KARNATAKA STATE OPEN UNIVERSITY

MANASAGANGOTRI, MYSORE- 570 006

DEPERTAMENT OF STUDIES IN INFORMATION TECHNOLOGY

M.SC IN INFORMATION T SCIENCE

I SEMESTER

ESSENTIAL MATHEMATICS

IS 1.1

KSOU NATIONAL INTERNATIONAL RECOGNITION

Karnataka State Open University (KSOU) was established on 1st June 1996 with the assent of H.E. Governor of Karnataka as a full fledged University in the Academic year 1996 vide Government notification No./EDI/UOV/dated 12th February 1996 (Karnataka State Open University Act – 1992). The Act was promulgated with the object to incorporate an Open University at the State Level for the introduction and promotion of Open University and Distance Education Systems in the education pattern of the State and the Country for the Co-ordination and determination of standard of such systems.

- With the virtue of KSOU Act of 1992, Karnataka State Open University is empowered to establish, maintain or recognize Institutions, Colleges, Regional Centres and Study Centres at such places in Karnataka and also open outside Karnataka at such places as it deems fit.
- All Academic Programmes offered by Karnataka State Open University are recognized by the Distance Education Council (DEC), Ministry of Human Resource Development (MHRD), New Delhi.
- Karnataka State Open University is a regular member of the Association of Indian Universities (AIU), New Delhi, since 1999.
- Karnataka State Open University is a permanent member of Association of Commonwealth Universities (ACU), London, United Kingdom since 1999. Its member code number: ZKASOPENUINI.
- Karnataka State Open University is a permanent member of Asian Association of Open Universities (AAOU), Beijing, CHINA, since 1999.
- Karnataka State Open University has association with Commonwealth of Learning (COL), Vancouver, CANADA, since 2003. COL is an intergovernmental organization created by commonwealth Heads of Government to encourage the development and sharing of open learning distance education knowledge, resources and technologies.

Higher Education To Everyone Everywhere

MSIT – 101
Essential Mathematics

First Semester M. Sc. IT

MODULE 1 MATHEMATICAL LOGIC AND SET THEORY

UNIT – 1 MATHEMATICAL LOGIC – PART I 7- 19

UNIT – 2 MATHEMATICAL LOGIC –PART II 20 - 33

UNIT – 3 SET THEORY – PART I 34 - 47

UNIT – 4 SET THEORY – PART II 48 - 63

MODULE 2 RELATIONS RECURRENCE RELATIONS AND FUNCTIONS

UNIT – 5 RELATIONS 64 - 85

UNIT – 6 RECURRENCE RELATION - I 86 - 97

UNIT – 7 RECURRENCE RELATION - II 98 - 106

UNIT – 8 FUNCTIONS 107 - 127

MODULE 3 GRAPH THEORY

UNIT – 9 GRAPH THEORY – BASICS 128 - 139

UNIT – 10 PATHS AND CIRCUITS 140 - 155

UNIT – 11 PLANAR GRAPHS AND COLORING 156 - 167

UNIT –12 GRAPH ALGORITHMS 168 - 179

MODULE 4 ALGEBRAIC STRUCTURES

UNIT – 13 INTRODUCTION 180 - 195

UNIT – 14 SUBGROUPS 196 - 211

UNIT – 15 ISOMORPHISM AND ALGEBRAIC SYSTEM 212 - 222

UNIT – 16 INTRODUCTION TO CODING THEORY 223 - 238

Preface

This material is prepared to make the reader strong in selected topics of Discrete Mathematics which is absolutely essential for learning advanced subjects of Information Technology. This is a course designed for first semester students of M.Sc Information Technology curriculum. The material is also suitable for students enrolled in post graduate studies in Computer Science, Information Science / Technology, Computer Applications. Computers are being extensively used in daily life at all levels, for a variety of purposes and by organizations to individuals. Certain mathematical topics related to design of computers, algorithm design and applications of computer science are taught to students of Computer Science, Information Science / Technology, Computer Applications in the first year of the course. Discrete Mathematics for Computer Scientists may be a difficult course to teach and to learn for several reasons. This is a hybrid course. It is Mathematics but most of its contents are applications of Mathematics. The number of substantive and diverse topics covered in this course is high. The whole course is organized into four modules and each with four units. Each unit lists out a set of objectives. The reader is urged to identify and write answers to all questions at the end of each unit so that learning is complete. Also the material is to be treated like notes, which is not complete in itself. The reader should refer to original texts for all units for a thorough and complete understanding. Content of each module is given in brief next.

Module-1: Mathematical logic is an age old subject and finds its application in the circuit design of electronic computers. Sets are important structures from computer science point of view. These two topics are discussed extensively with plenty of illustrations in this module. Truth tables of simple and compound statements (using logic connectives on simple statements), equivalence of logic formulas, tautology, contradiction, duality, normal forms are discussed in the first two units of the module. Later two units focus on set theory. Set is a common concept which is introduced right from high school. Representation of sets, operations on sets, laws of set theory may be found in Part I in unit 3. Two primary methods of counting namely, permutation and combination, pigeon hole principle and induction are introduced in the last unit of this module.

Module-2: This module is about relations and an important type called recurrence relation. Representation of relation on sets in the form of graph and matrix, recurrence relations and the methods of finding explicit solutions to these are discussed in this module. Also functions which are particular relations are introduced in this module. Several supporting examples clear the definition and concepts to the reader.

Module-3: In this module, another interesting topic of Discrete Mathematics namely Graph Theory is elaborated. Graph theory has lots of applications in a variety of fields. Beginning from introduction, representation, some special sub graphs like paths, walks and circuits, as well as advanced concepts like planarity, coloring, matching problems are discussed in length in this module. Again as in the previous modules concepts are introduced with plenty of illustrations.

Module-4: Algebraic structures are not only important for Mathematicians. Computer Science is incomplete without knowledge of groups, rings and fields. Applications of these areas in Computer Science are numerous. Algebraic structures are introduced in this module. Monoid, semi group, group, sub group, normal group, are discussed in great detail here. A very important of application of group structure namely, encoding and decoding of information is outlined in the end. Also other structures like rings, fields are dealt with superficially in this module.

We have kept in mind the difficulty of self study, in particular topics in mathematics, and hence we have tried to make discussions simple and supported the concepts with numerous examples. As said in the beginning of the preface, it is important that the reader should go through original text(s) for a full appreciation of the subject and should address all questions given at the end of the units.

We thank everyone who helped us directly or indirectly in preparing this material. Without their support, this material would not have been a reality.

Dr. Lalitha Rangarajan & Dr. B. Sharada

Course Design and Editorial Committee

Prof. K. S. Rangappa
Vice Chancellor & Chairperson
Karnataka State Open University
Manasagangotri, Mysore – 570 006

Prof. Vikram Raj Urs
Dean (Academic) & Convener
Karnataka State Open University
Manasagangotri, Mysore – 570 006

Head of the Department – Incharge

Prof. Kamalesh
DIRECTOR IT&Technology
Karnataka State Open University
Manasagangotri, Mysore – 570 006

Course Co-Ordinator

Mr. Mahesha DM
Lecturer, DOS in Information
Technology
Karnataka State Open University
Manasagangotri, Mysore – 570 006

Course Writers

Dr. Lalitha Rangarajan **Modules 1 and 3** **Units 1-4 and 9-12**
Associate Professor
DoS in Computer Science
University of Mysore
Manasagangotri, Mysore – 570 006

And

Dr. B. Sharada **Modules 2 and 4** **Units 5-8 and 13-16**
Assistant Professor
DoS in Computer Science
University of Mysore
Manasagangotri, Mysore – 570 006

Publisher

Registrar
Karnataka State Open University
Manasagangotri, Mysore – 570 006

Developed by Academic Section, KSOU, Mysore
Karnataka State Open University, 2012

Further information on the Karnataka State Open University Programmes may be obtained from the University's Office at Manasagangotri, Mysore – 6.

Printed and Published on behalf of Karnataka State Open University, Mysore-6 by the **Registrar (Administration)**

MODULE 1: Mathematical logic and Set Theory

UNITS: 1 to 4

UNIT -1: MATHEMATICAL LOGIC - PART I

Structure

1.0 Objectives

1.1 Introduction

1.2 Notation

1.3 Logical connectives

1.4 Well formed formulas- WFF

1.5 Tautology and contradiction

1.6 Summary

1.7 Keywords

1.8 Questions

1.9 References

1.0 OBJECTIVES

After studying this unit, you will be able to

- ✓ Understand basic concepts of logic
- ✓ Understand simple and compound statements using connectives
- ✓ Compute truth values of compound statements
- ✓ Explain the importance of WFF, tautology & logical implication

1.1 INTRODUCTION

Logic is the discipline that deals with the methods of reasoning. On an elementary level, logic provides rules and techniques to determine whether a given statement (argument) is valid. Logical reasoning is used in mathematics to prove theorems, and in computer science to verify the correctness of programs. Logic has its applications in various other fields such as natural science, social science and physical science. Logic is extensively used in design of digital circuits. Here we discuss some basics of logic.

1.2 NOTATIONS

The fundamental objects we work with in arithmetic are numbers. In a similar way, the fundamental objects in logic are propositions .

Definition

A proposition is a statement (declaration) which, in a given context, can be said to be either true or false but not both.

Propositions are usually denoted by small letters such as p, q, r, s,...

Examples

1. The following statements are propositions.

(a) I like logic. (b) 3+4=5

2. The following sentences are not propositions.

(a)Let me go! (Exclamation)

(b) x+3=5 (x is unknown)

Definition -Truth value

The truth or the falsity of a proposition is called its truth value. If a proposition is true, we will indicate its truth value by the symbol T and if it is false by the symbol F.

Definition - Truth Table

The table showing the truth values of a statement is called a truth table. It is a compact way of listing symbols to show all possible truth values for a set of sentences.

Examples

If we denote the proposition "The number 3 is a prime number" by p, then the truth value of p is T. Similarly, if we denote the proposition "Every rectangle is a square" by q, then the truth value of q is F.

Statements can be connected by the words like 'not', 'and', 'or', 'conditional', 'bi-conditional' etc. These words are known as logical connectives. The statements which do not contain any of the connectives are called atomic statements or simple statements. For example the two statements *p* and *q* in the above example are simple statements. The common connectives are: 'negation', 'and', 'or', 'if then', 'if and only if' and 'equivalence'. We use the following notations to the corresponding connections.

Connectives	**Notations**
Negation	~
and	Λ
or	V
if-then	→
if and if only if	↔
equivalence	≡ (or ⇔)

1.3 LOGICAL CONNECTIVES

Definition - Negation (~)

A proposition obtained by inserting the word 'not' at an appropriate place in a given proposition is called the negation of the given proposition. The negation of a proposition p is denoted by ~ p read not p), the symbol '~' denoting the word 'not'.

Examples

1. Let the proposition "2 is a prime number" be denoted by *p*, i.e., p: 2 is a prime number.

Then ~ p: 2 is not a prime number.

2. q: Every rectangle is a square. Then ~q: Not every rectangle is a square.

Following is the truth table for negation.

p	~p
T	F
F	T

In the above example p is true and hence ~ p is false and q is false and therefore ~q is true. .

Definition – Conjunction (∧)

Conjunction is compound statement formed by using the word 'and' to combine two simple sentences. If p and q represent two simple statements, the conjunction of p and q is written symbolically as $p \wedge q$

Examples

Consider the following statements:

1. p: Ashok likes Mathematics and q: Deepa likes Science. Then the conjunction of these two statements is

   p ∧ q: Ashok likes Mathematics and Deepa likes Science.

2. p: Ram goes by plane and q: Sam goes by car. Then the conjunction of these two statements is

   p∧ q: Ram goes by plane and Sam goes by car.

Truth table for conjunctive statements is as follows:

p	q	p∧ q
T	T	T
T	F	F
F	T	F
F	F	F

The conjunction of two statements is true only when both the statements are true.

Definition – Disjunction (∨)

Disjunction is compound statement formed by using the word 'or' to combine two simple sentences. If p and q represent two simple statements, the disjunction of *p* and *q* is written symbolically as p ∨q

Examples

Consider the following statements:

1. p: It is summer in India, q: It is winter in Australia. The disjunction of the two statements is

   p ∨ q: It is summer in India or it is winter in Australia

2. p: It will rain, q: It will be hot. The disjunction of these two statements is

   p ∨ q: It will rain or it will be hot.

Truth table for disjunctive statements is as follows:

p	q	p∨ q
T	T	T
T	F	T
F	T	T
F	F	F

The disjunction of two statements is true when one of the statements is true.

Definition – Conditional (→)

A compound proposition obtained by combining two given propositions by using the words 'if ' and 'then' at appropriate places is called a conditional proposition or just a conditional.

Examples

1. Let p: I study well.   q: I will get distinction.
   Then, p → q: If I study well, then I will get distinction.
2. Let p: Ramya is interested in discrete mathematics.   q: Ramya will find a good job.
   Then, p → q: If Ramya is interested in discrete mathematics then Ramya will find a good job.

A conditional is sometimes called an implication. Thus, we may also read the symbol for conditional p → q as p implies q. The antecedent usually follows the word 'if' and the consequent usually follows the word 'then'. Given below is the truth table for condition statement or implication.

p	q	p→ q
T	T	T
T	F	F
F	T	T
F	F	T

The implication is false when antecedent is true but not the consequent.

Definition – Bi conditional (↔)

Let p and q be two propositions. Then the conjunction of the conditionals p → q and q → p is called the bi conditional of p and q, it is denoted by p ↔ q. Thus p ↔ q is the same as (p → q) ∧ (q → p). As such p ↔ q is read as 'if p then q and if q then p'. The truth table for bi conditional statement is given by,

p	q	p→ q	q→ p	p ↔ q
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Examples

1. 2+2 = 4 if and only if 3+5 = 8
2. Bangalore is cosmopolitan city if and only if people of Bangalore are from all parts of India.
3. p: You can take the train. q: You buy a ticket. Then the bi conditional statement is,

   p ↔ q: You can take the train if and only if you buy the ticket.

Definition – Converse

If p → q is a statement then q→ p is called converse and the truth table for converse is as follows:

p	q	p→ q	q→ p
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Definition – Inverse

If p → q is a statement then ~p→ ~q is called inverse and the truth table for inverse is as follows:

p	q	~p	~q	~p → ~q
T	T	F	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Definition – Contra positive

If p → q is a statement then ~q→ ~p is called contra positive and the truth table for contra positive is as follows:

p	q	~p	~q	~q → ~p
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Example

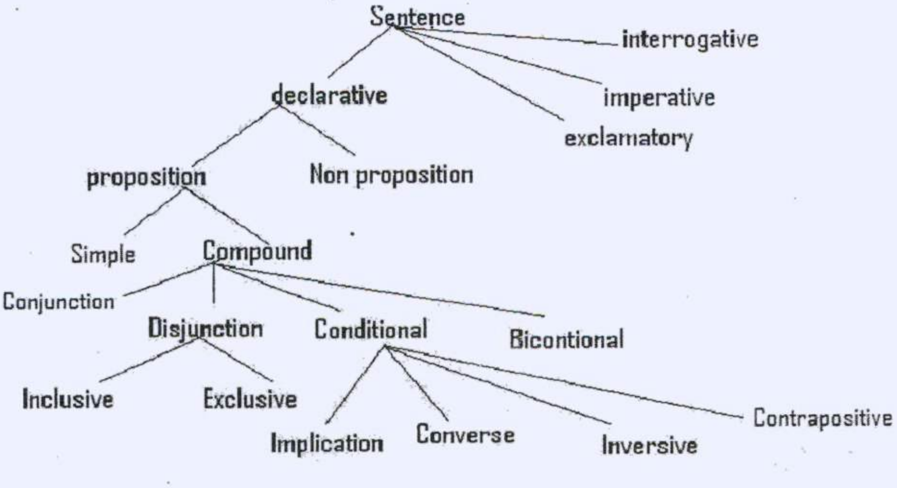
Let p: It's -6^0 and q: It's cold.

The converse of p → q is q → p: If it is cold, then it's -6^0.

The inverse of p → q is ~p → ~q: If it is not -6^0 then it is not cold.

Contra positive of p → q is ~q → ~p: if it is not cold then it is not -6^0

Various types of sentences and propositions can be summarized using a diagram below:



Definition - Other Connectives

We now introduce the connectives NAND, NOR which have useful applications in the design of computers.

The word NAND is a combination of "NOT" and "AND" where NOT stands for negation and AND stands for the conjunction. It is denoted by the symbol ↑.

If p and q are two propositions then p ↑ q is nothing but ~ (p ∧ q). The truth table of NAND is given by,

p	q	p ∧ q	p ↑ q
T	T	T	F
T	F	F	T
F	T	F	T
F	F	F	T

Connective NOR is a combination of "NOT" and "OR", where NOT stands for negation and OR stands for the disjunction. The connective NOR is denoted by the symbol ↓, and is called joint p ↓ q is read as "Neither p nor q". The truth table of NOR is given by,

p	q	p ∨ q	p ↓ q
T	T	T	F
T	F	T	F
F	T	T	F
F	F	F	T

1.4 WELL FORMED FORMULAS (WFF)

A statement formula contains one or more simple statements and some connectives. If p and q are any two statements, then p ∨ q, p ∧~ p ∧ q are some statement formulas derived from the statements variables p and q, where p and q are called components of the statement formulas. A statement formula has no truth value. It is only when the statement variables in a statement formula are replaced by definite statement that we get a statement, which has a truth value that depends upon the truth values of its statements used in replacing the variables. A statement formula is a string consisting of variables, parentheses and connective symbols. A statement formula is called a Well formed formulas (WFF) if it can be generated by the following rules:

1. A statement variable p standing alone is a well formed formula.

3. If p and q are well formed formulas, then $p \wedge q$, $p \vee q$, $p \rightarrow q$ and $p \leftrightarrow q$ are well formed formulas.

3. A string of symbols is a well formed if and only if it is obtained by finitely many applications of the rules 1, 2.

According to the above recursion definition of a well formed formula, the formulas, $\sim (p \vee q)$, $(\sim p \wedge q)$, $p \rightarrow (p \wedge q)$ are well formed formulas.

A statement formula is not a statement and has no truth values. But if we substitute definite statements in place of variables in a given formula we get a statement. The truth value of this resulting statement depends upon the truth values of the statement substituted for the variables, which appears as one of the entries in the final column of the truth table constructed. Therefore, the truth value of a well formed formula is the summary of truth values of the resulting statements for all possible assignments of truth values of the variables appearing in the formula. The final column entries of the truth table of a well formed formula give the truth value of the formulas.

Examples

1. $p \vee \sim q$ is a well formed formula. The truth table of this formula is:

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

For instance, let p: It is summer and q: It is cool.

Suppose it is month of March in Bangalore then p is true and q is false and the truth value of $p \vee \sim q$ from the table (row 2) is T.

Suppose it is month of November in Bangalore then p is false and q is true and from row 3, the WFF $p \vee \sim q$ is false.

Note that as said above the truth value of component statements decide the truth value of the given WFF.

2. $\sim(p \wedge q) \vee r$ is a well formed formula.

The truth table of this formula is given in the table below.

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

If p, q and r are T, F, T then from the table it is evident that the WFF $\sim(p \wedge q) \vee r$ is T (refer row 3). If truth values of components p, q, r are F, F, T then the truth value of WFF $\sim(p \wedge q) \vee r$ is T (refer row 7 of the table).

1.5 TAUTOLOGY AND CONTRADICTION

Propositional logic is to study of propositions and the propositional connectives. It is the study not only of one particularly interpretation of a formula but also of what can be deduced about all interpretations of a formula of particular interest are those formulas that are true "by virtue of pure logic". Here we introduce the concept of tautology and contradiction. A tautology is a WFF which is **true** independent of the truth values of its components. A contradiction is a WFF which is **false** independent of the truth values of its components.

Examples –Tautologies

1. $(p \wedge (p \rightarrow q)) \rightarrow q$

Examination of the truth table of the statement reveals that WFF is always true independent of the status of its components.

p	q	p→ q	p ∧ p→ q	p ∧ (p→ q) → q
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

2. (p→ q) ↔ (~p ∨ q) is a tautology. Truth table of this compound statement is given here.

p	q	p→ q	~p	~p ∨ q	(p→ q) ↔ (~p ∨ q)
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Examples –Contradictions

1. (p ∧ q) ∧~ p is a contradiction. We see from its truth table that we get the truth value of this WFF to be false irrespective of the component truth values.

p	q	p∧ q	~p	(p ∧ q) ∧~ p
T	T	T	F	F
T	F	F	F	F
F	T	F	T	F
F	F	F	T	F

WFF that are neither tautology nor contradiction are called contingency. All well formed formulas in sections 1.3 and 1.4 are contingencies.

1.6 SUMMARY

In this unit mathematical logic is introduced. In section 1.1 some applications of this theory is briefed. Notations for understanding of the discussion are discussed in the next section. Section 1.3 gives a detailed account of all operations of the mathematical logic. The section next we present WFF and then discuss the concept of tautology and contradiction, which are WFF always true and always false.

1.7 KEYWORDS

Mathematical logic, Logical operators, Well formed formulas, Tautology, Contradiction

1.8 QUESTIONS

1. Mention some statements whose truth values are true / false.
2. Define and write the truth tables of all operators.
3. Construct truth tables for $p\vee\sim q$, $(p\vee q)\vee\sim p$, $p\vee(q\wedge r)$, $\sim p\vee(q\wedge r)$.
4. What is bi conditional statement and find the truth table of such a statement.
5. Define well formed formulas and give example statements that are WFF and those that are not.
6. Construct truth table for the bi conditional statement $\sim(p\vee q) \leftrightarrow (\sim p\wedge\sim q)$.
7. What is tautology, contradiction and contingency?
8. Give some WFF that are tautologies and contradictions.

1.9 REFERENCES

1. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL
2. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
3. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

UNIT -2: MATHEMATICAL LOGIC - PART II

Structure

2.0 Objectives

2.1 Equivalence

2.2 Tautological implications

2.3 Duality

2.4 Normal forms

2.5 Inference

2.6 Summary

2.7 Keywords

2.8 Questions

2.9 References

2.0 OBJECTIVES

When you have gone through this unit, you will be able to

- ✓ Find out when two compound statements are equivalent
- ✓ Understand the concept of duality
- ✓ Work out normal forms for any statement
- ✓ Make new inferences from a set of premises

2.1 EQUIVALENCE

Two propositions p and q are said to be logically equivalent or simply equivalent if $p \rightarrow q$ is a tautology. Let p and q be two well formed formulas having n components. The statement formulas p and q are said to be equivalent if they have the same truth values for all 2^n combinations of individual n components. Equivalence is denoted by ⇔ or ≡.

Examples

1. $\sim\sim p \equiv p$

Let us examine the truth table of both expressions.

p	$\sim p$	$\sim\sim$**p**
T	F	**T**
F	T	**F**

The truth values of p and $\sim\sim p$ are the same. Hence they are equivalent.

2. $p \vee \sim p \equiv q \vee \sim q$

Truth tables of both expressions given below imply that both expressions are equivalent.

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

3. $(p \vee \sim p)\vee q \equiv q$ are equivalent and truth table of both expressions are one and the same.

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

Some equivalent formulas are given here.

1. Idempotent laws: $a \vee a \equiv a$ (b) $a \wedge a \equiv a$
2. Commutative laws: (a)$p \vee q \equiv q \vee p$ (b) $p \wedge q \equiv q \wedge p$
3. Associative laws: (a) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ (b) $(p \vee q) \vee r \equiv p\vee (q \vee r)$
4. Distributive laws: (a) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (b) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
5. Identity laws: (a) (i) $p \vee f \equiv p$ (ii) $p \vee t \equiv t$ (b) (i) $p \wedge f \equiv f$ (ii) $p \wedge t \equiv p$
6. Complement laws: (a) (i) $p \vee f \equiv p$ (ii)$p\vee \sim p \equiv t$

   (b)(i) $p\wedge \sim p \equiv f$ (ii) $\sim t \equiv f$, $\sim f \equiv t$
7. De-Morgan's laws: (a) $\sim (p \wedge q) \equiv\sim p\vee \sim q$ (b) $\sim (p \vee q) \equiv \sim p\wedge \sim q$

where t and f are used to denote the variables which are restricted to the truth values true and false respectively.

Proof for De Morgan's laws

p	q	$p \vee q$	$\sim(\mathbf{p} \vee \mathbf{q})$	$\sim p$	$\sim q$	$\sim\mathbf{p} \wedge \sim\mathbf{q}$
T	T	T	**F**	F	F	**F**
T	F	T	**F**	F	T	**F**
F	T	T	**F**	T	F	**F**
F	F	F	**T**	T	T	**T**

p	q	$p \wedge q$	$\sim(\mathbf{p} \wedge \mathbf{q})$	$\sim p$	$\sim q$	$\sim\mathbf{p} \vee \sim\mathbf{q}$
T	T	T	**F**	F	F	**F**
T	F	F	**T**	F	T	**T**
F	T	F	**T**	T	F	**T**
F	F	F	**T**	T	T	**T**

Another important equivalence very useful in proving theorems is $(\mathbf{p} \rightarrow \mathbf{q}) \equiv \sim\mathbf{p} \vee \mathbf{q}$

p	q	$\mathbf{p} \rightarrow \mathbf{q}$	$\sim p$	$\sim\mathbf{p} \vee \mathbf{q}$
T	T	**T**	F	**T**
T	F	**F**	F	**F**
F	T	**T**	T	**T**
F	F	**T**	T	**T**

Some more equivalence formulas with three prepositions are given here.

(i) $a \rightarrow (b \vee c) \equiv (a \rightarrow b) \vee (a \rightarrow c)$

(ii) $(a \rightarrow b) \wedge (c \rightarrow b) \equiv (a \vee c) \rightarrow b$

(iii) $(\sim p \wedge (\sim q \vee r)) \vee (q \wedge r) \vee (p \wedge r) \equiv r$

(iv) $((a \vee b) \wedge \sim(\sim a \wedge (\sim b \vee \sim c))) \vee ((\sim a \wedge \sim b) \vee (\sim a \wedge \sim c))$ is tautology

The equivalence of (i) and (ii) is proved using truth tables. Equivalence can also be shown using simplification. This is how (iii) and (iv) are solved.

Truth table for equivalence of (i)

a	b	c	$b \vee c$	$\mathbf{a \to (b \vee c)}$	$a \to b$	$a \to c$	$\mathbf{(a \to b) \vee (a \to c)}$
T	T	T	T	**T**	T	T	**T**
T	T	F	T	**T**	T	F	**T**
T	F	T	T	**T**	F	T	**T**
T	F	F	F	**F**	F	F	**F**
F	T	T	T	**T**	T	T	**T**
F	T	F	T	**T**	T	T	**T**
F	F	T	T	**T**	T	T	**T**
F	F	F	F	**T**	T	T	**T**

Truth table for equivalence of (ii)

a	b	c	$a \to b$	$c \to b$	$\mathbf{(a \to b) \wedge (c \to b)}$	$a \vee c$	$\mathbf{(a \vee c) \to b}$
T	T	T	T	T	**T**	T	**T**
T	T	F	T	T	**T**	T	**T**
T	F	T	F	F	**F**	T	**F**
T	F	F	F	T	**F**	T	**F**
F	T	T	T	T	**T**	T	**T**
F	T	F	T	T	**T**	F	**T**
F	F	T	T	F	**F**	T	**F**
F	F	F	T	T	**T**	F	**T**

Equivalence of (iii) by simplification:

Solution:

$(\sim p \wedge(\sim q\wedge r)) \vee (q \wedge r) \vee (p\wedge r)$	
$\equiv ((\sim p \wedge\sim q)\wedge r) \vee (q \wedge r) \vee (p\wedge r)$	Associative law
$\equiv (\sim(p \vee q)\wedge r) \vee((q \vee p) \wedge r)$	De Morgan's law and distributive law
$\equiv (\sim(p \vee q)\wedge r) \vee((p \vee q) \wedge r)$	Commutative law
$\equiv (\sim(p \vee q) \vee (p \vee q)) \wedge r$	Distributive law
$\equiv T \wedge r$	$(\sim(p \vee q) \vee (p \vee q))$ is tautology
$\equiv r$	

Equivalence of (iv) by simplification:

Solution:

Let $x = ((a \vee b)\wedge \sim(\sim a\wedge (\sim b \vee\sim c)))$	
$\equiv (a \vee b)\wedge \sim(\sim a\wedge (\sim(b \wedge c))$	De Morgan's law
$\equiv (a \vee b)\wedge (a\vee (b \wedge c))$	De Morgan and complement law
$\equiv (a \vee b)\wedge (a \vee b)\wedge (a \vee c)$	Distributive law
$\equiv (a \vee b)\wedge (a \vee c) \quad \ldots (1)$	Idempotent law
Let $y = ((\sim a\wedge\sim b) \vee (\sim a \wedge\sim c))$	
$\equiv \sim(a\vee b) \vee \sim(a \vee c)$	De Morgan's law
$\equiv \sim((a\vee b) \wedge (a \vee c))$	De Morgan's law
$\equiv \sim x$	(from (1))

Now (iv) is same as $x \vee y \equiv x \vee\sim x \equiv T$

Thus given statement is a tautology.

Logic problems can also be solved by contradiction. Here are some examples. The proof procedure is called proof by refutation.

(i) Let k^2 be an odd integer. Show that k is odd.

Solution:

Assume contrary what has to be proved. Assume k to be even. Let k=2c. Then $k^2 = 4c^2 = 2(2c^2)$. That is k^2 even. Thus there is contradiction to given statement: k^2 odd integer. The contradiction is due to the assumption that k is even. Thus the assumption is wrong. Hence k is odd.

(ii) Prove that √2 is irrational.

Solution:

Assume √2 is rational. Suppose that there elitists integers p and q so that √2 = p/q (here pand q do not have a common factor).

Squaring the above equation we get $2 = p^2/q^2$.

That is, $p^2 = 2\ q^2$. Hence p^2 is even. Let p=2k. Then $p^2 = 4k^2 = 2\ q^2$. Thus $q^2 = 2\ k^2$.

Both and are even means that p and q are even. Thus p and q have a common factor of 2. This contradicts our assumption .Thus our assumption that √2 is rational is wrong. That is√2 is irrational.

2.2 TAUTOLOGICAL IMPLICATIONS

Definition

Let p and q be two statements. The statement p is said to tautologically imply q if and only if p→ q is a tautology. The tautological implication is represented as p ⇒ q and read as "p implies q". We now give some simple tautological implications.

Examples

(i) $(a \wedge b) \Rightarrow a$

(ii) $(a \wedge b) \Rightarrow (a \rightarrow b)$

(iii) $a \Rightarrow (a \rightarrow b)$

(iv) $(a \rightarrow (b \rightarrow c)) \Rightarrow ((a \rightarrow b) \rightarrow (a \rightarrow c))$

Truth table for (i)

a	b	$a \wedge b$	$(a \wedge b) \rightarrow a$
T	T	T	**T**
T	F	F	**T**
F	T	T	**T**
F	F	T	**T**

Truth table for (ii)

a	b	a ∧ b	a→b	**(a ∧ b)→ (a→b)**
T	T	T	T	**T**
T	F	F	F	**T**
F	T	F	T	**T**
F	F	F	T	**T**

Truth table for (iii)

a	b	b → a	**a →(b→a)**
T	T	T	**T**
T	F	T	**T**
F	T	F	**T**
F	F	T	**T**

Truth table for (iv)

a	b	c	b →c	a→ x	a→ b	a→ c	y→ z	**u→ v**
			x	u	y	z	v	
T	T	T	T	T	T	T	T	**T**
T	T	F	F	F	T	F	F	**T**
T	F	T	T	T	F	T	T	**T**
T	F	F	T	T	F	F	T	**T**
F	T	T	T	T	T	T	T	**T**
F	T	F	F	T	T	T	T	**T**
F	F	T	T	T	T	T	T	**T**
F	F	F	T	T	T	T	T	**T**

2.3 DUALITY

Definition

Let p and p' be two formulas. If p can be obtained from p' or if p' can be obtained from p by replacing $\wedge$ by $\vee$, $\vee$ by $\wedge$, T by F and F by T, then the statements p and p' are called dual statements.

Examples

Dual of the following statements are:

(i) $(a \vee b) \wedge (c \vee d)$

(ii) $(a \wedge b) \vee T$

(iii) $\sim(a \vee b) \wedge (a \vee \sim(b \wedge \sim c))$

(iv) $(p \vee q) \wedge r$

Solution:

Changing $\wedge$ by $\vee$, $\vee$ by $\wedge$, T by F and F by T we get the dual statements as follows:

(i) $(a \wedge b) \vee (c \wedge d)$

(ii) $(a \vee b) \wedge F$

(iii) $\sim(a \wedge b) \vee (a \wedge \sim(b \vee \sim c))$

(iv) $(p \wedge q) \vee r$

2.4 NORMAL FORMS

Although two formulas may be logically equivalent, one may be "easier" for someone to understand or to manipulate. It may be fairly obvious that one formula is a tautology but quite difficult to conclude that from the other form of the same formula. Decision of tautology or contradiction using logic table is difficult because a formula with n components contains 2^n rows. In this section, we discuss two special forms or representations for formulas logically equivalent to a given formula. These forms are ***disjunctive*** and ***conjunctive normal forms***. If the formula is expressed as sequence of elementary statements connected by $\wedge$ (this form is called conjunctive normal form) then when of the statement is false then compound statement is false (given statement is contradiction). On the other hand if the compound is expressed as composition of simple statements connected only by $\vee$ (this form is called disjunctive normal form) then if one of the statement is true then the compound statement is true (given statement is tautology).

Disjunctive Normal Form: Consider the following two formulas,

$$\varphi=(p\rightarrow(q\vee r))\leftrightarrow(q\rightarrow p) \text{ and}$$
$$\psi=(p\wedge q)\vee(p\wedge r\wedge\sim q)\vee(\sim p\wedge\sim q)$$

The truth table for φ and ψ would show that these two formulas are logically equivalent. By some measures, ψ is more complicated. For example φ has four propositional connectives, whereas ψ has five connectives. Nevertheless, many people find ψ to be far easier to understand. The formula ψ explicitly lists three cases in which the formula is true.

1. p and q are both T.

2. p and r are T and q is F.

3. p and q are both F.

For all other interpretation of p, q and r the truth value of ψ is F. It is not nearly so obvious what φ "says". Although φ is shorter, it is much more complex.

A formula like ψ that is just a list of cases that make the formula have a truth value of T is called a disjunctive normal form (DNF). Each of the three cases $(p \wedge q)$, $(p\wedge \sim q \wedge r)$ and $(\sim p\wedge \sim q)$ is called a term. One might think of each term as describing single case. The entire disjunctive normal form formula is just a disjunction of terms that make the formula T. One might think of each term as describing single case. The entire disjunctive normal form formula is just a disjunction of terms that make the formula T. (The words term and disjunctive normal form will be defined formally below). The difference in comprehensibility is even more extreme if the formula φ is negated. The formula $\sim ((p \rightarrow (q \vee r)) \leftrightarrow (q \rightarrow p))$ is logically equivalent to the disjunctive normal form formula $(\sim p \wedge q) \vee (p\wedge \sim q\wedge \sim r)$. The disjunctive normal form is a disjunction of only two terms, which makes it particularly easy to understand.

Definition

Let p be a proposition letter. Then, p is positive literal, and ~ p is a negative literal. A literal is a positive literal or a negative literal.

Definition

Let λ_1, $\lambda_{2,} \ldots\lambda_m$ be a set of m literals with m is a natural number (positive integer). A conjunctive normal form (CNF) is the conjunction $\lambda_1 \wedge \lambda_2 \wedge \ldots \wedge \lambda_m$ of m literals. A formula φ is in DNF if it is a disjunction $\varphi_1 \vee \varphi_2 \vee \ldots \vee \varphi_k$ of k terms where k is a natural number.

The disjunction of zero formulas is F. The conjunction of zero formulas is T. This is analogous to defining the sum of zero numbers to be zero and the product of zero numbers to be 1.

For example, the formula $(a \wedge b \wedge c) \vee (\sim a \wedge \sim b \wedge \sim c) \vee (a \wedge \sim c \wedge q)$ is in disjunctive normal form. $(a \wedge b \wedge c)$ is a term. As another example consider T. It is conjunction of zero literals.$(a \wedge b \wedge c)$ is in conjunctive normal form.

We now focus on conversion of a given statement to DNF or CNF. We first make a truth table of the given compound statement. We then identify the compound statements for which the final formula is T. Now the given statement is disjunction of all these compound statements.

Example

Disjunctive normal form of $\psi = (\sim (p \rightarrow q)) \rightarrow (q \wedge \sim r)$

Truth table of the given expression is as follows:

p	q	r	$(\sim (p \rightarrow q)) \rightarrow (q \wedge \sim r)$
T	**T**	**T**	**T**
T	**T**	**F**	**T**
T	F	T	F
T	F	F	F
F	**T**	**T**	**T**
F	**T**	**F**	**T**
F	**F**	**T**	**T**
F	**F**	**F**	**T**

In the table above, all rows that result in T for the final statement is in bold font. Now the DNF is collection of all compound statements corresponding to these rows connected by ∨ given by,

$(p \wedge q \wedge r) \vee (p \wedge q \wedge \sim r) \vee (\sim p \wedge q \wedge r) \vee (\sim p \wedge q \wedge \sim r) \vee (\sim p \wedge \sim q \wedge r) \vee (\sim p \wedge \sim q \wedge \sim r)$.

To convert a given statement to CNF we negate the statement and find the truth table. Now equivalent conjunctive normal form is found from those compound statements which has T in the table in the last (corresponding to given statement). Consider the same example above namely, the expression: $(\sim (p \to q)) \to (q \land \sim r)$

Now let φ be the negation of this statement. That is $\varphi = \sim((\sim (p \to q)) \to (q \land \sim r))$. The truth table of φ is as given below.

p	q	r	$\sim(\sim (p \to q)) \to (q \land \sim r)$
T	T	T	F
T	T	F	F
T	**F**	**T**	**T**
T	**F**	**F**	**T**
F	T	T	F
F	T	F	F
F	F	T	F
F	F	F	F

DNF of the given statement is $\sim ((p \land \sim q \land r) \lor (p \land \sim q \land \sim r))$. Push ~ inside. We then get

$(\sim (p \land \sim q \land r)) \land (\sim(p \land \sim q \land \sim r))$ De Morgan's law

$= (\sim p \lor q \lor\land\sim r) \land (\sim p \lor q \lor r)$ (CNF) De Morgan's law

2.5 INFERENCE

In mathematical logic, assumptions or axioms or hypotheses are called premises. Inference is based on premises. A number of premises lead to conclusion (opinion). The process of arriving at conclusions is called inference. Inference can be made using logic table.

