattice. Define $x \leq y \Leftrightarrow x \wedge y = x$, Then $(L, \leq)$ is a lattice ordered set.

Proof: Part-(i): Let $(L, \leq)$ be a lattice ordered set and $x, y, z \in L$.

Commutative laws: $x \wedge y = \inf (x, y) = \inf (y, x) = y \wedge x$, $x \vee y = \sup (x, y) = \sup (y, x) = y \vee x$.

Associative laws: $x \wedge (y \wedge z) = x \wedge \inf (y, z) = \inf (x, \inf (y, z)) = \inf (x, y, z) = \inf (\inf(x, y), z) = \inf (x, y) \wedge z = (x \wedge y) \wedge z$. Similarly, we have that $x\vee(y\vee z) = (x \vee y) \vee z$.

Absorption laws: $x \wedge (x \vee y) = x \wedge \sup (x, y) = \inf (x, \sup (x, y)) = x$. Also $x \vee (x \wedge y) = x \vee \inf (x, y) = \sup (x, \inf (x, y)) = x$.

Part-(ii): Let $(L, \wedge, \vee)$ be an algebraic lattice. Let $x, y, z \in L$.

Step-(i): In this step we prove that $(L, \leq)$ is a partially ordered set.

Reflexive: Follows from the idempotent laws, since $x \wedge x = x$ and $x \vee x = x$ and so $x \leq x$.

Anti-symmetric: Suppose $x \leq y$ and $y \leq x$

$\Rightarrow x \wedge y = x$ and $y \wedge x = y$

$\Rightarrow x = x \wedge y = y \wedge x$ (by commutative law) $= y \Rightarrow x = y$.

Transitive: Suppose $x \leq y$ and $y \leq z$

$\Rightarrow x \wedge y = x$ and $y \wedge z = y$

Now $x = x \wedge y = x \wedge (y \wedge z)$

$= (x \wedge y) \wedge z$ (by associative law)

$= x \wedge z \Rightarrow x = x \wedge z \Rightarrow x \leq z$.

This shows that $\leq$ is transitive. So we can conclude that $(L, \leq)$ is a poset.

Step-(ii): In this step we prove that $\sup(x, y) = x \vee y$. By Remark 1.13, we have that $x \leq y \Leftrightarrow x \vee y = y \Leftrightarrow x \wedge y = x$ …. (i).

Let $x, y \in L$. Then $x \wedge (x \vee y) = x \Rightarrow x \leq x \vee y$.

Similarly $y \leq x \vee y$. Therefore $x \vee y$ is an upper bound for $\{x, y\}$.

Suppose $z \in L$ be an upper bound for $\{x, y\}$.

Then $x \leq z$ and $y \leq z$. By (i), we get that $x \vee z = z$ and $y \vee z = z$. Now $(x \vee y) \vee z = x \vee (y \vee z)$ (by associative law) $= x \vee z$ (by (i)) $= z \Rightarrow x \vee y \leq z$. This shows that $\sup(x, y) = x \vee y$. In a similar way, we prove that $\inf(x, y) = x \wedge y$.

Step-(iii): From the above steps (i) to (ii), we conclude that $(L, \leq)$ is a lattice ordered set.

Observation: From the Theorem 17.3.6, it is clear that there exists a one-to-one relationship between lattice ordered sets and algebraic lattices. In other words, the concepts "lattice ordered set" and "algebraic lattice" are equivalent. So we can use the term lattice for both concepts: lattice ordered sets and algebraic lattices. (ii) We write $|L|$ to denote the number of elements of L. (iii) If N is a subset of a POset, then $\vee_{x\in \mathrm{N}}\, x$ and $\wedge_{x\in \mathrm{N}}\, x$ denote the supremum and infimum of N, respectively, whenever they exist. We say that the **supremum** of N is the join of all elements of N and the **infimum** is the meet of all elements of N.

17.3.7 Duality Principle: Any “formula” involving the operations $\wedge$ and $\vee$ which is valid in any lattice $(L, \wedge, \vee)$ remains valid if we replace $\wedge$ by $\vee$, and $\vee$ by $\wedge$ everywhere in the formula. This process of replacing is called **dualyzing**.

17.4 Bounded and Complemented lattices

17.4.1 Definition: If a lattice L contains a smallest (greatest, respectively) element with respect to $\leq$, then this uniquely determined element is called the **zero element** (**unit element**, respectively). The zero element is denoted by 0, and the unit element is denoted by 1. The elements 0 and 1 are called **universal bounds**. If the elements 0 and 1 exist, then we say that the lattice L is a **bounded lattice**.

17.4.2 Example: In the lattice, $(D_{36}, \leq)$, 1 is the least element and 36 is the greatest element. In general, $(D_n, \leq)$ is a bounded lattice for any positive integer n.

17.4.3 Example: (i) In the lattice $(Z^+, \leq)$ with $\leq$ means usual $\leq$ is not a bounded lattice as 1 is the least element and there is no greatest element.

Self Assessment Question 2: Verify whether the lattice $(Z^+, \leq)$ with $\leq$ defined as $a \leq b \Leftrightarrow a \mid b$ is a bounded lattice.

17.4.4 Note: If a lattice L is bounded (by 0 and 1), then every x in L satisfies $0 \leq x \leq 1$, $0 \wedge x = 0$, $0 \vee x = x$, $1 \wedge x = x$, and $1 \vee x = 1$.

17.4.5 Theorem: Let L be a lattice, and $x, y, z \in L$. Then L satisfy the following distributive inequalities:

(i) $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$

(ii) $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

Proof: We know that $x \wedge y \leq x$, and $x \wedge y \leq y \leq y \vee z$.

So $x \wedge y$ is a lower bound for x and $y \vee z$

$\Rightarrow x \wedge y \leq x \wedge (y \vee z)$.

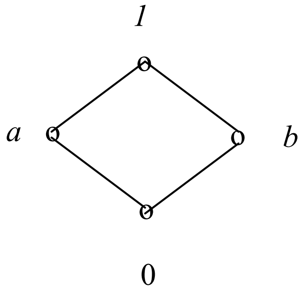
Now $x \wedge z \leq x$ and $x \wedge z \leq z \leq y \vee z \Rightarrow x \wedge z$ is a lower bound for x and $y \vee z$ $\Rightarrow x \wedge z \leq x \wedge (y \vee z)$.

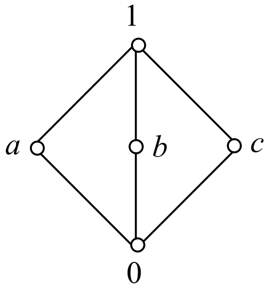
Therefore, we have that $x \wedge(y \vee z)$ is an upper bound for $x \wedge y$ and $x \wedge z$ and so $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$. This completes the proof for (i). The proof of (ii) is similar.

17.4.6 Definition: A lattice L with 0 and 1 is called **complemented** if for each $x \in L$ there exists at least one element y such that $x \wedge y = 0$ and $x \vee y = 1$. Each such y is called a **complement** of x. We denote the complement of x by x^1.

17.4.7 Example: In the lattice fig 1, a and b are complements of each other.

Self Assessment Question 3: In the lattice fig 2, write complements of a, b, and c.





17.4.8 Example: (i) Let $L = \wp(M)$. Then B = $M \setminus A$ is the unique complement of A.

(ii) In a bounded lattice, 1 is a complement of 0, and 0 is a complement of 1. (iii) Every chain with more than two elements is not a complemented lattice.

(iv) The complement need not be unique. For example, in the diamond lattice, both the two elements b and c, are complements for the element a.

(v) Let L be the lattice of subspaces of the vector space $\mathbb{R}^2$. If T is a complement of a subspace S, then $S \cap T = \{0\}$ and $S + T = \mathbb{R}^2$. Hence a complement is a complementary subspace.

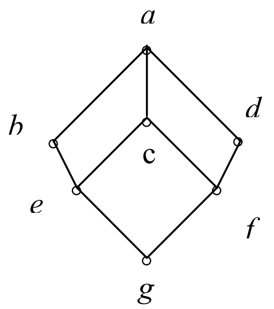
17.4.9 Example: (i) In a bounded lattice, 1 is a complement of 0, and 0 is a complement of 1.

(ii) Every chain with more than two elements is not a complemented lattice.

(iii) The complement need not be unique. For example, in the diamond lattice, both the two elements b and c, are complements for the element a.

17.4.10 Definition: Let L be a lattice with zero. An element $a \in L$ is said to be an **atom** if $a \neq 0$ and if it satisfies the following condition: $b \in L$, $0 < b \leq a$ implies that $b = a$.

Self Assessment Question 4: Find the atoms in the following lattice.



17.5 Distributive Lattices

17.5.1 Definition: A lattice $(L, \vee, \wedge)$ is called a **modular lattice** if it satisfies the following condition: $x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$ for all $x, y, z \in L$. This condition is called as **modular identity**.

17.5.2 Example: Consider the lattice $L_1 = \{0, a, b, c, 1\}$ whose Hasse diagram is given. This lattice L_1 is a modular lattice. This lattice called as **diamond lattice.**

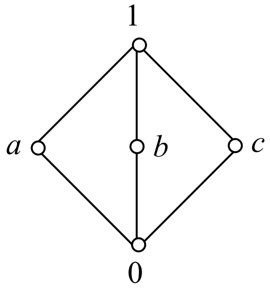


Fig. 17.5.2

17.5.3 Example: Consider the lattice $L_2 = \{0, a, b, c, 1\}$ whose Hasse diagram is given. This lattice L_2 is not a modular lattice. Since $b \leq c$, by modular law, we have that $b \vee (a \wedge c) = (b \vee c) \wedge c \Rightarrow b \vee 0 = 1 \wedge c \Rightarrow b = c$, a contradiction. Hence L_2 is not a modular lattice.

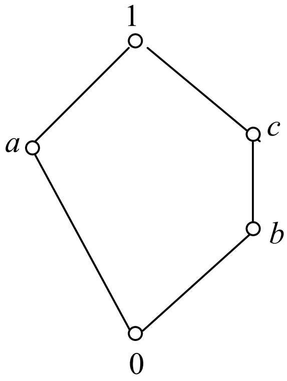


Fig. 17.5.3

17.5.4 Definition: A lattice L is said to be a **distributive lattice** if it satisfies the following laws: (i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, and (ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, for all $a, b, c \in L$. These two laws are called the **distributive laws**.

17.5.5 Example: (i) For any set X, the lattice $(\wp(X), \cup, \cap)$ is a distributive lattice.

(ii) Every chain is a distributive lattice.

