

BT 0069
Discrete Mathematics

Contents

Unit 1

Mathematical Preliminaries	1
----------------------------	---

Unit 2

Elementary Combinatorics	33
--------------------------	----

Unit 3

Recurrence Relations	64
----------------------	----

Unit 4

Partially Ordered Sets	85
------------------------	----

Unit 5

Lattices	98
----------	----

Unit 6

Algebraic Structures	117
----------------------	-----

Unit 7

Propositional Calculus and Quantifiers	145
--	-----

Unit 8

Predicate Calculus	166
--------------------	-----

Unit 9	
Finite Boolean Algebras	181
<hr/>	
Unit 10	
Formal Languages	200
<hr/>	
Unit 11	
Finite Automata	219
<hr/>	
Unit 12	
Basic Graph Theory	243
<hr/>	
Unit 13	
Algebraic Codes and Cryptography	278
<hr/>	
References	299
<hr/>	

Prof. V. B. Nanda Gopal

Director & Dean

Directorate of Distance Education

Sikkim Manipal University of Health, Medical & Technological Sciences (SMU DDE)

Board of Studies**Dr. U. B. Pavanaja (Chairman)**General Manager – Academics
Manipal Universal Learning Pvt. Ltd.
Bangalore**Prof. Bhushan Patwardhan**Chief Academics
Manipal Education
Bangalore**Dr. Harishchandra Hebbar**Director
Manipal Centre for Info. Sciences
Manipal**Dr. N. V. Subba Reddy**HOD-CSE
Manipal Institute of Technology, Manipal**Dr. Ashok Hegde**Vice President
MindTree Consulting Ltd., Bangalore.**Dr. Ramprasad Varadachar**Director, Computer Studies
Dayanand Sagar College of Engg.
Bangalore.**Mr. M. K. N. Prasad**Controller of Examinations
Sikkim Manipal University – DDE, Manipal.**Mr. Nirmal Kumar Nigam**HOP- IT
Sikkim Manipal University – DDE
Manipal.**Dr. A. Kumaran**Research Manager (Multilingual)
Microsoft Research Labs India
Bangalore.**Mr. Ravindranath.P.S.**Director (Quality)
Yahoo India
Bangalore.**Dr. Ashok Kallarakkal**Vice President
BM India, Bangalore.**Mr. H. Hiriannaiah**Group Manager
EDS Mphasis, Bangalore.**Mr. Ashok Kumar K**Additional Registrar
Sikkim Manipal University - DDE
Manipal.

Content Preparation Team**Content Writing****Dr. Kuncham Syam Prasad**Associate Professor-Dept. of Mathematics
Manipal Institute of Technology
Manipal.**Language Editing****Mrs. Aparna Ramanan**Assistant Professor (English)
Sikkim Manipal University – DDE, Manipal.**Content Editing****Mr. Deepak Shetty**Assistant Professor (Mathematics)
Sikkim Manipal University – DDE
Manipal.

Edition: Spring 2009

This book is a distance education module comprising a collection of learning material for our students. All rights reserved. No part of this work may be reproduced in any form by any means without permission in writing from Sikkim Manipal University of Health, Medical and Technological Sciences, Gangtok, Sikkim. Printed and published on behalf of Sikkim Manipal University of Health, Medical and Technological Sciences, Gangtok, Sikkim by Mr. Rajkumar Mascreen, GM, Manipal Universal Learning Pvt. Ltd., Manipal – 576 104. Printed at Manipal Press Limited, Manipal.

SUBJECT INTRODUCTION

This book, 'Discrete Mathematics' deals with different concepts in computer oriented mathematics which are interrelated to one another. To be a successful professional one should know all the techniques involved in Discrete Mathematics.

Unit 1: In this unit, we study the concept of set theory and discuss the idea of relations and functions.

Unit 2: In this unit we study the concept of Permutations and Combinations with some illustrations. Further we present the partition of integers and sets. Some basic identities involving binomial coefficients are also discussed

Unit 3: In this unit we study an alternative approach to represent the sequence by finding a Relationship among its terms. Also a few applications of Recurrences are discussed here.

Unit 4: In this unit, our focus is on Partially Ordered relation, which is defined on a set, referred as Partially Ordered Sets. We also discuss various properties of Partially Ordered Relations on a Set.

Unit 5: In this unit, we discuss the algebraic structure defined by a Lattice. Some characterizations of complemented and distributive Lattices are explained.

Unit 6: In this unit we study Algebraic Structures by investigating sets associated with single operations that satisfy certain reasonable axioms.

Unit 7: In this unit, we discuss the concept of Statements, Propositions and Tautologies. The concept of Equivalence of Formulas, Normal

Forms and Logical Inferences is discussed here with simple examples.

Unit 8: In this unit we study the concept of Predicates, Quantifiers. The terms. Free and Bound Occurrences, Rules of inference are discussed here with standard examples.

Unit 9: In this unit, we represent a Boolean function in a gating network. Various gates are used here to represent the expressions.

Unit 10: In this unit we learn about Grammars and Languages with the help of standard examples. Also the classification of Grammars is studied here with examples.

Unit 11: In this unit, we discuss the idea of Deterministic Finite Automata. The concept of Transition System is studied here with examples. The Language accepted by a DFA is also discussed here in a simple manner.

Unit 12: This unit deals with the idea of graph theory. Here we study Adjacency and Degree of a graph. The idea of Subgraphs, Trees is also discussed here. The different property of trees and Rooted Trees is stated in this unit in a simple manner.

Unit 13: This unit deals with the idea of Coding Theory. The concept of Hamming Distance, Linear Codes is discussed with simple examples. The concept of Cryptography is explained here in a simple manner

SUBJECT INTRODUCTION

This book of Discrete Mathematics deals with the different concepts in mathematics which are interrelated to one another. To be a successful professional one should be knowing all the techniques involved in Discrete Mathematics.

Unit 1: In this unit of Mathematical Preliminaries we study the concept of set theory and discuss the idea of relations and functions.

Unit 2: In this unit we study the concept of Permutations and Combinations with some illustrations. Further we present the partition of integers and sets, some basic identities involving binomial coefficients are also discussed

Unit 3: In this unit we study an alternative approach to represent the sequence by finding a relationship among its terms. Also few applications of recurrences are discussed here.

Unit 4: In this unit our interest is partially ordered relation which is defined on a set, referred as partially ordered sets. We also discuss various properties of partially ordered relations on a set.

Unit 5: In this unit we discuss the algebraic structure defined by a lattice. Some characterizations of complemented and distributive lattices are obtained

- Unit 6:** In this unit we study algebraic structures by investigating sets associated with single operations that satisfy certain reasonable axioms.
- Unit 7:** In this unit we discuss the concept of Statements, Propositions and Tautologies. The idea of Equivalence of formulas, normal forms and Logical Inferences is discussed here with simple examples.
- Unit 8:** In this unit we study the concept of Predicates, Quantifiers. The idea of Free and Bound Occurrences, Rules of inference is discussed here with standard examples.
- Unit 9:** In this unit we represent a Boolean function in a gating network. Various gates are used here for representing the expressions.
- Unit 10:** In this unit we learn about Grammars and Languages with the help standard examples. Also classification of Grammars is studied here with examples.
- Unit 11:** In this unit, we discussed the idea of Deterministic Finite Automata. The concept of Transition System is studied here with examples. The Language accepted by a DFA is also discussed here in a simple manner.
- Unit 12:** This unit deals with the idea of graph theory. Here we study Adjacency and Degree of a graph. The idea of Subgraphs, Trees is also discussed here. The different property of trees and Rooted Trees is stated in this unit in a simple manner.
- Unit 13:** This unit deals with the idea of Coding Theory. The concept of Hamming Distance, Linear Codes is discussed with simple examples. The concept of Cryptography is explained here in a simple manner

Unit 1

Mathematical Preliminaries

Structure

- 1.1 Introduction
 - Objectives
- 1.2 Sets
- 1.3 Relations
- 1.4 Functions
- 1.5 Basic Number Theory
- 1.6 Summary
- 1.7 Terminal Questions
- 1.8 Answers

1.1 Introduction

The concepts of set, relation and function are of fundamental importance in modern mathematics. The idea of a set has been intuitively used in mathematics since the time of ancient Greeks. Now set theory and its associated branches such as Group theory, Automata, Coding theory etc., have far reaching applications.

The systematic development of set theory is attributed to the German mathematician George Cantor (1845 – 1918).

Some elementary definitions of set theory have been studied by students in the high school standard. In this chapter we briefly give some preliminaries of set theory and discuss the relations and functions.

Objectives:

At the end of the unit you would be able to

- perform different operations on sets
- define functions and examples
- describe different types of relations and properties.
- learn the mathematical induction.

1.2 Sets

The notion of a set is common; intuitively a set is a well defined collection of objects. The objects comprising the set are called its member or elements. The sets are usually denoted by the capital letter A, B, X, Y etc., and its elements by small letters a, b, x, y, \dots . The statement, 'x' is an element of 'A' is denoted by $x \in A$ and is read as "x belongs to A". If 'x' is not an element of the set 'A' then it is denoted by $x \notin A$ (read as 'x' does not belong to A). Whenever possible a set is written by enclosing its elements by brace brackets $\{ \}$. For example, $A = \{a, e, i, o, u\}$. The other way of specifying the set is stating the characteristic property satisfied by its elements. The above example of the set can also be written as the set of vowels in the English alphabet and is written as,

$$A = \{x / x \text{ is a vowel in the English alphabet} \}.$$

If the number of elements in a set is finite then it is said to be a *finite set*, otherwise it is said to be an *infinite set*. If a set contains only one element it is called a *singleton set*. If a set contains no elements, it is called a *null set* or *empty set*, denoted by ϕ .

For example,

$$B = \{1, 2, 5, 8, 9\} \text{ is a finite set,}$$

$$N = \{x : x \text{ is a natural number}\} = \{1, 2, 3, 4, \dots\} \text{ is an infinite set,}$$

$$C = \{2\} \text{ is a singleton set and}$$

$$D = \{x: x^2 = 9 \text{ and } x \text{ is even} \} \text{ is an empty set.}$$

A set consisting of at least one element is called a *non – empty set*.

1.2.1 Definition

If every element of a set A is also an element of a set B then A is said to be a **subset** of B and it is denoted by $A \subset B$ or $B \supset A$.

Clearly $\phi \subseteq A, A \subseteq A$.

For example, let N , Z , Q , R respectively denote the set of natural numbers; the set of integers; the set of rational numbers; the set of real numbers.

Then

$$N \subset Z \subset Q \subset R.$$

A set 'A' is said to be a **proper subset** of 'B' if there exists an element of 'B' which is not an element of 'A'. That 'A' is a proper subset of B if $A \subset B$ and $A \neq B$.

For example, if $A = \{1, 3, 5\}$, $B = \{1, 3, 5, 7\}$ then A is a proper subset of B. Two sets A and B are said to be *equal* if and only if $A \subset B$ and $B \subset A$.

1.2.2 Family of sets

If the elements of a set A are themselves sets, then A is called a **family of sets** or a *class of sets*. The set of all subsets of set A is called the **power set** of A and it is denoted by $P(A)$.

For example if $A = \{1, 3, 5\}$ then.

$$P(A) = \{ \phi, \{1\}, \{3\}, \{5\}, \{1, 3\}, \{3, 5\}, \{5, 1\}, \{1, 3, 5\} \}$$

Note that there are $2^3 = 8$ elements in $P(A)$. If set A has n elements, then its power set $P(A)$ has 2^n elements.

1.2.3 Definition

If A is a finite set, then the cardinality of A is the total number of elements that comprise the set and is denoted by $n(A)$.

The cardinal number or cardinality of each of the sets

$$\phi, \{a\}, \{a, b\}, \{a, b, c\} \dots$$

is denoted by 0, 1, 2, 3, ... respectively.

In any discussion if all the sets are subsets of a fixed set, then this set is called the *universal set* and is denoted by U .

For example, in the study of theory of numbers the set Z of integers is considered as the universal set.

1.2.4 Union of sets

The union of two sets A and B denoted by $A \cup B$ is the set of elements which belong to A or B or both.

That is, $A \cup B = \{ x : x \in A \text{ or } x \in B \}$.

Properties:

1. $A \cup A = A$
2. $A \cup B = B \cup A$
3. $A \cup (B \cup C) = (A \cup B) \cup C$
4. $A \subset A \cup B$ and $B \subset A \cup B$

1.2.5 Intersection of sets

The intersection of two sets A and B denoted by $A \cap B$ is the set of elements, which belong to both A and B .

That is, $A \cap B = \{ x : x \in A \text{ and } x \in B \}$.

Properties:

1. $A \cap A = A$
2. $A \cap B = B \cap A$
3. $A \cap (B \cap C) = (A \cap B) \cap C$
4. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

If $A \cap B = \Phi$, then A and B are said to be *disjoint sets*.

1.2.6 Definition

The difference of two sets A and B , denoted by $A - B$ is the set of elements of A , which are not the elements of B . That is,

$$A - B = \{ x : x \in A, x \notin B \}$$

Clearly,

1. $A - B \subset A$
2. $A - B \neq B - A$
3. $A - B, A \cap B, B - A$ are mutually disjoint sets.

1.2.7 Definition

The complement of set A with respect to the universal set U is defined as $U - A$ and is denoted by A' or A^c . That is,

$$A' = \{x : x \in U, x \notin A\}$$

Clearly,

$$1. (A')' = A \quad 2. \phi' = U \quad 3. U' = \phi$$

1.2.8 De Morgan's laws

For any three sets A, B, C

1. $A - (B \cup C) = (A - B) \cap (A - C)$
2. $A - (B \cap C) = (A - B) \cup (A - C)$
3. $(A \cup B)' = A' \cap B'$
4. $(A \cap B)' = A' \cup B'$

1.2.9 Definition

Let A and B be two sets. Then the **Cartesian product** of A and B is defined as the set of all ordered pairs. (x, y) Where $x \in A$ and $y \in B$ and is denoted by $A \times B$.

Thus,

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$$

Two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$.

If A contains m elements and B contains n elements, then $A \times B$ contains mn ordered pairs.

1.2.10 Example

If $A = \{2, 3, 4\}$, $B = \{4, 5, 6\}$ and $C = \{6, 7\}$

Evaluate the following

- (a) $(A \cap B) \times (B - C)$ (b) $A \times (C - B)$
 (c) $(A - B) \times B$ (d) $(A - B) \times (B - C)$
 (e) $(A \times B) - (B \times C)$

Solution:

$$(a) \quad A \cap B = \{2, 3, 4\} \cap \{4, 5, 6\} = \{4\}$$

$$B - C = \{4, 5, 6\} - \{6, 7\} = \{4, 5\}$$

$$\text{Therefore } (A \cap B) \times (B - C) = \{4\} \times \{4, 5\} = \{(4, 4), (4, 5)\}$$

$$(b) \quad A = \{2, 3, 4\}; C - B = \{6, 7\} - \{4, 5, 6\} = \{7\}$$

Therefore

$$A \times (C - B) = \{2, 3, 4\} \times \{7\} = \{(2, 7), (3, 7), (4, 7)\}$$

$$(c) \quad A - B = \{2, 3, 4\} - \{4, 5, 6\} = \{2, 3\}$$

$$\begin{aligned} \text{Therefore } (A - B) \times B &= \{2, 3\} \times \{4, 5, 6\} \\ &= \{(2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6)\} \end{aligned}$$

$$(d) \quad \text{We have } (A - B) \times (B - C) = \{2, 3\} \times \{4, 5\} \\ = \{(2, 4), (2, 5), (3, 4), (3, 5)\}$$

$$(e) \quad A \times B = \{2, 3, 4\} \times \{4, 5, 6\} \\ = \{(2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6), (4, 4), (4, 5), (4, 6)\}$$

$$\begin{aligned} B \times C &= \{4, 5, 6\} \times \{6, 7\} \\ &= \{(4, 6), (4, 7), (5, 6), (5, 7), (6, 6), (6, 7)\} \end{aligned}$$

$$\begin{aligned} \text{Therefore } (A \times B) - (B \times C) &= \{(a, b) \in A \times B : (a, b) \notin B \times C\} \\ &= \{(2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6), (4, 4), (4, 5)\} \end{aligned}$$

Self Assessment Questions

1. Find x and y if $(3x+y, x-1) = (x+3, 2y-2x)$
2. If $A = \{1,2,3\}$, $B = \{2,4,5\}$ find
 - (a) $(A \cap B) \times (A - B)$
 - (b) $A \setminus (A - B)$
 - (c) $(A \Delta B) \times (A \cap B)$
3. If $A = \{x/x \in \mathbb{N} \text{ and } x < 3\}$, $B = \{x/x^2 - 16 = 0 \text{ and } x < 0\}$ find $B \times A$ where \mathbb{N} is a set of natural number
4. If $A = \{x \mid x \text{ is a positive prime. There are no negative primes } < 8 \}$
 $B = \{6, 7, 8\}$, $C = \{7, 8, 9\}$
 find $(A \cap B) \times (B \cap C)$
 (A prime number is a natural number other than one whose only factors are one and itself)
5. If $A = \{x/x^2 - 5x + 6 = 0\}$, $B = \{2,4\}$, $C = \{4,5\}$ find $(A - B) \times (B - C)$
6. Let $A = \{1,2,3,4\}$, $B = \{3,4,5,6\}$ and $C = \{1,4,7,8\}$ determine
 $A \cap B \cap C = (A \cap B) \cap C$ Also verify that
 - a) $A \cap B \cap C = (A \cap B) \cap C$
 - b) $A \cap B \cap C = A \cap (B \cap C)$
7. If $A = \{x : x^2 - 5x + 6 = 0\}$, $B = \{0, 3, 4\}$,
 $C = \{x : x \in \mathbb{N} \text{ and } x < 4\}$
 Evaluate the following:
 - (a) $A \times (B \cap C)$
 - (b) $(A \cup B) \times (B - C)$
 - (c) $(A - B) \times (C - B)$

1.3 Relations

A relation may involve equality or inequality. The mathematical concept of a relation deals with the way the variables are related or paired. A relation may signify a family tie 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 unit, we shall consider the relations called binary relations.

1.3.1 Definition

Relation R from a set A to another set B is a subset of $A \times B$. That is, $R \subseteq A \times B$.

1.3.2 Note

- (i) If $(a, b) \in R$, then we say that a is 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 .

1.3.3 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 .

1.3.4 Example

Take Z^+ , the set of positive integers.

Define $aRb \Leftrightarrow a$ divides b

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

1.3.5 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 .

1.3.6 Definition

Let R be relation from A to B .

The domain of R is defined as

$$\text{Dom } R = \{x \in A \mid (x, y) \in R \text{ for some } y \in B\}$$

and the range of R is defined as

$$\text{Range } R = \{y \in B \mid (x, y) \in R \text{ for some } x \in A\}.$$

1.3.7 Definition

Let R be a relation on 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 \bar{R} is a relation such that $a \bar{R} b \Leftrightarrow a \not R b$.

1.3.8 Example

- (i) Take $A = \{\text{Set of all living people}\}$. Define $B = \{(x, y) \mid x \text{ is parent of } y\}$ and $C = \{(y, x) \mid y \text{ is child of } x\}$. Then each of B and C is the inverse of other.
- (ii) Take $A = \{1, 2, 3\}$. Define $R = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$. Then $\bar{R} = \{(1, 1), (2, 1), (3, 1), (3, 2), (3, 3)\}$.

1.3.9 Definition

- (i) A relation R on set A is said to be **identity relation**, denoted by I_A , if $I_A = \{(x, x) \mid x \in A\}$
- (ii) A relation R on set A is said to be a **universal relation** if $R = A \times A$.

1.3.10 Example

- (i) Take $A = \{1, 2, 3\}$, then $I_A = \{(1, 1), (2, 2), (3, 3)\}$
- (ii) Take $A = \{(a, b)\}$. Define $R = \{(a, a), (a, b), (b, a), (b, b)\}$, which is a universal relation.

1.3.11 Definition

A relation R on a set A is

- *reflexive* if $a R a$ for all $a \in A$.
- *irreflexive* if $a \not R a$ for every $a \in A$.
- *symmetric* if $a R b \Rightarrow b R a$
- *anti-symmetric* if $a R b, b R a \Rightarrow a = b$
- *asymmetric* if $a R b$ implies $b \not R a$.
- *transitive* if $a R b$ and $b R c \Rightarrow a R c$

1.3.12 Example

- (i) Take $T = \{(a, b) \mid a, b \in A, a = b\}$. 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 $A = \mathbb{Z}^+$, the set of positive integers.

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

R is not reflexive, since a is not less than 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 $A = \mathbb{Z}^+$ 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 $(2, 16) \notin R$

1.3.13 Definition

A relation R on a set A is called an **equivalence relation** if R is reflexive, symmetric and transitive.

1.3.14 Example

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.

Take $A = \mathbb{Z}$, the set of integers.

Define: $R = \{(a, b) \mid a \leq b\}$. Now $a \leq a$ for all $a \in \mathbb{Z}$, R is reflexive. $a \leq b \Rightarrow b \geq a$, R is not symmetric.

$a \leq b, b \leq c \Rightarrow a \leq c$, R is transitive.

Therefore R is not an equivalence relation.

Take $A = \mathbb{Z}$, the set of integers.

Define: $R = \{(a, b) \mid a \equiv r \pmod{2}, b \equiv r \pmod{2}\}$.

That is $(a, b) \in R \Leftrightarrow a$ and b give the same remainder r when divided by 2.

R is an equivalence relation.

1.3.15 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 :

$$(i) \quad A_i \cap A_j = \phi \text{ for all } i \neq j$$

$$(ii) \quad \bigcup_{i \in I} A_i = S$$

1.3.16 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 $a \in A$ 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.

1.3.17 Properties of Equivalence Relations

Let R be an equivalence relation defined by A . Let $a, b \in A$ be arbitrary elements. Then,

$$(i) a \in [a]$$

$$(ii) b \in [a] \Rightarrow [a] = [b]$$

$$(iii) [a] = [b] \Leftrightarrow (a, b) \in R$$

$$(iv) [a] = [b] \text{ or } [a] \cap [b] = \phi$$

1.3.18 Definition

Let $A = \{a_1, a_2, \dots, a_n\}$ and $B = \{b_1, b_2, \dots, b_n\}$.

If R is relation from A to B , then R can be represented by matrix

$M_R = (M_{ij})_{m \times n}$, defined

$$(M_{ij})_{m \times n} = \begin{cases} 1 & \text{if } (a_i, a_j) \in R \\ 0 & \text{if } (a_i, a_j) \notin R \end{cases}$$

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.

1.3.19 Example

Let $A = \{1, 2, 3\}$ and $R = \{(x, y) \mid x < y\}$. Write M_R .

Solution: $R = \{(1, 2), (1, 3), (2, 3)\}$. Since $(1, 2) \in R$, we have $m_{12} = 1$; $(1, 3) \in R$, we have $m_{13} = 1$; also $m_{23} = 1$. Therefore:

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

1.3.20 Example

Let $A = \{1, 2, 3, 4\}$. Define $a R b \Leftrightarrow a < b$. Then

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

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

1.3.22 Definition

A relation R is **transitive** if and only if $M_R = [m_{ij}]$ has the property:

$$m_{ij} = 1 \text{ and } m_{jk} = 1 \Rightarrow m_{ik} = 1$$

1.3.22 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.

Self Assessment Questions

8. Take $A = \{1, 2, 3, 4\}$ and define
 $R = \{(1, 2), (2, 3), (1, 3), (3, 4)\}$. What are conditions that the relation R satisfies?
9. 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 these are reflexive, symmetric, anti-symmetric or transitive.
10. Let $R =$ Set of real numbers. Define;
 $(i) (a, b) \in R \Leftrightarrow |a| = |b|$
 $(ii) (a, b) \Leftrightarrow a \geq b$
 $(iii) (a, b) \in R \Leftrightarrow |a| > |b|$
 Which of these are equivalence relations?

1.4 Functions

1.4.1 Definition

Let A and B be two non – empty sets. A *function or a mapping* f from A to B is a rule, which associates every element of A with a unique element of B and is denoted by $f : A \rightarrow B$.

In other words, a function f from A to B is a relation satisfying the following:

- i) Every element of A is related to some element of B .
- ii) no element of A is related to two different elements of B .

If $f : A \rightarrow B$ is a function then A is called the *domain* and B is called the *co-domain* of f . If $x \in A$ is associated with a unique element $y \in B$ by the

function f , then y is called the *image* of x under f and is denoted by $y = f(x)$. Also x is called the pre-image of y under f .

The range of f is the set of those elements of B , which appears as the image of at least one element of A and is denoted by $f(A)$. Thus $f(A) = \{f(x) \in B : x \in A\}$. Clearly $f(A)$ is a subset of B .

1.4.2 Example

Let $A = \{1, 2, 3, 4\}$ and Z be the set of integers. Define $f : A \rightarrow Z$ by $f(x) = 2x + 3$. Show that f is a function from A to B . Also find the range of f .

Solution:

Now $f(1) = 5$, $f(2) = 7$, $f(3) = 9$, $f(4) = 11$

Therefore $f = \{(1, 5), (2, 7), (3, 9), (4, 11)\}$

Since every element of A is associated with a unique element of B , f is a function.

Range of $f = \{5, 7, 9, 11\}$

1.4.3 Example

Let N be the set of natural numbers. If $f : N \rightarrow N$ is defined by $f(x) = 2x - 1$ show that f is a function and find the range of f .

Solution:

Now $f(1) = 1$, $f(2) = 3$, $f(3) = 5, \dots$

Therefore $f = \{(1, 1), (2, 3), (3, 5), (4, 7), \dots\}$

Clearly f is a function.

Range of $f = \{1, 3, 5, 7, \dots\}$

1.4.4 Example

Let R be the set of real numbers. Define $f : R \rightarrow R$ by $f(x) = x^2$ for every $x \in R$. Show that f is a function and find the range of f .

Solution:

Here f associates every real number to its square, which is certainly a real number. Hence f is a function. Range of R is the set of all non – negative real numbers.

1.4.5 Definition

A function $f : A \rightarrow B$ is said to be one – one or injection if for all $x_1, x_2, \in A$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. The contrapositive of this implication is that for all $x_1, x_2, \in A$, $x_1 \neq x_2$ implies $f(x_1) \neq f(x_2)$

Thus a function $f : A \rightarrow B$ is said to be one – one if different elements of A have different images in B .

1.4.6 Example

Let R be the set of real numbers. Define $f : R \rightarrow R$ by

$$i) f(x) = 2x + 3$$

$$ii) f(x) = x^3 \text{ for every } x \in R \text{ prove that } f \text{ is one-one.}$$

Solution:

$$i) \text{ Let } f(x_1) = f(x_2) \text{ for some } x_1, x_2 \in R$$

$$\Rightarrow 2x_1 + 3 = 2x_2 + 3$$

$$\Rightarrow x_1 = x_2$$

Thus for every $x_1, x_2 \in R$, $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

Therefore f is one – one.

$$ii) \text{ Let } f(x_1) = f(x_2) \text{ for some } x_1, x_2 \in R$$

$$\Rightarrow x_1^3 = x_2^3$$

$$\Rightarrow x_1 = x_2 \quad \text{Therefore } f \text{ is one – one.}$$

1.4.7 Example

If $f : R \rightarrow R$ is defined by $f(x) = x^2$ for every $x \in R$, show that f is not one – one.

Solution:

$$\text{Let } f(x_1) = f(x_2) \Rightarrow x_1^2 = x_2^2 \Rightarrow x_1 = \pm x_2$$

Hence f is not one – one.

For example, $f(-2) = 4$ and $f(2) = 4$. The images of -2 and 2 are not different. Hence f is not one – one.

1.4.8 Definition

A function $f : A \rightarrow B$ is said to be *onto or surjection* if for every $y \in B$ there exists at least one element $x \in A$ such that $f(x) = y$. i.e., every element of the co-domain B appears as the image of at least one element of the domain A .

If f is onto then $f(A) = B$

1.4.9 Example

Define $f : R \rightarrow R$ by

$$(i) f(x) = 2x + 3 \quad (ii) f(x) = x^3 \text{ forever } x \in R$$

Show that f is onto

Solution:

i) Let $y \in R$. Then to find $x \in R$ such that $f(x) = y$ i.e., $2x + 3 = y$

$$\text{Solving for } x \text{ we get, } x = \frac{y - 3}{2}$$

$$\text{Since } y \in R, x = \frac{y - 3}{2} \in R$$

Hence for every $y \in R$ exists $x = \frac{y - 3}{2} \in R$ such

that $f\left(\frac{y - 3}{2}\right) = y$. Therefore f is onto.

ii) Let $y \in R$. We shall show that there exists $x \in R$ such that $f(x) = y$.

That is $x^3 = y$. Hence $x = y^{\frac{1}{3}}$. If $y \in R$, then $y^{\frac{1}{3}} \in R$. Thus for

every $y \in R$ there exists $y^{\frac{1}{3}} \in R$ such that $f\left(y^{\frac{1}{3}}\right) = \left(y^{\frac{1}{3}}\right)^3 = y$.

Therefore f is onto.

1.4.10 Example

If $f : R \rightarrow R$ is defined by $f(x) = x^2$ for every $x \in R$ then prove that f is not onto.

Solution:

Since a negative number is not the square of any real number, the negative numbers do not appear as the image of any element of R .

For example, $-9 \in R$ but there does not exist any $x \in R$ such that $f(x) = x^2 = -9$. Hence f is not onto.

1.4.11 Definition

A function $f : A \rightarrow B$ is said to be *one – to – one or bijection* if it is both one – one and onto.

For example, if $f : R \rightarrow R$ is defined by

i) $f(x) = 2x + 3$

ii) $f(x) = x^3$ for every $x \in R$ then f is one – to – one functions.

1.4.12 Definition

Let $f : A \rightarrow B$ be a function and $y \in B$. Then the inverse image of y under f denoted by $f^{-1}(y)$ is the set of those elements of A , which have y as their image.

That is, $f^{-1}(y) = \{x \in A : f(x) = y\}$

1.4.13 Example

If $f : \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = x^2 - 3x + 5$ find

(i) $f^{-1}(3)$ and (ii) $f^{-1}(15)$

Solution

i) Let $f^{-1}(3) = y$ then $f(y) = 3$

$$\Rightarrow y^2 - 3y + 5 = 3 \text{ or } y^2 - 3y + 2 = 0$$

$$\Rightarrow (y-1)(y-2) = 0$$

Therefore $y = 1$ or $y = 2$. Hence $f^{-1}(3) = \{1, 2\}$

ii) Let $f^{-1}(15) = y$ Hence $f(y) = 15$

$$\text{Therefore } y^2 - 3y + 5 = 15$$

$$y^2 - 3y - 10 = 0$$

$$(y-5)(y+2) = 0 \text{ Therefore } y = 5, \text{ or } y = -2$$

$$\text{Hence } f^{-1}(15) = \{-2, 5\}$$

1.4.14 Definition

If a function $f : A \rightarrow B$ is one – one and onto then the **inverse** of f denoted by $f^{-1} : B \rightarrow A$ is defined by $f^{-1} = \{(y, x) : (x, y) \in f\}$

Thus if $f : A \rightarrow B$ is both one – one and onto then $f^{-1} : B \rightarrow A$ is obtained by reversing the ordered pairs of f .

Note that f^{-1} exists only when f is both one – one and onto. Further f^{-1} is also one – one and onto.

1.4.15 Example

Let \mathbb{Q} be the set of the rationals. If $f : \mathbb{Q} \rightarrow \mathbb{Q}$ is defined by $f(x) = 2x - 3$ for every $x \in \mathbb{Q}$ then find f^{-1} if it exists.

Solution:

i) Let $f(x_1) = f(x_2)$

$$\Rightarrow 2x_1 - 3 = 2x_2 - 3 \quad \Rightarrow x_1 = x_2$$

Hence f is one – one.

ii) Let $y \in \mathbb{Q}$. Then to find $x \in \mathbb{Q} : f(x) = y$

i.e., $2x - 3 = y$ Therefore $x = \frac{y + 3}{2}$

Whenever y is rational, $x = \frac{y + 3}{2}$ is also a rational. Hence there

exists $\frac{y + 3}{2} \in \mathbb{Q}$ such that $f\left(\frac{y + 3}{2}\right) = y$

Hence f is onto. Therefore $f^{-1} : \mathbb{Q} \rightarrow \mathbb{Q}$ exists.

Let $x = f^{-1}(y)$ Therefore $y = f(x)$

i.e., $y = 2x - 3$ or $x = \frac{y + 3}{2}$

Define $f^{-1} : \mathbb{Q} \rightarrow \mathbb{Q}$ by $f^{-1}(y) = \frac{y + 3}{2}$ for every $y \in \mathbb{Q}$.

Replacing y by x , we get $f^{-1}(x) = \frac{x + 3}{2}$ $x \in \mathbb{Q}$.

This is required inverse function.

1.4.16 Definition

Let $a, b \in \mathbb{R}$ such that $a < b$.

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}.$$

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

Further, semi – open or semi – closed intervals are defined as below:

$$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$$

$$(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$$

Likewise, $[a, \infty) = \{x \in \mathbb{R} : a \leq x\}$ and $(-\infty, a] = \{x \in \mathbb{R} : x \leq a\}$ are semi-open intervals.

Let a be a real number. Then the open interval $(a - \delta, a + \delta)$ where $\delta > 0$ is a real number is called the δ -neighbourhood of a . If $x \in (a - \delta, a + \delta)$ then $a - \delta < x < a + \delta$.

1.5 Basic Number Theory

1.5.1 First Principle of Mathematical Induction

Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ (set of natural numbers) and suppose $S(n_0)$ is true for some integer n_0 . If for all integers k with $k \geq n_0$, $S(k)$ implies that $S(k+1)$ is true, then $S(n)$ is true for all integers n greater than n_0 .

For instance, If Z is a set of integers such that

a) $1 \in Z$,

b) $n \in Z \Rightarrow n+1 \in Z$

then all integers greater than or equal to 1 belongs to Z .

Second Principle of Mathematical Induction: Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ (set of natural numbers) and suppose $S(n_0)$ is true for some integer n_0 . If $S(n_0), S(n_0+1), \dots, S(k)$ 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 .

Well Ordering Principle: Any non-empty subset of the set of all positive integers contains a smallest (least) elements. However the set of integers is not well ordered.

For the set of positive integers, the principle of mathematical induction is equivalent to the well-ordering principle. A totally ordered set is said to be *well ordered* if any non-empty subset contains the smallest element. It is clear that the set of positive rational numbers \mathbb{Q}^+ under the usual ordering is not well-ordered.

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 $d \nmid n$.

1.5.2 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 $n \mid d \Rightarrow |d| = |n|$
- xi) $d \mid n$ and $d \neq 0 \Rightarrow (n/d) \mid n$.

1.5.3 Definitions

- 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 .

1.5.4 Note

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 aDb . If $(a, b) = 1$, then a and b are said to be *relatively prime*.

1.5.5 Properties (of greatest common divisor):

- i) $(a, b) = (b, a)$ or $aDb = bDa$ (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 $(a, 0) = (0, a) = |a|$.

1.5.6 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*.

1.5.7 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 $p | a$ or $p | b$. Generally, if a prime p divides a product $a_1 a_2 \dots a_n$, then $p | a_i$ for at least one i .

1.5.8 Fundamental Theorem of Arithmetic: (the unique factorization)

Every integer $n > 1$ can be written as a product of prime factors in only one way, apart from the order of the factors. (That is, any positive integer $a > 1$ can be factored in a unique way as $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_t^{\alpha_t}$ where p_1, p_2, \dots, p_t are prime numbers, $\alpha_i, 1 \leq i \leq t$ are positive integers and $p_1 > p_2 > \dots > p_t$).

[Example: $3000 = 2 \times 2 \times 2 \times 5 \times 5 \times 5 \times 3 = 2^3 \cdot 5^3 \cdot 3^1$]

1.5.9 Note

- i) Let n be an integer. If the distinct prime factors of n are p_1, p_2, \dots, p_r and if p_i occurs as a factor a_i times, then we write,

$$n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_r^{a_r} \text{ or } n = \prod_{i=1}^r p_i^{a_i}$$

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 $0 \leq c_i \leq a_i$ for $i = 1, 2, \dots, r$.
- 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 $c_i = \min\{a_i, b_i\}$

1.5.10 Note

- i) The infinite series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges where p_n 's are primes.
- ii) *Division Algorithm:* Let a, b be integers such that $b > 0$. Then there exist two integers p and q such that $a = pb + q$ where $0 \leq q < b$.
- iii) (*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 $r_2, r_3, \dots, r_n, r_{n+1}$ defined successively by the relations,
- $$\begin{aligned} r_0 &= r_1 q_1 + r_2 & 0 < r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3 & 0 < r_3 < r_2 \\ &\dots & \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n + r_{n+1} & r_{n+1} = 0 \end{aligned}$$
- Then r_n , the last non zero remainder in this process, is the *g.c.d.* of a and b .

1.5.11 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.

1.5.12 Definition

The *g.c.d* of n integers a_1, a_2, \dots, a_n is defined inductively by the relation $(a_1, a_2, \dots, a_n) = (a_1, (a_2, \dots, a_n))$. Again this number is independent of the order in which the a_i appear.

1.5.13 Note:

- i) If $d = (a_1, a_2, \dots, a_n)$, then d is a linear combination of the a_i . That is, there exist integers x_1, x_2, \dots, x_n such that $(a_1, a_2, \dots, a_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$.
- 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, \dots, a_n are said to be *relatively prime in pairs*. For instance, $\text{g.c.d } \{2, 3\} = 1$, $\text{g.c.d.}\{4, 9\} = 1$, $\text{g.c.d } \{75, 8\} = 1$.
- iv) If a_1, a_2, \dots, a_n are relatively prime in pairs, then $(a_1, a_2, \dots, a_n) = 1$.

1.5 14 Definitions

- i) For any real number x , we define the floor of x as $\lfloor x \rfloor =$ the greatest integer less than or equal to $x = \max \{n / n \leq x, n \text{ is an integer}\}$

For example, take $x = 2.52$, then

$$\lfloor x \rfloor = \max \{n / n \leq x, n \text{ is an integer}\} = \max \{1, 2\} = 2.$$

- ii) For any real number x , we define the ceiling of x as $\lceil x \rceil =$ the least integer greater than or equal to $x = \min \{n / n \geq x, n \text{ is an integer}\}$.

For example, take $x = 3.732$, then

$$\lceil x \rceil = \min \{n / n \geq x, n \text{ is an integer}\} = \min \{4, 5, 6, 7 \dots\} = 4.$$

1.5.15 Property

$a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$. (In other words, two integers are congruent modulo m if and only if they leave the same remainder when divided by m).

For example, $9 \bmod 5 = -16 \bmod 5$ if and only if $9 \equiv -16 \pmod{5}$.

1.5.16 Property

For any a, b , $a - b$ is a multiple of m if and only if $a \bmod m = b \bmod m$.

The relation " $a \equiv b \pmod{n}$ " defined above is an equivalence relation on \mathbb{Z} .

Proof: Reflexive: Let $a \in \mathbb{Z}$. Since n divides $a - a = 0$, we have $a \equiv a \pmod{n}$.

Symmetric: Let $a \equiv b \pmod{n}$

$$\Rightarrow n \text{ divides } a - b$$

$$\Rightarrow n \text{ divides } -(a - b)$$

$$\Rightarrow n \text{ divides } b - a$$

$$\Rightarrow b \equiv a \pmod{n}$$

Transitivity: Let $a, b, c \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$

$$\Rightarrow n \text{ divides } a - b, \text{ and } n \text{ divides } b - c$$

$$\Rightarrow n \text{ divides } (a - b) + (b - c)$$

$$\Rightarrow n \text{ divides } a - c$$

$$\Rightarrow a \equiv c \pmod{n}. \text{ Hence the relation is an equivalence relation.}$$

1.5.17 Example

Suppose $n = 5$. Then

$$[0] = \{x/x \equiv 0 \pmod{5}\}$$

$$= \{x/5 \text{ divides } x - 0 = x\}$$

$$= \{\dots, -10, -5, 0, 5, 10, \dots\},$$

$$[1] = \{x/x \equiv 1 \pmod{5}\}$$

$$= \{x/5 \text{ divides } x - 1\}$$

$$= \{\dots, -9, -4, 1, 6, \dots\},$$

$$\begin{aligned}
 [2] &= \{x / x \equiv 2 \pmod{5}\} \\
 &= \{x / 5 \text{ divides } x - 2\} \\
 &= \{\dots, -8, -3, 2, 7, 12, \dots\},
 \end{aligned}$$

$$\begin{aligned}
 [3] &= \{x / x \equiv 3 \pmod{5}\} \\
 &= \{x / 5 \text{ divides } x - 3\} \\
 &= \{\dots, -7, -2, 3, 8, 13, \dots\},
 \end{aligned}$$

$$\begin{aligned}
 [4] &= \{x / x \equiv 4 \pmod{5}\} \\
 &= \{x / 5 \text{ divides } x - 4\} \\
 &= \{\dots, -6, -1, 4, 9, 14, \dots\}.
 \end{aligned}$$

Also it is clear that $[0] = [5] = [10] = \dots$ $[1] = [6] = [11] = \dots$ $[2] = [7] = [12] = \dots$ $[3] = [8] = [13] = \dots$ $[4] = [9] = [14] = \dots$

Therefore the set of equivalence classes is given by $\{[0], [1], [2], [3], [4]\}$.

Self Assessment Questions

11. Find the gcd of 858 and 325.
12. If $a|c$ and $b|c$, then is it true that " $ab|c$ "?
13. If gcd of $\{a, b\} = 1$, then what is the gcd of $a + b$ and $a - b$?
14. Are every two consecutive integers co-prime?
15. If $a|b$ and $c|d$, $gcd\{b, d\} = 1$, then $gcd\{a, c\} =$ _____
16. If a and b are any two odd primes, then $(a^2 - b^2)$ is _____
17. State whether the following are true or false.
 - i) Sum of an integer and its square is even.
 - ii) Difference between the square of any number and the number itself is even.
18. If $p > 1$ and $2^p - 1$ is prime, then p is prime. Is the converse true? Justify.
19. Express 29645 in terms of their prime factors.
20. Find the $gcd\{963, 657\}$ and find the integers m and n such that $gcd\{963, 657\} = m.657 + n.963$.

1.6 Summary

In this unit we introduced the basic concept related to sets and the different ways of representing them. Some properties common to operations on sets and logical statements were discussed here. Cartesian product of sets was studied as relations between two sets. Lastly, we defined the function as a particular kind of relations. This unit also provides the broad idea of number system. The set of integers are the building blocks of modern mathematics. The concept congruence and integer's mod n are indispensable in various applications of algebra. We will learn some of the applications in cryptosystems in later units.

1.7 Terminal Questions

1. If $U = \{a, b, c, d, e\}$, $A = \{a, c, d\}$, $B = \{d, e\}$, $C = \{b, c, e\}$

Evaluate the following

- (a) $A' \times (B - C)$ (b) $(A \cup B)' \times (B \cap C)$
(c) $(A - B) \times (B - C)$ (d) $(B \cup C)' \times A$
(e) $(B - A) \times C'$

2. Find the sum of divisors of 360.
3. Find the number of multiples of 7 among the integers from 200 to 500.

1.8 Answers

Self Assessment Questions

- 1) The ordered Pairs are equal if $3x + y = x + 3$ and $x - 1 = 2y - 2x$
i.e. $2x + y = 3$
 $3x - 2y = 1$
Solving $x = 1$, $y = 1$

- 2) $A \cap B = \{2\}$
 $A - B = \{1, 3\}$
 $B - A = \{4, 5\}$
 $A \Delta B = (A - B) \cup (B - A) = \{1, 3, 4, 5\}$
 $(A \cap B) \times (A - B) = \{2\} \times \{1, 3\} = \{(2, 1), (2, 3)\}$
 $A \times (A - B) = \{1, 2, 3\} \times \{1, 3\} = \{(1, 1), (1, 3), (2, 1), (2, 3), (3, 1), (3, 3)\}$
 $(A \Delta B) \times (A \cap B) = \{1, 3, 4, 5\} \times \{2\} = \{(1, 2), (3, 2), (4, 2), (5, 2)\}$
- 3) Since $x^2 - 16 = 0$
 $A = \{1, 2\}$ and $B = \{-4\}$
 $(x - 4)(x + 4) = 0$
 $B \times A = \{-4\} \times \{1, 2\}$
 $= \{(-4, 1), (-4, 2)\} \implies x = -4, 4$
Therefore $x = -4$ ($x < 0$)
- 4) $A = \{2, 3, 5, 7\}$ $B = \{6, 7, 8\}$ $C = \{7, 8, 9\}$
 $(A \cap B) = \{7\}$ and $(B \cap C) = \{7, 8\}$
 $(A \cap B) \times (B \cap C) = \{7\} \times \{7, 8\} = \{(7, 7), (7, 8)\}$
- 5) $x^2 - 5x + 6 = 0 \implies (x - 2)(x - 3) = 0 \implies x = 2, 3$
 $A = \{2, 3\}$, $B = \{2, 4\}$ and $C = \{4, 5\}$
 $A - B = \{3\}$ and $B - C = \{2\}$
Therefore $(A - B) \times (B - C) = \{3\} \times \{2\} = \{(3, 2)\}$
- 6) $(A \cap B) = \{3, 4\}$, $(B \cap C) = \{4\}$
 $(A \cap B) \cap C = \{3, 4\} \cap \{1, 4, 7, 8\} = \{4\}$
 $A \cap (B \cap C) = \{1, 2, 3, 4\} \cap \{4\} = \{4\}$
Therefore $A \cap B \cap C = (A \cap B) \cap C = A \cap (B \cap C)$
- 7) Now $A = \{x : (x - 2)(x - 3) = 0\} = \{2, 3\}$
 $B = \{0, 3, 4\}$
 $C = \{x : x \in N \text{ and } x < 4\} = \{1, 2, 3\}$
(a) $A = \{2, 3\}$; $B \cap C = \{0, 3, 4\} \cap \{1, 2, 3\} = \{3\}$
Therefore $A \times (B \cap C) = \{2, 3\} \times \{3\} = \{(2, 3), (3, 3)\}$

$$(b) \quad A \cup B = \{2, 3\} \cup \{0, 3, 4\} = \{0, 2, 3, 4\}$$

$$B - C = \{0, 3, 4\} - \{1, 2, 3\} = \{0, 4\}$$

$$\begin{aligned} \text{Therefore } (A \cup B) \times (B - C) &= \{0, 2, 3, 4\} \times \{0, 4\} \\ &= \{(0, 0), (0, 4), (2, 0), (2, 4), (3, 0), (3, 4), (4, 0), (4, 4)\} \end{aligned}$$

$$(c) \quad A - B = \{2, 3\} - \{0, 3, 4\} = \{2\}$$

$$C - B = \{1, 2, 3\} - \{0, 3, 4\} = \{1, 2\}$$

$$\text{Therefore } (A - B) \times (C - B) = \{2\} \times \{1, 2\} = \{(2, 1), (2, 2)\}$$

8) 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

9) 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 $1 \neq 3$)

10) i) Equivalence relation

ii) Not Symmetric and so it is not an equivalence relation

iii) Not Symmetric and so not equivalence relation.