Inference using table

Let a and b be two statements formulas. Suppose b is the conclusion based on the premise a.

Then b is valid conclusion if and only if a → b is a tautology. It is called **a implies b** and denoted by a ⇒ b.

Conclusion

Let p_1, p_2, …p_n be n premises. Conclusion c is arrived at if $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow c$ is a tautology. This is denoted by $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \Rightarrow c$.

Examples

(i) Show that premise q leads to a conclusion $p \vee q$

(ii) Determine whether b can be concluded from the premises p_1: a → b, p_2: a and from the premises p_3: a → b, p_4: ~a

Solution:

(i) Find the truth table of $q \rightarrow (p \vee q)$

p	q	$p \vee q$	$q \rightarrow (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

As $q \rightarrow (p \vee q)$ is tautology, the premise q implies $(p \vee q)$.

(ii) Find the truth table of $(p_1 \wedge p_2) \rightarrow b$

a	b	a→ b p_1	$p_1 \wedge p_2$	$(p_1 \wedge p_2) \rightarrow b$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

As $(p_1 \wedge p_2) \rightarrow b$ is tautology, the premise p_1, p_2 leads to the conclusion b.

(iii) Find the truth table of $(p_3 \wedge p_4) \rightarrow b$

a	b	$a \rightarrow b$	~a	$(p_3 \wedge p_4)$	$(p_3 \wedge p_4) \rightarrow b$
		p_3	p_4		
T	T	T	F	F	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	F

As $(p_3 \wedge p_4) \rightarrow b$ is not tautology, p_3, p_4 does not lead to conclusion b.

2.6 SUMMARY

In this unit concepts like equivalence of WFFs, tautological implication, duality of WFF, two important normal forms namely disjunctive and conjunctive forms and finally inference process given some set of premises are discussed in various sections, in detail with several examples.

2.7 KEYWORDS

Equivalence of two statements, Tautological implication, Disjunctive normal form, Conjunctive normal form, Dual of WFF, Inference principles

2.8 QUESTIONS

1. Define equivalence.
2. State all equivalence laws.
3. Show that $\sim(a \leftrightarrow b) \equiv (a \vee b) \wedge \sim (a \wedge b)$
4. What do you mean by tautological implication? Give examples.
5. What is dual of a statement? Provide examples.
6. Define two normal forms. How do they help in finding if a statement is true or false?

7. How do you find the normal forms?
8. Find the two normal forms of $\sim(a\vee b) \leftrightarrow (a \vee b)$ and $\sim(p\rightarrow r)\vee (q\leftrightarrow p)$
9. Explain the process of inference and conclusion.

2.9 REFERENCES

1. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL
2. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
3. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

UNIT -3: SET THEORY- PART I

Structure

3.0 Objectives

3.1 Introduction

3.2 Basics

3.3 Set Types

3.4 Representation of Sets

3.5 Operations on Sets

3.5.1 Properties of set operations

3.6 Inclusion and Exclusion

3.7 Induction

3.8 Summary

3.9 Keywords

3.10 Questions

3.11 References

3.0 OBJECTIVES

When you have learnt the contents of this unit, you will be able to

- ✓ Understand the different types of sets
- ✓ Do simple problems using set operators
- ✓ Appreciate the power of induction principle in solving problems

3.1 INTRODUCTION

Set theory is being used in various fields of science and engineering. The main purpose of set theory is to study the importance of discrete objects and relationships among them. This unit deals with different types of sets, set operations and principle of induction.

3.2 BASICS

Definition-Set

A set may be viewed as a collection of objects, the elements or members of the set. We will ordinarily use capital letters, A,B,X,Y,…., to denote sets, and lowercase letters, a,b,x,y,…, to denote elements of sets. The statement "p is an element of A," or, equivalently, "p belongs to A," is written as $p \in A$. The negation of $p \in A$ is written as $p \notin A$.

Examples

1. A={Students of first semester M.Sc in KSOU}

   Each student is an element of set A.

2. B={1, 2, 3, 5, 7} or B={set of all positive integers that are prime and < 10}

   1, 2, 3, 5, 7 are members of the set B. i.e., 1 □ B, 2 □ B …

3. C={1, 2, 3, x, y, z}, Now $1 \in C$, $z \in C$, $5 \notin C$.

4. D=Letters of the word BANGALORE or D={B, A, N, G, L, O, R, E}

Observe that letter A is to be listed only once in the set.

All these are finite sets. Cardinality of a set is number of elements in the set. For instance, cardinalities of sets A, B, C and D are:

1. Number of students in first semester M.Sc of KSOU.
2. 5
3. 6
4. 8

Representation of a set

Sometimes it is inconvenient or impossible to mention individual elements of the set. Then we state the property which characterizes the elements of the set. The sets A and D in the above example are represented by the property of their elements. More examples of this type are given here.

Examples

1. E={x : x is an integer, x>0}

   Which reads "E is the set of x such that x is an integer and x is greater than 0," denotes the set E whose elements are the positive integers. A letter, usually x, is used to denote a typical member of the set; the colon is read as "such that" and the comma as "and".

2. F={x : x is a letter in the English alphabet, x is a vowel} or F={a, e, i, o, u}
3. G={x : x^2-3x+2=0}. In other words, G consists of those numbers which are solutions of the equation x^2-3x+2=0, sometimes called the solution set of the given equation. Since the solution of the equation are 1 and 2, we could also write G={1, 2}.
4. A= { x : x^2-3x+2=0}, B={2,1} and C={1,2,2,1,6/3}. Then A=B=C. Observe that a set does not depend on the way in which its elements are displayed. A set remains the same if its elements are repeated or rearranged.

Even if we can list the elements of a set, it may not be practical to do so. For example, we would not list the members of set of people born in the world during the year 1976 although theoretically it is possible to compile such a list. That is, we describe a set by listing its elements only if the set contains a few elements; otherwise we describe a set by the property which characterizes its elements.

The fact that we can describe a set in terms of a property is formally stated as the principle of abstraction.

3.3 SET TYPES

In section 3.2 we discussed some examples of sets, some of these finite, (A, B, C, D) and some infinite (E). We here discuss more types of sets.

Countable Set

If we can count elements of a set (equivalently if elements of a set are discrete) then the set is countable. All sets in the examples of previous section are countable. Note that countable set can also be infinite (E).

Uncountable Set

If the elements of a set cannot be enumerated, then the set is uncountable. For instance, the set of real numbers in the interval (1, 10) is an uncountable set.

Universal Set

In the application of the theory of sets, the members of all sets under investigation usually belong to some fixed large set called the universal set or universe of discourse. For example, in plane geometry, the universal set consists of all the points in the plane; and in human population studies the universal set consists of all the people in the world. We will let the symbol ***U*** to denote the universal set unless otherwise stated or implied.

Empty Set

For a given set U and a property P, there may not be any elements of U which have property P. For example the set

$$S=\{x: x \text{ is positive integer}, x^2=3\}$$

has no elements, since no positive integer has the required property.

The set with no elements is called the empty set or null set and is denoted by Φ.

Subsets

If every element of a set A is also an element of a set B, then A is called a subset of B. We also say that A is contained in B or B contains A. This relation is written as:

$$A \subset B \quad or\, B \supset A$$

If A is not a subset of B, i.e., if at least one element of A does not belong to B, we write

$$A \not\subset B\, or\, B \not\supset A$$

Examples

1. Consider the sets A={1, 3, 4, 5, 8, 9} B={1, 2, 3, 5, 7} C={1, 5} Then $C \subset A\ and\ C \subset B$ since 1 and 5, the elements of C, are also members of A and B. But $B \not\subset A$ since some of its elements, e.g. 2 and 7 do not belong to A. Furthermore, since the elements of A, B and C must also belong to the universal set U, we have that U must at least contain the set {1, 2, 3, 4, 5, 7, 8, 9}.
2. Some sets of numbers occur very often and so we use special symbols for them. Unless otherwise specified, we will let:

   N=the set of positive integers: 1, 2, 3,...
   Z=the set of integers: ...,-2, -1, 0, 1, 2,...
   Q=the set of rational numbers
   R=the set of real numbers

   The above sets are related as follows:

   $$\boldsymbol{N} \subset \boldsymbol{Z} \subset \boldsymbol{Q} \subset \boldsymbol{R}$$

3. The set E={2,4,6} is a subset of the set F={6,2,4}, since each number 2,4 and 6 belonging to E also belongs to F. In fact, E=F. In a similar manner it can be shown

that every set is a subset of itself.

Every set A is a subset of the universal set U since, by definition all the members of A belong to U. Also the empty set $\emptyset$ is a subset of A.

As noted above, every set is a subset of itself since, trivially the elements of A belong to A. If every element of a set A belongs to a set B, and every element of B belongs to a set C, then clearly, every element of A belongs to C. In other words, if $A \subset B$ and $B \subset C$, then $A \subset C$.

If $A \subset B$ and $B \subset A$, then A and B have the same elements, i.e. $A=B$. Conversely, if $A=B$, then $A \subset B$ and $B \subset A$ since every set is a subset of itself.

We state the above results formally:

Theorem 3.1

(i) For any set A, we have $\emptyset \subset A \subset U$

(ii) For any set A, we have $A \subset A$

(iii) If $A \subset B$ and $B \subset C$, then $A \subset C$

(iv) $A=B$ if and only if $A \subset B$ and $B \subset A$

Remark: If $A \subset B$, it is still possible that $A=B$. Some authors write $A \subseteq B$ to indicate that A is a subset of B, and write $A \subset B$ to indicate that A is a subset of B but is not equal to B.

Definition - Power Set

If A is a set, the set of all subsets of A is called the power set of A. It is denoted by P (A).

Examples

1. Let $A=\{a,b,c\}$

Power set, $P(A)=\{ \emptyset, \{a\},\{b\},\{c\},\{a, b\},\{b, c\},\{a, c\},\{a, b, c\}\}$.

2. Find (i) P(A), (ii) Cardinality of A, (iii) $|P(A)|$, for the sets (a) $A=\{3,7,9\}$, (b) $A=\{a, e, i, o\}$.

Solution

(a) $A=\{3,7,9\}$

(i) Power set, $P(A)=\{ \emptyset, \{3\},\{7\},\{9\}, \{3,7\},\{7,9\},\{3,9\},\{3,7,9\}\}$

(ii) Cardinality of A, $|A|=3$.

(iii) Cardinality of $P(A)=|P(A)|=8$.

(b) $A=\{a, e, i, o\}$

(i) $P(A) = \{ \emptyset, \{a\},\{e\},\{i\},\{o\},\{a, e\},\{a, i\},\{a, o\},\{e, i\},\{e, o\},\{i, o\},$

$\{a, e, i\},\{a, e, o\},\{e, i, o\},\{a, i, o\},\{a, e, i, o\}\}$.

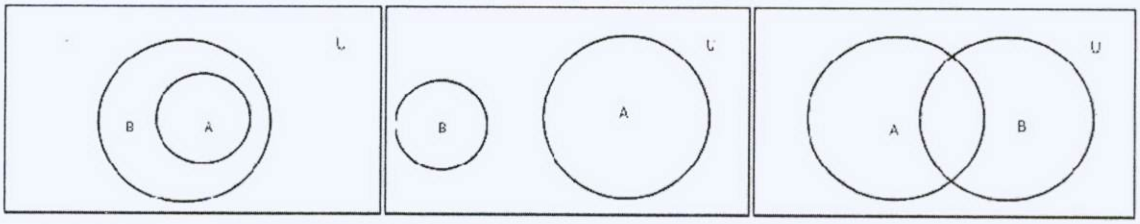
(ii) $|A| =4$.

(iii) $|P (A)|=16$.

3.4 REPRESENTATION OF SETS

Venn Diagrams

A Venn diagram is a pictorial representation of sets by set of points in the plane. The universal set U is represented by the interior of a rectangle, and the other sets are represented by disks lying within the rectangle. If $A \subset B$, then the disk representing A will be entirely within the disk representing B as in fig 3.1(a). If A and B are disjoint, i.e., have no elements in common, then the disk representing A will be separated from the disk representing B as in fig 3.1(b).



(a) $A \subset B$ (b) A and B are disjoint (c)

Fig 3.1

However, if A and B are two arbitrary sets, it is possible that some objects are in A but not in B. Some are in B but not in A. Some are in both A and B, and some are neither in A nor in B; hence in general we represent A and B as in fig 3.1(c).

3.5 OPERATIONS ON SETS

Union and Intersection

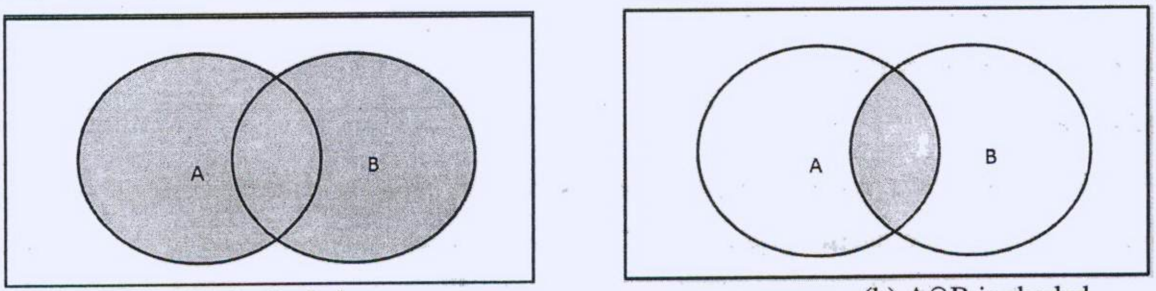
The union of two sets A and B, denoted by A U B, is the set of all elements which belong to A or to B. That is,

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

Here "or" is used in the sense of and/or. Figure 3.2(a) is a Venn diagram in which A U B is shaded. 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:

$$A \cap B = \{ x : x \in A , x \in B \}$$

Figure 3.2(b) is a Venn diagram in which $A \cap B$ is shaded.



(a) $A \cup B$ is shaded.

(b) $A \cap B$ is shaded.

Fig 3.2

Examples

3. Let $A=\{1, 2, 3, 4\}$, $B=\{3, 4, 5, 6, 7\}$, $C=\{2, 3, 5, 7\}$. Then

$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$ $\quad$ $A \cap B = \{3, 4\}$

$A \cup C = \{1, 2, 3, 4, 5, 7\}$ $\quad$ $A \cap C = \{2, 3\}$

$B \cup C = \{ 2, 3, 4, 5, 6, 7\}$ $\quad$ $B \cap C = \{3, 5, 7\}$

4. Let M denote the set of male students in a university C, and let F denote the set of female students in university C. Then

$$M \cup F = C$$

since each student in C belongs to either M of F. On the other hand,

$$M \cap F = \emptyset$$

since no student belongs to both M and F.

The operation of set inclusion is closely related to the operations of union and intersection, as shown by the following theorem.

Theorem 3.2

The following are equivalent: $A \subset B$, $A \cap B = A$, $A \cup B=B$.

Complements

Recall that all sets under consideration at a particular time are subsets of a fixed universal set U. The absolute complement or, simply, complement of a set A, denoted by A^c, is the set of elements which belong to U but which do not belong to A:

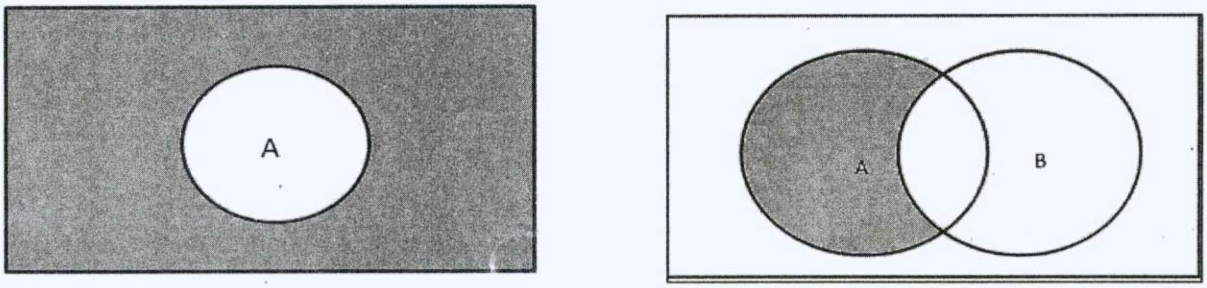
$$A^c = \{ x : x \in U, x \notin A\}$$

Some texts denote the complement of A by A' or $\overline{A}$. Figure 3.3(a) is a Venn diagram in which A^c is shaded.

The relative complement of a set B with respect to a set A or, simply, the difference of A and B , denoted by A\ B, is the set of elements which belong to A but which do not belong to B:

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

The set A \ B is read " A minus B", Many texts denote A \ B by A-B or A~B. Figure 3.3(b) is a Venn diagram in which A \ B is shaded.



(a) A^c is shaded.

(b) A \ B is shaded

Fig 3.3

Example

1. Let U={1, 2, 3,...}, the positive integers, be the universal set. Let A={1, 2, 3, 4}, B={3, 4, 5, 6, 7}, and let E={2, 4, 6, 8,...}, the even numbers. Then

   $A^c = \{5, 6, 7, 8,...\}$ $B^c =\{1, 2, 8, 9, 10,...\}$ and $E^c = \{1, 3, 5, 7,...\}$, the odd numbers.

3.5.1 PROPERTIES OF SET OPERATIONS

The operations on sets that we have just defined satisfy many algebraic properties, some of which resemble the algebraic properties satisfied by the real numbers and their operations. All the principal properties listed here can be proved using the definitions given and the rules of logic.

Commutative Properties

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$

Associative Properties

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

Distributive Properties

5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Idempotent Properties

7. $A \cup A = A$
8. $A \cap A = A$

Properties of the complement

9. $\overline{(\overline{A})} = A$
10. $A \cup \overline{A} = U$
11. $A \cap \overline{A} = \emptyset$
12. $\overline{\emptyset} = U$
13. $\overline{U} = \{\ \}$
14. $\overline{A \cup B} = \overline{A} \cap \overline{B}$
15. $\overline{A \cap B} = \overline{A} \cup \overline{B}$ Properties 14 and 15 are known as De Morgan's Laws.

Properties of Universal Set

16. $A \cup U = U$
17. $A \cap U = A$

Properties of Empty Set

18. $A \cup \emptyset = A$ or $A \cup \{\ \} = A$
19. $A \cap \emptyset = \emptyset$ or $A \cap \{\ \} = \{\ \}$

3.6 INCLUSION AND EXCLUSION

Let A and B be two finite sets. If A and B are disjoint sets, i.e., $A \cap B = \emptyset$, then $|A U B| = |A| + |B|$ .... (1)

If the sets overlap, the formula (1) is not a valid formula. In such situation we use the following theorem.

Theorem 3.3

If A and B are two sets, then $|A U B| = |A| + |B| - |A \cap B|$

Example

1. Verify the theorem 3.1 for the sets A= { a, b, c, d, e, f} B= {c, e, f, h, m, n, k}

   Solution

   By theorem 3.3,

   $|A U B| = |A| + |B| - |A \cap B|$

   A U B ={ a, b, c, d, e, f, h, m, n, k}

   $|A U B| = 10$

   Therefore, LHS=10

   $|A|=6$, $|B|=7$, $|A \cap B| = |\{c, e, f\}|$

   $|A \cap B| = 3$

   RHS=6+7-3=10

   LHS=RHS. The theorem is verified.

Theorem 3.4

If A,B and C are finite sets, prove that

$|A U B U C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$

Theorems 3.3 and 3.4 are extensively used in solving problems

Examples

1. A software firm wants to appoint 35 programmers to work on system programming jobs and 50 programmers for application programming. Out of these 20 candidates are capable of doing jobs of both types. How many programmers must be appointed?

   Solution:

   Let A be the set of system programmers.

   Let B be the set of application programmers.

   Then, $|A| = 35$, $|B|=50$, $|A \cap B|=20$

Number of programmers to be appointed is,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$= 35 + 50 - 20 = 65.$$

2. A Survey on mode of travel is conducted on the employees of an office. Every employee uses a bus, train or scooter as mode of travel to the office. More than one option was permitted. The survey results were: Bus- 40 people, Train – 45 people, Scooter – 90 people, Bus and Train – 25 people, Bus and Scooter – 25 people, Train and Scooter – 35 people and 10 people uses all 3 modes. How many were surveyed?

Solution:

Let A be the people travelling by bus.

Let B be the people travelling by train.

Let C be the people travelling by scooter.

$|A| = 40$, $|B|=45$, $|C|=90$, $|A \cap B|=25$, $|A \cap C|=25$, $|B\cap C|=35$ and $|A \cap B\cap C|=10$.

By using the principle of inclusion and exclusion, Number of people to be surveyed is $|A \cup B \cup C|$.

By Theorem 3.4,

$$|A \cup B \cup C| = |A|+ |B|+|C|-|A \cap B|-|B \cap C|-|A \cap C|+|A \cap B\cap C|$$

$$= 40+45+90-25-35-25+10 = 100.$$

3.7 INDUCTION

Induction Principle

Let P(n) be a proposition defined on the set of positive integers N.

(i) On the basis step the proposition $P(n_0)$ is true and

(ii) On induction step, if the proposition P(k+1) is true under the induction hypotheses that P(K) is true, then P(n) is true for all $n >= n_0$.

Examples

1. By mathematical induction, prove that

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

Solution:

Let the proposition P(n) be,

$1+2+3+\ldots+n= n(n+1)/2$

Basis Step

When n=1, $P(1) = \frac{1(1+1)}{2} = 1.$

When n=2, $P(2) = \frac{2(2+1)}{2} = 3.$

P(2): 3=3, P(2) is true.

So, $P(n_0)$ is true where n_0 is finite.

Induction Hypotheses

$P(k): \quad 1+2+3+\ldots+k = \frac{k(k+1)}{2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$

P(k) is true.

Induction Step

Adding (k+1) on both sides of (1),

$$P(k+1): \quad 1+2+3+\ldots+k+(k+1) = \frac{k(k+1)}{2}+(k+1)$$

$$=\frac{(k+1)((k+1)+1)}{2}$$

So. P(k+1) is true.

Thus, P(n) is true for $n>=n_0$.

2. By mathematical induction, prove that

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

Solution:

Let the proposition P(n) be,

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

Basis Step

When n=1, $P(1) = 1^2 = \frac{1(1+1)(2x1+1)}{6}$

P(1): 1= 1.

P(1) is true.

When n=2, $P(2) = 2^2 = \frac{2(2+1)(2x2+1)}{6}$

P(2): 1+4=5.

P(2) is true.

So, $P(n_0)$ is true where n_0 is finite.

Induction Hypotheses

$P(k)$: $1^2+2^2+3^2+\ldots+k^2 = \frac{k(k+1)(2k+1)}{6}$ …………………. (1)

P(k) is true.

Induction Step

Adding (k+1) on both sides of (1),

$$P(k+1) : 1^2+2^2+3^2+\ldots+k^2+(k+1)^2 = \frac{k(k+1)+(2k+1)}{6} + (k+1)^2$$

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

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

$$P(k+1) : 1^2+2^2+3^2+\ldots+(k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$$

So. P(k+1) is true.

Thus, P(n) is true for $n>=n_0$.

3.8 SUMMARY

In this unit a detailed discussion on set theoretic concepts may be found. Several examples of sets, types of sets such as countable, finite, uncountable, null and so on are defined and explained with illustrations. Use of principle of inclusion and exclusion in solving problems are also discussed. The very important, extensively used concept of induction is discussed here.

3.9 KEYWORDS

Sets- null set, empty set, subset, countable set, uncountable set. Set Operations- Union, intersection, complement, Inclusion and exclusion and Induction.

3.10 QUESTIONS

1. Define a set. Provide examples by listing and using abstraction.
2. Illustrate the concepts of countable, finite, uncountable, subsets, empty, null sets.
3. Name the operations on sets and illustrate.
4. State the complement properties.
5. State De Morgan's law and distributive properties.
6. What is |AUB| and |AUBUC|?
7. Verify the expressions in problem 6 in examples of your choice.
8. Using induction find 2+4+6+... and $2^2+4^2+6^2+\ldots$

3.11 REFERENCES

1. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL
2. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
3. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

UNIT -4: SET THEORY- PART II

Structure

4.0 Objectives

4.1 Counting principles

4.1.1 Permutatiсns

4.1.2 Combinations

4.2 Pigeon hole principle

4.2.1 Extended pigeon hole principle

4.3 Summary

4.4 Keywords

4.5 Questions

4.6 References

4.0 OBJECTIVES

After going through the contents of this unit,

✓ You will have better understanding of permutation and combination usages

✓ You will be able to use pigeon hole principle in solving problems.

4.1 COUNTING PRINCIPLES

Permutations and Combinations

Suppose there are four objects a, b, c, d. To make a selection of three things, choice must be one of the following: abc, abd, bcd, acd. These selections are called combinations of four things taken three at a time. The total number of these selections or combinations is 4.

Suppose to arrange four things taken three at a time, first select three things and then arrange them. Suppose we select abc. These three objects can be arranged as: abc, acb, bca, bac, cab, cba. Thus the number of arrangements that could be made from each selection is 6.

Hence, corresponding to four selections, there are 24 arrangements. These arrangements are called permutation of four things taken three at a time. Total number of these permutations is 24.

Generalization

If there are n things a, b, c, …, a selection of r out of these without reference to the order is called a combination of n things taken r at a time. It is denoted by ${}^{n}C_{r.}$

An arrangement formed by selecting r things out of n things and placing them in a definite order is called a permutation of n things taken r at a time. It is denoted by ${}^{n}P_{r.}$

4.1.1 PERMUTATIONS

Multiplication principle

Suppose two tasks T_1 and T_2 are to be performed in sequence. If T_1 can be performed in n_1 ways, and for each of these ways, T_2 can be performed in n_2 ways, then the tasks T_1 T_2 in a sequence can be performed in n_1n_2 ways.

Example

Let the task T_1 can be performed in three ways and for each of these ways, T_2 can be performed in 4 ways. Then the task T_1T_2 in a sequence can be performed in 3*4=12 ways.

Generalization

Suppose the task T_1 $T_{2........}T_k$ are to be performed in sequence. If T_1 can performed in n_1 ways, and for each of these ways T_2 can be performed in n_2 ways and for each of these n_1n_2 ways, T_3 can be performed in n_3 ways and so on. Then the sequence T_1 $T_{2........}T_k$ can be performed in exactly $n_1n_{2.......}$ n_k ways.

Examples

1. Students Id number consists of one letter followed by 3 digits. If repetitions are allowed, how many distinct Id numbers can be generated?

Solution:

letter	digit	digit	digit
26	**10**	**10**	**10**

The beginning letter can be done in 26 ways.

Each digit can be performed in 10 ways. Thus the distinct Id numbers can be generated in,

26*10*10*10=26,000 ways.

2. A computer password consists of two letters of English alphabet followed by three digits. How many different passwords can be generated?

   Solution:

letter	digit	digit	digit	digit
26	**10**	**10**	**10**	**10**

   First English letter can be done in 26 ways.

   Second English letter can be done in 26 ways.

   First digit can be performed in 10 ways.

   Second digit can be generated in 10 ways.

   Third digit can be done in 10 ways.

   Thus, the password can be generated in 26*26*10*10*10=676000 ways.

We state some important results here which may be of use in solving problems.

Result 1: Let A be a set of n elements. Then A can have 2^n numbers of subsets.

Result 2: Let A be a set of n elements. Allowing repetition, the number of sequences of length r can be constructed is n^r where $1 \leq r \leq n$.

Examples

1. How many three letter words can be formed from letters in the set {a, b, c, d, e}, if repetition of letters allowed?

   Solution:

   Here n=5, r=3.

   Number of three letter words can be performed=5^3=125.

2. How many 4 digit numbers can be formed with the 10 digits 0,1,2,3…9 if,

   (i) Repetitions are allowed.

   (ii) Repetitions are not allowed.

(iii) The last digit must be zero and repetitions are allowed.

Solution:

(i)

d_1	d_2	d_3	d_4
10	10	10	10

digit - 1 can be filled in 10ways.

digit - 2 can be filled in 10ways.

digit - 3 can be filled in 10ways.

Since, repetitions are allowed,

digit - 4 can also be filled in 10ways.

Thus possible 4 digit numbers = 10^4.

(ii)

d_1	d_2	d_3	d_4
10	9	8	7

digit - 1 can be filled in 10 ways. Since, repetitions are not allowed,

digit - 2 can be filled in 9 ways.

digit - 3 can be filled in 8 ways.

digit - 4 can be filled in 7 ways.

Thus possible 4 digit numbers

= 10x9x8x7

= 5040.

(iii)

d_1	d_2	d_3	0
10	10	10	1

digit - 1 can be filled in 10 ways. Since, repetitions are allowed,

digit - 2 can be filled in 10 ways.

digit - 3 can be filled in 10 ways.

Thus possible 4 digit numbers with last digit zero

= 10x10x10 = 10^3.

Result 3: Permutations of n objects taken r at a time can be done in ^nP_r ways.

Let A be a set of n elements. The number of different sequence of length r can be formed from A where all the elements in sequence must be distinct is ^nP_r.

Example

How many words of four distinct letters can be formed from the letters of the word MASTFRIEND?

Solution:

Here n=10, r=4.

$$^{10}P_4 = \frac{10!}{(10-4)!}$$

$$^{10}P_4 = \frac{10x9x8x7x6!}{6!}$$

$^{10}P_4$ = 5040 ways.

Result 4:

Let A be a set of n elements. Permutation of n elements taken all at a time can be done in n! ways.

Examples:

1. In an experiment a student has to arrange a book, a pencil, an eraser, a ruler and a sharpener in a row. How many different arrangements are possible?

Solution:

The number of objects in the experiment = 5

Permutation of 5 objects taken all at a time

= 5! ways

= 120 ways.

2. A coin is tossed 6 times. How many different sequences of heads and tails are possible?

Solution:

In one toss, it may be head or tails.

Different sequences possible = 2^6.

Different sequences possible = 64.

Result 5:

Let A be a set of n elements, in which first element appears K_1 times, second element appears K_2 times and so on. The number of distinguishable permutations that can be formed is:

$n!/ (K_1! \times K_2! \times \ldots\ldots \times K_i!)$

Examples:

1. Find the number of distinguishable words that can be formed from the letters

   (a) REFERENCE

   (b) STRUCTURES

   (c) CQDELETE

   Solution:

   (a) REFERENCE

   The letter R appears 2 times.

   The letter E appears 4 times.

   The letter F appears 1 time.

   The letter N appears 1 time.

   The letter C appears 1 time.

   The number of distinguishable words that can be formed is

$$= \frac{9!}{2! \times 4! \times 1! \times 1! \times 1!} = 1512 \text{ ways.}$$

   (b) STRUCTURES

   The number of distinguishable words that can be formed is

$$= \frac{10!}{2! \times 2! \times 2! \times 2! \times 1! \times 1!} = 226800 \text{ ways.}$$

   (c) CQDELETE

   The number of distinguishable words that can be formed is

$$= \frac{8!}{} = 6720 \text{ ways.}$$

1! x 1! x 1! x 3! x 1! x 1!

2. A mini-meal includes a soup, a course, a dessert and an ice cream. Suppose that a customer can select from 5 soups, 6 courses, 4 desserts and 3 types of ice creams. How many different mini=meals can be selected?

Solution:

Let T_1 be the task of selecting the soup.

This can be done in $^5P_1 = 5$ ways.

Let T_2 be the task of selecting the course.

This can be done in $^6P_1 = 6$ ways.

Let T_3 be the task of selecting the dessert.

This can be done in $^4P_1 = 4$ ways.

Let T_4 be the task of selecting the ice cream.

This can be done in $^3P_1 = 3$ways.

Different meals can be selected in 5 x 6 x 4 x 3 ways

= 360 ways.

3. How many numbers greater than a million can be formed with the digits 4, 5, 5, 0, 4, 5, 3?

Solution:

6	7	7	7	7	7	7

First digit cannot be 0. So, first digit can be selected in 6 ways.

The remaining digits form a string of length 6. This can be done in 7^6 ways.

Thus the number of numbers greater than a million that can be formed is

= 6 x 7^6 ways.

4. How many ways can 6 men and 6 women be seated in a row if

(a) Any person may sit next to any other.

(b) Men and women must occupy alternate seats?

Solution:

(a) 6 men and 6 women may sit next to any other can be done in (6+6)! = 12! ways.

M_1	W_1	M_2	W_2	M_3	W_3	M_4	W_4	M_5	W_5	M_6	W_6

Here, men first and women next.

6 men can be arranged in 6! Ways.

6 women can be arranged in 6! Ways.

W_1	M_1	W_2	M_2	W_3	M_3	W_4	M_4	W_5	M_5	W_6	M_6

Here, women first and men next.

6 women can be arranged in 6! Ways.

6 men can be arranged in 6! Ways.

Number of ways of arranging men and women alternately is,

= 6! x 6! x 6! x 6! Ways

= 1036800.

5. A committee of 4 is to be chosen out of 6 Englishmen, 5 Frenchmen and 4 Indians, the committee to contain 1 of each nationality.

(a) In how many ways can it be done?

(b) In how many arrangements will a particular Indian be included?

Solution:

(a)

M_1	M_2	M_3
6	5	4

An Englishman can be selected in 6 ways.

A Frenchman can be selected in 5 ways.

An Indian can be selected in 4 ways.

A committee can be done in = 6 x 5 x 4 ways.

A committee can be done in = 120 ways.

(b)

M_1	M_2	M_3
6	5	1

An Englishmen can be selected in 6 ways.

A Frenchmen can be selected in 5 ways.

A particular Indian can be selected in 1 way.

A committee of 3 members with a particular Indian can be done in = 6 x 5 x 1 ways

= 30 ways.

4.1.2 COMBINATIONS

Let A be the set of n elements. Number of combinations of the elements of A taken r at a time can be done in $\dfrac{n!}{r!\,(n-r)!}$ ways. It is denoted by ${}^{n}C_{r}$

$$\text{Thus, } {}^{n}C_{r} = \frac{n!}{r!\,(n-r)!}$$

Result 1: Let A be a set of n elements. Suppose K selections are made from n without considering the order and repetitions are allowed. The number of ways in which these selections can be made is ${}^{(n+k-1)}C_{k}$.

Examples:

1. A valid computer password consists of 8 characters, the first letter is chosen from the set {P,Q,R,S,T,U,V,W} and other seven characters are chosen from either English alphabet or a digit. How many different passwords are possible?

Solution:

The first letter from the given set can be chosen in ${}^{8}C_{1}$ ways.

The remaining seven can be chosen from 26 English alphabet and 10 digits where repetitions are allowed.

A string of 7 characters from 36 characters can be selected in 36^{7} ways.

By the multiplication principle the number of different passwords possible = ${}^{8}C_{1} \times 36^{7}$.

2. How many different 9 person committees can be formed each containing 4 women from a set of 20 women and 5 men from a set of 30 men?

Solution:

The selection of 4 women from 20 women can be done in ${}^{20}C_{4}$ ways.

The selection of 5 men from 30 men can be done in ${}^{30}C_{5}$ ways.

By the multiplication principle the number of 9 person committees that can be formed is

$= {}^{20}C_{4} \times {}^{30}C_{5}$

$= 690441570.$

Result 2: ${}^{n}C_{r} = {}^{n}C_{n-r}$

Examples

1. n=5 r=2

$${}^{n}C_{r} = {}^{5}C_{2} = \frac{5 \times 4}{1 \times 2} = 10.$$

$${}^{n}C_{n-r} = {}^{5}C_{5-2} = {}^{5}C_{3} = \frac{5 \times 4 \times 3}{1 \times 2 \times 3} = 10.$$

2. n=6 r=2

$${}^{n}C_{r} = {}^{6}C_{2} = \frac{6 \times 5}{1 \times 2} = 15.$$

$$^{n}C_{n-r} = {}^{6}C_{6-2} = {}^{6}C_{4} = \frac{6 \times 5 \times 4 \times 3}{1 \times 2 \times 3 \times 4} = 15.$$

3. In how many ways can a committee of 3 faculty members and 2 students be selected from 7 faculty and 8 students?

Solution:

3 faculty members from a set of 7 faculty members can be selected in $^{7}C_{3}$ ways.

2 students from a set of 8 students can be selected in $^{8}C_{2}$ ways.

By the multiplication principle the required committee can be selected in

$^{7}C_{3} \times {}^{8}C_{2} = 980$ ways.

4. How many different sets of 8 cards with 5 red cards and 3 black cards can be formed from a deck of 52 cards?

Solution:

The deck of 52 cards has 26 red cards and 26 black cards.

Selection of 5 red cards from 26 red cards can be done in $^{26}C_{5}$ ways.

Selection of 3 black cards from 26 black cards can be done in $^{26}C_{3}$ ways.

Number of different selection of set of 8 cards can be done in $^{26}C_{5} \times {}^{26}C_{3}$ ways.

5. An Urn contains 15 balls, 8 of which are red and 7 are black. In how many ways can 5 balls be chosen such that

(a) All 5 are red?

(b) All 5 are black?

(c) 2 are red and 3 are black?

(d) 3 are red and 2 are black?

Solution:

(a) Selection of 5 balls where all are red can be done in $^{8}C_{5} = 56$ ways.

(b) Selection of 5 balls where all are black can be done in $^{7}C_{5} = 21$ ways.

(c) Selection of 2 red balls can be done in $^{8}C_{2}$ ways and selection of 3 black balls can be done in $^{7}C_{3}$ ways. The required selection can be done in $^{8}C_{5} \times {}^{7}C_{5} = 980$ ways.

(d) Selection of 3 red balls can be done in ${}^{8}C_{3}$ ways and selection of 2 black balls can be done in ${}^{7}C_{2}$ ways. The required selection can be done in ${}^{8}C_{3} \times {}^{7}C_{2} = 1176$ ways.

4.2 PIGEONHOLE PRINCIPLE

Statement:

If n pigeons are assigned to m pigeonholes and $m < n$, then at least one pigeonhole contains two or more pigeons.