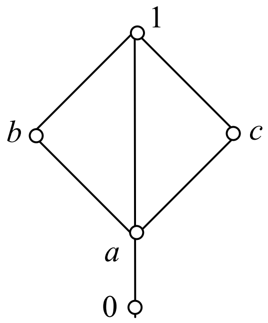


Fig. 17.5.5 (i)

(iii) Consider the lattice given by the diagram

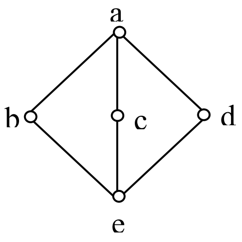


Fig. 17.5.5 (ii)

Now $b\wedge(c\vee d) = b \wedge a = b$, and $(b\wedge c) \vee(b\wedge d) = e \vee e = e$. Therefore this is not a distributive lattice.

17.5.6 Problem: In a distributive lattice, if an element has a complement, then it is unique.

Solution: Suppose that an element a has two complements, say b and c. That is,

$a \vee b = 1, a \wedge b = 0, a \vee c = 1, a \wedge c = 0$.

We have $b = b \wedge 1$ (since 1 is the universal upper bound)

$= b \wedge (a \vee c)$ (since $a \vee c = 1$)

$= (b \wedge a) \vee (b \wedge c)$ (by the distributive law)

$= (a \wedge b) \vee (b \wedge c)$ (since $\wedge$ is commutative)

$= 0 \vee (b \wedge c)$ (since $a \wedge b = 0$)

$= (a \wedge c) \vee (b \wedge c)$ (since $a \wedge c = 0$)

$= (a \vee b) \wedge c$ (by distributive law)

$= 1 \wedge c$ (since $a \vee b =1$)

$= c$ (since 1 is the universal upper bound).

Therefore the complement is unique.

17.5.7 Problem: Prove that the following properties of a lattice L are equivalent:

(i) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in L$;

(ii) $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$ for all $a, b, c \in L$;

(iii) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c)\wedge(c\vee a)$ for all $a, b, c \in L$.

Solution: **(i) ⇒ (ii)**: Suppose $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in L$;

$$\begin{aligned}(a\vee c)\wedge(b\vee c) &= [(a\vee c)\wedge b]\vee [(a\vee c)\wedge c] && \text{(by (i))}\\ &= [(a\vee c)\wedge b]\vee c && \text{(by commutative and absorption laws)}\\ &= [(a \wedge b) \vee (c \wedge b)] \vee c && \text{(by (i))}\\ &= (a \wedge b) \vee [(c \wedge b) \vee c] && \text{(by associative law)}\\ &= (a \wedge b) \vee c && \text{(by absorption law).}\end{aligned}$$

This proves (ii).

(ii) ⇒ (iii): Suppose (ii).

$$\begin{aligned}(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) &= (a \wedge b) \vee [(b \wedge c) \vee (c \wedge a)]\\ &= \{a\vee[(b\wedge c)\vee(c\wedge a)]\}\wedge\{b\vee[(b\wedge c)\vee(c\wedge a)]\} && \text{(by (ii))}\\ &= \{a \vee (b \wedge c)\} \wedge \{b \vee (c \wedge a)\} && \text{(by commutative, associative and absorption)}\\ &= \{(a \vee b) \wedge (a \vee c)\} \wedge \{(b \vee c) \wedge (b \vee a)\} && \text{(by (ii))}\\ &= (a \vee b) \wedge (b \vee c) \wedge (c \vee a) && \text{(by idempotent law)}\end{aligned}$$

(iii) ⇒ (i): Suppose that $a \leq c$. Then $a\wedge b \leq c \wedge b \Rightarrow (a\wedge b)\vee(c\wedge b) = (c\wedge b)$ ….. (A)

Also $a \vee c = c$. Now $(a \wedge c) \vee (b \wedge c)$

$$\begin{aligned}&= (a \wedge c) \vee [(a \wedge b)\vee (c \wedge b)] && \text{(by (A))}\\ &= (a \wedge b) \vee (b \wedge c)\vee (c \wedge a)\\ &= (a \vee b) \wedge (b \vee c) \wedge (c \vee a) && \text{(by (iii))}\\ &= (a \vee b) \wedge (b \vee c) \wedge c && \text{(since } a \leq c)\\ &= (a \vee b) \wedge c && \text{(by absorption law).}\end{aligned}$$

Now we proved that $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$.

This shows that (i) is true. This completes the proof.

17.5.8 Problem: If L is a distributive lattice, then it is a modular lattice.

Solution: Assume that L is a distributive lattice. Let $x, y, z \in L$ and $x \leq z$.

We have that $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = (x \vee y) \wedge (y \vee z) \wedge (z \vee x)$.

Since $x \leq z$, we have that $x \wedge z = x$ and $x \vee z = z$, and so

$(x \wedge y) \vee (y \wedge z) \vee x = (x \vee y) \wedge (y \vee z) \wedge z$.

This implies $x \vee (y \vee z) = (x \vee y) \wedge z$ (by absorption laws).

This shows that L is a modular lattice.

The converse of the above problem is not true. That is, there exist modular lattices which are not distributive. The following example is a modular lattice, but not distributive .

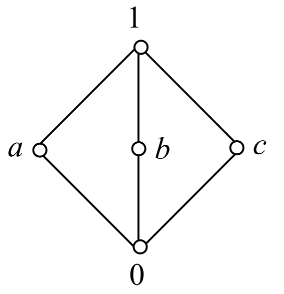


Fig. 17.5.8

17.5.9 Problem: For a given lattice L, the following two conditions are equivalent:

(a) $x\vee (y \wedge z) = (x\vee y) \wedge (x \vee z)$, and

(b) $x \wedge(y \vee z) = (x \wedge y) \vee (x\wedge z)$ for all $x, y, z \in L$.

Solution: Suppose that $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ … (i).

Now $(x \wedge y) \vee (x \wedge z) = [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z]$ (by (i))

$= x \wedge [(x \wedge y) \vee z]$ (by commutative and absorption laws)

$= x \wedge [z \vee (x \wedge y)]$ (by commutative law)

$= x \wedge [(z \vee x) \wedge (z \wedge y)]$ (by (i))

$= [x \wedge (z \vee x)] \wedge [z \wedge y]$ (by associative law)

$= x \wedge (z \wedge y)$ (by commutative and absorption law)

Other part is similar.

17.6 Answers to Self Assessment Questions

SAQ1.

This is a lattice.

SAQ 2.

This is not a bounded lattice, since there is no greatest element.

SAQ3.

Complements of a are b and c;

Complements of b are a and c;

Complements of c are a and b.

SAQ 4.

The atoms are *e* and *f*.

17.7 Summary

In this lesson we discussed the algebraic structure defined a lattice. Properties of lattices were discussed. Diagram representations of lattices are observed. Some characterizations of complemented and distributive lattices are obtained. The concepts are useful in logical circuits and Boolean algebras.

17.8 Technical Terms

Lower bound: An element $x \in P$ is called a *lower bound* for A if $a \geq x$, for all $a \in A$.

Upper bound: An element $x \in P$ is called an *upper bound* for A if $x \geq a$, for all $a \in A$.

Lattice: A poset $(L, \leq)$ is said to be a lattice (or lattice ordered) if supremum of x and y; and infimum of x and y exist for every pair $x, y \in L$.

Complete lattice: If every non-empty subset of a lattice has greatest lower bound and least upper bound.

Greatest element: An element g is called the greatest element of a lattice if a ≤ g for all a in a lattice.

Bounded lattice: A lattice with elements 0 and 1, called universal bounds.

Complement: $x \in L$, there exists at least one element y such that $x \wedge y = 0$ and $x \vee y = 1$

Atom: If $a \neq 0$ and satisfies: $b \in L$, $0 < b \leq a$ implies that $b = a$.

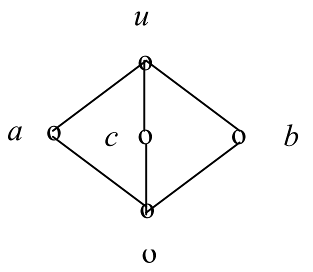
Modular lattice: $x \leq z \Rightarrow x \vee (y \wedge z) = (x \vee y) \wedge z$ for all x, y, z in a lattice.

Distributive lattice: A lattice that satisfies (i) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, and (ii) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, for all a, b, c in a lattice.

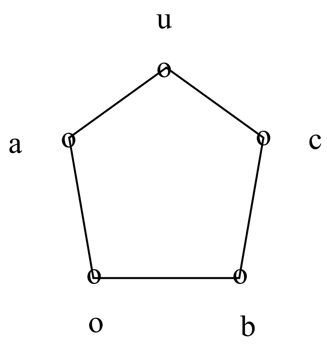
17.9 Model Questions

1. Verify whether or not the following are modular lattices.

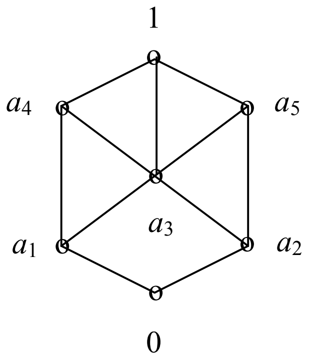
(i)



(ii)



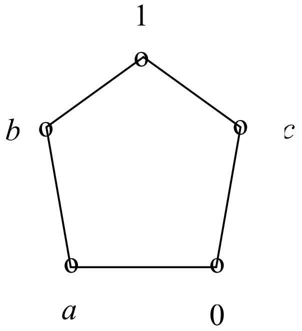
2. Consider the lattice A = {0, a_1, a_2, a_3, a_4, a_5, 1} given belo.. .



(i). Is *A* is a distributive lattice

(ii).What are the complements of a_1 and a_2

3. Write the complements *a*, *b* and *c* from the given lattice.



4. Define a distributive lattice and complemented lattice.

5. In a distributive lattice, if an element has a complement, then prove that it is unique.

6. Let $(L, \leq)$ be a lattice. Then for a, b, c, d $\in$ L,

(i) $a \leq b \Rightarrow a \vee c \leq b \vee c$

(ii) $a \leq b \Rightarrow a \wedge c \leq b \wedge c$

(iii) $a \leq b$ and $c \leq d \Rightarrow a \vee c \leq b \vee d$·

(iv) $a \leq b$ and $c \leq d \Rightarrow a \wedge c \leq b \wedge d$.

7. Let a and b be two elements in a lattice $(L, \leq)$. Show that $a \wedge b = b$ if and only if $a \vee b = a$.

8. (i) Let $(L, \leq)$ be a lattice ordered set. Define $x \wedge y = \inf(x, y)$, and $x \vee y = \sup(x, y)$. Then prove that $(L, \wedge, \vee)$ is an algebraic lattice.