11) gcd of 858 and 325 is 13.

12) If it is not true. For example, take $a = 3$, $b = 6$, $c = 12$. Now $3|12$ and $6|12$ but $3 \cdot 6 \nmid 12$.

13) Either 1 or 2.

- 14) Yes, the \gcd of $\{n, n+1\}$, $n \in \mathbb{N}$ is equal to 1.
- 15) $\gcd\{a, c\} = 1$.
- 16) Composite.
- 17) (i) Yes, it is true.
(ii) Yes, it is true.
- 18) 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 $a = 2^m > 2$
 $= (a - 1)(a^{n-1} + a^{n-2} + \dots + 1^{n-1})$
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.
- 19) $5 \times 7^2 \times (11)^2$.
- 20) $\gcd\{963, 657\} = 9$, $m = 22$, $n = -15$.

Terminal Questions

1. (a) $A' = U - A = \{a, b, c, d, e\} - \{a, c, d\} = \{b, e\}$
 $B - C = \{d, e\} - \{b, c, e\} = \{d\}$
Therefore $A' \times (B - C) = \{b, e\} \times \{d\} = \{(b, d), (e, d)\}$
- (b) $(A \cup B)' = U - (A \cup B) = \{a, b, c, d, e\} - \{a, c, d, e\} = \{b\}$
 $B \cap C = \{d, e\} \cap \{b, c, e\} = \{e\}$
Therefore $(A \cup B)' \times (B \cap C) = \{b\} \times \{e\} = \{(b, e)\}$
- (c) $A - B = \{a, c, d\} - \{d, e\} = \{a, c\}$
 $B - C = \{d, e\} - \{b, c, e\} = \{d\}$
Therefore $(A - B) \times (B - C) = \{a, c\} \times \{d\} = \{(a, d), (c, d)\}$

$$(d) B \cup C = \{d, e\} \cup \{b, c, e\} = \{b, c, d, e\}$$

$$\text{Therefore } (B \cup C)' = U - (B \cup C) = \{a\}$$

$$\begin{aligned} \text{Therefore } (B \cup C)' \times A &= \{a\} \times \{a, c, d\} \\ &= \{(a, a), (a, c), (a, d)\} \end{aligned}$$

$$(e) B - A = \{d, e\} - \{a, c, d\} = \{e\}$$

$$C' = U - C = U - \{b, c, e\} = \{a, d\}$$

$$\text{Therefore } (B - A) \times C' = \{e\} \times \{a, d\} = \{(e, a), (e, d)\}$$

Unit 2

Elementary Combinatorics

Structure

- 2.1 Introduction
 - Objectives
- 2.2 Principle of Counting
- 2.3 Permutation of Distinct Things
- 2.4 Combinations
- 2.5 Partitions and Binomial Coefficients
- 2.6 Principle of Inclusion and Exclusion
- 2.7 Summary
- 2.8 Terminal Questions
- 2.9 Answers

2.1 Introduction

Combinatorics, the study of arrangements of objects, is an important part of Discrete Mathematics. In this unit, we shall study the permutations and 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. Further, we present the partition of integers and the sets, some basic identities involving binomial coefficients. In formulas arising from the analysis of algorithms in computer science, the binomial coefficients occur.

Objectives:

At the end of the unit, you would be able to

- learn the principles of counting with certain natural objects.
- apply the techniques of generating function to partitions and compositions.
- apply the principles of inclusion and exclusion to various models.
- learn the partitions of sets and binomial coefficients.
- apply the principle of inclusion and exclusion in various situations.

2.2 Principle of Counting

When we consider the outcomes of several experiments, we shall follow the following rules.

2.2.1 Rules:

- 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.
- 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.

2.2.2 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:

- By the rule of product, there are 42×50 ways to select the representative for both the class A and class B ;
- By the rule of sum, there will be $42 + 50$ ways to select a representative for either class A or class B .

2.2.3 Example

Suppose a license plate contains 2 letters followed by four digits, with the first digit not a 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 –

$26 \times 26 \times 9 \times 10 \times 10$ 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 chosen 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 –

$26 \times 25 \times 9 \times 9 \times 8 \times 7$ ways.

Self Assessment Questions

1. a) How many different binary bit strings of length 7 are there?
 - b) Suppose a State's license plate 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 1 or 2 names. In how many ways can a child be named if we can choose from 100 names?

2.3 Permutation of Distinct Things

Let us recollect that the first of the members of an r -permutation of n distinct things may be chosen in n ways. The second is chosen in $(n - 1)$ ways, ..., the r^{th} is chosen in $n - (r - 1)$ ways.

So by the repeated application of product rule, the number required is – $n(n - 1) \dots (n - (r - 1))$ ways, $n \geq r$, it is denoted by $p(n, r)$.

If $r = n$, then $p(n, n) = n(n - 1) \dots (n - n + 1) = n(n - 1) \dots 2.1 = n!$.

Therefore

$$\begin{aligned} p(n, r) &= \frac{n(n-1)(n-2)\dots(n-(r-1))\dots 2.1}{(n-r)\dots 2.1} \\ &= \frac{n!}{(n-r)!} \\ &= \frac{p(n, n)}{p(n-r, n-r)} \end{aligned}$$

or $p(n, n) = p(n, r), p(n-r, n-r)$.

2.3.1 Problem

Prove that $p(n, r) = p(n - 1, r) + r p(n - 1, r - 1)$

Solution: Write $p(n, r)$

$= n(n - 1) \dots (n - (r - 1)) = (n - 1)(n - 2) \dots (n - (r - 1))[(n - r) + r]$, which is equal to $p(n - 1, r) + r.p(n - 1, r - 1)$, on multiplication.

2.3.2 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 chosen in ' n ' ways and so on. Therefore, in this case there are –

$$\underbrace{n \times n \times \dots \times n}_{r \text{ times}} = n^r = U(n, r) \text{ ways}$$

2.3.3 Example

A bit is either 0 or 1: a byte is a sequence of 8 bits. Find the number of bytes that,

- (a) can be formed
- (b) begin with 11 and end with 11
- (c) begin with 11 and do not end with 11
- (d) 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 at 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 $128 - 16 = 112$ bytes.

2.3.4 Example

A computer password consists of a letter of the alphabet followed by 3 or 4 digits. Find the total number of –

- (a) passwords that can be formed
- (b) passwords in which no digit repeats.

Solution:

(a) Since there are 26 letters and 10 digits and the digits can be repeated by product rules, the number of 4-character password is $26 \cdot 10 \cdot 10 \cdot 10 = 26000$.

Similarly the number of 5-character password is $26 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 260000$.

Hence the total number of passwords is $26000 + 260000 = 286000$.

(b) Since the digits are not repeated, the first digit after a letter 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 $26 \cdot 10 \cdot 9 \cdot 8 = 18720$ and the number of 5-character password is $26 \cdot 10 \cdot 9 \cdot 8 \cdot 7 = 131040$ by the product rule.

(c) Hence, the total number of passwords is 149760.

2.3.5 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.

2.3.6 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 occurs 6 times in unit place, 6 times in 10^{th} place, 6 times in 100^{th} place, 6 times in 1000 place.

Therefore sum of the numbers in the unit place is $= 6 \cdot 1 + 6 \cdot 2 + 6 \cdot 3 + 6 \cdot 4 = 60$;

Total sum of the digits in the 10^{th} place = 60×10

Total sum of the digits in the 100^{th} place = 60×100

Total sum of the digits in the 1000^{th} place = 60×1000

Therefore total sum of all 24 numbers = 66,660.

2.3.7 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.

2.3.8 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.

2.3.9 Example

Suppose there are 6 boys and 5 girls. In how many ways can they sit

- (i) in a row?
- (ii) in a row if the boys and girls are each to sit together?
- (iii) in a row if the girls are to sit together and the boys do not sit together?
- (iv) where no two girls are 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 = $5 \times 6! \times 5!$.
- (iv) The boys can sit in $6!$ ways. There are seven places where the girls can be placed. Thus total arrangements are $P(7, 5) \times 6!$.

2.3.10 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 $P(24, 5) \times 2 \times 20!$ ways.

2.3.11 Example

Find the number of ways in which 5 boys and 6 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 $P(6, 5) \times 5!$ arrangements.

Case (ii) Girls can be arranged in $5!$ ways.

_G_G_G_G_G_

There are 6 places for boys. Hence there are $P(6, 5) \times 5!$ ways.

Hence taking the two cases into account, there are $2 \times P(6, 5) \times 5!$ arrangements, in total.

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?

2.4 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 $\binom{n}{r}$.

(Refer: Section 2.5 for more on Binomial Coefficients)

2.4.1 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 of r -combinations of n objects without repetition (denoted by $C(n, r)$). Then

$$C(n, r) = \frac{n!}{(n-r)!}$$

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 $C(n, r) = \frac{n!}{(n-r)!r!} = \binom{n}{r}$.

Note that $C(n-1, r-1) + C(n-1, r) = C(n, r)$.

2.4.2 Problem

How many ways may one right and one left shoe be selected from six pairs of shoes without obtaining a pair.

Solution: Any one of the left shoe can be selected in six ways. We have five choices for selecting a right shoe without obtaining a pair. Therefore, the total number of ways selecting one left and one right shoe is $= 6 \times 5 = 30$ ways.

2.4.3 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 color?

Solution: The first strip can be selected in four different ways. Since no two adjacent strips have the same color, the second strip can be selected in three different ways. In a similar way, 3rd, 4th, 5th and 6th strips are selected in three different ways. Therefore, the total number of ways selecting the different colors in the strips are $4 \times 3 \times 3 \times 3 \times 3 \times 3 = 4 \times 3^5 = 972$ ways.

2.4.4 Problem

- (i) How many positive integers less than one million can be formed using 7s, 8s and 9s only ?
- (ii) How many using 0s, 8s and 9s 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 containing 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
 $= 2 + 2(3 + 3^2 + \dots + 3^5) = 728$.

2.4.5 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.

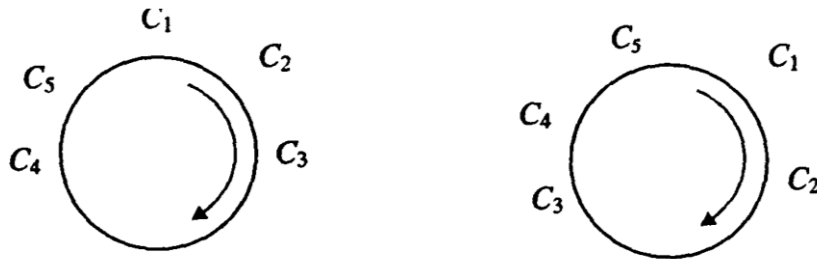


Figure 2.1.: Circular permutation.

The arrangements are considered to be the same if the objects are in the same order clockwise. Therefore, keeping c_1 in a fixed position there are $(n - 1)!$ arrangements for the remaining objects.

2.4.6 Note

There are $(n-1)!$ permutations of n distinct objects in a circle.

2.4.7 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 $10! \times 9!$ ways.

2.4.8 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.

2.4.9 Example

Here are 2^r , r -digit binary sequences. Out of these 2^r sequences how many of them have even number of 1'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 1s and other has odd number of 1s. Hence there are,

$$\frac{1}{2} \times 2^r = 2^{r-1}$$

r -digit binary sequences that contain even number of 1s.

2.4.10 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 $\sum_{i=1}^k m_i = n$.

2.4.11 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,

$$\frac{n!}{m_1!m_2!\dots m_k!},$$

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 $x \cdot m_1!$ permutations.

Now make m_2 identical objects all distinct. Then we get $x m_1! m_2!$ permutations of n objects in which m_3 are alike, ... m_k are alike.

Continuing this process we get $x m_1! m_2! \dots m_k!$ as the number of permutations of n objects of which are all distinct and hence equal to $n!$.

Therefore –

$$x = \frac{n!}{m_1! m_2! \dots m_k!}.$$

2.4.12 Example

Find the number of different letter arrangements can be formed using “MATHEMATICS”.

Solution: Total number of letters $n = 11$ (with repetitions)

Number of Ms = 2

Number of Ts = 2

Number of As = 2.

And the letters H, C, S, E, each is 1.

Therefore the required number of permutations is $\frac{11!}{2!2!2!1!1!1!1!} = 66, 52, 800$.

2.4.13 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) $C(10, 3) + C(10, 4) + C(10, 5) + \dots + C(10, 10)$, which is also equal to $2^{10} - C(10, 1) - C(10, 2)$.

2.4.14 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, 3, 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 –

$$C(15, 3) + C(15, 2)C(15, 1) = 560 \text{ ways.}$$

2.4.15 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

$$C(n, 0) + C(n, 1) + \dots + C(n, n)$$

Subsets of A. But from binomial theorem, we have the number of subsets of a set with n elements as –

$$C(n, 0) + C(n, 1) + \dots + C(n, n) = 2^n$$

2.4.16 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 $4^{15} - [3^{15} + 3^{14} C(15, 1) + 3^{13} C(15, 2)]$.

2.4.17 Example

A student is to answer 12 out of 15 questions in an examination. How many choices does the student have

- in all?
- if he must answer the first two questions.
- if he must answer the first or second question but not both.
- if he must answer exactly 3 of the first-five questions.
- if he must answer at least 3 of the first-five questions.

Solution:

- $C(15, 12)$ ways
- If the first-two questions are to be answered he has to select 10 questions out of remaining 13. Thus, he has $C(13, 10)$ choices.
- 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 = $2 \times C(13, 11)$.
- 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 $C(10, 9)$ choices. Thus in total he has $C(5, 3)C(10, 9)$ choices.
- 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.

2.4.18 Note (Combinations with repetitions):

Suppose 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 –

$$C(n + r - 1, r) = \frac{(n + r - 1)!}{r!(n - 1)!}.$$

2.4.19 Example

The number of ways to choose 3 out of 7 days (repetitions allowed) is
 $C(7 + 3 - 1, 3) = C(9, 3) = 84$.

2.4.20 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.

2.4.21 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 –

$$\frac{12!}{1!1!1!1!1!7!} = \frac{12!}{7!}$$

(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 the total number of ways =

$$5! \times C(6 + 7 - 1, 7) = 5! \times C(12, 7) = 5! \times \frac{12!}{5!7!} = \frac{12!}{7!}$$

2.4.22 Example

In how many ways can a lady wear five rings on the fingers (not the thumb) of her right hand?

Solution: There are five rings and four fingers. 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 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?
4. Find the number of arrangements of the letters in the word: ACCOUNTANT
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.

2.5 Partitions and Binomial Coefficients

2.5.1 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 $\{A_1, A_2, \dots, A_t\}$ of t subsets of S , such that

- (i) $S = A_1 \cup A_2 \cup \dots \cup A_t$
- (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.

2.5.2 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 .

2.5.3 Note

An ordered partition of S is of *type* (q_1, q_2, \dots, q_t) if $|A_i| = q_i$. That is., A_i contains q_i elements.

2.5.4 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.

2.5.5 Theorem

The number of ordered partition of a set with n elements of type (q_1, q_2, \dots, q_t) is

$$P(n, q_1, q_2, \dots, q_t) = \frac{n!}{q_1! q_2! \dots q_t!}.$$

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, \dots, q_t) is $C(n, q_1) C(n-q_1, q_2) \dots C(n-q_1-q_2 \dots -q_{t-1}, q_t)$, which is equal to $P(n, q_1, q_2, \dots, q_t)$.

2.5.6 Example

Let $S = \{a, b, c, d\}$. The number of ordered partition of type $(1, 2, 1)$ is

$$P(4, 1, 2, 1) = \frac{4!}{1!2!1!} = 12.$$

2.5.7 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 –

$$\frac{25!}{10!5!4!6!}$$

2.5.8 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, \dots, 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.

2.5.9 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.

2.5.10 Definition

Let A_1, A_2, \dots, A_n be subsets of S . Then a **minset** generated by A_1, A_2, \dots, A_n is of the form $B_1 \cap B_2 \cap \dots \cap B_n$, where B_i , may be either A_i , or A_i' ($A_i' = S - A_i$).

2.5.11 Theorem

Let A_1, A_2, \dots, A_n are subsets of S . Then the non-empty minsets generated by A_1, A_2, \dots, A_n form a partition of S .

Proof: Let A_1, A_2, \dots, A_n are n subsets of S . Then there are $k = 2^n$ minsets M_1, M_2, \dots, M_k (generated by A_1, A_2, \dots, A_n). Further

$$\bigcup_{i=1}^k M_i \subseteq S.$$

Now let $x \in S$. Then $x \in A_i$ or A_i' for $i = 1, 2, \dots, n$.

Thus x will be in one of the minsets. Hence

$$S = \bigcup_{i=1}^k M_i.$$

Hence M_1, M_2, \dots, M_k form a partition of S .

2.5.12 Example

Let $S = \{1, 2, 3, \dots, 9\}$. 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.

2.5.13 Definition (Binomial theorem):

Let n be a positive integer, we have –

$$(a + b)^n = a^n + na^{n-1}b + \frac{n(n-1)}{2!}a^{n-2}b^2 + \dots + \frac{n(n-1)(n-2)\dots(n-r+1)}{r!}a^{n-r}b^r + \dots + b^n.$$

The coefficients are –

$C(n, 0), C(n, 1), \dots, C(n, r), \dots, C(n, n)$.

These coefficients are called binomial coefficients, where;

$$C(n, r) = \frac{n!}{r!(n-r)!}$$

2.5.14 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. $C(n, 0) + C(n, 1) + \dots + C(n, n) = 2^n$.
2. $2.C(n, 1) + C(n, 3) + \dots = C(n, 0) + C(n, 2) + \dots = 2^{n-1}$.
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 $n \geq r \geq k \geq 0$.
5. Pascal Identity: $C(n+1, r) = C(n, r) + C(n, r-1)$
6. Vandermonde's Identity:

$$C(n+m, r) = C(n, 0).C(m, r) + C(n, 1).C(m, r-1) + \dots + C(n, r).C(m, 0)$$

$$= \sum_{k=0}^r C(m, r-k).C(n, k) \text{ for integers } n \geq r \geq 0 \text{ and } m \geq r \geq 0.$$

The combinatorial proofs of (3), (4) and (6) are given below and the remaining identities left as exercises.

2.5.15 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.

2.5.16 Problem

Prove the Pascal Identity

$$C(n + 1, r) = C(n, r) + C(n, r-1)$$

where n and r are positive integers with $r \geq n$.

Proof: A choice of r of the $n + 1$ objects x_1, x_2, \dots, 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, \dots, 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, \dots, 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

$$C(n + 1, r) = C(n, r) + C(n, r-1).$$

2.5.17 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 $k = 0, 1, 2, \dots, n$. 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

- The first ($k = 0$) and the last ($k = n$) entries are both equal to 1.
- For $1 \leq k \leq n-1$, the k^{th} entry in the n^{th} row is the sum of the $(k-1)^{\text{th}}$ and k^{th} entries in the $(n - 1)$ rows.

The first eight rows of Pascal's trinagle are shown in the following diagram.

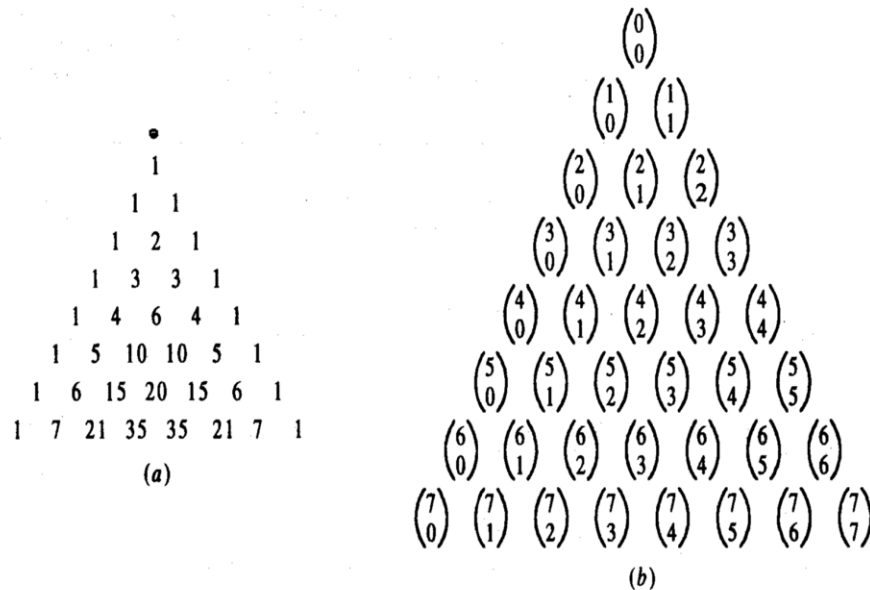


Figure 2.2

A basic property of binomial coefficients is illustrated by Pascal's triangle. If we evaluate the 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 it 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.

Self Assessment Questions

6. 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 .
7. Let $S = \{1, 2, 3, 4, 5, 6\}$; $A_1 = \{2, 5, 6\}$, $A_2 = \{1, 2, 3\}$, $A_3 = \{1, 4, 6\}$. Find the partition of S into minsets generated by A_1 , A_2 and A_3 .

2.6 Principle of Inclusion and Exclusion

For any two sets P and Q , we have ;

- i) $|P \cup Q| \leq |P| + |Q|$ where $|P|$ is the number of elements in P , and $|Q|$ is the number elements in Q .
- ii) $|P \cap Q| \leq \min(|P|, |Q|)$
- iii) $|P \oplus Q| = |P| + |Q| - 2|P \cap Q|$ where \oplus is the symmetric difference.

2.6.1 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.

2.6.2 Theorem

If A_1, A_2, \dots, A_n are finite sets, then $|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{i=1}^n |A_i|$

$$- \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.$$

2.6.3 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 don’t 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,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= 15 + 8 + 6 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + 3 \\ &= 32 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &\leq 32 - 3 - 3 - 3 = 23 \quad (\text{since } |A_i \cap A_j \cap A_k| \leq |A_i \cap A_j| \text{ for any } i, j, k) \end{aligned}$$

Therefore there are at most 23 cars with one or more options. This means there are at least 7 cars that do not have any options.

2.6.4 Example

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.

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

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

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

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

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

Therefore $|A_1 \cup A_2 \cup A_3 \cup A_4| = 125 + 83 + 50 + 35 - 41 - 25 - 17 - 16 - 11 - 7 + 8 + 5 + 3 + 2 - 1 = 193$.

2.6.5 Example

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?

Solution: Let A_{289} be the event of having pattern 289. Similarly A_{234} and A_{487} .

We have to find $|A_{289} \cup A_{234} \cup A_{487}|$.

Now $|A_{289}| = 8!$, as 289 considered as a group, which is a single object and the remaining seven single digits. Similarly $|A_{234}| = |A_{487}| = 8!$

Also since 2 cannot be followed by both 3 and 8, we have $|A_{289} \cap A_{234}| = 0$.

Similarly $|A_{289} \cap A_{487}| = 0$. But

$|A_{234} \cap A_{487}| = 6!$, since 23487 as a single object and remaining 5 single objects.

$$|A_{289} \cap A_{234} \cap A_{487}| = 0.$$

Therefore, by the principle of inclusion and exclusion –

$$|A_{289} \cup A_{234} \cup A_{487}| = 8! + 8! + 8! - 0 - 0 - 6! + 0 = 3 \times 8! - 6!.$$

2.6.6 Note

Among the permutations of $\{1, 2, 3, \dots, n\}$, there are some (called derangements), in which none of the n integers appears in its natural place.

In other words: (i_1, i_2, \dots, i_n) is a derangement if $i_1 \neq 1, i_2 \neq 2, \dots$, and $i_n \neq n$.

If ' D_n ' denote the number of derangements of $\{1, 2, 3, \dots, n\}$, then for $n = 1, 2, 3$, we have,

$$D_1 = 0,$$

$$D_2 = 1,$$

$$D_3 = 2 \text{ (that is, the only derangements of } (1, 2, 3) \text{ are } (2, 3, 1) \text{ and } (3, 1, 2)).$$

2.6.7 The formula for D_n for any positive integer n ,

Let U be the set of $n!$ Permutations of $\{1, 2, 3, \dots, n\}$.

For each i , let A_i be the permutation (b_1, b_2, \dots, b_n) of $\{1, 2, 3, \dots, n\}$ such that $b_i = i$.

Then $A_1 = \{(1, b_2, \dots, b_n) / (b_2, b_3, \dots, b_n) \text{ is a permutation of } \{2, 3, \dots, n\}\}$.

Therefore $|A_1| = (n-1)!$. In a similar way $|A_i| = (n-1)!$ for each i .

Also $A_1 \cap A_2 = \{(1, 2, b_3, \dots, b_n) / (b_3, b_4, \dots, b_n) \text{ is a permutation of } \{3, 4, \dots, n\}\}$. Therefore $|A_1 \cap A_2| = (n-2)!$.

In a similar way, $|A_i \cap A_j| = (n-2)!$ for all i, j . Therefore, for any integer k , $1 \leq k \leq n$.

$$|A_1 \cap A_2 \cap \dots \cap A_k| = (n-k)!$$

This is true for any k -combination of $\{1, 2, \dots, n\}$.

$$\begin{aligned}
\text{Therefore } D_n &= \left| \overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n} \right| \\
&= \left| \overline{(A_1 \cup A_2 \cup \dots \cup A_n)} \right| \\
&= |U| - |A_1 \cup A_2 \cup \dots \cup A_n| \\
&= n! - C(n, 1)(n-1)! + C(n, 2)(n-2)! + \dots + (-1)^n C(n, n) \\
&= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \dots + (-1)^n \frac{n!}{n!} \\
&= n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right] \\
&= n!e^{-1}, \text{ if } n \text{ is very large.}
\end{aligned}$$

2.6.8 Example

Let n books be distributed to n students. Assume that the books are returned and distributed to the students again later on. In how many ways can the books be distributed so that no student will get the same book twice?

Solution: First time the books are distributed in $n!$ ways; since no student gets the same book that he got first time, the second time D_n ways.

Therefore the total number of ways:

$$\begin{aligned}
n! D_n &= n! n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right] = (n!)^2 \\
&\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right].
\end{aligned}$$

Self Assessment Questions

8. Find the number of derangements of the integers from 1 to 10 inclusive, satisfying the condition that the set of elements in the first 5 places is –
- 1, 2, 3, 4, 5 in some order;
 - 6, 7, 8, 9, 10 in some order.

2.7 Summary

In this unit, 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 illustrations on permutations and combination with distinct objects are given. These are also useful in graph theoretical algorithm. Further we studied the partitions, binomial coefficients and the principle of inclusion and exclusion with some applications.

2.8 Terminal 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 is 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, \dots, 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 P_1 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?

2.9 Answers

Self Assessment Questions

1.
 - a) 2^7
 - b) $26^3 \times 10^4$
 - c) $10 \times 9 \times 8 = 720$
 - d) 6^{100}
 - e) $100 + (100 \times 99)$
2. 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 = $4 \times 4 \times 3 \times 2 \times 1 = 96$.

3. a) 6720, 840
b) I) $10!$, II) $P(10, 7)$, III) $9!$
c) $3! 8!$
d) 1080 (allowing leading zero).
4. The number of arrangements = $\frac{10!}{2!2!2!2!1!} = 226800$.
5. (i) 90, (ii) 100.
6. $M_1 = \{3, 4\}$, $M_2 = \{2\}$, $M_3 = \{5\}$, $M_4 = \{1\}$ form a partition into min-sets.
7. $M_1 = \{2\}$, $M_2 = \{6\}$, $M_3 = \{5\}$, $M_4 = \{1\}$, $M_5 = \{4\}$, $M_6 = \{3\}$ form a partition into min-sets.
8. (i). $D_5 \cdot D_5$ ways; (ii) $(5!)^2 = 14,400$ derangements.

Unit 3

Recurrence Relations

Structure

- 3.1 Introduction
 - Objectives
- 3.2 Recurrence Relation
- 3.3 Particular Solution
- 3.4 Generating Functions
- 3.5 Applications of Recurrences
- 3.6 Integer Functions
- 3.7 Summary
- 3.8 Terminal Questions
- 3.9 Answers

3.1 Introduction

A sequence can be defined by giving a general formula for its n^{th} term or by writing a 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 a few applications of recurrences and a brief explanation of the integer functions.

Objectives:

At the end of the unit, you would be able to:

- solve recurrences.
- use the generating functions to solve the recurrence relations.
- know the applications of recurrence relations.
- learn the integer function.

3.2 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, \dots, 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.

3.2.1 Example

Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} - a_{n-2}$ for $n=2, 3, 4, \dots$ 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.

3.2.2 Example

Determine whether the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \dots$ 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 $2a_1 - a_0 = 2 \cdot 2 - 1 = 3 \neq a_2$. Therefore $\{a_n\}$, where $a_n = 2^n$ is not a solution of the recurrence relation.

3.2.3 Definition

A recurrence relation of the form $C_0 a_r + C_1 a_{r-1} + C_2 a_{r-2} + \dots + C_k a_{r-k} = f(r)$, 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.

3.2.4 Example

$2a_r + 3a_{r-1} = 2^r$ is the first order linear recurrence, with constant coefficients.

3.2.5 Fibonacci sequence

The sequence of the form $\{1, 1, 2, 3, 5, 8, 13, \dots\}$ 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 $a_1 = 1$.

3.2.6 Note

$a_n = r^n$, where r is constant, is a solution of the recurrence relation

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} + \dots + C_k a_{n-k}$$

if and only if

$$r^n = C_1 r^{n-1} + C_2 r^{n-2} + \dots + C_k r^{n-k}.$$

Dividing both sides by r^{n-k} and the right hand side is subtracted from the left, we obtain the equation

$$r^k - C_1 r^{k-1} - C_2 r^{k-2} - \dots - C_{k-1} r - C_k = 0 \dots\dots\dots(i).$$

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.

3.2.7 Theorem

Let C_1 and C_2 be real numbers. Suppose that $r^2 - C_1 r - C_2 = 0$ has two distinct roots r_1 and r_2 . Then the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = C_1 a_{n-1} + C_2 a_{n-2}$ if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n = 0, 1, 2, \dots$ where α_1 and α_2 are constants.

3.2.8 Example

Find the solution of 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

$$a_0 = 2 = \alpha_1 + \alpha_2, \quad a_1 = 7 = \alpha_1 + \alpha_2 = 3 \text{ and } \alpha_2 = -1.$$

Therefore, the solution to the recurrence relation is $a_n = 3 \cdot 2^n - (-1)^n$.

3.2.9 Theorem

Let C_1 and C_2 be real numbers with $C_2 \neq 0$. Suppose that $r^2 - C_1 r - C_2 = 0$ has only one root r_0 . A sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = C_1 a_{n-1} + C_2 a_{n-2} \text{ if and only if } a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n, \text{ for } n = 0, 1, 2, \dots,$$

where α_1 and α_2 are constants.

3.2.10 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 $a_n = \alpha_1 3^n + \alpha_2 n 3^n$, for some constants α_1 and α_2 .

Using the initial conditions, we get $a_0 = 1 = \alpha_1$, $a_1 = 6 = \alpha_1 \cdot 3 + \alpha_2 \cdot 3$.

Solving these simultaneous equations, we get $\alpha_1 = 1$ and $\alpha_2 = 1$.

Therefore, the solution to the recurrence relation is $a_n = 3^n + n 3^n$.

3.2.11 Theorem

Let C_1, C_2, \dots, C_k be real numbers. Suppose that the characteristic equation $r^k - C_1 r^{k-1} - \dots - C_k = 0$ has k distinct roots r_1, r_2, \dots, r_k . Then a sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = C_1 a_{n-1} + C_2 a_{n-2} + \dots + C_k a_{n-k}$ if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \dots + \alpha_k r_k^n$, for $n = 0, 1, 2, \dots$, where $\alpha_1, \alpha_2, \dots, \alpha_k$ are constants.

3.2.12 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 $a_n = \alpha_1 \cdot 1^n + \alpha_2 \cdot 2^n + \alpha_3 \cdot 3^n$.

From the given initial condition, $a_0 = 2$, we get

$a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3$. Similarly, for $a_1 = 5 = \alpha_1 + \alpha_2 \cdot 2 + \alpha_3 \cdot 3$; $a_2 = 15 = \alpha_1 + \alpha_2 \cdot 4 + \alpha_3 \cdot 9$.

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 $a_n = 1 - 2^n + 2 \cdot 3^n$.

3.2.13 Theorem

Let C_1, C_2, \dots, C_k be real numbers. Suppose that the characteristic equation $r^k - C_1 r^{k-1} - \dots - C_k = 0$ has t -distinct roots r_1, r_2, \dots, r_t with multiplicities m_1, m_2, \dots, m_t , respectively, so that $m_i \geq 1$, for $i = 1, 2, \dots, t$ and $m_1 + m_2 + \dots + m_t = k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = C_1 a_{n-1} + C_2 a_{n-2} + \dots + C_k a_{n-k}$ if and only if $a_n = (\alpha_{1,0} + \alpha_{1,1} \cdot n + \dots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n + \dots + (\alpha_{t,0} + \alpha_{t,1} n + \dots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n$, for $n = 0, 1, 2, \dots$, where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_i - 1$.

3.2.14 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 3.2.13, the solutions are of the form $a_n = \alpha_{1,0}(-1)^n + \alpha_{1,1} \cdot n(-1)^n + \alpha_{1,2} \cdot n^2(-1)^n$. 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 $a_n = (1 + 3n - 2n^2)(-1)^n$.

3.3 Particular Solution

The particular solution depends on the form of $f(r)$. The particular solution for some simple functions $f(r)$ is given in the following table.

Table 3.1

$f(r)$	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 , $F_1r^t + F_2r^{t-1} + \dots + F_{t+1}\beta^r$	Polynomial of degree t in r , $P_1r^t + P_2r^{t-1} + \dots + P_{t+1}P\beta^r$ if β is not a root of the characteristic equation. If β is a root of multiplicity of m , then $Pr^m\beta^r$.
$(F_1r^t + F_2r^{t-1} + \dots + F_{t+1})\beta^r$	$(P_1r^t + P_2r^{t-1} + \dots + P_{t+1})\beta^r$ if β is not a root of the characteristic equation. $r^m(P_1r^t + P_2r^{t-1} + \dots + P_{t+1})\beta^r$ if β is a root of multiplicity m .

3.3.1 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.

3.3.2 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

$$P - 5P + 6P = 1 \text{ or } P = \frac{1}{2}.$$

Therefore, the total solution is $a_n = A_1(3)^n + A_2(2)^n + \frac{1}{2}$.

3.3.3 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

$$P_1n^2 + P_2n + P_3 - 4P_1(n-1)^2 - 4P_2(n-1) - 4P_3 + 4P_1(n-2)^2 + 4P_2(n-2) + 4P_3 = n^2 + 2n + 1.$$

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

$$P_1 = 1, P_2 - 8P_1 = 2, P_3 - 4P_2 + 12P_1 = 1.$$

Hence $P_1 = 1, P_2 = 10, P_3 = 29$.

Therefore, the total solution is –

$$a_n = (A_1n + A_2)2^n + n^2 + 10n + 29.$$

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 –

$$a_n = \left(\frac{19}{2}n - 29\right)2^n + n^2 + 10n + 29.$$

3.3.4 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

$$P3^n - 3P3^{n-1} - 4P3^{n-2} = 3^n.$$

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,

$$1 = A_1 + A_2 - \frac{9}{4}; \quad 2 = A_1 + 4A_2 - \frac{27}{4}.$$

We get $A_1 = \frac{17}{20}$, $A_2 = \frac{12}{5}$. Therefore, the total solution is –

$$a_n = \frac{17}{20}(-1)^n + \frac{12}{5}(4)^n - \frac{9}{4}(3)^n.$$

3.3.5 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,

$$Pn^22^n - 4P(n-1)^22^{n-1} + 4P(n-2)^22^{n-2} = 2^n.$$

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 $a_n = (A_1n + A_2)2^n + n^2 (2)^{n-1}$.

3.3.6 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 $n(P_1n + P_2)2^n$. Substituting,

$$n(P_1n + P_2)2^n - 2\{(n-1)[P_1(n-1) + P_2]\}2^{n-1} = (n+1)2^n.$$

That is., $(2P_1n + P_2 - P_1)2^n = (n+1)2^n$

Equating the coefficients, we get,

$$P_1 = \frac{1}{2} \text{ and } P_2 = \frac{3}{2}.$$

Thus particular solution is,

$$n\left(\frac{1}{2}n + \frac{3}{2}\right)2^n \text{ and } P_2 = \frac{3}{2}.$$

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 $a_0 = 1$, $a_1 = 4$.

3.4 Generating Functions

A generating function is a polynomial of the form $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$, which has infinitely many non-zero terms. There is a correspondence between generating functions and sequences.

(That is, $a_0 + a_1x + a_2x^2 + \dots \leftrightarrow a_0, a_1, a_2, \dots$).

3.4.1 Example

(i) The generating function of the sequence 1, 2, 3, ... of natural numbers is $f(x) = 1 + 2x + 3x^2 + \dots$

(ii) The generating function of the arithmetic sequence 1, 4, 7, 10, ... is

$$f(x) = 1 + 4x + 7x^2 + 10x^3 + \dots$$

3.4.2 Note

Let $f(x) = a_0 + a_1x + a_2x^2 + \dots$ and $g(x) = b_0 + b_1x + b_2x^2 + \dots$ be two generating sequences, then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots$ and $f(x)g(x) = (a_0b_0) + (a_1b_0 + a_0b_1)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots$, the coefficient of x^n in the product $f(x)g(x)$ is the finite sum: $a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \dots + a_nb_0$.

3.4.3 Example

If $f(x) = 1 + x + x^2 + \dots + x^n + \dots$ and $g(x) = 1 - x + x^2 - x^3 + \dots + (-1)^n x^n + \dots$, then

$$\begin{aligned} f(x) + g(x) &= (1 + 1) + (1 - 1)x + (1 + 1)x^2 + \dots + (1 + (-1)^n)x^n + \dots \\ &= 2 + 2x^2 + 2x^4 + \dots \end{aligned}$$

$$\begin{aligned} f(x)g(x) &= 1 + [1(-1) + 1(1)]x + [1(1) + 1(-1) + 1(1)]x^2 + \dots \\ &= 1 + x^2 + x^4 + x^6 + \dots \end{aligned}$$

3.4.4 Problem

Solve the recurrence relation $a_n = 3a_{n-1}$, $n \geq 1$, $a_0 = 1$ using generating function.

Solution: Consider the generating function $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$ of the sequence a_0, a_1, a_2, \dots

$$3x.f(x) = 3a_0x + 3a_1x^2 + \dots + 3a_{n-1}x^n + \dots$$

$$f(x) - 3x.f(x) = a_0 + (a_1 - 3a_0)x + (a_2 - 3a_1)x^2 + \dots + (a_n - 3a_{n-1})x^n + \dots$$

Since $a_0 = 1$, $a_1 = 3a_0$ and in general, $a_n = 3a_{n-1}$, we get $(1 - 3x) f(x) = 1$

$$\Rightarrow f(x) = \frac{1}{1-3x} = (1 - 3x)^{-1} = 1 + 3x + (3x)^2 + \dots + (3x)^n + \dots$$

Therefore a_n , which is the coefficient of x^n in $f(x)$, is equal to 3^n .

3.4.5 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 $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots$

$$2xf(x) = 2a_0x + 2a_1x^2 + \dots + 2a_{n-1}x^n + \dots$$

$$x^2f(x) = a_0x^2 + \dots + a_{n-2}x^n + \dots$$

Therefore,

$$f(x) - 2xf(x) + x^2f(x) = a_0 + (a_1 - 2a_0)x + (a_2 - 2a_1 + a_0)x^2 + \dots + (a_n - 2a_{n-1} + a_{n-2})x^n + \dots$$

$$= 3 - 8x \text{ (since } a_0 = 3, a_1 = -2 \text{ and } a_n - 2a_{n-1} + a_{n-2} = 0 \text{ for } n \geq 2).$$

$$\text{On simplification, we get } f(x) = \frac{1}{(1-x)^2} (3 - 8x)$$

$$= (1 + 2x + 3x^2 + \dots + (n+1)x^n + \dots)(3 - 8x)$$

$$= 3 - 2x - 7x^2 - 12x^3 + \dots + (-5n + 3)x^n + \dots$$

Therefore, the coefficient of x^n , that is.; $a_n = 3 - 5n$ is the solution.

3.4.6 Table of some generating functions

Table 3.2

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
$C(n, r)$	$(1+z)^n$

3.4.7 Example

Solve the recurrence relation $a_r - 7a_{r-1} + 10a_{r-2} = 0$ for $n \geq 2$ 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

$$\sum_{r=2}^{\infty} a_r z^r - 7 \sum_{r=2}^{\infty} a_{r-1} z^r + 10 \sum_{r=2}^{\infty} a_{r-2} z^r = 0$$

$$\Rightarrow [A(z) - a_0 - a_1 z] - 7z [A(z) - a_0] + 10z^2 [A(z)] = 0$$

$$\Rightarrow [A(z) - a_0 - a_1z] - 7z[A(z) - a_0] + 10z^2[A(z)] = 0$$

$$\begin{aligned}\Rightarrow A(z) &= \frac{a_0 + (a_1 - 7a_0)z}{1 - 7z + 10z^2} \\ &= \frac{a_0 + (a_1 - 7a_0)z}{(1 - 2z)(1 - 5z)} \\ &= \frac{C_1}{1 - 2z} + \frac{C_2}{1 - 5z} \\ &= C_1 \sum_{r=0}^{\infty} 2^r z^r + C_2 \sum_{r=0}^{\infty} 5^r z^r\end{aligned}$$

Thus $a_r = C_1 2^r + C_2 5^r$, $r \geq 2$.

Given that $a_0 = 10$, $a_1 = 41$. Substituting, we get $C_1 = 3$, $C_2 = 7$. Thus $a_r = 3 \cdot 2^r + 7 \cdot 5^r$.

3.4.8 Example

Solve $a_r - 5a_{r-1} + 6a_{r-2} = 2^r + r$, where $r \geq 2$, with $a_0 = 1$, $a_1 = 1$.

Solution: Multiplying the given equation by z^r and summing from 2 to ∞ , we get

$$\sum_{r=2}^{\infty} a_r z^r - 5 \sum_{r=2}^{\infty} a_{r-1} z^r + 6 \sum_{r=2}^{\infty} a_{r-2} z^r = \sum_{r=2}^{\infty} 2^r z^r + \sum_{r=2}^{\infty} r z^r$$

$$\Rightarrow [A(z) - a_0 - a_1z] - 5z[A(z) - a_0] + 6z^2[A(z)] = \frac{4z^2}{1-2z} + z \left[\frac{1}{(1-z)^2} - 1 \right]$$

$$\text{Therefore, } A(z) = \frac{1 - 8z + 27 - 35z^2 + 14z^4}{(1-z)^2(1-2z)^2(1-3z)}.$$

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

$$a_r = \frac{5}{4} + \frac{1}{2}(r+1) - 3 \times 2^r - 2(r+1)2^r + \frac{17}{4} = \frac{5}{4} + \frac{r}{2} - r2^{r+1} - 5 \times 2^r + \frac{17}{4}3^r$$

3.4.9 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 $a_0 = 0$ and $a_1 = 1$, we obtain

$$A(z) = \frac{1 + (1-1)z}{1 - z - z^2} = \frac{1}{1 - z - z^2} = \frac{1}{\left(1 - \frac{1+\sqrt{5}}{2}z\right)\left(1 - \frac{1-\sqrt{5}}{2}z\right)}$$

$$= \frac{C_1}{1 + \frac{1+\sqrt{5}}{2}z} + \frac{C_2}{1 - \frac{1-\sqrt{5}}{2}z}. \text{ Here}$$

$$C_1 = \frac{1}{\sqrt{5}} \frac{1+\sqrt{5}}{2}, \quad C_2 = -\frac{1}{\sqrt{5}} \frac{1+\sqrt{5}}{2}$$

$$\text{Hence } a_r = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{r+1} - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{r+1}.$$

Self Assessment Question

3. If $f(x) = 1 + x + x^2 + \dots + x^n + \dots$ and $g(x) = 1 - x + x^2 - x^3 + \dots + (-1)^n x^n + \dots$

Find $f(x) + g(x)$, and $f(x).g(x)$.