Proof

Pigeonhole	1	2	3	- - - - - - - - - -	m

Pigeons { 1, 2, 3,…m, (m+1), … n}

Assign Pigeon 1 to Pigeonhole 1

Pigeon 2 to Pigeonhole 2

Pigeon 3 to Pigeonhole 3

-----------------------------

-----------------------------

Pigeon m to Pigeonhole m

Since, $n > m$, the number of pigeons left with are $(n - m)$. The $(n - m)$ Pigeons are yet to be assigned to Pigeonholes. Thus, at least one Pigeonhole will be assigned to second Pigeon.

Examples

1. If 8 people are chosen in any way from some group, at least two of them will have born on the same day of the week. Here each person (pigeon) is assigned to the day of the week (Pigeonhole) on which he or she was born. Since there are eight people and only seven days of a week, the Pigeonhole principle tells us at least two people must be assigned to the same day of the week.

Note that the pigeonhole principle provides an existence proof; there must be an object or objects with a certain characteristic. In the example just discussed above, this characteristic is having been born on the same day of the week. The pigeonhole principle guarantees that there are at least two people with this characteristic, but gives no information on identifying these people. Only their existence is guaranteed. In contrast, a constructive proof guarantees the existence of an object or objects with a certain characteristic by actually constructing such an object or objects. For example, we could prove that, given two rational numbers p and q, there is a rational number between them by showing that (p+q)/2 is between p and q.

To use the pigeonhole principle, we must identify pigeons (objects) and pigeonholes (categories of the desired characteristic) and be able to count the number of pigeons and the number of pigeonholes.

2. Show that if any 5 numbers from 1 to 8 are chosen, then two of them will add up to 9.

Solution:

Construct four different sets, each containing two numbers that add up to 9 as follows: $A_1=\{1, 8\}$, $A_2=\{2, 7\}$, $A_3=\{3, 6\}$, $A_4=\{4, 5\}$. Each of the five numbers chosen should belong to one of these sets. Since there are only four sets, the pigeonhole principle tells us that two of the chosen numbers belong to the same set. These numbers add up to 9.

3. Show that in a group of 9 people at least three of them have been born on the same day.

Solution:

Number of people (pigeons) = 9

Number of days in a week (Pigeonholes) = 7.

Suppose that first seven people have born on distinct days.

Pigeonholes	S	M	T	W	Th	F	Sat
Pigeons	P_1	P_2	P_3	P_4	P_5	P_6	P_7 P_8 & P_9

Assigning one person for each of the days, we are left with P_8 & P_9.

Assume that the persons P_8 & P_9 are born on Saturday and assign P_8 & P_9 to the pigeonhole Saturday.

According to the pigeonhole principle one pigeonhole contains 3 pigeons.

Thus, at least three people have been on the same day of the week.

4. There are 13 students in a class room. Show that at least two of them have been born on the same month.

Solution:

Pigeonholes

J	F	M	A	M	J	J	A	S	O	N	D

Pigeons P_1, P_{13} P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12}

Here 12 months of the year are pigeonholes.

Assign person 1 to the Pigeonhole January.

Assign person 2 to the Pigeonhole February.

Continuing in the same way, assign person 12 to the pigeonhole December.

Person 13 is yet to be assigned to a pigeonhole.

Since, the pigeons have a common property; assign any one of the 12 pigeonholes to P_{13}.

Let it be January. Thus, at least one pigeonhole contains two or more pigeons.

4.2.1 EXTENDED PIGEONHOLE PRINCIPLE

Extended Pigeonhole Principle is used when the number of Pigeons is much larger than the number of Pigeonholes.

If P Pigeons are assigned to Q Pigeonholes, then one of the Pigeonholes must contain at least

$\lfloor (P-1)/Q \rfloor + 1$ Pigeons, where $\lfloor P/Q \rfloor$ stands for largest integer <= P/Q

Examples

1. Show that if 30 dictionaries in a library contain a total of 61,327 pages, then one of the dictionaries must have at least 2045 pages.

Solution:

Let the pages be the pigeons and the dictionaries the pigeonholes. Assign each page to the dictionary in which it appears. Then, by the extended pigeonhole principle, one dictionary must contain at least $\lfloor 61{,}326/30 \rfloor + 1$ or 2045 pages.

2. Show that if 8 colors are used to paint 49 houses, at least 7 houses will be of the same color.

Solution:

Here scooters are pigeons and colors are pigeonholes. So, P=49 and Q=8. According to the extended pigeonhole principle, one of the colors must be painted to at least,

$\lfloor (49 - 1)/8 \rfloor + 1 = \lfloor 48/8 \rfloor + 1$

$= 6 + 1$

$= 7$ houses will have same color.

3. Show that in a group of 30 people at least 5 of them were born on the same day of the week.

Solution:

Here people are pigeons and days of the week are pigeonholes. So, P=30 and Q=7.According to the extended pigeonhole principle, one of the colors must be painted to at least,

$\lfloor (30 - 1)/7 \rfloor + 1 = \lfloor 29/7 \rfloor + 1$

$= 4 + 1$

$= 5$ people are born on the same day of the week.

4.3 SUMMARY

In this unit we discussed basic methods of counting namely Permutation and Combination. Several illustrations are discussed for better understanding of the usage of permutation or combination. Later, Pigeonhole Principle and its extension are also stated and several examples solved.

4.4KEYWORDS

Counting, Permutation, Combination, Pigeonhole Principle.

4.5 QUESTIONS

1. Explain when to use permutation and when to use combination while counting.
2. A bank password consists of two letters of the English alphabet followed by 2 digits. How many different passwords can be formed?\
3. Compute $^{6}P_{5}$, $^{4}P_{4}$, $^{n+1}P_{n-1}$.
4. How many permutations are there of the set { r, s, t, u, o}. For this set find the number of permutations taken 3 at a time and two at a time.
5. Compute $^{7}C_{4}$, $^{n}C_{n-2}$.
6. In how many ways can a 6-card hand be dealt from a deck of 52 cards?
7. In how many ways can a committee of 6 people be selected from a group of 10 people if one person is to be designated as chair of the committee?
8. If 13 people are assembled in a room, show that at least two of them must have their birthday in the same month.
9. Show that if any eight positive integers are chosen, two of them will have the same remainder when divided by 7.
10. Prove that if any 14 members from 1 to 25 are chosen, then one of them is a multiple of another.

4.6 REFERENCES

1. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL
2. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
3. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

MODULE 2: Relations, Recurrence Relations, Functions

UNITS: 5 to 8

UNIT-5: RELATIONS

Structure

5.0 Objectives

5.1 Introduction

5.2 Relation

5.3 Relation matrix and Digraph

5.4 Properties of Relation

5.5 Partition and Covering

5.6 Equivalence Relation

5.7 Compatibility Relation

5.8 Composite Relation

5.9 Transitive Closure

5.10 Warshall's Algorithm

5.11 Solved problems

5.12 Summary

5.13 Keywords

5.14 Questions

5.15 References

5.0 OBJECTIVES

When you go through this unit, you will be able to

- ✓ Explain the Relations, Matrix and Digraph;
- ✓ Explain the properties of relations;
- ✓ Give an account of equivalence and compatibility relations;
- ✓ Analyze the composite relations.
- ✓ Analyze the Warshall's Algorithm.

5.1 INTRODUCTION

Relation is a basic concept in day to day life and Mathematics. A relation shows an association of objects of a set with objects of other sets (or the same set). The essence of relation is these associations. A collection of these individual associations is a relation. To represent these individual associations, a set of "related" objects, can be used. The order of the objects must also be taken into account. Thus sets with an order on its members are needed to describe a relation.

The relation matrix is used to represent a relation on a computer and is useful in studying the properties of a relation. The equivalence and compatibility relations have useful applications in the design of sequential machines and digital computers.

5.2 RELATION

Definition: Let A and B are two non-empty sets, the **Cartesian product** of A and B is defined by $A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$.

Example 1: Let A={a,b}, B={1,2,3}. Find (a) A × B (b) B × A

Solution: (a) A × B={(a,1), (a,2), (a,3), (b,1), (b,2), (b,3)}

(b) B × A={(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)}

Definition: Let A and B be two non-empty sets. A **Relation** (Binary relation) R from A to B is a subset of A × B.

If $(a,b) \in R$ then, a is related to b by the relation R. It is also denoted by ${}_aR_b$.

Example 2: Let A ={1, 2, 3}, B ={a, b}

A × B= {(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)}

R_1={(1,b), (2,a), (3,b)}

R_2={(2,a), (2,b), (3,b)}

Then, R_1, R_2 are the subsets of A × B. So, R_1, R_2 are called relational sets of A × B.

Example 3: Let A={1,2,3,4}. Construct the relational set R such that R={(a, b) | a ≥b}

Solution: Find A × A. Select the elements where a ≥ b.

R={(1,1), (2,1), (2,2), (3,1), (3,2), (3,3), (4,1), (4,2), (4,3), (4,4)}.

Definition: Let R be a relation from A to B. The **domain** of R is the set of elements in A that are related to some element in B. It is denoted by Dom(R).

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

Dom(R)={1, 2, 3, 4}.

Definition: Range of R is the set of all elements in B that are related to some element In A. It is denoted by Ran(R).

Example 5: Let R={(1,1), (2,1), (2,2), (3,1), (3,2), (3,3))}

Ran(R)={1, 2, 3}

5.3 RELATION MATRIX AND DIGRAPH

Definition: Let A= {a_1, a_2, …, a_m) and B={b_1,b_2,…, b_n} be two sets. Let R be the relation from A to B. The relation R can be represented by an m × n matrix called Relation Matrix, denoted by M_R and defined as

$$M_R= [m_{ij}] \text{ where } m_{ij}=1, \text{ if } (a_i, b_j) \in R$$
$$=0, \text{ if } (a_i, b_j) \notin R$$

Example 6: Let A = {1, 2, 3, 4} and B= {b_1, b_2}. Let R={(1,b_2), (2,b_1), (2,b_2), (3,b_1)}. Write the relation matrix M_R.

Solution:

A × B={(1,b_1), (1,b_2), (2,b_1), (2,b_2), (3,b_1), (3,b_2), (4,b_1), (4,b_2)}

The Relation matrix of R is of order 4×2.

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

Definition: Let A be a finite set and R be a relation on A. The **digraph** of R consists of elements of A as vertices and (a_i, a_j) in R as a directed edge from a_i to a_j.

Example 7: Let A= {1, 2, 3, 4, 5} and R={(1,2), (1,4), (1,5), (3,2), (4,1), (4,2), (4,5), (5,5)}, a relation on A. Draw the digraph of R.

Solution:

Digraph

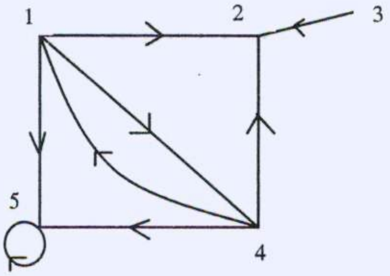


Fig 5.1

5.4 PROPERTIES OF RELATION

A relational set satisfies the following properties

Reflexive: - Let A be a set and R be a relation on A. R is said to be reflexive, if (a, a) ∈ R for all a∈ A.

Symmetric: Let A be a set and R be a relation on A. R is said to be symmetric, if whenever (a, b) ∈ R then (b, a) ∈R.

Anti symmetric: Let A be a set and R be a relation on A. R is said to be anti symmetric if whenever (a, b) ∈R, (b, a) ∈R, then a=b.

Transitive: Let A be a set and R be a relation on A. R is said to be transitive, if whenever (a, b) ∈ R and (b, c) ∈ R then (a, c) ∈ R.

Example 8: Let R={(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,3), (4,4), (5,5)} be a relation on A= {1, 2, 3, 4, 5}. Determine the properties of R.

Solution: R={(1,1), (1,2), (2,1), (2,2), (3,3), (3,4), (4,3), (4,4), (5,5)}

(1,1), (2,2), (3,3), (4,4), (5,5) $\in$ R. So R is reflexive.

(1,2), (2,1), (3,4), (4,3) $\in$ R. So R is symmetric.

(1,2), (2,1) $\in$ R, (1,1) $\in$ R

(3,4), (4,3) $\in$ R, (3,3) $\in$ R

Thus, for any (a,b), (b,c) $\in$ R, (a,c) $\in$ R. So R is transitive.

5.5 PARTITION AND COVERING

Definition: Let S be a given set and A = {A_1, A_2, ... , A_m} where each A_i, i = 1, 2, ….,m, is a subset of S and $\bigcup_{i=1}^{m} A_i = S$. Then the set A is called a *covering* of S, and the sets A_1, A_2, ... , A_m are said to *cover* S. If, in addition, the elements of A, are mutually disjoint, then A is called a *partition* of S, and the sets A_1, A_2, ……. , A_m are called the *blocks* of the partition.

Example 9: let S = {1, 2, 3} and consider the following collections of subsets of S.

A = {{1, 2}, {2, 3}}, B = {{1}, {1, 3}} C = {{1}, {2, 3}}

D = {{1, 2, 3}}, E = {{1}, {2}, {3}}, F = {{1}, {1, 2}, {1, 3}}

The sets A and F are coverings of S while C, D, and E are partitions of S. Of course, every partition is also a covering. The set B is neither a partitions nor a covering of S.

5.6 EQUIVALENCE RELATION

Definition: Let A be a set and R be a relation on A. R is said to be an equivalence relation if it is reflexive, symmetric and transitive.

Example 10: If R is the relation on Z, the set of integers such that R={(x,y)| x-y is divisible by 5}, show that R is an equivalence relation.

Solution: Let R= {(x,y)|(x-y) is divisible by 5}

Reflexive: For a$\in$Z, (a, a) $\in$R because (a-a)=0 is divisible by 5

So R is reflexive

Symmetric: For $(a,b) \in R \Rightarrow (a-b)$ is divisible by 5

$\Rightarrow (b-a)$ is also divisible by 5

$\Rightarrow (b,a) \in R$.

Hence, R is symmetric.

Transitive: For $(a,b) \in R \Rightarrow (a-b)$ is divisible by 5

and for $(b,c) \in R \Rightarrow (b-c)$ is divisible by 5

Then, $(a-c) = (a-b) + (b-c)$ is divisible by $5 \Rightarrow (a,c) \in R$

Hence, R is transitive.

Thus, R is an equivalence relation.

Definition: Let R be an equivalence relation on a set A. For any $a \in A$, the subset $[a]_R$ of A given by $[a]_R = \{b \in A \mid (a, b) \in R\}$ is called an R-*equivalence* class generated by $a \in A$.

Theorem: Every equivalence relation on a set generates a unique partition of the set. The blocks of this partition correspond to the R-equivalence classes.

5.7 COMPATIBILITY RELATION

Definition: A relation R is said to be a *compatibility relation* if it is reflexive and symmetric.

Obviously all equivalence relations are compatibility relations.

Example 11: Let A={1, 2, 3, 4}, R={(1,1), (1,2), (1,4), (2,1), (2,2), (2,3), (3,2), (3,3), (3,4), (4,1), (4,3), (4,4)}. Show that R is a compatibility relation.

Solution: (1,1), (2,2), (3,3), $(4,4) \in R$. So, R is Reflexive.

(1,2), (2,1), (1,4), (4,1), (2,3), (3,2),(3,4), $(4,3) \in R$

So, R is Symmetric.

Hence, R is a compatibility relation.

Graph of Compatibility Relation R

Since R is reflexive, each vertex has a self-loop. For simplicity omit the loops.

Since R is symmetric if there is a directed edge from a to b, definitely there is a directed edge from b to a. For simplicity, draw an edge from a to b omitting the arrow.

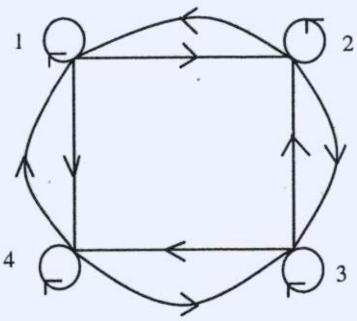


Fig 5.2: Digraph of R in Example 11

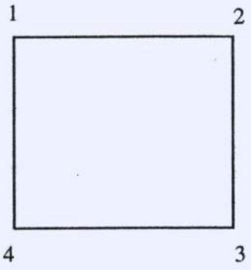


Fig 1.3: Simplified Graph

Matrix Representation

The relation matrix of a compatibility relation is symmetric and has its diagonal elements unity. It is, therefore, sufficient to give only the elements of the lower triangular part of the relation matrix.

Relation matrix of R

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

Compatibility Relation Matrix

$$\begin{array}{c|ccc} 2 & 1 & & \\ 3 & 0 & 1 & \\ 4 & 1 & 0 & 1 \\ \hline & 1 & 2 & 3 \end{array}$$

Definition: Let A be a set and R a compatibility relation on A. A subset B of A is called a *maximal compatibility block* if every element of B is related to every other element of B and no element of A-B is related to all the elements of B.

Example 12: Find the maximal compatibility blocks of the relation R in Example 10

Solution: Maximal compatibility blocks of R are

$$\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}$$

These sets are not mutually disjoint, and therefore they only define a covering of A.

5.8 COMPOSITION OF BINARY RELATIONS

Definition: Let R be a relation from A to B and S be a relation from B to C. Then a relation written as R · S is called a *composite relation* of R and S where

$$R \bullet S = \{(a, c) | (a, b) \in R \text{ and } (b, c) \in S\}$$

The operation of composition is a binary operation on relations, and it produces a relation from two relations. The same operations can be applied again to produce other relations. For example, let R be a relation from A to B, S a relation from B to C, and P a relation from C to D. Then R · S is a relation from A to C. We can form (R · S) · P, which is a relation from A to D. Similarly, we can also form R·(S·P), which again is a relation from A to D. So, we have

$(R \cdot S) \cdot P = R \cdot (S \cdot P) = R \cdot S \cdot P$

Example 13: Let R = {(1, 3), (4, 5), (2, 2)} and S = {(1, 2), (2, 1), (3, 3), (5, 2)} be relations on the set A= {1, 2, …, 5}. Find R · S, S · R, R · (S · R), (R · S) · R, R · R, S · S, and S · S · S.

Solution:

$$\begin{aligned}
R \cdot S &= \{(1, 3), (2, 1), (4, 2)\} \\
S \cdot R &= \{(1, 2), (2, 3), (5,2)\} \neq R \cdot S \\
R \cdot (S \cdot R) &= \{(2, 3), (4, 2)\} \\
(R \cdot S) \cdot R &= \{(2, 3), (4, 2)\} = R \cdot (S \cdot R) \\
R \cdot R &= \{(2, 2)\} \\
S \cdot S &= \{(2, 2), (3, 3), (1, 1)\} \\
S \cdot S \cdot S &= \{(1, 2), (2, 1), (3, 3)\}
\end{aligned}$$

Matrix of the Composite Relation:

Let the relations A and B be represented by n×m and m×r matrices respectively. Then the composition A·B which we denote by the relation matrix C is expressed as $C_{ij} = \bigvee_{k=1}^{m}(a_{ik} \wedge b_{kj}), \quad i = 1,2,\ldots,n; j = 1,2,\ldots,r$.

Example 14: Let R = {(1,2), (1, 3), (2, 2), (3, 3), (3,4), (4,2), (4,4), (4,5)} and S = {(1, 1), (1,3), (2, 1), (2, 4), (2, 5), (3, 1), (4, 2), (4,4)} be relations on the set A= {1, 2, …, 5}. Compute the relation matrices for R · S and S · R.

Solution:

$$\underset{M_R}{\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} \cdot \underset{M_S}{\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} = \underset{M_{R \cdot S}}{\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}$$

$$\underset{M_S}{\begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} . \underset{M_R}{\begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}} = \underset{M_{S \cdot R}}{\begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}}$$

5.9 TRANSITIVE CLOSURE

Definition: Let A be a set with $|A| = n$ and R be a relation on A. Then the transitive closure of R is defined as $R^{\infty} = R \text{ U } R^2 \text{ U } \ldots \text{ U } R^n$.

Example 15: Let A= {1, 2, 3, 4}, and let R={(1,2), (2,3), (3,4), (2,1)}. Find the transitive closure of R.

Solution: Given R={(1,2), (2,3), (3,4), (2,1)}

Method 1:

$R^2 = R \bullet R = \{ (1,1), (1,3), (2,2), (2, 4)\}$

$R^3 = R^2 \bullet R = \{(1, 2), (1,4), (2,1), (2,3)\}$

$R^4 = R^3 \bullet R = \{(1,3), (2, 2), (2,4)\}$

$R^{\infty} = R \text{ U } R^2 \text{ U } \ldots \text{ U } R^4$

$R^{\infty} = \{(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4), (3,4)\}$

Method 2: The matrix of R is

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

We may proceed algebraically and compute the powers of M_R. Thus

$$(M_R)^2_{\odot} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} , \qquad (M_R)^3_{\odot} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$(M_R)^4_{\odot} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Continuing in this way, we can see that $(M_R)^n_{\odot}$ equals $(M_R)^2_{\odot}$ if n is even and equals $(M_R)^3_{\odot}$ if n is odd and greater than 1. Thus

$$M_R^{\infty} = M_R \text{ V } (M_R)^2_{\odot} \text{ V } (M_R)^3_{\odot}$$

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

5.10 WARSHALL'S ALGORITHM

Warshall's Algorithm is a simple and easy procedure to compute the transitive closure of R. Starting with the matrix $W_0=M_R$, construct W_Ks recursively until we get $W_n=M_R^{\infty}$, which is the matrix of transitive closure. From the matrix, the transitive closure is obtained.

Algorithm

Initialize $W_0=M_R$.

The procedure for computing W_k from W_{k-1}.

Step 1: First transfer to W_k all 1's in W_{k-1}.

Step 2: List the location $p_1, p_2, \ldots$, in column k of W_{k-1}, where the entry is 1, and the locations $q_1,q_2, \ldots$, in row k of W_{k-1}, where the entry is 1.

Step 3: Put 1's in all the positions (p_i, q_j) of W_k(if they are not already there).

Repeat the above steps from k = 0, until $W_{k-1}=W_k$.

Example 16: Consider the relation R defined in Example 15. Then

$$W_0 = M_R = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

and n=4.

First we find W_1 from W_0 so that k = 1. W_0 has 1's in location 2 of column 1 and location 2 of row 1. Thus W_1 is just W_0 with a new 1 in position (2, 2).

$$W_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Now we compute W_2 from W_1 so that k=2. W_1 has 1's in locations 1 and 2 of column 2 and locations 1, 2, and 3 of row 2.

Thus, to obtain W_2, we must put 1's in positions (1,1), (1,2), (1,3), (2,1), (2,2), and (2,3) of matrix W_1 . Thus we get

$$W_2 = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

We compute W_3 from W_2 so that k=3.Processing, we see that column 3 of W_2 has 1's location 1 and 2, and row 3 of W_2 has a 1 in location 4. To obtain W_3, we must put 1's in positions (1,4) and (2,4) of W_2, so

$$W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

To find W_4, transfer all 1's from W_3 to W_4. W_3 has 1's in locations 1,2,3 of column 4 and no 1's in row 4, so no new 1's are added. Thus,

$$W_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Hence, $M_R^{\infty} = W_4 = W_3$.

So, R^{∞} ={(1,1), (1,2), (1,3), (1,4), (2,1), (2,2), (2,3), (2,4), (3,4)}

5.11 SOLVED PROBLEMS

1. Find the domain, range, relational matrix and the digraph of the relation R for the following.

i. A={a, b, c, d}, b={1, 2, 3, 4}

R={(a,1), (a,2), (b,1), (c,2), (d,1), (d,4), (c,4)}

ii. A= B={1, 2, 3, 4, 8, 10}, R={(a, b) | a=b}.

Solution:

i. Dom(R) = {a, b, c, d}

Ran(R) = {1, 2, 4}

Relational matrix: |A|=4, |B|=4, the order of M_R is 4×4

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

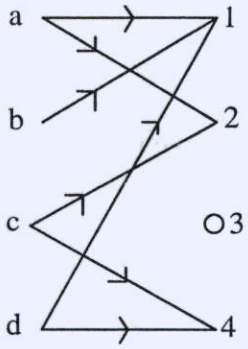


Fig 5.3: Digraph

ii. A={1,2,3,4,8,10}=B

R= {(a, b) |a=b}

R={(1,1),(2,2,),(3,3),(4,4,),(8,8),(10,10)}

Dom(R) = (1, 2, 3, 4, 8, 10}

Ran(R) = {1, 2, 3, 4, 8, 10}

Relational matrix

|A|=6, |B|=6, M_R is of order 6X6.

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

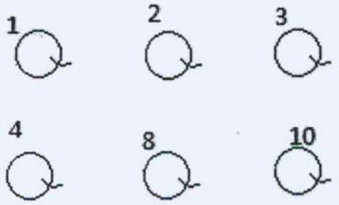


Fig 1.4: Digraph

2. Let A= {1, 2, 3, 4, 5}. Determine whether R is reflexive, symmetric, anti symmetric and transitive.

(a) R={(1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (5,5)}

(b) R={(1,3), (1,1), (3,1), (1,2), (3,3), (4,4)}

(c) R={(1,1), (2,2), (3,3), (5,5)}

Solution:

(a) R={(1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (5,5)}

For $a \neq 5 \in$ A, $(a, a) \notin$ R.

So, R is not reflexive.

For $(a,b) \in$ R, $(b, a) \notin$ R.

So, R is not symmetric.

For $(1,2)$ & $(2,3) \in R \Rightarrow (1,3) \in R$

$(1,3)$ & $(3,4) \in R \Rightarrow (1,4) \in R$

$(2,3)$ & $(3,4) \in R \Rightarrow (2,4) \in R$

$(1,2)$ & $(2,4) \in R \Rightarrow (1,4) \in R$

So, for all (a,b) & $(b,c) \in R$, $(a,c) \in R$

R is transitive

(b). R={(1,3),(1,1),(3,1),(1,2),(3,3),(4,4)}

$(2,2), (5,5) \notin R$

So, R is not reflexive

$(1,2) \in R$ but $(2,1) \notin R$

So, R is not symmetric

(3,1) & (1,2) $\in$ R but, (3,2) $\notin$ R

So, R is not transitive

(c) R={(1,1),(2,2),(3,3),(5,5)}

R is anti symmetric

R is not reflexive and transitive

3. Let Z denote the set of integers. Define a relation R on Z by R= {(a, b) | GCD (a, b)=1}. Discuss the properties of R.

Solution:

Reflexive: For 1$\in$Z, GCD (1, 1)=1 implies (1,1)$\in$R.

If a$\neq$1 $\in$ Z, GCD (a, a) =a $\neq$1 implies (a, a) $\notin$ R.

Hence, R is not reflexive.

Symmetric: For, a, b $\in$ Z, and GCD(a, b)=1, then (a, b) $\in$R

GCD(a, b)=1 implies GCD (b, a)=1, then (b, a) $\in$R

Hence, T is symmetric.

Transitive: For a, b $\in$ Z, and GCD(a, b)=1, then (a, b) $\in$R

For b, c $\in$ Z, and GCD(b, c)=1, then (b, c) $\in$ R

GCD (a, b)=1, GCD(b, c)=1 implies GCD(a, c) = 1 then (a, c) $\in$R.

Hence, T is transitive.

4. Let A = {1, 2, …, 7} and R = {(a, b) | a-b is divisible by 3}

Show that R is an equivalence relation. Draw the graph of R. Find the partition generated by R.

SOLUTION:

For any a $\in$A, a-a is divisible by 3; hence aRa, or R is reflexive.

For any a, b$\in$ A, a-b is divisible by 3, then b-a is also divisible by 3; that is, aRb => bRa. Thus R is symmetric.

For a, b, c ∈ A, if aRb and bRc, then both a-b and b-c are divisible by 3, so that a-c = (a-b) + (b-c) is also divisible by 3, and hence aRc. Thus R is transitive.

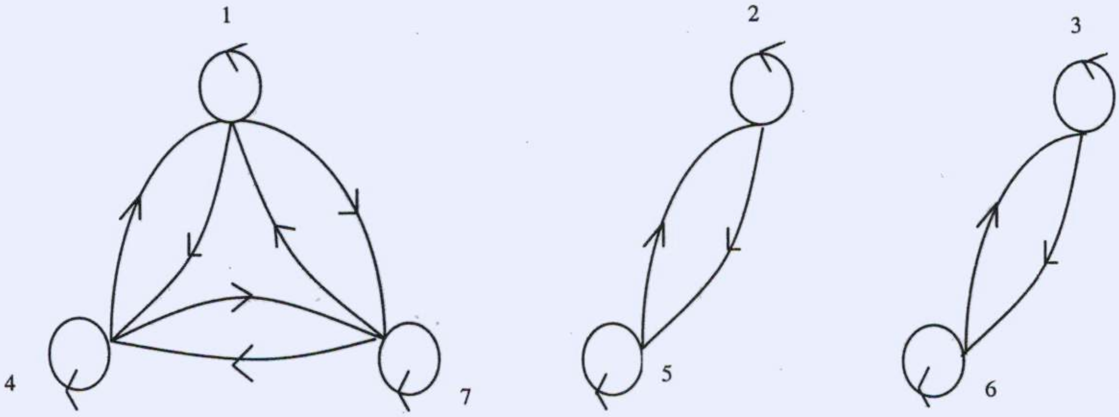


Fig 5.4: Digraph of R

Partition generated by R

$[1]_R$={b∈ A |(1, b) ∈R}

= {1, 4, 7}

$[2]_R$ = {b∈ A |(2, b) ∈R}

= {2, 5}

$[3]_R$ = {b∈ A |(3, b) ∈R}

={3, 6}

$[4]_R$={b∈ A |(4, b) ∈R}

= {1, 4, 7}

$[5]_R$ = {b∈ A |(5, b) ∈R}

= {2, 5}

$[6]_R$ = {b∈ A |(6, b) ∈R}

={3, 6}

$[7]_R$={b∈ A |(7, b) ∈R}

= {1, 4, 7}

Partition: {{1, 4, 7}, {2, 5}, {3, 6}} = {$[1]_R$, $[2]_R$, $[3]_R$} or {$[4]_R$, $[5]_R$, $[6]_R$}

5. Let A={1, 2, 3, 4} and R={(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,4)}. Is R an equivalence relation? If yes, find the partition of A induced by R.

Solution: Reflexive: For a∈ A, (a, a) ∈R, so R is reflexive

Symmetric: For (a,b) ∈R, (b,a) ∈ R.

Hence, R is symmetric.

Transitive: For (a,b) ∈ R, (b,c) ∈ R ⇒ (a,c) ∈R

Hence, R is transitive.

Hence R is an equivalence relation.

$[1]_R$={b∈ A |(1, b) ∈R}

= {1, 2, 3}

$[2]_R$ = {b∈ A |(2, b) ∈R}

= {1, 2, 3}

$[3]_R$ = {b∈ A |(3, b) ∈R}

={1, 2, 3}

$[4]_R$={b∈ A |(4, b) ∈R}

= {4}

Partition of A induced by R= {{1, 2, 3}, {4}}

6. Let the compatibility relation on a set {1, 2, …, 6} be given by the matrix

$$\begin{array}{c|ccccc}
2 & 1 & & & & \\
3 & 1 & 1 & & & \\
4 & 1 & 1 & 1 & & \\
5 & 0 & 1 & 0 & 0 & \\
6 & 0 & 0 & 1 & 0 & 1 \\
\hline
 & 1 & 2 & 3 & 4 & 5
\end{array}$$

Draw the graph and find all the maximal compatibility blocks of the relation.

Solution: The graph of the compatibility relation is

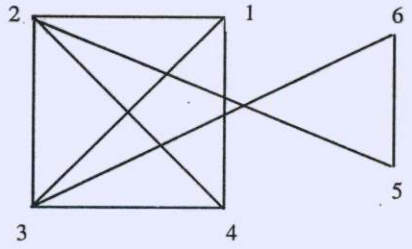


Fig 5.5: Simplified graph

The maximal compatibility blocks are

{1, 2, 3, 4}, {2, 5}, {3, 6}, {5, 6}

7. Let the compatibility relation on a set {1, 2, ..., 6} be given by the matrix

$$\begin{array}{c|ccccc}
2 & 1 & & & & \\
3 & 1 & 1 & & & \\
4 & 0 & 0 & 1 & & \\
5 & 0 & 0 & 0 & 0 & \\
6 & 1 & 0 & 1 & 1 & 0 \\
\hline
 & 1 & 2 & 3 & 4 & 5
\end{array}$$

Draw the graph and find all the maximal compatibility blocks of the relation.

Solution: The graph of the compatibility relation is

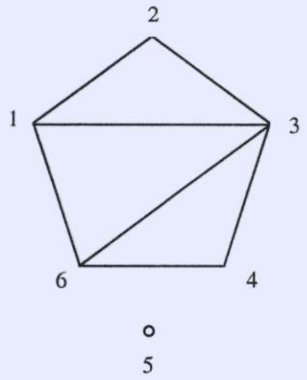


Fig 5.6: Simplified graph

The maximal compatibility blocks are

{1, 2, 3}, {1, 3, 6}, {3, 4, 6}, {5}

8. Let R and S be two relations on a set of Natural Numbers N:

$$R = \{(x, 2x) \mid x \in N\} \quad S = \{(x, 5x) \mid x \in N\}$$

Find R · S, R · R, R · R · R, and R · S · R.

SOLUTION:

$$R \cdot S = \quad \{(x, 10x) \mid x \in N\} = S \cdot R$$

$$R \cdot R = \quad \{(x, 4x) \mid x \in N\}$$

$$R \cdot R \cdot R = \quad \{(x, 8x) \mid x \in N\}$$

$$R \cdot S \cdot R = \quad \{(x, 20x) \mid x \in N\}$$

9. Let R = {(1,1), (1, 2), (2,1), (4,3)} be a relation on A={1, 2, 3, 4}. Find the transitive closure of R by Warshall's algorithm.

Solution:

$$W_0 = M_{R} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

First we find W_1 from W_0 so that k = 1. W_0 has 1's in locations 1 and 2 of column 1 and row 1. Thus W_1 is W_0 with a new 1 in the positions (1,1), (1,2), (2,1), (2, 2).

$$W_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Now we compute W_2 from W_1 so that k=2. W_1 has 1's in locations 1 and 2 of column 2 and row 2.

Thus, W_2 has no new 1's. So, we get

$$W_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Hence, $M_R^{\infty} = W_2 = W_1$.

So, R^{∞} ={(1,1), (1,2), (2,1), (2,2), (4,3)}

5.12 SUMMARY

Definition: Let A and B be two non-empty sets. A Relation (Binary relation) R from A to B is a subset of A × B.

Definition: Let A= {a_1, a_2, …, a_m) and B={b_1,b_2,…, b_n} be two sets. Let R be the relation from A to B. The relation R can be represented by an m × n matrix called Relation Matrix, denoted by M_R.

Definition: Let A be a finite set and R be a relation on A. The digraph of R consists of elements of A as vertices and (a_i, a_j) in R as a directed edge from a_i to a_j.

Definition: Let A be a set and R be a relation on A. R is said to be an equivalence relation if it is reflexive, symmetric and transitive.

Definition: A relation R is said to be a *compatibility relation* if it is reflexive and symmetric.

Definition: Let R be a relation from A to B and S be a relation from B to C. Then a relation written as R · S is called a *composite relation* of R and S where

$$R \bullet S = \{(a, c)|\ (a, b) \in R \text{ and } (b, c) \in S\}$$

Warshall's Algorithm is a simple and easy procedure to compute the transitive closure of R.

5.13 KEYWORDS

Relation, relation matrix, digraph, transitive closure

5.14 QUESTIONS

1. Find the domain, range, relational matrix and the digraph of the relation R for the following.

i. A={x, y, z}, B={1, 2, 3, 4}, R={(x,1), (y,2), (y,1), (x,2), (z,1), (z,4), (y,4)}

ii. A= B={1, 2, 3, 4, 9, 10}, R={(a, b) | $a=b^2$}.

2. Let A= {1, 2, 3, 4, 5}. Determine whether R is reflexive, symmetric, anti symmetric and transitive.

i. R={(1,1), (1,3), (1,4), (2,1), (2,4), (3,4),(4,5), (5,5)}

ii. R={(1,1), (2,2), (3,3), (3, 5), (5,5)}

3. If R is the relation on Z, the set of integers such that R={(x,y)| x congruent to y (mod 2)}. Determine whether R is an equivalence relation. If so, find the partition generated by R.
4. Let the compatibility relation on a set {1, 2, …, 6} be given by the matrix

$$\begin{array}{c|cccc} 2 & 0 & & & \\ 3 & 1 & 1 & & \\ 4 & 1 & 0 & 1 & \\ 5 & 0 & 1 & 0 & 1 \\ \hline & 1 & 2 & 3 & 4 \end{array}$$

Draw the graph and find all the maximal compatibility blocks of the relation.

iii. Let R = {(1, 2), (4, 5), (2, 2), (3,1)} and S = {(1, 1), (2, 1), (3, 3), (5, 3)} be relations on the set A= {1, 2, …, 5}. Find R · S, S · R, R · (S · R), (R · S) · R, matrices of R · S and S · R.

5. Let R = {(1,1), (1, 4), (2,1), (2,2), (2,4), (3,3), (4,4)} be a relation on A={1, 2, 3, 4}. Find the transitive closure of R by Warshall's algorithm.

5.15 REFERENCES

1. Discrete mathematics for computer science, by Kolman, Busby and Ross, PHI publications.
2. Discrete Mathematical Structures, by N. G. Goudru, Himalaya Publishing House.
3. Discrete mathematical structures with applications to computer science, by Tremblay and Manohar (McGraw-Hill publications).

UNIT-6: RECURRENCE RELATION I

Structure

6.0 Objectives

6.1 Introduction

6.2 Recurrence relation

6.3 Backtracking method

6.4 Characteristic equation method

6.5 Solved Problems

6.6 Summary

6.7 Keywords

6.8 Questions

6.9 References

6.0 OBJECTIVES

When you go through this unit, you will be able to

- ✓ Explain the meaning of a recurrence relation;
- ✓ Evaluate the recurrence relation by the method of backtracking.
- ✓ Evaluate the recurrence relation by the method of characteristic equation.