(ii) Let $(L, \wedge, \vee)$ be an algebraic lattice. Define $x \leq y \Leftrightarrow x \wedge y = x$. Then prove that $(L, \leq)$ is a lattice ordered set.

17.10 References

1. Akerkar Rajendra and Akerkar Rupali. “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, “Discrete Mathematical Structures” PHI, New Delhi, 1999.

3. Liu.C.L., “Elements of Discrete Mathematics”, Mc Hill.

4. Satyanarayana Bhavanari, Syam Prasad Kuncham, Dharma Rao Vatluri, Pradeep Kumar T. V., and Madhavilatha T. “Quantitative Methods”, Technical P.G. Series, Venkateswara Publishers, Guntur, 2000.

5. Satyanarayana Bhavanari “Lattices and Boolean Algebras”, Satyasri Maths Study Centre, Guntur, (0863 – 2232138) 2002.

6. Shanker Rao, G., “Discrete Mathematical Structures”, New Age International Publishers, New Delhi, 2002.

7. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

8. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Mr. T. V. Pradeep Kumar**

Lesson 18

Finite Boolean Algebras

Objectives

At the end of the Lesson the student must be able to:

(i) Extend the notion of Boolean algebra from a lattice.
(ii) Learn various properties of Boolean algebras
(iii) Write the dnf and cnf of a Boolean function
(iv) Learn several applications of Boolean algebras in science and engineering.

Structure

18.1 Introduction

Boolean Algebra is an algebra of logic. One of the earliest investigators of symbolic logic was George-Boole (1815-1864) who invented a systematic way of manipulating logic symbols which is referred as Boolean Algebra. It has become now an indispensable tool to computer scientists because of its direct applicability to switching circuits theory and the logical design of digital computers. The symbols 0 and 1 used in this unit have logical significance.

18.2 Boolean Algebras

18.2.1 Definition: A **Boolean Algebra** is a complemented distributive lattice. The operations $\wedge$ and $\vee$ are also denoted by $\oplus$ and *. We denote a * b is some times as ab. The bounds are denoted by 1 and 0. Thus a Boolean algebra B with operations $\oplus$ and * and bounds 1 and 0 satisfy the following properties.

1. $a \oplus a = a$; $\quad a * a = a$
2. $a \oplus b = b \oplus a$; $\quad a * b = b*a$.
3. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$; $\quad a * (b *c) = (a * b) * c$;
4. $a \oplus (a * b) = a$; $a \oplus (a * b) = a$;
5. $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$; $\quad a * (b \oplus c) = (a * b) \oplus (a * c)$
6. $0 \leq a$ for all $a \in L$; $\quad a \leq 1$ for all $a \in L$;
7. $a \oplus 0 = a$; $\quad a * 1 = a$;
8. $a \oplus 1 = a$; $\quad a * 0 = 0$;

Note: For $a \in L$, let a^1 be the (unique) complement of a.

9. $a \oplus a^1 = 1$; $\quad a * a^1 = 0$
10. $1^1 = 0$; $\quad 0^1 = 1$;
11. $(a \oplus b)^1 = a^1 * b^1$; $\quad (a * b)^1 = a^1 \oplus b^1$

Note that (i) Properties 1 to 4 are lattice properties; 5 are distributive properties; 6 and 8 are properties of bounds; 9 and 11 are properties of complements.

(ii) The properties 11 are called D' Morgan laws.

18.2.2 Definition: A Boolean Algebra with finite number of elements is called a **finite Boolean Algebra**.

18.2.3 Example: Let S be a finite set. Consider the lattice (P(S), $\subseteq$) with operations $\cup$ and $\cap$, in which the universal upper bound is S, the universal lower bound is ϕ (empty set), and the complement of any set T in P(S) is the set S - T.

Take S = {a, b, c}

P(S) = {s, {a}, {b}, {c}, {a, b}, {b,c}, {a, c} ϕ}

Then (P(S), $\subseteq$) is a lattice. The Boolean algebra is represented by the following diagram.

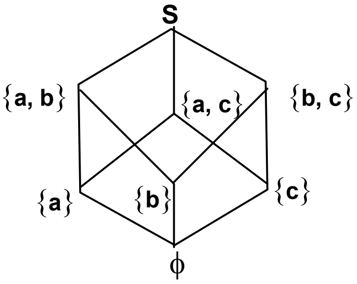


Fig. 18.2.3

18.2.4 Example: Let B = {0, 1}. The operations $\vee$ and $\wedge$ are given in the following tables

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

The complement of '0' is 1 and vice versa. Then (B,$\vee$,$\wedge$,–) is a Boolean Algebra.

18.2.5 Example: Let B_n be the set of n-tuples of 0's and 1's. For a, b $\in$ B_n, define a $\oplus$ b = ($a_1 \vee b_1$, $a_2 \vee b_2$, …, $a_n \vee b_n$) and a * b = ($a_1 \wedge b_1$, $a_2 \wedge b_2$, …, $a_n \wedge b_n$) where a = (a_1, a_2, …, a_n) and b = (b_1, b_2, …, b_n).

Now a_i = 0 or 1 and b_i = 0 or 1 for i = 1, 2, ..., n. Also a^1 = (a_1^1, a_2^1, …, a_n^1) and b = (b_1^1, b_2^1, …, b_n^1) where $\vee$ and $\wedge$ complementation are as in above example over {0, 1}. Then (B_n, $\oplus$, *) is a Boolean Algebra with bounds 0_n and 1_n where 0_n = (0, 0, …, 0) and 1_n = (1,1,…,1).

18.2.6 Theorem: If $S_1 = \{ x_1, x_2, ... x_n\}$ and $S_2 = \{y_1, y_2, ... y_n\}$ are any two finite sets with n elements, then the lattices $(P(S_1), \subseteq)$ *and* $(P(S_2), \subseteq)$ are isomorphic. Consequently the Hasse diagrams of these lattices may be drawn identically.

Proof: Arrange the sets as known in Fig. 1,

so that each element of S_1 is directly over the correspondingly numbered element in S_2

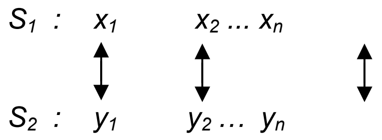
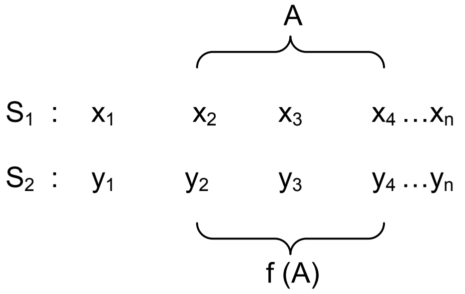


Fig. 18.2.6

Let A be a subset of S_1

Define $f(A)$ = subset of S_2 consisting of all elements that correspond to the elements of A (see fig (2))



A
S_1 : x_1 x_2 x_3 $x_4 ... x_n$
S_2 : y_1 y_2 y_3 $y_4 ... y_n$
f (A)

It can be easily seen that f is one one and onto. Also $A \subseteq B$ if and only if $f(A) \subseteq f(B)$ for all $A, B \in P(S_1)$.

Therefore the lattices $(P(S_1), \subseteq)$ and $(P(S_2), \subseteq)$ are isomorphic.

18.2.7 Example: Let $S = \{a, b, c\}$, $T = \{2, 3, 5\}$. Define $f : P(S) \rightarrow P(T)$ by $f(\{a\}) = \{2\}, f(\{b\}) = \{3\}, f(\{c\}) = \{5\}$,

$f(\{a, b\}) = \{2,3\}, f(\{b, c\}) = \{3, 5\}, f(\{a, c\}) = \{2, 5\}$

$f(\{a, b, c\}) = \{2, 3, 5\}, f(\phi) = \phi$

The Boolean lattices $(P(S), \subseteq)$ *and* $(P(T), \subseteq)$ are isomorphic.

18.2.8 Note:

a) Any finite Boolean algebra has exactly 2^n elements for some positive integer n. Also there is a unique (up to isomorphism) Boolean algebra of 2^n elements for every $n > 0$.

b) From the above theorem, it is clear that the lattice (P(S), ⊆) is completely determined as a poset by the number $|S|$ and does not depend in any way on the nature of the elements in S.

c) Each lattice (P(S), ⊆) is isomorphic to B_n (n– tuples, Boolean Algebra, over {0, 1}) where $n = |S|$

18.2.9 Example: Consider the lattice

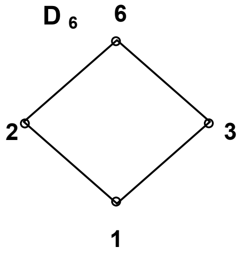
$D_6 = \{x \in Z^+ |\ x$ is a divisor of $6\} = \{1, 2, 3, 6\}$

Define $f = D_6 \rightarrow B_2 = \{0, 1\}$ by

$f(1) = 00, f(2) = 10, f(3) = 01, f(6) = 11$

Then f is an isomorphism. These can be represented by a following diagrams

Fig. 18.2.9 (i)



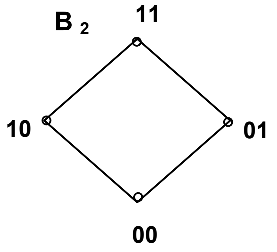


Fig. 18.2.9 (ii).

18.2.10 Example: (i) The lattice $D_{20} = \{1, 2, 4, 5, 10, 20\}$ has $6 \neq 2^n$ (for any positive integer n) elements and hence not a Boolean algebra.

(ii) The lattice $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ has 2^3 elements and hence a Boolean algebra. Observe that D_{30} is isomorphic to B_3 (over $\{0, 1\}$), *w*here the isomorphism:

f:$D_{30} \to B_3$ defined by f(1) = 000, f (2) = 100, f (3) = 010, f (5) = 001, f (6) = 110, f (10) = 101, f (15) = 011, f (30) = 111.

18.2.11 Note: To draw the Hasse diagram for B_n (n – tuples over $\{0, 1\}$) we join two n – tuples if they differ by exactly are component.

18.2.12 Theorem: Let $n = p_1 \; p_2 \; .... \; p_k$ where $p_i \; (1 \leq i \leq k)$ are distinct primes. Then D_n is a Boolean Algebra.

18.2.13 Example:

a) $210 = 2. \; 3. \; 5. \; 7$. Therefore D_{210} is a Boolean algebra.

b) $66 = 2. \; 3. \; 11$, D_{66} is a Boolean algebra.

c) $646 = 2. \; 17. \; 19$, D_{646} is a Boolean algebra.