3.5 Applications of Recurrences

3.5.1 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 one 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, $T_1 = 1$, $T_2 = 3$

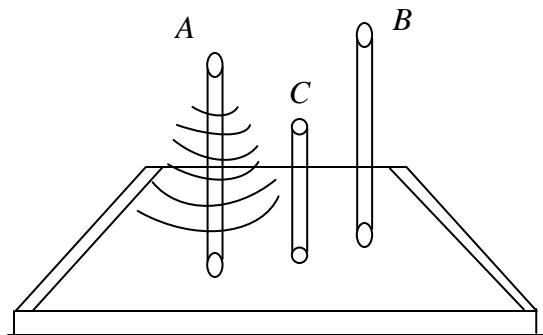


Figure 3.1

Now transfer the top disks to the middle peg, then move the third, then bring the other two onto it. So we get,

$$T_3 = 7 = 2 \cdot 3 + 1 = 2 T_2 + 1.$$

Induction hypo: Assume for $n-1$ disks. That is., $T_{n-1} = 2 \cdot T_{n-2} + 1$.

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 $2T_{n-1} + 1$ moves.

Thus $T_n \leq 2T_{n-1} + 1$ for $n > 0$.

This shows that $2T_{n-1} + 1$ moves are sufficient 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 Hanoi problem.

From this it is clear that $T_3 = 2 \cdot 3 + 1 = 7$, $T_4 = 2 \cdot 7 + 1 = 15$, and so on.

3.5.2 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.

3.5.3 Problem

Find the shortest sequence e of moves that transfers a tower of n disks from the left peg A to the right peg B, if direct moves between A and B are disallowed.

(Each move must be to or from the middle peg. As usual a large disk must never appear above a smaller one).

Solution

Let X_n denote the number of moves.

For $n = 0$, $X_0 = 0$

For $n = 1$, $X_1 = 2$.

For $n = 2$, consider the sequence of steps:

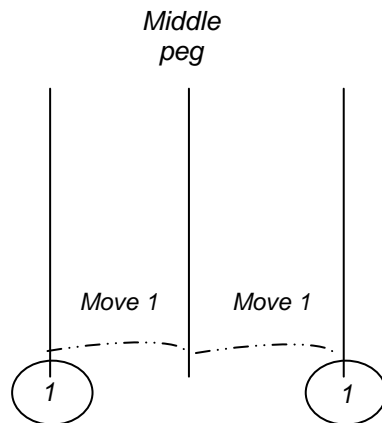


Figure 3.2

- (i) Transfer disk 1 from A to M } 2 moves
- (ii) Transfer disk 1 from M to B }
- (iii) Transfer disk 2 from A to M } 1 moves
- (iv) Transfer disk 1 from B to M } 2 moves
- (v) Transfer disk 1 from M to A }
- (vi) Transfer disk 2 from M to B } 1 moves
- (vii) Transfer disk 1 from A to M } 2 moves
- (viii) Transfer disk 1 from M to B }

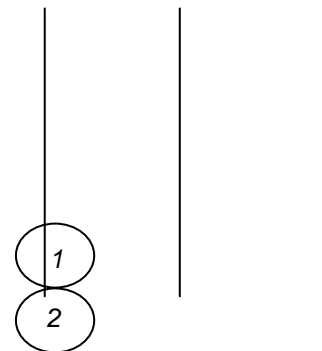


Figure 3.3

Total number of moves is 8.

That is., $X_2 = X_1 + 1 + X_1 + 1 + X_1 = 2 + 1 + 2 + 1 + 2 = 8$

Similarly, $X_3 = X_2 + 1 + X_2 + 1 + X_2 = 8 + 1 + 8 + 1 + 8 = 26$

In general, $X_n = X_{n-1} + 1 + X_{n-1} + 1 + X_{n-1}$; $n > 0$, is the recurrence required.

By induction, one can prove that $X_n = 3^n - 1$, $n \geq 0$.

3.6 Integer Functions

3.6.1 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 = $\max \{n / n \leq x, n \text{ is an integer}\}$

3.6.2 Example

Take $x = 2.52$, then

$\lfloor x \rfloor = \max \{n / n \leq x, n \text{ is an integer}\} = \max \{1, 2\} = 2.$

3.6.3 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 = $\min \{n / n \geq x, n \text{ is an integer}\}.$

3.6.4 Example

Take $x = 3.732$, then

$\lceil x \rceil = \min \{n / n \geq x, n \text{ is an integer}\} = \min \{4, 5, 6, 7 \dots\} = 4.$

Observe that for any real number x , $\lfloor x \rfloor \leq x$ and $\lceil x \rceil \geq x.$

3.6.5 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 $x = e = 2.71828 \dots$. We describe floor and ceiling of e as follows:

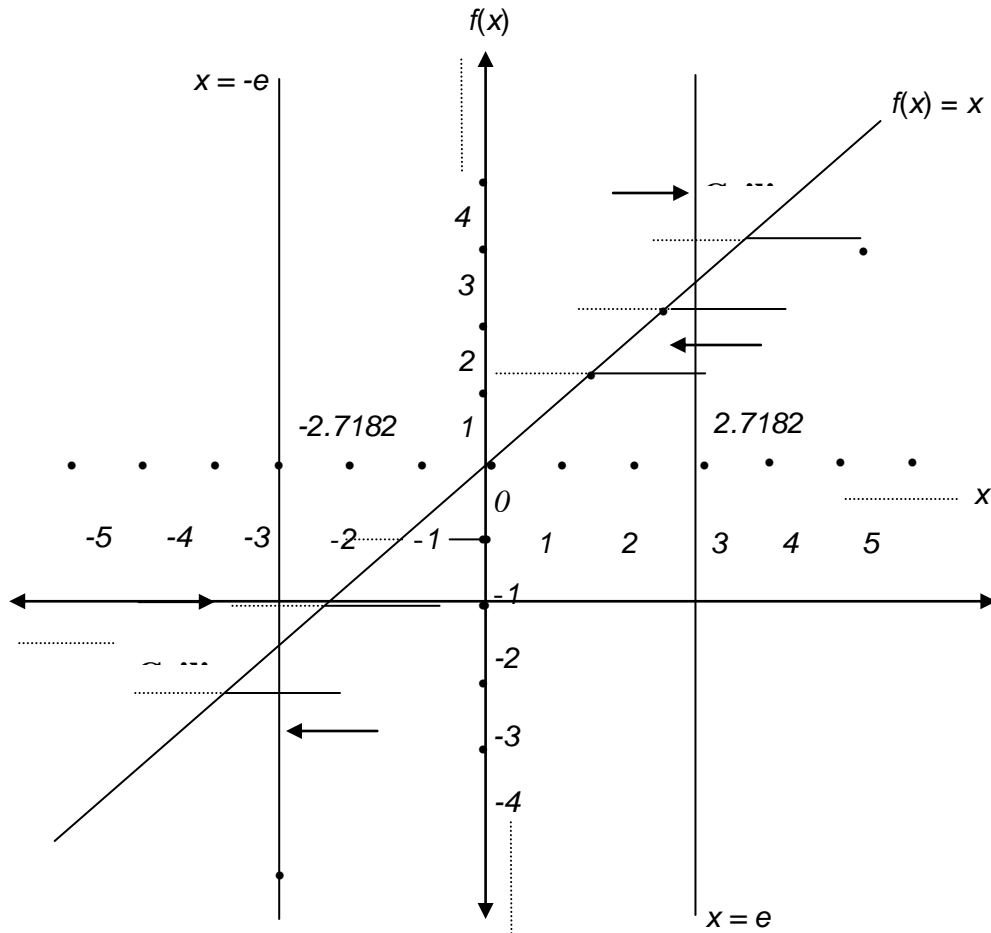


Figure 3.4

From the graph, $\lfloor e \rfloor = 2$ $\lceil x \rceil = \dots\dots\dots$
 $\lfloor -e \rfloor = -3$ $\lfloor x \rfloor = \underline{\hspace{1cm}}$
 $\lceil -e \rceil = -2$

3.6.7 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 $\Leftrightarrow \lceil x \rceil = x$.

$$\text{ii) } \lceil x \rceil - x = [x \text{ is not an integer}]$$

$$\text{That is, } \lceil x \rceil - \lfloor x \rfloor = \begin{cases} 1, & \text{if } x \text{ is not an integer} \\ 0, & \text{otherwise} \end{cases}$$

$$\text{iii) } x - 1 < \lfloor x \rfloor \text{ and } x + 1 > \lceil x \rceil \Rightarrow x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$$

$$\text{iv) } \lfloor -x \rfloor = -\lceil x \rceil \text{ and } \lceil -x \rceil = -\lfloor x \rfloor.$$

3.6.8 Some Rules on floor and ceiling functions

In all the following cases, x is real and n is an integer.

$$1. \lfloor x \rfloor = n \Leftrightarrow n \leq x < n + 1$$

$$2. \lfloor x \rfloor = n \Leftrightarrow x - 1 < n \leq x$$

$$3. \lceil x \rceil = n \Leftrightarrow n - 1 < x \leq n$$

$$4. \lceil x \rceil = n \Leftrightarrow x \leq n < x + 1.$$

3.6.9 Example

The above rules can be illustrated, by taking $x = 4.5$.

$$\lfloor 4.5 \rfloor = 4 \Leftrightarrow 4 \leq 4.5 < 5$$

$$\lfloor 4.5 \rfloor = 4 \Leftrightarrow 3.5 < 4 \leq 4.5$$

$$\lceil 4.5 \rceil = 5 \Leftrightarrow 4 < 4.5 \leq 5$$

$$\lceil 4.5 \rceil = 5 \Leftrightarrow 4.5 \leq 5 < 5.5$$

3.7 Summary

The applications of recurrence relations were discussed in this unit, you 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. The concept of integer functions is given which is useful in the analysis and design of algorithms.

3.8 Terminal 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 $a_n = -a_{n-1} + 2n - 3$, $n \geq 1$, given $a_0 = 1$.

3.9 Answers

Self Assessment Questions

1. $a_n = -2^n + 2(3^n)$.
2. $a_n = 2^n + n(2^n) = (n + 1) \cdot 2^n$.
3. $f(x) + g(x) = 2 + 2x^2 + 2x^4 + \dots$
 $f(x) \cdot g(x) = 1 + x^2 + x^4 + x^6 + \dots$

Terminal Questions

4. (Ans: $a_n = -\frac{2}{7}(-5)^n + \frac{9}{7}(2^n)$).

Unit 4

Partially Ordered Sets

Structure

- 4.1 Introduction
 - Objectives
- 4.2 Partially Ordered Sets
- 4.3 Diagram Representation of Posets
- 4.4 Summary
- 4.5 Terminal Questions
- 4.6 Answers

4.1 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 various properties of partial order relations on a set, and representation of partially ordered sets.

Objectives:

At the end of the unit, you would be able to

- know and explain the order relations.
- draw representation of partial ordered sets.
- know and explain the properties of partial order relations

4.2 Partially Ordered Sets

4.2.1 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 $(a, b) \in R$, we write $a \geq b$. If $a \geq b$ and $a \neq b$, then we write $a > b$.

4.2.2 Example

Let $A = \mathbb{Z}^+$ 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.

4.2.3 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 .

4.2.4 Example

Let A be a non-empty set and $S = P(A)$, the power set of A . Define a relation R on S as –

$$R = \{(X, Y) \mid X, Y \text{ are in } P(A) \text{ such that } X \text{ contains } Y\}.$$

Now we verify that the relation is reflexive.

R is reflexive: For this take $X \in S$. Then X is a subset of A . Since X contains X , we have $(X, X) \in R$.

R is anti-symmetric: Let $(X, Y), (Y, X) \in R$. Then X contains Y , and Y contains X , which imply $X = Y$. Hence the relation is anti-symmetric.

R is transitive: Let $(X, Y), (Y, Z) \in R$. Then X contains Y , and Y contains Z . So X contains Z , which implies $(X, Z) \in R$. Hence R is transitive. Therefore, S is a Poset.

4.2.5 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 (\mathbb{Z}^+, R) where R is defined on \mathbb{Z}^+ as aRb if and only if $a \leq b$ is a chain.

4.2.6 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 .

4.2.7 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 given below 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 .

Also note that B joined to E by a sequence of line segments all going downwards.

So we have $B \geq E$.

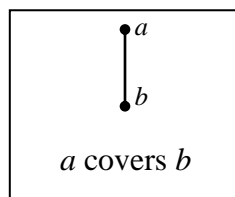


Figure 4.1

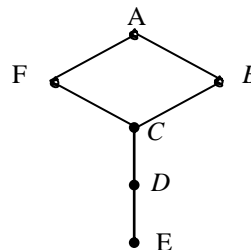


Figure 4.2

4.2.8 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 $b \geq a \Rightarrow b = a$.

4.2.9 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.

4.2.10 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, \dots , 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 for a minimal element is parallel to that of part-I.

4.2.11 Definition

- (i) A **chain** in a Poset is a sequence a_0, a_1, \dots, a_n of elements of the Poset such that $a_i > a_{i+1}$. The length of this chain is said to be n .

4.2.12 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 the 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 the least upper bound of A if $b \geq a$ for all upper bounds b of A .

4.2.13 Note

Let R be the set of all real numbers, $\emptyset \neq A \subseteq R$. 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 $\sup A = \max A$.

4.2.14 Zorn's Lemma

If P is a partially ordered set in which every chain has an upper bound, then P possesses a maximal element.

Self Assessment Questions

1. Determine whether the relation R is a partial ordered on the Z .
 - (i) $a R b \Leftrightarrow a = 2b$
 - (ii) $a R b \Leftrightarrow b^2 / a$, where $a, b \in Z$.
2. Determine which of the following are equivalence relations and / or partial ordering relations for the given sets.
 - (i) $S = \{\text{lines in the plane}\}; xRy \Leftrightarrow x \text{ is parallel to } y$
 - (ii) $N = \{\text{set of natural numbers}\}; xRy \Leftrightarrow |x - y| \leq 5$.

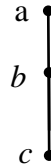
4.3 Diagram Representation of Posets**4.3.1 Definition**

The covering matrix of a finite Poset $P = \{ p_i / 1 \leq i \leq n \}$ is the matrix $(b_{ij})_{n \times n}$ where $b_{ij} = 1$ if p_i covers p_j or $i = j$;
 $= 0$ otherwise.

4.3.2 Example

The diagram of a Poset was given on the right side. The covering matrix of

this Poset is given by
$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$



4.3.3 Note

- (i) The chain $p_0 > p_1 > p_2 > \dots > p_k$ is said to have **length** k .
- (ii) An element p of a finite Poset is on **level** k if there exists a sequence $p_0 > p_1 > \dots > p_k = p$ and any other such sequence has length less than or equal to k .
- (iii) Suppose p is on level k and $p_0 > p_1 > \dots > p_k = p$. 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 $p^1 > p_0 > p_1 > \dots > p_k$ 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 $\Leftrightarrow b_{ij} = 0$ for all $i \neq j$ and $i = 1, 2, \dots, n$. $\Leftrightarrow j^{\text{th}}$ column of (b_{ij}) 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).

4.3.4 Definition

A partial ordering \leq on A Poset, is represented by a diagram called Hasse diagram. In a Hasse diagram, each element is represented by a small circle.

4.3.5 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.

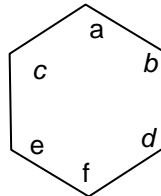


Figure 4.3

4.3.6 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:

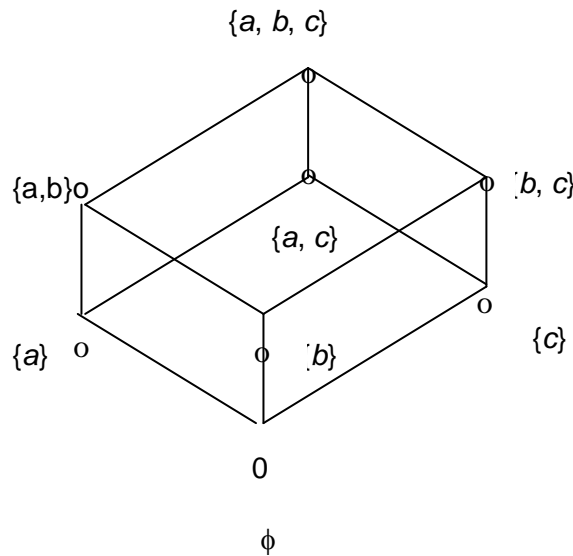


Figure 4.4

4.3.7 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. Finally we get a Poset diagram shown below.

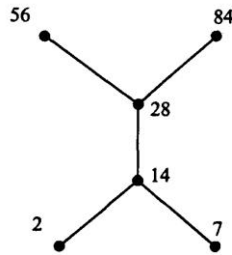


Figure 4.5

4.3.8 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.

$D_6 = \{1, 2, 3, 6\}$,

$D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$

$D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

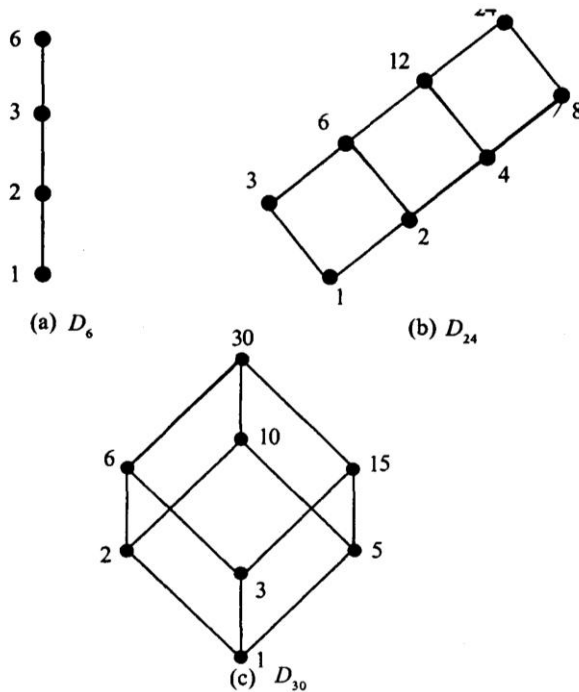


Figure 4.6

4.3.9 Example

Consider the Posets S and T represented in the following figures (a) and (b).

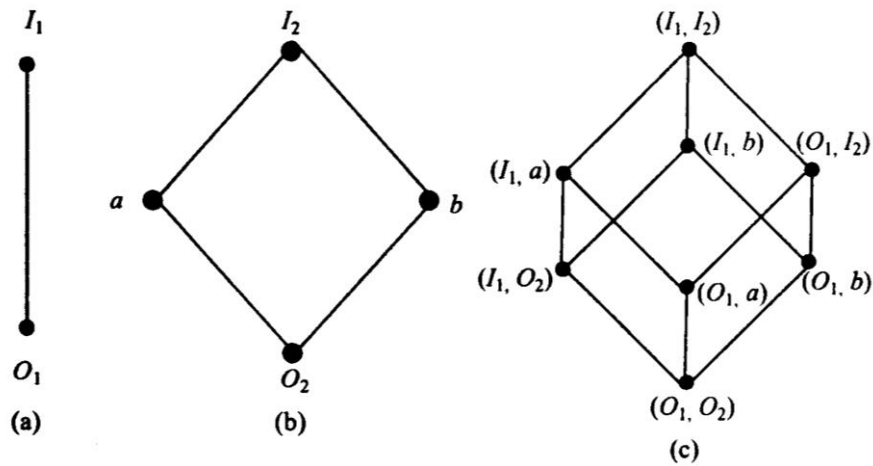


Figure 4.7

Then the Poset $(S \times T, \leq)$ is given in figure (c).

4.3.10 Example

Consider the Posets (D_4, \leq) and (D_9, \leq) given in (a) and (b). The Hasse diagram for $L = D_4 \times D_9$ under the partial order, is given by figure (c).

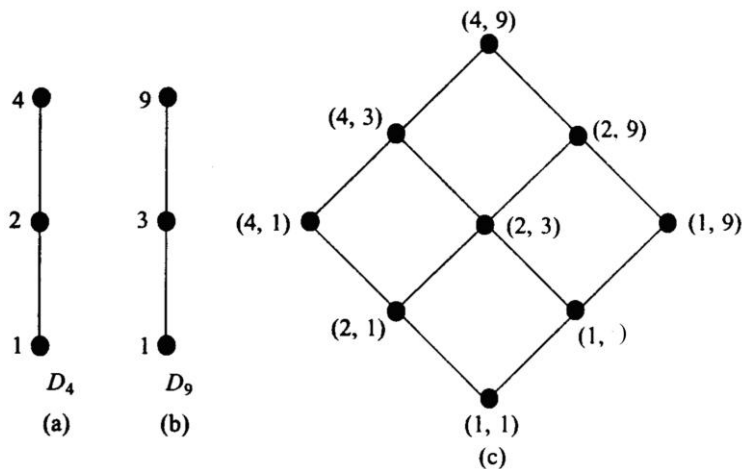


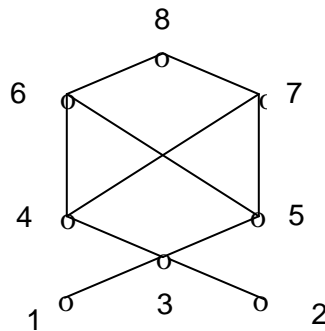
Figure 4.8

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, \geq) can be obtained by rotating the Hasse diagram of the Poset (A, \leq) through 180° .

Self Assessment Questions

3. Let $A = \{1, 2, 3, 4, 5, 6\}$. The relation " \mid " (divides) is a partial order relation on A . Draw the Hasse diagram of (A, \mid) .
4. Consider the partial ordered set $S = \{1, 2, 3, 4, 5, 6, 7, 8\}$ under the relation whose Hasse diagram is 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) $\text{glb } S_1$, $\text{lub } S_1$, $\text{glb } S_2$, $\text{lub } S_2$.

**Figure 4.9****4.4 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 have learnt the interrelations between the algebraic structures, Posets and Lattices and obtained some of their important equivalences. These concepts are the base for the Boolean algebra and logical circuits.

4.5 Terminal Questions

- Determine whether the relation R is a partial ordered on the Z .
 - $a R b \Leftrightarrow a = 2b$
 - $a R b \Leftrightarrow b^2 / a$, where $a, b \in Z$.
- Determine which of the following are equivalence relations and / or partial ordering relations for the given sets
 - $S = \{\text{lines in the plane}\}$; $xRy \Leftrightarrow x$ is parallel to y
 - $N = \{\text{set of natural numbers}\}$; $xRy \Leftrightarrow |x - y| \leq 5$.
- Determine which of the following are partial order?
 - $R_1 = \{(a, b) \in Z \times Z / |a - b| \leq 1\}$ on Z
 - $R_2 = \{(a, b) \in Z \times Z / |a| \leq |b|\}$ on Z
 - $R_3 = \{(a, b) \in Z \times Z / a \text{ divides } b \text{ in } Z\}$ on Z
 - $R_4 = \{(a, b) \in Z \times Z / a - b \leq 0\}$
- Define a relation R on Z , the set of all integers as: $aRb \Leftrightarrow a + b$ is even for all $a, b \in Z$. Is R a partial order relation on Z ?
- Let $A = \{1, 2, 3, 4, 5, 6\}$. The relation “ $|$ ” (divides) is a partial order relation on A . Draw the Hasse diagram of $(A, |)$.
- Let $S = \{a, b, c\}$. Define “ \subseteq ” on $P(S)$, the power set of S as set inclusion. Draw the Hasse diagram for the partially ordered set $(P(S), \subseteq)$.
- Find the atoms in the following lattice,

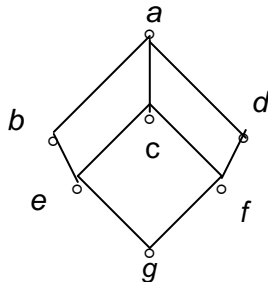


Figure 4.10

- A relation R is symmetric if and only if the relation matrix is _____
- The elements in the level -1 of a Poset are called _____
- Define $x R y \Leftrightarrow |x - y| \leq 5$ for all natural numbers x and y . Then R is _____

4.6 Answers

Self Assessment Questions

- (i) No (ii) No
- (i) It is an equivalence relation, but not partial ordering as R is not antisymmetric.
(ii) Not transitive and so it is neither.

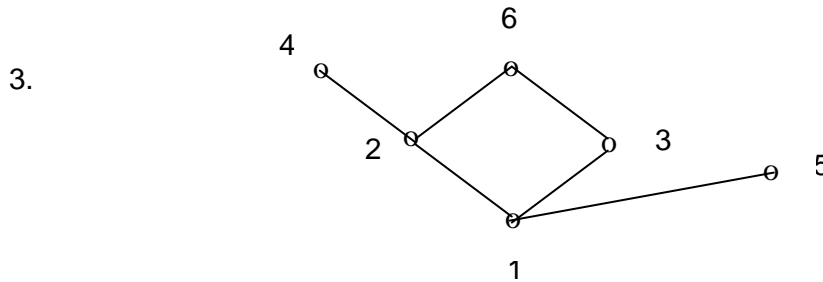


Figure 4.11

- 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.

Terminal Questions

- (i) No (ii) No
- (i) It is an equivalence relation, but not partial ordering as R is not anti-symmetric.
- Not transitive and so it is neither.
- (i) No (ii) No (iii) No (iv) Yes.
- Not a partial order relation. (Reason: $1R3$ (since $1 + 3$ is even), $3R1$ (since $3 + 1$ is even), but $1 \neq 3$).

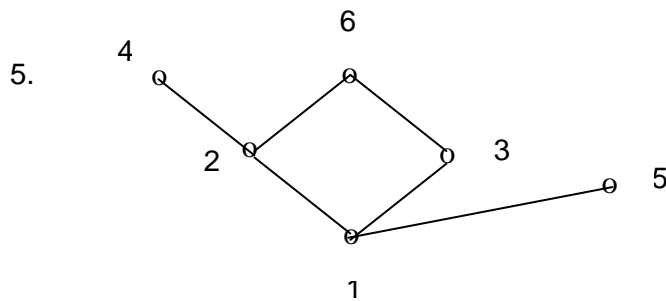


Figure 4.12

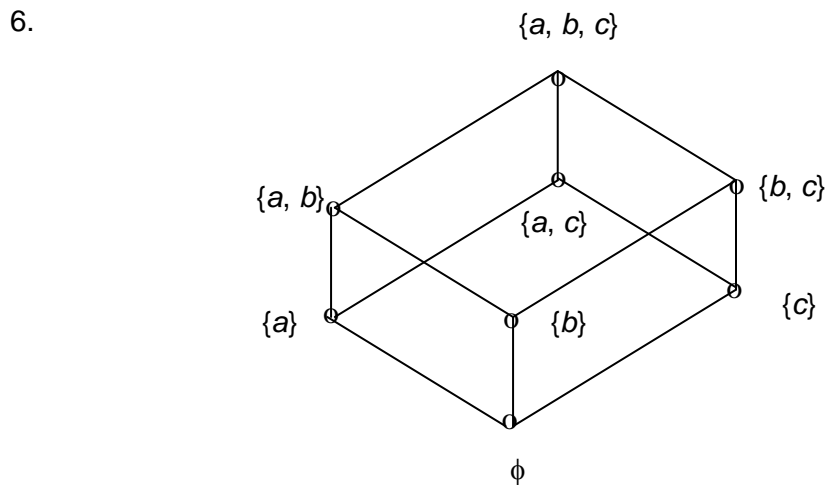


Figure 4.13

- 7. e and f are atoms.
- 8. Symmetric.
- 9. Atoms
- 10. Not partial order and not an equivalence relation.

Unit 5

Lattices

Structure

- 5.1 Introduction
 - Objectives
- 5.2 Definitions and Examples
- 5.3 Properties of Lattices
- 5.4 Bounded and Complemented Lattices
- 5.5 Distributive Lattices
- 5.6 Summary
- 5.7 Terminal Questions
- 5.8 Answers

5.1 Introduction

This unit introduces the algebraic structure defined by a lattice. Properties of lattices will also be discussed here. Lattices with universal lower and upper bounds are considered. Diagram representations of lattices are observed. Two equivalent form of lattices are defined. Some characterizations of complemented and distributive lattices are also obtained. The concepts play important role in logical circuits and Boolean algebras.

Objectives:

At the end of the unit, you would be able to

- explain the structure of a lattice.
- define the properties of lattices.
- draw the lattice diagrams.
- describe bounded and complemented lattice.
- explain distributive and modular lattice and their characterization.

5.2 Definitions and Examples

5.2.1 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 .

5.2.2 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 $A = \{24, 48, 72, \dots\}$. 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 $\sup A = \max A$.

5.2.3 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 $x, y \in L$.

5.2.4 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: $x \leq y \Leftrightarrow \sup(x, y) = y \Leftrightarrow \inf(x, y) = x$.

5.2.5 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).

5.2.6 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 $a \vee b = \text{lcm}\{a, b\}$.

5.2.7 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*.

5.2.8 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.

5.2.9 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 $s_1 \vee s_2 \in S$).

5.2.10 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 $a \wedge b \in S$ for $a, b \in S$.

5.2.11 Example

The lattice (D_n, \leq) is a sublattice of (Z^+, \leq) where \leq is the divisibility relation.

5.2.12 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 $a \in A$.

5.2.13 Example

- (i) Consider $N =$ the set of all natural numbers. Define $a \leq b \Leftrightarrow a$ divides b , for all $a, b \in N$. Then (N, \leq) is a POset. For any $x, y \in N$, we write $x \wedge y = \text{gcd} \{x, y\}$ and $x \vee y = \text{lcm} \{x, y\}$. Then (N, \leq) is a lattice. Here 1 is the zero element. The greatest element does not exist.
- (ii) Let A be a set. Consider $P(A) =$ the power set of A . $(P(A), \subseteq)$ is a POset (where \subseteq is the set inclusion) For any $X, Y \in P(A)$, we write $X \wedge Y = X \cap Y$ and $X \vee Y = X \cup Y$. Then $(P(A), \subseteq)$ is a lattice. In this lattice, ϕ is the smallest element and A is the greatest element.

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.

5.3 Properties of Lattices**5.3.1 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. $x \vee (x \wedge y) = x, x \wedge (x \vee y) = x$ (Absorption)

5.3.2 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 anti-symmetric 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).

5.3.3 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

$$\begin{aligned} a &= a \vee (a \wedge b) && \text{(by absorption law)} \\ &= a \vee b && \text{(supposition)} \end{aligned}$$

Part (ii): Suppose $a \vee b = a$. Now

$$\begin{aligned} b &= b \wedge (b \vee a) && \text{(by absorption)} \\ &= b \wedge (a \vee b) && \text{(by commutative)} \\ &= b \wedge a && \text{(supposition)} \\ &= a \wedge b && \text{(by commutative)} \end{aligned}$$

5.3.4 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 $c \leq d \Rightarrow a \vee c \leq b \vee d$.
- (iv) $a \leq b$ and $c \leq d \Rightarrow a \wedge c \leq b \wedge d$.

Proof:

(i) From the above theorem 5.3.2, we have $a \leq b \Leftrightarrow a \vee b = b$.

$$\begin{aligned} \text{Now } (a \vee c) \vee (b \vee c) &= (a \vee c) \vee (c \vee b) \quad (\text{by commutative}) \\ &= a \vee (c \vee c) \vee b \quad (\text{by associative}) \\ &= a \vee (c \vee b) \quad (\text{by idempotent}) \\ &= (a \vee b) \vee c \\ &= b \vee c. \end{aligned}$$

By theorem 5.3.2, we have $a \vee c \leq b \vee c$.

(ii) Similar

(iii) From the theorem 5.3.2, $a \leq b \Leftrightarrow a \vee b = b$ and $c \leq d \Rightarrow c \vee d = d$.

$$\begin{aligned} \text{Now } (a \vee c) \vee (b \vee d) &= a \vee (c \vee b) \vee d \quad (\text{by associative}) \\ &= a \vee (b \vee c) \vee d \quad (\text{commutative}) \\ &= (a \vee b) \vee (c \vee d) \quad (\text{associative}) \\ &= b \vee d \quad (\text{since } a \leq b \text{ and } c \leq d) \end{aligned}$$

Therefore $a \vee c \leq b \vee d$ (by theorem 5.3.2).

(iv) Similar.

5.3.5 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 $\text{lub}\{a, b\}$ and $\text{glb}\{a, b\}$ exist.
- (ii) (L, \wedge, \vee) be an algebraic system satisfying commutative, associative, absorption and idempotent laws with $a \leq b$ if and only if $a \wedge b = a$.

5.3.6 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: $x \wedge (x \vee y) = x \wedge \sup(x, y)$

$$= \inf(x, \sup(x, y))$$

$$= x. \text{ Also } x \vee (x \wedge y)$$

$$= x \vee \inf(x, y)$$

$$= \sup(x, \inf(x, y))$$

$$= x.$$

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 $y \leq x$

$$\Rightarrow x \wedge y = x \text{ and } y \wedge x = y$$

$$\Rightarrow x = x \wedge y = y \wedge x \text{ (by commutative law)}$$

$$= y$$

$$\Rightarrow x = y.$$

Transitive: Suppose $x \leq y$ and $y \leq z$

$$\Rightarrow x \wedge y = x \text{ and } y \wedge z = y$$

$$\text{Now } x = x \wedge y = x \wedge (y \wedge z)$$

$$= (x \wedge y) \wedge z \text{ (by associative law)}$$

$$= x \wedge z \Rightarrow x = x \wedge z \Rightarrow x \leq z.$$

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 5.3.2, we have that

$$X \leq y \Leftrightarrow x \vee y = y \Leftrightarrow x \wedge y = x \dots (i)$$

$$\text{Let } x, y \in L. \text{ Then } x \wedge (x \vee y) = x \Rightarrow x \leq x \vee y.$$

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 $(x \vee y)$

$$\vee z = x \vee (y \vee z) \text{ (by associative law)}$$

$$= x \vee z \text{ (by (i))}$$

$$= z.$$

This implies $x \vee y \leq z$.

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) and (ii), we conclude that (L, \leq) is a lattice ordered set.

Observation: From the Theorem 5.3.6, 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 $\bigvee_{x \in N} x$ and $\bigwedge_{x \in N} x$ 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 .

5.3.7 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 *dualizing*.

Self Assessment Question

2. The dual of $a \wedge a = a$ is _____
3. The dual of $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ is _____
4. The dual of $a \wedge (a \vee b)$ is _____

5.4 Bounded and Complemented Lattices

5.4.1 Definition

If a lattice L contains the 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*.

5.4.2 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 .

5.4.3 Example

- (i) In the lattice (\mathbb{Z}^+, \leq) with \leq means usual \leq is not a bounded lattice as 1 is the least element and there is no greatest element.

5.4.4 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 $1 \vee x = 1$.

5.4.5 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.

5.4.6 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 .

5.4.7 Example

- (i) Let $L = P(M)$. 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.

5.4.8 Example

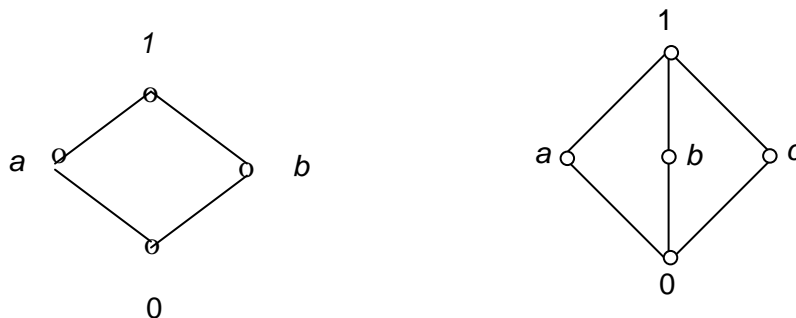
- (i) In a bounded lattice, 1 is a complement of 0, and 0 is a complement of 1.
- (ii) Every chain with more than two elements is not a complemented lattice.
- (iii) The complement need not be unique. For example, in the diamond lattice, both the two elements b and c , are complements for the element a .

5.4.9 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 Questions

2. The dual of $a \wedge a = a$ is _____
3. The dual of $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ is _____
4. The dual of $a \wedge (a \vee b)$ is _____
5. Verify whether the lattice (\mathbb{Z}^+, \leq) with \leq defined as $a \leq b \Leftrightarrow a \mid b$ is a bounded lattice.
6. In the lattice given below write complements of a , b , and c .

**Figure 5.1**

7. Find the atoms in the following lattice.

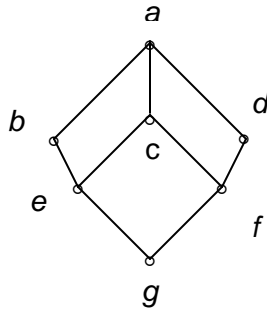


Figure 5.2

5.5 Distributive Lattices

5.5.1 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**.

5.5.2 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 is called as *diamond lattice*.

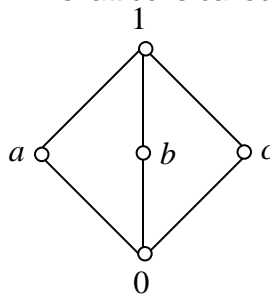


Figure 5.3

5.5.3 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

$$b \vee (a \wedge c) = (b \vee c) \wedge c$$

$$\Rightarrow b \vee 0 = 1 \wedge c$$

$$\Rightarrow b = c, \text{ a contradiction.}$$

Hence L_2 is not a modular lattice.

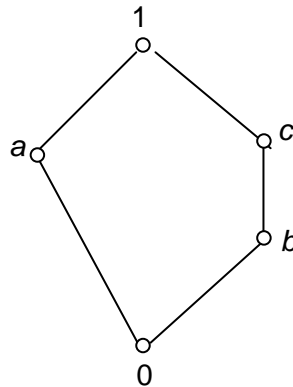


Figure 5.4

5.5.4 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**.

5.5.5 Example

- (i) For any set X , the lattice $(P(X), \cup, \cap)$ is a distributive lattice.
- (ii) Every chain is a distributive lattice.

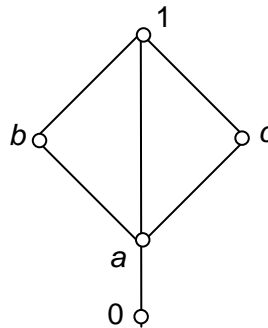


Figure 5.5

(iii) Consider the lattice given by the diagram

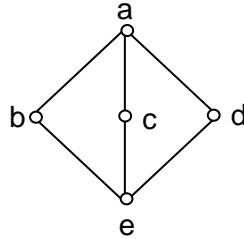


Figure 5.6

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.

5.5.6 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, $a \vee b = 1$, $a \wedge b = 0$, $a \vee c = 1$, $a \wedge c = 0$.

$$\begin{aligned}
 \text{We have } b &= b \wedge 1 && \text{(since 1 is the universal upper bound)} \\
 &= b \wedge (a \vee c) && \text{(since } a \vee c = 1\text{)} \\
 &= (b \wedge a) \vee (b \wedge c) && \text{(by the distributive law)} \\
 &= (a \wedge b) \vee (b \wedge c) && \text{(since } \wedge \text{ is commutative)} \\
 &= 0 \vee (b \wedge c) && \text{(since } a \wedge b = 0\text{)} \\
 &= (a \wedge c) \vee (b \wedge c) && \text{(since } a \wedge c = 0\text{)} \\
 &= (a \vee b) \wedge c && \text{(by distributive law)} \\
 &= 1 \wedge c && \text{(since } a \vee b = 1\text{)} \\
 &= c && \text{(since 1 is the universal upper bound).}
 \end{aligned}$$

Therefore, the complement is unique.

5.5.7 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) \Rightarrow (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) \Rightarrow (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) \Rightarrow (i): Suppose that $a \leq c$. Then $a \wedge b \leq c \wedge b \Rightarrow (a \wedge b) \vee (c \wedge b) = (c \wedge b) \dots$

$$\begin{aligned} \text{(A) Also } a \vee c = c. \text{ Now } (a \wedge c) \vee (b \wedge c) &= (a \wedge c) \vee [(a \wedge b) \vee (c \wedge b)] \\ &= (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \\ &= (a \vee b) \wedge (b \vee c) \wedge (c \vee a) && \text{(by (iii))} \\ &= (a \vee b) \wedge (b \vee c) \wedge c && \text{(since } a \leq c) \\ &= (a \vee b) \wedge c && \text{(by absorption law).} \end{aligned}$$

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.

5.5.8 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.

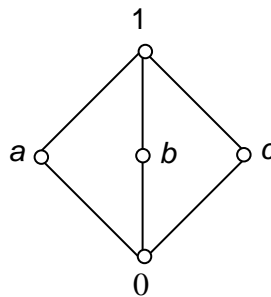


Figure 5.7

5.5.9 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

$$\begin{aligned}
 (x \wedge y) \vee (x \wedge z) &= [(x \wedge y) \vee x] \wedge [(x \wedge y) \vee z] \text{ (by (i))} \\
 &= x \wedge [(x \wedge y) \vee z] \text{ (by commutative and absorption laws)} \\
 &= x \wedge [z \vee (x \wedge y)] \text{ (by commutative law)} \\
 &= x \wedge [(z \vee x) \wedge (z \wedge y)] \text{ (by (i))} \\
 &= [x \wedge (z \vee x)] \wedge [z \wedge y] \text{ (by associative law)} \\
 &= x \wedge (z \wedge y) \text{ (by commutative and absorption law)}
 \end{aligned}$$

Other part is similar.

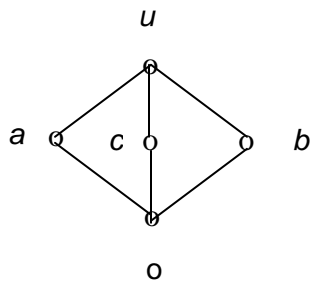
5.6 Summary

In this unit, we discussed the algebraic structure defined as a lattice. Properties of lattices were discussed. Diagrammatic representations of lattices are observed. Some characterizations of complemented and distributive lattices are studied. The concepts are useful in logical circuits and Boolean algebras.

5.7 Terminal Questions

1. Verify whether the following are modular lattices.

(i)



(ii)

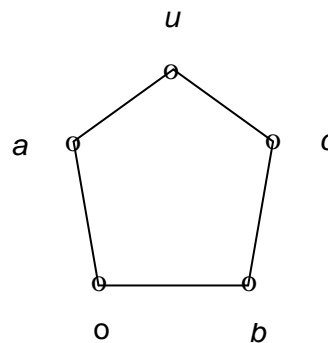


Figure 5.8

2. Consider the lattice $A = \{0, a_1, a_2, a_3, a_4, a_5, 1\}$ given below.

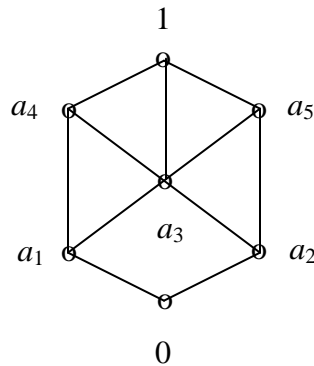


Figure 5.9

- (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.

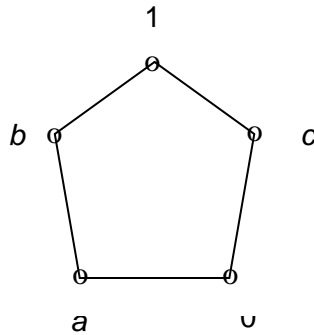


Figure 5.10

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 $a, b, c, d \in L$,
- $a \leq b \Rightarrow a \vee c \leq b \vee c$
 - $a \leq b \Rightarrow a \wedge c \leq b \wedge c$
 - $a \leq b$ and $c \leq d \Rightarrow a \vee c \leq b \vee d$
 - $a \leq b$ 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.

5.8 Answers**Self Assessment Questions**

1. This is a lattice.
2. $a \vee a = a$
3. $a \vee (b \vee c) = (a \vee b) \vee c$
4. $a \vee (a \wedge b)$
5. This is not a bounded lattice, since there is no greatest element.
6. Complements of a are b and c
Complements of b are a and c
Complements of c are a and b .
7. The atoms are e and f .

Unit 6

Algebraic Structures

Structure

- 6.1 Introduction
 - Objectives
- 6.2 Semigroups
- 6.3 Monoids
- 6.4 Groups
- 6.5 Permutation Groups
- 6.6 Summary
- 6.7 Terminal Questions
- 6.8 Answers

6.1 Introduction

In this unit, 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 will also deal with the special kind of groups namely, permutation groups.

Objectives:

At the end of the unit, you would be able to

- describe the algebraic systems with one binary operation.
- generalize the structure of semigroup to a monoid.
- explain the structure of a group and its substructures.
- explain the permutations groups.

6.2 Semigroups

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 “ $*$, \circ , \square , $+$, \cdot ” etc.

In this section, we will consider a set with one binary operation. This has several applications in the theory of finite state machines, Automata theory etc.

6.2.1 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 $a, b, c \in S$.

6.2.2 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.
- iii) For any $2, 3, 4 \in Z^+$, $2 * 3 = 2^2 + 3 = 4 + 3 = 7$, $(2 * 3) * 4 = 7 * 4 = 49 + 4 = 53$.

Where $2 * (3 * 4) = 17$. Therefore ‘ $*$ ’ on Z^+ is not associative.

6.2.3 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 $a, b, c \in A$.