6.1 INTRODUCTION

A recurrence relation is an equation that recursively defines a sequence: each term of the sequence is defined as a function of the preceding terms. The term difference equation sometimes refers to a specific type of recurrence relation. Note however that "difference equation" is frequently used to refer to *any* recurrence relation. Some simply defined recurrence relations can have very complex (chaotic) behaviors, and they are a part of the field of mathematics known as nonlinear analysis. Solving a recurrence relation means obtaining a closed-form solution: a non-recursive function of n.

6.2 RECURRENCE RELATION

Definition: An equation that expresses a_n i.e. general term of the sequence$\{a_n\}$ in terms of one or more of the previous terms of the sequence, namely $a_0, a_1,\ldots, a_{n-1}$ for all integers n with $n \geq n_0$ where n_0 is a non-negative integer is called a recurrence relation for $\{a_n\}$or a difference relation.

Every recurrence relation must have an initial value.

Examples 1:

(i) $x_n = 5x_{n-1}+ 8x_{n-2}, x_1 = 4$.

(ii) $x_n = 2x_{n-1} + 5, x_1 = -2$.

Definition: A recurrence relation of the form $C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \ldots + C_K a_{n-K} = f(n)$ is called a linear recurrence relation of degree K with constant coefficients where $C_0, C_1,\ldots, C_K$ are real numbers and $C_K \neq 0$.

Note:

1) The recurrence relation is called linear because each a_n is raised to the power 1.

2) The degree of the recurrence relation is the difference between the greatest and least subscripts of the members of the sequence occurring in the recurrence relation.

3) If $f(n) = 0$ the recurrence relation is said to be homogeneous; otherwise it is said to be non-homogeneous.

Examples 2:

i. A relation, $C_n = -2\ C_{n-1}$ is a linear homogeneous recurrence relation of degree 1.

ii. A relation $x_n = 4\ x_{n-1} + 5$ is a linear non-homogeneous recurrence relation because second term in RHS is a constant. It does not contain x_{n-2} factor.

iii. A relation $x_n = x_{n-1} + 2\ x_{n-2}$ is a linear homogeneous relation of degree 2.

iv. A relation $x_n = x^2_{n-1} + x_{n-2}$ is a non-linear, non-homogeneous relation, because the first term in RHS is a second degree term.

Method of Solving Recurrence Relations

The important methods to solve a recurrence relation are:

(i) Backtracking method

(ii) Characteristic equation method.

(iii) Generating function method.

6.3 BACKTRACKING METHOD

This is a suitable method for linear non-homogeneous recurrence relation of the type $x_n = rx_{n-1} + s$. The method is explained below using an example.

Example 3: Using backtrack method solve the recurrence relation

$x_n = x_{n-1} + 5, x_1 = 5.$

Solution:

$x_n = x_{n-1} + 5, x_1 = 2.$ ....(1)

Put $n= n$-1 in (1)

$x_{n-1} = x_{n-2} + 5$ ....(2)

Using (2) in (1)

$x_n = (x_{n-2} + 5)+5$

$x_n = x_{n-2} + 2 \times 5$ ....(3)

Put $n = n$-2 in (1)

$x_{n-2} = x_{n-3} +5$ ....(4)

Using (4) in (3)

$x_n = (x_{n-3} +5) + 2 \times 5$

$x_n = x_{n-3} + 3 \times 5$

....

....

Repeating for (n-1) times, we get

$x_n = x_1 + 5(n-1), x_1 = 5.$

$x_n = 5 + 5(n-1).$

$x_n=5n.$

6.4 CHARACTERISTIC EQUATION METHOD

By the Characteristic Equation method, there are two parts to the total solution of the recurrence relation. The Complementary Function (homogeneous part) of the solution depends only on the LHS of the recurrence relation. The Particular Integral (particular solution) depends on the *RHS* and has the same form as the *RHS*. The two parts are computed to form the total solution.

Given the recurrence relation $aU_{n+2} + bU_{n+1} + cU_n = f(n)$ with $U_0 = \alpha$, $U_1 = \beta$ we proceed as follows.

Step 1: Rule to find the complementary function.

Frame the auxiliary (characteristic) equation

$$am^2 + bm + c = 0$$

Depending on the nature of the roots of above, *CF* is got as follows:

Nature of Roots	***CF***
Real distinct λ, μ	$c_1 \lambda^n + c_2 \mu^n$
Real repeated λ, λ	$(c_1 + c_2^n) \lambda^n$
Complex roots $r\, e^{\pm i\theta}$	$r^n(c_1 \cos n\theta + c_2 \sin n\theta)$

Step 2: Finding *Particular Integral* (*PI*) by the method of indeterminant coefficients.

The *PI* is formed for each term or group of terms on RHS. A suitable trial *PI* function U_n is chosen from the table below, substituted in the recurrence relation and the unknowns are found.

The choice of trial PI function depends on the type of term in $f(n)$. Refer table 6.1.

Step 3 Using the initial conditions C_1, C_2 are evaluated to get the total solution.

Table of trial function

Type of term	Trial function
a^n	$A a^n$ $An\, a^n$ *if* a^n*is in CF* An^2a^2*if* a^n and $n\, a^n$ are in *CF*
$a^n(\alpha n^2 + \beta n + c)$	$a^n(An^2 + Bn + C)$ Take higher order polynomial if needed
$\alpha n^2 + \beta n + c$	$An^2 + Bn + C$ Take higher order if needed
$\alpha \cos nA + \beta \sin nA$	$A \cos nA + B \sin nA$
$a^n(\alpha \cos nA + \beta \sin nA)$	$a^n(A\cos nA + B \sin nA)$

Table 6.1

Example 4: Solve $a_n = 4a_{n-1} - 4a_{n-2} + (n + 1)2^n$ by the characteristic equation method.

Solution: By rearranging the given equation we get,

$$a_n - 4a_{n-1} + 4a_{n-2} = (n + 1)2^n$$

The auxiliary equation is

$$m^2 - 4m + 4 = 0$$

$$m = 2, 2$$

$$CF = (c_1 + c_2n)2^n$$

We assume the particular solution as

$$a_n = n^2(c_1 + c_2n)2^n$$

$$a_{n-1} = (n-1)^2\ (c_1 + c_2(n-1))2^{n-1}$$

$$a_{n-2} = (n-2)^2\ (c_1 + c_2(n-2))2^{n-2}$$

$$n^2(c_1 + c_2n)2^n - 4(n-1)^2(c_1 + c_2(n-1))2^{n-1} + 4(n-2)^2\ (c_1 + c_2(n-2))2^{n-2} = (n + 1)2^n$$

$$n^2(c_1 + c_2n)2^n - 4(n^2-2n+1)(\ c_1 + c_2n-c_2)\ 2^{n-1} + 4(n^2-4n+4)(\ c_1 + c_2n-2c_2)\ 2^{n-2} = n2^n + 2^n$$

Equating the coefficient of n^2 on both sides

$$n^2(c_1 + c_2n) - 2(n^2-2n+1)(\ c_1 + c_2n-c_2) + (n^2-4n+4)(\ c_1 + c_2n-2c_2) = n + 1$$

$$c_1 - 2c_1 + 2c_2 + 4c_2 + c_1 - 2c_2 - 4c_2 = 0$$

Equating the coefficient of n, $4c_1 - 4c_2 - 2c_2 - 4c_1 + 8c_2 + 4c_2 = 1$

$$6c_2 = 1$$

$$c_2 = 1/6$$

Equating constant terms

$$-2c_1 + 2c_2 + 4c_1 - 8c_2 = 1$$

$$2c_1 - 6c_2 = 1$$

$$2c_1 - 1 = 1$$

$$c_1 = 1$$

$$a_n = (c_1 + c_2 n)2^n + n^2[1 + (n/6)]2^n$$

$$= [1 + (1/6)n]2^n + n^2[1 + (n/6)]2^n$$

6.5 SOLVED PROBLEMS

1. Solve $C_n = C_{n-1} + n$, $C_1 = 5$, by the method of backtracking.

Solution:

Given, $C_n = C_{n-1} + n$, $C_1 = 5$ ....(1)

Put $n=n-1$ in (1)

$C_{n-1} = C_{n-2} + (n-1)$ ....(2)

Using (2) in (1)

$C_n = C_{n-2} + (n-1) + n$ ....(3)

Put $n= n-1$ in (1)

$C_{n-2} = C_{n-3} + (n-2)$ ....(4)

Using (4) in (3),

$C_n = C_{n-3} + [(n-2) + (n-1) + n]$

....

....

$C_n = C_1 + [\, 1 + 2 + 3 + ... + (n\text{-}2) + (n\text{-}1) + n]$

$C_n = C_1 + \frac{n(n-1)}{2}$

$C_n = 5 + \frac{n(n-1)}{2}$.

2. **Using backtrack method solve $e_n = e_{n-1} - 2$, $e_1 = 2$.**

Solution:

$e_n = e_{n-1} - 2,\ e_1 = 2$ ....(1)

Put $n=n$-1 in (1)

$e_{n-1} = e_{n-2} - 2$ ....(2)

Using (2) in (1)

$e_n = e_{n-2} - 2\text{-}2$

$e_n = e_{n-2} - 2(2)$ ....(3)

Put $n=n$-2 in (1)

$e_{n-2} = e_{n-3} - 2$ ....(4)

Using (4) in (3),

$e_n = e_{n-3} - 2\text{-}2(2)$

$e_n = e_{n-3} - 2(3)$

....

....

$e_n = e_1 - 2(n\text{-}1)$

$e_n = 2 - 2(n\text{-}1)$

$2 - 2n + 2$

$e_n = 4 - 2n$.

3. Solve $a_{n+2} - 3a_{n+1} + 2a_n = 2^n$; $n \geq 0$ given $a_0 = 3$, $a_1 = 6$ by the characteristic equation method.

Solution: The characteristic equation is

$m^2 - 3m + 2 = 0$

$m = 1, 2$

$$CF = c_1 1^n + c_2 2^n = c_1 + c_2 2^n$$

Assume the trial solution as

$a_n = An2^n$

$a_{n+1} = A(n+1)2^{n+1} = 2(An+A)2^n = 2An2^n + 2A2^n$

$a_{n+2} = A(n+2)2^{n+2} = 2^2(An+2A)2^n = 4An2^n + 8A2^n$

$$4An2^n + 8A2^n - 3(2An2^n + 2A2^n) + 2An2^n = 2^n$$

$$4An + 8A - 6An - 6A + 2An = 1$$

Equating coefficient of n, $4A - 6A + 2A = 0$

Equating constants c, $2A = 1$, $A = ½$

$a_n = c_1 + c_2 2^n + (1/2)n2^n = c_1 + c_2 2^n + n2^{n-1}$

put $n=0$, $a_0 = c_1 + c_2 \Rightarrow c_1 + c_2 = 3$

$n=1$, $a_1 = c_1 + 2c_2 + 1 \Rightarrow c_1 + 2c_2 = 5$

$c_2 = 2$ and $c_1 = 1$

$\therefore$ $a_n = 1 + 2.2^n + n2^{n-1}$

$a_n = 1 + 2^{n+1} + n2^{n-1}$

4. Solve $a_{n+1} - 2a_n = 5$; $n \geq 0$ $a_0 = 1$, by the Characteristic equation method.

Solution: The auxiliary equation is

$m - 2 = 0$

$m = 2$

$CF = c_1 2^n$

Assume the trial particular solution as

$a_n = A$; $a_{n+1} = A$

$A - 2A = 5$

$-A = 5$; $A = -5$

$a_n = c_1 2^n - 5$

put $n=0$, $a_0 = c_1 - 5$

$c_1 = 6$

$a_n = 6(2^n) - 5$

5. Solve $a_n - 2a_{n-1} = 2n^2$; $n \geq 1$ given $a_0 = 4$, by the method of characteristic equation.

Solution: The auxiliary equation is

$m - 2 = 0$; $m = 2$; $CF = c_1 2^n$

Assume the trial particular solution as

$a_n = An^2 + Bn + C$

$a_{n-1} = A(n-1)^2 + B(n-1) + C$

$An^2 + Bn + C - 2\,An^2 + 4An - 2A - 2Bn + 2B - 2C = 2n^2$

Equating coefficient of n^2, $A - 2A = 2$

$A = -2$

Equating coefficient of n, $B + 4A - 2B = 0$

$4A - B = 0$

$-8 - B = 0$

$B = -8$

Equating constants, $C - 2A + 2B - 2C = 0$

$-2A + 2B - C = 0$

$C = -2(-2) + 2(-8)$

$C = -12$

$a_n = -2n^2 - 8n - 12$

$\therefore$ $a_n = c_1\, 2^n - 2n^2 - 8n - 12$

put $n=1$, $a_1 = 2c_1 - 2 - 8 - 12$

$4 = 2c_1 - 22$

$\Rightarrow 2c_1 = 26$; $c_1 = 13$

$a_n = 13(2^n) - 2(n^2 + 4n + 6)$

6. Solve $a_{n+2} - 7a_{n+1} - 8\, a_n = n(n-1)\, 2^n = (n^2 - n)2^n$

Solution: The auxiliary equation is

$m^2 - 7m - 8 = 0$

$(m - 8)(m + 1) = 0$

$m = 8, -1$

$CF = c_1 8^n + c_2(-1)^n$

Assume the trial particular solution as

$a_n = (An^2 + Bn + C)2^n$

$a_{n+1} =[A (n^2 +2n +1)+ B(n + 1)+ C]2^{n+1}$

$a_{n+2} =[A (n^2 +4n +4)+ B(n + 2)+ C]2^{n+2}$

$(An^2 + 4An + 4A + Bn + 2B + C)2^{n+2} – 7(An^2 + 2An + A$

$+ Bn + B + C)2^{n+1} – 8(An^2 + Bn + C)2^n = (n^2 – n)2^n$

$4An^2 + 16An + 16A + 4Bn + 8B + 4C -14An^2 – 28An – 14A$

$-14Bn – 14B – 14C - 8An^2 - 8Bn - 8C)\ \ C) = n^2 – n$

Equating coefficients of n^2,

$$4A – 14 A – 8A = 1$$

$$A = -(1/18)$$

Equating coefficient of n,

$$16A + 4B – 28A – 14B – 8B = -1$$

$$-12A – 18B = -1$$

$$18B = 1 – 12A$$

$$= 1 – 12[-(1/18)]$$

$$= 1 + (2/3) =5/3$$

$$B = 5/54$$

Equating constant,

$$16A + 8B + 4C – 14A – 14B – 14C – 8C = 0$$

$$2A – 6B -18C = 0$$

$$18C = 2A – 6B$$

$$9C = A – 3B$$

$$= (-1/18) – 3(5/54)$$

$$= -(1/18) – (5/54)$$

$$= -(6/18) = -1/3$$

$$C = -1/54$$

$\therefore \quad a_n = \left(\frac{-1}{18} n^2 + \frac{5}{54} n - \frac{1}{54}\right) 2^n$

$a_n = c_1 8^n +c_2(-1)^n – (1/54)(3n^2 – 5n + 1)2^n.$

6.6 SUMMARY

A recurrence relation is an equation that recursively defines a sequence: each term of the sequence is defined as a function of the preceding terms.

A recurrence relation of the form $C_0a_n + C_1a_{n-1} + C_2a_{n-2} + \ldots + C_K a_{n-K} = f(n)$ is called a linear recurrence relation of degree K with constant coefficients where $C_0, C_1, \ldots, C_K$ are real numbers and $C_K \neq 0$.

The important methods to solve a recurrence relation are:

(i) Backtracking method

(ii) Characteristic equation method.

(iii) Generating function method.

Backtracking is a suitable method for linear non-homogeneous recurrence relation of the type $x_n = rx_{n-1} + s$.

The characteristic equation method involves the computation of complementary function and particular integral to solve linear recurrence relation.

6.7 KEYWORDS

Recurrence relation, sequence, auxiliary equation.

6.8 QUESTIONS

1. Solve the following recurrence relations by the method of backtracking.

i) $b_n = 3b_{n-1} + 1, b_1 = 7$

ii) $a_n = a_{n-1} + 2\ n, a_1 = 5.$

2. Solve the following recurrence relations by the characteristic equation method.

i) $a_n = 3\ a_{n-1} - 2\ a_{n-2}$, $a_0 = 5$ and $a_1 = 4$.

ii) $a_n = 4a_{n-1} - 4a_{n-2} + 2^n$, $a_0 = 3$, $a_1 = 6$.

iii) $a_{n+2} - 7a_{n+1} - 12\ a_n = n(n-1)\ 2^n$

iv) $a_{n+1} - 8a_n = 5$; $n \geq 0$ $a_0 = -2$.

6.9 REFERENCES

1. Discrete mathematics, by P. Geetha, Scitech publications.
2. Discrete mathematics for computer science, by Kolman, Busby and Ross, PHI publications.
3. Discrete Mathematical Structures, by N. G. Goudru, Himalaya Publishing House.

UNIT-7: RECURRENCE RELATION II

Structure

7.0 Objectives

7.1 Introduction

7.2 Generating functions

7.3 Solved problems

7.4 Summary

7.5 Keywords

7.6 Questions

7.7 References

7.0 OBJECTIVES

When you go through this unit, you will be able to

- ✓ Explain the meaning of the generating functions;
- ✓ Evaluate homogeneous recurrence relation by the method of generating functions.
- ✓ Evaluate non-homogeneous recurrence relation by the method of generating functions.

7.1 INTRODUCTION

A generating function is a formal power series in one indeterminate, whose coefficients encode information about a sequence of numbers that is indexed by the natural numbers. Generating functions were first introduced by Abraham de Moivre in 1730, in order to solve the general linear recurrence problem.

Generating functions are often expressed in closed form (rather than as a series), by some expression involving operations defined for formal power series. Indeed, the closed form expression can often be interpreted as a function that can be evaluated at (sufficiently small) concrete values of x, and which has the formal power series as its Taylor series; this explains the designation "generating functions". Generating functions are not functions in the formal sense of a mapping from a domain to a codomain; the name is merely traditional, and they are sometimes more correctly called generating series.

The particular generating function, if any that is most useful in a given context will depend upon the nature of the sequence and the details of the problem being addressed.

7.2 GENERATING FUNCTION

Definition: The generating function of a sequence $a_0, a_1, a_{2,}, \ldots$ is the expression

$$G(x) = a_0 + a_1 x + a_2 x^2 + \ldots$$
$$= \sum_{n=0}^{\infty} a_n x^n.$$

7.3 SOLVED PROBLEMS

1. Solve the recurrence relation $a_n = 3a_{n-1} + 1$, $n \geq 1$; given that $a_0 = 1$, by the method of generating function.

Solution:

Let the generating function of $\{a_n\}$ be $G(x) = \sum_{n=0}^{\infty} a_n x^n$

.Multiply the given RR by x^n and sum $n=1$ to ∞

$$= \sum_{n=1}^{\infty} a_n x^n = 3 \sum_{n=1}^{\infty} a_{n-1} x^n + \sum_{n=1}^{\infty} x^n$$

$$G(x) - a_0 = 3x \sum_{n=1}^{\infty} a_{n-1} x^{n-1} + x + x^2 + \ldots\ldots \infty$$

$$G(x) - a_0 = 3x\, G(x) + x(1-x)^{-1}$$

$$(1-3x)G(x) = 1 + \frac{x}{1-x} = \frac{1-x+x}{1-x} = \frac{1}{1-x}$$

$$G(x) = \frac{1}{(1-x)(1-3x)} = \frac{-\frac{1}{2}}{1-x} + \frac{\frac{3}{2}}{1-3x}$$

$$= \frac{-1}{2}(1-x)^{-1} + \frac{3}{2}(1-3x)^{-1}$$

$$\sum_{n=0}^{\infty} a_n = \frac{-1}{2}\sum_{n=0}^{\infty} x^n + \frac{3}{2}\sum_{n=0}^{\infty} 3^n\, x^n$$

$\therefore a_n =$ Coefficient of x^n in $G(x)$

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

2. Use the method of generating function to solve the recurrence relation $a_n = 4a_{n\text{-}1} - 4a_{n\text{-}2} + 4^n$; $n \geq 2$, given that $a_0 = 2$, $a_1 = 8$.

Solution: Let $G(x) = \sum_{n=0}^{\infty} a_n\ x^n$

Multiply the Recurrence Relation by x^n and sum n=2 to ∞

$$\sum_{n=2}^{\infty} a_n\ x^n = 4\sum_{n=2}^{\infty} a_{n-1}\ x^n - 4\sum_{n=2}^{\infty} a_{n-2}\ x^n + \sum_{n=2}^{\infty} 4^n\, x^n$$

$$G(x) - a_0 - a_1x = 4x\sum_{n=2}^{\infty} a_{n-1}\ x^{n-1} - 4x^2\sum_{n=2}^{\infty} a_{n-2}\ x^{n-2} + [(4x)^2 + (4x)^3 + \ldots]$$

$$= 4x\,(G(x) - a_0) - 4x^2G(x) + (4x)^2(1\text{-}4x)^{-1}$$

$$G(x)\text{-}2\text{-}8x = 4x\,(G(x) - 2) - 4x^2G(x) + (4x)^2(1\text{-}4x)^{-1}$$

$$(4x^2\text{-}4x\text{-}1)\ G(x) = 2 + 8x\text{-}8x + \frac{16^2}{1-4x}$$

$$= 2 + \frac{16^2}{1-4x} = \frac{2-8x+16x^2}{1-4x}$$

$$G(x) = \frac{2-8x+16x^2}{(1-4x)(1-2x)^2}$$

Consider

$$\frac{2-8x+16x^2}{(1-2x)(1-2x)^2} = \frac{A}{1-2x} + \frac{B}{(1-2x)^2} + \frac{C}{1-4x}$$

$$2 - 8x + 16x^2 = \text{A}\ (1\text{-}2x)\ (1\text{-}4x) + \text{B}(1\text{-}4x) + \text{C}(1\text{-}2x)^2$$

Put $x = \frac{1}{2}$ $\quad -B = 2\text{-}4\text{+}4$

$B = -2$

Put $x = \frac{1}{4}$ $\quad \frac{C}{4} = 2\text{-}2\text{+}1 = 1$

$C = 4$

Put x=0 $\quad A+B+C=2$

$A = 0$

$$G(x) = \frac{2-8x+16x^2}{(1-4x)(1-2x)^2}$$

$$= \frac{4}{1-4x} - \frac{2}{(1-2x)^2}$$

$$= 4(1\text{-}4x)^{-1} - 2(1\text{-}2x)^{-2}$$

$= 4(1+4x+(4x)^2+ \ldots. +(4x)^n + \ldots \infty) - 2(1+2(2x)+3(2x)^2+ \ldots. +(n+1)(2x)^n+$

$\ldots\ldots. \infty)$

$a_n = 4.4^n - 2.2^n(n+1)$

$= 4^{n+1}\text{-}2^{n+1}(n+1)$

3. Use the method of generating function to solve a_n - $a_{n-1} - 2a_{n-2} = 0$ with $a_0 = 5$, $a_1 = -3$.

Solution: Let $G(x) = \sum_{n=0}^{\infty} a_n \ x^n$

Consider, a_n - $a_{n-1} - 2a_{n-2} = 0$

a_nx^n - $a_{n-1}x^n - 2a_{n-2}x^n = 0.$ [By multiplying by x^n]

$\sum_{n=2}^{\infty} a_n x^n - \sum_{n=2}^{\infty} a_{n-1} x^n - 2\sum_{n=2}^{\infty} a_{n-2} x^n = 0$ [By taking summation]

$[G(x) - a_0 - a_1x] - x[G(x) - a_0] - 2x^2G(x) = 0$

$(1\text{-}x\text{-}2x^2)\ G(x) - 5 + 3x + 5x = 0$

$(1\text{-}x\text{-}2x^2)\ G(x) = 5 - 8x$

$$G(x) = \frac{5-8x}{1-x-2x^2}$$

$$= \frac{8x-5}{(2x-1)(x+1)}$$

Consider, $\frac{8x-5}{(2x-1)(x+1)} = \frac{A}{2x-1} + \frac{B}{x+1}$

$8x - 5 = A(x + 1)+ B(2x - 1)$

$A + 2B = 8$

$A - B = -5$

$3B = 13$

$B = 13/3$

$A = B - 5 = (13/3) - 5$

$A = -2/3$

$$G(x) = \frac{8x-5}{(2x-1)(x+1)}$$

$$= \frac{-2/3}{(2x-1)} + \frac{13/3}{(x+1)}$$

$$= \frac{2}{3}\ \frac{1}{1-2x} + \frac{13}{3}\ \frac{1}{1+x}$$

$$= \frac{2}{3}(1-2x)^{-1} + \frac{13}{3}(1+x)^{-1}$$

$$= \frac{2}{3}[1 + (2x) + (2x)^2 + \ldots. + (2x)^n + \ldots\ \infty]$$

$$+ \frac{13}{3}[1 - x + x^2 - \ldots.. + (-1)^n x^n + \ldots..\ \infty]$$

$$\therefore \quad \sum_{n=0}^{\infty} a_n x^n = \frac{2}{3}\sum_{n=0}^{\infty} 2^n x^n + \frac{13}{3}\sum_{n=0}^{\infty}(-1)^n x^n = 0$$

$$\therefore \quad a_n = \frac{2}{3} \cdot 2^n + \frac{13}{3}(-1)^n.$$

4. Solve u_{n+1} -3 u_n =7.2^n with $u_0 = 1$

Solution: Let $G = \sum_{n=0}^{\infty} u_n\ z^n$ be the generating function of the sequence u_n.

Given, u_{n+1} -3 u_n =7.2^n ....(1)

Multiply (1) by z^{n+1} and sum from n=0 to ∞

$$\sum_{n=0}^{\infty} u_{n+1}\ z^{n+1} - 3\sum_{n=0}^{\infty} u_n\ z^{n+1} = 7\sum_{n=0}^{\infty} 2^n z^{n+1}$$

$$= 7z\sum_{n=0}^{\infty} 2^n z^n$$

$$G - u_0 - 3zG = 7z\,(1-2z)^{-1} = \frac{7z}{1-2z}$$

$$(1-3z)G = 1 + \frac{7z}{1-2z}$$

$$= \frac{1-2z+7z}{1-2z} = \frac{1+5z}{1-2z}$$

$$G = \frac{1+5z}{(1-2z)(1-3z)} = \frac{A}{1-2z} + \frac{B}{1-3z}$$

$$\frac{1+5z}{(1-2z)(1-3z)} = \frac{A}{1-2z} + \frac{B}{1-3z}$$

$$1 + 5z = A(1-3z) + B(1-2z)$$

Equating coefficient of z, $-3A - 2B = 5$ $\quad -3A - 2B = 5 \quad B = 1 - A$

Equating constant c, $A + B = 1$ $\quad 2A + 2B = 2 \quad B = 1 + 7$

$-A = 7 \quad B = 8$

$A = -7$

$$G = \frac{-7}{1-2z} + \frac{8}{1-3z}$$

$$u_n = -7(2)^n + 8(3)^n$$

check $u_0 = -7 + 8 = 1$

5. Solve u_{n+2} -5u_{n+1} + 6u_n =n+2 with u_0 = 0, u_1=1.

Solution: Let $G = \sum_{n=0}^{\infty} u_n \ z^n$ be the generating function of the sequence u_n.

Given u_{n+2} -5u_{n+1} + 6u_n =n+2 ....(1)

Multiply (1) by z^{n+2} and sum from n=0 to ∞

$$\sum_{n=0}^{\infty} u_{n+2} \ z^{n+2} - 5\sum_{n=0}^{\infty} u_{n+1} \ z^{n+2} + 6 \sum_{n=0}^{\infty} u_n \ z^{n+2} = \sum_{n=0}^{\infty} (n+2) \ z^{n+2}$$

$$G - (u_0 + u_1 z) - 5z(G - u_0) + 6z^2 G = z^2 \sum_{n=0}^{\infty} n \ z^n + 2z^2 \sum_{n=0}^{\infty} \quad z^n$$

$$G - z - 5zG + 6z^2G = z^2[z + 2z^2 + 3z^3 + \ldots.] + 2z^2[\ 1 + z + z^2 + \ldots\ldots\ ]$$

$$(1 - 5z + 6z^2)G - z = z^3(1 - z)^{-2} + 2z^2(1 - z)^{-1}$$

$$= \frac{z^3}{(1-z)^2} + \frac{2z^2}{1-z}$$

$$(1 - 5z + 6z^2)G = z + \frac{2z^2}{1-z} + \frac{z^3}{(1-z)^2}$$

$$= \frac{z(1-z)^2 + 2z^2(1-z) + z^3}{(1-z)^2}$$

$$= \frac{z(1+z^2-2z) + 2z^2 - 2z^3 + z^3}{(1-z)^2}$$

$$= \frac{z + z^3 - 2z^2 + 2z^2 - 2z^3 + z^3}{(1-z)^2} = \frac{z}{(1-z)^2}$$

$[6z^2 - 5z + 1 = 0$

$$z = \frac{5 \pm \sqrt{25-24}}{12}$$

$$= \frac{5 \pm 1}{12} = \frac{1}{2}, \frac{1}{3}$$

$(2z - 1)\ (3z - 1) = 0]$

$$G = \frac{z}{(1-z)^2(1-5z+6z^2)}$$

$$= \frac{z}{(1-z)^2(2z-1)(3z-1)}$$

$$\frac{z}{(1-z)^2(2z-1)(3z-1)} = \frac{A}{1-z} + \frac{B}{(1-z)^2} + \frac{C}{2z-1} + \frac{D}{3z-1}$$

$$z = A(1 - z)\ (2z - 1)\ (3z - 1) + Bz(2z - 1)(3z - 1) + C(1 - z)^2(3z - 1) + D(1 - z)^2(2z\text{-}1)$$

Put z=1, $1 = 2B \Rightarrow B = ½$

Put z=0, $0 = A - C - D$

$A - D = 4$

$A + (9/4) = 4 \Rightarrow A = 7/4$

Put z=1/2 $(1/2) = C.\ (1/8)$

$C = 4$

Put $z = 1/3$ $\quad$ $(1/3) = (-4/27)D$

$$D = (-27/4)\,(1/3) = -9/4$$

$$G = \frac{7/4}{1-z} + \frac{1z/2}{(1-z)^2} + \frac{4}{2z-1} - \frac{9/4}{3z-1}$$

$$= \frac{7}{4}\frac{1}{(1-z)} + \frac{1}{2}\frac{z}{(1-z)^2} - \frac{4}{1-2z} + \frac{9}{4}\frac{1}{1-3z}$$

$$u_n = \frac{7}{4}(1)^n + \frac{7}{4}n - 4(2)^n + \frac{9}{4}(3)^n$$

Check:

$$u_0 = \frac{7}{4} - 4 + \frac{9}{4} = \frac{7-16-9}{4} = 0$$

$$u_1 = \frac{7}{4} + \frac{1}{2} - 8 + \frac{27}{4} = \frac{7+2-32+27}{4} = \frac{4}{4} = 1$$

6. Solve $y_{n+2} -6y_{n+1} +5y_n =0$ with $y_0 = 2$, $y_1=6$.

Solution: Let $G(z) = \sum_{n=0}^{\infty} y_n\ z^n$ be the generating function of the sequence y_n

Given, $y_{n+2} -6y_{n+1} +5y_n =0$ ....(1)

Multiply (1) by z^{n+2} and sum from n=0 to ∞

$$\sum_{n=0}^{\infty} y_{n+2}\ z^{n+2} - 6\sum_{n=0}^{\infty} y_{n+1}\ z^{n+2} + 5\sum_{n=0}^{\infty} y_n z^{n+2} = 0$$

$$G(z) - [y_0 + y_1 z] - 6z[G(z) - y_0] + 5z^2 G(z) = 0$$

$$G(z) - [2 + 6z] - 6z[G(z) - 2] + 5z^2\ G(z) = 0$$

$$(1 - 6z + 5z^2)\ G(z) - 2 - 6z + 12z = 0$$

$$(1 - 6z + 5z^2)\ G(z) = 2 - 6z$$

$$[5z^2 - 6z + 1 = 0$$

$$z = \frac{6 \pm \sqrt{36-20}}{10}$$

$$= \frac{6 \pm 4}{10};\ 1,\ 1/5$$

$$(z - 1)(5z - 1) = 0]$$

$$(1 - 6z + 5z^2)G = 2 - 6z$$

$$G(z) = \frac{2-6z}{5z^2-6z+1} = \frac{A}{z-1} + \frac{B}{5z-1}$$

$$2 - 6z = A(5z - 1) + B(z-1)$$

$5A + B = -6$

$-A - B = 2$

$4A = -4;$ $A = -1$ and $B = -1$

$$G(z) = \frac{-1}{z-1} - \frac{1}{5z-1}$$

$$= \frac{1}{1-z} + \frac{1}{1-5z}$$

$y_n = 1 + 5^n$

7.4 SUMMARY

The generating function of a sequence (a_n) is the expression

$$G(x) = \sum_{n=0}^{\infty} a_n \; x^n.$$

Generating functions were first introduced by Abraham de Moivre in 1730, in order to solve the general linear recurrence problem. Generating functions are not functions in the formal sense of a mapping from a domain to a co-domain; the name is merely traditional, and they are sometimes more correctly called generating series.

7.5 KEYWORDS

Generating function, sequence, recurrence relation.

7.6 QUESTIONS

1. Solve the recurrence relation $a_n = 5a_{n-1} + 2$, $n \geq 1$; given that $a_0 = 3$, by the method of generating function.
2. By the generating function method, solve $u_n - 2u_{n-1} - u_{n-2} = 0$ with $u_0 = 3$, $u_1 = -5$.
3. Solve $u_{n+1} - 3\,u_n = 7.2^n$ with $u_0 = -2$.
4. Solve the recurrence relation $a_n = 2a_{n-1} - 2a_{n-2} + 3^n$; $n \geq 2$, given that $a_0 = 2$, $a_1 = 8$.
5. Solve $y_{n+2} - 6y_{n+1} + 5y_n = 0$ with $y_0 = 2$, $y_1 = 6$.

7.7 REFERENCES

1. Discrete Mathematics, by P. Geetha (Scitech publications).
2. Discrete Mathematics for Computer Science, by Kolman, Busby and Ross, PHI publications.

UNIT-8: FUNCTIONS

Structure

8.0 Objectives

8.1 Introduction

8.2 Basic terminology

8.3 Types of functions

8.4 Composition of functions

8.5 Inverse of a function

8.6 Characteristic function

8.7 Permutation functions

8.8 Hashing functions

8.9 Recursive functions

8.10 Solved problems

8.11 Summary

8.12 Keywords

8.13 Questions

8.14 References

8.0 OBJECTIVES

When you go through this unit, you will be able to

- ✓ Explain the meaning of a function;
- ✓ Analyse the composition of functions.
- ✓ Evaluate the various types of functions.

8.1 INTRODUCTION

A relation is mainly a correspondence between the members of two sets, associating members of the first set with those of the second. It is possible that a given relation associates with any member of the first set several different members of the second set. It is possible that some elements of the first set are not associated with any from the second. A special type of relation is that which associates with each member of the first set only one member of the second. Such a relation or correspondence is called a function from one set into the other. Thus a function is only a special type of relation or correspondence.

8.2 BASIC TERMINOLOGY

Definition: Let X and Y are any two sets. A relation f from X to Y is called a function if for every $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in f$.

Note:

1) A function f from X to Y is an assignment of exactly one element of Y to every element of X.

2) If $y=f(x)$, then y is called the image of x and x is called the pre-image of y under f.

3) The set X is called the domain of f denoted by *Dom* (f) and Y is called the co domain of f.

4) The set of the images of all elements of X is called the range of f denoted by *Ran* (f).

$$\text{Ran } (f) = \{f(x) : x \in \text{X}\}.$$

5) *Ran*(f) is a subset of Y.

Example 1: Let $X= \{x, y, z, w\}$ and $Y = \{1, 2, 3, 4\}$. If *Dom* $(f) = \{x, y, z, w\}$ and $f(x) = 2$, $f(y) = 4$, $f(z) = 1$, $f(w) = 2$, then the pictorial representation of f is

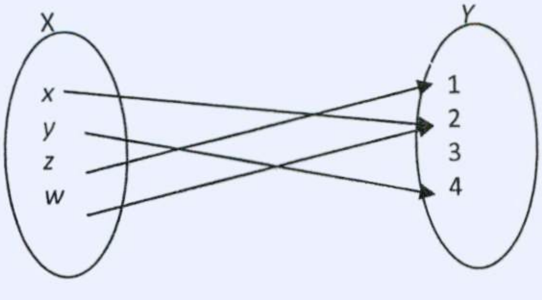


Fig 8.1: A function from A to B

Ran$(f) = \{ 1, 2 , 4 \}$ which is a subset of the co domain Y.

8.3 TYPES OF FUNCTIONS

Definition: A function f: $X \rightarrow Y$ is called one-to-one or injective if distinct elements of X are mapped into distinct elements of Y.

In other words, f is one-to-one if and only if

$f\ (x_1) \neq f\ (x_2\ )$ whenever $x_1 \neq x_2$ or equivalently

$f(x_1) = f(\ x_2)$ whenever $x_1{=}x_2$.

Example 2: The following function is one-to-one, since distinct elements of X are mapped into distinct elements of Y.

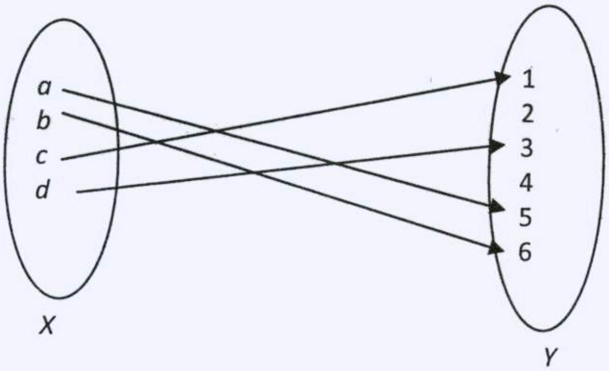


Fig 8.2: One-to-one function

The function in Example 1 is not one-to-one, since

$f\ (x) = f\ (w) = 2$ but $x \neq w$.

Definition: A function f: $X \rightarrow Y$ is called onto or surjective if the range $Ran(f) = Y$. Otherwise it is called into.

In other words, a function f is onto, iff for every element $y \in Y$, there is an element $x \in X$ such that $f\ (x) = y$.