18.2.14 Theorem: If n is a positive integer and $p^2 \mid n$, where p is prime number, then D_n is not a Boolean algebra.

18.2.15 Example:

a) Take $n = 40$, then $= 2^3 \; . \; 5$, so 2 divides n three times. Therefore D_{40} is not a Boolean algebra.

Self Assessment Question 1: Test Whether D_{75} is a Boolean Algebra ?

18.2.16 Note: (i) Let $(A, \leq)$ be a finite lattice with a universal lower bound. For any non zero element b, there exists at least one atom (smallest non zero element in a Boolean algebra) *'a'* such that $a \leq b$.

(ii) There is an isomorphism from Boolean lattice *$(A, \leq)$* to *$(P(S), \subseteq)$*, where *S* is the set of atoms.

18.2.17 Theorem: Let *$(A, \vee, \wedge, -)$* be a finite Boolean algebra. Let *S* be the set of atoms. Then *$(A, \vee, \wedge, -)$* is isomorphic to the algebraic system defined by the lattice *$(P(S), \subseteq)$*.

18.3 Functions of Boolean Algebras

18.3.1 Definition: Let *$(A, \vee, \wedge, -)$* be a Boolean algebra. A Boolean expression over *$(A, \vee, \wedge, -)$* is defined as :

(i) 0 and 1 are Boolean expressions

(ii) $x_1, x_2, \ldots, x_n$ are Boolean expressions

(iii) If α is a Boolean expression, then α^1 is also a Boolean expression. Further if α_1 and α_2 are Boolean expressions then $(\alpha_1)*(\alpha_2)$ and $(\alpha_1) \oplus (\alpha_2)$ are also Boolean expressions.

(iv) If x_1 and x_2 are Boolean expressions, then $\overline{x_1}$, $x_1 \vee x_2$, $x_1 \wedge x_2$, $\overline{x_2}$ are Boolean expressions.

(v) No strings of symbols except those formed according to rules (i) to (iv) are Boolean expressions.

18.3.2 Definition: Two Boolean expressions are called **equivalent** if one can be obtained from the other by a finite number of applications of the identities of Boolean Algebra.

18.3.3 Example:

a) $0 \vee x$

b) $\left(x_1 \vee \overline{x_2}\right) \wedge \left(\overline{x_1 \wedge x_3}\right)$

c) $\overline{2 \wedge 3}$

are Boolean expressions.

Self Assessment Question 2: Write an equivalent Boolean expression for E (x_1, x_2, x_3) = $(x_1 \wedge x_2) \vee (x_1 \wedge \overline{x_3})$.

Self Assessment Question 3: Find equivalent Boolean expression for $(x \vee y) \wedge (x^1 \vee y)$

Self Assessment Question 4: Are there any Boolean algebra having 3 or 5 elements? Why or why not.

18.3.4 Definition: Let $f(x_1, x_2, ..., x_n)$ be a Boolean expression of n variables over a Boolean algebra *{0, 1}* (That is, for an assignment of values *1* (true) or *0* (false) to the variables). The values of f for various values of $x_1, x_2, ..., x_n$ can be listed in a table is called truth table.

18.3.5 Notation: $f : B^n \longrightarrow B$ where $B = \{ 0, 1\}$ $f\left(x_1, x_2, ..., x_n\right) = 0 \text{ or } 1$ where each $x_1 \in$ $\{0, 1\}, 1 \leq i \leq n$ (f is called a Boolean function on n variables)

18.3.6 Example: $E\left(x_1, x_2, x_3\right) = \left(\overline{x_1} \wedge x_2 \wedge \overline{x_3}\right) \vee \left(x_1, \wedge \overline{x_2}\right) \vee = \left(x_1 \wedge x_3\right)$ over ({0, 1}), ∨, ∧ , *–)* tabulated below.

(x_1, x_2, x_3)	$E(x_1, x_2, x_3)$
(0, 0, 0)	0
(0, 0, 1)	0
(0, 1, 0)	1
(0, 1, 1)	0
(1, 0, 0)	1
(1, 0, 1)	1
(1, 1, 0)	0
(1, 1, 1)	1

18.3.7 Definition: A Boolean expression on n variables $(x_1, x_2, ..., x_n)$ is said to be a **minterm** if it is of the form $\tilde{x}_1 \wedge \tilde{x}_2 \wedge ... \wedge \tilde{x}_n$, where $\tilde{x}_i = x_i \; or \; \overline{\overline{x}}_i$

18.3.8 Definition: A Boolean expression over *({0, 1}, ∨, ∧, –)* is said to be in **disjunctive normal form** (denoted as, dnf)if it is the join of minterm. (dnf also called as sum of products of canonical form).

18.3.9 Example: The expression $\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}$, $x_1 \wedge x_2 \wedge x_3$, $\overline{x_1} \wedge x_2 \wedge \overline{x_3}$ minterms.

The expression $\left(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}\right) \vee \left(\overline{x_1} \wedge x_2 \wedge \overline{x_3}\right) \wedge \left(x_1 \wedge x_2 \wedge x_3\right)$ is in dnf.

18.3.10 Example: Write the following Boolean expressions in an equivalent sim of products canonical form in three variables x_1, x_2, x_3.

(i) $x_1 * x_2^1$ (ii) $x_2 \oplus x_3^1$ (iii) $(x_1 \oplus x_2)^1 \oplus (x_1^1 * x_3)$.

Solution: From the laws of Boolean Algebra, we get

(i) $x_1 * x_2^1 = x_1 * x_2^1 * 1$

$= x_1 * x_2^1 * (x_3 \oplus x_3^1)$

$= (x_1 * x_2^1 * x_3) \oplus (x_1 * x_2^1 * x_3^1)$

(ii) $x_2 \oplus x_3^1 = [x_2 * (x_3 \oplus x_3^1)] \oplus [x_3^1 * (x_2 \oplus x_2^1)]$

$= (x_2 * x_3) \oplus (x_2 * x_3^1) \oplus (x_3^1 * x_2) (x_3^1 \oplus x_2^1)$

$= (x_2 * x_3) \oplus (x_2 * x_3^1) \oplus (x_3^1 \oplus x_2^1)$

$= [(x_1 \oplus x_1^1) * (x_2 * x_3)] \oplus [(x_1 \oplus x_1^1) * (x_2 * x_3^1)] \oplus [(x_1 \oplus x_1^1) * (x_2^1 \oplus x_3^1)].$

$= [(x_1 * x_2 * x_3) \oplus (x_1^1 * x_2 * x_3) \oplus (x_1 \oplus x_2 * x_3^1) \oplus (x_1^1 * x_2 * x_3^1)$

$\oplus (x_1 * x_2^1 * x_3^1) \oplus (x_1^1 * x_2^1 * x_3^1)].$

(iii) Similar.

18.3.11 Definition: A Boolean expression of n variables $x_1, x_2, \ldots x_n$ is said to be a **maxterm** if it is of the form $\tilde{x}_1 \vee \tilde{x}_2 \vee \ldots \vee \tilde{x}_n$ where $\tilde{x}_i = x_i$ *or* $\overline{x_i}$

18.3.12 Definition: A Boolean expression over *({0, 1}, ∨, ∧ , −)* is said to be in **conjunctive normal form** (denoted as, C*nf*) if it is a meet of maxterms. (cnf is also called as product of sums canonical form).

For example, $(x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3)$ is in Cnf.

18.3.13 Note: (i) Consider f : $\{0, 1\}^n \to \{0, 1\}$

To each $(x_1, x_2, \ldots, x_n)$, we have minterm, $\tilde{x}_1 \wedge \tilde{x}_2 \wedge \ldots \wedge \tilde{x}_n$, where $\tilde{x}_i = \quad x_i$ if the i^{th}

component of the *n*-tuple is 1, and $\tilde{x}_i = \overline{x_i}$ if the i^{th} component of the *n* tuple is 0.

(ii) Given $f : \{0, 1\}^n \rightarrow \{0, 1\}$, we can obtain a Boolean expression in dnf (respectively, *cnf*) corresponding to this function by having a minterm (respectively, maxterm), corresponding to each ordered n – tuple of 0's and 1's for which the value of the function *f* is 1 (respectively, 0).

(iii) *cnf* of *f* is the complement of dnf of $\overline{f}$

$f : \{0, 1\}^n \rightarrow \{0, 1\}$, maxterm,

$$\tilde{x}_1 \vee \tilde{x}_2 \vee ... \vee \tilde{x}_n \text{ where } \tilde{x}_j = \begin{cases} x_i \textit{ if the } i^{th} \textit{ component of } n - \textit{tuple is } 0 \\ \tilde{x}_i \textit{ if the } i^{th} \textit{ component of } n - \textit{tuple is } 1 \end{cases}$$

18.3.14 Example: Consider the Boolean expression

$$f(x_1, x_2, x_3) = \left[x_1 \wedge \left(\overline{x_2 \vee x_3}\right)\right] \vee \left[\left[(x_1 \wedge x_2) \vee \overline{x_3}\right] \wedge x_1\right] \text{ over } (\{0, 1\}, \wedge, \vee, -).$$

Write *dnf* and *cnf.*

Solution:

$x_1\ x_2\ x_3$	f	$\overline{f}$
0 0 0	0	1
0 0 1	0	1
0 1 0	0	1
0 1 1	0	1
1 0 0	1	0
1 0 1	0	1
1 1 0	1	0
1 1 1	1	0

Minterms: $x_1 \wedge \overline{x_2} \wedge \overline{x_3}$, $x_1 \wedge x_2 \wedge \overline{x_3}$, $x_1 \wedge x_2 \wedge x_3$

dnf f: $\left(x_1 \wedge \overline{x_2} \wedge \overline{x_3}\right) \vee \left(x_1 \wedge x_2 \wedge \overline{x_3}\right) \vee \left(x_1 \wedge x_2 \wedge x_3\right)$

Maxterm: $x_1 \vee x_2 \vee x_3$, $x_1 \vee x_2 \vee \overline{x_3}$, $x_1 \vee \overline{x_2} \vee x_3$, $x_1 \vee \overline{x_2} \vee \overline{x_3}$, $\overline{x_1} \vee x_2 \vee \overline{x_3}$

Cnf: $\left(x_1 \vee x_2 \vee x_3\right) \wedge \left(x_1 \vee x_2 \vee \overline{x_3}\right) \wedge \left(x_1 \vee \overline{x_2} \vee x_3\right)$

$$\wedge \left(x_1 \vee \overline{x_2} \vee \overline{x_3}\right) \wedge \left(\overline{x_1} \vee x_2 \vee \overline{x_3}\right)$$

Alternatively, *cnf* of can be found as follows :

$$\text{dnf } \overline{f} = \left(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}\right) \vee \left(\overline{x_1} \wedge \overline{x_2} \wedge x_3\right) \vee \left(\overline{x_1} \wedge x_2 \wedge \overline{x_3}\right)$$

$$\vee \left(\overline{x_1} \wedge x_2 \wedge x_3\right) \vee \left(x_1 \wedge \overline{x_2} \wedge x_3\right)$$

$$\overline{dnf\ \overline{f}} = \left(\overline{\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}}\right) \wedge \left(\overline{\overline{x_1} \wedge \overline{x_2} \wedge x_3}\right) \wedge \left(\overline{\overline{x_1} \wedge x_2 \wedge \overline{x_3}}\right)$$

$$\wedge \left(\overline{\overline{x_1} \wedge x_2 \wedge x_3}\right) \wedge \left(\overline{x_1 \wedge \overline{x_2} \wedge x_3}\right)$$

$$= \left(x_1 \vee x_2 \vee x_3\right) \wedge \left(x_1 \vee x_2 \vee \overline{x_3}\right) \wedge \left(x_1 \vee \overline{x_2} \vee x_3\right)$$

$$\wedge \left(x_1 \vee \overline{x_2} \vee \overline{x_3}\right) \wedge \left(\overline{x_1} \vee x_2 \vee \overline{x_3}\right)$$

$$= cnf\ \ f$$

18.4 Answers to Self Assessment Questions

SAQ 1.