6.2.4 Example

- i) Take $A = \{a_1, a_2, \dots, a_n\}$ 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 $\alpha = a_1 a_2 \dots a_n$ and $\beta = b_1 b_2 \dots b_k$, then $\alpha.\beta = a_1 a_2 \dots a_n b_1 b_2 \dots b_k$. It can be verified that for any α, β and γ of A^* , $\alpha.(\beta.\gamma) = (\alpha.\beta).\gamma$. Therefore, $(A^*, .)$ is a semi group.

- ii) 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.
- iii) The set Z (the set of integers) with the binary operation subtraction is not a semigroup, since subtraction is not associative.

6.2.5 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.

6.2.6 Example

Test whether the set 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 $(Z, *)$ is NOT a semigroup.

6.2.7 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 $(S, *)$.

6.2.8 Definition

Let $(S, *)$ and (S^1, \circ) be two semigroups. A function $f: S \rightarrow S^1$ is called an **isomorphism** from $(S, *)$ to (S^1, \circ) 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)

6.2.9 Result

If f is an isomorphism from $(S, *)$ to (S^1, \circ) , then f^{-1} is an isomorphism from (S^1, \circ) 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 $f^{-1}(a^1 \circ b^1) = f^{-1}(f(a) \circ f(b)) = f^{-1}(f(a * b))$ (Since f is homomorphism)

$$\begin{aligned} &= (f^{-1} \circ f)(a * b) \\ &= a * b \\ &= f^{-1}(a^1) * f^{-1}(b^1). \end{aligned}$$

Therefore, f^{-1} is an isomorphism.

6.2.10 Problem

Show that the semigroups $(\mathbb{Z}, +)$ and $(T, +)$ where T is the set of all even integers, are isomorphic.

Solution: Define $f: \mathbb{Z} \rightarrow T$ 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 $b \in T$. Then b is an even integer. Write $a = \frac{b}{2} \in \mathbb{Z}$.

$$\text{Now } f(a) = f\left(\frac{b}{2}\right) = 2\left(\frac{b}{2}\right) = b.$$

Therefore, f is one-one and onto.

f is homomorphism: Let $m, n \in \mathbb{Z}$.

$$f(m + n) = 2(m + n) = 2m + 2n = f(m) + f(n).$$

Therefore, f is a homomorphism and hence $(\mathbb{Z}, +)$ and $(T, +)$ are isomorphic.

6.2.11 Note

If $(S, *)$ and (S^1, o) are semigroups such that S has an identity and S^1 does not have identity, then $(S, *)$ and (S^1, o) cannot be isomorphic.

6.2.12 Definition

An equivalence relation ' R ' on the semigroup $(S, *)$ is called a ***congruence relation*** if aRa^1 and bRb^1 imply $(a * b) R (a^1 * b^1)$.

6.2.13 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 $2 \mid a - b$.

Now $a \equiv b \pmod{2}$ and $c \equiv d \pmod{2} \Rightarrow 2 \mid a - b$ and $2 \mid c - d$.

$\Rightarrow a - b = 2m, c - d = 2n$, where $m, n \in \mathbb{Z}$

Adding $(a - b) + (c - d) = 2(m + n) \Rightarrow (a + c) - (b + d) = 2(m + n)$.

This shows that the relation is a congruence relation.

6.2.14 Example

Consider the semigroup $(\mathbb{Z}, +)$ where '+' is the ordinary addition.

Let $f(x) = x^2 - x - 2$. Define a relation R on \mathbb{Z} by $a R b \Leftrightarrow f(a) = f(b)$.

Reflexive: aRa

Symmetric: $aRb \Leftrightarrow f(a) = f(b) \Leftrightarrow bRa$

Transitive: aRb and $bRc \Leftrightarrow f(a) = f(b)$ and $f(b) = f(c)$

$\Leftrightarrow f(a) = f(c) \Leftrightarrow aRc$

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 $f(5) = 8$.

6.2.15 Theorem

If $(S, *)$ and (T, \circ) are semigroups, then $(S \times T, \oplus)$ is a semigroup, where \oplus defined by $(s_1, t_1) \oplus (s_2, t_2) = (s_1 * s_2, t_1 \circ t_2)$.

6.2.16 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 $S/R = \{[a] / a \in S\}$.

6.2.17 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.

$$\text{Now } [a] \otimes ([b] \otimes [c]) = [a] \otimes [b * c]$$

$$= [a * (b * c)] = [(a * b) * c] \quad (\text{by associativity of } *)$$

$$= [a * b] \otimes [c] = ([a] \otimes [b]) \otimes [c].$$

Therefore, \otimes satisfies associative property. Hence S/R is a semigroup.

6.2.18 Definition

The semigroup S/R verified above is called the **quotient semigroup** or

factor semigroup.

6.2.19 Example

Observation: $a \equiv b \pmod{n} \Rightarrow a = qn + r$ and $b = tn + r$ for some $q, t, r \in \mathbb{Z}$
 $\Rightarrow a - b$ is a multiple of n . That is, $n \mid a - b$.

Take a semigroup $(\mathbb{Z}, +)$. Define a relation 'R' on \mathbb{Z} as 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 $a \equiv b \pmod{n}$

$$\begin{aligned} &\Leftrightarrow n \mid a - b \\ &\Leftrightarrow n \mid -(a - b) \\ &\Leftrightarrow n \mid b - a \\ &\Leftrightarrow b \equiv a \pmod{n}. \end{aligned}$$

Therefore, $aRb \Rightarrow bRa$.

Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

Then $n \mid a - b$ and $n \mid b - c \Rightarrow n \mid (a - b) + (b - c) \Rightarrow n \mid a - c$.

This implies $a \equiv c \pmod{n}$.

Therefore $aRb, bRc \Rightarrow aRc$. So R is an equivalence relation.

Take $n = 4$. The equivalence classes determined by the congruence relation $\equiv \pmod{4}$ on \mathbb{Z} . (It is denoted by \mathbb{Z}_4).

$$[0] = \{\dots - 8, -4, 0, 4, 8, 12, \dots\} = [4] = [8] = \dots$$

$$[1] = \{\dots - 7, -3, 1, 5, 9, 13, \dots\} = [5] = [9] = \dots$$

$$[2] = \{\dots - 6, -2, 2, 6, 10, 14, \dots\} = [6] = [10] = \dots$$

$$[3] = \{\dots - 5, -1, 3, 7, 11, 15, \dots\} = [7] = [11] = \dots$$

Define \oplus on \mathbb{Z}_4 as follows:

\oplus	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]

$$[3] \mid [3] \quad [0] \quad [1] \quad [2]$$

In general, $[a] \oplus [b] = [a + b]$. Thus \mathbb{Z}_n has the 'n' equivalence classes $[0], [1], [2], \dots, [n-1]$ 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 $(S/R, \otimes)$, where R is a congruence relation on $(S, *)$.

6.2.20 Theorem

Let R be congruence relation on a semigroup $(S, *)$ and let $(S/R, \otimes)$ be the corresponding quotient semigroup. Then the function $f_R: S \rightarrow S/R$ 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.

$$\begin{aligned} \text{Let } a, b \in S, \text{ then } f_R(a * b) &= [a * b] \\ &= [a] \otimes [b] \\ &= f_R(a) \otimes f_R(b). \end{aligned}$$

Therefore, f_R is a homomorphism.

6.2.21 Fundamental Theorem of homomorphism

Let $f: S \rightarrow T$ be a homomorphism of the semigroup $(S, *)$ onto the semigroup (T, \circ) . Let R be the relation on S defined by $aRb \Leftrightarrow f(a) = f(b)$ for a and b in S . Then (i) R is a congruence relation; (ii). (T, \circ) and the quotient semigroup $(S/R, \otimes)$ are isomorphic.

6.3 Monoids

6.3.1 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.

6.3.2 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 right identity.

6.3.3 Definition

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

6.3.4 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.

6.3.5 Definition

Let $(A, *)$ be an algebraic system, where $*$ is a binary operation on A . $(A, *)$ is called a **monoid** if the following conditions are satisfied:

i) $*$ is a closed operation

- ii) $*$ is an associative operation
- iii) existence of identity.

6.3.6 Example

Let X be a non empty set. Write $X^X = \{f / f: X \rightarrow X\}$. Let 'o' denote the operation of composition of mappings. That is, $(f \circ g)(x) = f(g(x))$ 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 $(g \circ f)(x) = g(f(x)) = g(x) = f(g(x)) = (f \circ g)(x)$ for all $g \in X^X$. Therefore, (X^X, o) is a monoid.

6.3.7 Example

- i) For any set S , $(\wp(S), \cup)$ where $\wp(S)$ is a power set of S , is a commutative semigroup. It is also a monoid with the empty set ϕ as 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.

6.3.8 Example

Let T be the set of even integers. Then (T, \cdot) is a subsemigroup of the monoid (\mathbb{Z}, \cdot) where " \cdot " is usual multiplication. But (T, \cdot) is not a submonoid, since the identity $1 \notin T$.

6.3.9 Example

- i) Suppose $(S, *)$ is a semigroup, and let $a \in S$. For any $n \in \mathbb{Z}^+$, we

define the integral powers of a^n recursively as follows:

$$a^1 = a, a^n = a^{n-1} * a, n \geq 2. \text{ Write } T = \{a^n / n \in \mathbb{Z}^+\}.$$

Then $(T, *)$ is a subsemigroup of $(S, *)$.

ii) Let $(S, *)$ be a monoid and $a \in S$.

Define $a^0 = e, a^1 = a, a^n = a^{n-1} * a, n \geq 2$ (as in (i))

Write $T^1 = \{a^n / n \in \mathbb{Z}^+, \cup \{0\}\}$. Then $(T^1, *)$ is a submonoid of $(S, *)$.

Self Assessment Questions

- Let E be the set of all even integers. Show that the semigroups $(\mathbb{Z}, +)$ and $(E, +)$ are isomorphic.
- Let $A = \{x, y\}$. Which of the following tables define a semigroup on A ? Which define a monoid on A ?

(i)

*	x	y
x	x	y
y	x	x

(ii)

*	x	y
X	x	y
y	y	y

- Determine whether $(\mathbb{Z}^+, *)$ where $a*b = a$ is a semigroup?
- Check whether $(\mathbb{Z}^+, *)$ where $a*b = \max\{a, b\}$, a semigroup or monoid?
- Let $S = \{a, b\}$. Write the operation table for the semigroups S . Is the semigroup commutative?
- Let $A = \{a, b, c\}$ and consider the semigroup (A^*, \cdot) where \cdot is the operation of catenation. If $\alpha = abac, \beta = cba$ and $\gamma = babc$, compute
 (i) $(\alpha\beta).\gamma$ (ii) $\gamma.(\alpha.\alpha)$ (iii) $(\gamma.\beta).\alpha$.

6.4 Groups

In this section we study the important algebraic object known as group, which serves 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 and chemistry. Some of exciting applications of group theory have arisen in fields such as Particle Physics, and Binary Codes.

6.4.1 Definition

Let us 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 $*$, \cdot , \circ etc.

6.4.2 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 $a*b = e = b*a$.

6.4.3 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 .

6.4.4 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 $a, b \in G$.

6.4.5 Example

Take $G = \{-1, 1\}$. Then $(G, .)$ is a commutative group *w. r. t.* the usual multiplication of numbers.

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.

.	-1	+1
-1	1	-1
1	-1	1

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.

6.4.6 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 $O(G)$.

6.4.7 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 $O(G) = 2$.

6.4.8 Lemma

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 .

$$\begin{aligned} \text{Now } a_1 &= a_1.e && \text{(since } e \text{ is the identity)} \\ &= a_1.(a.a_2) && \text{(since } a_2 \text{ is the inverse of } a) \\ &= (a_1.a).a_2 && \text{(by associativity)} \\ &= e.a_2 && \text{(since } a_1 \text{ is the inverse of } a) \\ &= a_2. \end{aligned}$$

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

6.4.9 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 operation o in G .

6.4.10 Lemma

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) and (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, \cdot) is a subgroup of (G, \cdot) .

6.4.11 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 $a^3 \in H, \dots, a^m \in H, \dots$

Therefore, $H \supseteq \{a, a^2, \dots\}$.

Since H is finite, we have that there must be repetitions in a, a^2, \dots

Therefore, there exist integers r, s with $r > s > 0$ such that $a^r = a^s$

$$\Rightarrow a^r \cdot a^{-s} = a^0$$

$$\Rightarrow a^{r-s} = e \Rightarrow e \in H \text{ (since } r-s > 0 \text{ and } a \in H \Rightarrow a^{r-s} \in H \text{)}.$$

Since $r-s-1 \geq 0$, we have $a^{r-s-1} \in H$ and $a \cdot a^{r-s-1} = a^{r-s} = e \in H$.

Therefore a^{r-s-1} acts as the inverse of $a \in H$. Hence H is a subgroup.

6.4.12 Example

Consider $G = \mathbb{Z}$, the group of integers with respect to addition. Write

$H = \{5x \mid x \in G\}$. 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 .

6.4.13 Problem

Let G be a group, $a \in G$. Then $\langle a \rangle = \{a^i \mid i = 0, \pm 1, \dots\}$ is a subgroup of G .

Solution: Let $x, y \in \langle a \rangle \Rightarrow x = a^i$ and $y = a^j$ for some $i, j \in \mathbb{Z}$. Now
 $x \cdot y = a^i \cdot a^j = a^{i+j} \in \langle a \rangle$ (since $i+j \in \mathbb{Z}$).

Also $x^{-1} = (a^i)^{-1} = a^{-i} \in \langle a \rangle$ (since $a^i \cdot a^{-i} = a^{i-i} = a^0 = e \Rightarrow (a^i)^{-1} = a^{-i}$).

Therefore, $x, y \in \langle a \rangle \Rightarrow x \cdot y \in \langle a \rangle$ and $x^{-1} \in \langle a \rangle$. Hence $\langle a \rangle$ is a subgroup of G .

6.4.14 Definition

- i) Let G be a group and $a \in G$. Then $\langle a \rangle = \{a^i \mid i = 0, \pm 1, \dots\}$ is called the **cyclic subgroup** generated by the element $a \in G$.
- ii) G is said to be a **cyclic group** if there exists an element $a \in G$ such that $G = \langle a \rangle$.
- iii) Let G be a group, H be a subgroup of G , $a, b \in G$. We say that a is **congruent to b (mod H)**, written as $a \equiv b \pmod{H}$ if $a b^{-1} \in H$. The relation $a \equiv b \pmod{H}$ is an equivalence relation.
- iv) If H is a subgroup of G and $a \in G$, then write $Ha = \{ha \mid h \in H\}$ is called the **right coset** of H in G . $aH = \{ah \mid h \in H\}$ is called the **left coset**.

6.4.15 Example

- i) Consider the group $Z_6 = \{0, 1, 2, 3, 4, 5\}$. Then $H = \{0, 3\}$ is a subgroup of G . The left cosets of the subgroup H in Z_6 are:
 $\{H = \{0, 3\}, 1 + H = \{1, 4\}, 2 + H = \{2, 5\}\}$.
- ii) Let $G =$ the additive group of integers. Let $H = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$. Then H is a subgroup of G . We have $1 \in G$, $1 + H = \{\dots, -8, -5, -2,$

$1, 4, 7, \dots\}$ and $2 \in G$, $2 + H = \{-7, -4, -1, 2, 5, 8, 11, \dots\}$. The sets H , $1 + H$, $2 + H$ are all distinct right cosets of H in G .

6.4.16 Properties of Cosets

Let H be a subgroup of G and $a, b \in G$. Then,

- i) $a \in aH$
- ii) $aH = H$ if and only if $a \in H$
- iii) $aH = bH$ or $aH \cap bH = \phi$
- iv) $aH = bH$ if and only if $a^{-1}b \in H$.

Analogous properties hold for right cosets.

6.4.17 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 $\phi: Ha \rightarrow Hb$ by $\phi(ha) = hb$ for all $ha \in Ha$.

ϕ is one-one: Let $h_1a, h_2a \in Ha$ such that $\phi(h_1a) = \phi(h_2a)$

$$\Rightarrow h_1b = h_2b$$

$$\Rightarrow h_1 = h_2 \quad (\text{by cancellation Law})$$

$$\Rightarrow h_1a = h_2a.$$

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.

6.4.18 Note

Since $H = He$ we have that H is also a right coset of H in G and by the

problem 6.4.17, any right coset of H in G have $O(H)$ elements.

6.4.19 Lagrange's Theorem

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, \dots, Ha_k are only distinct right coset of H in G

$$\Rightarrow G = Ha_1 \cup Ha_2 \cup \dots \cup Ha_k$$

$$\Rightarrow O(G) = O(Ha_1) + O(Ha_2) + \dots + O(Ha_k)$$

$$= O(H) + O(H) + \dots + O(H) \text{ (k times)}$$

(since every right coset has $O(H)$ elements)

$$\Rightarrow O(G) = k \cdot O(H)$$

$$\Rightarrow n = k \cdot m \Rightarrow (n/m) = k.$$

Hence $O(H)$ divides $O(G)$.

6.4.20 Note

Converse of the Lagrange's 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.

6.4.21 Example

Consider the symmetric group S_4 . We know that $S_4 = \{f : A \rightarrow A / f \text{ is a bijection and } A = \{1, 2, 3, 4\}\}$. 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 cannot form a subgroup. Therefore, $6 \mid O(A_4)$ but A_4 contains no subgroup of order 6. (refer the section: Permutation Groups).

6.4.22 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 $i(H)$.
- ii) If G is a group and $a \in G$, then the *order* of ' a ' is defined as the least positive integer m such that $a^m = e$.

6.4.23 Definition

If there is no positive integer n such that $a^n = e$ then ' a ' is said to be of ***infinite order***.

6.4.24 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 $g \in G$.

6.4.25 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 $\phi(ab) = \phi(a) \cdot \phi(b)$.
- ii) If ϕ is a homomorphism of G into G^1 , then the ***kernal*** of ϕ (denoted by $\ker \phi$) is defined by

$$\ker \phi = \{x \in G / \phi(x) = e^1, \text{ where } e^1 \text{ is the identity in } G^1\}.$$

6.4.26 Example

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 $\phi: (G, +) \rightarrow (G^1, \cdot)$ by $\phi(a) = 2^a$. Now consider

$$\phi(a + b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b).$$

Therefore, ϕ is a homomorphism.

6.4.27 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 $\phi(x) = \phi(x) \cdot e^1$ and $\phi(x) = \phi(xe) = \phi(x) \cdot \phi(e)$ (since ϕ is homo.).

Therefore $\phi(x) \cdot e^1 = \phi(x) \cdot \phi(e)$

$\Rightarrow e^1 = \phi(e)$ (by cancellation laws).

ii) By (i), $e^1 = \phi(e) = \phi(xx^{-1}) = \phi(x) \cdot \phi(x^{-1})$

$\phi(x^{-1})$ is the inverse of $\phi(x)$.

That is $\phi(x^{-1}) = [\phi(x)]^{-1}$. This is true for all $x \in G$.

6.4.28 Problem

If ϕ is a homomorphism of G into G^1 with kernel 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 $\phi(y) = e^1$

$\Rightarrow \phi(xy) = \phi(x) \cdot \phi(y)$ (since ϕ is homomorphism)

$$= e^1 \cdot e^1 = e^1$$

$\Rightarrow xy \in K$. This proves the closure axiom.

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 $g \in G, k \in K$.

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1})$$

$$= \phi(g) \cdot e^1 \cdot \phi(g^{-1}) \quad (\text{since } k \in K \Rightarrow \phi(k) = e^1)$$

$$= \phi(g) \cdot \phi(g^{-1}) = \phi(g) \cdot [\phi(g)]^{-1} = e^1$$

$\Rightarrow \phi(gkg^{-1}) = e^1 \Rightarrow gkg^{-1} \in K$. Hence K is a normal subgroup of G .

6.4.29 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 $f: G/K \rightarrow G^1$ by $f(Ka) = \phi(a)$ for all $Ka \in G/K$.

f is well defined: Let $a, b \in G$ and $Ka = Kb$

$$\begin{aligned} &\Rightarrow ab^{-1} \in K \\ &\Rightarrow \phi(ab^{-1}) = e^1 \\ &\Rightarrow \phi(a) \cdot [\phi(b)]^{-1} = e^1 \\ &\Rightarrow \phi(a) = \phi(b) \\ &\Rightarrow f(Ka) = f(Kb). \end{aligned}$$

f is 1-1: Suppose $f(Ka) = f(Kb)$

$$\begin{aligned} &\Rightarrow \phi(a) = \phi(b) \\ &\Rightarrow \phi(a) \cdot [\phi(b)]^{-1} = e^1 \\ &\Rightarrow \phi(a) \cdot \phi(b^{-1}) = e^1 \\ &\Rightarrow \phi(ab^{-1}) = e^1 \\ &\Rightarrow ab^{-1} \in K \\ &\Rightarrow Ka = Kb. \end{aligned}$$

Therefore f is 1-1.

f is onto: Let $y \in G^1$. Since $\phi: G \rightarrow G^1$ 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 $Ka, Kb \in G/K$.

$$\begin{aligned} f(Ka.Kb) &= f(Kab) \\ &= \phi(ab) = \phi(a) \cdot \phi(b) \text{ (since } \phi \text{ is homomorphism)} \\ &= f(Ka) \cdot f(Kb). \end{aligned}$$

Therefore, f is a homomorphism.

Hence $f: G/K \rightarrow G^1$ is an isomorphism.

Self Assessment Questions

7. Give an example of abelian group of 2×2 matrices over real numbers with respect to multiplication.
8. Consider the group $(\mathbb{Z}, +)$. Let $H = \{3n \mid n \in \mathbb{Z}\}$. Show that the set H is a subgroup of \mathbb{Z} .
9. Prove that $(G, +_6)$ is cyclic where $G = \{0, 1, 2, 3, 4, 5\}$.
10. If $*$ is a binary operation in \mathbb{Q}^+ defined by
 - (i) $a * b = \frac{ab}{3}$
 - (ii) $a * b = \frac{ab}{2}$
 where $a, b \in \mathbb{Q}^+$ (set of all positive rationals). Show that $(\mathbb{Q}^+, *)$ is an abelian group.
11. Examine which of the following are groups. For those which fail to be groups mention which group axioms 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 $a * b = a + b + 1$, $a, b \in \mathbb{Z}$.
 - iii) $G = \mathbb{R}$, $a * b = a + b - ab$ for all $a, b \in \mathbb{R}$.

6.5 Permutation Groups

6.5.1 Definition

If the set S contains n elements, then the group

$$A(S) = \{f: S \rightarrow S \mid f \text{ is a one-one and onto function}\}$$

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.

6.5.2 Example

If $S = \{x_1, x_2, x_3, x_4\}$ and $\phi \in A(S)$ by $\phi(x_1) = x_2, \phi(x_2) = x_4, \phi(x_3) = x_1, \phi(x_4) = x_3$.

$(x_4) = x_3$ 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 $x \in S$.

6.5.3 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 $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$.

6.5.4 Definition

A permutation $\sigma \in S_n$ is a *cycle* of length k if there exists elements $a_1, a_2, \dots, a_k \in S$ such that $\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_k) = a_1$ and $\sigma(x) = x$ for all other elements $x \in S$. We will write (a_1, a_2, \dots, a_k) to denote the cycle σ . Cycles are the building blocks of the permutations.

6.5.5 Example

The permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$ is a cycle of length 6,

whereas $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (243)$ is a cycle of length 3. Also, not every

permutation is a cycle. Consider the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56)$.

Example: Compute the product of cycles $\sigma = (1352), \tau = (256)$.

Solution: $\sigma\tau = (1356)$.

6.5.6 Note

Two cycle (a_1, a_2, \dots, a_k) and (b_1, b_2, \dots, b_k) are said to be disjoint if $a_i \neq b_j$ for all i and j .

For instance, the cycles (135) and (27) are disjoint; however, the cycles (135) and (347) are not. Calculating their products, we find that

$$(135)(27) = (135)(27)$$

$$(135)(347) = (13475).$$

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 $(a_1, a_2, \dots, a_n) = (a_1 a_n) (a_1 a_{n-1}) \dots (a_1 a_3) (a_1 a_2)$, any cycle can be written as the product of transpositions.

6.5.7 Definition

- i) A permutation is said to be an **odd permutation** if it is the product of an odd number of transpositions (or 2- cycles).
- ii) A permutation is said to be an **even permutation** if it is the product of an even number of transpositions (or 2 – cycles).

6.5.8 Example

Consider the permutation $(16)(253) = (16)(23)(25) = (16)(45)(23)(45)(25)$. 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 $(12)(21)$, as $(13)(24)(13)(24)$, 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 (16) by $(23)(16)(23)$ or by $(35)(16)(13)(16)(13)(35)(56)$ but (16) will always be the product of an odd

number of transpositions.

6.5.9 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.

Self Assessment Questions

12. 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) $(1\ 3)(1\ 2\ 4)(1\ 5\ 3)$

6.6 Summary

The algebraic structures with one binary operation were discussed. Some important characterizations of the algebraic systems Semigroups, Monoid and Groups were given. Interrelations between these were obtained. A special kind of set of one-to-one mappings, referred as permutation groups, which are the central to the study of the Geometric symmetries and to Galois Theory were discussed. These also provide abundant examples of nonabelian groups.

6.7 Terminal Questions

1. Find the inverse of each of the following permutations

$$(i) \begin{pmatrix} 1234 \\ 1342 \end{pmatrix} \quad (ii) \begin{pmatrix} 12345 \\ 23154 \end{pmatrix} \quad (iii) \begin{pmatrix} 1234 \\ 3412 \end{pmatrix}$$

2. Express each of the following as a product of transpositions and hence determine whether it is odd or even.

$$(i) \begin{pmatrix} 123 \\ 213 \end{pmatrix} \quad (ii) \begin{pmatrix} 123 \\ 321 \end{pmatrix} \quad (iii) \begin{pmatrix} 1234 \\ 4321 \end{pmatrix}$$

3. If G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, then show that G is abelian.
4. In the following, determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.
- The set of all integers. Operation: $aob = a - b$.
 - The set of all positive integers. Operation: $aob = a.b$.
 - $\{a_0, a_1, \dots, a_6\}$ where $a_ia_j = a_{i+j}$ if $i + j < 7$ and $a_ia_j = a_{i+j-7}$ (that is, if $i + j \geq 7$).
 - The set of all rational numbers with odd denominators. Operation: $aob = a + b$.

5. If a group G has only three elements, show that it must be abelian.

6. Let G be the set of all real 2×2 – matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ where $ad \neq 0$.

Prove that G forms a group under matrix multiplication. Is G is abelian?

Q.7-8: State whether True/False.

- The set Z (set of integers) with the operation 'addition' is commutative.
- The set R (real numbers) is commutative with the operation 'addition'.
- The number of elements in the symmetric group of order 3 is _____

6.8 Answers

Self Assessment Questions

1. Define $f: \mathbb{Z} \rightarrow E$ by $f(a) = 2a$. Suppose that $f(a_1) = f(a_2)$. Then $2a_1 = 2a_2$ and so $a_1 = a_2$. Therefore, f is one-to-one. For any even integer b , take $a = \frac{b}{2} \in \mathbb{Z}$ and $f(a) = f(\frac{b}{2}) = 2(\frac{b}{2}) = b$. Therefore, f is onto.

Also $f(a+b) = 2(a+b) = 2a+2b = f(a)+f(b)$. Therefore f is homomorphism and hence f is an isomorphism.

2. Semigroup (ii) Monoid (ii)
 3. Yes
 4. Monoid: (identity).
 5. 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, Since $f_1 \circ f_3 \neq f_3 \circ f_1$

\circ	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

6. (i) $abaccbababc$, (ii) $babcabacabac$, (iii) $babccbaabac$

7. 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:

\cdot	A	B	C	D
A	A	B	C	D
B	B	A	D	C

C	C	D	A	B
D	D	C	B	A

8. H is nonempty. For $x, y \in H$, then there exist $p, q \in \mathbb{Z}$ such that $x = 3p$, $y = 3q$, we have $x - y = 3(p - q) \in \mathbb{Z}$.
9. $1^1 = 1$, $1^2 = 1 +_6 1 = 2$, $1^3 = 1 +_6 1^2 = 3$, $1^4 = 1 +_6 1^3 = 1 +_6 3 = 4$, - - -
Thus $G = \{1^0, 1^2, 1^3, 1^4, 1^5, 1^6 = 0\}$. Therefore 1 is a generator. Also 5 is another generator.
10. (i) Identity $e = 3$, $a^{-1} = \frac{9}{a}$
(ii) Identity $e = 2$ and the inverse of a i.e., $a^{-1} = \frac{4}{a}$.
11. (i) doesnot have identity (ii) is a group.
12. (i) even, (ii) odd (iii) even (iv) even (v) odd.

Terminal Questions

1. Ans/Hint: (i) $\begin{pmatrix} 1234 \\ 1423 \end{pmatrix}$ (ii) $\begin{pmatrix} 12345 \\ 31254 \end{pmatrix}$ (iii) $\begin{pmatrix} 1234 \\ 3412 \end{pmatrix}$
2. Ans / Hint (i) (1, 2) odd (ii) (1, 3) odd (iii) (1, 4) (2, 3) even
3. Ans / Hint: For any $a, b \in G$, we have $a(ba)b = (ab)(ab) = (ab)^2 = a^2b^2 = a(ab)b$ and so the conclusion follows by left and right cancellations laws)
4. Ans / Hint: (a) is not a group since it has no identity element with respect to multiplication. (b), (c), (d) are left to the reader
5. Hint: Let $G = \{e, a, b\}$ and $e \neq a \neq b \neq e$. Now observe the multiplication table for G .

.	e	a	b
e	e	a	b
a	a	a^2	ab
b	b	b	b^2

6. Ans: Not Abelian
7. True
8. True
9. Ans: 6 elements

Unit 7 Propositional Calculus and Quantifiers

Structure

- 7.1 Introduction
 - Objectives
- 7.2 Statements, Propositions and Tautologies
- 7.3 Equivalence of Formulas
- 7.4 Normal Forms
- 7.5 Logical Inferences
- 7.6 Summary
- 7.7 Terminal Questions
- 7.8 Answers

7.1 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.

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:

1. Moscow is the capital city of Italy.
2. $2 + 3 = 7$.
3. Bangalore is the capital city of Karnataka.
4. Gangtok is the capital of Sikkim
5. New Delhi is the capital city of Germany.
6. Open the door
7. $1 + 2 = 3$

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

7.1.1 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 is 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

Table 7.1

Classification	Examples
Universal and affirmative judgment	All X is Y All men are mortal All monkeys are tree climbers All integers are real numbers
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 **sylogism** is an argument consisting of two propositions called **premises** and a third proposition called the **conclusion**.

Objectives:

At the end of the unit, you would be able to:

- recognise the propositions.
- explain the validity of the arguments and tautologies.
- explain the disjunctive and conjunctive normal forms.
- explain the equivalence forms and inference rules.

7.2 Statements, Propositions and Tautologies**7.2.1 Definition**

A Proposition is a statement that is either TRUE or FALSE, but not both.

7.2.2 Example

- “($x > 3$)” 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.
- “(10 > 3)” is a statement. This statement is TRUE. Therefore “(10 > 3)” is a proposition.
- “(10 < 3)” is a statement. This statement is FALSE (or NOT TRUE). Therefore “(10 < 3)” is a proposition.

7.2.3 Examples

- “($x + y + 4 = 7$)” is a statement but it is NOT a proposition.
- “($x \geq 3$)” and “($x \geq 5$)” are statements but NOT propositions
- “($x \geq 3$ for all x such that $x \geq 5$)” is a statement. This statement is TRUE. Therefore it is a proposition.

7.2.4 Examples

- (i) “Bangalore is the capital of Karnataka” (TRUE statement). Therefore it is a proposition.
- (ii) “Chennai is the capital of Sikkim” (FALSE statement). 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.

7.2.5 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 “ \sim ” is called “curl” or “twiddle” or “tilde”. The notation “ $\sim p$ ” is that of asserting the falsity of “ p ”. If “ p ” is considered to be FALSE, then “ $\sim p$ ” will be considered to be TRUE.

7.2.6 Example

Let p be the statement “Bangalore is a city”. Now $\sim p$ is the statement “Not, Bangalore is a city” (equivalently, “Bangalore is NOT a city”).

7.2.7 Definition

Let p be a statement. The statement “it is the case that p ” is another statement, called the *negation* of p .

7.2.8 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.
 $\sim S$: 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 using straightedge and compass alone.

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

The truth Table for the negation of a statement

P	$\sim P$
T	F
F	T

Here T stands for "TRUE" and F stands for "FALSE".

7.2.9 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 .

7.2.10 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

7.2.11 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”.

7.2.12 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.

7.2.13 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

7.2.14 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”.

7.2.15 The Conditional (or Implication)

The Conditional sentences are of type “if, then.....”

7.2.16 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:

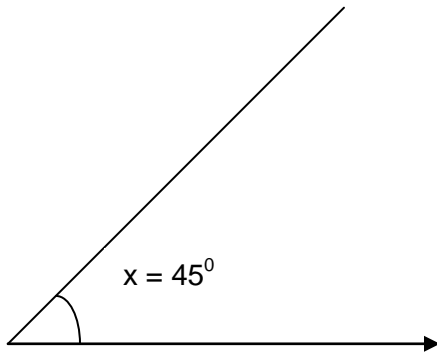


Figure 7.1

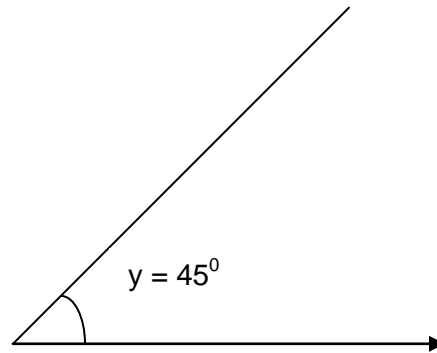


Figure 7.2

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

7.2.17 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

7.2.18 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 \Rightarrow tomorrow is a Monday) is TRUE.
- (iii) If “today is a Sunday, then tomorrow is a Saturday” is NOT TRUE.

7.2.19 Note

“ $P \rightarrow Q$ ” 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 .

7.2.20 Example

If “ $x = 5$ ”, then “ $2x = 10$ ” is a TRUE statement.

7.2.21 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	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

7.2.22 Note

- (i) $p \leftrightarrow q$ may be read as “ p is and only if q ”
- (ii) $p \leftrightarrow q$ means “ $p \rightarrow q$ and $q \rightarrow p$ ”
- (iii) It is clear that $p \leftrightarrow q$ is TRUE precisely when both $p \rightarrow q$ and $q \rightarrow p$ are TRUE.

7.2.23 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, $P \vee \sim P$ is a tautology and $P \wedge \sim P$ is a contradiction

7.2.24 Example

Construct the truth table for $((p \wedge \sim q) \rightarrow r) \rightarrow (p \rightarrow (q \vee r))$

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

Table 7.1

p	q	r	$p \wedge \sim q$	$(p \wedge \sim q) \rightarrow r$	$p \rightarrow (q \vee r)$	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

7.2.25 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.

Table 7.2Truth 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

7.2.26 Problem

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

Solution: Now we write down the truth table

Table 7.3

P	q	$p \vee q$	$p \wedge (p \vee q)$	\bar{p}	$[p \wedge (p \vee q)] \wedge \bar{p}$
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 $[p \wedge (p \vee q)] \wedge \bar{p}$ is always

FALSE. Hence $[p \wedge (p \vee q)] \wedge \bar{p}$ is a contradiction.

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). $x = 2 \Rightarrow x^2 = 4$.

2. Construct the truth table for $\bar{p} \wedge \bar{q}$

7.3 Equivalence of Formulas

7.3.1 Definition

Let A and B be two statements involving the variables P_1, P_2, \dots, 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, \dots, P_n and is denoted by $A \Leftrightarrow B$. In other words $A \Leftrightarrow B$ is a tautology.

7.3.2 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	T	T	T

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

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

7.4 Normal Forms

7.4.1 Definition

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

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

7.4.2 Example

Let P, Q, R be the three variables.

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

7.4.3 Definition

- (i) For a given formula, an equivalent formula consisting of disjunctions 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.

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

7.4.5 Example

Obtain the DNF and CNF of the following formula:

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

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

$$\begin{aligned} E &\Leftrightarrow (\sim P \vee \sim Q) \rightarrow ((P \rightarrow \sim Q) \wedge (\sim Q \rightarrow P)) \\ &\Leftrightarrow (\sim P \vee \sim Q) \rightarrow ((\sim P \rightarrow \sim Q) \wedge (Q \vee P)) \\ &\Leftrightarrow \sim(\sim P \vee \sim Q) \vee ((\sim P \vee \sim Q) \wedge (Q \vee P)) \\ &\Leftrightarrow (P \wedge Q) \vee ((\sim P \wedge Q) \vee (\sim P \wedge P)) \vee (\sim Q \wedge Q) \vee (Q \wedge P) \\ &\Leftrightarrow (P \wedge Q) \vee (\sim P \wedge Q) \vee (P \wedge Q) \\ &\Leftrightarrow (P \wedge Q) \vee (\sim P \wedge Q), \text{ which is in disjunctive normal form.} \end{aligned}$$

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

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

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,

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

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

$$\begin{aligned} &\Leftrightarrow (\sim P \vee Q) \wedge (\sim P \vee R) \wedge (P \vee \sim Q) \wedge (P \vee \sim R) \\ &\Leftrightarrow (\sim P \vee Q \vee R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee \sim Q \vee R) \\ &\Leftrightarrow (P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee \sim R) \wedge (P \vee Q \vee \sim R) \\ &\Leftrightarrow (\sim P \vee Q \vee R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee \sim Q \vee R) \wedge (P \vee \sim Q \vee R) \wedge \\ &\quad (P \vee \sim Q \vee \sim R) \wedge (P \vee Q \vee \sim R). \end{aligned}$$

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

3. 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) $P \rightarrow ((P \rightarrow Q) \wedge \sim(\sim Q \vee \sim P))$

7.5 Logical Inferences

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

7.5.1 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 $A \rightarrow B$ is a tautology, that is, $A \Rightarrow B$.

7.5.2 Validity using truth table

Let P_1, P_2, \dots, P_n be the variables appearing in the premises H_1, H_2, \dots, H_m and the conclusion C. Let all possible combinations of truth values are assigned to P_1, P_2, \dots, P_n and let the truth values of H_1, H_2, \dots, H_m and C are entered in the table. We say that C follows logically from premises H_1, H_2, \dots, H_m if and only if $H_1 \wedge H_2 \wedge \dots \wedge H_m \Rightarrow C$. This can be checked from the truth table using the following procedure:

- Look at the rows in which C has the value F.
- In every such row if at least one of the values of H_1, H_2, \dots, H_m is F then the conclusion is valid.

7.5.3 Example

Show that the conclusion $C: \sim P$ follows from the premises

$H_1: \sim P \vee Q$, $H_2: \sim (Q \wedge \sim R)$ and $H_3: \sim R$.

Solution: Given that $C: \sim P$, $H_1: \sim P \vee Q$, $H_2: \sim (Q \wedge \sim R)$ and $H_3: \sim R$.

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 row 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 from H_1 , H_2 , and H_3 .

7.5.4 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 S is 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.

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.

7.5.5 Example

Show that the conclusion C: $\sim P$ follows from the premises

$H_1: \sim P \vee Q$, $H_2: \sim(Q \wedge \sim R)$ and $H_3: \sim R$.

Solution: We get

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

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

7.5.6 Example

Show that $S \vee R$ is tautologically implied by $(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow S)$.

Solution: We have

	(1) $P \vee Q$	Rule P
{1}	(2) $\sim P \rightarrow Q$	Rule T
	(3) $Q \rightarrow S$	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

7.5.7 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

7.5.8 Validity by Indirect Method

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

7.5.9 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 $\sim P \wedge \sim Q$.

7.6 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 argument. Logic provides 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.

7.7 Terminal 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) $P \rightarrow Q, Q \rightarrow R$	$P \rightarrow R$
(b) $\sim Q, P \rightarrow Q$	$\sim P$
(c) $\sim(P \wedge \sim Q), \sim Q \vee R, \sim R$	$\sim P$
(d) $(P \wedge Q) \rightarrow R, \sim R \vee S, \sim S$	$\sim P \vee \sim Q$.
3. Prove the following using the Rule CP if necessary:

(a) $P \rightarrow Q \Rightarrow P \rightarrow (P \wedge Q)$
(b) $P, P \rightarrow (Q \rightarrow (R \wedge S)) \Rightarrow Q \rightarrow S$
(c) $P \rightarrow (Q \rightarrow R), Q \rightarrow (R \rightarrow S) \Rightarrow P \rightarrow (Q \rightarrow S)$.

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

7.8 Answers

Self Assessment Questions

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.
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

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

Unit 8

Predicate Calculus

Structure

- 8.1 Introduction
 - Objectives
- 8.2 Predicates
- 8.3 Quantifiers
- 8.4 Free and Bound Occurrences
- 8.5 Rules of Inference
- 8.6 Summary
- 8.7 Terminal Questions
- 8.8 Answers

8.1 Introduction

Let us first consider the two statements:

Ram is a bachelor

Smith is a bachelor.

Obviously, if we express these statements by symbols, we require 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.

Objectives:

At the end of the unit, you would be able to

- explain the fundamental idea of logical statements.
- identify the symbolic representation of statements.
- use the predicate formulas
- use the logical quantifiers.

8.2 Predicates

The part “is a bachelor” is called a *predicate*. Consider the following argument.

All the human beings

Ram is a human being.

Therefore, Ram 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 without confusion. Every predicate describes something about one or more objects.

We again consider the statements

1. Ram is a bachelor.
2. Smith is a bachelor.

Denote the predicate “is a bachelor” symbolically by the predicate letter B, “Ram ” by r, and “Smith” by s. Then statements (1) and (2) can be written as B(r) 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.

8.2.1 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.”

8.2.2 Examples

3-place predicate: Susan sits between Ralph and Bill.

4-place predicate: Green and Miller played bridge against Ram and Smith.

8.2.3 Note

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

8.2.4 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.

8.2.5 Example

Let H be a predicate ‘is beautiful’, s be the name ‘Sneha’ 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.

8.2.6 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.

8.2.7 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.

8.3 Quantifiers**8.3.1 Definition**

The word 'all' is called the **universal quantifier** and is denoted by (x) or $\forall x$. This symbol is placed before the statement function.

8.3.2 Example

Consider the statement functions:

$M(x)$: 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".

8.3.3 Note

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

8.3.4 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 ”.

8.3.5 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”.

8.3.6 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”.

8.3.7 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*.

8.3.8 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.

8.3.9 Example

Consider the predicate $Q(x)$: x is less than 10 and the statements $(\forall x) Q(x)$ and $\exists x Q(x)$.

Now, consider the following universes:

$$U_1: \{-1, 0, 1, 2, 4, 6, 8\}$$

$$U_2: \{3, -2, 12, 14, 10\}$$

$$U_3: \{10, 20, 30, 40\}$$

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

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

8.3.10 Example

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

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

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

8.3.11 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 –

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

WITHOUT universe of discourse: Let $P(x)$ stands for x is a positive integer.

Then we can symbolize the given statement as $(x) (P(x) \rightarrow (\exists y) (P(y) \wedge G(y, x)))$.

Self Assessment Questions

2. Translate each of the statement into symbols, using quantifiers, variables and predicate symbols.

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

- (a) There is a student who can speak Kannada and who knows C^{++}
 - (b) There is a student who can speak Kannada but does not know C^{++}
 - (c) Every student either can speak Kannada or knows C^{++}
 - (d) No student can speak Kannada or knows C^{++} .
3. Symbolize the statement “All men are giants.”

8.4 Free and Bound Occurrences**8.4.1 Definition**

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

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

8.4.2 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 $(A \Leftrightarrow B)$ are also wff.
- (d) If A is a wff and x is any variable, then $(\forall x)A$ and $(\exists x) A$ are wff.
- (e) Only those formulas obtained by using rules (1) to (4) are wff.

8.4.3 Definition

In a formula a part of the form $(\forall x) p(x)$ 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 $(\forall x) p(x)$ 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.

8.4.4 Example

Consider the following formulas:

$$(\forall x)P(x, y) \text{ -----(1)}$$

$$(\forall x)(P(x) \rightarrow Q(x)) \text{ ----- (2)}$$

$$(\forall x) (P(x) \rightarrow (\exists y)R(x, y)) \text{ -----(3)}$$

$$(\forall x)(P(x) \rightarrow R(x)) \vee (\forall x)(P(x) \rightarrow Q(x)) \text{ -----(4)}$$

$$(\exists x)(P(x) \wedge Q(x)) \text{ ----- (5)}$$

$$(\exists x)P(x) \wedge Q(x) \text{ -----(6)}$$

Observations:

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

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

In (3), the scope of (x) is $P(x) \rightarrow (\exists y) R(x,y)$, 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 $P(x) \rightarrow R(x)$, and the scope of the second is $P(x) \rightarrow Q(x)$. 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.

8.4.5 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 $(x) (B(x) \rightarrow F(x))$

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

$$\sim [(x)(B(x) \rightarrow F(x))] \text{ or } \exists x (B(x) \wedge \sim F(x)).$$

Self Assessment Question

4. Symbolize the expression “All the world respect selfless Leaders”.

8.4.6 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

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

8.4.7 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.
- For each integer x , if x is even then $x^2 + x$ is even.
 - There is an integer x such that $x^2 = 9$.

8.5 Rules of Inference

8.5.1 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.