Example 3 :

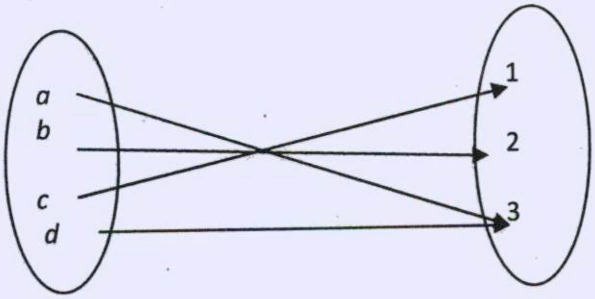


Fig 8.3: An onto function

The above two examples are not onto.

Definition: A function f: $X \rightarrow Y$ is called bijective or bijection or one-to-one correspondence if it is both one-to-one and onto.

Obviously if X and Y are finite such that f: $X \rightarrow Y$ is bijective, then X and Y have the same number of elements.

Example 4:

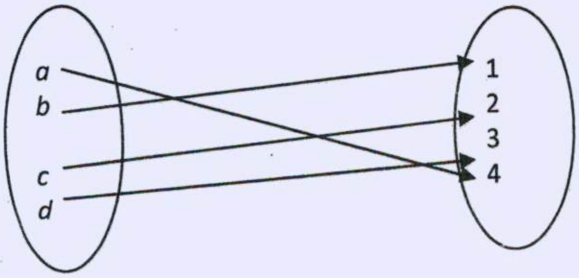


Fig 8.4: A bijective function

8.4 COMPOSITION OF FUNCTIONS

Definition: If f: $A \rightarrow B$ and g : $B \rightarrow C$ then the composition of f and g is a new function from A to C denoted by $g \circ f$ given by:

$(g^\circ f) (x) = g\{f (x)\}$ for all $x \in A$

Properties:

1. Composition of functions is associative.
   i.e., If f: $A \rightarrow B$, g: $B \rightarrow C$ and h: $C \rightarrow D$ are functions then $h \circ (g \circ f) = (h \circ g) \circ f$.

2. If f: $A \rightarrow B$ and $g : B \rightarrow C$ are functions, then $gof : A \rightarrow C$ is an injection; surjection or bijection accordingly as f and g are injections, surjections or bijections.

Identity Function:

The function f: $A \rightarrow A$ where $f(x) = x$, $x \in A$ is called the identity function on A. In other words, the identity function is the function that assigns each element of A to itself and is denoted by I_A or simply I. The function I_A is a bijection.

8.5 INVERSE OF A FUNCTION

Definition: If f: $A \rightarrow B$ and g: B→A, then the function g is called the inverse of the function f, if g o f = I_A and f o g =I_B.

In other words, if x€A and y€B then, the function g: B→A is called the inverse of f : A→B if x = g(y) whenever y = f(x).

The inverse of f is denoted by f^{-1}. Thus if f^{-1} is the inverse of f then $x = f^{-1}(y)$ where y = f(x).

Properties:

1. The inverse of a function f, if exists is unique.

2. The necessary and sufficient conditions for the function f : A→B to be invertible is that f is one- to-one and onto.

3. If f : A→B and g : B → C are invertible function, then $g\,o f$: A → C is also invertible and $(g \text{ o } f)^{-1} = f^{-1} \text{ o } g^{-1}$.

8.6 CHARACTERISTIC FUNCTION

Definition: If A is a subset of a universal set $\mho$, the characteristic function f_A of A is defined as the function from $\mho$ t o the set {0,1} such that

$$f_A(x) = \begin{cases} 1 & if\ x \in A \\ 0 & if\ x \notin A \end{cases}$$

Example 5: If $\mho$ = {1, 2, 3, 4, 5} and A ={2, 4} then

$f_A(1) = 0 = f_A(3) = f_A(5)$ and

$f_A(2) = f_A(4) = 1$ since 2, 4 ∈ A and 1,3,5 ∉ A

Properties of characteristic functions

1. If A is a subset of $\mho$ then $f_{\overline{A}}(x) = 1 - f_A(x)$ for all $x \varepsilon \mho$

Proof :

$$f_{\overline{A}}(x) = 1 \quad \Leftrightarrow \quad x \in \overline{A}$$

$$\Leftrightarrow x \notin A$$

$$\Leftrightarrow f_A(x) = 0$$

$$\Leftrightarrow 1 - f_A(x) = 1$$

$$\therefore \quad f_{\overline{A}}(x) = 1 - f_A(x), \quad for\ x \notin A.$$

$$f_{\overline{A}}(x) = 0 \quad \Leftrightarrow \quad x \notin \overline{A}$$

$$\Leftrightarrow x \varepsilon A$$

$$\Leftrightarrow f_A(x) = 1$$

$$\Leftrightarrow 1 - f_A(x) = 0$$

$$\therefore \quad f_{\overline{A}}(x) = 1 - f_A(x).$$

2. If A and B are any two subsets of $\mho$ then $f_{A \cap B}(x) = f_A(x) f_B(x), \ for\ all\ x \in \mho.$

Proof: $f_{A\cap B}(x) = 1 \quad \Leftrightarrow \quad x \in A \cap B.$

$$\Leftrightarrow x \in A \text{ and } x \in B$$

$$\Leftrightarrow \text{f}_A(\text{x}) = 1 \text{ and } \text{f}_B(\text{x}) = 1$$

$$\Leftrightarrow \text{f}_A(\text{x})\ \text{f}_B(\text{x}) = 1$$

$$\therefore f_{A\cap B}(x) = f_A(x) f_B(x),\ \textit{when } x \in A \cap B.$$

$$f_{A\cap B}(x) = 0 \ \Leftrightarrow\ x \notin A \cap B.$$

$$\Leftrightarrow \text{x} \notin \text{A and x} \notin \text{B}.$$

$$\Leftrightarrow \text{f}_A(\text{x}) = 0 \text{ and } \text{f}_B(\text{x}) = 0$$

$$\Leftrightarrow \text{f}_A(\text{x})\ \text{f}_B(\text{x}) = 0$$

$$\therefore f_{A\cap B}(x) = f_A(x) f_B(x),\ \textit{when } x \notin A \cap B.$$

Hence, $f_{A\cap B}(x) = f_A(x) f_B(x),\ \textit{for all } x \in \mho.$

3. If A and B are any two subsets of $\mho$ then

$$f_{A\cup B}(x) = f_A(x) + f_B(x) - f_{A\cap B}(x),\ \textit{where } x \in \mho.$$

Proof: $f_{A\cup B}(x) = 1 \ \Leftrightarrow\ x \in A \cup B.$

$$\Leftrightarrow \text{x} \in \text{A or x} \in \text{B}$$

$$\Leftrightarrow \text{f}_A(\text{x}) = 1 \text{ or } \text{f}_B(\text{x}) = 1$$

$$\Leftrightarrow f_A(x) + f_B(x) - f_A(x) f_B(x) = 1$$

$$\Leftrightarrow f_A(x) + f_B(x) - f_{A\cap B}(x) = 1$$

$$\therefore f_{A\cup B}(x) = f_A(x) + f_B(x) - f_{A\cap B}(x),\ \textit{where } x \in A \cup B.$$

$$f_{A\cup B}(x) = 0 \ \Leftrightarrow\ x \notin A \cup B.$$

$$\Leftrightarrow\ x \notin A \ \textit{or}\ x \notin B$$

$$\Leftrightarrow \text{f}_A(\text{x}) = 0 \text{ or } \text{f}_B(\text{x}) = 0.$$

$$\Leftrightarrow f_A(x) + f_B(x) - f_A(x) f_B(x) = 0$$

$$\Leftrightarrow f_A(x) + f_B(x) - f_{A\cap B}(x) = 0$$

$$\therefore f_{A\cup B}(x) = f_A(x) + f_B(x) - f_{A\cap B}(x),\ \textit{where } x \notin A \cup B.$$

$$\cdot\, f_{A\cup B}(x) = f_A(x) + f_B(x) - f_{A\cap B}(x),\ \textit{where } x \in \mho.$$

4. Using characteristic functions, prove that

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

Proof: $f_{(A \cup B)}(x) \cdot f_{(A\cup C)}(x) = [f_A(x)+f_B(x)- f_{A\cap B}]\ [f_A(x)+f_C(x)- f_{A\cap C}(x)]$

$= f_A(x)\, f_A(x)+ f_A(x)\, f_C(x) - f_A(x)\, f_{A\cap C}(x)+ f_B(x)\, f_A(x)+ f_B(x)\, f_C(x) - f_B(x)\, f_{A\cap C}(x)-$

$f_{A\cap B}(x)\, f_A(x)- f_{A\cap B}(x)\, f_C(x) + f_{A\cap B}(x)\, f_{A\cap C}(x)$

$= f_A(x) + f_{A\cap C}(x)- f_{A\cap C}(x)+f_{A\cap B}(x)+ f_{B\cap C}(x)- f_{A\cap B\cap C}(x)- f_{A\cap B}(x)- f_{A\cap B\cap C}(x)+ f_{A\cap B\cap C}(x)$

$= f_A(x)+ f_{B\cap C}(x)- f_{A\cap B\cap C}(x)$

$= f_{A\cup(B \cap C)}(x)$ by property (3)

Hence the result.

8.7 PERMUTATION FUNCTION

Definition: A bijective function from A to A is called a permutation function from A to A.

Definition: The set of all bijective functions from A to A is called the set of permutation functions from A to A.

8.8 HASHING FUNCTIONS

Definition: If *n* is the number of available memory locations and *k* is non-negative integer representing the key, the hashing function h(k) representing the address of the memory cell in which k is stored is defined as:

$$h(k) = k(\text{mod } n).$$

i.e., h(k) is simply the remainder when k is divided by n and it takes values from the set {0, 1, 2, …, n-1} known as address set.

A hashing function quite often maps different keys to the same address. In general a collision for a hash function occurs if $h(k_1)=h(k_2)$ but $k_1 \neq k_2$. It is necessary to provide storage space for and also a method of finding the colliding records. There are many techniques called collision resolution techniques for this purpose. The method called open addressing inserts the colliding record at the first empty location found.

8.9 RECURSIVE FUNCTIONS

~~**Definition:** A partial function f: X→Y is a rule which assigns to every element of X atmost one~~ element of Y.

Definition: A total function f: X→Y is a rule which assigns to every element of X a unique element of Y.

Example 6: The function $f(r) = +\sqrt{r}$ is a partial function since f(r) is defined only for the positive real numbers and not for negative numbers.

Note:

A partial function can be made a total function if we restrict the domain of the function only to those values for which function value is defined.

Definition: The initial functions over N are (i) zero function, (ii) successor function, (iii) projection function which are defined by

(i) Zero function Z defined by $Z(x) = 0$

(ii) Successor function S defined by $S(x) = x+1$

(iii) Projection function U^n_i defined by $U^n_i\ (x_1, x_2, ..., x_n) = x_i$

Note:

As $U_1'\ (x) = x$ for every x in N, U_1' is simply the identify function on N.

Definition: If $f_1, f_2, ..., f_k$ are partial functions of n variables and g is a partial function of k variables, then the composition of g with $f_1, f_2, ..., f_k$ is a partial function h of n variables defined by

$h(x_1, x_2, ..., x_n) = g(\ f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), ..., f_k(x_1, x_2, ..., x_n))$.

Example 7:

Let $f_1(x, y) = x+y$, $f_2(x, y) = 2x$, $f_3(x, y) = xy$ and $g(x, y, z) = x+y+z$.

Then,

$g(f_1(x, y), f_2(x, y), f_3(x, y)) = g(x+y, 2x, xy) = x+y+2x+xy$.

Thus the composition of g with f_1, f_2, f_3 is given by a function h defined by

$$h(x, y) = x+y+2x+xy.$$

Definition: The following operation which defines a function $f(x_1, x_2, ..., x_n, y)$ of n+1variables by using two other functions $g(x_1, x_2, ..., x_n)$ and $h(x_1, x_2, ..., x_n, y, z)$ of n and n+2 variables, respectively, is called recursion.

$$f(x_1, x_2, ..., x_n,0) = g(x_1, x_2, ..., x_n)$$

$$f(x_1, x_2, ..., x_n ,y+1) = h(x_1, x_2, ..., x_n, y, f(x_1, x_2, ..., x_n, y))$$

Definition: A function f is called primitive recursive if and only if it can be obtained from the initial functions by a finite number of operations of composition and recursion.

Definition: Let $g(x_1, x_2, ..., x_n, y)$ be a total function over N. g is said be a regular function if there exists some $y_0 \in N$ such that $g(x_1, x_2, ..., x_n, y_0) = 0$ for all n-tuples $(x_1, x_2, ..., x_n)$ in N^n.

Example 8: G(x, y) = min(x, y) is a regular function since g(x, 0) =0 for all x ∈ N.

Definition: A function $f(x_1, x_2, ..., x_n)$ is said to be defined from a total function $g(x_1, x_2, ..., x_{n,} y)$ by minimization if

$$f(x_1, x_2, ..., x_n) = \begin{cases} \mu_y(g(x_1, x_2, ..., x_n, y) = 0) & \textit{if there is such a y} \\ \quad\quad \textit{undefined} & \textit{otherwise} \end{cases}$$

where μ_y means the least y greater than or equal to zero.

Definition: A function is said to be recursive if and only if it can be obtained from the initial functions by a finite number of applications of the operations of composition, recursion and minimization over regular functions.

8.10 SOLVED PROBLEMS

1. Determine whether or not each of the following relations is a function with domain {1, 2, 3, 4}. If any relation is not a function, explain why?

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

b) R_2= {(1, 2), (2,3), (4,2)}

c) $R_3 = \{(1, 1), (2, 1), (3, 1), (4,1)\}$

d) $R_4 = \{(1, 4), (2, 3), (3,2), (4, 1)\}$

Solution:

a) R_1 is not a function since there are 2 pairs (3, 1) and (3, 3) which means that the image of the element 3 is not unique.

b) R_2 is not a function since there is no image for the element for the element 3 of the domain.

c) R_3 is a function even though the images of 1, 2, 3, 4 of the domain are one and the same element 1.

d) R_4 is a function.

2. If f: $R \to R$ and g: $R \to R$ are functions defined by $f(x) = x^2 + 3x + 1$ and $g(x) = 2x-3$, find $f \circ g$, $f \circ f$, $g \circ g$.

Solution:

$(f \circ g)(x) = f[g(x)] = f(2x-3)$

$= (2x-3)^2 + 3(2x-3) + 1$

$= 4x^2 - 6x + 1$

$(g \circ f)(x) = g[f(x)] = g[x^2 + 3x + 1]$

$= 2(x^2 + 3x + 1) - 3$

$= 2x^2 + 6x - 1.$

$(f \circ f)(x) = f[f(x)] = f[x^2 + 3x + 1]$

$= (x^2 + 3x + 1)^2 + 3(x^2 + 3x + 1) + 1$

$= x^4 + 6x^3 + 14x^2 + 15x + 5.$

$(g \circ g)(x) = g[g(x)] = g[2x-3]$

$= 2(2x-3) - 3$

$= 4x - 9$

3. Check whether the function $f(x) = x^2 - 11$ from R to R is 1- 1? Onto or both? Justify.

Solution. Given that $f(x) = x^2 - 11, \quad x \in R$

For 1-1:

Suppose, $\quad f(x) = f(y)$, then

$$x^2 - 11 = y^2 - 11$$

$$x^2 = y^2$$

$$x = \pm y$$

:. f is not 1-1

For onto: For all $y \in R$., we have to show that there exists x such that $f(x) = y$.

$$x^2 - 11 = y$$

$$x^2 = y + 11$$

$X = \sqrt{y+11}$ which is not in R for various values of y

:. f is not onto.

4. If S = {1, 2, 3, 4, 5} and if f, g, h: $S \rightarrow S$ are given by

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

$$g = \{(1, 3), (2, 5), (3, 1), (4, 2), (5, 4)\}$$

$$h = \{(1, 2), (2, 2), (3, 4), (4, 3), (5, 1)\}$$

a). Verify whether $f \circ g = g \circ f$

b). Verify whether f, g and h have inverses..

c). Find f^1 and g^{-1}.

d). Show that $(f \circ g)^{-1} = g^{-1} \circ f^{-1} \neq f^{-1} \circ g^{-1}$.

Solution:

a) $\quad (f \circ g)(1) = f[g(1)] = f(3) = 4$

$(f \circ g)(2) = f[g(2)] = f(5) = 3$

$(f \circ g)(3) = f[g(3)] = f(1) = 2$

$(f \circ g)(4) = f[g(4)] = f(2) = 1$

$(f \circ g)(5) = f[g(5)] = f(4) = 5$

$\therefore \quad f \circ g = \{(1, 4), (2, 3), (3, 2), (4, 1), (5, 5)\}$

$|||^{ly} \quad g \circ f = \{(1, 5), (2, 3), (3, 2), (4, 4), (5, 1)\}$

$\therefore \quad f \circ g \neq g \circ f.$

b) Both f and g are 1-1 and onto

$\therefore$ They are invertible

$$h(1) = h(2) = 2$$

But $1 \neq 2$

$\therefore$ h is not 1-1.

Also range (h) = $\{1, 2, 3, 4\} \neq S$.

$\therefore$ h is also not onto.

Hence, the inverse of h does not exist.

c) f^{-1} is obtained by reversing the elements in all the ordered pairs of f.

$$f^{-1} = \{(2, 1), (1, 2), (4, 3), (5, 4), (3, 5)\}.$$

It is easy to verify that

$$fof^{-1} = f^{-1}of = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\} = I.$$

Similarly, $g^{-1} = \{(3, 1), (5, 2), (1, 3), (2, 4), (4, 5)\}$.

d) From f o g,

$$(fog)^{-1} = \{(4, 1), (3, 2), (2, 3), (1, 4), (5, 5)\}.$$

From f^{-1} and g^{-1}

$$g^{-1}o\, f^{-1} = \{(2, 3), (1, 4), (4, 1), (5, 5), (3, 2)\}.$$

But, $f^{-1}o\, g^{-1} = \{ (3, 2), (5, 1), (1, 5), (2, 3), (4, 4)\}$.

Therefore, $(f \circ g)^{-1} = g^{-1} \circ f^{-1} \neq f^{-1} \circ g^{-1}$.

5. Show that the function f: R → R defined by $f(x) = \frac{x}{x+4}$ is one-to-one and onto and hence find the inverse.

Solution: Given that f: R→ R is defined as $f(x) = \frac{x}{x+4}$

f is one-one:

Let f(x) = f(y) then $x/(x+4) = y/(y+4)$

$$x(y+4) = y(x+4)$$

i. e. $4x = 4y$

i. e. $x = y$.

Therefore, f is one-to-one

f is onto: if for every y □ R there is a pre- image x □ R , such that f(x) = y .

i.e, $y = f(x) = \frac{x}{x+4}$

$$y(x+4) = x$$

$$xy + 4y = x$$

$$x(y - 1) = -4y$$

$$x = \frac{4y}{1-y}$$

Therefore, $f^{-1}(x) = \frac{4x}{1-x}$ is the inverse function.

6. Find all permutation of A = {1, 2, 3}.

Solution: The permutation of A are

$$P_1=\begin{bmatrix}1 & 2 & 3\\1 & 2 & 3\end{bmatrix} \quad P_2=\begin{bmatrix}1 & 2 & 3\\1 & 3 & 2\end{bmatrix} \quad P_3=\begin{bmatrix}1 & 2 & 3\\2 & 1 & 3\end{bmatrix}$$

$$P_4=\begin{bmatrix}1 & 2 & 3\\3 & 2 & 1\end{bmatrix} \quad P_5=\begin{bmatrix}1 & 2 & 3\\2 & 3 & 1\end{bmatrix} \quad P_6=\begin{bmatrix}1 & 2 & 3\\3 & 1 & 2\end{bmatrix}$$

7. Let A = {1, 2, 3, 4}, f : A → A be defined by f(1) = 2, f(2) = 1, f(3) = 4, f(4) = 3. Write this in permutation notation.

Solution:

$$\begin{bmatrix}1 & 2 & 3 & 4\\2 & 1 & 4 & 3\end{bmatrix}$$

8. Find the inverse of permutation $\begin{bmatrix}1 & 2 & 3\\2 & 3 & 1\end{bmatrix}$

Solution:

Inverse permutation is $\begin{bmatrix}1 & 2 & 3\\3 & 1 & 2\end{bmatrix}$

9. If $p_1=\begin{bmatrix}1 & 2 & 3\\2 & 1 & 3\end{bmatrix}$, $p_2=\begin{bmatrix}1 & 2 & 3\\3 & 1 & 2\end{bmatrix}$, find $p_2 \text{ o } p_1$.

Solution:

$$\begin{array}{cccc} & 1 & 2 & 3 \\ p_1: & \downarrow & \downarrow & \downarrow \\ & 2 & 1 & 3 \\ & \downarrow & \downarrow & \downarrow \\ p_2: & 1 & 3 & 2 \end{array}$$

Hence, $p_1 \text{ o } p_2 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$.

10. A company has 10,000 customers. Each customer id is an eight digit number. The hashing function takes the first four digits as one number and the last four digits as another number, add them and then applies (mod 64) function to assign an address to the customer record. Determine the address assigned to the following numbers.

(a) 27266036 (b) 35674690

Solution:

(a) 27266036

$$2726 + 6036 = 8762$$

$$h(8762) = 8762 \pmod{64}$$

$$\therefore \; h(8762)=58.$$

The number 27266036 is stored in the address 58.

(b) 35674690

$$3567 + 4690 = 8257$$

$$h(8257) = 8257 \pmod{64}$$

$$\therefore \; h(8257)=1.$$

The number 35674690 is stored in the address 1.

11. Compute the addresses of 6 memory cells in which the integers 23, 38, 46, 55, 67 and 71 are to be stored, assuming there are 6 records in the file.

Solution:

Let n = 7, then the address of the memory cells are given by the hashing function h(k) = k(mod 7).

The address set is {0, 1, 2, 3, 4, 5, 6}.

When k= 23, 38, 46, 55 the value of h(k)= 2, 3, 4, 6 respectively. The integers 23, 38, 46 and 55 are stored in the memory cells with addresses 2, 3, 4, 6.

h(k)	0	1	2	3	4	5	6
K	71	-	23	38	46	67	55

The next integer to be stored is 67. When k = 67, h(k)= 4.

i.e., 67 must be stored in the cell with address 4. But this cell with address 4 has been already occupied by 46. So, a collision has occurred.

By collision resolution policy, the first empty cell that follows the already occupied cell is used to store the current value of k.

The first unoccupied cell that follows the memory cell numbered as 4 is that with address 5. The integer 67 is thus stored in this cell. The last integer 71 is then stored in the cell with address 0. The cell with address 1 will remain as an unoccupied cell.

12. For the hashing function h(x) = x (mod 17) show how the following data would be interested in the order in given initially empty cells. Use the collision resolution policy of inserting the number in the next higher unoccupied cell. Cells are indexed from 0 to 16.

Given data: 714, 681, 26, 373, 775, 906, 509, 2032, 42, 4,136, 1028

Solution:

h(k)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k	7 1 4	5 0 9	6 3 1	1 3 6	4	9 0 6	-	-	4 2	2 6	7 7 5	2 0 3 2	1 0 2 8	-	-	-	3 7 3

0 = 714(mod 17)

2 = 631(mod 17)

9 = 26(mod 17)

10 =775 (mod 17)

5 = 906 (mod 17)

16 = 509(mod 17)

8 =42 (mod 17)

4 = 4(mod 17)

0 = 136(mod 17)

$16 = 373(\text{mod } 17)$ $\quad 9 = 2032(\text{mod } 17)$ $\quad 8 = 1028(\text{mod } 17)$

13. For the hashing function $h(x) = x^2(\text{mod } 11)$ show how the following data would be inserted in the order given initially empty cells. Use the collision resolution policy of inserting the number in the next higher occupied cell. All cells are indexed from 0 to 10.

Data: 53, 13, 281, 743, 377, 20, 10, 796.

Solution:

$4 = 53^2(\text{mod } 11)$ $\quad 3 = 281^2(\text{mod } 11)$ $\quad 9 = 377^2(\text{mod } 11)$

$1 = 10^2(\text{mod } 11)$ $\quad 4 = 13^2(\text{mod } 11)$ $\quad 3 = 743^2(\text{mod } 11)$

$4 = 20^2(\text{mod } 11)$ $\quad 5 = 796^2(\text{mod } 11)$

h(x)	0	1	2	3	4	5	6	7	8	9	10
x^2	-	10^2	-	281^2	53^2	13^2	743^2	796^2	-	377^2	20^2

14. Show that $f(x, y) = x+y$, $x, y \in N$ is primitive recursive.

Solution:

Note that $x+(y+1) = (x+y)+1$ (1)

L.H.S. of (1) can be expressed in terms of f. R.H.S. of (1) can be expressed in terms of the successor function S.

That is $f(x, y+1)=f(x, y)+1 =S(f(x, y))$.

Also, $f(x, 0) = x$.

Define $f(x, y)$ as

$$f(x, 0) = x = U_1'(x)$$

$$f(x, y+1) = S(U_3^3(x, y, f(x, y)).$$

Now U_1^1, U_3^3, S are initial functions.

Thus, f is got by applying recursion for the functions U_1^1, U_3^3 and S. Hence f is primitive recursive.

15. Show that $f(x, y) = x*y$ is a primitive recursive function.

Solution: $f(x,0) = x*0 = 0$ (1)

$f(x, y+1) = x*(y+1) = (x*y)+x = f(x, y) + x$ (2)

Comparing (1) & (2) with definition we can write

$f(x, 0) = z(x)$ (3)

$f(x, y+1) = f_1(U_3^3(x, y, f(x, y)), U_1^3(x, y, f(x, y))$ (4)

where $f_1(x, y) = x+y$ which is primitive recursive.

Taking g = Z and h defined by $h(x, y, z) = f_1(U_3^3(x, y, z), U_1^3(x, y, z))$, we see that (3), (4) define f_1 by recursion. As Z is an initial function of g = Z is primitive recursive.

As h is defined using composition of f_1, which is primitive recursive, $U^3{}_3$, $U^1{}_3$ which are initial functions, h is primitive recursive. Hence f_2, obtained from g and h, using recursion is primitive recursive.

16. Show that $f(x, y) = x^y$ is primitive recursive .

Solution:

Let $f(x, 0)= x^0 = 1$

$f(x, y+1) = x^{y+1}+1 = x * x^y = x * f(x, y)$

Define $f(x, 0) = 1$

$f(x, y+1) = x* f(x, y)$

$= U_1^3((x, y, f(x, y)) * U_3^3 (x, y , f(x, y))$

Now $f(x, 0) = S(Z(x))$ (S o Z is primitive recursive)

$f(x, y+1) = h(x, y, f(x, y))$

where $h(x, y, z) = U_1^3(x, y, z) * U_3^3(x, y, z)$.

U_1^3, U_3^3 are initial functions and $f_2(x, y) = x*y$ is primitive recursive, we see that f is defined by applying recursion to primitive recursive functions S(z(x)) and h. hence f is primitive recursive.

8.11 SUMMARY

Definition: Let *X* and *Y* are any two sets. A relation *f* from *X* to *Y* is called a function if for every $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in f$.

Definition: A function *f*: *X* →*Y* is called one-to-one or injective if distinct elements of *X* are mapped into distinct elements of *Y*.

Definition: A function f: $X \rightarrow Y$ is called onto or surjective if the range $Ran(f) = Y$.

Definition: If f: $A \rightarrow B$ and g: $B \rightarrow C$ then the composition of f and g is a new function from A to C denoted by $g\,^\circ f$ given by:

$$(g^\circ f)\,(x) = g\{f\,(x)\} \text{ for all } x \in A$$

Definition: If f: $A \rightarrow B$ and g: B→A, then the function g is called the inverse of the function f, if g o f = I_A and f o g =I_B.

Definition: If A is a subset of a universal setꓴ, the characteristic function f_A of A is defined as the function from ꓴ t o the set {0,1} such that

$$f_A(x) = \begin{cases} 1 & if \;\; x \in A \\ 0 & if \;\; x \notin A \end{cases}$$

Definition: The set of all bijective functions from A to A is called the set of permutation functions from A to A.

Definition: If n is the number of available memory locations and k is non-negative integer representing the key, the hashing function h(k) representing the address of the memory cell in which k is stored is defined as:

$$h(k) = k(\text{mod } n).$$

Definition: A function f is called primitive recursive iff it can be obtained from the initial functions by a finite number of operations of composition and recursion.

Definition: A function is said to be recursive iff it can be obtained from the initial functions by a finite number of applications of the operations of composition, recursion and minimization over regular functions.

8.12 KEYWORDS

Function, one-one, onto, inverse, composite function, hashing function, recursion, permutation.

8.13 QUESTIONS

1. Let A = {a, b, c}, B = {x, y, z}. Determine whether or not each relation below is a function from A to B. Find the range if the relation is a function.

   (i) f = {(a, y), (c, z)}

   (ii) g = {(a, y),(b, z),(c, x),(c, z)}

2. State which of the following are injections, surjections or bijections from R into R, where R is the set of all real numbers.

   i) $f(x) = -2x$ ii) $g(x) = x^2 - 1$.

3. Let X={1, 2, 3, 4} and a mapping f:→X X be given by f={(1, 2), (2, 3), (3, 4), (4, 1)}. Form the composite functions f^2, f^3, f^4.

4. If A = {1,2,3} and f,g,h are functions from A to A given by f = [(1,2), (2,3), (3,1)}, g={(1,2),(2,1), (3,3)} and h= {(1,1), (2,2), (3,1)}, find (i)fog, (ii) fohog, (iii) gof.

5. Show that the function $f(x) =x^3$ and $g(x) = x^{1/3}$ for $x \in R$ are inverse of each other.

6. Show that the function f: R – {3} → R –{1} given by $f(x)= \frac{x-2}{x-3}$ is a bijection and find its inverse.

7. If A and B are any two subsets of $\mathcal{U}$ then prove that $f_{A-B}(x)= f_A(x)[1-f_B(x)]$

8. Using characteristic function, prove that

   $f_{A\cap B}(x) = f_A(x) f_B(x),$ *for all* $x \in \mathcal{U}$.

9. Let A={1,2,3,4,5,6} and $p_1= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{bmatrix}$, $p_2= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{bmatrix}$,

$p_3= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 5 & 4 & 1 \end{bmatrix}$, find (i) p_2^{-1}, (iii) $p_1 \circ (p_3 \circ p_2^{-1})$,

10. For each hashing function, show how the corresponding data given would be inserted in the order given in initially empty cells. Use the usual collision resolution policy to resolve collision.

(i) $H(x)=(x^2+x)(\text{mod}17)$; cells indexed 0 to 16; data: 714, 631, 26, 373, 775, 906, 509, 2032, 42, 4, 136, 1028.

(ii) $H(x) = x+5(\text{mod } 11)$; cells indexed 0 to 10; data: 53, 13, 281, 743, 377, 20, 10, 796.

11. Show that the following functions over N are primitive recursive

   (i) Constant function over N.

(ii) Zero test function.

(iii) Odd and even parity function.

8.14 REFERENCES

1. Discrete mathematics, by P. Geetha (Scitech publications).

2. Discrete mathematics for computer science, by Kolman, Busby and Ross, PHI publications.

3. Discrete mathematical structures with applications to computer science, by Tremblay and Manohar (McGraw-Hill publications).

MODULE 3: Graph Theory

UNITS: 9 to 12

UNIT -9: GRAPH THEORY - BASICS

Structure

9.0 Objectives

9.1 Definition and representation

9.2 Applications of graphs

9.3 Types of graph

9.4 Matrix representation

9.5 Summary

9.6 Keywords

9.7 Questions for self study

9.8 References

9.0 OBJECTIVES

After studying this unit, you will be able to

- ✓ Define graph and its components, vertices and edges
- ✓ Understand and appreciate some important applications of graphs
- ✓ Learn about various types of graphs: simple, complete, regular, null
- ✓ Represent a graph by a matrix

9.1 DEFINITION AND REPRESENTATION

Here we discuss the definition of a graph and representation of a graph.

Definition

A graph G = (V, E) consists of a set of vertices V = {v_1, v_2, …} and edges E = {e_1, e_2, …}. Each edge e_k is denoted by a pair of vertices (v_i, v_j). These vertices v_i, v_j are end vertices of edge e_k.

Representation

Most common representation is a diagram such as the one given in figure 9.1.

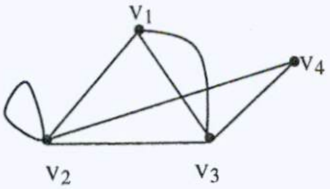


Fig 9.1: A graph

There are 4 vertices (shown as dots) v_1, v_2, v_3, v_4 and 7 edges (shown in the figure as lines/curves/loops). Observe there are 2 edges connecting v_1 and v_3 and these edges are called parallel edges. Also there is an edge that begins and ends at v_2. This is called self loop. You may observe that edge connecting v_2 and v_4 intersects two other edges but not every intersection of edges should be a vertex. Such intersecting edges should be thought of as being in different planes and thus have no common points. Note that vertices are also referred to as nodes, points, junctions and edges can also be called as arcs, branches, lines.

It should be noted that in drawing a graph, it is immaterial whether the lines are drawn straight or curved, long or short. What is important is incidence between the edges and vertices. For example the graphs in figures 9.2 and 9.2a are the same, because the incidence between edges and vertices are the same. Also the graphs in figures 9.3 and 9,3a are the same.

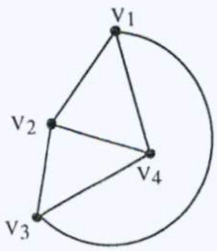


Fig 9.2

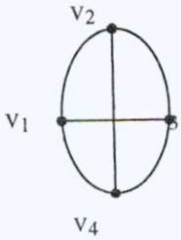


Fig 9.2a

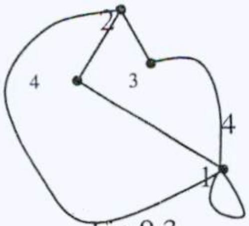


Fig 9.3

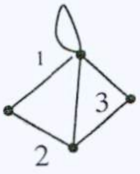


Fig 9.3a

Same graphs differently drawn

In the figures 9.2 and 9.3 we have graphs with 4 vertices v_1, v_2, v_3, v_4 and 6 edges (v_1, v_2), (v_1, v_4), (v_1, v_3), (v_2, v_4), (v_2, v_3), (v_3, v_4).

9.2 APPLICATIONS OF GRAPHS

Application fields are diverse. Here we mention some key fields such as physical, social, engineering, computer science where graphs are used commonly.

9.2.1 Origin of graph theory

Königsberg bridge problem:

Figure 9.4 below shows two islands C and D formed by the river Pregel (in Königsberg-present name Kaliningrad, Russia) and the seven bridges connecting the two banks A and B. An interesting question here is whether or not a person can start from a land area (A, B, C or D) and walk over all the bridges exactly once and return to the starting place. Such a tour is called Euler line.

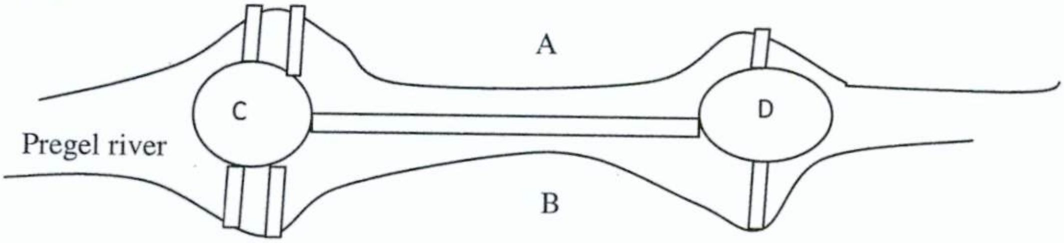


Fig 9.4: Bridges (shown as rectangles) on the river Pregel

Euler (a renowned mathematician of 18th century) published his first ever paper in the then new subject 'Graph Theory' and proved that above tour is not possible. Euler converted this problem to a simple graph where each land area is a vertex and bridges are edges connecting the vertices. The graph of Königsberg bridge problem is given in figure 9.5.

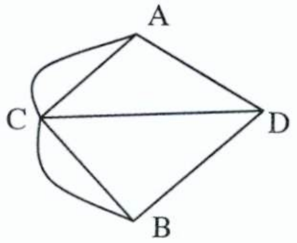


Fig 9.5: Graph of Königsberg bridge problem

Königsberg bridge problem is the same as drawing the graph in figure 9.5without lifting the pen and without retracing any edge.

9.2.2 Utilities problem (application for physical)

There are 3 houses H1, H2, H3 and 3 utilities Water (W), Electricity (E) and Gas (G) are to be provided to each of the house by means of conduits. Is it possible to make such connections without any crossovers of the conduits?

This problem can be represented by the graph below (figure 9.6).

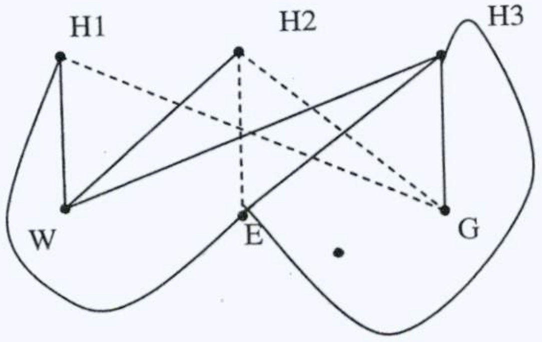
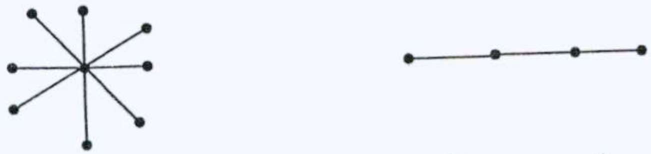


Fig 9.6: Graph of utilities problem

In the graph above, houses, utilities are vertices and conduits are edges. Note that in the graph above, some crossovers are unavoidable. The crossovers are shown in dotted lines.

9.2.3 Network problem (application in the field of engineering/computer science)

The interconnection of computing systems (LAN, WAN) can be represented using a graph. Nodes (vertices) are systems and edges are connections between systems. Some special types of connections are shown below in figure 9.7.