Take n $= 75$. Then $5^2 \mid 75$ (since $75 = 3.5^2$), we have D_{75} is not a Boolean algebra.

SAQ 2.

The equivalent Boolean expression is: $x_1 \wedge (x_2 \vee \overline{x_3})$.

SAQ3.

(i). x.

(ii). $x \wedge y$.

(iii). $x \vee y$.

SAQ4.

No, each Boolean Algebra must have 2^n elements.

18.5 Summary

This unit provides the fundamental idea of the algebraic system namely Boolean algebra with two binary operations (join and meet) and a unary operation (complementation). Several properties of the Boolean algebras were discussed. The reader able to know application of Boolean algebra in various branches like computer science, electrical engineering (switching networks), and communication engineering. Particularly, devices such as mechanical switches, diodes, magnetic dipoles, and transistors are two state devices.

18.6 Technical Terms

Finite Boolean Algebra: A Boolean Algebra with finite number of elements is called a finite Boolean Algebra.

Truth Table: Let $f(x_1, x_2, ..., x_n)$ be a Boolean expression of n variables over a Boolean algebra $\{0, 1\}$ (That is, for an assignment of values (true) or 0 (false) to the variables). The values of f for various values of $x_1, x_2, ..., x_n$ can be listed in a table.

Boolean Function on n-variables:	$f : B^n \longrightarrow B$ where $B = \{ 0, 1\}$ $f\left(x_1, x_2, ..., x_n\right) = 0$ *or 1* where each $x_1 \in \{0, 1\}, 1 \le i \le n$
DNF:	The join of minterm. (or sum of products of canonical form).
CNF:	The meet of maxterms (or a product of sums canonical form).

18.7 Model Questions

1. Find equivalent Boolean expression for the following

(i). $x \wedge (y \vee (y^1 \wedge (y \vee y^1)))$

(ii). $(z^1 \vee x) \wedge ((x \wedge y) \vee z) \wedge (z^1 \vee y)$

(iii). $\left[(x \wedge z) \vee (y^1 \vee z)^1\right] \vee \left[(y \wedge z) \vee (x \wedge z^1)\right]$

2. Write the Boolean function values for f : A^2 → A, where A = {0, 1} with f (x$_1$, x$_2$) = $(x_1 \wedge \overline{x_1}) \vee x_2$.

3. Consider the Boolean polynomial f (x, y, z) = x ∧ (y ∨ z^1). If B = {0, 1}, compute the truth table of the function f : B$_3$ → B defined by f.

4. Consider the Boolean polynomial f(x, y, z) = $(x \wedge y^1) \vee (y \wedge (x^1 \vee y))$.

If B = {0, 1}, compute the truth table of the function f: B$_3$ → B defined by f.

5. Rewrite the given Boolean polynomial to obtain the requested format.

(i). $(x \wedge y^1 \wedge z) \vee (x \wedge y \wedge z)$; two variables and one operation.

(ii). $(z \vee (y \wedge (x \vee x^1)) \wedge (y \wedge z^1)^1$; one variable.

(iii). $(y \vee z) \vee x^1 \vee (w \wedge w^1)^1 \vee (y \wedge z^1)$; two variables and two operations.

6. Write the disjunctive and conjuctive normal form for f $(x_1, x_2, x_3) = [\left[x_1 \wedge \overline{(x_2 \vee x_3)}\right]] \vee \left\{\left[(x_1 \wedge x_2) \vee \overline{x_3}\right] \wedge x_1\right\}$, by writing minterms and maxterms.

18.8 References

1. Akerkar Rajendra and Akerkar Rupali "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, "Discrete Mathematical Structures" PHI, New Delhi, 1999.

3. Liu.C.L., "Elements of Discrete Mathematics", Mc Hill.

4. Satyanarayana Bhavanari "Lattices and Boolean Algebras", Satyasri Maths Study Centre, Guntur, 2002.

5. Shanker Rao, G., "Discrete Mathematical Structures", New Age International Publishers, New Delhi, 2002.

6. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

7. Trembly, J.P., and Manohar, R. "Discrete Mathematical Structures with Applications to Computer Science", Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Mr. T. V. Pradeep Kumar**

Lesson 19

Boolean Functions and Gating Networks

Objectives

At the end of the Lesson the student must be able to:

(i) Write the values of Boolean expressions
(ii) Representation of Boolean algebra through gating network.
(iii)Learn several applications of Boolean algebras in science and engineering.

Structure

19.1 Introduction

Some special type of net-works is used in digital computers for the processing of information in it. These networks are represented by block diagrams. Logic circuits are structures which are built up from certain elementary circuits called logic gates. In this lesson we shall represent a

Boolean function in a gating network. Various gates will be used for representing the expressions.

First let us construct the truth tables for the following Boolean expressions.

19.2 Boolean Functions

Let $f(x_1, x_2, \ldots, x_n)$ be a Boolean expression of n variables over a Boolean Algebra B_n. For an assignment of values 1 or 0 (True or False) to the variables, we can evaluate the value of the expression $f(x_1, x_2, \ldots, x_n)$ by substiting the variables, in the expression by their values. The values of f for several of $x_1, x_2, \ldots, x_n$ can be listed in a truth table.

19.2.1 Example:

a) $f_1(x_1, x_2) = x_1 \vee x_2$

b) $f_2(x_1, x_2) = x_1 \wedge x_2$

c) $f_3(x_1) = x_1'$

Solution: The truth table for $x_1 \vee x_2$, $x_1 \wedge x_2$, x_1' are given below.

x_1	x_2	$f_1 = x_1 \vee x_2$	$f_2 = x_1 \wedge x_2$	$f_3 = x_1'$
0	0	0	0	1
0	1	1	0	1
1	0	1	0	0
1	1	1	1	0

19.2.2 Example: Find the truth values for $f(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (x_1' \vee x_2') \wedge (x_2 \vee x_3')$.

Solution: The table for $f(x_1, x_2, x_3)$ given below.

x_1	x_2	x_3	$x_1 \vee x_2$	$x_1' \vee x_2'$	$x_2 \vee x_3'$	$f(x_1, x_2, x_3)$
0	0	0	0	1	1	0
0	0	1	0	1	0	0
0	1	0	1	1	0	0
0	1	1	1	1	0	0
1	0	0	1	1	1	1
1	0	1	1	1	0	0
1	1	0	1	0	0	0
1	1	1	1	0	0	0

19.3 Gating Networks

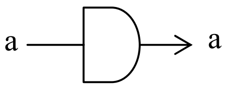
19.3.1 Definition: (i) Two Boolean expressions of n variables are said to be **equivalent** if they assume the same value for every assignment of values to the n variables.

(ii) Some switches or switching circuits may be represented by some new type of diagrams which are called as **gates**. By using these gates, we can represent any switching circuit as a combination of the gates. This is a **symbolic representation.**

(ii) From (i) we can conclude that a gate (or a combination of gates) is a polynomial *p*.

(iii) A symbolic representation (that is, a combination of gates) which represents a polynomial, is called a **gating network**.

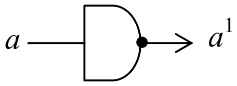
19.3.2 Notation: Different gates that we use are given below:

(i) 

identity-gate (symbolizes x);

If the input is x then the output is converted into x^1 by an inverter.

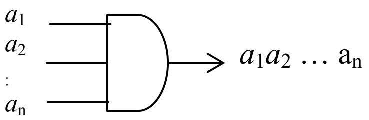
(ii)



NOT-gate (or *inverter*)
(symbolizes x^1);

AND Gate: If there be two or more inputs then the output will be a function of those inputs given below.

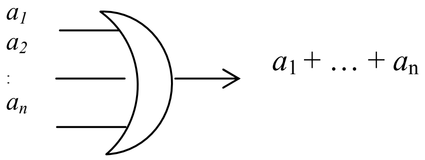
(iii)



AND-gate
(Symbolizes)
$x_1x_2 \ldots x_n$);

OR gate: It converts two and more inputs into a single function given as follows.

(iv)

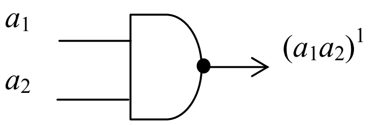


OR-gate
(symbolizes
$x_1 + \ldots + x_n$)

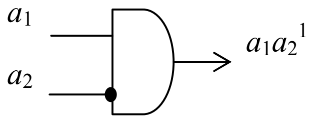
We also use a small black disk (either before or after) one of the other gates to indicate an inverter.

19.3.3 Example:

(i)



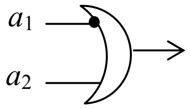
(ii)



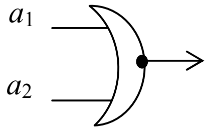
19.3.4 Note: In Boolean Algebra, we have three basic operations namely, AND, OR and NOT. Some other operations can be defined in terms of these operations.

The NAND operation is the complement of OR operation and also written as not-OR and uses an OR system followed by a small circle. Thus a NOR gate is equivalent to an OR gate followed by a NOT gate.

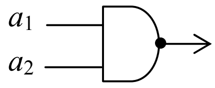
The NAND operation is the complement of AND operation and written as not-AND and uses an AND symbol followed by a small circle.