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

8.5.3 Example

Show that $(\forall x)(P(x) \rightarrow Q(x)) \wedge (\forall x)(Q(x) \rightarrow R(x)) \Rightarrow (\forall x)(P(x) \rightarrow R(x))$

Solution: The given statement is symbolized as

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

8.5.4 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 |

8.5.5 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.

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

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

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

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

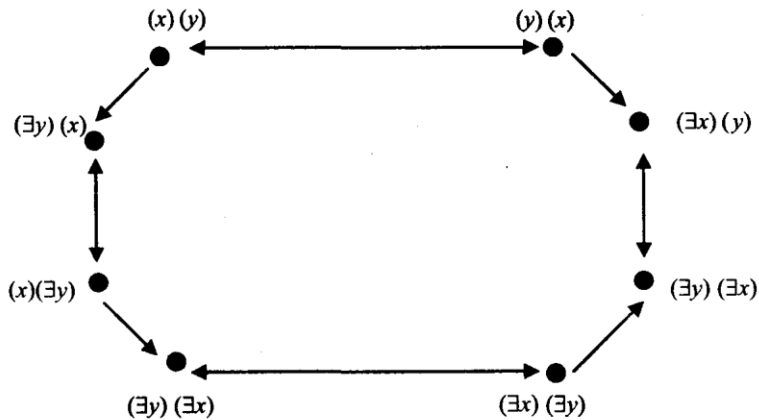


Figure 8.1

8.5.6 Example

Show that $\sim P(a, b)$ follows logically from $(x)(y) P(x, y) \rightarrow W(x, y)$ and $\sim W(a, b)$.

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) |

8.6 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.

8.7 Terminal 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) $(x)(x^2 - 10x + 21 = 0)$.
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 national numbers. Therefore, some integers are powers of 3.

8.8 Answers

Self Assessment Questions:

1. (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
2. (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) $\forall x \sim (P(x) \vee Q(x))$
3. Let $G(x)$: x is a giant; $M(x)$: x is a man.
 WITHOUT universe of discourse: $(x) (M(x) \rightarrow G(x))$.
 WITH universe of discourse as "class of men": $(x)G(x)$.
4. 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 $(x) (P(x) \rightarrow (y) (P(y) \wedge S(y) \rightarrow R(x, y)))$.
5. (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 $(x) (\sim P(x))$.

Unit 9

Finite Boolean Algebras

Structure

- 9.1 Introduction
 - Objectives
- 9.2 Boolean Algebras
- 9.3 Functions of Boolean Algebras
- 9.4 Gating Networks
- 9.5 Summary
- 9.6 Terminal Questions
- 9.7 Answers

9.1 Introduction

Boolean algebra is 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 an indispensable tool to computer scientists because of its direct applicability to switching theory of circuits and the logical design of digital computers. The symbols 0 and 1 used in this unit have logical significance. 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 unit we shall represent a Boolean function in a gating network. Various gates will be used for representing the expressions.

Objectives:

At the end of the unit you would be able to

- extend the notion of Boolean algebra from a lattice.
- identify and explain various properties of Boolean algebras
- write the dnf and cnf of a Boolean function.
- explain several applications of Boolean algebras in science and engineering.
- describe the Boolean functions and gating networks.

9.2 Boolean Algebras

9.2.1 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. $a \oplus a = a$; | $a * a = a$ |
| 2. $a \oplus b = b \oplus a$; | $a * b = b * a$. |
| 3. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$; | $a * (b * c) = (a * b) * c$; |
| 4. $a \oplus (a * b) = a$; $a \oplus (a * b) = a$; | |
| 5. $a \oplus (b * c) = (a \oplus b) * (a \oplus c)$; | $a * (b \oplus c) = (a * b) \oplus (a * c)$ |
| 6. $0 \leq a$ for all $a \in B$; | $a \leq 1$ for all $a \in B$; |
| 7. $a \oplus 0 = a$; | $a * 1 = a$; |
| 8. $a \oplus 1 = a$; | $a * 0 = 0$; |

Note: For $a \in B$, let a^1 be the (unique) complement of a .

- | | |
|------------------------------------|------------------------------|
| 9. $a \oplus a^1 = 1$; | $a * a^1 = 0$ |
| 10. $1^1 = 0$; | $0^1 = 1$; |
| 11. $(a \oplus b)^1 = a^1 * b^1$; | $(a * b)^1 = a^1 \oplus b^1$ |

Note:

- (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 De' Morgan laws.

9.2.2 Definition: A Boolean algebra with finite number of elements is called a finite Boolean algebra.

9.2.3 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 $S = \{a, b, c\}$

$$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, S\}$$

Then $(P(S), \subseteq)$ is a lattice. The Boolean algebra is represented by the following diagram.

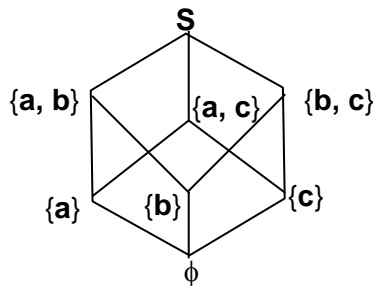


Figure 9.1

9.2.4 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

Figure 9.2

The complement of '0' is 1 and vice-versa. Then $(B, \vee, \wedge, -)$ is a Boolean Algebra.

9.2.5 Example

Let B_n be the set of n -tuples of 0's and 1's. For $a, b \in B_n$, define

$a \oplus b = (a_1 \vee b_1, a_2 \vee b_2, \dots, a_n \vee b_n)$ and $a * b = (a_1 \wedge b_1, a_2 \wedge b_2, \dots, a_n \wedge b_n)$ where $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$.

Now $a_i = 0$ or 1 and $b_i = 0$ or 1 for $i = 1, 2, \dots, n$. Also $a^1 = (a_1^1, a_2^1, \dots, a_n^1)$ and $b = (b_1^1, b_2^1, \dots, b_n^1)$ 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 $0_n = (0, 0, \dots, 0)$ and $1_n = (1, 1, \dots, 1)$.

9.2.6 Theorem

If $S_1 = \{x_1, x_2, \dots, x_n\}$ and $S_2 = \{y_1, y_2, \dots, y_n\}$ 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 shown in Fig. 9.3: so that each element of S_1 is directly over the correspondingly numbered element in S_2

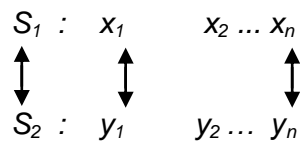


Figure 9.3

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. 9.4)

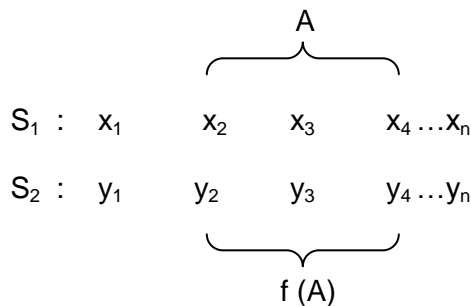


Figure 9.4

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.

9.2.7 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.

9.2.8 Note

- 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 $n > 0$.
- From the above theorem, it is clear that the lattice $(P(S), \subseteq)$ 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 .
- Each lattice $(P(S), \subseteq)$ is isomorphic to B_n (n -tuples, Boolean Algebra, over $\{0, 1\}$) where $n = |S|$

9.2.9 Example

Consider the lattice,

$$D_6 = \{x \in \mathbb{Z}^+ \mid x \text{ is a divisor of } 6\} = \{1, 2, 3, 6\}$$

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 the following diagrams:

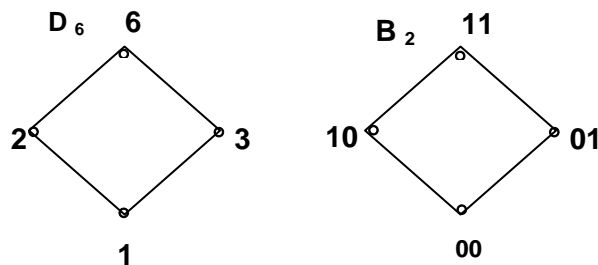


Figure 9.5

9.2.10 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 $\{0, 1\}$), where the isomorphism:
 $f: D_{30} \rightarrow B_3$ defined by
 $f(1) = 000, f(2) = 100, f(3) = 010, f(5) = 001, f(6) = 110, f(10) = 101,$
 $f(15) = 011, f(30) = 111.$

9.2.11 Theorem

Let $n = p_1 p_2 \dots p_k$ where p_i ($1 \leq i \leq k$) are distinct primes. Then D_n is a Boolean algebra.

9.2.12 Example

- a) $210 = 2 \cdot 3 \cdot 5 \cdot 7$. Therefore, D_{210} is a Boolean algebra.
- b) $66 = 2 \cdot 3 \cdot 11$, D_{66} is a Boolean algebra.
- c) $646 = 2 \cdot 17 \cdot 19$, D_{646} is a Boolean algebra.

9.2.13 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.

9.2.14 Example

- a) Take $n = 40$, then $n = 2^3 \cdot 5$, 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.

9.2.16 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.

9.2.17 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 $(P(S), \subseteq)$.

9.3 Functions of Boolean Algebras**9.3.1 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, \dots, 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.

9.3.2 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.

9.3.3 Example

a) $0 \vee x$

b) $(x_1 \vee \overline{x_2}) \wedge (\overline{x_1 \wedge x_3})$

c) $\overline{2 \wedge 3}$

are Boolean expressions.

Self Assessment Question

2. Write an equivalent Boolean expression for $E(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge \overline{x_3})$.

3. Find equivalent Boolean expression for $(x \vee y) \wedge (\overline{x} \vee \overline{y})$

4. Are there any Boolean algebra having 3 or 5 elements? Why or why not?

9.3.4 Definition

Let $f(x_1, x_2, \dots, x_n)$ 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, \dots, x_n can be listed in a table is called truth table.

9.3.5 Notation

$$f : B^n \longrightarrow B \text{ where } B = \{0, 1\} \text{ } f(x_1, x_2, \dots, x_n) = 0 \text{ or } 1$$

where each $x_i \in \{0, 1\}$, $1 \leq i \leq n$

(f is called a Boolean function on n variables)

9.3.6 Example

$$E(x_1, x_2, x_3) = (\overline{x_1} \wedge x_2 \wedge \overline{x_3}) \vee$$

$(x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_3)$ over $(\{0, 1\})$, $\vee, \wedge, -$ 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

9.3.7 Definition

A Boolean expression on n variables (x_1, x_2, \dots, x_n) is said to be a min-term if it is of the form,

$$\tilde{x}_1 \wedge \tilde{x}_2 \wedge \dots \wedge \tilde{x}_n, \text{ where}$$

$$\tilde{x}_i = x_i \text{ or } \overline{x_i}$$

9.3.8 Definition

A Boolean expression over $(\{0, 1\}, \vee, \wedge, -)$ is said to be in disjunctive normal form (denoted as, dnf) if it is the join of min-term. (dnf also called as sum of products of canonical form).

9.3.9 Example

The expression $\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}, x_1 \wedge x_2 \wedge x_3, \overline{x_1} \wedge x_2 \wedge \overline{x_3}$ min-terms.

The expression

$$(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge x_2 \wedge \overline{x_3}) \wedge (x_1 \wedge x_2 \wedge x_3) \text{ is in dnf.}$$

9.3.10 Example

Write the following Boolean expressions in an equivalent sum 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 –

$$\begin{aligned}
 \text{(i)} \quad x_1 * x_2^1 &= x_1 * x_2^1 * 1 \\
 &= x_1 * x_2^1 * (x_3 \oplus x_3^1) \\
 &= (x_1 * x_2^1 * x_3) \oplus (x_1 * x_2^1 * x_3^1) \\
 \text{(ii)} \quad x_2 \oplus x_3^1 &= [x_2 * (x_3 \oplus x_3^1)] \oplus [x_3^1 * (x_2 \oplus x_2^1)] \\
 &= (x_2 * x_3) \oplus (x_2 * x_3^1) \oplus (x_3^1 * x_2) \oplus (x_3^1 * x_2^1) \\
 &= (x_2 * x_3) \oplus (x_2 * x_3^1) \oplus (x_3^1 * x_2) \oplus (x_3^1 * x_2^1) \\
 &= [(x_1 \oplus x_1^1) * (x_2 * x_3)] \oplus [(x_1 \oplus x_1^1) * (x_2 * x_3^1)] \oplus [(x_1 \oplus x_1^1) * \\
 &\quad (x_2^1 * x_3^1)]. \\
 &= [(x_1 * x_2 * x_3) \oplus (x_1^1 * x_2 * x_3) \oplus (x_1 \oplus x_2 * x_3^1) \oplus (x_1^1 * x_2 * x_3^1) \\
 &\quad \oplus (x_1 * x_2^1 * x_3^1) \oplus (x_1^1 * x_2^1 * x_3^1)].
 \end{aligned}$$

(iii) Similar.

9.3.11 Definition

A Boolean expression of n variables x_1, x_2, \dots, x_n is said to be a max-term if it is of the form $\tilde{x}_1 \vee \tilde{x}_2 \vee \dots \vee \tilde{x}_n$ where $\tilde{x}_i = x_i$ or $\overline{x_i}$

9.3.12 Definition

A Boolean expression over $(\{0, 1\}, \vee, \wedge, -)$ is said to be in conjunctive normal form (denoted as, *Cnf*) if it is a meet of max-terms. (*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*.

9.3.13 Note

(i) Consider $f : \{0, 1\}^n \rightarrow \{0, 1\}$

To each (x_1, x_2, \dots, x_n) , we have min-term, $\tilde{x}_1 \wedge \tilde{x}_2 \wedge \dots \wedge \tilde{x}_n$, where

$\tilde{x}_i = x_i$ 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 min-term (respectively, max-term), corresponding to each ordered n -tuple of 0s and 1s for which the value of the function f is 1 (respectively, 0).
- (iii) cnf of f is the complement of dnf of \overline{f}

$f: \{0, 1\}^n \rightarrow \{0, 1\}$, max-term,

$\tilde{x}_1 \vee \tilde{x}_2 \vee \dots \vee \tilde{x}_n$ where

$$\tilde{x}_j = \begin{cases} x_i & \text{if the } i^{\text{th}} \text{ component of } n\text{-tuple is } 0 \\ \overline{x_i} & \text{if the } i^{\text{th}} \text{ component of } n\text{-tuple is } 1 \end{cases}$$

9.3.14 Example

Consider the Boolean expression,

$$f(x_1, x_2, x_3) = \left[x_1 \wedge (\overline{x_2 \vee x_3}) \right] \vee \left[\left[(x_1 \wedge x_2) \vee \overline{x_3} \right] \wedge x_1 \right]$$

over $(\{0, 1\}, \wedge, \vee, -)$. Write dnf and cnf.

Solution:

Table 9.1

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

Min-terms: $x_1 \wedge \overline{x_2} \wedge \overline{x_3}$, $x_1 \wedge x_2 \wedge \overline{x_3}$, $x_1 \wedge x_2 \wedge x_3$

dnf f: $(x_1 \wedge \overline{x_2} \wedge \overline{x_3}) \vee (x_1 \wedge x_2 \wedge \overline{x_3}) \vee (x_1 \wedge x_2 \wedge x_3)$

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: $(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$
 $\wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3})$

Alternatively, *cnf* of can be found as follows:

dnf \overline{f} = $(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge \overline{x_2} \wedge x_3) \vee (\overline{x_1} \wedge x_2 \wedge \overline{x_3})$
 $\vee (\overline{x_1} \wedge x_2 \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge x_3)$

$\overline{\text{dnf } \overline{f}}$ = $(\overline{\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}}) \wedge (\overline{\overline{x_1} \wedge \overline{x_2} \wedge x_3}) \wedge (\overline{\overline{x_1} \wedge x_2 \wedge \overline{x_3}})$
 $\wedge (\overline{\overline{x_1} \wedge x_2 \wedge x_3}) \wedge (\overline{x_1 \wedge \overline{x_2} \wedge x_3})$
 $= (x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee x_3)$
 $\wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3})$
 $= \text{cnf } f$

Self Assessment Question

5. Write the truth table for $f_1(x_1, x_2) = x_1 \vee x_2$, $f_2(x_1, x_2) = x_1 \wedge x_2$ and $f_3(x_1) = x_1^1$

9.4 Gating Networks

9.4.1 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*.
- (iii) From (i) we can conclude that a gate (or a combination of gates) is a polynomial p .
- (iv) A symbolic representation (that is, a combination of gates) which represents a polynomial is called a *gating network*.

9.4.2 Notation

Different gates that we use are given below:

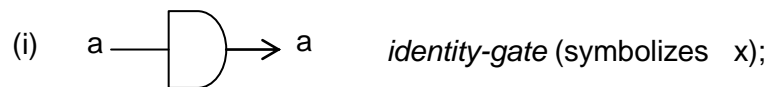


Fig. 9.6

If the input is x then the output is converted into x^1 by an inverter.

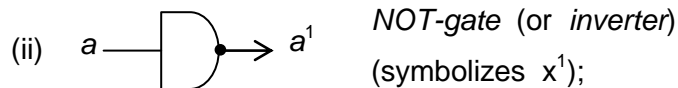


Fig. 9.7

AND Gate: If there be two or more inputs then the output will be a function of those inputs given below –

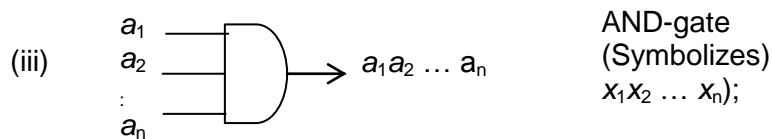


Fig. 9.8

OR gate: It converts two and more inputs into a single function given as follows.

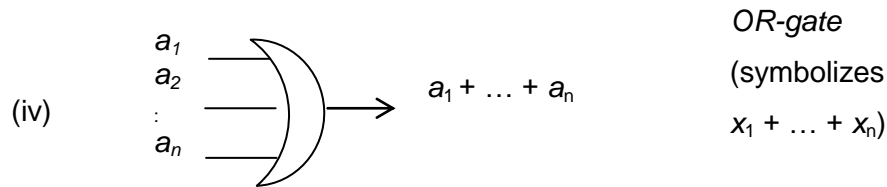


Fig. 9.9

We also use a small black disk either before or after one of the other gates to indicate an inverter.

9.4.3 Example

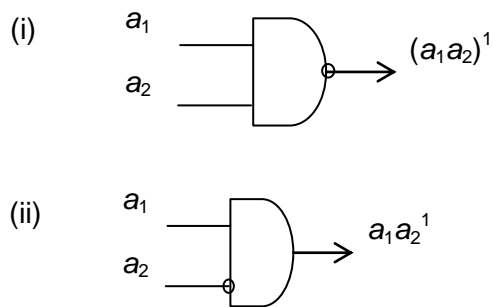


Fig. 9.10

9.4.4 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.

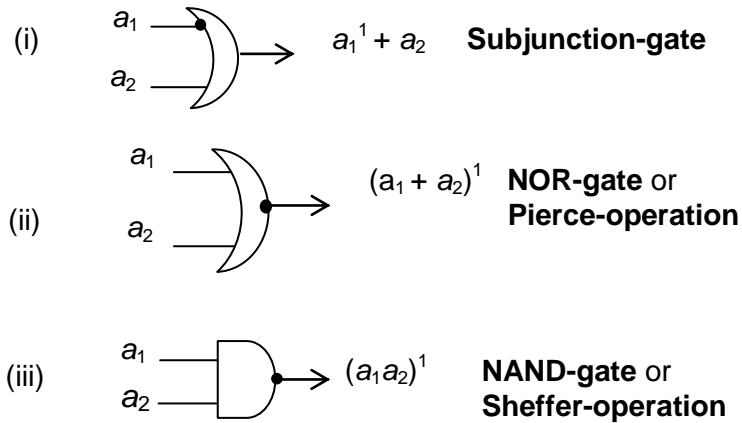


Fig. 9.11

9.4.5 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.

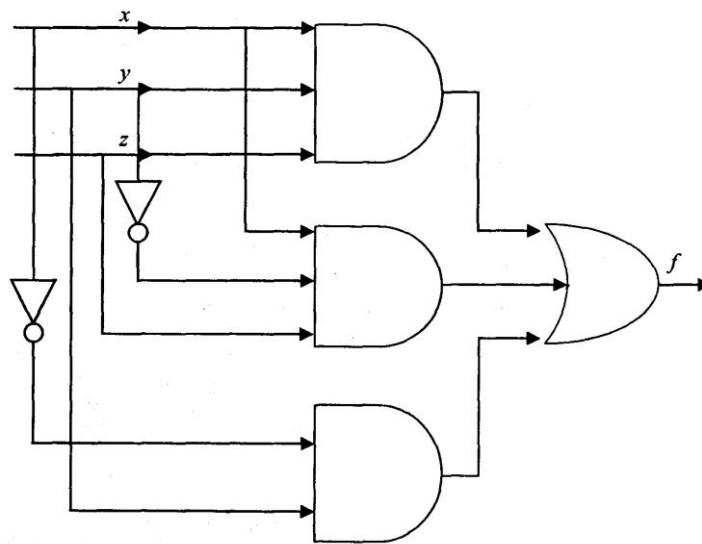


Fig. 9.12

9.4.6 Example

Find the Boolean expression for the following logic diagram:

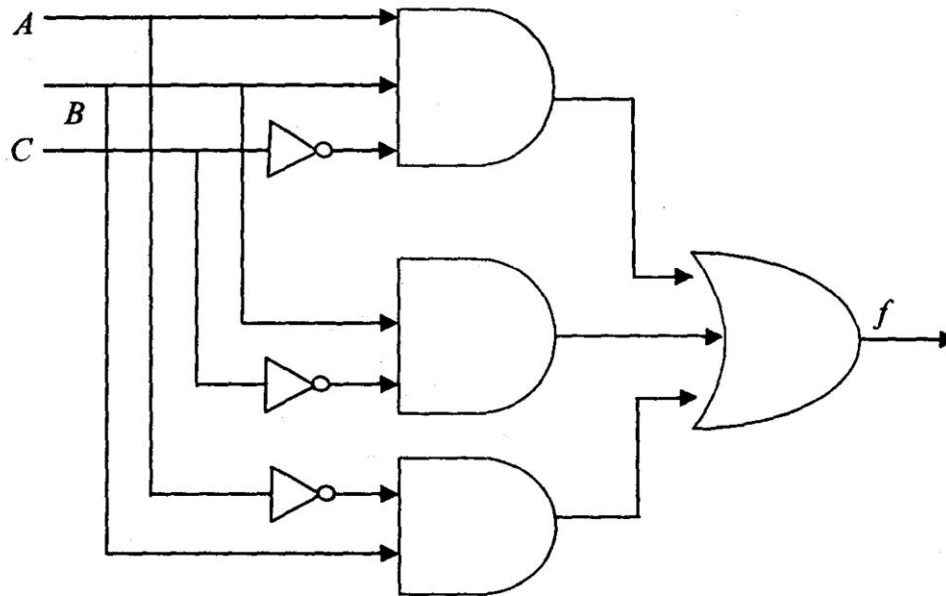


Fig. 9.13

Solution: $ABC^1 + BC^1 + A^1B$.

9.4.7 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 in the Figure.

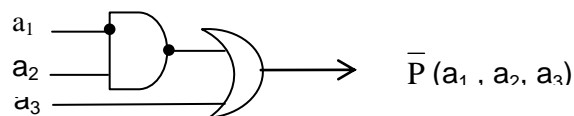
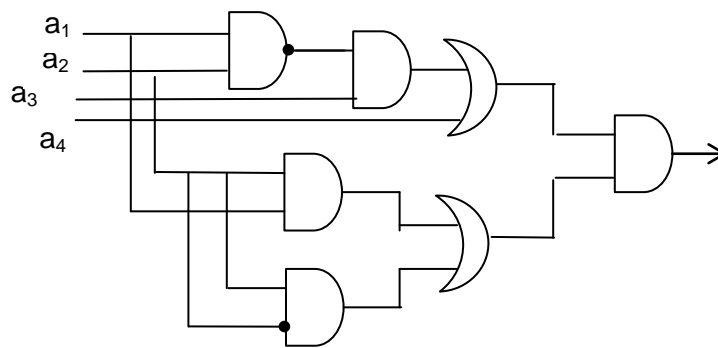


Fig. 9.14

9.4.8 Problem: Find

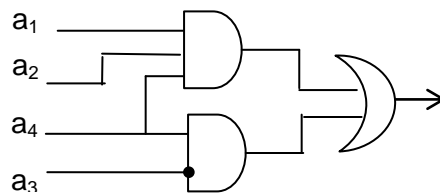
- (i) the polynomial p which, corresponds to the gating network given in the Figure.
- (ii) a simplified gating network, which operates in the same way as the gating network given in Figure. 9.15

**Fig. 9.15****Solution:**

- (i) The polynomial that represents the given gating network is

$$p = ((x_1x_2)^1x_3 + x_4) (x_1x_2 + x_3^1x_4).$$
- (ii) By using the Quine-Mc Cluskey algorithm we get a simplified form

$$q = x_1x_2x_4 + x_3^1x_4 \text{ of } p.$$

**Fig. 9.16**

Now, the gating network, which represents q is given by the Figure.

9.5 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. You are now able to know the 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.

9.6 Terminal Questions

1. Find equivalent Boolean expression for the following:

$$(i) \quad x \wedge (y \vee (y^1 \wedge (y \vee y^1)))$$

$$(ii) \quad (z^1 \vee x) \wedge ((x \wedge y) \vee z) \wedge (z^1 \vee y)$$

$$(iii) \quad [(x \wedge z) \vee (y^1 \vee z)^1] \vee [(y \wedge z) \vee (x \wedge z^1)]$$

2. Write the Boolean function values for $f : A^2 \rightarrow A$, where $A = \{0, 1\}$ with $f(x_1, x_2) = (x_1 \wedge \overline{x_1}) \vee x_2$.

3. Consider the Boolean polynomial $f(x, y, z) = x \wedge (y \vee z^1)$. If $B = \{0, 1\}$, compute the truth table of the function $f : B_3 \rightarrow B$ 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 $f : B_3 \rightarrow B$ defined by f .

5. Rewrite the given Boolean polynomial to obtain the requested format.

$$(i) \quad (x \wedge y^1 \wedge z) \vee (x \wedge y \wedge z); \text{ two variables and one operation.}$$

$$(ii) \quad (z \vee (y \wedge (x \vee x^1))) \wedge (y \wedge z^1)^1; \text{ one variable.}$$

$$(iii) \quad (y \vee z) \vee x^1 \vee (w \wedge w^1)^1 \vee (y \wedge z^1); \text{ two variables and two operations.}$$

6. Write the disjunctive and conjunctive normal form for $f(x_1, x_2, x_3) = [x_1 \wedge \overline{(x_2 \vee x_3)}] \vee \{[(x_1 \wedge x_2) \vee \overline{x_3}] \wedge x_1\}$, by writing min-terms and max-terms.

9.7 Answers

Self Assessment Questions

- Take $n = 75$. Then $5^2 \mid 75$ (since $75 = 3 \cdot 5^2$), we have D_{75} is not a Boolean algebra.
- The equivalent Boolean expression is: $x_1 \wedge (x_2 \vee \overline{x_3})$.
- x .
 - $x \wedge y$.
 - $x \vee y$.
- No, each Boolean algebra must have 2^n elements.
- 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

Unit 10

Formal Languages

Structure

- 10.1 Introduction
 - Objectives
- 10.2 Grammars and Languages
- 10.3 Classification of Grammars
- 10.4 Summary
- 10.5 Terminal Questions
- 10.6 Answers

10.1 Introduction

The basic machine instructions of a digital computer are very primitive compared with the complex operations that must be performed in various disciplines such as engineering, science, management and mathematics. Even though a complex procedure can be programmed in machine language, it is desirable to use a high level language that contains instructions similar to those required in a particular application. The specification of a programming language involves a set of symbols and a set of correct programs.

Objectives:

At the end of the unit, you would be able to

- construct the language using grammar.
- construct the grammar, for a given language.

10.2 Grammars and Languages

A language L can be considered as a subset of the free monoid on an alphabet. It is a set of strings or sentences over some finite alphabet. Finite languages can be specified by exhaustively enumerating all their sentences.

Any device, which specifies a language should be finite. A simple method of specification, which satisfies this requirement uses a generative device is called as grammar. Precisely, a grammar consists of a finite set of rules or productions, which specify the syntax of the language.

The theory of formal languages exclusively involves the study of the language syntax and this theory incepts from the works of well-known linguist Noam Chomsky.

The goal of Chomsky was to define the syntax of natural languages using simple and clear mathematical rules in order to precisely characterize the structure of language. The primary idea behind this concept was to define a formal grammar for describing the natural languages like English so that language translation using a computer would become easy. Chomsky developed the mathematical model of grammar in 1956. However, rather than becoming useful for natural languages, this model turned out to be suitable for the grammar of computer languages.

Before presenting the formal definition of grammar, we review some preliminary notations and definitions.

10.2.1 Definition

Let S denote a nonempty set of symbols, called an **alphabet**. We assume that S to be finite. The elements of the set are called **letters**. A word or a string on the set S is a finite sequence of the elements.

10.2.2 Example

Take $S = \{a, b\}$. Then $x = abab$, $y = aaab$, $z = aaabb$ are strings on S .

10.2.3 Definition

The **length** of the string is the number of symbols in the string.

In the above example, length of x is 4, length of z is 5.

(Denote respectively are $|x| = 4$, $|z| = 5$)

Note that a string λ is called empty if $|\lambda| = 0$. In this unit, we denote the empty string by “ \wedge ”.

10.2.4 Properties of strings

Let S be the set of symbols, and S^* denote the set of all strings (including empty string).

i) **Concatenation on S^* associative**

For any $x, y, z \in S^*$, $x(yz) = (xy)z$.

ii) **Identity:** The empty string is an identity element for the operation.

That is, $\lambda x = x\lambda = x$ for all $x \in S^*$

iii) **Cancellation:** For any $x, y, z \in S^*$,

$xy = xz$ implies $y = z$ (left cancellation)

$yx = yw$ implies $x = w$ (right cancellation)

iv) For $x, y \in S^*$, $|xy| = |x| + |y|$

10.2.5 Notation

V_T = Finite non empty set of symbols (alphabet), called terminal symbols.

(The strings of terminal symbols are denoted by lower case letters x, y, z, \dots)

V_N = Set of non – terminal symbols, which are used to define the syntax (or structure) of the language ($A, B, C, \dots, X, Y, Z, \dots$)

$V_N \cup V_T$ = Consisting of non terminal and terminal symbols, called vocabulary of the language. (Strings of symbols over the vocabulary are given by $\alpha, \beta, \gamma, \dots$).

$V_N \cap V_T = \phi$, empty set (assumption).

If $A \rightarrow \alpha_1, A \rightarrow \alpha_2, \dots, A \rightarrow \alpha_n$ are n A -productions, then they can be written as $A \rightarrow \alpha_1 | \alpha_2 | \dots | \alpha_n$.

10.2.6 Definition

A **grammar** (phrase structure) is defined by a 4 – tuple $G = (V_N, V_T, S, \phi)$ where S is a distinguished element of V_N (called the starting symbol), ϕ is a finite subset of the relation from

$$(V_T \cup V_N)^* V_N (V_T \cup V_N)^* \text{ to } (V_T \cup V_N)^* .$$

In general, an element (α, β) is written as $\alpha \rightarrow \beta$ (called a production rule or a rewriting rule).

10.2.7 Example

Let the symbols

- L : letter
- D : digit
- I : identifier

Write the grammar $G = (V_N, V_T, S, \Phi)$

$$\text{Where } V_N = \{I, L, D\}$$

$$V_T = \{a, b, c, \dots, x, y, z\}$$

$$S = I$$

$$\Phi = \{I \rightarrow L, I \rightarrow IL, I \rightarrow ID, L \rightarrow a, L \rightarrow b, \dots, L \rightarrow z,$$

$$D \rightarrow 0, D \rightarrow 1, \dots, D \rightarrow 9\}$$

10.2.8 Definition

Let $G = (V_N, V_T, S, \Phi)$ be a grammar. For $\sigma, \psi \in (V_N \cup V_T)^* - \{\text{empty string}\}$,

σ is said to be a **direct derivative** of ψ , (denoted as $\psi \Rightarrow \sigma$) if there are strings

ϕ_1 and ϕ_2 (including possibly empty strings) such that

$\psi = \phi_1 \alpha \phi_2$ and $\sigma = \phi_1 \beta \phi_2$ and $\alpha \rightarrow \beta$ is a production of G . If $\psi \Rightarrow \sigma$, then

we say that ψ directly produces σ (or σ directly reduces to ψ).

10.2.9 Example

Consider the above example, the direct derivatives are as follows:

Table 10.1

ψ	σ	Rule used	ϕ_1	ϕ_2
I	L	$I \rightarrow L$	Λ	Λ
Ib	Lb	$I \rightarrow L$	Λ	b
Lb	Ab	$L \rightarrow a$	Λ	b
LD	L1	$D \rightarrow 1$	L	Λ
LD	aD	$L \rightarrow a$	Λ	D

10.2.10 Definition

Let $G = (V_N, V_T, S, \phi)$ be a grammar. The string ψ produces σ (or σ is the direct derivative of ψ), written as $\psi \Rightarrow^+ \sigma$, if there are strings $\phi_0, \phi_1, \dots, \phi_n$, ($n > 0$) such that $\psi = \phi_0 \Rightarrow \phi_1, \phi_1 \Rightarrow \phi_2 \dots \phi_{n-1} \Rightarrow \phi_n = \sigma$ (The relation \Rightarrow^+ is the transitive closure of \Rightarrow).

If $n = 0$, then the reflexive transitive closure of \Rightarrow as

$$\psi \Rightarrow^* \sigma \Leftrightarrow \psi \Rightarrow^+ \sigma \text{ or } \psi = \sigma.$$

10.2.11 Definition

A **sentential** form is any derivative of the unique non terminal symbol S .

The language L generated by a grammar G is the set of all sentential forms whose symbols are terminal.

$$\text{That is, } L(G) = \left\{ \sigma / S \Rightarrow^* \sigma \text{ and } \sigma \in V_T^* \right\}$$

This means that, the **language** is a subset of all terminal strings over V_T .

10.2.12 Example

$$\text{Let } G = (\{E, T, F\}, \{a, +, *, (\cdot)\}, E, \Phi)$$

where Φ consists of productions

$$\begin{aligned}
 E &\rightarrow E + T \\
 E &\rightarrow T \\
 T &\rightarrow T * F \\
 T &\rightarrow F \\
 F &\rightarrow (E) \\
 F &\rightarrow a
 \end{aligned}$$

where the variables E (expression), T (term), and F (factor) used in conjunction with arithmetic expressions.

We wish to derive the expression $a * a + a$ as follows: Starting with the symbol E .

$$\begin{aligned}
 E &\Rightarrow E + T \\
 &\Rightarrow T + T \\
 &\Rightarrow T * F + T \\
 &\Rightarrow F * F + T \\
 &\Rightarrow a * F + T \\
 &\Rightarrow a * a + T \\
 &\Rightarrow a * a + F \\
 &\Rightarrow a * a + a
 \end{aligned}$$

10.2.13 Problem

Generate the language $L(G) = \{a^n b^n c^n / n \geq 1\}$ by the following grammar

$$G = (\{S, B, C\}, \{a, b, c\}, S, \Phi)$$

where Φ consists of productions,

$$\begin{aligned}
 S &\rightarrow asBC \\
 S &\rightarrow aBC \\
 CB &\rightarrow BC \\
 aB &\rightarrow ab \\
 bB &\rightarrow bb \\
 bC &\rightarrow bc \\
 cC &\rightarrow cc
 \end{aligned}$$

Solution:

We generate the language for $n = 2$. That is, we derive the string $a^2b^2c^2$.

$$\begin{aligned}
 S &\Rightarrow aSBC \\
 &\Rightarrow aaBCBC \\
 &\Rightarrow aaBBCC \\
 &\Rightarrow aabBCC \\
 &\Rightarrow aabbCC \\
 &\Rightarrow aabbcC \\
 &\Rightarrow aabbcc
 \end{aligned}$$

10.2.14 Example

Consider the grammar $G = (\{S, C\}, \{a, b\}, S, \Phi)$

where Φ is the set of productions : $S \rightarrow aCa$

$$C \rightarrow aCa$$

$$C \rightarrow b$$

Generate the language: $\{a^nba^n/n \geq 1\}$.

Solution:

Derivation for $n = 2$. i.e., the string a^2ba^2

$$\begin{aligned}
 S &\Rightarrow aCa \\
 &\Rightarrow aaCaa \\
 &\Rightarrow aabaa
 \end{aligned}$$

10.2.15 Problem

Generate the language $L(G) = \{a^nba^m/n, m \geq 1\}$ by the grammar.

$G = (\{S, A, B, C\}, \{a, b\}, S, \Phi)$ where Φ is the set of productions.

$$\{S \rightarrow aS, S \rightarrow aB, B \rightarrow bC, C \rightarrow aC, C \rightarrow a\}$$

Solution

Take $n = 2, m = 3$. We generate the string a^2ba^3

$$\begin{aligned} S &\Rightarrow aS \\ &\Rightarrow aaB \\ &\Rightarrow aabC \\ &\Rightarrow aabaC \\ &\Rightarrow aabaaC \\ &\Rightarrow aabaaa \end{aligned}$$
10.2.16 Problem

If $G = (\{S\}, \{0, 1\}, \Phi: \{S \rightarrow 0S1, S \rightarrow \wedge\}, S)$, then find $L(G)$, the language generated by G .

Solution: Since $S \rightarrow \wedge$ is a production, $S \Rightarrow \wedge$. This implies that $\wedge \in L(G)$.

Now, for all $n \geq 1$, we can write the following:

$$S \Rightarrow 0S1 \Rightarrow 00S11 \dots \Rightarrow 0^n S 1^n \Rightarrow 0^n 1^n.$$

Therefore, $0^n 1^n \in L(G)$.

In the above derivation, at every step, $S \rightarrow 0S1$ is applied, except in the last step where $S \rightarrow \wedge$ is applied.

Therefore, $\{0^n 1^n \mid n \geq 0\} \subseteq L(G)$.

Now suppose $w \in L(G)$. So we should start the derivation of w with S .

If we are applying $S \rightarrow \wedge$ first, then we will get $w = \wedge$.

Otherwise, the first production that we need to apply is $S \rightarrow 0S1$.

However, at any stage we can apply $S \rightarrow \wedge$ to obtain the terminating string.

Therefore, w can be derived in the following form.

$$S \Rightarrow 0^n S 1^n \Rightarrow 0^n 1^n, \text{ for some } n \geq 1, \text{ That is } L(G) \subseteq \{0^n 1^n \mid n \geq 0\}.$$

Hence $L(G) = \{0^n 1^n \mid n \geq 0\}$.

10.2.17 Problem

Suppose $G = (\{S, A, B\}, \{0, 1\}, \Phi, S)$ where Φ consists of productions: $S \rightarrow 0AB0$, $A \rightarrow 10AB1$, $B \rightarrow A01$, $0A \rightarrow 100$ and $1B1 \rightarrow 0101$. Show that $w = 100110100011010$ is in $L(G)$.

Solution: To prove that the given $w \in L(G)$, we need to start with an S -production and subsequently apply the suitable productions in order to derive w . The following sequences show the derivation of w .

$$\begin{aligned} S &\Rightarrow \underline{0}AB0 \\ &\Rightarrow 100\underline{B}0 \\ &\Rightarrow 100\underline{A}010 \\ &\Rightarrow 1001\underline{0}AB1010 \\ &\Rightarrow 1001100\underline{B}1010 \\ &\Rightarrow 1001100\underline{A}011010 \\ &\Rightarrow 100110100011010 = w \in L(G). \end{aligned}$$

In this sequence, the strings that can be replaced are underlined.

10.2.18 Problem

Suppose $G = (\{S, A, B\}, \{a, b\}, \Phi, S)$, where Φ consists of the following productions.

$S \rightarrow abAB$, $A \rightarrow aBb$, $B \rightarrow abA$, $bA \rightarrow bab$, $aB \rightarrow aaa$.

Show that $w = abaaababaaab \in L(G)$.

Solution: Here, we can follow the proof by starting with an S -production and subsequently applying the suitable productions in order, we can derive w . The following sequences show the derivation of w :

$$\begin{aligned} S &\Rightarrow ab\underline{A}B \\ &\Rightarrow ab\underline{a}BbB \\ &\Rightarrow abaaab\underline{B} \\ &\Rightarrow abaaabab\underline{A} \\ &\Rightarrow abaaababa\underline{B}b \\ &\Rightarrow abaaababaaab. \text{ Hence } w \in L(G). \end{aligned}$$

Self Assessment Questions

1. Suppose $G = (\{S, A, B\}, \{a, b\}, \Phi, S)$ where Φ consists of the following productions: $S \rightarrow abAB$, $A \rightarrow aBb$, $B \rightarrow abA$, $\epsilon \rightarrow bab$, $aB \rightarrow aaa$. Then verify whether or not $w = abaaababaaab \in L(G)$.
2. Consider the string $x = well$, find all prefixes and suffixes of x . Also find all subwords of x .
3. Let $x = 0100$, $y = 11$. Find xy and yx .
4. Given the strings $u = a^2bab^2$ and $v = bab^2$, find the strings uv , vu , v^2 , λu . Also find their lengths.
5. Let $A = \{ab, bc, ca\}$. Find whether the following strings (i) abc , (ii) $ababab$, (iii) $abba$, (iv) $bcabbab$ belongs to A^* .

10.3 Classification of Grammars

Every language is specified by a particular grammar. The classification of languages is based on the classification of the grammar used to specify them. Grammars are classified accordingly to the types of productions.

10.3.1 Definition

- i) A grammar in which there are no restrictions on its productions is called type – 0 grammar or unrestricted grammar $(L(T_0))$.
- ii) A grammar that contains only productions of the form $\alpha \rightarrow \beta$ where $|\alpha| \leq |\beta|$ is called **type – 1 grammar or context sensitive grammar**.

The language generated by this grammar is called context sensitive language $(L(T_1))$.

- iii) A grammar that contains only productions of the form $\alpha \rightarrow \beta$ where $|\alpha| \leq |\beta|$ and $\alpha \in V_N$ is called **type – 2 grammar or context free grammar**. The language generated by this grammar is called context free language ($L(T_2)$).
- iv) A grammar that contains only productions of the form $\alpha \rightarrow \beta$, where $|\alpha| \leq |\beta|$, $\alpha \in V_N$ and β has the form a, B or aB , where $a \in V_T, B \in V_N$ is called **type -3 grammar or regular grammar**. The language generated by this grammar is called a regular language ($L(T_3)$).
- v) A grammar $G(V_N, V_T, S, \Phi)$ is called **monotonic** when every production in Φ is of the form $\alpha \rightarrow \beta$ having $|\alpha| \leq |\beta|$ or $S \rightarrow \wedge$. In the second situation, S does not appear on the right hand side of any of the production of G .

In other words, in any production, the left hand string is always a single non – terminal and right hand string is either a terminal or a terminal followed by a non – terminal.

10.3.2 Theorem

If G be type 0 grammar, then we can find an equivalent grammar G_1 where each production is either of the form $\alpha \rightarrow \beta$ or $A \rightarrow a$. Here, α and β are the strings variables, A is a variable and a is a terminal.

Proof: To construct G_1 , consider a production $\alpha \rightarrow \beta$ in G with α or β having the same terminals. Let, in both α and β , a new variable C_a replace each of the terminals to produce α' 's and β' 's.

Now, for every $\alpha \rightarrow \beta$, where α and β have same terminals, we can get a corresponding $\alpha \rightarrow \beta$ with productions of the form $C_a \rightarrow a$ for each terminal that appears on α or β . Therefore, the new productions obtained from the above constrictioin are the new productions for G_1 . Also, the variables of G along with the new variables of the form C_a are the variables of G_1 . Similarly, the terminals and the start symbol of G_1 are also same as those of G . Hence, G_1 satisfies the required conditions for a grammar and it is equivalent to G . Therefore $L(G) = L(G_1)$.

10.3.3 Note

- (i) The above theorem also holds for grammars of type 1, 2 and 3.
- (ii) $L(T_3) \subseteq L(T_2) \subseteq L(T_1) \subseteq L(T_0)$.

10.3.4 Theorem

Every monotonic grammar G is equivalent to type 1 grammar.

10.3.5 Problem

Construct a grammar for the language.

$$L = \{aaaa, aabb, bbaa, bbbb\}$$

Solution:

Since L has a finite number of strings, we can list all strings in the language.

Let $V_T = \{a, b\}$ be the set of terminals.

$$V_N = \{S\}, \text{ non terminal (starting symbol)}$$

$$\text{Productions: } S \rightarrow aaaa$$

$$S \rightarrow aabb$$

$$S \rightarrow bbaa$$

$$S \rightarrow bbbb$$

We simplify the productions as follows.

$$\text{Let } V_N = \{S, A\}$$

$$\Phi: S \rightarrow AA, A \rightarrow aa, A \rightarrow bb.$$

Therefore, the Grammar $G = (V_T = \{a, b\}, V_N = \{S, A\}, S, \Phi)$

10.3.6 Problem

Construct a grammar for the language.

$$L = \{x \mid x \in \{a, b\}^*, \text{the number of } a\text{'s in } x \text{ is a multiple of } 3\}$$

Solution:

Let $T = \{a, b\}$ and $N = \{S, A, B\}$,

S is a starting symbol.