Star connection

Bus connection

Fig 9.7: Interconnections of computing systems

When a connection fails, it is equivalent of removal of an edge. Strength of a network, connectivity between two systems etc can be studied using concepts of graph theory.

9.2.4 Club meet problem (Social application of graph theory)

Six members of club meet daily for lunch together at a round table. They decide to sit with new neighbor during each day. How many days can this arrangement last?

Equivalent graph: Vertex can be used to represent members and edges represent neighbor relationship. Figure 9.8 shows two such seating arrangements.

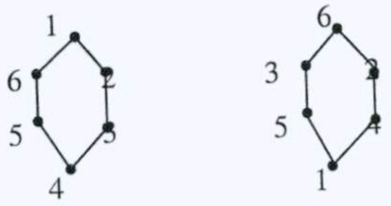


Fig 9.8: Two seating arrangements with different neighbors

The number of such arrangements can be found using by graph theoretic considerations.

9.3 TYPES OF GRAPHS

Simple graph is one which does not have any self loop or parallel edges. Referring to figure 9.1 if the self loop connecting v_2 to v_2 and one of the edges connecting v_1 and v_3 are removed it becomes simple graph. The graph after deletion of the two edges is shown in figure 9.9.

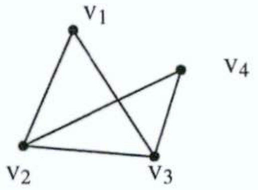


Fig 9.9: A simple graph

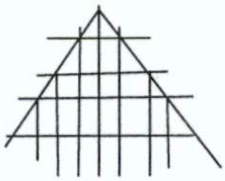


Fig 9.10: An infinite graph

So far we discussed graphs having finite number of vertices and edges (called ***finite graph***). A graph can also have infinite number of vertices and edges which is then called ***infinite graph***. Figure 9.10 above shows portion of one such infinite graph. Assume every intersection of lines to be vertices.

A simple graph with edges connecting every pair of vertices is called ***complete graph***. Figure 9.11is an illustration of a complete graph of 4 vertices.

If an edge e_k connects v_i to v_j we say that e_k is ***incident*** on v_i and v_j. The ***degree of a vertex*** is the number of edges incident on it. Note the in case of complete graph of *n* vertices the degree of every vertex is *n*-1. Figure 9.12 shows a graph and the degree of each vertex indicated.

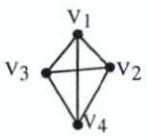


Fig 9.12: Complete graph 4 vertices. Degree of every vertex is 3

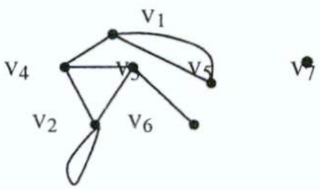


Fig 9.13: Degrees of vertices 1 to 7 in order are 3, 4 (self loops are incident twice), 3, 3, 2, 1, 0

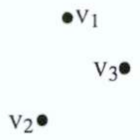


Fig 9.14: Null graph of of 3 vertices

A vertex having no edge is called ***isolated vertex***. In figure 9.13 v_7 is an isolated vertex. Isolated vertex has degree 0. A vertex of degree one is called ***pendant vertex***. In figure 9.13 v_5 is a pendant vertex.

Number of vertices is ***order of a graph*** and the number of edges is its ***size***. For example the order and size of graphs in figures 9.12, 9.13 are 4, 6 and 7, 8 respectively.

A graph with no edges is a ***null graph***. This graph has only vertices and no edges. All vertices are isolated vertices. Figure 9.14 above is a null graph of three vertices.

Adjacent edges are those which are incident on a common vertex. For example in figures 9.12 and 9.13 (v_1, v_2), (v_1, v_3) and (v_2, v_3), (v_3, v_6) are adjacent edges.

Vertices are said to be ***adjacent*** if they are end vertices of an edge. For example in figures 9.12 and 9.13 vertices v_2, v_4 and v_1, v_5 are adjacent.

A graph with some parallel edges is called ***multi-graph***. Graphs in figures 9.1, 9.5 and 9.13 are multi-graphs.

A graph is said to be ***regular graph*** if all vertices are of same degree. Figures 9.15 and 9.16 below illustrate regular and not a regular graph.

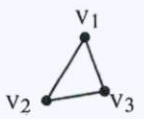


Fig 9.15: 3 vertex regular graph

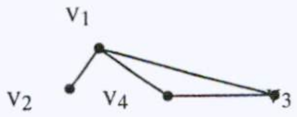


Fig 9.16: Not regular

A graph with weights attached to edges is said to be ***weighted graph***. Graph below (figure 9.17) is a weighted graph.

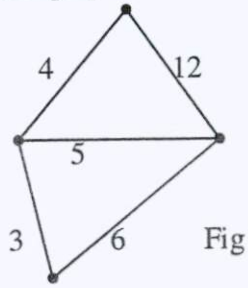


Fig 9.17: Weighted graph

Graphs discussed so far contain no direction for edges. Such graphs are called are ***undirected*** graphs. In these graphs edges (1,2) and (2,1) are one and the same edge. ***Digraph*** (or ***directed graph***) is a graph where edges have directions. In a digraph edge (1,2) is an edge with initial vertex 1 and terminal vertex 2. Edges (1,2) and (2,1) are different in digraphs. If both (1,2) and (2,1) are present in a digraph, then it can be replaced by an undirected edge (1,2). Graphs can have directed and undirected edges. Such graphs are ***mixed graphs***. Figure 9.18 shows diagrams of digraph and mixed graph.

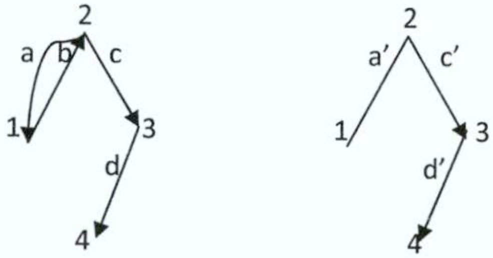


Fig 9.18: Digraph and equivalent mixed graph

Note: Most discussions in this module are focused on undirected graphs. Unless otherwise mentioned, by graph we mean undirected graph.

We close the section by stating frequently used yet very simple results.

Theorem 9.1

The sum of the degrees of all vertices is twice the number of edges.

Proof:

Each edge is incident on two vertices. Hence each edge contributes to two degrees. If total number of edges is e, then the sum of all degrees is $2e$.

For example consider the graph in figure 9.17. Total number of edges is 5. The degrees of vertices of the graph are 2,3,2,3 (beginning from top and in clockwise direction) their sum being 2+3+2+3=10 = 2*number of edges.

Considering the graph in figure 9.13, the number of edges is 8. The degrees of vertices v_1 to v_7 in order are 3, 4, 3, 3, 2, 1, 0. The sum of degrees is 16 which is 2*8=2*number of edges.

Theorem 9.2

The number of vertices of odd degree in a graph is always even.

Proof:

Suppose that d(x) denotes the degree of the vertex x in the graph. Group the vertices into even and odd degrees. Then Σ_{all} d(x) = Σ_{even} d(y) +Σ_{odd} d(z). From previous theorem left hand side of the equation is an even number. Also first term on the right hand side is even. Hence the second summation on the right hand side should also be even. But each d(z) in the summation is odd. Hence total number of terms in the summation, Σ_{odd} d(z), should be even to make the sum even. Therefore the number of odd degree vertices is even.

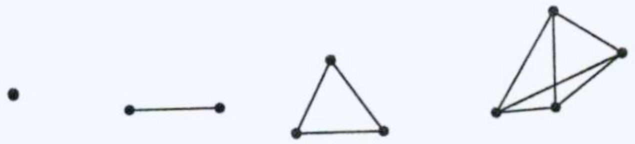
Theorem 9.3

Maximum number of edges in a simple graph of *n* vertices is $n(n-1)/2$

Proof:

You may observe that a simple graph with maximum number of edges is nothing but a complete graph.

Let us draw simple graphs of 1, 2 3, 4 vertices, with maximum number of edges.



The maximum number of edges in the these graphs of 1, 2, 3, 4 vertices are 0, 1, 2, 6 … Thus in an *n* vertex graph the maximum number of edges is $n(n-1)/2$. (This is nothing but the n^{th} term of the series 0, 1, 2, 6 …)

9.4 MATRIX REPRESENTATION

Although pictorial representation is simple and convenient, other representations are better for computer processing. Graphs can also be represented in the form of a matrix. Many derivations are easy with matrix representation. There are two types of matrix representation. ***Incidence matrix or vertex edge incidence matrix*** is used to represent undirected graphs with no self loops. This is vertex by edge binary matrix. The number of rows is same as number of vertices and number of columns is same as number of edges. Given below are an undirected graph and its incidence matrix.

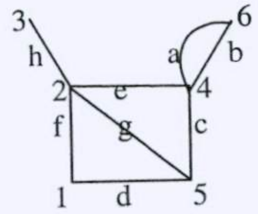


Fig 9.19: An undirected graph G

$$\begin{array}{c|cccccccc} & a & b & c & d & e & f & g & h \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 4 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 5 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 6 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

Incidence matrix A(G)

Some observations on incident matrix:

1. Each column has two 1s, since each edge is incident on two vertices. (No incident matrix representation for graphs with self loops). Observe that column 1 has two ones at rows 4 and 6. (edge a is incident on vertices 4 and 6)
2. The number of 1s in a row is degree of the vertex. Observe that row has two 1s at column d and f. (edges d and f are incident on vertex 1)
3. A row with only 0s represent isolated vertex.
4. Parallel edges produce two identical columns. (columns 1 and 2 corresponding to parallel edges a and b are identical)

As an alternative to incidence matrix, it is sometimes more convenient to use another representation called ***adjacency matrix or connection matrix***. Adjacency matrix can be used for undirected graphs and digraphs. This cannot represent graphs with parallel edges. Self loops can be represented. It is vertex by vertex matrix and also binary like incidence matrix. Adjacency matrix X is defined thus: $x_{ij} = 1$ if there is an edge from i to j and this entry is 0 in absence of the edge. The adjacency matrices corresponding to the graphs in figure 9.3 (undirected graph) and 9.18 (mixed graph) are given below.

$$\begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 0 & 1 & 1 \\ 3 & 1 & 1 & 0 & 0 \\ 4 & 1 & 1 & 0 & 0 \end{array}$$

Adjacency matrix of graph in figure 9.3

$$\begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 \end{array}$$

Adjacency matrix of graph in figure 9.18

Observe that adjacency matrix of undirected graph is symmetric. Entries in diagonal position are 1 only if there is a self loop. Degree of a vertex is number of 1s in the row or column. For example, number of 1s in row 2 of matrix (on the left) is 3 (= degree of vertex 2 in the graph of figure 9.3). In case of self loop the degree is number of 1s in the row plus one. (Degree of vertex 1 is 5 = number of 1s in row 1 +1).

9.5 SUMMARY

In this unit an important concept called graph is introduced. Some interesting applications are discussed here. Diagrammatic representation of a graph, types of graphs and matrix representation of graphs also are discussed.

9.6 KEYWORDS

Diagrammatic representation of graphs, graphs-various types, incidence matrix, adjacency matrix

9.7 QUESTIONS

1. Draw a graph with 6 vertices having self loops, parallel edges, pendant vertices, isolated vertices. Indicate each of these.
2. Mention some applications of graph theory.
3. Describe the origin of graph theory.
4. Define complete graph, simple graph, and regular graph. Illustrate each one of these. Also provide illustration for not complete, not simple and not regular graph. Give reasons for each of the illustration.
5. What do you mean by infinite, null and weighted graphs?
6. Find the degree of each of the vertices in the illustrations of problem 2.
7. Find order and size of the graph for every illustration of problem 2.
8. Define adjacency of vertices and edges.
9. Draw digraphs and mixed graphs with 3, 4, 5 vertices.
10. Find incidence and adjacency of all graphs (whenever possible) you have drawn.

9.8 REFERENCES

1. Narsingh Deo, Graph Theory with applications to Engineering and Computer Science, PHI
2. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL
3. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
4. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

UNIT - 10: PATHS AND CIRCUITS

Structure

10.0 Objectives

10.1 Isomorphism

10.2 Sub-graphs

10.3 Walks, paths and circuits

10.4 Connected graphs and components

10.5 Euler graphs

10.6 Hamiltonian circuits and paths

10.7 Summary

10.8 Key words

10.9 Practice problems

10.10 References

10.0 OBJECTIVES

After studying this unit, you should be able to

- ✓ Solve some very interesting and practical problems
- ✓ Discuss isomorphism, sub-graphs, connectivity and components
- ✓ Discuss matrix form for these
- ✓ To learn concepts like path, walk, circuit, Euler graph
- ✓ Discuss Hamiltonian paths, circuits and travelling salesman problem - an important application of graph theory

10.1 ISOMORPHISM

Isomorphism is similar to the concept of 'congruent' or 'equivalent' in geometry. Two graphs G and G' are called isomorphic if there is a one to one correspondence between their vertices and their edges preserve incidence relationship. In other words if an edge e is incident on vertices v_1 and v_2 in G, then the corresponding edge e' in G' must be incident on the vertices v_1' and v_2' that correspond to v_1 and v_2. Given below (figure 10.1) is a pair of isomorphic graphs.

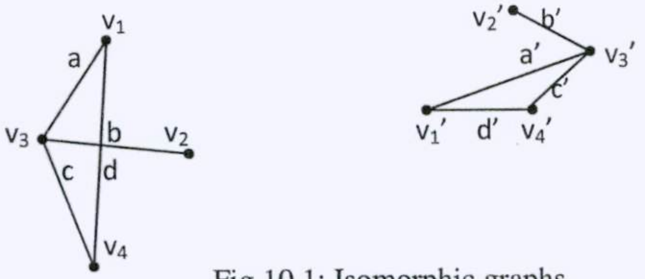


Fig 10.1: Isomorphic graphs

The correspondence between vertices and edges in the graphs of figure 10.1 are as follows: Vertices v_1, v_2, v_3, v_4 correspond to v_1', v_2', v_3', v_4'and edges a, b, c, d correspond to a', b', c', d'.

Given below are more graphs in figures 10.2 and 10.3.

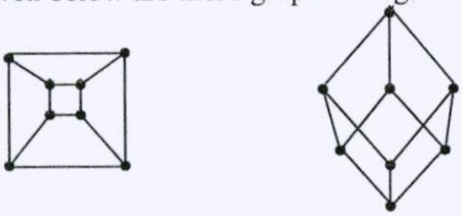


Fig 10.2: Isomorphic graphs

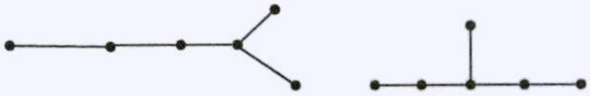


Fig 10.3: Not isomorphic graphs

Except for relabeling of vertices and edges, isomorphic graphs are the same, perhaps drawn differently. It is not easy to discover isomorphism. Definition of isomorphism is as follows: Isomorphic graphs must have: (i) The same number of vertices (ii) The same number of edges (iii) An equal number of vertices with a given degree. However these are not sufficient. For example the graphs in figure 10.3 satisfy all these and yet not isomorphic. This is because there are two pendant vertices that are adjacent to a vertex of degree three in the graph on the left whereas there is only one pendant vertex adjacent to the vertex of degree 3 in the graph to the right. Hence these graphs are not isomorphic.

We now discuss the concept of isomorphism with the aid of matrix representation of graphs. Graphs G and G' are isomorphic if and only if their incidence matrices A(G) and A(G') differ by permutations of rows and columns.

As an example let us consider the following graphs of 4 vertices.

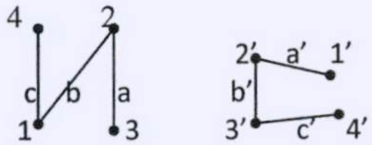


Fig 10.4: Isomorphic graphs

These are isomorphic with correspondence as follows: Vertices 1,2,3,4 correspond to 3', 2', 1', 4'. Edges a, b, c correspond to a', b', c'. Let us examine their incidence matrices, which are given below.

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \qquad \begin{array}{c} \\ 1' \\ 2' \\ 3' \\ 4' \end{array}\begin{array}{c} \begin{array}{ccc} a' & b' & c' \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

Observe that after exchange of rows 1' and 3' we see that matrix on right is same as that on the left. Hence G and G' are isomorphic.

10.2 SUBGRAPHS

A graph g is said to be a sub-graph of a graph G if all the vertices and all the edges of g are present in G. A graph of 6 vertices and its sub-graph with 3 vertices are given in figure 2.4.

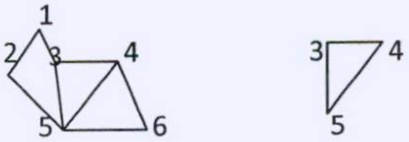


Fig 10.5: Graph and a sub-graph

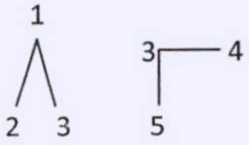


Fig 10.6: Edge disjoint sub-graphs

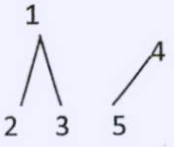


Fig 10.7: Vertex disjoint sub-graphs

The concept of sub-graph is similar to that of subset. Sometimes the symbol "⊂" ($g \subset G$) is used instead of the word sub-graph.

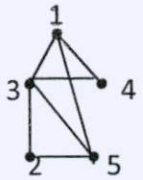
The following observations can be made immediately and without any difficulty.

1. Every graph is its own sub-graph.
2. A sub-graph of a sub-graph of G is also a sub-graph of G.

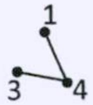
3. A single vertex in a graph is a sub-graph.
4. A single edge together with its end vertices is a sub-graph.

Two or more sub-graphs that do not have any edge in common are called edge disjoint sub-graphs. However they can have common vertices. Refer figures 2.4 and 2.5 for such examples.

Coming to matrix form, g is a sub-graph of G if A(g) is a sub-matrix of A(G). Sub-matrix is one which is obtained after deletion of some rows and columns. As an example let us consider the following graph and its sub-graph.



Graph G



Sub-graph g

$$\begin{array}{c|ccccccc} & a & b & c & d & e & f & g \\ \hline 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 4 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \qquad \begin{array}{c|cc} & b & f \\ \hline 1 & 1 & 0 \\ 3 & 0 & 1 \\ 4 & 1 & 1 \end{array}$$

Incidence matrices of G and g

In the graph G assume that a, b, c, d, e, f, g are the edges (1,3), (1,4), (1,5), (2,3), (2,5), (3,4), (3,5) respectively.

It is obvious that second (on the right) matrix is a sub-matrix of first one on the left.

10.3 WALKS, PATHS AND CIRCUITS

Walk is an alternating sequence of vertices and edges beginning and ending with vertices. Also each edge in the sequence is such that its beginning vertex is the ending vertex of the previous edge. No edge can appear more than once in a walk. Length of the walk is the number of the edges in the walk.

Refer the graph in figure 10.5 with 6 vertices.

Examples:

1. 1, (1,2), 2, (2,5), 5, (5,3), 3 is a walk. It begins at 1 and ends at 3. Terminal vertices of this walk are 1 and 3. These vertices are distinct. This walk is called ***open walk***. Length of this walk is 3.
2. 1, (1,2), 2, (2,5), 5, (5,4), 4, (4,3), 3, (3,1), 1 is also a walk. Length is 5. Terminal vertices are same. This is called ***closed walk***.

3. 3, (3,5), 5, (5,6), 6, (6,4), 4, (4,5), 5, (5,2), 2 is another walk. This is also an open walk. Observe that vertex 5 is visited twice in the walk. Length of this walk is 5.
4. 1, (1,2), 2, (2,5), 5, (5,2), 2 is not a walk. This is because the same edge (2,5) (note that (2,5) and (5,2) are the same edge) is traversed twice.

Path is an open walk with no vertex repetition in the sequence. That is no vertex is revisited. Length of the path is the number of edges in the sequence.

Example 1 above is a path. The length of this path is 3.

Example 2 is not a path. Since terminal vertices are the same and hence not open walk. Example 3 although is an open walk is not a path since vertex 5 is revisited for a second time in the walk.

Notice that walks and paths are sub-graphs. In a path all vertices except the beginning and ending are of degree two. The terminal vertices are of degree one.

A closed walk in which no vertex repeats more than once is called a ***circuit***. In other words circuit is a closed non-intersecting walk.

For example referring to the graph of six vertices in figure 10.5,

1, (1,2), 2, (2,5), 5, (5,3), 3, (3,1), 1 is a circuit of 4 vertices and 4 edges.

5, (5,6), 6, (6,4), 4, (4,3), 3, (3,1), 1, (1,2), 2, (2,5), 5 is another circuit of length 6

Observe that the degree of every vertex in a circuit is two. Other names for a circuit are ***cycle***, ***elementary cycle***, ***circular path***, ***loop***. Note that every self loop is a circuit.

The definitions in this section are summarized in the figure 10.8 below. The arrows are in the direction of increasing restriction.

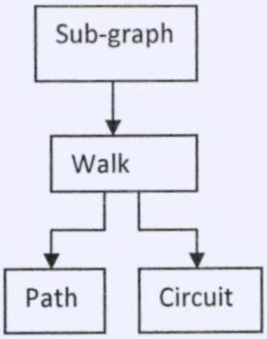


Fig 10.8: Walks, paths and circuits as sub-graphs

10.4 CONNECTED GRAPHS AND COMPONENTS

The concept of connectedness is obvious. A graph is connected if we can reach any vertex from any other by travelling along the edges. A formal definition of connectedness is as follows:

A graph is said to be connected if there is at least one path between every pair of vertices. Otherwise the graph is disconnected. The graphs in figures 2.8 and 2.9 are examples of connected and disconnected graphs.

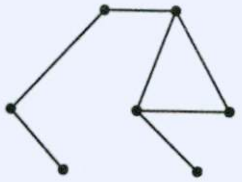


Fig 10.9: 7 vertex connected graph

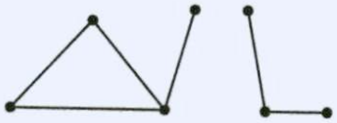


Fig 10.10: 7 vertex disconnected graph

Disconnected graphs consist of two or more connected sub-graphs. The graph in figure 10.10 has two connected sub-graphs. Each of these connected sub-graphs is called a component. An easy way to find a component is to find all vertices that are reachable from a vertex v_i. Vertex v_i and all the vertices of the graph that have paths to v_i, together with all the edges incident on them form a component. It is evident that a component itself is a graph. To be precise, a component is a sub-graph of the given one. We now discuss some important theorems on connectivity of a graph.

Theorem 10.1

A graph G is disconnected if and only if its vertex set V can be partitioned into two nonempty, disjoint subsets V1 and V2 such that there is no edge connecting a vertex in V1 to any vertex in V2.

Proof:

If: Assume a partition as described exists. We need to show that the graph is disconnected. Consider two vertices x and y, where x$\in$ V1 and y $\in$ V2. Let us examine if there can be a path from x to y. Note that a path from x to y requires connection between a vertex in V1 and some vertex in V2. By assumption there is no such connection. Hence it is evident that there is no path from x to y. That is the graph G is disconnected.

Only if: Assume G is a disconnected graph. We need to prove that the described partition exists in the graph.

Consider a vertex x in G. Let V1 be the set of vertices can be reached from x. Since G is disconnected V1 does not include all vertices (follows from the definition of connectedness). The remaining set of vertices will form a set V2. No vertex in V1 is joined to any vertex in V2. Thus the partition V1 and V2 is found.

Theorem 10.2

If a graph (connected or disconnected) has exactly two vertices x and y of odd degree, there must be a path joining these two vertices.

Proof:

Let G be graph with all even vertices except the odd vertices x and y. From theorem 1.2, which is true for every graph and therefore for any component, no graph can have odd number of odd degree vertices. Therefore in G, x and y must belong to the same component and hence there should be a path between them.

Theorem 10.3

A simple graph (a graph having no parallel edges or self loops) G with n vertices and k components can have at most (n-k)(n-k+1)/2 edges.

Proof:

Let $n_1, n_2, \ldots n_k$ be the number of vertices in the k components. Then $n_1+n_2+\ldots n_k=n$. The proof of the theorem depends on the following algebraic inequality.

$$\Sigma n_i^2 \leq n^2 - (k-1)(2n-k) \qquad \text{------------ (1)}$$

From the theorem 9.3, we know that maximum number of edges in the i^{th} component is $n_i(n_i-1)/2$. Therefore the maximum number of edges in G is

$$\Sigma n_i(n_i-1)/2 = \Sigma(n_i^2)/2 - n/2$$

$$\leq [n^2 - (k-1)(2n-k)]/2 - n/2 \qquad \text{(using inequality (1) above)}$$

$$= (n-k)(n-k+1)/2$$

Observe that this theorem is generalization of theorem 9.3.

We close this section after a discussion of matrix form of disconnected graphs.

If a graph G is disconnected (with no common vertex and common edge) with two components g and g′ then A(G) will be in the form

$$\left(\begin{array}{c|c} A(g) & 0 \\ \hline 0 & A(g') \end{array}\right)$$

Example: Consider the disconnected graph G with components g and g′ below.

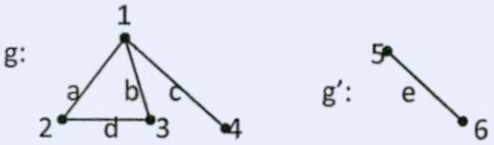


Fig 10.11: Disconnected graph

The incidence matrix is given by,

$$\begin{array}{cc} & \begin{array}{ccccc} a & b & c & d & e \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} & \left(\begin{array}{cccc|c} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right) \end{array} = \left(\begin{array}{c|c} A(g) & 0 \\ \hline 0 & A(g') \end{array}\right)$$

10.5 EULER GRAPHS

Euler is the founder of Graph theory. Euler solved the bridge problem, which was when Graph theory became a subject of study. In fact in that paper, on the problem about the bridge, he posed a more general problem. His problem goes as follows:

In what type of graph G is it possible to find a closed walk running through every edge exactly once?

Such a walk is now called ***Euler line / Euler walk***. The graph which contains an Euler line is called an Euler graph. In other words if some closed walk in a graph contains all edges of the graph, then the walk is called an Euler line and the graph an Euler graph. By definition walk is always connected. Since Euler line contains all edges of the graph, an Euler graph is always connected, except for any isolated vertex the graph may have. As isolated vertices do not contribute anything to concept of Euler line or graph, henceforth we assume that Euler graphs are always connected. Next we prove an important theorem which will enable us to conclude if the graph is Euler graph or not.

Theorem 10.4

A given connected graph G is an Euler graph if and only if all vertices of G are of even degree.

Proof:

If: Suppose that G is an Euler graph. G contains an Euler line. When the walk hits a vertex it goes through two new edges; one we traversed to reach the vertex and the other through which we exit through. In this process we encounter two new edges incident on a vertex, each time we pass through. This is also true of terminal vertices. Thus every vertex is of even degree.

Only if: Assume all vertices of G are of even degree. Start the walk from an arbitrary vertex v. Go to a neighboring vertex. Since every vertex is even, when we enter a new vertex x there is an edge to exit from this vertex x. When you get back to v you have completed a closed walk h. See if all edges are traversed. If so the graph G is Euler graph. If not, remove from G all those edges which are part of h and obtain a sub-graph G'. Since G and h have all vertices with even degrees, vertices of G' are also of even degree. Moreover h and G' must have a common vertex, since G is connected. Find a closed walk j in G' starting from a vertex w (this is possible since vertices of G' are all even). Construct a new walk combining h and w. This walk has more edges than h or j. If all edges are covered then G is Euler. If not the above process is repeated until we obtain a closed that traverses all edges of G. Thus G is an Euler graph.

Example: Follow the arrows to find a walk in the graphs below.

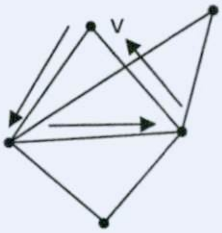


Fig 10.12(a): Closed walk h in G starting at v

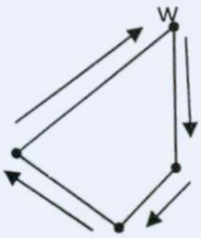


Fig 10.12(b): Sub-graph G' and the closed walk j starting at w

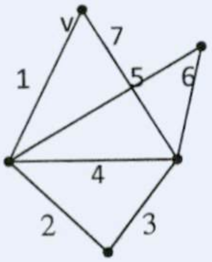


Fig 10.12(c): Combining h and j. All edges covered. Numbers indicate order of traversal of edges

Now coming back to Königsberg bridge problem recall figure 9.5, which is the graph corresponding to the problem. Observe that degrees of vertices C and D (5 and 3 respectively) are odd. Hence the graph is not Euler. Therefore a closed walk covering all edges does not exist.

One often encounters Euler graphs in various puzzles. The problem common to these puzzles is to find how to draw a picture in one continuous line without retracing and without lifting the pencil from the paper.

In defining Euler line some authors drop the requirement that the walk be closed. For example the traversal 4, (4,6), 6, (6,5), 5, (5,4), 4, (4,3), 3, (3,5), 5, (5,2), 2, (2,1), 1, (1,3), 3 in the graph of figure 10.5 includes all edges just once but starting and ending vertices are different. This kind of walk is called ***open Euler line*** or ***unicursal line***. A connected graph that has a unicursal line is called unicursal graph. It is clear that by adding an edge between starting and ending vertices of unicursal line we get an Euler line. Thus a connected graph is unicursal if and only if there are exactly two vertices that are of odd degree. The generalization of this statement is the following theorem. An interested reader can refer the text by Narsingh Deo for a detailed proof.

Theorem 10.5

In a connected graph G with exactly 2k odd vertices, there exist k edge disjoint sub-graphs such that they together contain all edges of G and that each is a unicursal graph.

10.6 HAMILTONIAN CIRCUITS AND PATHS

An Euler line is characterized by closed walk covering all edges exactly once. Hamiltonian circuit is a closed walk going through each vertex exactly once except that first and last vertex in the tour is the same (recall definition of closed walk).

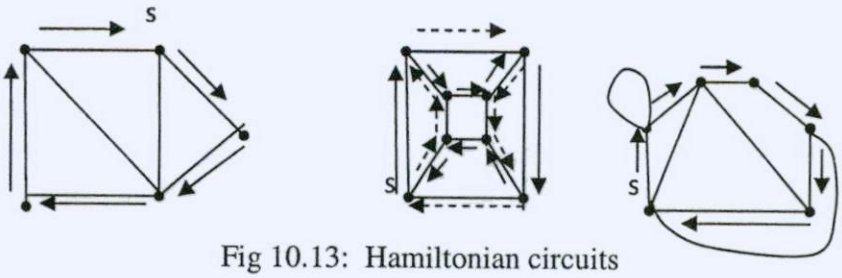


Fig 10.13: Hamiltonian circuits

The three graphs in the figure 10.13 are with vertices 5, 8 and 6 in number. s is the starting vertex of the Hamiltonian circuit in each graph. Follow the arrow marks for the Hamiltonian circuits in these graphs. Recall the definition of circuit in section 10.3. It is a closed walk where no vertex repeats. In addition if the circuit includes every vertex it is Hamiltonian circuit. A Hamiltonian circuit of n vertex graph consists of n edges. A graph can have many Hamiltonian circuits. For example second graph in figure 10.13 has one more circuit indicated in dashed arrows.

Not every graph will have Hamiltonian circuit. Two graphs (with vertices numbered) in the figure next (figure 10.14) do not have Hamiltonian circuit.

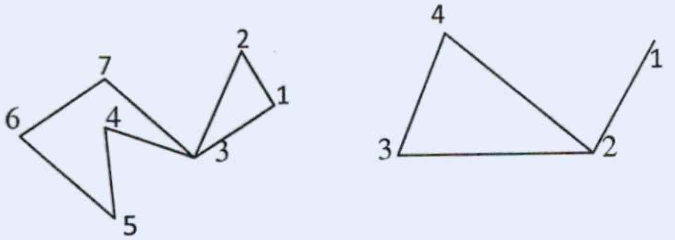


Fig 10.14: Graphs with no Hamiltonian circuit

Hamiltonian circuits and Euler lines are different. Hamiltonian circuit is much more complex. The problem of necessary and sufficient condition in a graph for the presence of Hamiltonian circuit is still unsolved. This problem was first posed by Sir William Rowan Hamilton and hence the name Hamiltonian circuit.

Hamiltonian path

If we remove the last edge from a Hamiltonian circuit, we get a Hamiltonian path. Hamiltonian path is sub-graph of Hamiltonian circuit. Every graph that has Hamiltonian circuit should have a Hamiltonian path. However not vice versa. That is there may be graphs with Hamiltonian paths but yet no Hamiltonian circuits. For example both the graphs in figure 10.14 have Hamiltonian paths. Follow the vertices beginning from 1 in the increasing order to get the Hamiltonian paths. These are 1 to 2 to 3 to 4 to 5 to 6 to 7 and 1 to 2 to 3 to 4 respectively. Note that length of Hamiltonian path is n-1 in an n vertex graph.

In considering existence of Hamiltonian circuits or paths we need only consider simple graphs. This is because a Hamiltonian circuit or path traverses each vertex only once. Hence it cannot include parallel edges or self loops. Thus it may be sensible to remove parallel edges and self loops before looking for a Hamiltonian circuit. Finally not all graphs have Hamiltonian paths. Graphs below in figure 10.15 are examples of graphs that do not have Hamiltonian paths.

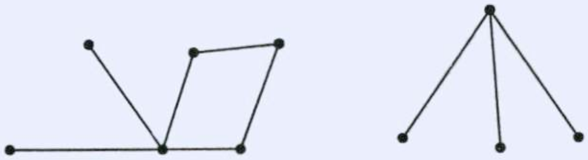


Fig 10.15: Graphs not having Hamiltonian paths

Complete graph was discussed in unit 9. It is nothing but a simple graph with edges connecting every pair of vertices. This is also referred to as ***universal graph*** or a ***clique***. Every vertex is joined to every other vertex in a complete graph. Hence the degree of every vertex in complete graph of n vertices is n-1. Also the number of edges in a complete graph of n vertices is $n(n$-1)/2 (refer theorem 9.3).

It is easy to construct a Hamiltonian circuit in a complete graph. Let the vertices be numbered 1 to n. Traverse the vertices in the order 1 to 2 to 3 … n-1 to n to 1. A graph may contain many Hamiltonian circuits. Number of edge disjoint Hamiltonian circuits is an unsolved problem. However something can be said about this number in some graphs.

Theorem 10.6

In a complete graph with n vertices there are (n-1)/2 edge-disjoint Hamiltonian circuits, if n is odd and ≥ 3.

Proof:

In a complete graph of n vertices there are $n(n$-1)/2 edges. A Hamiltonian circuit in an n vertex graph has n edges. Hence number of edge-disjoint Hamiltonian circuits cannot exceed (n-1)/2. That there are (n-1)/2 edge disjoint Hamiltonian circuits if n is odd can be shown as follows:

Here we propose an informal proof for the above statement. Let us find the number of Hamiltonian circuits in complete graphs of 3, 5, 7 vertices. Later we conclude by extrapolation for n vertices.

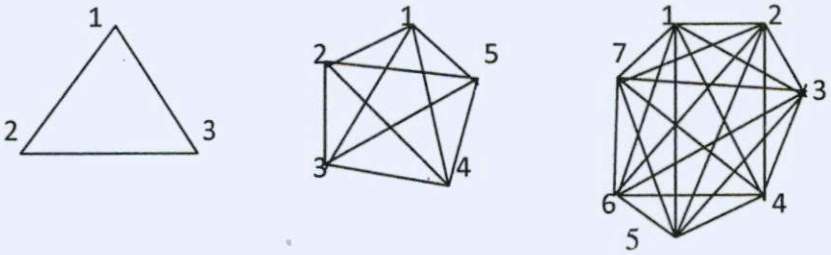


Fig 10.16: Complete graphs of 3, 5 and 7 vertices

The edge-disjoint Hamiltonian cycles in these graphs are:

3 vertex graph: 1, (1,2), 2, (2,3), 3, (3,1), 1 (only one [(3-1)/2] Hamiltonian cycle)

5 vertex graph:

1, (1,2), 2, (2,3), 3, (3,4), 4, (4,5), 5 (5,1), 1;

1, (1,3), 3, (3, 5), 5, (5,2), 2, (2,4), 4, (4,1), 1 (two [(5-1)/2] cycles

1, (1,2), 2, (2,3), 3,(3,4), 4, (4,5), 5, (5,6), 6, (6,7), 7, (7,1),1;

1, (1,3), 3, (3,5), 5, (5,7), 7, (7,2), 2, (2,4), 4, (4, 6), 6, (6,1), 1;

1, (1,4), 4, (4,7), 7, (7,3), 3, (3, 6), 6, (6,2), 2, (2, 5), 5, (5, 1),1 (three [(7-1)/2] cycles)

Hence number of edge disjoint cycles in an n vertex complete graph is $(n-1)/2$, if n is odd and greater than 1.

Travelling salesman problem

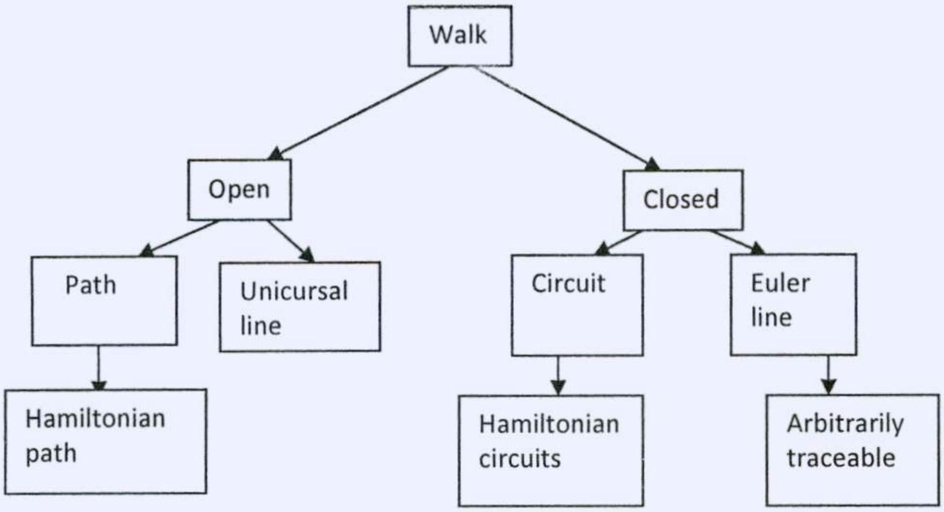
A problem closely related to the question of Hamiltonian circuits is travelling salesman problem, stated as follows: A salesman is required to visit a number of cities during his trip. Given the distances between the cities, in what order should he travel so that he visits each city exactly once and return home, with the minimum distance travelled?