(i) 

$a_1{}^1 + a_2$ **Subjunction-gate**

(ii) 

$(a_1 + a_2)^1$ **NOR-gate** or **Pierce-operation**

(iii) 

$(a_1a_2)^1$ **NAND-gate** or **Sheffer-operation**

19.3.5 Example: For the expression $f = (x \wedge y \wedge z) \vee (x \wedge y^1 \vee z) \vee (x^1 \wedge y)$ design the logic diagram.

Solution: The following logic diagram shows the given function.

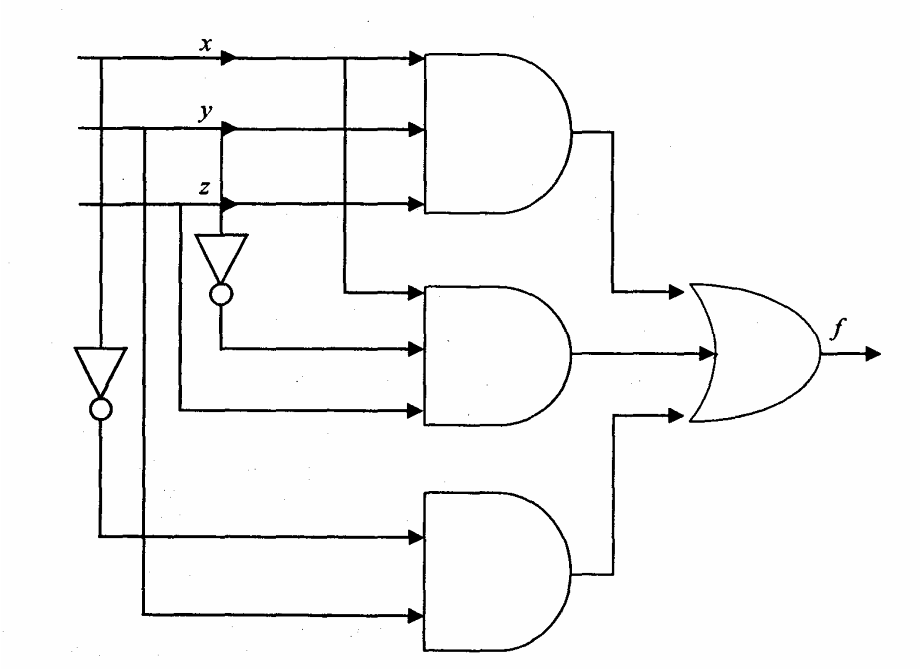


Fig. 19.3.5

19.3.6 Example: Find the Boolean expression for the following logic diagram.

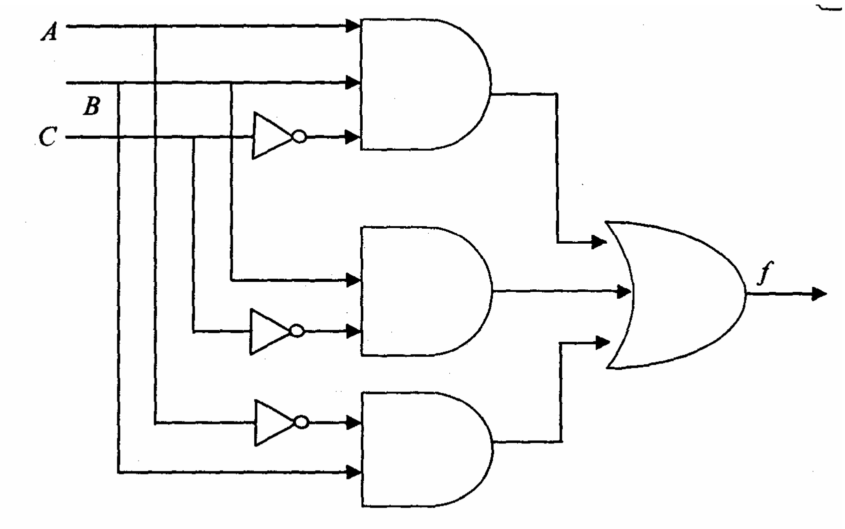
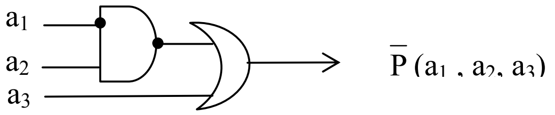


Fig. 19.3.6

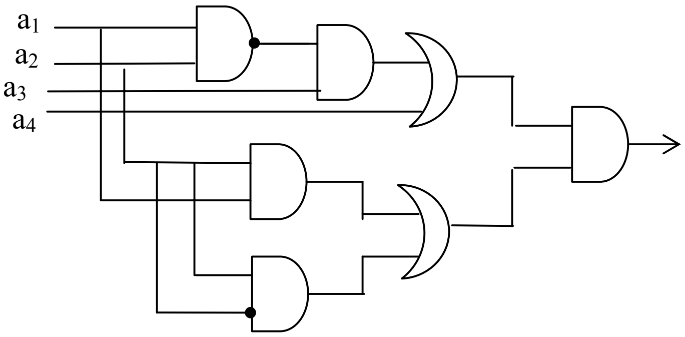
Solution: $ABC^1 + BC^1 + A^1B$.

19.3.7 Problem: Write down the gating network for the polynomial $p = (x_1{}^1 x_2)^1 + x_3$.

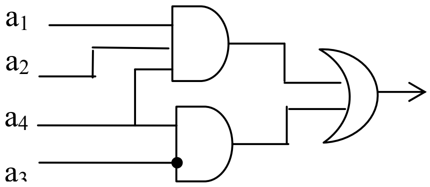
Solution: The required gating network is given by the Figure.



19.3.8 Problem: (i) Find the polynomial p which corresponds to the gating network given in the Figure-12. (ii) Find a simplified gating network which operates in the same way as the gating network given in Figure.



Solution: (i) The polynomial that represents the given gating network is $p = ((x_1x_2)^1x_3 + x_4)(x_1x_2 + x_3{}^1 x_4)$. (ii) By using the Quine-McCluskey algorithm we get a simplified form $q = x_1x_2x_4 + x_3{}^1 x_4$ of p.

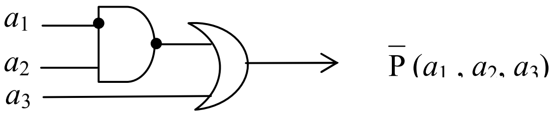


Now, the gating network which represents q is given by the Figure-13.

19.4 Answers to Self Assessment Questions

SAQ 1.

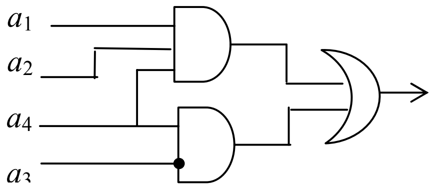
The required gating network is given by the Figure1.



SAQ2.

(i) The polynomial that represents the given gating network is $p = ((x_1x_2)^1x_3 + x_4)\,(x_1x_2 + x_3{}^1\,x_4)$.

(ii) By using the Quine-McCluskey algorithm we get a simplified form $q = x_1x_2x_4 + x_3{}^1\,x_4$ of p.



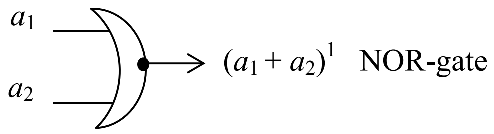
Now, the gating network which represents q is given by the Figure.

19.5 Summary

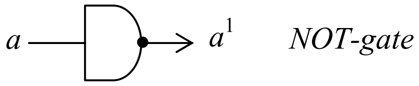
This lesson provides the diagram representations of Boolean algebras. This has lot of importance in digital and signal communication systems. This lesson also milieu for the many branches of science, engineering and technology.

19.5 Technical Terms

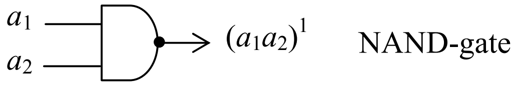
NOR Gate



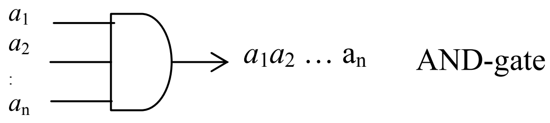
NOT Gate



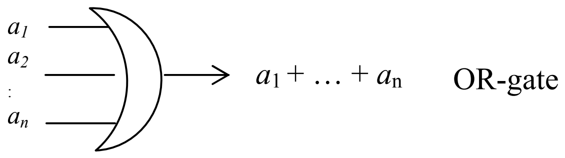
NAND Gate



AND Gate



OR Gate.



19.7 Model Questions

1. Write down the gating network for the polynomial $p = (x_1{}^1 x_2)^1 + x_3$.

2. (i) Find the polynomial p which corresponds to the gating network given in the Figure (ii) Find a simplified gating network which operates in the same way as the gating network given in Figure.

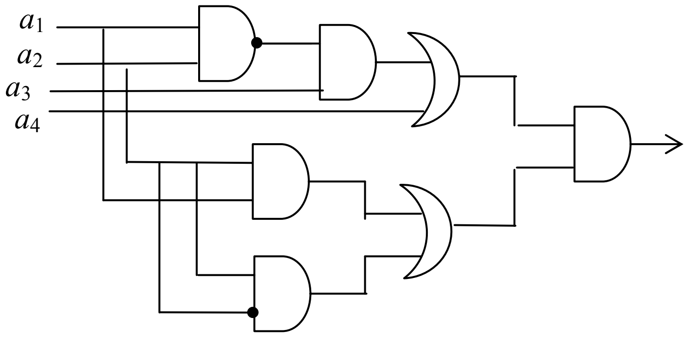


Fig. 19.7.2

3. Draw the gating network corresponding to the Boolean function

$(x + y)(x^1 + y + z^1)$.

4. Construct a logic circuit corresopnding to Boolean function

$f(x, y, z) = xyz + xy^1z$.

5. Construct the truth table for the following Boolean expressions.

(i) $(x * y) \oplus (x * z^1)$

(ii) $y * (x * (y * z)^1)$

19.8 References

1. Akerkar Rajendra and Akerkar Rupali. “Discrete Mathematics”, Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, “Discrete Mathematical Structures” PHI, New Delhi, 1999.