The set of productions: Φ

$$S \rightarrow bS$$

$$S \rightarrow b$$

$$S \rightarrow aA$$

$$A \rightarrow bA$$

$$A \rightarrow aB$$

$$B \rightarrow bB$$

$$B \rightarrow aS$$

$$B \rightarrow a$$

For instance,

bbababbab can be generated as follows.

$$\begin{aligned} S &\Rightarrow bS \Rightarrow bbS \Rightarrow bbaA \Rightarrow bbabA \Rightarrow bbabaB \Rightarrow bbababbB \Rightarrow bbababbaS \\ &\Rightarrow bbababbab \end{aligned}$$

Therefore, the grammar $G = (V_T = \{a, b\}, V_N = \{S, A, B\}, \Phi, S)$

10.3.7 Problem

Find the highest type number that can be applied to the following productions:

$$1. S \rightarrow A0, A \rightarrow 1 \mid 2 \mid B0, B \rightarrow 012.$$

$$2. S \rightarrow ASB \mid b, A \rightarrow bA \mid c$$

$$3. S \rightarrow bS \mid bc.$$

Solution:

1. Here, $S \rightarrow A0$, $A \rightarrow B0$ and $B \rightarrow 012$ are of type 2, while $A \rightarrow 1$ and $A \rightarrow 2$ are type 3. Therefore, the highest type number is 2.
2. Here, $S \rightarrow ASB$ is of type 2, while $S \rightarrow b$, $A \rightarrow bA$ and $A \rightarrow c$ are type 3. Therefore, the highest type number is 2.
3. Here, $S \rightarrow bS$ is of type 3, while $S \rightarrow ab$ is of type 2. Therefore, the highest type number is 2.

Notation: Let L_0 , L_{cs} , L_{cf} and L_r are the family of type 0, context sensitive, context free and regular languages respectively.

10.3.8 Operations on Languages

In formal languages, there are certain common operations. These operations include standard set operations such as intersection, union and complementation operations. There are other operations such as string operations that are applied element-wise on the languages. For example, if we consider two languages L_1 and L_2 over some common alphabets, then we can define the following operations.

Concatenation: It combines the two languages to produce the concatenated language denoted by L_1L_2 . Here, L_1L_2 consists of all the strings of type xy , where x is a string in L_1 and y is a string in L_2 .

Intersection: It produces the language $L_1 \cap L_2$ which consists of all the strings that are contained in both the languages L_1 and L_2 .

Union: It produces the languages $L_1 \cup L_2$ which consists of all the strings that are contained in either of the languages L_1 and L_2 .

Complement: It produces the language $\neg L_1$ from the language L_1 . Here, $\neg L_1$ is known as the complement of the language L_1 with respect to an alphabet, where $\neg L_1$ consists of all the strings over the alphabets that are not in the language L_1 .

These operations are generally used in determining the closure properties of the classes of languages. A class of languages is called closed under some operation, when applying the operation to the class of languages always produces a language in the same class.

10.3.9 Theorem

The languages L_0 , L_{cs} , L_{cf} and L_r are closed under the operations concatenation and union.

10.3.10 Problem

Construct a grammar for the language.

$$L = \{a^i b^j / i, j \geq 1, i \neq j\}$$

Solution:

We decompose $L = L_1 \cup L_2$ where

$$L_1 = \{a^i b^j / i > j\} \text{ and } L_2 = \{a^i b^j / i < j\}$$

Grammar for L_1 : Set of production for L_1

$$A \rightarrow aA$$

$$A \rightarrow aB$$

$$B \rightarrow aBb$$

$$B \rightarrow ab,$$

where $V_T = \{a, b\}$, $V_N = \{A, B\}$

A is a starting symbol.

Grammar for L_2 :

$V_T = \{a, b\}$, $V_N = \{C, D\}$, C is starting symbol.

Productions: $C \rightarrow Cb$

$$C \rightarrow Db$$

$$D \rightarrow aDb$$

$$D \rightarrow ab$$

Now by adding the two sets of productions, $S \rightarrow A$, $S \rightarrow C$ with S as the starting symbol, we get the grammar –

$$G = (V_T = \{a, b\}, V_N = \{S, A, B, C\}, S, \Phi)$$

where $\Phi : S \rightarrow A, S \rightarrow C, A \rightarrow aA, A \rightarrow aB, B \rightarrow aBb, B \rightarrow ab, C \rightarrow Cb, C \rightarrow Bb$.

10.3.11 Problem

Obtain a grammar to generate the language

$$L = \{0^i 1^j \mid i \neq j, i \geq 0 \text{ and } j \geq 0\}.$$

Solution: It is clear from the statement that if a string has n number of 0s as the prefix, this prefixed string should not be followed by n number of 1s, that is, we should not have equal number of 0's and 1s. At the same time 0s should precede 1s. The grammar for this can be written as:

$G = (V_N, V_T, \Phi, S)$ where

$$V_N = \{S, A, B, C\}$$

$$V_T = \{0, 1\}$$

Productions

$$\begin{aligned} \Phi: \quad & S \rightarrow 0S1 \text{ (generates } 0^i 1^j \text{ recursively)} \\ & S \rightarrow A \quad \text{(to generate more 0s than 1s)} \\ & S \rightarrow B \quad \text{(to generate more 1s than 0s)} \\ & A \rightarrow 0A \mid 0 \text{ (at least one 0 is generated)} \\ & B \rightarrow 1B \mid 1 \text{ (at least one 1 is generated); and} \end{aligned}$$

S is the starting symbol.

10.3.12 Problem

Obtain a grammar to generate the language $L = \{x \mid x \bmod 3 = 0\}$ on the set $V_T = \{a\}$.

Solution: The language accepted by the grammar can also be written as

$$L = \{\wedge, aaa, aaaaaa, aaaaaaaaa, \dots\}.$$

It is clear from this definition that any string generated should have the length multiple of 3 which can be easily done by the production rule:

$$S \rightarrow aaaS \mid \wedge.$$

Therefore, the final grammar is:

$$G = (V_T, V_N, \Phi, S), \text{ where}$$

$$V_T = \{S\}$$

$$V_N = \{a\}, \text{ and the set of productions}$$

$$\Phi: S \rightarrow aaaS \mid \wedge,$$

S is the starting symbol.

Self assessment Questions

6. Find the language for the grammar.

$$G = (V_T = \{0,1\}, V_N = \{S\}, \Phi, S)$$

where the set of productions

$$\Phi: S \rightarrow 11S, S \rightarrow 0.$$

7. Find the language L (G), generated by the grammar.

$$G = (V_T = \{x, y, z\}, V_N = \{S, A\}, S, \Phi)$$

where $\Phi: S \rightarrow xS, S \rightarrow yA, A \rightarrow yA, A \rightarrow Z.$

8. Find the language L (G), generated by the grammar

$$G = (V_T = \{a, b\}, V_N = \{S\}, S, \Phi) \text{ where}$$

$$\Phi: S \rightarrow aaS, S \rightarrow a, S \rightarrow b.$$

10.4 Summary

In this unit, we study the formal languages and develop mathematical expressions, phrase structure grammar, a simple device for the construction of useful formal languages. Some types of grammars depending on their productions were discussed. These are useful for generating algorithms.

10.5 Terminal Questions

1. Construct the grammar which generates the following language and also specify their types.

i) $L = \{a^n b^m / n \geq 1, m \geq 3\}$

ii) $L = \{a^n b a^n / n \geq 1\}$

iii) $L = \{a^n b a^m / n \geq 1, m \geq 1\}$

10.6 Answers

Self Assessment Questions

1. Yes, $w \in L(G)$.

2. $\lambda, w, we, wel, well;$

$\lambda, l, ll, ell, well;$

$\lambda, w, e, l, we, el, ll, wel, ell, well.$

3. $xy = 010011, yx = 110100.$

4. $uv = a^2 bab^4 ab^2, |uv| = 11$

$vu = bab^2 a^2 bab^3, |vu| = 11;$

$v^2 = bab^3 ab^2, |v^2| = 8;$

$\lambda u = a^2 bab^2, |\lambda u| = 6$

5. No, Yes, No, No.

6. $L(G) = \{0, 110, 11110, 1111110, \dots\}$

7. $L(G) = \{x^n y^m z / n \geq 0, m \geq 1\}$

8. $L(G) = \{a^{2n+1} / n \geq 0\} \cup \{a^{2n} b / n \geq 0\}$

Terminal Questions

i) $G = (V_T = \{a, b\}, V_N = \{S, B\}, S, \Phi)$

Where Φ is : $S \rightarrow aS, S \rightarrow bbB, B \rightarrow bB, B \rightarrow b.$

It is a regular language.

ii) $G = (V_T = \{a, b\}, V_N = \{S\}, S, \Phi)$

Where Φ is: $S \rightarrow aSa, S \rightarrow b$.

It is a context – free – language.

iii) $G = (V_T = \{a, b\}, V_N = \{S, A\}, S, \Phi)$, where

$\Phi: S \rightarrow aAb, S \rightarrow bAa, A \rightarrow bAa, A \rightarrow aAb, A \rightarrow ab, A \rightarrow ba$.

iv) It is a context – free – language).

Unit 11

Finite Automata

Structure

- 11.1 Introduction
 - Objectives
- 11.2 Basic Terms
- 11.3 Deterministic Finite Automata (DFA)
- 11.4 Transition System (Transition graph)
- 11.5 Language Accepted by a DFA
- 11.6 Summary
- 11.7 Terminal Questions
- 11.8 Answers

11.1 Introduction

A study of finite automaton is their applicability to the design of several common types of computer algorithms and programs. For example, the lexical analysis phase of a compiler (in which program units such as 'begin' and '+' are identified) is often based on the simulation of a finite automaton. Also, the problem of finding an occurrence of a string within another, for example, whether any of the strings air, water, earth, and fire occur in the text of Elements of the Theory of Computation, can also be solved efficiently by methods originating from the theory of finite automata.

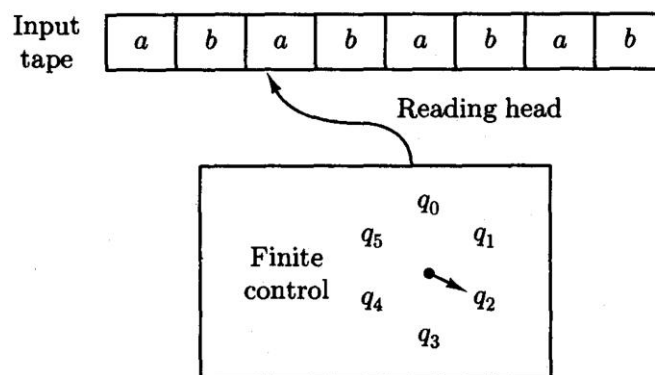


Figure 11.1

Let us now describe the operation of a finite automaton in more detail. Strings are fed into the device by means of an **input tape**, which is divided into squares, with one symbol inscribed in each tape square (see figure 11.1). The main part of the machine itself is a “black box” with innards that can be, at any specified moment, in one of a finite number of distinct internal **states**. This black box - called the **finite control** - can sense what symbol is written at any position on the input tape by means of a movable **reading bead**. Initially, the reading head is placed at the leftmost square of the tape and the finite control is set in a designated **initial state**.

At regular intervals the automaton reads one symbol from the input tape and then enters a new state *that depends only on the current state and the symbol just read*. This is why we shall call this device a *deterministic finite automaton*. After reading an input symbol, the reading head moves one square to the right on the input tape so that on the next move it will read the symbol in the next tape square. This process is repeated again and again; a symbol is read, the reading head moves to the right, and the state of the finite control changes. Eventually the reading head reaches the end of the input string. The automaton then indicates its approval or disapproval of what it has read by the state it is in at the end: if it winds up in one of a set of **final states** the input string is considered to be accepted. The **language accepted by the machine** is the set of strings it accepts.

Objectives:

At the end of the unit, you would be able to

- explain DFA.
- draw transition diagram.
- find the language accepted by a DFA.
- apply the techniques to various finite automata problems.
- know and explain applications of DFA.

11.2 Basic Terms

Input: The various inputs i_1, i_2, \dots, i_p applied at the input side of the model are the elements of an input set, Σ , also called the input alphabet.

Output: The various outputs o_1, o_2, \dots, o_q generated at the output side of the model are the elements of an output set O , also called the output alphabet.

States: The entire automaton system, at any given instant of time, is in any one of the states q_1, q_2, \dots, q_n . (These are labeled with circles)

State relation: State relation helps determine the next state that the automaton system is going to attain. State relation takes into consideration the present input and the present state of the system in determining its next state.

Output relation: It helps to determine the next output of the automaton system. The output relation may take into consideration only the current input or both the current input and the current state for determining the next output.

11.2.1 Definition

An automaton system in which the output depends only on the present input is called a **Moore machine**. Alternatively, an automaton system in which the output depends both on the present input and the present state is called **Mealy machine**.

Self Assessment Questions

1. The symbol Σ is used for _____
2. The symbol O is used for _____
3. In an automaton system, the states are represented by _____
4. State relation helps to determine _____

5. An automaton system in which the output depends only on the present input is called a _____
6. An automaton system in which the output depends both on the present input and the present state is called _____

11.3 Deterministic Finite Automata (DFA)

11.3.1 Definition

A **DFA is 5-tuple** or **quintuple** $M = (Q, \Sigma, \delta, q_0, F)$ where,

Q is non-empty, finite set of states.

Σ is non-empty, finite set of input alphabets.

δ is transition function, which is a mapping from $Q \times \Sigma$ to Q . For this transition function the parameters to be passed are state and input symbol.

Based on the current state and input symbol, the machine may enter into another state.

$q_0 \in Q$ is the start state.

$F \subseteq Q$ is set of accepting or final states.

11.3.2 Note

For each input symbol a , from a given state there is exactly one transition (there can be no transitions from a state also) and we are sure (or can determine) to which state the machine enters. So, the machine is called **Deterministic machine**. Since it has finite number of states the machine is called Deterministic finite machine (automaton).

11.3.3 Illustration

Let us take the pictorial representation of DFA shown in figure 11.2 and understand the various components of DFA.

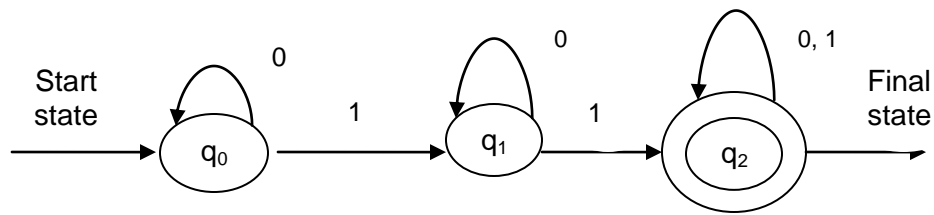


Figure 11.2

It is clear from this diagram that, the DFA is represented using circles, arrows and arcs labeled with some digits, concentric circles etc. The circles are nothing but the states of DFA. In the DFA shown in the figure, there are three states viz., q_0 , q_1 and q_2 . An arrow enters into state q_0 and is not originating from any state and so it is quite different from other states and is called the start state or initial state. The state q_2 has two concentric circles and is also a special state called the final state or accepting state. In this DFA, there is, only one final state. Based on the language accepted by DFA, there can also be more than one final state.

The states other than start state and final states are called intermediate states. Always the machine will initially be in the start state. It is clear from the figure that, the machine in state q_0 , after accepting the symbol 0, stays in state q_0 and after accepting the symbol 1, the machine enters into state q_1 . Whenever the machine enters from one state to another state, we say that there is a transition from one state to another state. Here we can say that there is a transition from state q_0 to q_1 on input symbol 1.

In state q_1 , on input symbol is 0, the machine will stay in q_1 and on symbol 1, there is a transition to state q_2 . In state q_2 , on input symbol 0 or 1, the machine stays in state q_2 only. This DFA has three states q_0 , q_1 and q_2 and can be represented as

$Q = \{q_0, q_1, q_2\}$, the possible input symbols set $\Sigma = \{0, 1\}$, which is set of input symbols (alphabets) for the machine.

There will be a transition from one state to another based on the input alphabets. If there is a transition from v_i , to v_j on an input symbol a , it can be represented as $\delta(v_i, a) = v_j$.

The transitions from each state of the machine shown in figure 11.2 based on the input alphabets $\{0, 1\}$ are shown in table.

Table 11.1

State	input	Output	Transition Representation
q_0	0	q_0	$\delta(q_0, 0) = q_0$
q_0	1	q_1	$\delta(q_0, 1) = q_1$
q_1	0	q_1	$\delta(q_1, 0) = q_1$
q_1	1	q_2	$\delta(q_1, 1) = q_2$
q_2	0	q_2	$\delta(q_2, 0) = q_2$
q_2	1	q_2	$\delta(q_2, 1) = q_2$

Self Assessment Questions

6. Consider the example 11.3.3.

Write the states, input alphabet, final states, starting state.

11.4 Transition System (Transition graph)

A finite directed labeled graph in which each node or vertex of the graph represents a state and the directed edges from one node to another represent transition of a state. All the edges of the transition graph are labeled as input/output. For example, an edge labeled 1/0 specifies that for a certain initial state if the input is 1, then the output is 0.

Consider the following diagram:

In the transition graph as shown in the figure,

- The initial state, q_0 , of the system is represented by a circle with an arrow pointing towards it.
- The final state, q_1 , is represented by two concentric circles.

- The directed edges from the initial state to the final state are labeled as input/output.

11.4.1 Example

The graph represents the DFA,

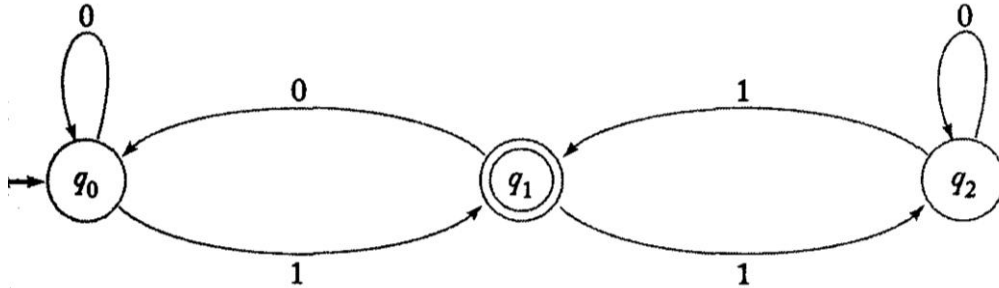


Figure 11.3

$M = (Q = \{q_0, q_1, q_2\}, \Sigma = \{0, 1\}, \delta, q_0 = \text{initial state}, F = \{q_1\})$, where δ is given by

$$\delta(q_0, 0) = q_0,$$

$$\delta(q_0, 1) = q_1,$$

$$\delta(q_1, 0) = q_0,$$

$$\delta(q_1, 1) = q_2,$$

$$\delta(q_2, 0) = q_2,$$

$$\delta(q_2, 1) = q_1.$$

Representation of DFA using Transition table

In this method, the DFA is represented in the tabular form. This table is called transitional table. There is one row for each state, and one column for each input. Since, in the transition diagram shown in the fig., there are three states, there are three rows for each state. The input symbols are only 0 and 1 so, there are two columns for the input symbols. The transitional table for the diagram is given below.

	Σ	
States	0	1
$\rightarrow q_0$	q_0	q_1
q_1	q_1	q_2
q_2	q_2	q_1

Table 11.2

Self Assessment Questions

7. Construct the state table for the following DFA.

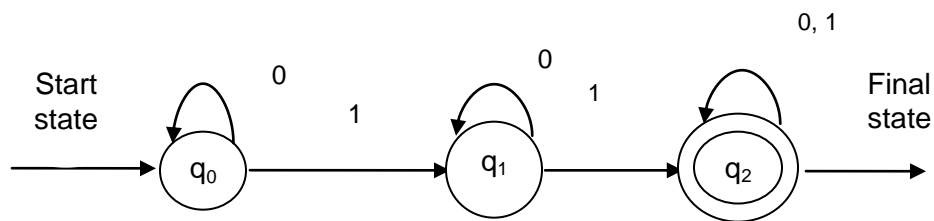


Figure 11.4

11.5 Language Accepted by a DFA

Consider the transition diagram or DFA shown in the figure. The start state is q_0 and the final state is q_2 . To start with, the machine will be in start state q_0 .

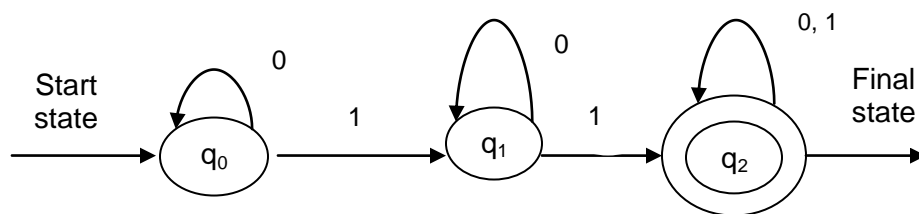


Figure 11.5

Verification of acceptance of the string 1011

Let us assume that the string 1011 is the input. On first input symbol 1, the machine enters into state q_1 . In state q_1 , on input symbol 0, the machine stays in state q_1 only. In state q_1 , on input symbol 1, the machine enters into state q_2 . In state q_2 , on the input symbol 1, the machine stays in state q_2 . Now we encounter end of the input and note that we are in the accepting state q_2 . The moves is made by the DFA for the string 1011. Therefore, after scanning the input string 1011, the machine finally stays in state q_2 .

Verification of non-acceptance of the string 1011

Take the string 0100: The moves made by the machine for the string 0100 are clear from the following figure. Note that after scanning the string 0100 the machine stays in state q_1 which is not a final state. Therefore, the string 0100 is rejected by the machine.

11.5.1 Definition

Let $M = (Q, \Sigma, \delta, q_0, F)$ be a DFA where –

Q is non-empty, finite set of states.

Σ is a non-empty, finite set of input alphabets.

δ is a transition function, which is a mapping from $Q \times \Sigma$ to Q . For this transition function the parameters to be passed are state and input symbol. Based on the current state and input symbol, the machine may enter into another state.

$q_0 \in Q$ is the start (or initial) state.

$F \subseteq Q$ is set of accepting or final states.

The **string** (also called **language**) w **accepted** by a DFA can be defined as follows.

$$L(M) = \{w \mid w \in \Sigma^* \text{ and } \hat{\delta}(q_0, w) \in F\}.$$

Non-acceptance means that after the string is processed, the DFA will not

be in the final state and so the string is rejected. The non-acceptance of the string w by a DFA can be defined in notation as:

$\overline{L(M)} = \{w \mid w \in \Sigma^* \text{ and } \hat{\delta}(q_0, w) \notin F\}$, where $\hat{\delta}: Q \times \Sigma^* \rightarrow Q$, is an extended transition function. The second argument of $\hat{\delta}$ is a string, rather than a single symbol, and its value gives the state the automaton will be in, after reading that string.

(For example, in the above figure 11.5 $\delta(q_0, 1) = q_1$ and $\delta(q_1, 1) = q_2$. So, $\hat{\delta}(q_0, 11) = q_2$).

11.5.2 Properties

1. $\delta(q, \wedge) = \hat{\delta}(q, \wedge) = q$
2. $\delta(q, wa) = \delta(\hat{\delta}(q, w), a)$
3. $\delta(q, aw) = \hat{\delta}(\delta(q, a), w)$, where $q \in Q, a \in \Sigma, w \in \Sigma^*$.

11.5.3 Example

For the DFA shown in fig. given below, what is $\hat{\delta}(q_0, 101)$?

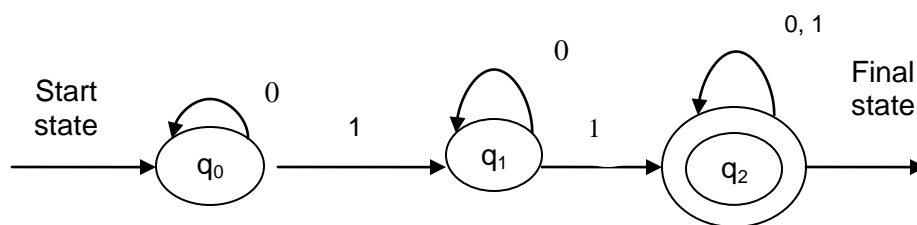


Figure 11.6

Solution:

Property 1: This means that when the current state of the machine is q and when there is no input (\wedge means no input), the machine will not move to any new state, instead, it stays in the same state q .

Property 2: Consider $\hat{\delta}(q_0, 101) = \delta(\hat{\delta}(q_0, 10), 1)$, here $w = 10$ and $a = 1$.

$$\begin{aligned} \text{Now } \hat{\delta}(q_0, 10) &= \delta(\hat{\delta}(q_0, \wedge), 1) \\ &= \delta(q_0, 1) \\ &= q_1. \end{aligned}$$

Therefore, $\hat{\delta}(q_0, 101) = \delta(\hat{\delta}(q_0, 10), 1) = \delta(q_1, 1) = q_2$.

11.5.4 Example

Obtain a DFA to accept strings of *as* and *bs* starting with the string *ab*.

Solution: It is clear that the string should start with *ab* and so, the minimum string that can be accepted by the machine is *ab*.

To accept the string *ab*, we need three states and the machine can be written as –

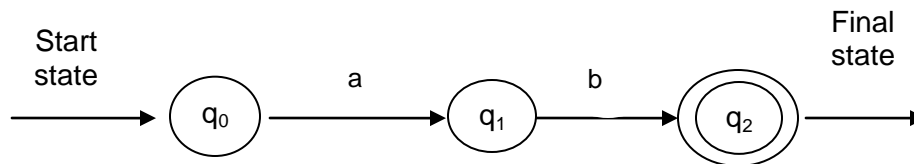


Figure 11.7

where q_2 is the final or accepting state. In state q_0 , if the input symbol is b , the machine should reject b (note that the string should start with a). So, in state q_0 , on input b , we enter into the rejecting state q_3 . The machine for this can be of the form –

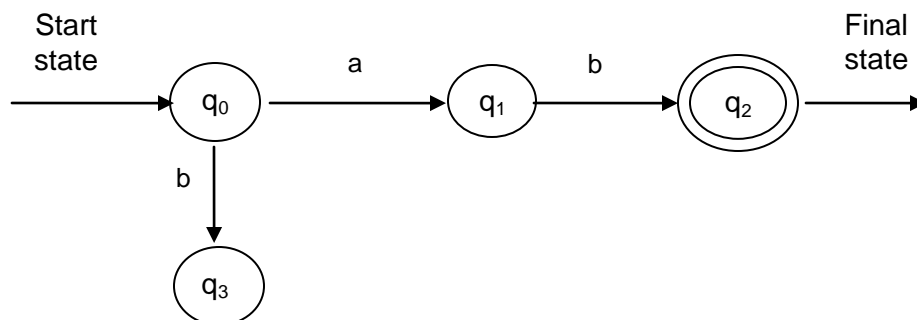


Figure 11.8

The machine will be in state q_1 , if the first input symbol is a . If this a is followed by another a , the string aa should be rejected by the machine. So, in state q_1 , if the input symbol is a , we reject it and enter into q_3 which is the rejecting state. The machine for this can be of the form –

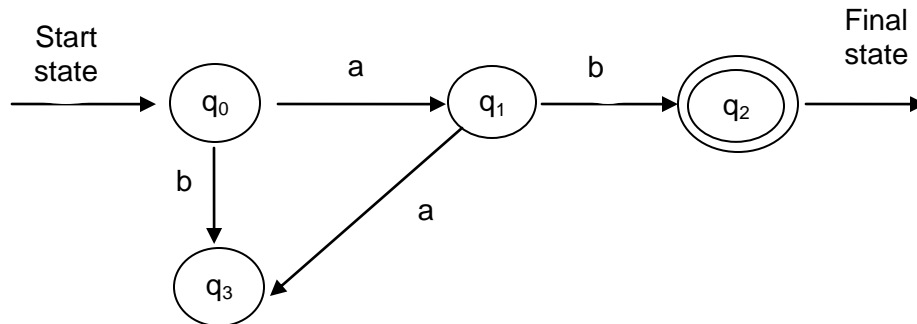


Figure 11.9

Whenever the string is not starting with ab , the machine will be in state q_3 which is the rejecting state. So, in state q_3 , if the input string consists of as and bs of any length, the entire string can be rejected and can stay in state q_3 only.

The resulting machine can be of the form –

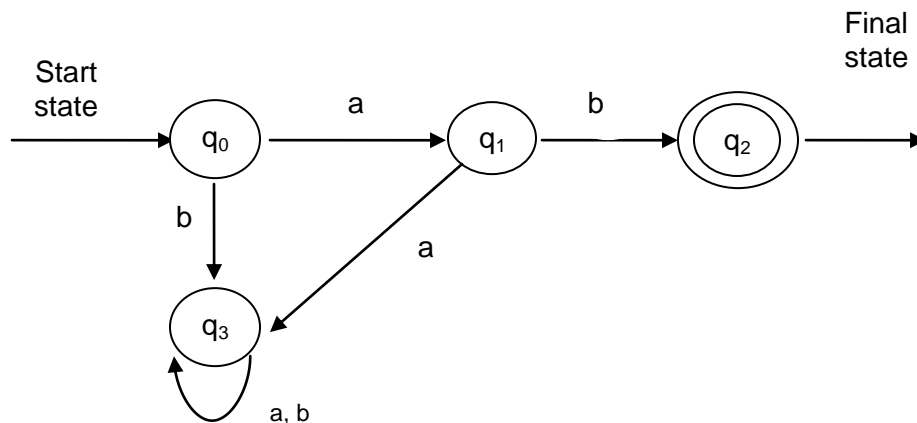


Figure 11.10

The machine will be in state q_2 , if the input string starts with ab . After the string ab , the string containing any combination of as and bs , can be accepted and so remain in state q_2 only. The complete machine to accept the strings of as and bs starting with the string ab is shown in figure 11.10.

The state q_3 is called *trap state* or *rejecting state*.

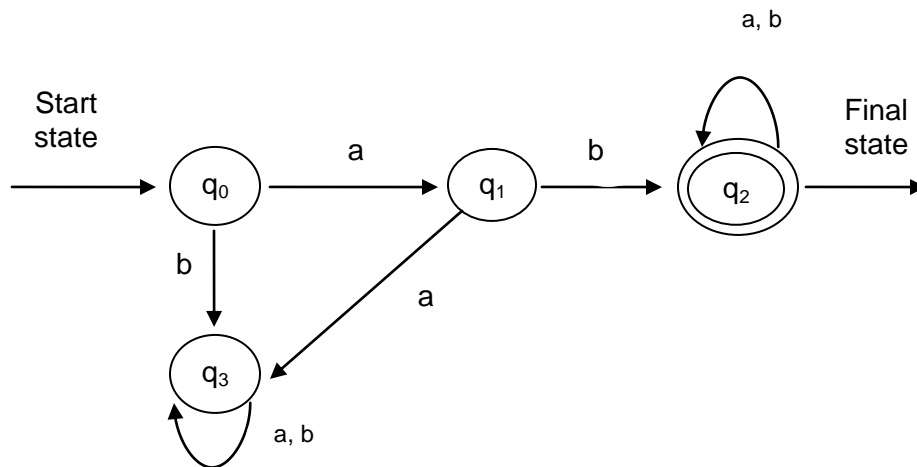


Figure 11.11

In the set notation, the language accepted by DFA can be represented as

$$L = \{ab(a + b)^n \mid n \geq 0\}$$

Or

$$L = \{ab(a + b)^*\}$$

Therefore, the DFA which accepts strings of as and bs starting with the string ab is given by $M = (Q, \Sigma, \delta, q_0, F)$, where

$Q = \{q_0, q_1, q_2, q_3\}$, $\Sigma = \{a, b\}$, q_0 : initial state, $F = \{q_2\}$, and the transition function δ is defined as –

Table 11.3

δ	$\leftarrow \Sigma \rightarrow$	
States	a	b
$\rightarrow q_0$	q_1	q_3
q_1	q_3	q_2
q_2	q_2	q_2
q_3	q_3	q_3

To accept the string abab: The string is accepted by the machine.

$$\begin{aligned}
 \hat{\delta}(q_0, abab) &= \delta(\hat{\delta}(q_0, aba), b) \\
 &= \delta(\delta(\hat{\delta}(q_0, ab), a), b) \\
 &= \delta(\delta(\delta(\delta(q_0, a), b), a), b) \\
 &= \delta(\delta(\delta(q_1, b), a), b) \\
 &= \delta(\delta(q_2, a), b) \\
 &= \delta(q_2, b) \\
 &= q_2 \in F.
 \end{aligned}$$

To reject the string aabb:

$$\begin{aligned}
 \hat{\delta}(q_0, aabb) &= \delta(\hat{\delta}(q_0, aab), b) \\
 &= \delta(\delta(\hat{\delta}(q_0, aa), b), b) \\
 &= \delta(\delta(\delta(\delta(q_0, a), a), b), b) \\
 &= \delta(\delta(\delta(q_1, a), b), b) \\
 &= \delta(\delta(q_3, b), b) \\
 &= \delta(q_3, b) \\
 &= q_3 \notin F.
 \end{aligned}$$

Therefore, the string *aabb* is not accepted by the machine.

11.5.5 Note

Sometimes we ignore the extended notion $\hat{\delta}$ and we use only δ (assuming that the reader is well-aware of it).

11.5.6 Example

Consider a finite automaton that will accept the set of natural numbers, which are divisible by 3,

$M = (Q, \Sigma, q_0, \delta, F)$, where $\Sigma = \{0, 1, 2, \dots, 9\}$, $Q = \{q_0, q_1, q_2\}$

$F = \{q_0\}$, q_0 is the starting state.

$\delta : Q \times I \rightarrow I$ defined by

δ	a	b	c
q_0	q_0	q_1	q_2
q_1	q_1	q_2	q_0
q_2	q_2	q_0	q_1

$a \in \{0, 3, 6, 9\}$, $b \in \{1, 4, 7\}$, $c \in \{2, 5, 8\}$.

Consider the string 142.

$$\begin{aligned}
 \delta(q_0, 142) &= \delta(\delta(q_0, 14), 2) \\
 &= \delta(\delta(\delta(q_0, 1), 4), 2) \\
 &= \delta(\delta(q_1, 4), 2) \\
 &= \delta(q_2, 2) \\
 &= q_1 \notin F
 \end{aligned}$$

Therefore, the string 142 is not accepted by M.

Consider the string 150.

$$\begin{aligned}
 \text{Now } \delta(q_0, 150) &= \delta(\delta(\delta(q_0, 1), 5), 0) \\
 &= \delta(\delta(q_1, 5), 0) \\
 &= \delta(q_0, 0) \\
 &= q_0 \in F
 \end{aligned}$$

Therefore, 150 is accepted by M.

11.5.7 Example

Obtain a DFA to accept even number of as, and odd number of as.

Solution: Observe the following transition diagrams.

Consider the string aa: $\delta(q_0, aa) = \delta(\delta(q_0, a), a) = \delta(q_1, a) = q_0$, which is a final state (acceptable state).

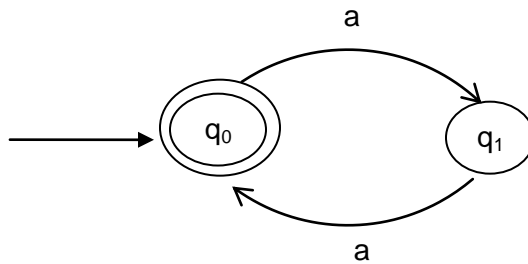


Figure 11.12

Consider the string aaa: $\delta(q_0, aaa) = \delta(\delta(\delta(q_0, aa), a), a) = \delta(\delta(\delta(q_0, a), a), a) = \delta(\delta(q_1, a), a) = \delta(q_0, a) = q_1$, which is an acceptable state.

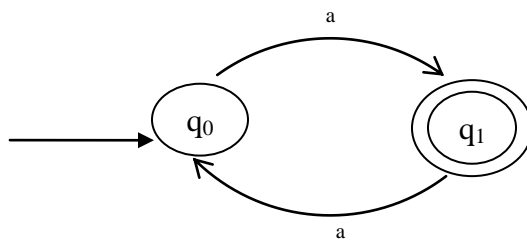


Figure 11.13

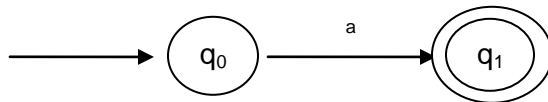
11.5.8 Problem

Obtain DFA to accept strings of as and bs having exactly one a , at least one a , not more than three as .

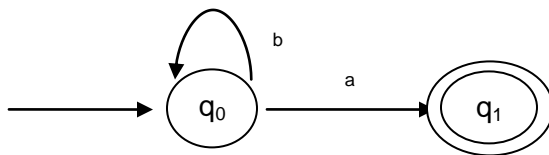
Solution:

To accept exactly one a :

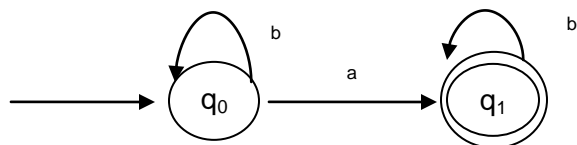
To accept exactly one a , we need two states q_0 and q_1 and make q_1 as the final state. The machine to accept one a is shown below,

**Figure 11.14**

In q_0 , on input symbol b , remain q_0 only so that any number of b 's can end with one a . The machine for this can be of the form,

**Figure 11.15**

In q_1 , on input symbol b , remain q_1 and machine can take the form,

**Figure 11.16**

But, in state q_1 , if the input symbol is a , the string has to be rejected as the machine can have any number of b s but exactly one a . So, the string has to be rejected and we enter into a trap state q_2 . Once the machine enters into trap state, there is no way to come out of the state and the string is rejected by the machine. The complete machine is shown in the figure 11.7:

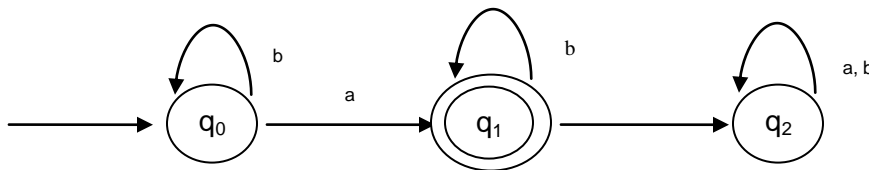


Figure 11.17

In the set notation, the language accepted by DFA can be represented as $L = \{b^m a b^n \mid m, n \geq 0\}$.

The machine $M = (Q, \Sigma, \delta, q_0, F)$, where

$Q = \{q_0, q_1, q_2\}$, $\Sigma = \{a, b\}$, q_0 : initial state, $F = \{q_1\}$, and the transition function δ is defined as:

Table 11.4

δ	$\leftarrow \Sigma \rightarrow$	
States	a	b
$\rightarrow q_0$	q_1	q_0
q_1	q_2	q_1
q_2	q_2	q_2

The machine to accept at least one a : The minimum string that can be accepted by the machine is a . For this, we need two states q_0 and q_1 where q_1 is the final state. The machine for this is shown below:

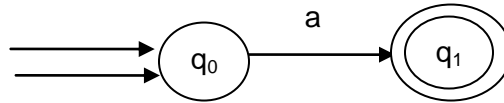


Figure 11.18

In state q_0 , if the input symbol is b , remain in q_0 . Once the final state q_1 is reached, whether the input symbol is a or b , the entire string has to be accepted. The machine to accept at least one a is shown in fig.:

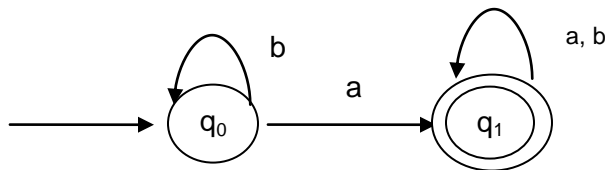


Figure 11.19

In set notation, the language accepted DFA can be represented as,

$$L = \{b^m a (a + b)^n \mid m, n \geq 0\}.$$

The machine $M = (Q, \Sigma, \delta, q_0, F)$, where

$Q = \{q_0, q_1\}$, $\Sigma = \{a, b\}$, q_0 : initial state, $F = \{q_1\}$, and the transition function δ is defined as

Table 11.5

δ	$\leftarrow \Sigma \rightarrow$	
States	a	b
$\rightarrow q_0$	q_1	q_0
$\bigcirc q_1$	q_1	q_1

The machine to accept not more than three as: The machine should accept

not more than three *as* means,

It can accept zero *as*

It can accept one *a*

It can accept two *as*

It can accept 3 *as*

But, it cannot accept more than three *as*.

In this machine maximum of three *as* can be accepted (that is, the machine can accept zero *as*, one *a*, two *as*). So, we need maximum four states q_0 , q_1 , q_2 and q_3 where all these states are final states and q_0 is the start state.

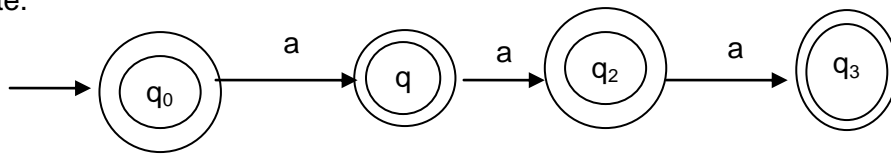


Figure 11.20

In state q_3 , if the input symbol is *a*, the string has to be rejected and we enter into a trap state q_4 . Once this trap state is reached, whether the input symbol is *a* or *b*, the entire string has to be rejected and remain in state q_4 . Now, the machine can take the form as shown below,

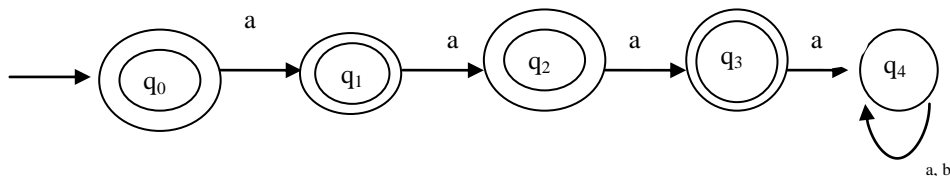


Figure 11.21

In state q_0 , q_1 , q_2 and q_3 , if the input symbol is *b*, stay in their respective states and the final transition diagram is shown below.

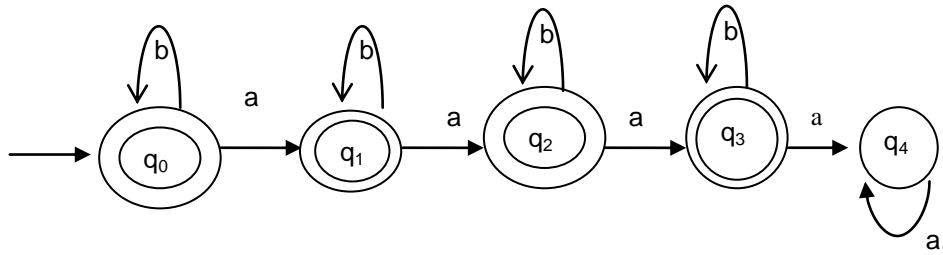






Figure 11.22

In set notation, the language accepted DFA can be represented as,

$$L = \{b^i a b^j a b^k a b^l \mid i, j, k, l \geq 0\}$$

The DFA is $M = (Q, \Sigma, \delta, q_0, F)$ where $Q = \{q_0, q_1, q_2, q_3, q_4\}$, $\Sigma = \{a, b\}$, q_0 is the start state, $F = \{q_0, q_1, q_2, q_3\}$, and δ is the transition function.

Table 11.6

δ	$\leftarrow \Sigma \rightarrow$	
States	a	b
\rightarrow 	q ₁	q ₀
	q ₂	q ₁
	q ₃	q ₂
	q ₄	q ₃
q ₄	q ₄	q ₄

11.5.9 Problem

Obtain a DFA to accept the language $L = \{w \mid |w| \bmod 5 \neq 0\}$ on $\Sigma = \{a, b\}$.

Solution: The number of symbols in a string consisting of *as* and *bs* should not have multiples of 5. The machine to accept the corresponding language is shown below:

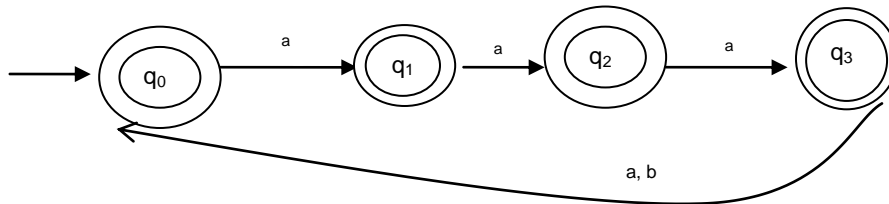


Figure 11.23

Self Assessment Questions

8. Draw a DFA to accept strings of *as* and *bs* with even number of *as* and even number of *bs*. Also find the language accepted by DFA.

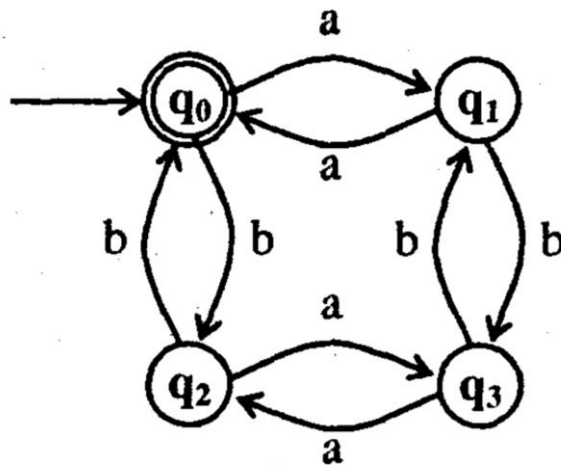


Figure 11.24

11.6 Summary

The concept of finite automata is used in wide applications. Large natural vocabularies can be described using finite automaton, which includes the

applications such as spell checkers and advisers, multi-language dictionaries, to indent and documents, in calculators to evaluate complex expressions based on the priority of an operator etc. In this unit, we have given a comprehensive idea about the DFA and a graphical representation of DFA. Further, we discussed the language accepted by DFA with certain examples.