Representing the cities by vertices and the roads between cities as edges, we get a graph. In this graph, edges are weighted, weights being distances between cities. In our problem, if each of the cities has a road to every other city, we have a complete graph and there are numerous Hamiltonian circuits. The tour of the salesman is after all a Hamiltonian circuit beginning at starting city and ending at the same city. We are to pick that cycle whose sum of distances is minimum. The total number of Hamiltonian cycles (not necessarily edge disjoint ones) in complete graph is $(n-1)!/2$. This follows from the fact that there are n-1 choices of cities at first (starting) city, n-2 at the second city and so on. These being independent choices, we get $(n-1)!$

possible number of choices. This number is to be divided by 2 since each cycle is counted twice. (Remember the graph is not directed. The cycle 1 to 2 to 3 … n to 1 is same as 1 to n to n-1 to … 3 to 2 to 1).

Theoretically the travelling salesman problem can be solved by finding all cycles and its distances and the minimum distance cycle can be chosen. However for a large value of n, it is too tedious to find all cycles. The problem is to find a manageable algorithm to find a solution in reasonable time. No such algorithms exist. This being a very important problem in Operations Research, many attempts have been made. There are some good heuristic algorithms available. These heuristic methods may not give us an optimal solution. But will definitely get one very close to optimal solution, called near optimal solutions.

Various types of walks and circuits discussed in this unit are classified in the following diagram.



10.7 SUMMARY

The unit begins with isomorphism of graphs. Concepts like walks, paths, circuits and Euler graphs are discussed with ample examples. Connectedness is an important concept useful for many applications. This idea is discussed in length here also giving the matrix structure of disconnected graphs. Special circuits and paths called Hamiltonian circuits and Hamiltonian paths and a very important problem in computer science are discussed in detail.

10.8 KEYWORDS

Isomorphism, sub-graph, walk, path, circuit, connected graphs, Euler graphs, Hamiltonian circuit, travelling salesman problem

10.9 QUESTIONS

1. Draw graphs of 4 and 5 vertices that are isomorphic.
2. State the conditions for graphs to be isomorphic.
3. Draw graphs that satisfy all 3 conditions of isomorphism and yet not isomorphic. State the reasons why they are not isomorphic.
4. Define sub-graph and provide examples.
5. Draw a graphs and sub-graphs that are edge disjoint and that are vertex disjoint.
6. Define walks, paths, circuits. Illustrate.
7. Illustrate closed and open walk.
8. Distinguish circuit and walk. Give examples.
9. Comment about the degrees of vertices in walks, paths and circuits.
10. Define connected graph. Give examples of connected and disconnected graphs with various numbers of vertices.
11. What is component?
12. State and prove the necessary and sufficient conditions for a graph to be disconnected.
13. If a graph has exactly two vertices that of odd degree, prove that there must be path connecting these two.
14. What is the maximum number of edges in a simple graph of n vertices and k components? Justify your answer. Also draw some graphs and verify.
15. What is Euler graph? Draw one that is Euler and one that is not.
16. State and prove the theorem on Euler graphs.
17. What is Hamiltonian circuit? Why are they called so?
18. Distinguish Hamiltonian circuit and Euler line. Give examples.
19. Define unicursal line. Illustrate.

20. Comment on the maximum number of edge-disjoint Hamiltonian circuits. Verify your statement in some graphs.
21. What do you mean by Hamiltonian path? Give an example.
22. What can you say about presence of Hamiltonian circuit and path?
23. State the problem of travelling salesman. How is this similar to Hamiltonian circuit?
24. Why is travelling salesman problem difficult to solve by enumeration?

10.10 REFERENCES

1. Narsingh Deo, Graph Theory with applications to Engineering and Computer Science, PHI
2. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL
3. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
4. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

UNIT - 11: PLANAR GRAHS AND COLORING

Structure

11.0 Objectives

11.1 Introduction

11.2 Planar graphs

11.2.1 Kuratowski's graphs

11.2.2 Detection of planarity

11.3 Chromatic number of a graph

11.3.1 Proper coloring

11.3.2 Chromatic partitioning

11.4 Matching

11.5 Keywords

11.6 Summary

11.7 Questions

11.8 References

11.0 OBJECTIVES

After studying this unit, you will understand

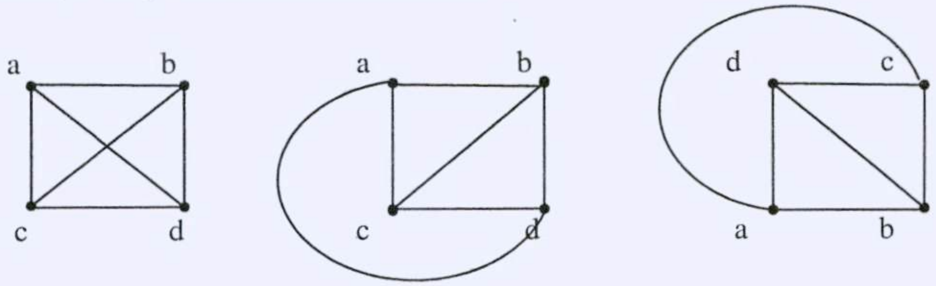
- ✓ Concepts of planar graphs
- ✓ Conditions for a graph to be planar
- ✓ Coloring of vertices
- ✓ Chromatic number of graphs and some important results
- ✓ A special graph called bi-partite graph

11.1 INTRODUCTION

In this unit, we discuss planar graphs. The question of planarity is of great significance in many practical situations, such as printed circuit board (to determine if a single layer is sufficient to make all connections), proper coloring of a graph and the partitioning of vertices. Partitioning of vertices has many practical applications such as coding theory, state reduction of sequential machines etc.

11.2 PLANAR GRAPHS

You may be aware that a graph is an abstract object of vertices and edges and often it is represented by a geometric figure in a plane. For example graph G with vertex set V= {a,b,c,d} and edge set E={(a,b), (a,c), (a,d), (b,c), (b,d), (c,d)} is complete graph of 4 vertices and can be represented by the figures (11.1 to 11.3) below.



Figs 11.1, 11.2 and 11.3: 4 vertex complete graphs

There are numerous other possible representations.

Definition- embedding

Geometric representation of a graph on any planar surface (board, paper etc) without edge intersection is called embedding.

Definition- planar graph

A graph G is said to be planar graph, if there exists some geometric representation of G which can be drawn on a plane such that no two of its edges intersect. Alternatively, a graph is a planar graph if one of the geometric representations is an embedding.

Note that the 4 vertex complete graph is planar although the graph in figure 11.1 is not embedded. Note that the graphs in figures 11.2 and 11.3 are embedded. Thus the 4 vertex complete graph is planar.

Example

The graphs G_1, G_2 given in figures 9.4 and 9.5 are isomorphic (can be called identical). The representation in figure 9.4 is an embedding whereas the figure 9.5 shows non-embedded version of the graph. Thus the graph is planar.

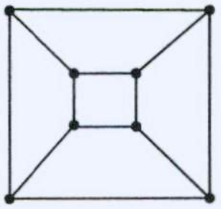


Fig 11.4: Graph G_1

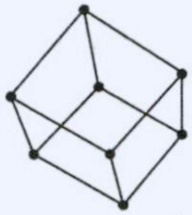


Fig 11.5: Graph G_2

Example

Observe the graphs G_1, G_2 and G_3 below with 10 vertices and 15 edges in figures 9.6,9.7 and 9.8. The graphs are isomorphic. The graphs in figures 9.7 and 9.8 are different representation of G_1 in figure 9.6. But none of the geometric representation is embedded. In fact there is no embedded version of the graph. Thus it is non-planar.

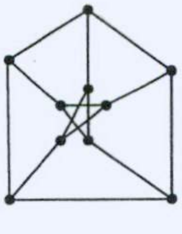


Fig 11.6: Graph G_1

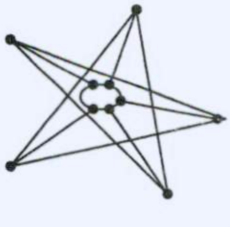


Fig 11.7: Graph G_2

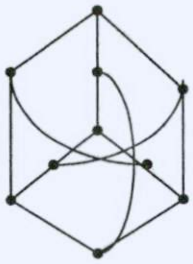


Fig 11.8: Graph G_3

Following are the steps to determine if the given connected graph G is planar.

1. If the geometric representation of the graph in a plane is embedded then conclude G it is planar and exit. Else go to step 2.

2. Find a new geometric representation G_1 by redrawing the graph G such that G and G_1 are isomorphic. If none exists conclude G is non planar. Else go to step 3.
3. If G_1 is embedded then conclude G planar and exit. Else repeat step 2.

11.2.1 KURATOWSKI'S GRAPHS

Now we discuss an important theorem on planar graphs, called Kuratowski's theorem. Kuratowski is a Polish mathematician who stated a unique property of non planar graphs.

Theorem 11.1

A complete graph of 5 vertices, called K_5 (Kuratowski's first graph) is non planar.

Proof

Let the vertices be *a*, *b*, *c*, *d*, *e*. join adjacent vertices. Now we have a pentagon. Join *a*, *c* and *a*, *d*. edges (*b*, *e*) and (*b*, *d*) can be drawn outside the pentagon. Thus 9 edges have been drawn without intersection (refer figure 11.9). The last edge (*c*, *e*) cannot be drawn without intersecting one or the other previously drawn edges.

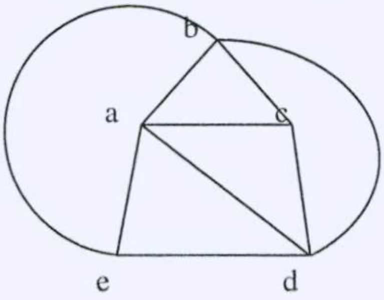


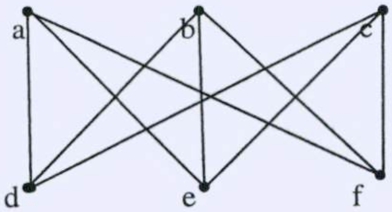
Fig 11.9: K_5 with 9 edges

Theorem 11.2

A regular connected graph with 6 vertices and 9 edges, called $K_{3,3}$ (Kuratowski's second graph) is non planar.

Proof

A regular graph degree of vertices are equal. 6 vertex regular graph with 9 edges is shown in figure 11.10. This representation is non planar. Let us try to redraw the graph. Let G_1 be the redrawn graph. After 8 non-intersecting edges the last edge (*b*, *e*) can neither be drawn inside or outside the hexagon without intersecting some of the previously drawn edges. Thus $K_{3,3}$ is non planar. Refer figure 9.12 for G_1 with 8 non-intersecting edges.



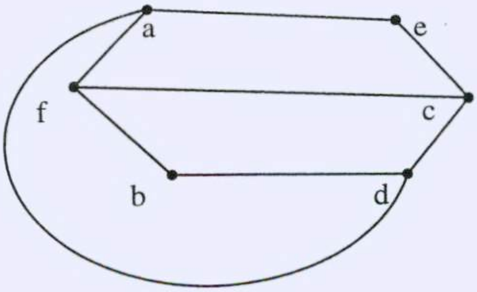


Fig 11.10: $K_{3,3}$ Fig 11.11: Redrawn $K_{3,3}$, with 8 non-intersecting edges

Some observations on Kuratowski's graphs are:

1. Both K_5 and $K_{3,3}$, are regular.
2. Both are non planar.
3. Removal of one edge makes it planar.
4. K_5 is a non planar graph with smallest number of vertices.
5. $K_{3,3}$ is the non planar graph with smallest number of edges.

11.2.2 DETECTION OF PLANARITY

Here we discuss algorithmic way of detecting planarity. The previously discussed method of redrawing is not efficient. We now give the steps to be executed find if a graph is planar.

1. A disconnected graph is planar if and only if each of its components is planar. We check planarity of only connected graphs. Also a separable graph is planar if and only if each of its blocks is planar. Hence for the given graph G we first find its non separable blocks G_1, G_2, … G_k. Steps 2 to 4 detect planarity of a non separable block G_i.
2. Since addition or removal of self loops does not affect planarity, remove self loops.
3. Since parallel edges also do not affect planarity, remove all but one edge of the parallel edges.
4. Elimination of a vertex of degree 2 by merging two edges in series does not affect planarity. Hence eliminate all edges in series.

After these steps the graph G1 (separable block) is reduced to H1.

Theorem 11.3

Graph H_1 is:

1. A single edge or
2. A complete graph of 4 vertices or
3. A non separable simple graph with $n \geq 5$ and $e \leq 7$.

Example

Figure 11.12 is 5 vertex 7 edge graph. Figures 11.13 to 11.16 show reductions. The graph is reduced to a single edge. Edges are labeled 1 to 7 in G_1.

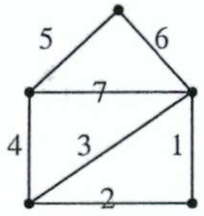


Fig 11.12: G_1

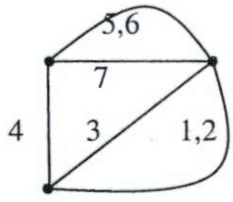


Fig 11.13: Adjacent vertices reduced

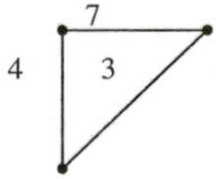


Fig 11.14: Parallel edges reduced

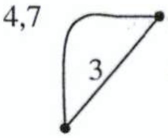


Fig 11.15 Adjacent vertices reduced

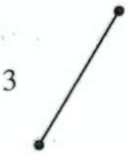


Fig 11.16 Parallel edges reduced

From now on, we therefore need to investigate only simple connected non separable graphs of at least five vertices and with every vertex of degree three or more. Next we check if $e \leq 3n-6$. If not, graph is non planar. If the inequality is satisfied we have to test the graph further using the theorem given next.

Definition- Homeomorphic graphs

Two graphs are said to be ***homeomorphic*** if one graph can be obtained from the other by the creation of edges in series or by merger of edges in series. Note that the graphs in figures 11.12 to 11.16 are homeomorphic. A graph is planar if and only if every graph that is homeomorphic to G is planar.

Theorem 11.4

A necessary and sufficient condition for a graph G to be planar is that G does not contain either of Kuratowski's graphs or any graph homeomorphic to either of them.

11.3 CHROMATIC NUMBER OF A GRAPH

We now address the next important concept of this unit, coloring and chromatic number.

11.3.1 PROPER COLORING

Suppose a graph has *n* vertices. Suppose we are faced with the task of painting the vertices so that no two adjacent vertices have the same color. The determination of least number of colors is the coloring problem. We introduce and define some terminologies.

Proper coloring

Painting all the vertices of a graph with colors such that no two adjacent vertices have the same color is called proper coloring.

Chromatic number

A graph G that requires a minimum of *k* different colors for its proper coloring is called *k*-chromatic graph. The number *k* is called the chromatic number of the graph.

Example

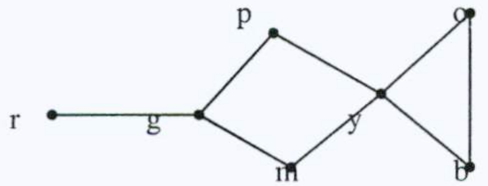


Fig 11.17: Graph of 7 vertices properly colored with 7 colors

Colors used: r-red, g-green, p-purple, m-magenta, y-yellow, o-orange, b-blue

Note that not all 7 colors are needed for proper coloring of vertices. For instance, instead of magenta purple could be used for that vertex.

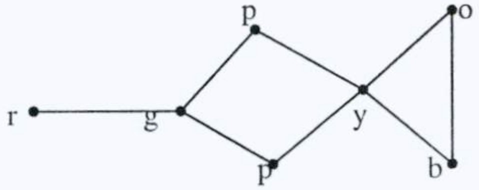


Fig 11.18: Proper coloring with 6 colors for the graph in figure 11.17

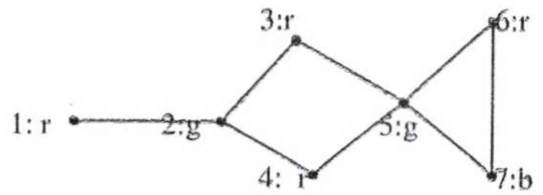


Fig 11.18: Proper coloring with 3 colors (minimum number) for the graph in figure 11.17

Note that the minimum number of colors needed is 3. Thus chromatic number of G = 3.

In coloring graphs there is no point in considering disconnected graphs. How we color vertices in one component of a disconnected graph has no effect on coloring other components. Hence it is enough if we investigate coloring in a connected graph. All parallel edges can be replaced by a single edge. For determination of chromatic number we reduce the graph to simple graph. Some observations that follow directly from the definitions stated.

1. Graph which is just one vertex is 1-chromatic.
2. A simple graph with one or more vertices is at least 2-chroamtic.
3. A complete graph of *n* vertices is *n*-chromatic.
4. A graph of simply one circuit is with $n \geq 3$vertices is 2-chromatic. If *n* is even and 3-chromatic if *n* is odd.
5. Chromatic number of tree with 2 or more vertices is 2.

We now state a very important result on chromatic number: If d_{max} is the maximum degree of all vertices in G then chromatic number of G $\leq 1+d_{max}$; and if G has no component graph of $1+d_{max}$ vertices then chromatic number of G $\leq d_{max}$.

11.3.2 CHROMATIC PARTITIONING

In this section we discuss a partitioning of vertices of graph induced by proper coloring. We begin the section with special graph called bipartite.

Definition

A graph G is bipartite if its vertex set V can be decomposed into two disjoint subsets V_1 and V_2 such that every edge in G joins a vertex in V_1 to a vertex in V_2. Note that every tree is bipartite graph. Clearly every 2-chromatic graph is a bipartite graph. The two colors create a partition of the vertex set. In generalizing this concept a graph G is called *p*-partite if its vertex set can be portioned into p disjoint subsets $V_1, V_2, \ldots V_p$ so that no edge in G joins the vertices in the same subset. Clearly k-chromatic graph is p-partite if and only if $k \leq p$.

Chromatic partitioning

Proper coloring of a graph induces a partitioning of the vertices. If minimum number of colors are used the partition is called chromatic partitioning. For instance the chromatic partitioning of the graph in figure 11.8 is {1, 3, 4, 6}, {2, 5}, {7}. No two vertices in any of the subset of the partition are adjacent. These are independent sets. However if no vertex can be added to any subset without destroying its independence property then it is called maximal independent set. For instance {7} is not maximal independent set, since vertex 1 can be added without destroying the independence property; but {1, 3, 4, 6} is maximal independent set. Independence number is the number of vertices in the largest independent set. For instance the independence number of the graph in figure 11.18 is 4. This number is denoted by β(G). We know state an important result connecting independence number and chromatic number. If chromatic number of a graph with n vertices is k then $\beta(G) \geq n/k$. As an example consider the graph in figure 11.18. In this graph n=7, k=3 and β(G) = 4. It is easy to verify $\beta(G) \geq n/k$.

11.4 MATCHING

This unit is concluded with a discussion on matching. Suppose there are 4 applicants (a_i, for i=1 to 4) for 6 vacant positions (p_j, j= 1 to 6). Vacant positions and applicants can be denoted by vertices. The edges joining a_i and p_j denote that i^{th} applicant is suitable (qualified) for position j. The graph is bipartite. The question we have is identifying maximum number of positions that can be filled by applicants. This problem is called matching (or assignment) of one set of vertices into another. More formally matching is a subset of edges in which no two edges are adjacent. A maximal matching is a matching to which no edge can be added. The graphs given in the figures below illustrate these concepts.

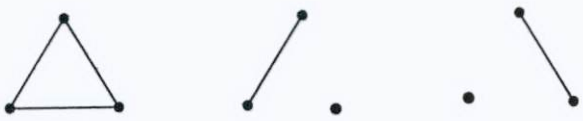


Fig 11.19: A graph (to the left) and two matching

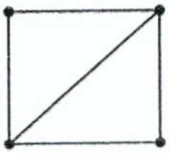


Fig 11.20: Graph G

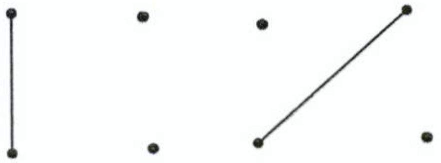


Fig 11.21: Two matching

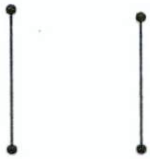


Fig 11.22: Maximal Matching

Although matching is possible in any graph, it is mostly studied in bipartite graph. In a bipartite graph with vertex partitions V_1 and V_2, a complete matching is where no vertex in V_1 is left out. That is there are edges incident on vertices of V_1. Refer figures below for illustrations of matching.

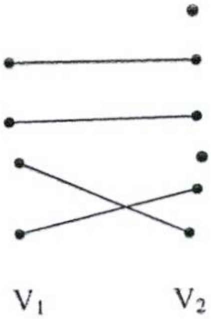


Fig 11.23: Complete matching

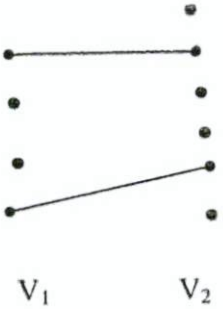


Fig 11.24: A matching

For the existence of a complete matching, of V_1 into V_2 the number of vertices in $V_1 \leq$ number of vertices in V_2. But this is not sufficient. Refer figure below for illustration of this point.

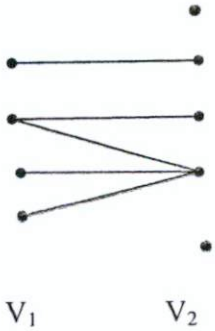


Fig 11.25: No complete matching possible in this bipartite graph

The complete matching is not possible because two applicants qualify for only one job (identical). Hence only one of these edges should have to be excluded from the matching set. Then not vertices of V_1 are matched into vertices of V_2.

11.5 SUMMARY

In this unit a detailed discussion of planar graph, steps of reduction for checking planarity and conditions for planarity is done in section 11.2. Section 11.3 describes another useful concept namely coloring, chromatic number and independence number. The unit is closed with a discussion of matching, complete matching and conditions for complete matching.

11.6 KEYWORDS

Planar graphs, Kuratowski's graphs, Theorems on planarity, Detection of planarity, Proper coloring, Chromatic number, Chromatic partition, Independence number, Matching

11.7 QUESTIONS

1. Define and illustrate planar and non planar graphs.
2. Write the steps for checking planarity.
3. Show that Kuratowski's graphs are non planar.
4. State theorems on planarity.
5. What is proper coloring?
6. Draw a graph of 7 or more vertices with 9 or more edges. Show proper coloring and what is the chromatic number?
7. Show the relation between independence number and chromatic number in the above graph (in problem 6).
8. Define matching and complete matching. Illustrate.
9. State the necessary condition for complete matching. Show that it is not sufficient.

11.8 REFERENCES

1. Narsingh Deo, Graph Theory with applications to Engineering and Computer Science, PHI
2. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL

3. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
4. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

UNIT - 12: GRAPH ALGORITHMS

Structure

12.0 Objectives

12.1 Introduction

12.2 Tree

12.3 Spanning tree

12.4 Minimum weight spanning tree

12.4.1 Algorithms to find minimum weight spanning tree

12.5 Searching graphs

12.5.1 Depth first search

12.5.2 Breadth first search

12.6 Summary

12.7 Keywords

12.8 Questions

12.9 References

12.0 OBJECTIVES

After studying this unit, you will

- ✓ Come to know about the special graph called tree
- ✓ Understand what a spanning tree is
- ✓ Understand minimum weight spanning tree computation and applications
- ✓ Get to know the search methods

12.1 INTRODUCTION

In this unit we describe a graph structure called tree and state some interesting properties of trees. Spanning tree is important structure with many applications. Spanning tree is discussed and two algorithms for finding minimum weight spanning tree are discussed in length. Searching graphs is another important procedure in computer science. Two search procedures, depth first and breadth first are also discussed in the end of the unit.

12.2 TREE

Tree is a special graph. The concept of tree is very important in graph theory and also in many applications of computer science. Also tree is an important data structure in computer science.

Definition

Tree is a connected graph without any circuits. The graphs in figure 12.1 are all trees with varying number of vertices.

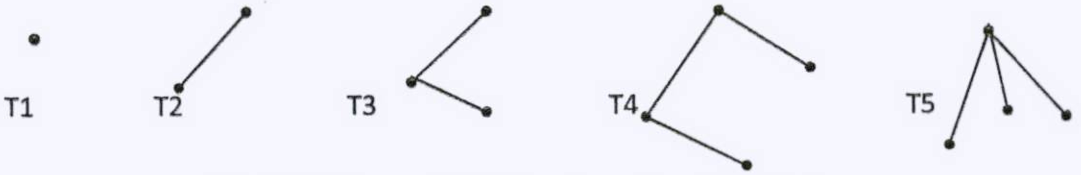


Fig 12.1: Trees with different number of vertices

Parallel edges and self loops form circuits. Hence, it is obvious that trees are simple graphs. Trees can be infinite as graphs. But our discussions focus on finite trees only.

Applications

Trees are useful in describing any structure which involves hierarchy. Familiar examples of such trees are family trees, decimal classification of books in a library, the hierarchy of positions in an organization, an algebraic expression involving operations which comes with precedence, sorting of mails according to PIN code etc. Figure 12.2 shows mail sorting process as a tree diagram. All mails arrive at a local office N. PIN codes of mails are read at N. Mails are first sorted using the most significant digit in the PIN code and are divided into 10 piles N0, N1, …N9. Each pile is then divided into 10 piles and this continues for 4 more times (the number of digits in a PIN code is 6).

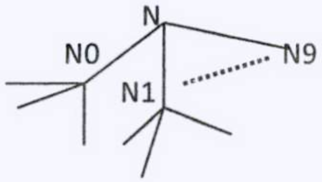


Fig 12.2: Mail sorting process

We now state some useful properties of trees in this section. These properties can also be treated as alternate definitions of a tree.

A graph G with n vertices is called a tree if

1. G is connected and is circuitless, or
2. G is connected and has n-1 edges, or
3. G is circuitless and has n-1 edges, or
4. There is exactly one path between every pair of vertices, or
5. G is minimally connected graph.

Another interesting property we state here again without proof.

A tree (of two or more vertices) has at least two pendant vertices. Note that this true of al trees in figure 12.1.

12.3 SPANNING TREE

In the previous section we discussed graphs which are trees. In this unit we identify a tree in a graph.

Definition

Let G be a graph. A spanning tree is a tree connecting all vertices of G.

Examples

Given below in figure 12.3 are some graphs and spanning trees for each graph.

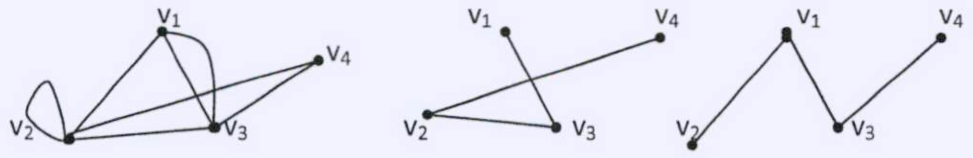


Fig 12.3(a): Graph (b) Spanning tree T_1 (c) Spanning tree T_2

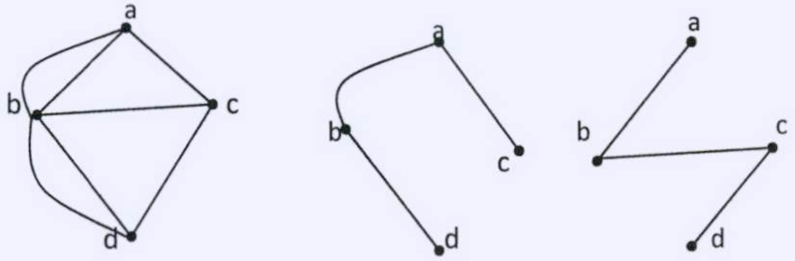


Fig 12.4 (a): Graph (b) Spanning tree T_1 (c) Spanning tree T_2

Finding a spanning tree

Finding a spanning tree in graph is easy. If G has no circuit, then it is a spanning tree. If G has a circuit, delete an edge from the circuit. This will still leave the graph connected. If there are more circuits, repeat the above operation until there are no more circuits. As the resulting graph is connected and has no circuits, it is a tree and has all vertices. Thus a spanning tree in G is found.

Let us go back to the graph in figure 12.3 (a). Self loop at v_2 is a circuit. Remove the self loop. Edges (v_1, v_2), (v_2, v_3) and (v_3, v_1) form a circuit. Remove an edge say (v_1, v_2) from this circuit. There is a set of parallel edges between v_2 and v_3. This is also a circuit. Remove one of the edges. Edges (v_4, v_2), (v_2, v_3) and (v_3, v_4) form a circuit. Remove an edge say (v_3, v_4) from this circuit. What we have is spanning tree T_1 in figure 12.3 (b).

We now discuss some elementary properties of a spanning tree.

Theorem 12.1

Every connected graph has at least one spanning tree.

This is evident from the previous discussion of finding a spanning tree in a graph.

An edge in a spanning tree is called as branch and the edges not in the spanning tree are called chords. Refer figure 12.3 (a) and the spanning tree T_1. The branches of this spanning tree are (v_4, v_2), (v_2, v_3) (one of the parallel edges) and (v_3, v_2). Chords are self loop at v_2, (v_1, v_2), (v_3, v_4) and one of the parallel edges between v_1 and v_3. The number of vertices in the graph is 4. The number of edges is 7. The number of branches is 3 and the chords are 4 in number. The following theorem is a formal statement of these details.

Theorem 12.2

With respect to any of its spanning trees, a connected graph of n vertices and e edges has n-1 tree branches and e-n+1 chords.

This has been verified in figure 12.3 (a) in the previous paragraph.

12.4 MINIMUM WEIGHT SPANNING TREE

As discussed in the previous section a spanning tree is a minimally connected sub-graph of a graph. If there are real numbers associated with edges we call such a graph as weighted graph. A spanning tree of a weighted graph is a weighted tree. The weight of the tree is the sum of weights of all edges in the tree. We already discussed that a graph can have many spanning trees and each having different weights. In this section we give examples of weighted graphs and find some weighted spanning trees of the graphs. Figure 12.5 below has some weighted graphs and spanning trees with associated weights.

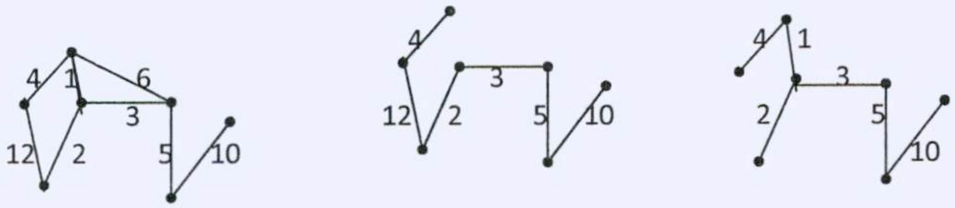


Fig 12.5 (a): Weighted graph (b): Spanning tree T_1 (c): Spanning tree T_2

The spanning tree in figure 12.5 (b) has weight 4+12+2+3+5+10 = 36 and the spanning tree in 12.5 (c) has weight 4+1+2+3+5+10 = 25. There may be many more spanning trees each with their own weight. A spanning tree with minimum weight is called ***minimum weight spanning tree or shortest spanning tree or shortest distance spanning tree or minimal spanning tree***. Often this minimal spanning tree is of interest. One possible application of the shortest spanning tree is as follows: Suppose that we are to connect n cities 1, 2, 3, …, n through a network of roads. The cost of building road between city i and city j be c_{ij}. These are weights of the network of roads, which is our graph. The question is 'what is the minimum expense of connecting all cities by a network of roads?' This can be solved by finding minimal spanning tree. This sub-graph connects all cities and at the same time cost of this network is least.

12.4.1 ALGORITHMS TO FIND MINIMUM WEIGHT SPANNING TREE

Here we discuss two algorithms to find minimum weight spanning tree one proposed by Kruskal and the other by Prim.

Kruskal's method

List all edges of the graph in the order of non-decreasing weights. Pick edges (one at a time from this list) corresponding to these weights and add them to the partial tree if it does not form a cycle with previously selected edges. Stop selection once you have collected n-1 edges (assuming graph has *n* vertices). The edges selected will form a spanning tree and has minimum weight.

Prim's method

This algorithm does not require ordering of edges according to weights. Also a check on whether a cycle is formed is not needed, as proposed by Kruskal. Suppose that the graph has *n* vertices. Prim's method requires you to tabulate the weights of edges in an *n* x *n* array (like adjacency matrix; but entries are not binary. They are weights of edges) called weight matrix. Diagonals in this matrix are blank. Note that even if there is self loop with least weight we won't select it in the tree because it forms cycle. So the diagonal elements in the weight matrix are left blank. Also it is evident that the matrix is symmetric. Set the weights of the non-existent edges to be infinity. Start from vertex 1 and connect to its nearest vertex say *i*. The vertices in the tree are 1 and *i* and the only edge is (1, *i*). Next find a vertex nearest to 1 or *i*, say *j* (assume (*i*, *j*) is smallest weights of all edges incident on 1 and *i*) and make a connection from *i* to *j* in the tree. Now, the tree has vertices 1,*i* and *j* and edges (1,*i*) and (*i*,*j*). As we always add a new vertex to the tree, checking for cycle formation is not needed. Continue this process until all vertices are included in the tree. What we have then is a minimum weight spanning tree.

Let us run (hand simulate) these algorithms on a graph given in figure 12.6.

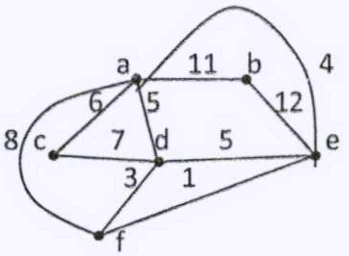


Fig 12.6: Graph G of 6 vertices *a* to *f* and 10 edges

Kruskal's method

As a first step we order the edges according to their weights. The order is {(e,f), (d,f), (a,e), (a,d), (d,e), (a,c), (c,d), (a,f), (a,b), (b,e)} with weights {1, 3, 4, 5, 5, 6, 7, 8, 11,12}

The table below shows selection of edges from the list above that makes up the spanning tree. One edge from the list is added to the tree at a time.

Edge	Weight	Total weight so far
(e,f)	1	1
(d,f)	3	4
(a,e)	4	8
(a,d) – not selected.	-	8
(d,e)-not selected	-	8
(a,c)	6	14
(c,d)-not selected	-	14
(a,f)-not selected	-	14
(a,b)	11	25

Spanning tree is complete as five edges (the graph has 6 vertices) are selected already and its weight is 25. The edges in the spanning tree are (e,f), (d,f), (a,e), (a,c) and (a,b). The spanning tree is shown in figure 12.7.

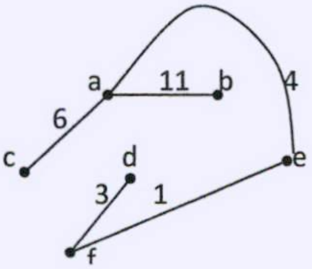


Fig 12.7: Kruskal's spanning tree

Prim's method

Here we need to prepare a matrix of weights.

$$\begin{array}{c|cccccc|}
 & a & b & c & d & e & f \\
a & - & 11 & 6 & 5 & 4 & 8 \\
b & 11 & - & \infty & \infty & 12 & \infty \\
c & 6 & \infty & - & 7 & \infty & \infty \\
d & 5 & \infty & 7 & - & 5 & 3 \\
e & 4 & 12 & \infty & 5 & - & 1 \\
f & 8 & \infty & \infty & 3 & 1 & -
\end{array}$$

Begin the tree with vertex *a* and add one new vertex to the tree at a time. The order of addition of vertices is shown in the table below.

Vertices in the tree	Min weight edge and weight	Total weight so far
a	(a,e): 4	4
a,e	(e,f): 1	5
a,e,f	(d,f): 3	8
a,e,f,d	(a,c): 6	14
a,e,f,d,c	(a,b): 11	25

Figure 12.8 is the spanning tree of Prim's method.

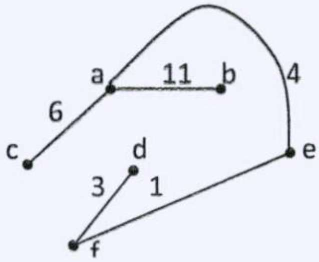


Fig 12.8: Spanning tree of Prim's method

Note that both the methods have generated the same spanning tree; this need not be so in all cases. However, the total weight of both the trees will be the same.

12.5 SEARCHING GRAPHS

In this section we discuss two powerful techniques to systematically traverse all edges of a given graph such that each edge is traversed only once and each vertex is visited at least once. This search procedure is useful for answering many questions about the graph such as connectedness, separability, planarity, etc. The two procedures are discussed in the flowing sub sections.

12.5.1 DEPTH FIRST SEARCH

In depth first search method, we traverse edges by moving from a vertex along a new edge to next vertex (or same vertex if self loop is traced) and repeat the above step until no more edges are left. This method of traversing the graph is called depth first search. The outline of the search algorithm is given below.

Algorithm DFS

Input: Adjacency matrix/edge list, number of edges *num-edge*

Output: Ordered set of edges

```
1. Select a vertex to start say v
2. For i=1 to num-edge
3. edge(i)=' '   // Array edge will give us the order in which edges are traversed in DFS
4. edge-count =0
5. If edge-count = num-edge then Output edge and exit
6. If there is a new (not in edge array) edge (v, x) or (x, v) incident on v then
        7. Move to the vertex x
        8. v← x
        9. edge-count=edge-count+1
        10. edge (edge-count) = (x, v)
        11. Go to step 5
12. Else (v is a dead end and hence back track)
        13. Else v← u where u is the vertex from where we reached v; Go to step 5.
```

Examples

Consider the graph in figure 12.9. Suppose we start at vertex a.