3. Richard Johnsonbaugh “Discrete Mathematics”, Pearson Education, Asia, 2001.

4. Satyanarayana Bhavanari “Lattices and Boolean Algebras”, Satyasri Maths Study Centre, Guntur, (0863 – 2232138) 2002.

5. Shanker Rao, G., “Discrete Mathematical Structures”, New Age International Publishers, New Delhi, 2002.

6. Somasundaram Rm. “Discrete Mathematical Structures” Prentice Hall India Pvt. Limited, New Delhi, 2003.

7. Trembly, J.P., and Manohar, R. “Discrete Mathematical Structures with Applications to Computer Science”, Mc-Graw Hill, 1975.

Name of the Lesson Writer: **Dr T. Srinivas**

Lesson 20

Minimization of Boolean Functions-Karnaugh Maps

Objectives

At the end of the Lesson the student must be able to:

(i) Know the Boolean functions and minimization process
(ii) Learn technique of Karnaugh map.
(iii)Write the simplified expressions using Karnaugh map.
(iv)Learn several applications of Boolean functions in science and engineering.

Structure

20.1 Introduction

Boolean algebra is used as a tool for expressing problems of circuit design. In the previous sections, we have seen some of them viz., Hasse diagrams, truth tables and logical diagrams. In this lesson, yet another widely -used way is discussed. This type of representation helps us to simplify the functions. We discussed a new structure, called Karnaugh map, is an area which is subdivided into 2^n cells, one for each possible input combination for a Boolean function of n variables. Half the number of cells is associated with an input value of 1 for one of the variables and the other half the number of cells, with the input value 0 for the same variable. More precisely, the Karnaugh map corresponding to Boolean expressions in n variables is an area which is subdivided into 2^n cells (squares) each of which corresponds to one of the fundamental products or minterms in n variables.

20.2 Representation of Boolean Functions

For example, K-map in 3 variables has 2^3 = 8 cells each of which correspond to one of the following minterms xyz, xyz^1, xy^1z, xy^1z^1, x^1yz, x^1yz^1, x^1y^1z, $x^1y^1z^1$.

The following fig. shows the K-maps for different variables.

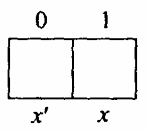


Fig 1: K-map for 1 variable

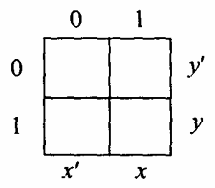


Fig 2: K-map for 2 variable

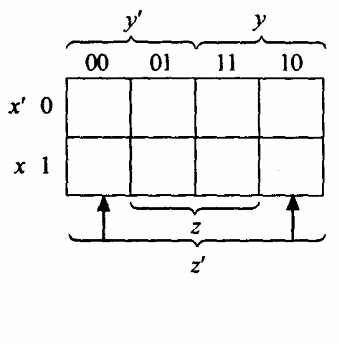


Fig 3: K-map for 3 variables

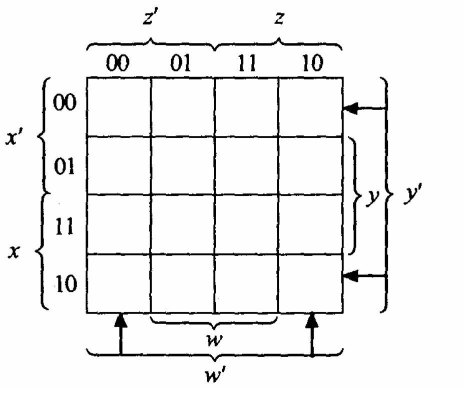


Fig 4: K-map for 4 variables

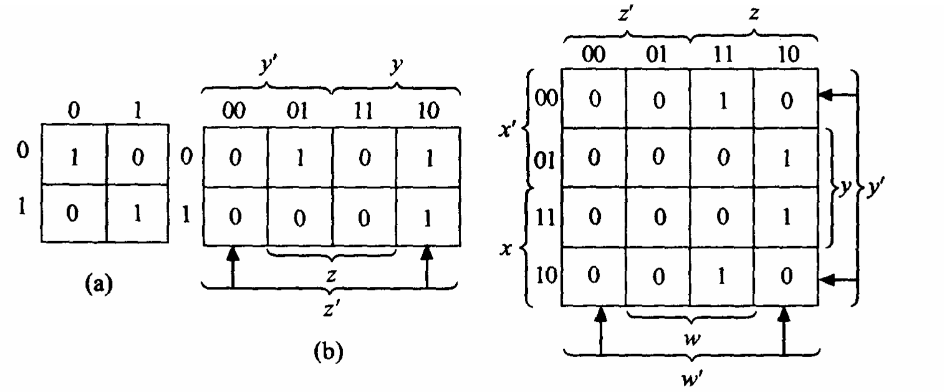
20.2.1 Example: Find the K-map for the following expression:

(a) $(x * y) \oplus (x^1 * y^1)$

(b) $(x^1 * y^1 * z \oplus x^1 * y * z^1 \oplus x * y * z^1)$

(c) $(x^1 * y^1 * z * w) \oplus (x^1 * y * z * w^1) \oplus (x * y^1 * z * w) \oplus (x * y * z * w^1)$

Solution: K- maps for the above expressions are in the following fig.

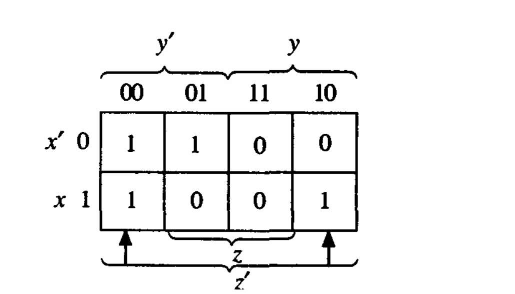


20.2.2 Example: For the Boolean expression represented by the following truth table, give K-map representation. Also write the expression.

x	y	z	f(x, y, z)
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Solution: The following fig. represents the K-map for the given Boolean expression.

The expression is $x^1y^1z^1 \oplus x^1y^1z \oplus xy^1z^1 \oplus xyz^1$.



	00	01	11	10
x′ 0	1	1	0	0
x 1	1	0	0	1

20.3 Minimization of Boolean Expressions

The process of minimization of circuits is important in circuit design. The aim of minimization is to reduce the number of gates to a minimum. Minimization of an expression is the selection of the simplest representative expression of an equivalence class to serve as our circuit. K-maps are used in the minimization process for functions of six or fewer variables.

Two minterms or fundamental products (cells in a K-map) are said to be adjacent if they have the same variables and if they differ in exactly one literal which must be a complemented variable in one product and uncomplemented in the other. For example,

1. xyz^1 and xy^1z^1 are adjacent
2. x^1yzw and x^1yz^1w are adjacent
3. x^1yzw and xyz^1w are not adjacent as they differ in two literals.

20.3.1 Theorem: Sum of two adjacent products P_1 and P_2 is a fundamental product with one less literal.

Proof: Two adjacent products P_1 and P_2 are represented as

$$P_1 = a_1a_2 \ldots a_{r-1}a_ra_{r+1} \ldots a_k$$

and $P_2 = a_1a_2 \ldots a_{r-1}\, a_r^1\, a_{r+1} \ldots a_k$

Then $P_1 \oplus P_2 = a_1a_2 \ldots a_{n-1}a_ra_{r+1} \ldots a_k(a_r \oplus a_r^1) = a_1a_2 \ldots a_{r-1}a_{r+1} \ldots a_k$

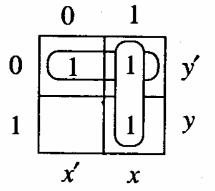
20.3.2 Example: For three variables, $xyz^1 \oplus xy^1z^1 = xz^1 (y \oplus y^1) = zz^1$.

The above result and the absorption operation xyz + xy = xy help us in grouping the terms. Minimization involves grouping of adjacent cells with l's in them into a largest possible block of such cells. Simplified expression must contain minimum number of such blocks.

20.3.3 Note: In case of two variables, a block will be either a pair of adjacent squares or an individual square.

20.3.4 Example: Minimize the expression $f = xy \oplus xy^1 \oplus x^1y^1$

Solution: The K-map for the given expression is shown in Fig.



Therefore f contains two blocks corresponding to x and other to y^1. Hence $f = x \oplus y^1$.

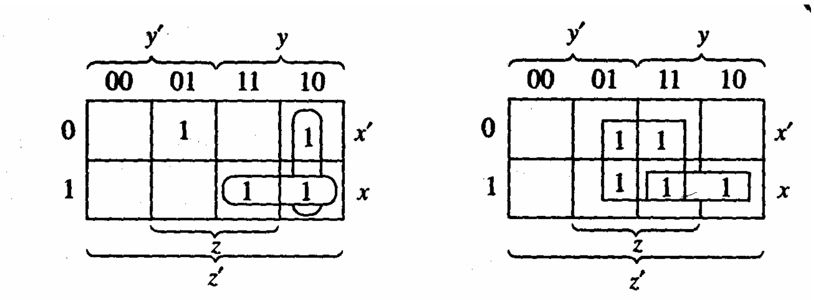
20.3.5 Note: In the case of 3 variables, a basic rectangle contains either a square, or two adjacent squares, or four squares which form a one-by-four or a two-by- two rectangle. A maximal basic rectangle is a block.

20.3.6 Example: Minimize the following expressions:

(a) $f_1 = xyz \oplus xyz^1 \oplus x^1yz^1 \oplus x^1y^1z$

(b) $f_2 = xyz \oplus xyz^1 \oplus xy^1z \oplus x^1yz \oplus x^1y^1z$

Solution: K-maps for the given expressions are given in Figures.



Their minimized expressions are

(a) $x^1y^1z \oplus yz^1 \oplus xy$, (b) $z \oplus xy$.