11.7 Terminal Questions

1. What is DFA ? Explain with example.
2. When do we say that a language is accepted by the machine? Illustrate with example.
3. Obtain a DFA to accept strings of 0s and 1s starting with at least two 0s and ending with at least two 1s. Also find the language accepted by this.
4. Obtain a DFA to accept strings of as and bs with at most two consecutive bs.

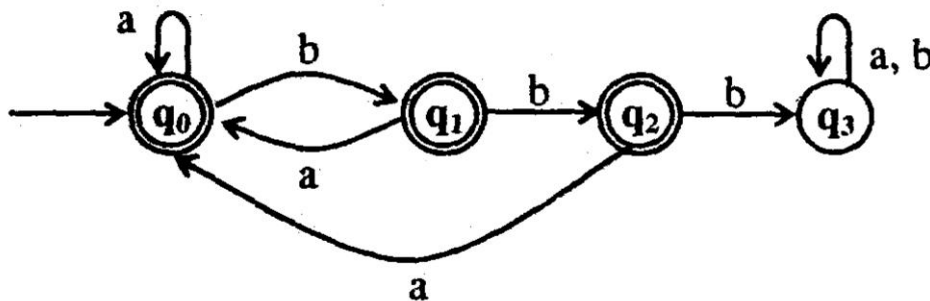


Figure 11.25

11.8 Answers

Self Assessment Questions

1. Input alphabet.
2. Output alphabet.
3. These are labeled with circles.
4. The next state that the automaton system is going to attain.

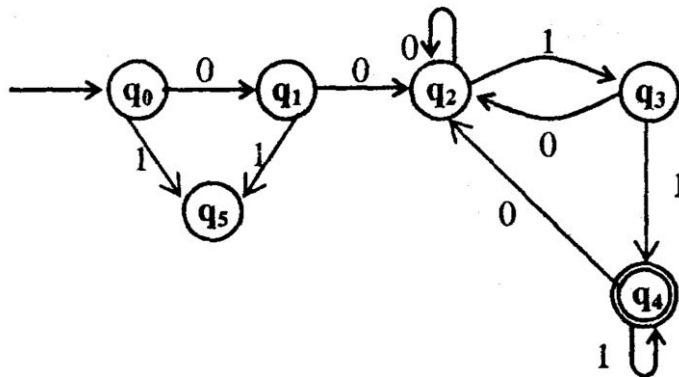
5. Moore machine; Mealy machine.
6. States: $\{q_0, q_1, q_2\}$, Input alphabet: $\{0, 1\}$, final state: $\{q_2\}$, starting state $\{q_0\}$.
- 7.

	Σ	
State	0	1
s		
$\rightarrow q_0$	q_0	q_1
q_1	q_1	q_2
q_2	q_2	q_2

8. The language accepted by DFA is –
 $L = \{w \mid w \in (a + b)^*$ and total number of strings in both a and b are even $\}$.

Terminal Questions

- 3.



The language accepted by DFA can be represented as
 $L = \{w \mid w \in 00(0+1)^*11\}$

Unit 12

Basic Graph Theory

Structure

- 12.1 Introduction
 - Objectives
- 12.2 Definitions and Examples
- 12.3 Adjacency and Degree
- 12.4 Subgraphs
- 12.5 Trees
- 12.6 Properties of Trees
- 12.7 Rooted Trees and Applications
- 12.8 Summary
- 12.9 Terminal Questions
- 12.10 Answers

12.1 Introduction

Graph theory was introduced in 1736 with Euler's paper in which he solved the Kongsberg Bridges problem. In 1847, Kirchhoff (1824 - 87) developed the theory of trees to applications in electrical networks. Cayley discovered trees while he was trying to enumerate the isomers of $(C_n H_{2n+2})$. The last three decades have witnessed more interest in Graph Theory, particularly among applied mathematicians and engineers. Graph Theory has a surprising number of applications in many developing areas. The Graph Theory is also intimately related to many branches of mathematics including Group Theory, Matrix Theory, Automata and Combinatorics. One of the features of Graph Theory is that it depends very little on the other branches of mathematics. Graph Theory serves as a mathematical model for any system involving a binary relation. One of the attractive features of Graph Theory is its inherent pictorial character. The development of high-speed computers is also one of the reasons for the recent growth of interest in Graph Theory.

Objectives:

At the end of the unit, you would be able to

- appreciate the relevance of Graph Theory in real life situation
- explain different fundamental definitions
- observe the difference between different concepts defined with the examples
- explain some techniques used in proving simple theorems
- find the sub-graphs of a given graph.
- study connected graphs without any circuits (called trees).
- explain some properties of trees.

12.2 Definitions and Examples**12.2.1 Definition**

- A **linear graph** (or simply a **graph**). $G = (V, E)$ consists of a nonempty set of objects, $V = \{v_1, v_2, \dots\}$ called **vertices** and another set, $E = \{e_1, e_2, \dots\}$ of elements called **edges** such that each edge ' e_k ' is identified with an unordered pair $\{v_i, v_j\}$ of vertices. The vertices v_i, v_j associated with edge e_k are called the **end vertices** of e_k .
- An edge associated with a vertex pair $\{v_i, v_i\}$ is called a **loop** (or) **selfloop**.
- If there are more than one edge associated with a given pair of vertices, then these edges are called **parallel edges** (or) **multiple edges**.

12.2.2 Example

Consider the graph given here,

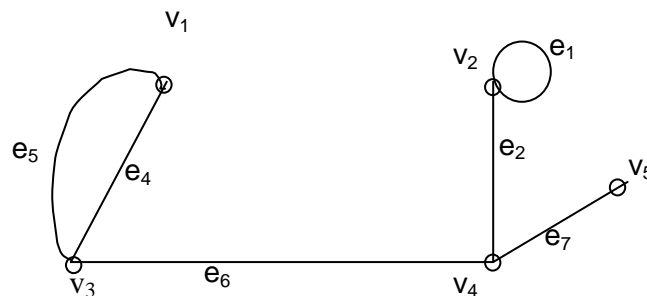


Figure 12.1

This is a graph with five vertices and six edges. Here $G = (V, E)$ where

$V = \{v_1, v_2, v_3, v_4, v_5\}$ and $E = \{e_1, e_2, e_4, e_5, e_6, e_7\}$.

The identification of edges with the unordered pairs of vertices is given by

$e_1 \leftrightarrow \{v_2, v_2\}$, $e_2 \leftrightarrow \{v_2, v_4\}$, $e_4 \leftrightarrow \{v_1, v_3\}$, $e_5 \leftrightarrow \{v_1, v_3\}$, $e_6 \leftrightarrow \{v_3, v_4\}$.

Here ' e_1 ' is a loop and e_4, e_5 are parallel edges.

12.2.3 Definition

A graph that has neither self-loops nor parallel edges is called a **simple graph**. Graph containing either parallel edges or loops is referred as **general graph**. A graph 'G' with a finite number of vertices and a finite number of edges is called a **finite graph**. A graph 'G' that is not a finite graph is said to be an **infinite graph**.

Observation: The two graphs given below are one and the same.

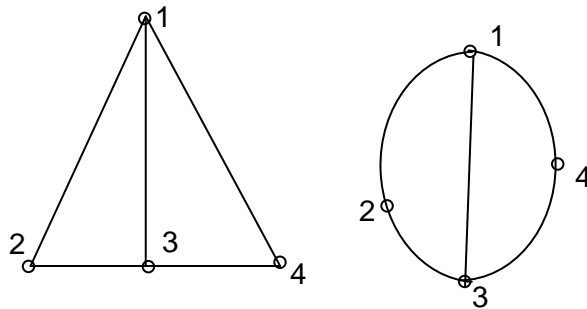


Figure 12.2

12.2.4 Example

Consider the following three graphs;

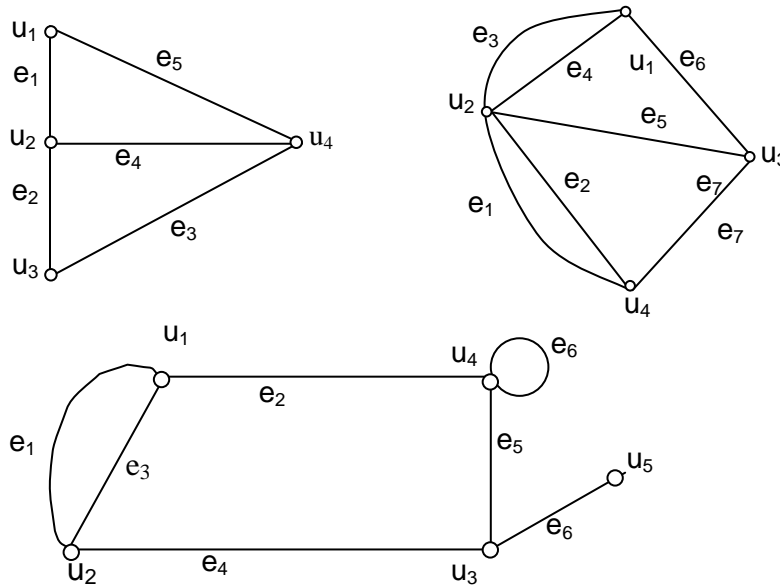


Figure 12.3

It can be observed that the number of vertices, and the number of edges are finite. Hence these three graphs are finite graphs.

Consider the two graphs given here. It can be understood that the number of vertices of these two graphs is not finite. So we conclude that these two figures represent infinite graphs.

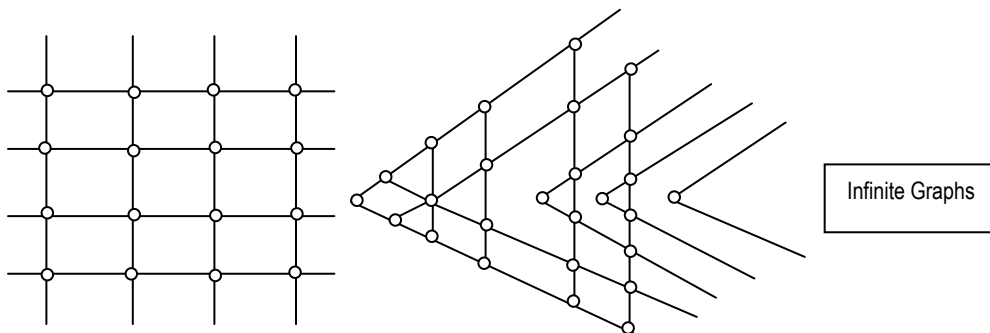


Figure 12.4

12.2.5 Example

The diagrams of fig. 12.5(a) and 12.5 (b) illustrate two non directed graphs. The graph G , shown in Fig. 12.5(a) is not simple since there is a loop incident on vertex c .

The graph G^1 shown in Fig. (b) is simple since there are no self loops and parallel edges.

The graph G^{11} in fig. (c) represents a multi-graph since there are three edges between the vertices b and c .

$V(G) = \{a, b, c, d\}$ and $E(G) = \{\{a, b\}, \{a, c\}, \{b, c\}, \{c, c\}, \{a, d\}, \{c, d\}\}$. Therefore, G is of order 4 and size 6.

Similarly, the graph G^1 has order 4 and size 5, and the multi-graph G^{11} has order 4 and size 7.

Observation: The non-directed graphs may be viewed as symmetric directed graphs, in which for every edge (u, v) between two vertices in direction there is also an edge (v, u) between the same vertices in the other direction.

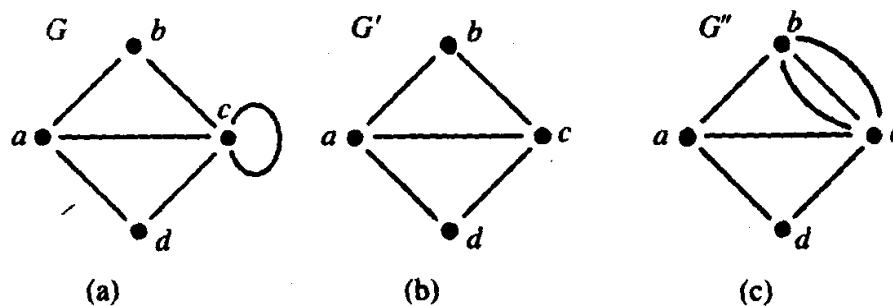


Figure 12.5

12.2.6 Definition

If a vertex v is an end vertex of some edge e , then v and e are said to be **incident** with (or on, or to) each other.

12.2.7 Example

Consider the graph given in Fig. 12.6 Here the edges e_2 , e_6 , e_7 are incident with the vertex u_4 .

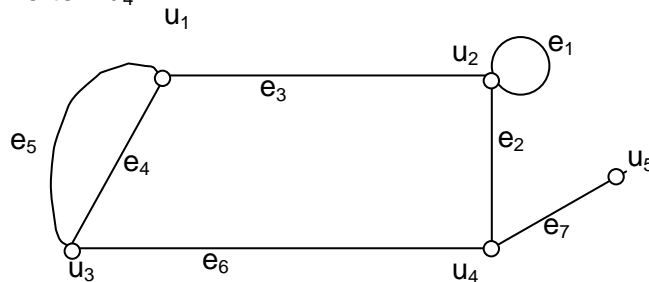


Figure 12.6

12.3 Adjacency and Degree**12.3.1 Definition**

- (i) Two non-parallel edges are said to be **adjacent** if they are incident on a common vertex.
- (ii) Two vertices are said to be **adjacent** if they are the end vertices of the same edge.

12.3.2 Example

Consider the graph given. Here the vertices u_4 , u_5 are adjacent. The vertices u_1 and u_4 are not adjacent. The edges e_2 and e_3 are adjacent.

12.3.3 Definition

The number of edges incident on a vertex v is called the **degree (or valency)** of v . The degree of a vertex v is denoted by $d(v)$. It is to be noted that a self-loop contributes two to the degree of the vertex.

12.3.4 Example

Consider the graph given in Fig. 12.7. Here $d(u_1) = 2$; $d(u_2) = 1$; $d(u_3) = 3$; $d(u_4) = 2$; $d(u_5) = 2$; $d(u_6) = 2$; $d(u_7) = 1$; $d(u_8) = 3$; $d(u_9) = 2$; $d(u_{10}) = 2$.

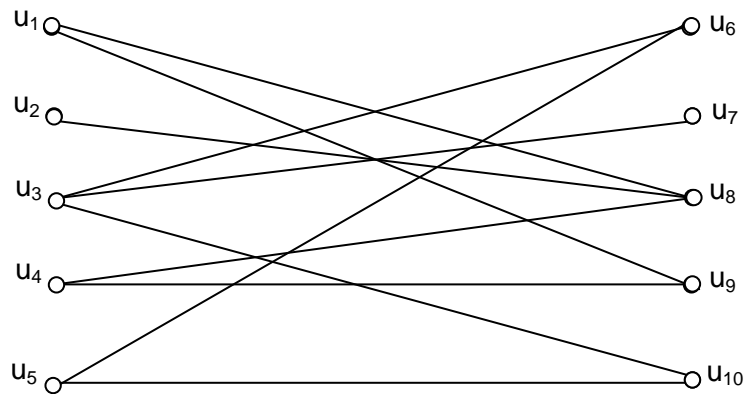


Figure 12.7

12.3.5 Example

Consider the graph given in Fig. 12.8

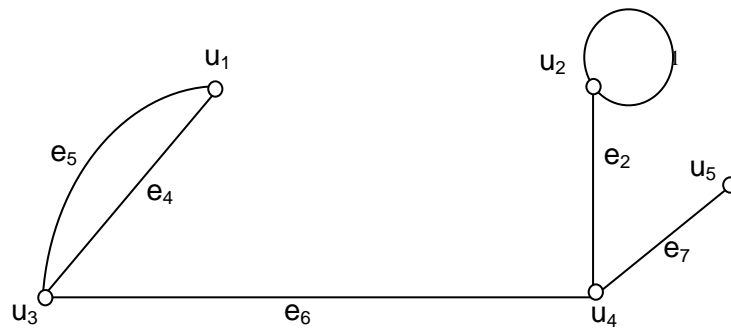


Figure 12.8

Here $d(u_1) = 2$, $d(u_3) = d(u_4) = 3$; $d(u_2) = 3$; $d(u_5) = 1$

So, $d(u_1) + d(u_2) + d(u_3) + d(u_4) + d(u_5) = 2 + 3 + 3 + 3 + 1 = 12 = 2(6) = 2e$, where e denotes the number of edges. Hence we can observe that

$d(u_1) + d(u_2) + d(u_3) + d(u_4) + d(u_5) = 2e$ (that is, the sum of the degrees of all vertices is equal to twice the number of edges).

12.3.6 Theorem

The sum of the degrees of the vertices of a graph G is twice the number of

edges. That is, $\sum_{v_i \in V} d(v_i) = 2e$. (Here e is the number of edges).

Proof: (The proof is by induction on the number of edges 'e').

Case-(i): Suppose $e = 1$. Suppose f is the edge in G with $f = uv$.

Then $d(v) = 1, d(u) = 1$. Therefore,

$$\begin{aligned}\sum_{x \in V} d(x) &= \sum_{x \in V \setminus \{u, v\}} d(x) + d(u) + d(v) \\ &= 0 + 1 + 1 \\ &= 2 \\ &= 2 \times 1 \\ &= 2 \times (\text{number of edges}).\end{aligned}$$

Hence the given statement is true for $n = 1$.

Now we can assume that the result is true for $e = k - 1$.

Take a graph G with k edges. Now consider an edge 'f' in G whose end points are u and v . Remove f from G . Then we get a new graph $G^* = G - \{f\}$.

Suppose $d^*(v)$ denotes the degree of vertices v in G^* . Now for any $x \notin \{u, v\}$, we have $d(x) = d^*(x)$, and $d^*(v) = d(v) - 1, d^*(u) = d(u) - 1$.

Now G^* has $k - 1$ edges. So by induction hypothesis –

$$\sum_{v_i \in V} d^*(v_i) = 2(k - 1).$$

$$\begin{aligned}\text{Now } 2(k - 1) &= \sum_{v_i \in V} d^*(v_i) = \sum_{v_i \notin \{u, v\}} d^*(v_i) + d^*(u) + d^*(v) \\ &= \sum_{v_i \notin \{u, v\}} d(v_i) + (d(u) - 1) + (d(v) - 1) \\ &= \sum_{v_i \notin \{u, v\}} d(v_i) + d(u) + d(v) - 2 \\ &= \sum_{v_i \in V} d^*(v_i) - 2\end{aligned}$$

$$\Rightarrow 2(k - 1) + 2 = \sum_{v_i \in V} d^*(v_i) \Rightarrow 2k = \sum_{v_i \in V} d(v_i)$$

Hence by induction we get that “the sum of the degrees of the vertices of the graph G is twice the numbers of edges”.

12.3.7 Theorem

The number of vertices of odd degrees is always even.

Proof: We know that the sum of degrees of all the ‘ n ’ vertices (say, v_i , $1 \leq i \leq n$) of a graph G is twice the number of edges (e) of G . So we have,

$$\sum_{i=1}^n d(v_i) = 2e \text{ ----- (i)}$$

If we consider the vertices of odd degree and even degree separately, then –

$$\sum_{i=1}^n d(v_i) = \sum_{v_j \text{ is even}} d(v_j) + \sum_{v_k \text{ is odd}} d(v_k) \text{ ----- (ii)}$$

Since the L.H.S of (ii) is even (from (i)) and the first expression on the RHS side is even, we have that the second expression on RHS is always even.

Therefore ,

$$\sum_{v_k \text{ is odd}} d(v_k) \text{ is an even number ----- (iii)}$$

In (iii), each $d(v_k)$ is odd. The number of terms in the sum must be even to make the sum an even number. Hence the number of vertices of odd degree is even.

12.3.8 Example

Show that the number of people who dance (at a dance where the dancing is done in couples) an odd number of times is even.

Solution: Suppose the people are vertices. If two people dance together, then we can consider it as an edge. Then the number of times a person v danced is $\delta(v)$. By Theorem 9.5.9, the number of vertices of odd degree is even. Therefore, the number of people who dance odd number of times is even.

12.3.9 Definition

A vertex having no incident edge is called an **isolated vertex**. In other words, a vertex v is said to be an isolated vertex if the degree of v is equal to zero.

12.3.10 Example

Consider the graph given in Fig. The vertices v_4 and v_7 are isolated vertices.

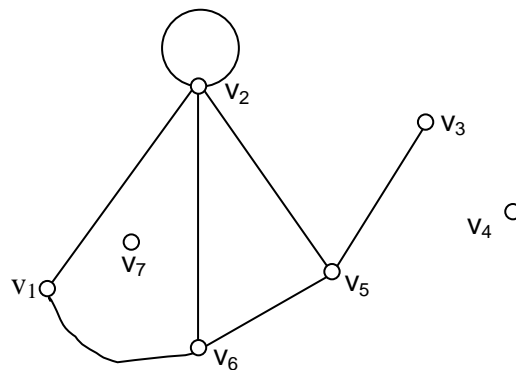


Figure 12.9

12.3.11 Definition

A vertex of degree one is called a **pendent vertex** or an **end vertex**. Two adjacent edges are said to be in **series** if their common vertex is of degree two.

12.3.12 Example

In the Example 12.3.10, the vertex ' v_3 ' is of degree 1, and so it is a pendent vertex. The two edges incident on v_1 are in series.

12.3.13 Definition

The **minimum** of all the degrees of the vertices of a graph G is denoted by $\delta(G)$, and the **maximum** of all the degrees of the vertices of G is denoted by $\Delta(G)$. If $\delta(G) = \Delta(G) = k$, that is, if each vertex of G has degree k , then G is said to be **k -regular** or regular of degree k . 3-regular graphs are called **cubic** graphs.

12.3.14 Example:

- (i) Consider the graph G given in Fig (a). It is easy to observe that the degree of every vertex is equal to 3. Hence the graph G is a regular graph of degree 3.

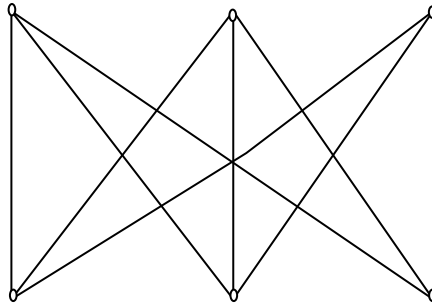


Figure 12.10

- (ii) The following graph fig (b) is a regular graph of degree-4.

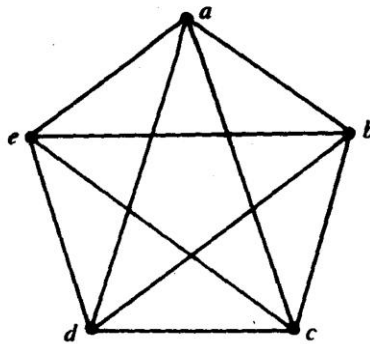


Figure 12.11

12.3.15 Definition

If v_1, v_2, \dots, v_n are the vertices of G , then the sequence (d_1, d_2, \dots, d_n) where $d_i = \text{degree}(v_i)$, is the **degree sequence** of G . Usually, we order the vertices so that the degree sequence is monotone increasing, that is, so that $\delta(G) = d_1 \leq d_2 \leq \dots \leq d_n = \Delta(G)$.

12.3.16 Example

The vertex c of the graph G in Example 12.2.5 is degree 5 while the degree of c in G^1 is 3. The degree sequence of G is $(2, 2, 3, 5)$ while the degree sequence of G^1 is $(2, 2, 3, 3)$.

12.3.17 Definition

A graph $G = (V, E)$ is said to be a **null graph** if $E = \phi$.

12.3.18 Example

The graph G given in Fig, contains no edges and hence G is a null graph.

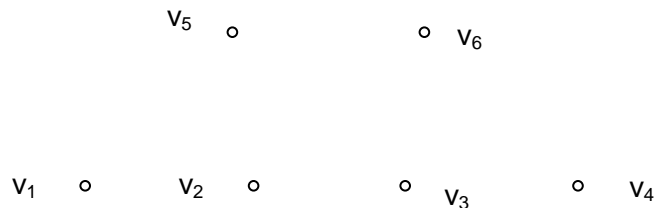


Figure 12.12

12.3.19 Definition

In a non-directed graph G a sequence P of zero or more edges of the form $\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{n-1}, v_n\}$, (in this repetition of vertex is allowed) is called a path from v_0 to v_n . The vertex v_0 is called the **initial** vertex and v_n is the **terminal** vertex, and they both are called endpoints of path P .

We denote this path P as a $v_0 - v_n$ path. If $v_0 = v_n$ then it is called a **closed** path, and if $v_0 \neq v_n$ then it is called an **open** path.

12.3.20 Definition

A path P may have no edges at all, in which case, the length of P is zero, P is called a **trivial** path, and $V(P) = \{v_0\}$. A path P is **simple** if all edges and vertices on the path are distinct except possibly the endpoints. Two paths in a graph are said to be **edge-disjoint** if they share no common edges; they are vertex-disjoint if they share no common vertices.

12.3.21 Note

An open simple path of length n has $n + 1$ distinct vertices and n distinct edges, while a closed simple path of length n has n distinct vertices and n distinct edges. The trivial path is taken to be a simple closed path of length zero.

12.3.22 Definition

A path of length ≥ 1 with no repeated edges and whose endpoints are equal is called a **circuit**. A circuit may have repeated vertices other than the endpoints; a **cycle** is a circuit with no other repeated vertices except its endpoints.

Observation

- A cycle is a simple circuit, and, in particular, a loop is a cycle of length 1.
- In a graph, a cycle that is not a loop must have length at least 3, but there may be cycles of length 2 in a multi-graph.

12.3.23 Example

Consider the graphs given in example 12.2.5.

- (i) The path $\{c, c\}$ is a cycle of length 1; the sequence of edges $\{a, b\}$, $\{b, c\}$, $\{c, a\}$ and $\{a, d\}$, $\{d, c\}$, $\{c, a\}$ form cycles of length 3.
- (ii) The path $\{a, b\}$, $\{b, c\}$, $\{c, d\}$, $\{d, a\}$ is a cycle of length 4.
- (iii) The sequence $\{a, b\}$, $\{b, c\}$, $\{c, c\}$, $\{c, a\}$ is a circuit of length 4; it is not a cycle because the sequence of vertices $a-b-c-c-a$ includes more than one repeated vertex. Similarly the sequence of edges $\{a, b\}$, $\{b, c\}$, $\{c, a\}$, $\{a, d\}$, $\{d, c\}$, $\{c, a\}$ forms a closed path of length 6, but this path is not a circuit because the edge $\{c, a\}$ is repeated twice.

12.3.24 Example

Consider the following graph:

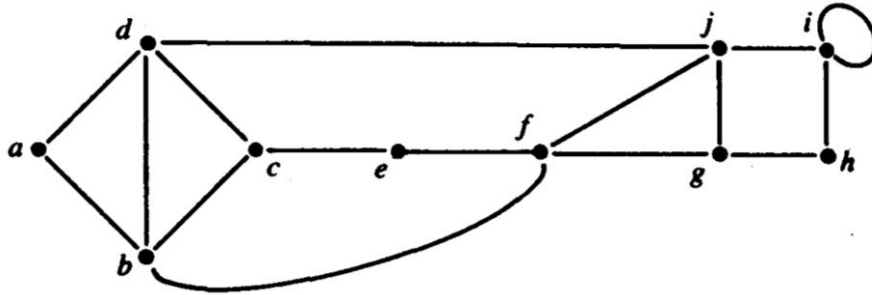


Figure 12.13

Table 12.1

Path	Length	Simple (yes/no)	Closed (yes/no)	Circuit (yes/no)	Cycle (yes/no)
a-d-c-e-g-j-d-a	7	no	yes	no	no
b-c-e-f-g-j-f-b	7	no	yes	yes	no
a-b-a	2	No	Yes	No	No
a-d-c-b-a	4	Yes	Yes	Yes	Yes
i-i	1	Yes	Yes	Yes	Yes
a	0	Yes	Yes	No	No
e-f-g-j-f-b	5	No	No	No	No
d-b-c-d	3	yes	yes	yes	Yes

Observation: A simple path is certainly a path and the converse statement need not be true.

12.3.25 Theorem

In a graph G , every u - v path contains a simple u - v path.

Proof: If a path is a closed path, then it indeed contains the trivial path.

Assume that P is an open u - v path.

Use induction on the length of path: If P has length one, then P is itself a simple path. Induction hypo: Suppose that all open u - v paths of length k , where $1 \leq k \leq n$, contains a simple u - v path.

Now suppose that P is the open u - v path $\{v_0, v_1\}, \dots, \{v_n, v_{n+1}\}$ where $u = v_0$ and $v = v_{n+1}$. It may be that P has repeated vertices, but if not, then P is a simple u - v path.

If there are repeated vertices in P , let i and j be distinct positive integers where $i < j$ and $v_i = v_j$. If the closed path v_i - v_j is removed from P , an open path P^1 is obtained having length $\leq n$ since at least the edge $\{v_i, v_{i+1}\}$ was deleted from P . Therefore, by the inductive hypothesis, P^1 contains a simple u - v path. Hence P contains simple u - v path.

Self Assessment Questions

1. Find the degree of all the vertices of the graph G given in 12.2.7 (Incidence and degree)
2. Can a simple graph exist with 15 vertices each of degree five.
3. How many vertices does a regular graph of degree 4 with 10 edges have ?
4. Is there a non-simple graph G with degree sequence $(1, 1, 3, 3, 3, 4, 6, 7)$?

12.4 Subgraphs

12.4.1 Definition

A graph H is said to be a **sub-graph** of a graph G if all the vertices and all the edges of H are in G , and each edge of H has the same end vertices in H as in G .

12.4.2 Example

The graphs H and K are subgraphs of graph G .

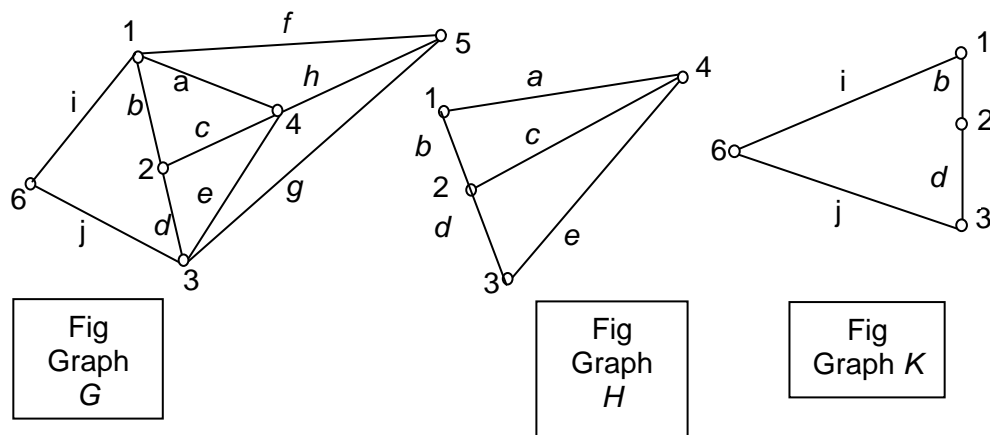


Figure 12.14

Observations:

- Every graph is a subgraph of itself;
- A subgraph of a subgraph of G is a subgraph of G ;
- A single vertex in a graph G is a subgraph of G ; and
- A single edge in G together with its end vertices is a subgroup of G .

12.4.3 Definition

Two subgraphs G_1 and G_2 of a graph G are said to be **edge-disjoint** if G_1 and G_2 do not have any edges in common. The subgraphs that do not have vertices in common are said to be **vertex disjoint**.

12.4.4 Example

Observe the two graphs given in Figures A and B below. These two graphs are subgraphs of the graph given in the Figure-C. There are no common edges in these two subgraphs. Hence these two subgraphs are edge disjoint subgraphs.

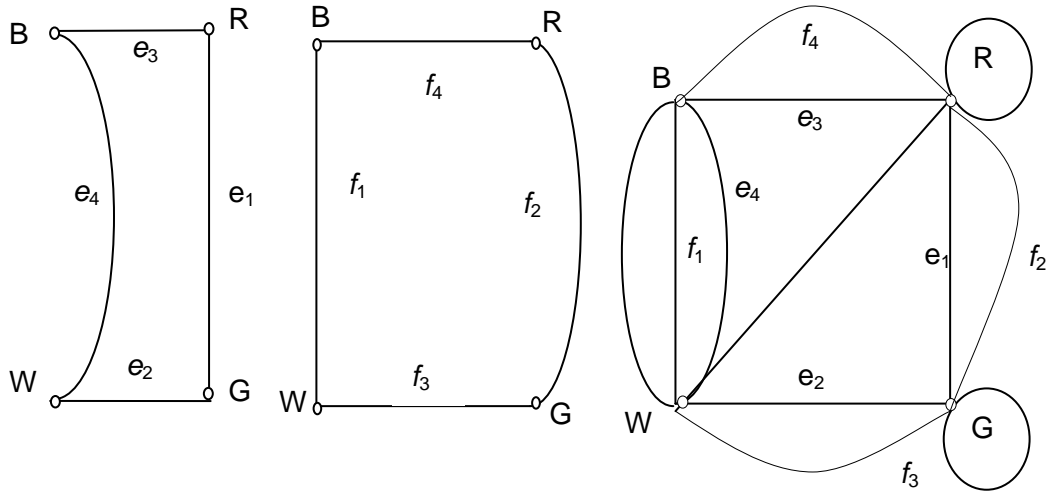


Figure 12.15 A

Figure 12.15 B

Figure 12.15 C

12.4.5 Definition

If H is a sub-graph of G, then the complement of H in G, denoted by $\overline{H}(G)$, is the subgraph $G-E(H)$; that is, the edges of H are deleted from those of G.

12.4.6 Example

Consider the graph G, subgraph H of G, and the complement of H in G.

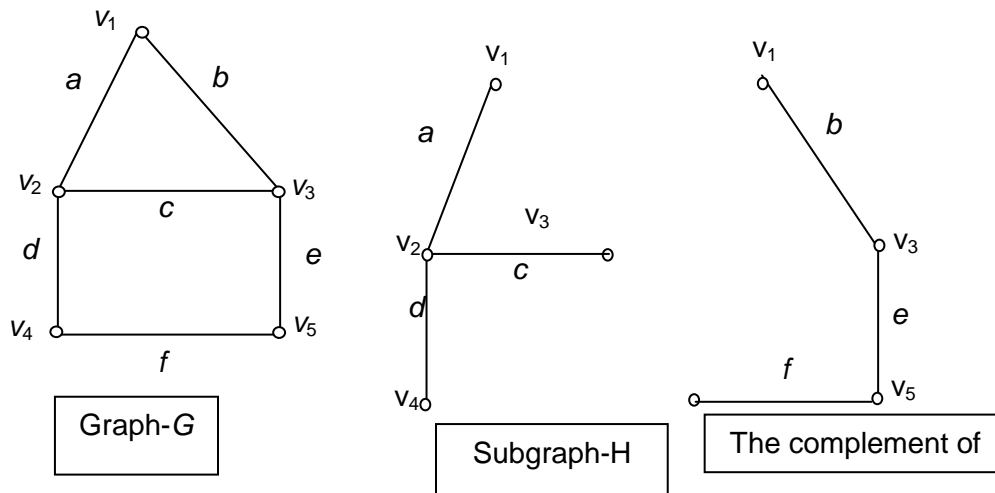


Figure 12.16

12.5 Trees

The concept of a ‘tree’ plays a vital role in the theory of graphs. First we introduce the definition of ‘tree’, study some of its properties and its applications. We also provide equivalent conditions for a tree.

12.5.1 Definition

A connected graph without circuits is called a **tree**.

12.5.2 Example

Trees with one, two, three and four vertices are given in the Fig. below:

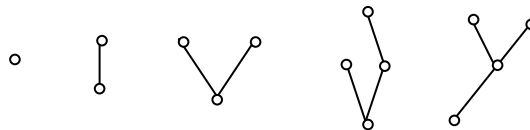


Figure 12.17

12.5.3 Example

Consider the two trees $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ where

$$V = \{a, b, c, d, e, f, g, h, i, j\}$$

$$E_1 = \{\{a, c\}, \{b, c\}, \{c, d\}, \{c, e\}, \{e, g\}, \{f, g\}, \{g, i\}, \{h, i\}, \{i, j\}\}$$

$$E_2 = \{\{c, a\}, \{c, b\}, \{c, d\}, \{c, f\}, \{f, e\}, \{f, i\}, \{g, d\}, \{h, e\}, \{j, g\}\}$$

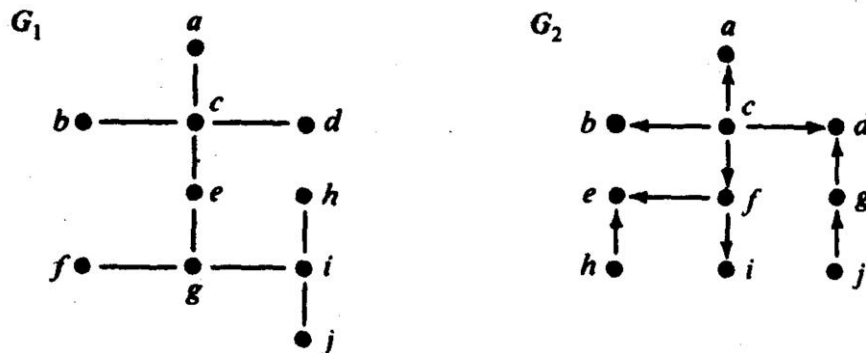


Figure 12.18

Neither of these two trees is a directed tree.

If vertex c is designated as the root of each tree, vertex j is a level 4 in G_1 and at level 3 in G_2 .

12.5.4 Example

A directed tree T is shown in the following fig. Here $T = (V, E)$ where $V = \{a, b, c, d, e, f, g, h\}$ and $E = \{(a, b), (a, c), (a, d), (b, e), (d, f), (e, g), (e, h)\}$. The root of T is the vertex a and the vertices at level 2 are e and f .

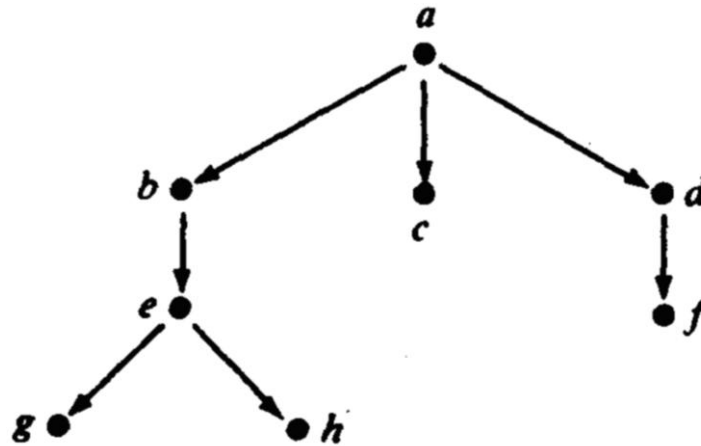


Figure 12.19

12.5.5 Note

Directed trees are conventionally drawn with the root at the top and all edges going from the top of the page toward the bottom so that the direction of edges is sometimes not explicitly shown.

Observations

- Since a tree is a graph, we have that a tree contains at least one vertex.
- A tree without any edge is referred to as a **null tree**.
- Since we are considering only finite graphs, we have that the trees considered are also finite.
- A tree is always a simple graph.
- A vertex of degree of 1 is called a **pendent** vertex.

12.5.6 Note

Let $G = (V, E)$ be a disconnected graph. We define a relation \sim on the set of vertices as follows: $v \sim u \Leftrightarrow$ there is a walk from v to u .

Then this relation \sim is an equivalence relation.

Let $\{V_i\}_{i \in \Delta}$ be the collection of all equivalence classes. Now

$$V = \bigcup_{i \in \Delta} V_i .$$

Write $E_i = \{e \in E \mid \text{an end point of } e \text{ is in } V_i\}$ for each i .

Then (V_i, E_i) is a connected subgraph of G for every $i \in \Delta$.

This connected subgraph (V_i, E_i) of G is called a **connected component** (or **component**) of G for every $i \in \Delta$.

The collection $\{(V_i, E_i)\}_{i \in \Delta}$ of subgraphs of G is the collection of all connected components of G .

Observations:

- If G is a connected graph, then G is the only connected component of G .
- A disconnected graph G consists of two or more connected components.
- Connected component of a graph G is a maximal connected subgraph of G .
- A graph is connected if it has exactly one component.
- Consider the graph given in Fig. 12.20

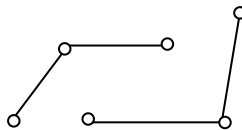


Fig. 12.20

This graph is a disconnected graph with two components.

12.5.7 Formation of Components

If G is a connected graph, then G contains only one connected component and it is equal to G .

Now suppose that G is a disconnected graph. Consider a vertex v in G . If each vertex of G is joined by some path to v , then the graph is connected, a contradiction. So there exists at least one vertex, which is not joined by any path to v .

The vertex v and all the vertices of G that are joined by some paths to v together with all the edges incident on them form a component (G_1).

To find another component, take a vertex u (from G) which is not in G_1 . The vertex u and all the vertices of G that are joined by some paths to u together with all the edges incident on them form a component (G_2).

Continue this procedure to find the components. Since the graph is a finite graph, the procedure will stop at a finite stage. In this way, we can find all the connected components of G . It is clear that, a component itself is a graph.

12.5.8 Definition

Let G be a connected graph. A **cut-set** is a subset C of the set of all edges of G whose removal from the graph G leaves the graph G disconnected; and removal of any proper subset of C does not disconnect the graph G .

(Equivalently, cut-set can also be defined as a minimal set C of edges in a connected graph G whose removal reduces the rank of the graph by one).

12.5.9 Example

Observe Graph in Fig-A. If we remove $\{a, c, d, f\}$ from the graph, then we get the subgraphs given in Fig-B.

So in the Graph-(A), the subset $\{a, c, d, f\}$ of edges, is a cut-set.

Also there are many other cut-sets such as $\{a, b, g\}$, $\{a, b, e, f\}$, $\{d, h, f\}$.

Also edge set $\{k\}$ is a cut-set.

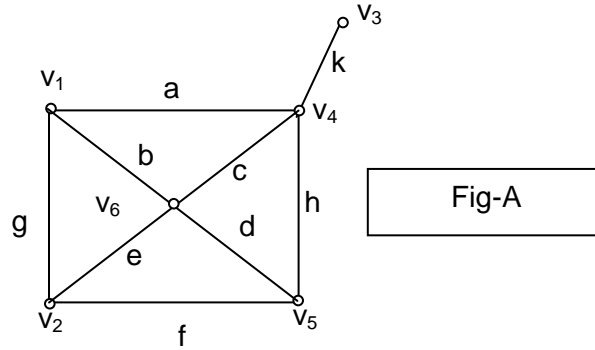


Figure 12.21

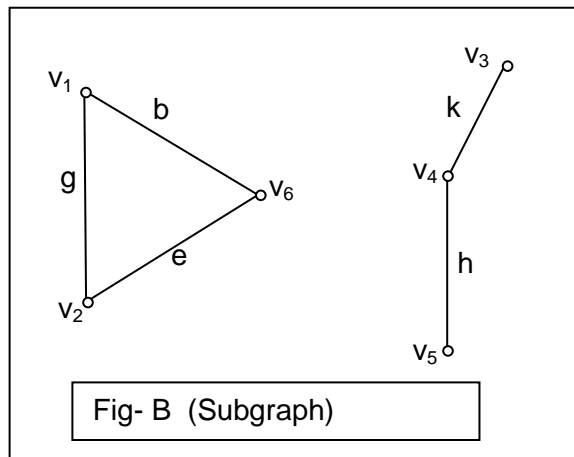


Figure 12.22

12.6 Properties of Trees

12.6.1 Theorem

T is a tree \Leftrightarrow there is one and only one path between every pair of vertices.

Proof: Suppose T is a tree. Then T is a connected graph and contains no circuits.

Since T is connected, there exists at least one path between every pair of vertices in T .

Suppose that between two vertices a and b of T , there are two distinct paths.

Now, the union of these two paths will contain a circuit in T , a contradiction (since T contains no circuits).

This shows that there exists one and only one path between a given pair of vertices in T .

Converse: Let G be a graph.

Assume that there is one and only one path between every pair of vertices in G .

This shows that G is connected.

If possible suppose that G contains a circuit.

Then there is at least one pair of vertices a, b such that there are two distinct paths between a and b . But this is a contradiction to our assumption.

So G contains no circuits. Thus G is a tree.

12.6.2 Theorem

A tree G with ' n ' vertices has $(n-1)$ edges.

Proof: We prove this theorem by induction on the number vertices n .

If $n = 1$, then G contains only one vertex and no edge.

So the number of edges in G is $n - 1 = 1 - 1 = 0$.

Suppose the induction hypothesis that the statement is true for all trees with less than ' n ' vertices. Now let us consider a tree with ' n ' vertices.

Let ' e_k ' be any edge in T whose end vertices are v_i and v_j .

Since T is a tree, by Theorem 12.3.1, there is no other path between v_i and v_j .

So by removing e_k from T , we get a disconnected graph.

Furthermore, $T - e_k$ consists of exactly two components (say T_1 and T_2).

Since T is a tree, there were no circuits in T and so there were no circuits in T_1 and T_2 .

Therefore, T_1 and T_2 are also trees.

It is clear that $|V(T_1)| + |V(T_2)| = |V(T)|$ where $V(T)$ denotes the set of vertices in T .

Also $|V(T_1)|$ and $|V(T_2)|$ are less than n .

Therefore, by the induction hypothesis, we have –

$$|E(T_1)| = |V(T_1)| - 1 \quad \text{and} \quad |E(T_2)| = |V(T_2)| - 1.$$

$$\text{Now } |E(T)| - 1 = |E(T_1)| + |E(T_2)| = |V(T_1)| - 1 + |V(T_2)| - 1$$

$$\Rightarrow |E(T)| = |V(T_1)| + |V(T_2)| - 1$$

$$= |V(T)| - 1 = n - 1.$$

This completes the proof.

12.6.3 Problem

If T is a tree (with two or more vertices), then there exists at least two pendant (a vertex of degree 1) vertices.

Solution:

Let n = the number of vertices in G . Then G has $n-1$ edges. Now

$$\sum_{i=1}^n \deg(v_i) = 2|E| = 2(n-1) = (2n-2).$$

Now if there is only one vertex, say v_1 of degree 1, then

$\deg(v_i) \geq 2$ for $i = 2, 3, \dots, n$ and

$$\sum_{i=1}^n \deg(v_i) = 1 + \sum_{i=2}^n \deg(v_i) \geq 1 + 2n - 2 = 2n - 1.$$

But $2n-2 \geq 2n-1$ or $-2 \geq -1$, a contradiction.

Therefore, there are at least two vertices of degree 1.

12.6.4 Problem

If 2 nonadjacent vertices of a tree T are connected by adding an edge, then the resulting graph will contain a cycle.

Proof: If T has n vertices then T has $n - 1$ edges and then if an additional edge is added to the edges of T the resulting graph G has n vertices and n edges. Hence G cannot be a tree by Problem 12.7.3.

But, the addition of an edge has not affected the connectivity.

Hence, G must have a cycle.

12.6.5 Problem

Any connected graph with ' n ' vertices and $n - 1$ edges is a tree.

Solution: Let ' G ' be a connected graph with n vertices and $n - 1$ edges. It is enough to show that G contains no circuits.

If possible, suppose that G contains a circuit.

Let ' e ' be an edge in that circuit.

Since ' e ' in a circuit, we have that $G - e$ is still connected.

Now $G - e$ is connected with ' n ' vertices, and so it should contain at least $n - 1$ edges, a contradiction (to the fact that $G - e$ contain only $(n - 2)$ edges).

So G contains no circuits. Therefore, G is a tree.

12.6.6 Theorem

If a graph G contains n vertices, $n - 1$ edges and no circuits, then G is a connected graph.

Proof: Let G be a graph with ' n ' vertices, $n - 1$ edges and contains no circuits.

In a contrary way, suppose that G is disconnected.

G consists of two or more circuitless components (say, g_1, g_2, \dots, g_k).

Now $k \geq 2$. Select a vertex v_i in g_i , for $1 \leq i \leq k$.

Add new edges e_1, e_2, \dots, e_{k-1} where $e_i = \overline{v_i v_{i+1}}$ to get a new graph G^* .

It is clear that G^* contains no circuits and connected, and so G^* is a tree.

Now G^* contains n vertices and $(n - 1) + (k - 1) = (n + k - 2) \geq n$ edges, a contradiction (since a tree contains $(n - 1)$ edges).

This shows that G is connected.

This completes the proof.

Self Assessment Questions

5. Which of the following graphs are trees?

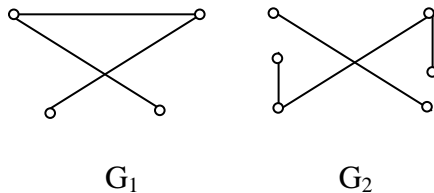


Figure 12.23

6. Draw all trees with five vertices.
7. Consider the following graph.

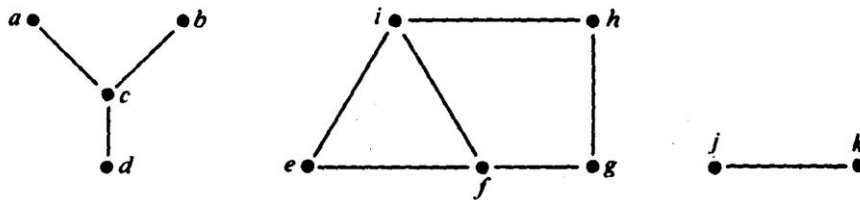


Figure 12.24

The number of components in this graph is _____

12.7 Rooted Trees and Applications

Rooted trees are extensively used in the computer search methods, binary identification problems, and variable length binary codes.

12.7.1 Definition

A tree in which one vertex (called the *root*) is distinguished from all the other vertices, is called a **rooted tree**. In a rooted tree, the root is generally marked in a small triangle (or small circle).

12.7.2 Example

Distinct rooted trees with four vertices, are given in Fig. 12.25

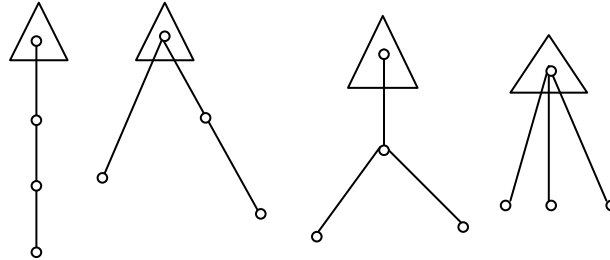


Figure 12.25

Generally, the term 'tree' means trees without any root. However they are sometimes called *free trees* (or) *non-rooted trees*. A variety of rooted trees (called the *Binary rooted trees*) is of particular interest.

12.7.3 Definition

A tree in which there is exactly one vertex of degree 2, and all other remaining vertices are of degree one or three, is called a **binary tree**.

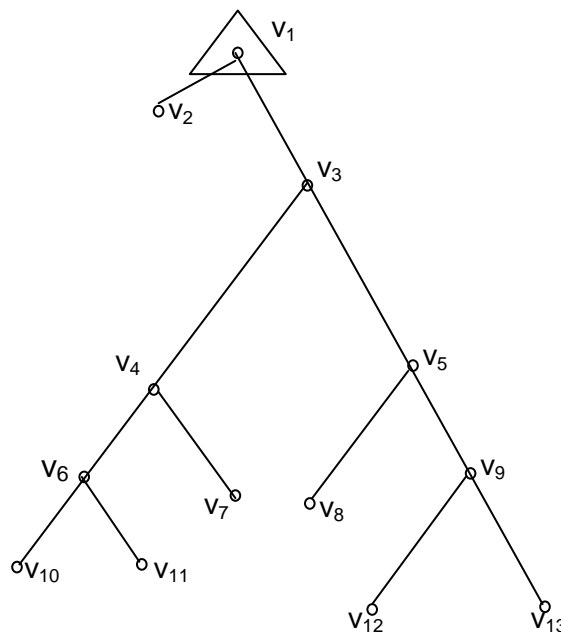


Fig. 12.26

- i) The above Fig. represents a binary tree (since the only vertex 'v₁' is of degree 2, and all other vertices are of degree either 1 or 3).
- ii) The vertex of degree 2 (that is, v₁) is distinct from all other vertices, this vertex v₁ is the root.
- iii) In a binary tree, the vertex with degree 2 serves as a root. So every binary tree is a rooted tree.

12.7.4 Properties of Binary trees

Property (i): The number of vertices n , in a binary tree is always odd.

Property (ii): The number of pendent vertices is $\frac{n+1}{2}$.

Property (iii): Number of vertices of degree 3 is $= n - p - 1 = n - \left(\frac{n+1}{2}\right) - 1$
 $= \frac{n-3}{2}$.

12.7.5 Example

In the graph given in Fig. we have that $n = 13$, $p = \frac{n+1}{2} = \frac{13+1}{2} = \frac{14}{2} = 7$.

Therefore, number of vertices of degree 3 is $\frac{n-3}{2} = \frac{13-3}{2} = 5$.

12.7.6 Definition

A non-pendent vertex in a tree is called an *internal* vertex.

Observation:

- i) The number of internal vertices in a Binary tree is –

$$\frac{n-1}{2} = (p-1) \text{ where } p = \text{the number of pendent vertices.}$$

- ii) In the binary tree given in Fig. 12.3.3, the internal vertices are v₁, v₃, v₄, v₅, v₆, v₉. These are 6 (=7 - 1 = p - 1) in number.

12.7.7 Definition

Let v be a vertex in a binary tree. Then v is said to be at *level* l if v is at a distance of l from the root.

12.7.8 Example

i) A 13-vertex, 4-level binary tree was given in Fig.

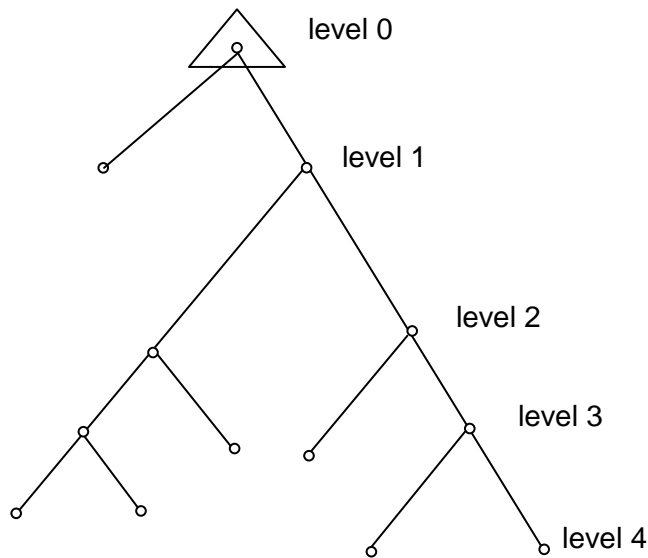


Figure 12.27

Here the number of vertices at levels 0, 1, 2, 3, 4 are 1, 2, 2, 4 and 4 respectively.

12.7.9 Definition

The sum of path lengths from the root to all pendent vertices is called the **path length** (or) *external path length* of a tree.

12.7.10 Example

i) The path length of the binary tree given in Fig. 12.28 is:

$$1 + 3 + 3 + 4 + 4 + 4 + 4 = 23.$$

ii) In the Figures A and B , there are two 11-vertex binary trees.

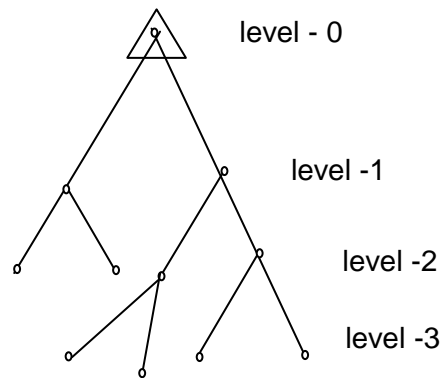


Figure 12.28

The path length of graph (fig. A): $2 + 2 + 3 + 3 + 3 + 3 = 16$.

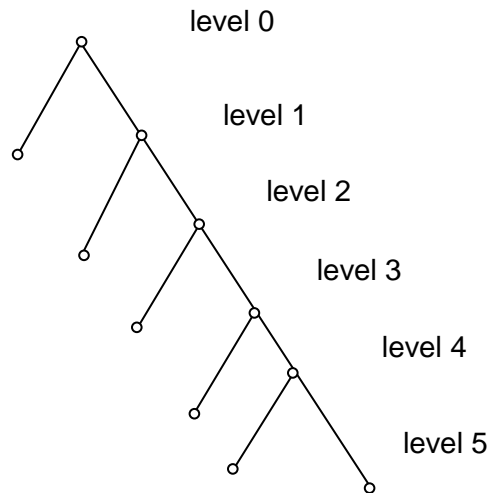


Figure 12.29

The path length of graph (fig. B): $1 + 2 + 3 + 4 + 5 + 5 = 20$.

12.7.11 Search procedures

Each vertex of a binary tree represents a test with two possible outcomes. We start at the root. The outcome of the test at the root sends us to one of the two vertices at the next level, where further tests are made and so on.

Reaching a specified pendent vertex (that vertex, which represents the goal of the search), terminates the search.

For such search procedures, it is often important to construct a binary tree in which, for a given number of vertices n , the vertex farthest from the root is as close to the root as possible.

i) There can be only one vertex (the root) at level 0. Number of vertices at level one is at the most 2. Number of vertices at level two is at the most 2^2 and so on. So the maximum number of vertices possible in a k -level binary tree is $2^0 + 2^1 + 2^2 + \dots + 2^k$.

$$\text{So } n \leq 2^0 + 2^1 + 2^2 + \dots + 2^k$$

ii) The maximum number among the levels of the vertices in a binary tree is called *height* of the tree. So height = $\max \{ \text{level of a vertex } v / v \in V \}$. This height is denoted by l_{\max} .

iii) To construct a binary tree for a given n such that the farthest vertex is as far as possible from the root, we must have exactly two vertices at each level, except at the 0 level. So $\max l_{\max} = \frac{n-1}{2}$.

12.7.12 Coke Machine Problem

Suppose that there is a coke machine. The machine is to have a sequence of tests (for example, it should be capable of identifying the coin that is put into the machine). We assume that five rupee coin, two rupee coin, one rupee coin and fifty paise coin can go through the slot. So the machine can identify only these four coins. Every coin put in, is to be tested by the machine. Each test has the effect of partitioning the coins into two complementary sets. [Suppose a coin is put into the machine. It should test whether the coin is “five rupee coin”. If it is not a five rupee coin, then it should test whether it is a two rupee coin and so on]. We suppose the time taken for each test is.

Test Pattern-1: One type of testing pattern was shown in Graph-(i), given in Fig. A.

Suppose the statistical data tells that

w_1 = probability of putting a Rs 5 coin = 0.5

w_2 = probability of putting a Rs 2 coin = 0.2

w_3 = probability of putting a Rs 1 coin = 0.2

w_4 = probability of putting a Rs 0.5 coin = 0.1

Now

$$\begin{aligned} \sum w_i \cdot l(v_i) &= w_1 \cdot l(v_1) + w_2 \cdot l(v_2) + w_3 \cdot l(v_3) + w_4 \cdot l(v_4) \\ &= (0.5)(1) + (0.2)(2) + (0.2)(3) + (0.1)(4) = 1.12 \end{aligned}$$

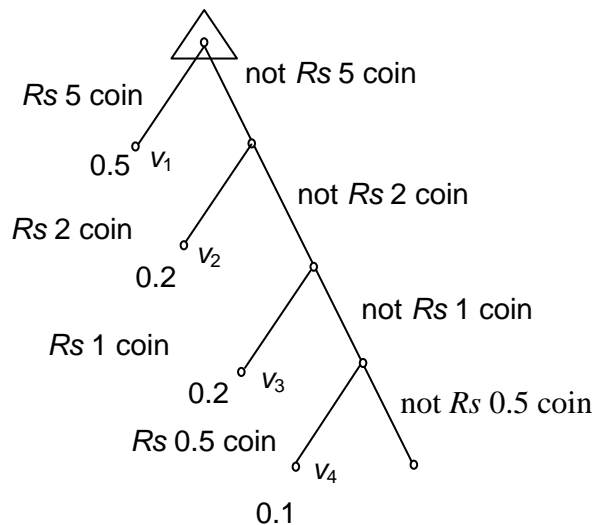


Figure 12.30

So expected time to be taken by the machine for testing one coin is 1.9t.

Thus if the machine follows (for its testing pattern) the binary tree given in Graph-(a), then the expected time for testing one coin is equal to 1.9t.

Test Pattern-2: Another type of testing pattern was given in the Fig. 12.3.12 B.

$$\sum w_i \cdot l(v_i) = w_1 \cdot l(v_1) + w_2 \cdot l(v_2) + w_3 \cdot l(v_3) + w_4 \cdot l(v_4)$$

$$= (0.5) (2) + (0.2) (2) + (0.2) (2) + (0.1) (2) = 2.0$$

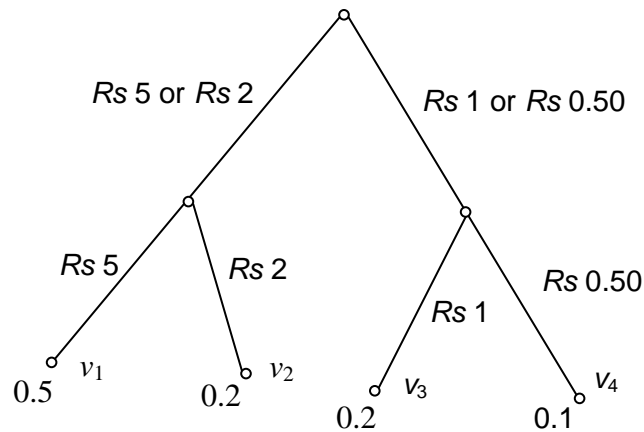


Figure 12.31

So here, the expected time to be taken by the machine for testing one coin is $2t$.

Thus if the machine follows (for its testing pattern) the binary tree given in graph B then the expected time for testing one coin is $2t$.

12.8 Summary

This unit is meant for beginning your process of learning Graph Theory. It started with the definition of Graph and Moved on to illustrate the concepts of finite and infinite graph, incidence, degree, isolated vertex, pendent vertex and null graph. We also discussed the isomorphism between graphs and subgraphs of a given graph with appropriate illustrations. In this unit, we dealt with a special type of graphs called trees and studied some of their properties. The concept of minimally connected graphs was introduced. By listing all the properties of tree, it was easy to observe that there are five different equivalent conditions for tree.

12.9 Terminal Questions

1. Define the terms: Graph, finite graph, infinite graph, incidence, degree, isolated vertex, pendent vertex, null graph
2. Show that the sum of the degrees of the vertices of a finite graph G is twice the number of edges.
3. Show that the number of vertices of odd degree is always even.
4. Show that an infinite graph with finite number of edges must have an infinite number of isolated vertices.
5. Show that the maximum degree of any vertex in a simple graph is $(n - 1)$.
6. Show that the maximum number of edges in a simple graph with n vertices is $\frac{n(n-1)}{2}$.
7. Define the terms: tree, pendent vertex. How many different trees are there of order 2, 3, 4, 5 ?
8. Show that G is a tree \Leftrightarrow there is one and only one path between every pair of vertices.
9. (i) Show that a tree G with n vertices has $n - 1$ edges.
(ii) Show that any connected graph G with n vertices and $n - 1$ edges is tree.
10. Show that in a tree there exist at least two pendant vertices.
11. Prove any three equivalent conditions for a tree ?

12.10 Answers

Self Assessment Questions

1. Here $d(u_1) = 3$; $d(u_2) = 4$; $d(u_3) = 3$; $d(u_4) = 3$; and $d(u_5) = 1$

$$\text{Now } \sum_{i=1}^5 u_i = 3 + 4 + 3 + 3 + 1 = 14. \quad |E| = 7.$$

$$\text{So } \sum_{i=1}^5 d(u_i) = 2 |E|$$

Therefore, the sum of degrees of all the vertices of a graph G is twice the number of edges in G .

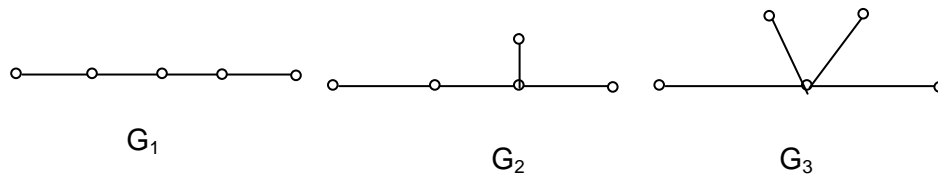
2. No, since the sum of the degrees of the vertices cannot be odd.
3. Let G be a regular graph of degree 4 with 10 edges and let 'n' be the number of vertices in G . Then $\sum_{u \in V} d(u) = 2 \times 10 = 20$.

$$\Rightarrow n \cdot 4 = 20. \Rightarrow n = 5.$$

Yes

5. G_1 is a tree, since it is a connected graph without circuits. G_2 is not a tree (since it is not connected).

6.



First draw five vertices. Then connect them, so that no cycles are created. In this process, we must be careful not to repeat trees since two trees which appear different may just be drawn differently. Here there are three trees with five vertices as shown above.

Unit 13 Algebraic Codes and Cryptography

Structure

- 13.1 Introduction
 - Objectives
- 13.2 Preliminaries
- 13.3 Hamming Distance
- 13.4 Linear Codes
- 13.5 Introduction to Cryptography
- 13.6 Summary
- 13.7 Terminal Questions
- 13.8 Answers

13.1 Introduction

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.

Objectives:

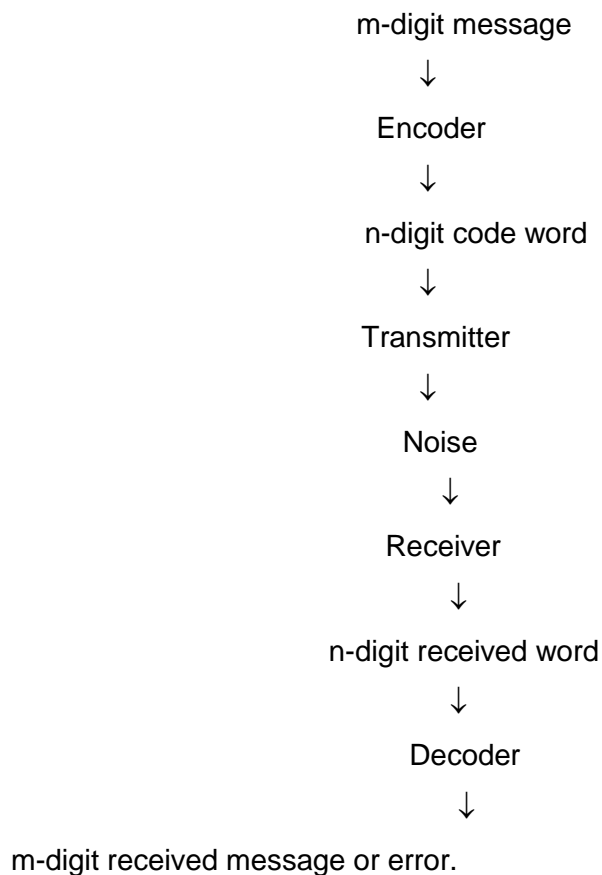
At the end of the unit, you would be able to:

- understand the fundamental idea of coding system
- explain the hamming distance between the code words
- learn the group codes, linear codes and parity check codes
- apply the concepts to real world problems in communication technology

13.2 Preliminaries

Let us examine a simple model of a communications system for transmitting and receiving coded messages. 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 device 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:



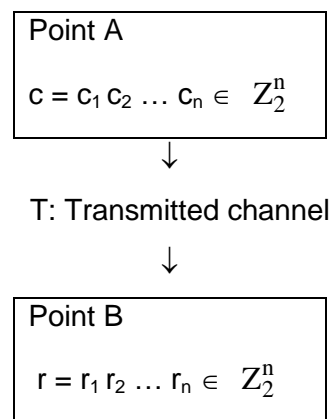
Consider the set $Z_2 = \{0, 1\}$ and additive group $(Z_2, +)$, where $+$ denotes addition modulo 2. Then, for any positive integer n , we have

$$Z_2^n = Z_2 \times Z_2 \times \dots \times Z_2 \text{ (} n \text{ factors)} = \{(a_1, a_2, \dots, a_n) / a_i \in Z_2 \text{ for each } i\}.$$

Thus, every element of Z_2^n is an n -tuple (a_1, a_2, \dots, a_n) in which every entry is either 0 or 1. Some times the n -tuple can be written as $a_1 a_2 \dots a_n$ called a word or a string. Each a_i (either 0 or 1) is called a bit. For example,

11001 is a word in Z_2^5 . That is $(1,1,0,0,1) \in Z_2^5$.

Suppose a string $c = c_1 c_2 \dots c_n \in Z_2^n$ is transmitted from a point A through a transmitted channel T. In normal situations, this word would be received at a point B without any change. But in practice, transmission channel experiences 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 $r = r_1 r_2 \dots r_n$ where each r_i is either 0 or 1, $r_j \neq c_j$ for some j , $1 \leq j \leq n$.



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 $e \in Z_2^n$.

13.2.1 Note

Suppose p is the probability that an event happens in a single trial. Now $q = (1 - p)$ is the probability that the event will fail in a single trial. Then the probability of the event to occur exactly x times in n trials (that is, x successes and $(n - x)$ failures) is given by $P(x) = {}^n C_x \cdot p^x q^{n-x}$ for $x = 0, 1, 2, \dots$. Such a distribution is called a **Binomial distribution**. Its probability function (or density function) is given by –

$P(X = x) = {}^n C_x p^x q^{n-x}$, $x = 0, 1, 2, 3, \dots, n$, where $p = (1 - q)$, and $P(x) = 0$ for the other values of x . The two constants n and p appearing in the density function are called parameters of the Binomial distribution. We can fit in a Binomial distribution if –

- The result of any trial is either a success (occurrence) or a failure (non-occurrence),
- The probability of success in each trial is a constant p ,
- The trials are independent.

Binomial distribution is a discrete distribution as X can take only the integral values: $0, 1, 2, \dots, n$. Any variable, which follows binomial distribution is known as binomial variants.

For example, a fair coin is tossed 6 times (or equivalently six fair coins are tossed). Success means getting a head. Then,

- i. The probability that exactly two heads occur (that is, $k = 2$) is

$${}^6 C_2 \left(\frac{1}{2}\right)^2 \left(\frac{1}{2}\right)^4 = \frac{6!}{2!(6-2)!} \left(\frac{1}{2}\right)^6 = \frac{6!}{2!4!} \cdot \frac{1}{64} = \frac{6 \times 5}{2} \times \frac{1}{64} = \frac{15}{64}.$$

- ii. The probability of getting at least four heads (that is, $k = 4, 5$ or 6) is

$${}^6 C_4 \left(\frac{1}{2}\right)^4 \left(\frac{1}{2}\right)^2 + {}^6 C_5 \left(\frac{1}{2}\right)^5 \left(\frac{1}{2}\right) + {}^6 C_6 \left(\frac{1}{2}\right)^6 = \frac{15}{64} + \frac{6}{64} + \frac{1}{64} = \frac{11}{32}.$$

- iii. The probability of getting no heads is $q^6 = \left(\frac{1}{2}\right)^6 = \frac{1}{64}$.

$$\text{So the probability of getting at least one head is } 1 - q^6 = 1 - \frac{1}{64} = \frac{63}{64}$$

13.2.2 Binary Symmetric Channel

It is a model consisting 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 $(0.9999)^{10,000} \approx 0.00005$.

13.2.3 Theorem

If a binary n -tuple (x_1, x_2, \dots, 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 –

$$\binom{n}{k} q^k p^{n-k}$$

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 –

$$\binom{n}{k} q^k p^{n-k}.$$

13.2.4 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

$$\binom{n}{2} q^2 p^{n-2} = \frac{500 \cdot 499}{2} (0.005)^2 (0.995)^{498} \approx 0.257.$$

The probability of more than two errors is approximately

$$1 - 0.082 - 0.204 - 0.257 = 0.457$$

13.2.5 Example

The word $c = 1010110$ is transmitted through a binary symmetric channel. If $e = 0101101$ is the error pattern, find the word r received. If $p = 0.05$ is the probability that a signal is incorrectly received, find the probability with which r is received.

Solution: Given $c = 1010110 \in \mathbb{Z}_2^7$ and error pattern $e = 0101101 \in \mathbb{Z}_2^7$.

Therefore, the received word is $r = c + e = 1010110 + 0101101 = 1111011$

(where $+$ is the addition in \mathbb{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).

The probability with which r is received is –

$$p^4(1-p)^{7-4} = (0.05)^4(1-0.05)^3 = (0.05)^4(0.95)^3 \approx 0.000005.$$

13.2.6 Example

The word $c = 1010110$ is transmitted through a binary symmetric channel. If $p = 0.02$ is the probability of incorrect receipt of a signal, find the probability that c is received as $r = 1011111$. Determine the error pattern.

Solution: The words c and r in Z_2^7 differ in two places (fourth and seventh).

The probability that c is received as r is –

$$p^2(1-p)^{7-2} = (0.02)^2(1-0.02)^5 = 0.00036.$$

The error pattern e is given by $r = c + e$, where $+$ is the component wise addition in Z_2^7 .

Let $e = e_1 e_2 \dots e_7$, we have $r = c + e_1 e_2 \dots e_7$.

This implies $1011111 = 1010110 + e_1 e_2 \dots e_7$.

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, $e = 0001001$.

13.2.7 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 a (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. More precisely, an (n, m) -block code consists of an encoding function,

$$E: Z_2^m \rightarrow Z_2^n$$

and a decoding function,

$$D: Z_2^n \rightarrow Z_2^m.$$

A code word is any element in the image of E . We also require that E be one-to-one so that two information blocks will not be encoded into the same codeword. If the code is to be error-correction, then D must be onto.

13.2.8 Example

Define an encoding function,

$$E: Z_2^8 \rightarrow Z_2^9$$

by $E(e_1 e_2 \dots e_8) = e_1 e_2 \dots e_8 e_9$ where,

$$e_9 = \sum_{i=1}^8 e_i,$$

the summation being taken under addition modulo 2. If $p = 0.001$ is the probability that a signal is received incorrectly, find the probability that the code word 110101101 is received with at the most one error.

Solution: Let $e = e_1 e_2 \dots e_8$. Using the definition of e_9 , we have that if odd number of e_i s in e are 1s (and the rest are 0s), then $e_9 = 1$. In this case, $c = E(e) = e_1 e_2 \dots e_8 e_9$ contains even number of 1s. On the other hand, if an even number of e_i s in e are 1s (and the rest are 0s), then $e_9 = 0$.

Hence in this case $c = E(e)$ contains an even number of 1s.

Thus the given encoding function is such that the code word $c = E(e)$ of every word $e \in Z_2^8$ contains an even number of 1s. Now consider the given code word –

$$c = 110101101 \in Z_2^9.$$

If p is the probability that a signal is incorrectly received, then the probability of receiving c correctly is $(1-p)^9$, and the probability of receiving c with one error is,

$$\binom{9}{1} p (1-p)^8.$$

Therefore, the probability of receiving c with at the most one error is –

$$(1-p)^9 + \binom{9}{1} p (1-p)^8.$$

Given that $p = 0.001$. Therefore, the required probability is,

$$(1-0.001)^9 + 9 \times 0.001 \times (1-0.001)^8 = 0.999964167.$$

13.2.9 Parity Check Code

Define an encoding function

$$E: Z_2^m \rightarrow Z_2^{m+1}$$

by

$$E(e_1 e_2 \dots e_m) = e_1 e_2 \dots e_{m+1} \text{ where}$$

$$e_{m+1} = \begin{cases} 0 & \text{if } e \text{ contains even number of 1s} \\ 1 & \text{if } e \text{ contains odd number of 1s} \end{cases}, \text{ and the corresponding}$$

decoding function is $D: Z_2^{m+1} \rightarrow Z_2^m$ defined by

$$D(r_1 r_2 \dots r_m r_{m+1}) = r_1 r_2 \dots r_m.$$

Using the definition of $E: Z_2^3 \rightarrow Z_2^4$,

$$E(000) = 0000, E(001) = 0011, E(011) = 0110, \dots, E(111) = 1111$$

Using the definition of $D: Z_2^4 \rightarrow Z_2^3$,

$$D(0000) = 000, D(0001) = 000, \dots, D(1010) = 101, D(1100) = 110, \dots, D(1111) = 111.$$

13.3 Hamming Distance

Let $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ 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. The distance between two code words is the minimum number of transmission errors required to change one codeword into the other. The minimum distance for a code, d_{\min} is the minimum of all distances $d(x,y)$ where x and y are distinct code words. The weight $w(x)$ of a binary code word x is the number of 1's in x . Clearly $w(x) = d(x, 0)$ where $0 = (00\dots 0)$.

13.3.1 Example

Let $x = (10101)$, $y = (11010)$ and $z = (00011)$ be all of the code words 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.

$$w(x) = 3, w(y) = 3, w(z) = 2.$$

13.3.2 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 code words.

13.3.3 Note

For all $x, y \in Z_2^m$ we have $w(x + y) \leq w(x) + w(y)$.

13.3.4 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 0s $\Leftrightarrow x$ and y contains only 1s or only 0s $\Leftrightarrow x = y$.
- iii) $d(x, y) = w(x + y) = w(y + x) = d(y, x)$
- iv) $d(x, z) = w(x + z)$
- v) $= w(x + y + y + z)$ (since $y + y = 0$ in Z_2)
 $\leq w(x + y) + w(y + z)$ (by the above note)
 $= d(x + y) + d(y + z)$

13.3.5 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,
 $S(a, k) = \{x \in Z_2^n / d(x, a) \leq k\}$.

13.3.6 Definition

Let x_1, x_2, \dots, x_n denote the codewords in a block code. The conditional probability $P(x_i | y)$ for $i = 1, 2, \dots, n$ 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***.

13.3.7 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

13.4 Linear Codes

13.4.1 Definition

Let $E: Z_2^m \rightarrow Z_2^n$, $n > m$ be an encoding function and $C = \{E(w) \mid w \in Z_2^m\}$ be the set of codes. Then C is called a *group code* if C is a subgroup of Z_2^n .

13.4.2 Example

Consider the encoding function $E: Z_2^2 \rightarrow Z_2^6$ 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.

13.4.3 Example

Suppose that a code consists of the following 7-tuples:

(000000) (000111) (001010) (0011010)
 (0100110) (0101001) (0110011) (0111100)
 (1000011) (1001100) (1010110) (1011001)
 (1100101) (1101010) (1110000) (1111111)

It can be easily verified that this code is a subgroup of Z_2^7 and hence a group code.

13.4.4 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:

$$\begin{aligned} d_{\min} &= \min \{d(x, y) \mid x \neq y\} \\ &= \min \{d(x, y) \mid x + y \neq 0\} \\ &= \min \{w(x + y) \mid x + y \neq 0\} \\ &= \min \{w(z) \mid z \neq 0\}. \end{aligned}$$

13.4.5 Definition

The inner product of two binary n -tuples to be $x \cdot y = x_1y_1 + \dots + x_ny_n$, where $x = (x_1, x_2, \dots, x_n)^t$ and $y = (y_1, y_2, \dots, y_n)^t$ are column vectors.

We can also write an inner product as the product of a row matrix with a

column matrix. That is, $x \cdot y = x^t y = (x_1 \ x_2 \ \dots \ x_n) \begin{pmatrix} y_1 \\ y_2 \\ \cdot \\ \cdot \\ \cdot \\ y_n \end{pmatrix} = x_1 y_1 + \dots + x_n y_n$.

For instance, if $x = (011001)^t$ and $y = (110101)^t$, then $x \cdot y = 0$.

13.4.6 Notation

$M_{m \times n}(Z_2)$ = the set of all $m \times n$ matrices with entries in Z_2 . We adopt the usual matrix operations except that all addition and multiplication operations occur in Z_2 .

13.4.7 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 $Hx = 0$. We denote the null space of a matrix H by $\text{Null}(H)$.

13.4.8 Example

Suppose $H = \begin{pmatrix} 01010 \\ 11110 \\ 00111 \end{pmatrix}$. For a 5-tuple $x = (x_1, x_2, \dots, x_5)^t$ to be in the null

space of H , $Hx = 0$.

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.

13.4.9 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 $x, y \in \text{Null}(H)$ for some $H \in M_{m \times n}(\mathbb{Z}_2)$.

Then $Hx = 0$ and $Hy = 0$. So $H(x + y) = Hx + Hy = 0 + 0 = 0$. Therefore $x + y$ is in the null space of H and so must be a code word.

Inverse: Each element of \mathbb{Z}_2^n is its own inverse.

Hence $\text{Null}(H)$ is a code word.

13.4.10 Definition

A code is a **linear code** if it is determined by the null space of some matrix $H \in M_{m \times n}(\mathbb{Z}_2)$.

13.4.11 Example

Let C be the code given by the matrix

$$H = \begin{pmatrix} 000111 \\ 011011 \\ 101001 \end{pmatrix} \text{ Suppose that the 7-tuple } x = (010011)^t \text{ is received.}$$

$$\text{Now } Hx = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \text{ Therefore, the received word is not a code word.}$$

Self Assessment Questions

- By doing any type of addition, explain why the following set of 4-tuples in \mathbb{Z}_2^4 cannot be a group code.
(0110) (1001) (1010) (1100)
- Compute the hamming distances between the following pairs of n-tuples
(i) (011010), (011100) (ii) (00110), (01111).
- Compute the weighs of the following n-tuples
(i) (011010) (ii) (01111)
- 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)

5. For $e = 110 \in \mathbb{Z}_2^3$, find the sphere $S(e, 1)$.

13.5 Introduction to Cryptography

Cryptography is the study of sending and receiving secret messages. The aim of cryptography is to send messages across a channel so only the intended recipient of the message can read it. In addition, when a message is received, the recipient usually requires some assurance that the message is authentic. Modern cryptography is fully dependant on basic algebraic systems like semigroups / groups and number theory.

13.5.1 Definitions

The message to be sent is called the *plaintext*. The disguised message is called the *ciphertext*. The plaintext and ciphertext are both written in an *alphabet*, consisting of *letters* or *characters*. Characters can include not only the familiar alphabetic characters A, ..., Z and a, ..., z but also digits, punctuation marks, and blanks.

13.5.2 Note

A *cryptosystem* has two parts

- i) **Encryption:** The process of transforming a plaintext message to a ciphertext message (The parameter used to the encryption function is called a *Key*).
- ii) **Decryption:** The reverse transformation of changing a ciphertext message into a plaintext message.

Systems that use two separate keys, one for encoding and another for decoding, are called **public key cryptosystems**. Since knowledge of the encoding key does not allow anyone to guess at the decoding key, the encoding key can be made public.

To encrypt a plaintext message, we apply to the message some function which is kept secret, say f . This function will yield an encrypted message. Given the encrypted form of the message, we can recover the original message by applying the inverse transformation f^{-1} .

13.5.3 Example

- i) We consider the private key cryptosystems in which the shift code was used by Julius Caesar.

The encoding function $f(p) = p + 3 \pmod{26}$ with the encoded message *DOJHEUD*.

Step 1: We first digitize the alphabet by $A = 00, B = 01, \dots, Z = 25$.

Step 2: Using encoding function $f(p) = p + 3 \pmod{26}$ we get $A \rightarrow D, B \rightarrow E, \dots, Z \rightarrow C$.

Step 3: Digitize *DOJHEUD*: we get 3, 14, 9, 7, 4, 20, 3.

Step 4: Consider the decoding function is $f^{-1}(p) = p - 3 \pmod{26} = p + 23 \pmod{26}$.

Step 5: Apply the inverse transformation (step 4) to get 0, 11, 6, 4, 1, 17, 0

Step 6: Decode to get *ALGEBRA*.

- ii) The encoding function $f(x) = x + 5 \pmod{26}$ with the encoded message *SJFMMDIB*.

Step 1: We first digitize the alphabet by $A = 00, B = 01, \dots, Z = 25$.

Step 2: Using encoding function $f(x) = x + 5 \pmod{26}$ we get $A \rightarrow F, B \rightarrow G, \dots, Z \rightarrow E$.

Step 3: Digitize *SJFWWNSL*: we get 18, 9, 5, 22, 22, 13, 18, 11.

Step 4: Consider the decoding function is $f^{-1}(x) = x - 5 \pmod{26} = x + 21 \pmod{26}$.

Step 5: Apply the inverse transformation (step 4) to get 13, 4, 0, 17, 17, 8, 13, 6.

Step 6: Decode to get *NEARRING*.

13.5.4 Remark

Simple shift codes are examples of monoalphabetic cryptosystems. In these ciphers a character in the enciphered message represents exactly one character in the original message. Such cryptosystems are not very sophisticated and are quite easy to break. In a simple shift as described in the example 2.6.3, there are only 26 possible keys. It would be quite easy to try them all rather than to use frequency analysis.

Let us investigate a slightly more sophisticated cryptosystems.

13.5.5 Affine Cryptosystem

Suppose that the encoding function is given by

$$f(p) = ap + b \pmod{26}.$$

We first need to find out when a decoding function f^{-1} exists. Such a decoding function exists when we can solve the equation

$c = ap + b \pmod{26}$ for p . This is possible exactly when a has an inverse or equivalently, when $\gcd(a, 26) = 1$. In this case, $f^{-1}(p) = a^{-1}p - a^{-1}b \pmod{26}$.

13.5.6 Example

Let us consider the affine cryptosystem $f(p) = ap + b \pmod{26}$. For this cryptosystem to work we must choose an $a \in \mathbb{Z}_{26}$ that is invertible. This is only possible if $\gcd(a, 26) = 1$. Let $a = 5$. Then a is invertible and $a^{-1} = 21$. Since $\gcd(5, 26) = 1$. Therefore, we can take the encryption function to be $f(p) = 5p + 3 \pmod{26}$. Thus, *ALGEBRA* is encoded as 3, 6, 7, 23, 8, 10, 3, or *DGHXIKD*. The decryption function will be $f^{-1}(p) = 21p - 21 \cdot 3 \pmod{26} = 21p + 15 \pmod{26}$.

13.5.7 Public Key Cryptography

If the routine (traditional) cryptosystems are used, anyone who knows enough to encode a message will also know enough to decode an intercepted message. The public key cryptography which is based on the observation that the encryption and decryption procedures need not have

the same key. This removes the requirement that the encoding key be kept secret. The encoding function f must be relatively easy to compute, but f^{-1} must be extremely difficult to compute without some additional information, so that someone who knows only the encrypting key cannot find the decrypting key without prohibitive computation.

13.5.8 The RSA Cryptosystem

The RSA cryptosystem introduced by R. Rivest, A. Shamir and L. Adleman in 1978, is based on the difficulty of factoring large numbers. Though it is not a difficult task to find two large random primes and multiply them together, factoring a 150-digit number that is the product of two large primes would take 100 million computers operating at 10 million instructions per second about 50 million years under the fastest algorithms currently known.

13.5.9 Working of the RSA cryptosystem

Assume that we choose two random 150-digit prime numbers p and q . Next, we compute the product $n = pq$ and also compute $\phi(n) = m = (p-1)(q-1)$, where ϕ is the Euler ϕ -function. Now we start choosing random integers E until we find one that is relatively prime to m ; that is, we choose E such that $\gcd(E, m) = 1$. Using the Euclidean algorithm, we can find a number D such that $DE = 1 \pmod{m}$. The numbers n and E are now made public.

Suppose now the person B (Bob) wishes to send person A (Alice) a message over a public line. Since E and n are known to everyone, anyone can encode messages. Bob first digitizes the messages according to some scheme, say A = 00, B = 02, ..., Z = 25. If necessary, he will break the message into pieces such that each piece is a positive integer less than n . Suppose x is one of the pieces. Bob forms the number $y = x^E \pmod{n}$ and sends y to Alice. For Alice to recover x , she only needs to compute $x = y^D \pmod{n}$. Only Alice knows D .

13.5.10 Example

Suppose we wish to send some message, which when digitized is 23.

Let $p = 23$ and $q = 29$. Then $n = pq = 667$

and $\phi(n) = m = (p-1)(q-1) = 616$.

Let $E = 487$, since $\gcd(616, 487) = 1$.

The encoded message is computed to be $23^{487} \bmod 667 = 368$.

This computation can be reasonably done by using the method of repeated squares as described. Using the Euclidean algorithm, we determine that $191E = 1 + 151m$; therefore, the decrypting key is $(n, D) = (667, 191)$. We recover the original message by calculating $368^{191} \bmod 667 = 23$.

Self Assessment Questions

6. An encoding function $E: Z_2^3 \rightarrow Z_2^4$ 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.

13.6 Summary

This unit provides a brief idea about the encoding and decoding of the messages in a transmitted channel. This concept is an application of modern algebra. The student will be 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 and generator matrices are useful in solving practical problems in communications systems. We also discussed the elementary concepts of cryptosystems.

13.7 Terminal Questions

1. Explain Parity check code.
2. Explain Hamming distance.
3. Describe cryptosystems.

13.8 Answers**Self Assessment Questions**

1. $(0000) \notin C$
2. (i) 2, (ii) 2
3. (i) 3, (ii) 4
4. (i) $d_{\min} = 2$, (ii) $d_{\min} = 1$.
5. $S(e, 1) = \{110, 010, 100, 111\}$.
6. (i) $\{0000, 0011, 0101, 1001, 1100, 1010, 0110, 1111\}$
7. (ii) $H = [1111]$

References:

1. Bernard Kolman, R. C. Busby, Sharon Ross, "Discrete Mathematical Structures" PHI, 1999.
2. Fraleigh J. B. "A First Course in Abstract Algebra", Narosa Pub. House, New Delhi, 1992.
3. Graham R. L., Knuth, D. E., and Patashnik O., Concrete Mathematics, A Foundation for Computer Science, 2nd Ed., Addison Wesley, 1994.
4. Herstein I. N. "Topics in Algebra", New York, Blaisdell, 1964.
5. Liu.C.L., Elements of Discrete Mathematics, Mc Hill.
6. Liu. C. L. Introduction to Combinatorial Mathematics, Mc-Graw – Hill, New York, 1968
7. Richard Johnsonbaugh, Discrete Mathematics Pearson Education Asia, 2001.
8. Rosen K. H., Hand Book of Discrete and Combinatorial Mathematics, CRC Press, 1999.
9. Trembly J. P. and Manohar R. "Discrete Mathematical Structures with Applications to Computer Science", Mc-Graw Hill, 1975.