Note that in the case of 4 variables, a basic rectangle is a square, two adjacent squares, four squares which form one-by-four or two-by-two rectangle or eight squares which form a two-by-four rectangle. A maximal basic rectangle is a *block.*

20.3.7 Example: Minimize the following expressions:

$$\text{(a) } w^1 \oplus y * (x^1 \oplus z^1)$$

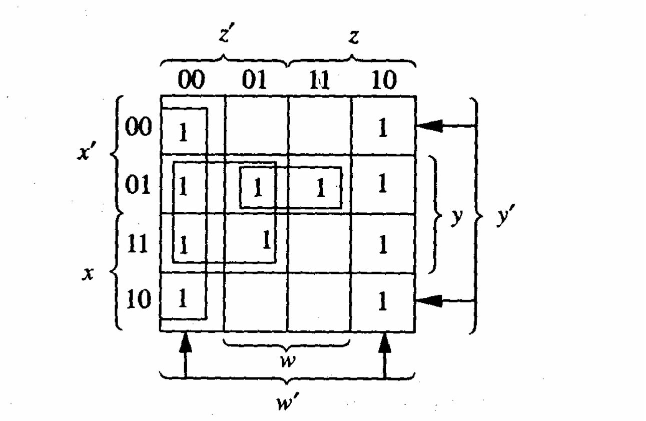
$$\text{(b) } x^1y^1zw \oplus yzw^1 \oplus y^1z^1 \oplus y^1w^1.$$

Solution: Minimized expressions are: (a) $w^1 \oplus yz^1 \oplus wx^1y$ and

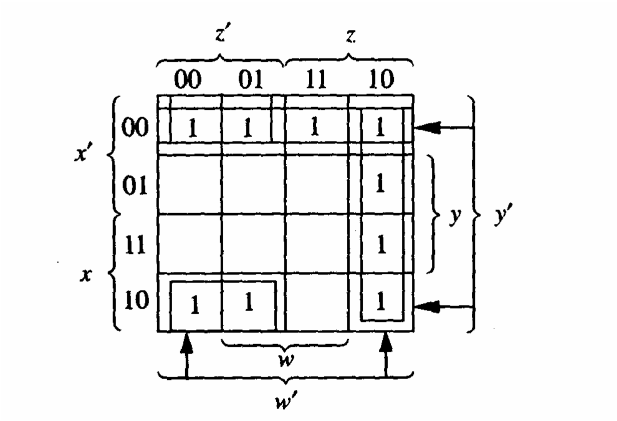
(b) $y^1z^1 \oplus x^1y^1 \oplus zw^1$.

Their K-maps are shown in Fig.

(a) K-map for $w^1 \oplus y * (x^1 \oplus z^1)$



(b) The K-map for $x^1y^1zw \oplus yzw^1 \oplus y^1z^1 \oplus y^1w^1$.



Self Assessment Question 1: Express the K-map in two variables corresponding to Boolean expression E (x_1, x_2) for two variables using binary digits 0 and 1.

Self Assessment Question 2: Express the K-map corresponding to Boolean expression E(x, y, z) with three variables x, y, z and represent three variables using binary digits 0 and 1.

20.3.8 Case of Four Variables

The Karnaugh map corresponding to Boolean expression E(x, y, z, t) is shown in table (a) and the alternative way of representing using binary digits 0 and 1 shown in table (b). There are exactly 16 minterms with four variables.

	x′y′	x′y	xy′	xy
z′t	x′y′z′t′	x′yz′t′	xy′z′t′	xyz′t
z′t	x′y′z′t	x′yz′t	xy′z′t	xyz′t
zt′	x′yzt′	x′yzt′	xy′zt′	xyzt′
zt	x′y′zt	x′yzt	xy′zt	xyzt

Table (a)

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

Table (b)

20.3.9 Example: Use Karnaugh maps to find minimal form for the following Boolean functions.

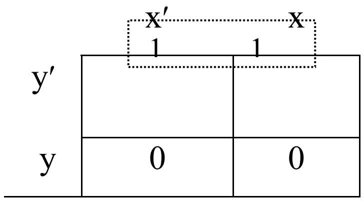
(i) E (x, y) = x′y′ + xy′

(ii) E (x, y) = x′y′ + x′y + xy′

(iii) E (x, y) = xy + xy′

(iv) E (x, y) = xy + x′y′

Solution: (i) Boolean expression E(x, y) = x′y′ + xy′ is shown by two variables K – map by putting 1 in the square which correspond to x′y′ and xy′. The remaining squares are filled with 0’s as shown in the table.



Two adjacent squares x′y′ and xy′ containing 1 have been enclosed in a rectangle. These two terms can be looped to give a resultant that eliminates x since it appears in both complimented and uncomplemented forms

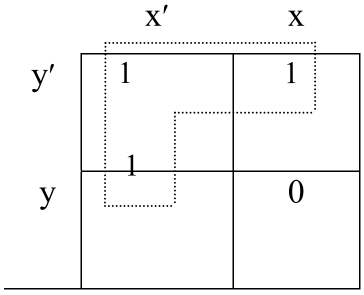
so $E(x_1, x_2) = y'$

We can verify this by algebraically as

$$E(x, y) = x'y' + xy'$$
$$= (x' + x)\, y' = 1.y' = y'$$

(ii) $E(x, y) = x'y' + x'y + xy'$

Karnaugh-map for the given function is

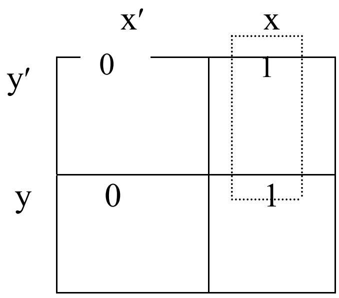


There are two pairs of 1s and can be combined as shown in the table. Since 1 value of first column and first row has been enclosed twice therefore decomposition into rectangles is not unique. We should try to use largest possible rectangles. The group of horizontal 1 square give y′ and vertical 1 square give x′. Hence the simpler expression is

$$E\,(x, y) = x' + y'$$

(iii) $E(x, y) = xy + xy'$

Karnaugh-map for the given function is given by



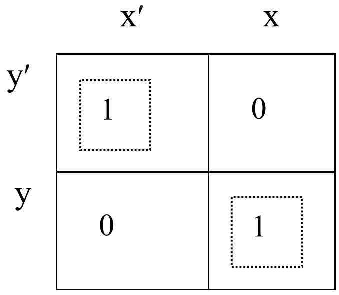
	x'	x
y'	0	1
y	0	1

We represent two squares with 1s in them by a rectangle. This is corresponding to x.

$E(x, y) = x$

$E(x, y) = xy + x'y'$

Karnaugh map for the given function is



	x'	x
y'	1	0
y	0	1

We observe that given function consists of two isolated square which represent xy and $x'y'$ (they are known also as prime implicants)

$E(x, y) = xy + x'y'$ is the minimal form.

Self Assessment Question 3: Simplify the following Boolean expressions using K– map

(i) E(x, y, z) = x′y′z′ + xy′z′

(ii) E(x, y, z) = xyz′ + xyz

(iii)E(x, y, z) = x′y′z′ + x′yz′ + xyz′ + xy′z

(iv) E(x, y, z) = xyz + xyz′ + x′yz′ + x′y′z

20.4 Answers to Self Assessment Questions

SAQ 1.

Karnaugh Map for two variables.

	x′	x
y′	x′y′	xy′
y	x′y	xy

(a)

x y	0	1
0	00	10
1	01	11

(b)

SAQ 2.

Karnaugh map with three variables

	x′y′	x′y	xy′	xy
z′	x′y′z′	x′yz′	xy′z′	xyz′
z	x′y′z	x′yz	xy′z	xyz

$x_1\,x_2$ x_3	00	01	10	11
0	000	010	100	110
1	001	011	101	111

3. (i) Three variables K–map of the expression is shown in the table

	x′y′	xy′	xy	xy′
z	1	0	1	0
z′t	0	0	0	0

In the K – map the top and bottom rows of squares are considered to be adjacent. Thus the two 1s in this map can be looped to provide a simpler result.

E (x, y, z) = y′z′

(ii) Karnaugh map for the function

E (x, y, z) = xyz′ + xyz

	x′y′	xy′	xy	xy′
z′	0	0	1	0
z′t	0	0	1	0

In the grouped rectangle the square represent terms xyz′ and xyz then leaving variable z since it appear in both complimented and uncomplimented forms. The simplified Boolean expression is E = x, y.

(iii) Karnaugh map corresponding to the given function

E (x, y, z) = x′y′z′ + x′yz′ + xyz′ + xy′z is shown in the figure

	x′y′	x′y	xy	xy′
z′	1	1	0	1
z	0	0	0	1

We can combine two pairs of 1s. Only 1 representing the term xy′z is isolated so answer is

$$E = x'z' + yz' + xy'z$$

(iii) E = (x, y, z) = xyz + xyz′ + x′y′z

Karnaugh map is given by

0	x′y′	x′y	xy	xy′
z′	0	1	0	0
z	1	0	1	0

We can observe that we have three maximal basic rectangles. Minimal Boolean function is

$$E = yz' + xy + x'y'z$$

20.5 Summary

In this lesson we discussed the process of reducing the number of terms in a Boolean expression representing a circuit using Karnaugh map. The method described was introduced by Maurice Karnaugh in 1953. This method is usually applied only when the function involve six or four variables. The Karnaugh map is used in minimization algorithms in digital and signal process systems. It has enormous applications in electronics and communications engineering and information technology.

20. 5 Technical Terms

Karnaugh map: Corresponding to Boolean expressions in n variables, the area is subdivided into 2^n cells (squares) each of which corresponds to one of the fundamental products or minterms in n variables.

Adjacent: Two minterms or fundamental products (cells in a K-map) are said to be adjacent if they have the same variables and if they differ in exactly one literal which must be a complemented variable in one product and uncomplemented in the other.

Looping: $E(x, y)$ with two variables x, y squares containing binary digit 1 can be represented by two rectangles. The horizontal squares represent the output of the expression $E(x, y)$ corresponding x' whereas vertical square represent the output corresponding to y'. Thus $E(x, y) = x' + y'$ (or $x' \vee y'$). The process of combining these digits is called looping.

20.7 Model Questions

1. Simplify the following Boolean expressions using K– map

(i) $E(x, y, z) = xyz + xyz' + xy'z + x'yz + x'y'z$

(ii) $E(x, y, z) = xyz + xyz' + x'yz' + x'yz' + x'y'z$

2. Minimize the following expressions:

(a) $w^1 \oplus y * (x^1 \oplus z^1)$

(b) $x^1y^1zw \oplus yzw^1 \oplus y^1z^1 \oplus y^1w^1$.

20.8 References

1. Akerkar Rajendra and Akerkar Rupali. "Discrete Mathematics", Pearson Education (Singapore) Pvt. Ltd, New Delhi, 2004.

2. Bernard Kolman, Busby R.C., Sharon Ross, "Discrete Mathematical Structures" PHI, New Delhi, 1999.

3. Hari Kishan and Shivraj Pundir "Discrete Mathematics", Pragati Prakashan, Meerut, 2005.

4. Richard Johnsonbaugh "Discrete Mathematics", Pearson Education, Asia, 2001.

5. Satyanarayana Bhavanari "Lattices and Boolean Algebras", Satyasri Maths Study Centre, Guntur, (0863 – 2232138) 2002.

6. Shanker Rao, G., "Discrete Mathematical Structures", New Age International Publishers, New Delhi, 2002.

7. Somasundaram Rm. "Discrete Mathematical Structures" Prentice Hall India Pvt. Limited, New Delhi, 2003.

Name of the Lesson Writer: **Dr T. Srinivas**