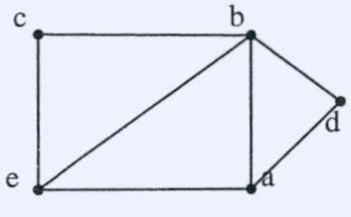


Fig 12.9

One order of traversal is (a, e), (e, b), (b, a), (a, d), (d, b), (b, c), (c, e). Here the start vertex is *a*.

Consider the graphs in figures 12.10 and 12.11. Both are trees of three vertices. In the graph of figure 12.10 the DFS traverses the edges (a, b), (b, c) and (back track to b) (b, d). In the figure 12.11 DFS when it starts at a, traversal is in the order (a, c), (c, b), (b, d); whereas with the start vertex *c*, the traversal is in the order (c, a), (back track to c) (c, b), (b, d).

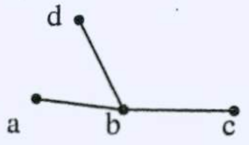


Fig 12.10

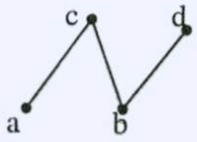


Fig 12.11

12.5.2 BREADTH FIRST SEARCH

In breadth first search, once at a vertex *v* we scan all edges incident on v and then move to an adjacent vertex *w*. At *w* we scan all edges incident on *w* (and those not traversed) and this process continues until all edges are scanned.

Algorithm BFS

Input: Adjacency matrix/list of edges, number of edges *num-edge*

```
1. Select a vertex to start say v
2. For i=1 to num-edge
3. edge(i) = ' '    // Array edge will give us the order in which edges are traversed in BFS
4. edge-list = null  //list of traversed edges is empty
5. edge-count = 0
6. If edge-count=num-edge then
      7. Output edge and exit
8. While x is adjacent to v and (v, x) or (x, v) not in edge-list
      9. Traverse edge (v, x)
      10. Add (v, x) to edge-list
      11. edge-count=edge-count+1
      12. edge(edge-count)=(v, x)
      while at step 8 ends
```

13. Select *w* adjacent to *v* so that there is an edge (w, x) not in edge list.

14. v← w

15. Go to step 6

Examples

Consider the graph in figure 12.9. Suppose we start at vertex *a*. The traversal order is (a, b), (a, d), (a, e), (b, d), (b, e), (b, c), (c, e)

In graphs of figure 12.10 with the start vertex *b* the order of traversal is (b, a), (b, c), (b, d). If the start vertex is *a* then order of traversal is (a, b), (b, c), (b, d). In the graph of figure 12.11 if we start at vertex *b* the traversal is (b, c), (b, d), (c, a).

12.6 SUMMARY

The unit began with discussion on tree and its properties. Spanning tree of any graph is introduced next. For a weighted graph each spanning tree will have varying weights. Two algorithms to find the minimum weight spanning tree are discussed. Finally in the last section the search methods depth first and breadth first are describes in detail.

12.7 KEYWORDS

Tree, Spanning tree, Weighted graph, Minimum weight spanning tree, Kruskal and Prim's methods, Depth first traversal, Breadth first traversal

12.8 QUESTIONS

1. Define a tree
2. Enumerate the properties of trees
3. Verify all properties in various example trees.
4. Define and provide examples of spanning trees.
5. What is weighted graph? Draw some and find the weights of each.
6. What is minimum weight spanning tree? Find this in each of the graph in the previous question.
7. Mention some applications of search methods.

8. Explain the two search procedures with examples.

12.9 REFERENCES

1. Narsingh Deo, Graph Theory with applications to Engineering and Computer Science, PHI
2. J.P.Tremblay, R.Manohar, Discrete Mathematical Structures with applications to Computer Science, TATA McGRAW-HILL
3. Dr. N.G.Goudru, Discrete Mathematical Structures, Himalaya Publishing House
4. Bernard Kolman, Robert C. Busby, Sharon Cutler Ross, Discrete Mathematical Structures, PEARSON Education

MODULE 4: Algebraic Structures

UNITS: 13 to 16

UNIT-13: INTRODUCTION TO GROUP THEORY

Structure

13.0 Objectives

13.1 Introduction

13.2 Semigroups

13.3 Monoids

13.4 Groups

13.5 Solved problems

13.6 Summary

13.7 Keywords

13.8 Questions

13.9 References

13.0 OBJECTIVES

When you go through this unit, you will be able to

- ✓ Explain semigroup, monoid and group;
- ✓ Give an account of the properties of a group;
- ✓ Analyze some theorems on group.

13.1 INTRODUCTION

Semigroups are the simplest algebraic structures which satisfy the properties of closure and associativity. They are very important in the theory of sequential machines, formal languages and in certain applications relating to computer arithmetic such as multiplication.

A monoid in addition to being a semigroup, also satisfies the identity property. Monoids are used in a number of applications, but most particularly in the area of syntactic analysis and formal languages.

Groups are monoids which also possess the inverse property. The application of group theory is important in the design of fast adders and error correcting codes.

13.2 SEMIGROUPS

Definition: An n-ary operation is a mapping f: $X^n \rightarrow X$ and n is called the order of the operation. For n=1, f: $X \rightarrow X$ is called a unary operation. For n=2 it is called a binary operation.

Definition: Let X be a set and f: $X \times X \rightarrow X$ be a mapping. Then f is called a binary operation on X. A binary operation is denoted by the symbol *.

For x, $y \in X$, if $x*y \in X$, then * is a binary operation.

Properties of Binary Operation:

- A binary operation * is said to be associative if for every x, y, $z \in X$, i.e., $(x*y)*z=x*(y*z)$
- Let * be a binary operation on X. If there exists an element $e \in X$ such that $a*e = e*a = a$, $\forall a \in X$, then e is called the identity element.
- Let * be a binary operation on X with the identity e. If there exists an element $a^{-1} \in X$ such that $a*a^{-1} = a^{-1}*a = e$, then a^{-1} is called the inverse element of a.
- A binary operation * is said to be commutative if for every x, $y \in X$, $x*y=y*x$.

Definition: A non-empty set G together with an associative binary operation * is called a semigroup. It is denoted by $(G, *)$. In other words, $(G, *)$ is called a semigroup if for all a, b, $c \in G$, $(a * b)*c = a*(b*c)$.

Example 1: Let the binary operation * be defined by $x*y= xy$ on the set of all integers Z. Show that (Z, *) is a semigroup.

Solution: We know that Z= {…-2,-1, 0, 1, 2….}

For -3,-2,-1 $\in$ Z

$(-3*-2)*(-1) = 6*(-1) = -6 \in Z$

$-3*(-2*-1) = -3*(2) =-6 \in Z$

Thus, for any x, y, $z \in Z$, $(x*y)*z = x*(y*z)$

So, the binary operation * is associative

Thus, $(Z, *)$ is a Semi group.

Example 2: Let the binary operation * be defined by $x*y= xy +2y$ on the set of all real numbers R. Is $(R, *)$ a semigroup?

Solution: For $-2,-3,-4 \in R$

$$
\begin{aligned}
(-2*-3)*(-4) &= ((-2)(-3) + 2(-3))*(-4) \\
&= (6-6)*(-4) \\
&= 0*(-4) \\
&= (0)(-4) + 2(-4) \\
&= 0-8
\end{aligned}
$$

$(-2*-3)*(-4) = -8$ ------------- (1)

$$
\begin{aligned}
(-2)*(-3*-4) &= (-2)*((-3)\ (-4) +2(-4)) \\
&= (-2)*(12-8) \\
&= (-2)*(4) \\
&= (-2)\ (4) + 2(4) \\
&= -8+8
\end{aligned}
$$

$(-2)*(-3*-4) = 0$ ------------- (2)

From (1) & (2)

$(-2*-3)*(-4) \neq (-2)*\ (-3*-4)$

For $x, y, z \in R$, $x*(y*z) \neq (x*y)*z$

So the binary operation * is not associative

Hence $(R, *)$ is not a semi-group.

Example 3: Show that the set of all natural numbers is a semigroup under the binary operation addition '+'.

Solution: We know that the set of all natural numbers is $N = \{1, 2, 3, \ldots\}$

For $3,2,1 \in N$

$(3 + 2) + 1 = 5 + 1 = 6 \in N$

$3 + (2 + 1) = 3 + 3 = 6 \in N$

Thus, for any $x, y, z \in N$, $(x*y)*z = x*(y*z)$

So, the binary operation * is associative

Thus, $(N, +)$ is a Semi group.

13.3 MONOIDS

Definition: A **monoid** is a semigroup with identity. In other words a non-empty set G, together with a binary operation * is called a monoid if

(i) * is associative

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

(ii) $\exists$ an element $e \in G$ such that

$$a * e \ = e * a = a, \quad \forall\, a \in G$$

Example 4: Show that the set of all integers is a monoid under ordinary multiplication "."

Solution: We know that $Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

(i) For $-3, -2, 1 \in Z$

$(-3 \,.\, -2) \,.\, 1 = 6 \,.\, 1 = 6 \in Z$

$(-3) \,.\, (-2 \,.\, 1) = (-3).(-2) = 6 \in Z$

Thus, for any $x, y, z \in N$, $(x*y)*z = x*(y*z)$

So, the binary operation * is associative.

(ii) 1 is the identity element

$1.\,x = x.1 = x, \quad \forall x \in Z.$

Therefore $(Z, .)$ is a monoid.

Example 5: Let Z^+ denote the set of all positive integers and the binary operation * be defined by $x * y = \max\{x, y\}$. Is $(Z^+, *)$ a monoid?

Solution: We know that $Z^+ = \{1, 2, 3\ldots.\}$

For $x, y, z \in Z^+$

$(x * y)*z = (\max\ \{x, y\})*z$

$(x * y) *z = \max\ \{x, y, z\} \rightarrow (1)$

$x*(y*z) = x*(\max\{y, z\})$

$x*(y*z) = \max\{x, y, z\}$

Hence $(x*y)*z = x*(y*z)$

So the binary operation * is associative

Now $1 \in Z^+$ acts as identity element

For $x \in Z^+$, $1 * x = \max\{1, x\} = x$

$$x * 1 = \max\{x, 1\} = x$$

Hence 1 is identity element

Therefore $(Z^+, *)$ is a Monoid.

Note: If binary operation is addition +, then 0 is the identity element.

13.4 GROUPS

Definition: A non empty set G together with a binary operation * is called a group if the following axioms are satisfied.

(i) Associative axiom.

$(a*b)*c = a*(b*c)$ for all $a, b, c \in G$

(ii) Identity axiom.

There exists an element $e \in G$ such that

$$a * e = e * a = a, \qquad \forall\ a \in G$$

(iii) Inverse axiom.

For each $a \in G$, there exists $a^{-1} \in G$ such that

$a * a^{-1} = a^{-1} * a = e$

Commutative group:

A group $(G, *)$ is called commutative (abelian)

if $a*b = b*a \qquad \forall\ a, b \in G$.

Example 6: Show that the set of all integers is an abelian group under addition '+'.

Solution: We know that $Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

(i) For $-3, -2, 1 \in Z$

$((-3)+(-2))+1=(-5)+1=-4 \in Z$

$(-3)+((-2)+1)=(-3)+(-1)=-4 \in Z$

Thus, for any $x, y, z \in Z$, $(x+y)+z=x+(y+z)$

So, the binary operation + is associative.

(ii) 0 is the identity element

$0+x=x+0=x, \quad \forall\ x \in Z.$

(iii) For any $x \in Z$, there exists an element $-x \in Z$ such that

$x+(-x)=(-x)+x=0.$

(iv) For $x, y \in Z$, $x+y=y+x$.

Therefore $(Z, +)$ is an abelian group.

Example 7: Show that the set of all positive integers is not a group under ordinary multiplication.

Solution: We know that $Z^+ = \{1, 2, 3, \ldots\}$

(i) For any $x, y, z \in Z^+$, $(x.y).z = x.(y.z)$

So, the binary operation . is associative.

(ii) 1 is the identity element

$1.x = x.1 = x, \quad \forall\ x \in Z^+.$

(iii) For $2 \in Z^+$, ½ does not belong to Z^+.

Thus for any $x \in Z^+$ with $x \neq 1$, $1/x \notin Z^+$.

So, inverse axiom is not satisfied.

Therefore $(Z^+, .)$ is not a group.

Example 8: Show that the set of all non-zero real numbers R is an abelian group under the binary operation * defined by $a * b = ab/2$.

Solution:

(i) For any $x, y, z \in R$, $(x*y)*z = (xy/2)*z = xyz/4$.

$x*(y*z) = x*(yz/2) = xyz/4$.

Hence $(x*y)*z = x*(y*z)$.

So, the binary operation * is associative.

(ii) $2 \in R$ is the identity element

For, $2 * x = 2x/2 = x$.

$x * 2 = x2/2 = x, \quad \forall\ x \in R$.

(iii) If $x \in R$, then $4/x$ is the inverse of x.

For, $x*4/x = x(4/x)/2 = 2$

$4/x*x = (4/x)x/2 = 2$.

Therefore $(R, *)$ is a Group.

For any $x, y \in R$, $x*y = xy/2 = yx/2 = y*x$.

Therefore the binary operation * is commutative.

Thus $(R, *)$ is an abelian group.

Theorem 13.1:

If $(G, *)$ is a group, then

(1) The identity of G is unique.

(2) For each $a \in G$, a^{-1} is unique.

(3) $(a^{-1})^{-1} = a$, for $a \in G$.

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

Proof:

(i) If possible, let e_1 and e_2 be two identities of G.

If e_1 is the identity then $e_2 * e_1 = e_1 * e_2 = e_2$

If e_2 is the identity then $e_1 * e_2 = e_2 * e_1 = e_1$

$\therefore\ e_1 = e_1 * e_2 = e_2$

$\therefore\ e_1 = e_2$

(ii) Suppose a and b are two inverses of c. Let e be the identity of G. Then,

$a * c = c * a = e$ -------(1)

$b*c = c* b = e$ --------(2)

$b = b*e$, by identity law

$b = b* (c*a)$, by (1)

$b = (b*c)* a$, by associative law

$= e * a$, by (2)

$= a$, by identity law.

(iii) Now,

$(a^{-1})^{-1}* a^{-1} = e$ [By definition]

$((a^{-1})^{-1}*a^{-1})*a = e*a$ [By multiplying on the right by a]

$(a^{-1})^{-1}*(a^{-1}*a) = a$ [By associative and identity axioms]

$(a^{-1})^{-1} * e = a$ [By inverse axiom]

$(a^{-1})^{-1} = a$ [By identity axiom]

$\therefore$ Inverse of a^{-1} is a.

(iv) Let a, $b \in G$. Let a^{-1} and b^{-1} be inverses of a and b.

Consider,

$(a*b) * (b^{-1}*a^{-1}) = a*(b*(b^{-1}*a^{-1}))$ [By associative axiom]

$= a*((b*b^{-1})*a^{-1})$ [By associative axiom]

$= a*(e*a^{-1})$ [By inverse axiom]

$= a*a^{-1}$ [By identity axiom]

$= e$ [By inverse axiom]

$\therefore (a*b)^{-1} = b^{-1} *a^{-1}$

Theorem 13.2: If a, b, c are elements of a group G, then

i) $ab = ac$ implies $b = c$ (left cancellation law)

ii) $ba = ca$ implies $b = c$ (right cancellation law)

Proof:

i) Suppose that $ab = ac$

Multiplying on the left by a^{-1}, we get

$a^{-1}(ab) = a^{-1}(ac)$

$(a^{-1}a)b = (a^{-1}a)c$ [By associative axiom]

$(e)b = (e)c$ [By inverse axiom]

$b = c$ [By identity axiom]

ii) Suppose that $ba = ca$

Multiplying on the right by a^{-1}, we get

$(ba)a^{-1} = (ca)a^{-1}$

$b(aa^{-1}) = c(aa^{-1})$ [By associative axiom]

$b(e) = c(e)$ [By inverse axiom]

$b = c$ [By identity axiom]

Theorem 13.3: If a and b are elements of a group G, then

i) The equation $ax = b$ has a unique solution in G

ii) The equation $ya = b$ has a unique solution in G.

Proof: (i) We observe that $a(a^{-1}b) = (aa^{-1})b = eb = b$

So, $x = a^{-1}b$ is a solution of $ax = b$.

To prove the uniqueness, let x_1 and x_2 be two solutions of the equation $ax = b$.

Thus, $ax_1 = b$ and $ax_2 = b$.

So, $ax_1 = ax_2$

$x_1 = x_2$, by left cancellation law.

Hence, the equation $ax = b$ has a unique solution.

(ii) Similarly, we observe that $(ba^{-1})a = b(a^{-1}a) = be = b$

So, $y = ba^{-1}$ is a solution of $ya = b$.

To prove the uniqueness, let y_1 and y_2 be two solutions of the equation $ya = b$.

Thus, $y_1a = b$ and $y_2a = b$.

So, $y_1a = y_2a$.

$y_1 = y_2$, by right cancellation law.

Hence, the equation $ya = b$ has a unique solution.

Example 9: Let Z be set of all integers with the binary operation * defined by $a*b = a + b + 1$ for $a, b\in Z$. Then show that $(Z, *)$ is an abelian group.

Solution: For $a, b, c \in Z$, $(a*b)*c = (a+b+1)*c$

$$= (a+b+1) + c + 1$$

$$= a+b+c+2.$$

$$a*(b*c) = a*(b+c+1)$$

$$= a+(b+c+1)+1$$

$= a+b+c+2$

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

$\therefore$ * is associative.

Let $e\in Z$ be such that $e*a = a$

$\Rightarrow e + a + 1= a$

$\Rightarrow e = -1$

$\therefore$ Identity of (Z, *) is -1

For $a\in Z$, let $b\in Z$ be the inverse of a, then

$a*b = -1$

$\Rightarrow a + b + 1 = -1$

$\Rightarrow b = -a-2$

$\therefore$ Inverse of a is $-a-2$

Also, $a*b = a + b + 1$

$= b + a + 1$

$= b *a$

$\therefore$(Z, *) is an abelian group.

13.5 SOLVED PROBLEMS

1. Determine whether the set $G = \{1, w, w^2)$, where w is the cube root of unity forms a group under multiplication.

Solution: The multiplication table for G is given by

×	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Table 13.1

All the entries in the table belong to the set G. Therefore closure axiom holds.

For $a \in G$, $a*1 = 1*a = a$. Therefore 1 is the identity element.

Inverse of 1, w, w^2 are 1, w^2, w respectively.

All the entries are symmetric with respect to the diagonal. Therefore the commutative axiom is satisfied.

Thus $(G, \times)$ is an abelian group.

2. Let $G = \{1,-1\}$. Determine whether G is a group under multiplication of real numbers.

Solution: Construct the multiplication table,

×	1	-1
1	1	-1
-1	-1	1

Table 13.2

Clearly from the table,

(i) '×' is associative.

(ii) 1 is the identity element

(iii) The inverse of 1 is itself; -1 is the inverse of itself.

Hence, $(G, \times)$ is a group.

3. Is the set $\{1, 2, 3, 4, 5\}$ a group under addition modulo 6?

Solution: Construct the addition table,

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

Table 13.3

From the table, given composition is not binary, as $5 + 1 = 0$ but $0 \not\subset \{1, 2, 3, 4, 5\}$.

Therefore the given set is not a group.

4. Let $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \neq 0 \in R \right\}$. Is G a group under matrix multiplication?

Solution: Let $A = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G$ with $a, b \neq 0$ in R.

Consider,

$$AB = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in G \text{ as } ab \neq 0.$$

Therefore G is closed w.r.t. matrix multiplication.

Similarly matrix multiplication is associative.

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity element. For $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ for any $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ in G.

Consider, $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

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

$$\Rightarrow ax = 1;\ x = 1/a$$

$\therefore \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix}$ is the inverse of $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

Also, $AB = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ba & 0 \\ 0 & 0 \end{pmatrix} = BA$

$\therefore$ G is an abelian group.

5. If $(G,*)$ is an abelian group, then for all $a, b \in G$ show that $(a*b)^n = a^n * b^n$.

Solution: We prove the result by induction on n.

If n=1, then $(a*b)^1 = a*b$ [trivial]

If n=2, then $(a*b)^2 = (a*b)*(a*b)$

$$\begin{aligned} &= a*(b*a)*b && \text{[By associative axiom]} \\ &= a*(a*b)*b && \text{[}G\text{ is abelian]} \\ &= (a*a)*(b*b) && \text{[By associative axiom]} \\ &= a^2*b^2 \end{aligned}$$

Result is true for n=2.

We assume that the result is true for n=m.

i.e. $(a*b)^m = a^m * b^m$

Consider ,

$(a*b)^{m+1}=(a*b)^m*(a*b)$

$=(a^m*b^m)*(a*b)$ [By the assumption]

$=(a^m*b^m)*(b*a)$ [G is abelian]

$=a^m*(b^m*b)*a$ [By associative axiom]

$=a^m*(b^{m+1})*a$

$=a^m*(b^{m+1}*a)$ [By associative axiom]

$=a^m*(a*b^{m+1})$ [G is abelian]

$=(a^m*a)*b^{m+1}$ [By associative axiom]

$=a^{m+1}*b^{m+1}$

$\therefore$ Result is true for $n=m+1$. Thus by induction result is true for all n.

6. Show that in a group $(G,*)$, if for $a, b\in G$, $(a*b)^2=a^2*b^2$ then $(G,*)$ must be abelian.

Solution: Given: $(a*b)^2=a^2*b^2$

$\Rightarrow (a*b)*(a*b)=(a*a)*(b*b)$

$\Rightarrow a*(b*a)*b=a*(a*b)*b$ [By associative axiom]

$\Rightarrow b*a=a*b,$ [By cancellation law]

$\therefore$ G is abelian.

7. Show that if every element in a group is its own inverse, then the group G must be abelian.

Solution: Let $a, b\in G \Rightarrow ab\in G$

We have, $a=a^{-1}$, $b=b^{-1}$, $ab=(ab)^{-1}$ [Given: Every element is its own inverse]

$\Rightarrow a^2=e$, $b^2=e$, $(ab)^2=e$

Consider, $(ab)^2=e$

$\Rightarrow (ab).(ab)=e$

$\Rightarrow a(ba)b=e$ [By associative axiom]

$\Rightarrow a(a(ba)b)b= aeb$ [Multiplying by a on the left and by b on the right]

$\Rightarrow (aa)(ba)(bb)=ab$ [By associative axiom]

$\Rightarrow a^2(ba)b^2=ab$

$\Rightarrow e(ba)e=ab$

$\therefore ba=ab$

$\therefore G$ is abelian.

13.6 SUMMARY

A binary operation is a rule that assigns to each ordered pair of elements of a set, a unique element of it.

A non-empty set together with an associative binary operation is called a semigroup.

A monoid is a semigroup with identity.

A non empty set together with a binary operation is called a group if it satisfies associative, identity and inverse axioms.

Properties of a group: If $(G, *)$ is a group, then

(1) The identity of G is unique.

(2) For each $a \in G$, a^{-1} is unique.

(3) $(a^{-1})^{-1} = a$, for $a \in G$.

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

Theorem: If a, b, c are elements of a group G, then

i) $ab = ac$ implies $b = c$ (left cancellation law)

ii) $ba = ca$ implies $b = c$ (right cancellation law)

Theorem: If a and b are elements of a group G, then

i) The equation $ax = b$ has a unique solution in G

ii) The equation $ya = b$ has a unique solution in G.

13.7 KEYWORDS

Semigroup, monoid, group..

13.8 QUESTIONS

1. Define $x \times y = x - y$ on the set of all +ve integers. Is * a binary operation?

2. Show that the set N of natural numbers is a semigroup under the operation $x*y=max\{x, y\}$. Is it a monoid?
3. Let S be a finite set and $P(S)$ be the power set of S. Determine whether $(P(S),□)$ is a semigroup or a monoid.
4. Determine whether $(Z^+,*)$ where $x*y=x+y-xy$ is a semigroup or a monoid.
5. Determine whether the set of even integers with the binary operations $x*y=\frac{xy}{2}$ forms a semigroup or a monoid.
6. Determine whether the set Z with the binary operation *, ordinary multiplication is a group.

13.9 REFERENCES

1. Discrete mathematics for computer science, by Kolman, Busby and Ross, PHI publications.
2. Discrete Mathematical Structures, by N. G. Goudru, Himalaya Publishing House.
3. Discrete mathematical structures with applications to computer science, by Tremblay and Manohar (McGraw-Hill publications).

4. Topics in Algebra, by I. N. Herstein, Wiley eastern Ltd.

UNIT-14: SUBGROUPS

Structure

14.0 Objectives

14.1 Introduction

14.2 Subgroup

14.3 Cosets

14.4 Lagrange's Theorem

14.5 Normal subgroup

14.6 Solved problems

14.7 Summary

14.8 Keywords

14.9 Questions

14.10 References

14.0 OBJECTIVES

When you go through this unit, you will be able to

- ✓ Explain the subgroups and cosets;
- ✓ Analyse some theorems on subgroups and cosets;
- ✓ Give an account of the Lagrange's theorem;
- ✓ Explain the normal subgroup;
- ✓ Analyse some theorems on normal subgroups;

14.1 INTRODUCTION

Application of subgroups is in the construction of computer modules which perform group operations. Such modules are constructed by joining various subgroup modules that do operations in subgroups.

Every subset of a group need not be a subgroup. To find those subsets which can qualify to become subgroups is an interesting problem. An important relationship exists between the subgroups and the group itself. This relationship is explained by a theorem known as Lagrange's theorem. This theorem has important application in the development of efficient group codes required in the transmission of information.

14.2 SUBGROUP

Definition: A non-empty set H of a group G is called a subgroup if H itself is a group under the operation defined in G.

Any group G has at least two subgroups namely $\{e\}$, the set containing the identity element e and G itself. These two subgroups are called trivial subgroups.

Examples 1:

- Let $G = \{1, -1, i, -i\}$, a multiplicative group. Then $H = \{1,-1\}$ is subgroup of G.
- Set of all integers Z is a subgroup of the set of all rationals Q under addition.

Theorem 14.1:

A non-empty subset H of a group G is a subgroup of G if and only if

1) $a, b \in H$ implies that $ab \in H$.

2) $a \in H$ implies that $a^{-1} \in H$.

Proof: Let H be subgroup of G and $a, b \in H$

Now $a \in H$ and $b \in H \Rightarrow ab \in H$. (by the closure axiom in H, being a subgroup)

Since H is a subgroup, for any $a \in H \Rightarrow a^{-1} \in H$.

Conversely, suppose condition (1) and (2) holds. To prove that H is a subgroup of G, it is enough to prove that associative and identity axioms hold in H.

Each element of H is an element of G. Since associative axiom holds good in G, being a group. Thus associative law holds good for elements of H also.

Now for any $a \in H$ by condition (2), $a^{-1} \in H$ and by (1), $e = a.\ a^{-1} \in H$.

$\therefore e \in H$.

$\therefore H$ is a group. Since $H \subseteq G$, H is a subgroup of G.

Theorem 14.2: (Necessary and sufficient condition for the subgroup)

A non-empty set H of a group G is subgroup of G, if and only if $a, b \in H \Rightarrow ab^{-1} \in H$

Proof: Let H be subgroup of G and $a, b \in H$

Since H is a subgroup, for any $b \in H \Rightarrow b^{-1} \in H$.

Now $a \in H$ and $b^{-1} \in H \Rightarrow ab^{-1} \in H$. (by the closure axiom in H, being a subgroup)

Thus for $a, b \in H \Rightarrow ab^{-1} \in H$

Conversely, suppose $a, b \in H \Rightarrow ab^{-1} \in H$.

We prove that H is a subgroup of G.

Let $a \in H$ be arbitrary.

Given, $a \in H, b \in H \Rightarrow ab^{-1} \in H$.

Choose $b = a$, then $a \in H, a \in H \Rightarrow aa^{-1} = e \in H$.

Therefore identity element exists.

Now $e \in H, a \in H \Rightarrow e\, a^{-1} = a^{-1} \in H$

Hence the inverse of every element of H exists and belongs to H.

Let $a, b \in H \Rightarrow a \in H, b^{-1} \in H$.

$\Rightarrow a\,(b^{-1})^{-1} \in H$.

$\Rightarrow ab \in H$.

Therefore closure axiom is satisfied.

Since the binary operation is associative in G, it is associative in H also.

Thus H is a subgroup of G.

Example 2: Let $G = \{1, -1, i.\ -i\}$ be a multiplicative group. Show that $H = \{1, -1\}$ is a subgroup of G.

Solution: Clearly H□G and the multiplicative identity $1 \in H$

Now i) For $1, -1 \in H \Longrightarrow 1(-1) = -1 \in H$.

For $1, 1 \in H \Longrightarrow 1(1) = 1 \in H$.

$\therefore$ Condition (1) of theorem is satisfied.

ii) $1.1 = 1, \in$ the inverse of 1 is 1

$(-1) . (-1) = 1 \in$ the inverse of -1 is -1

for every $a \in H$, $a^{-1} \in H$

$\therefore$ Condition (2) of theorem is satisfied.

H is a subgroup of *G*

Example 3: Prove that the set of all integers *Z*, is a subgroup of set of all rationals *Q*, under addition.

Solution: Clearly *Z* is a subset of *Q*

The identity element 0 of *Q* belongs to *Z*

Now i) For *a, b*$\in Z$ ☒ $a+b \in Z$

ii) For every $a \in Z$, there exists $-a \in Z$ such that

$$a + (-a) = (-a) + a = 0$$

$\therefore$ By the theorem, *Z* is a subgroup of *Q*.

Example 4:

$$\text{Let } G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big/ \begin{matrix} a,b,c,d \in R \\ ad - bc \neq 0 \end{matrix} \right\}$$

$$\text{and } H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \Big/ \begin{matrix} a,b,d \in R \\ ad \neq 0 \end{matrix} \right\} \text{ then show that}$$

H is a subgroup of *G* under multiplication,

Solution: Let $A=\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$, $B=\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ be two elements of *H*.

$$\text{Consider } AB = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix} \in H$$

Since, $a_1 d_1 \neq 0$ and $a_2 d_2 \neq 0$

$\Rightarrow (a_1a_2)\ (d_1d_2)= (a_1d_1)\ (a_2d_2) \neq 0$

For any $A=\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in H$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} ax+bz & ay+bw \\ dz & dw \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\Rightarrow \quad ax+bz=1,\ ay+bw=0,\ dz=0,\ dw=1$

Now, $d \neq 0$ as $ad \neq 0$

$\therefore dz=0 \quad \Rightarrow \quad z=0$

$\therefore ax+bz=1 \quad \Rightarrow \quad ax=1 \ \Rightarrow x=1/a$

$dw=1 \quad \Rightarrow w=1/d$

$\therefore ay+bw=0 \ \Rightarrow \quad y= -bw/a$

$= -b/a(1/d)$

$\therefore \quad y = -b/ad$

Inverse of $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is $\begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix}$

and, $ad \neq 0 \Rightarrow 1/ad \neq 0$

$\therefore \begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix} \in H$

$\therefore$ H is subgroup.

14.3 COSETS

Definition: Let H be a subgroup of G and $a \in G$. Then the set, $Ha = \{ha \,/\, h \in H\}$ is called the right coset of H generated by a. Similarly the set $aH = \{ah \,/\, h \in H\}$ is called the left coset of H generated by a.

Note: Since $eH=H=He$, we see that H itself is a right as well as a left coset. If the group operation is "addition" we define the right coset of H in G by $H+a=\{h+a \, / \, h\in H\}$. Similarly for the left coset of H in G by $a+H=\{a+h \, / \, h\in H\}$. Observe that cosets are not necessarily subgroups of G.

Example 5: Let $G=(Z,+)$ be the additive group of integers and $H=(2Z, +)$ the subgroup of even integers. Find the left cosets of H in G.

Solution:

The left cosets of H in G are,

$0+H=\{\ldots, 0+(-2), 0+0, 0+2, \ldots\}=\{\ldots, -2, 0, 2, \ldots\} = H$.

$1+H = \{\ldots, 1+(-2), 1+0, 1+2, \ldots\}=\{\ldots, -3, -1, 1, 3, \ldots\}$.

$2+H = \{\ldots,-4, -2, 0, 2, 4, 6 \ldots\}=H$.

$3+H=\{\ldots, -3, -1, 1, 3, \ldots\}$ and so on.

Notice that $2+H$ coincides with H, $3+H$ coincides with $1+H$, $4+H$ coincides with H, $5+H$ coincides with $1+H$ and so on. Hence there are only two distinct left cosets namely H and $1+H$.

Example 6: Let $G = \{1, -1, i, -i\}$ be a multiplicative group and $H=\{1, -1\}$ be a subgroup of G. Find the right cosets of H in G.

Solution: The right cosets are

$$H1 = \{1(1), -1(1)\}= \{1, -1\}=H.$$
$$H(-1)=\{1(-1), -1(-1)\}=\{-1, 1\}=H.$$
$$Hi=\{i, -i\}.$$
$$H(-i) = \{-i, i\}=Hi.$$

Note:

1) If G is abelian then right and left cosets of G coincide.
2) If $a \in H$, then $Ha=H$. If $a\in$ G such that $a\notin H$, then $Ha\neq H$.
3) H itself is a right coset and the number of elements in each right coset is the same as the number of elements in H.

Theorem 14.3: There is one-to-one correspondence between any two right cosets of a subgroup H of a group G.

Proof: Let $a, b\in G$. Let Ha and Hb be any two right cosets of H in G.

Define f: $Ha \rightarrow Hb$ by $f(ha) = hb$ $\forall$ $ha \in Ha$.

***f* is one-one:**

Let $h_1, h_2 \in H$

Then, $h_1a, h_2a \in Ha$

Now, $f(h_1a) = h_1b$, $f(h_2a)=h_2b$.

Suppose $f(h_1a) = f(h_2a)$

$\Rightarrow h_1b = h_2b$

$\Rightarrow h_1 = h_2$

$\Rightarrow h_1a = h_2a$.

$\therefore$ f is one-one .

***f* is onto:**

Let $hb \in Hb$ be arbitary.

$\Rightarrow h \in H$, then there exists $ha \in Ha$.

$\therefore f(ha) = hb$ by the definition of f.

$\therefore f$ is onto

This proves the theorem.

Theorem 14.4: Let H be a subgroup of G and $a, b \in G$. Then $Ha=Hb$ if and only if ab^{-1}□H

Proof: Let $Ha=Hb$.

Then there exist elements $h_1$and h_2 in H such that

$h_1a= h_2b$

$h_1^{-1}(h_1a) = h_1^{-1}(h_2b)$ [By multiplying on the right by h_1^{-1}]

$(h_1^{-1}h_1)a = (h_1^{-1}h_2)b$

$ea = (h_1^{-1}h_2)b$

$a = (h_1^{-1}h_2)b$

$ab^{-1} = [(h_1^{-1}h_2)b]\, b^{-1}$

$ab^{-1} = (h_1^{-1}h_2)(\, bb^{-1})$

$ab^{-1} = \ (h_1^{-1}h_2)e$

$ab^{-1} = \ h_1^{-1}h_2$

Since $h_1 \in H$, $h_1^{-1} \in H$. Also $h_2 \in H$

$h_1^{-1}h_2 \in H$, $ab^{-1} \in H$.

Conversely, suppose $ab^{-1} \in H$ for $a,b \in G$

Then $H=H(ab^{-1})$ [$H=Hh$ when $h \in H$]

$Hb=Hab^{-1}b$

$\Rightarrow Ha=Hb$.

Theorem 14.5: Any two left (right) cosets of a subgroup are either disjoint or identical.

Proof: Let H be any subgroup of G and let aH and bH be two left cosets of H in G.

Suppose that aH and bH are not disjoint.

Let $c\in aH \cap bH$. Then,

$c\in aH$ and $c\in bH$.

Then $c=ah$ for some $h\in H$ and $c= bh^1$ for some $h^1 \in H$.

$\Rightarrow ah=bh^1$

$\Rightarrow a=bh^1h^{-1}$

Since H is a subgroup, $h^1h^{-1} \in H$.

$\therefore a=bh_1$ for $h_1=h^1h^{-1}$.

$\therefore\ aH=(bh_1)H$.

$=b(h_1H)$

But, $h_1H = H$ [because $h_1\in H$]

$\therefore\ aH=bH$

Thus, $aH \cap bH = \phi$ or $aH=bH$

Theorem 14.6: Let H be a subgroup of a group G. Then G is equal to the union of all right cosets of H in G i.e. $G=\bigcup_{a\in G} Ha$

Proof: Since G is a group and H is a subgroup, for $a\in G$, $Ha \subseteq G$.

$\therefore \bigcup_{a\in G} Ha \subseteq G$ -------------- (1)

Let $x \in G$ be arbitrary.

Then, $x.e = x \in Hx$

$\therefore\ x \in \bigcup_{a\in G} Ha$

$\therefore G \subseteq \bigcup_{a\in G} Ha$ --------------(2)

From (1) and (2)

$G{=}\bigcup_{a\in G} Ha$

Note: Similarly it can be proved that G is also equal to the union of left cosets of H in G.

Coset decomposition:

We have seen that any two left (right) cosets are either disjoint or identical. Also, the union of all left (right) cosets of a subgroup H of G is equal to G. Hence the set of all left (right) cosets of a subgroup H constitutes a decomposition of G into mutually disjoint classes. As a matter of fact, the partition of a group G into mutually disjoint classes known as "cosets" is accomplished by defining an equivalence relation in G known as **Congruence relation.**

Relation of congruence modulo a subgroup *H* in a group *G*:

Definition: If H is a subgroup of a group G and a, b are two elements of G such that $ab^{-1} \in H$. Then we say that a is congruent to b modulo H, and write as $a \equiv b\ mod(H)$.

Theorem 14.7: If H is a subgroup of G with $a,\ b \in G$ then $a \equiv b\ mod(H)$ if and only if $ab^{-1} \in H$ is an equivalence relation.

Proof: The identity element $e \in H$ (H is a subgroup)

$aa^{-1} = e \in H$, for $a \in G$,

Thus $a \equiv a(mod\ H)$, for $a \in G$

$\equiv$ is reflexive.

Suppose $a \equiv b(mod\ H)$, for $a,b \in G$ *then* $ab^{-1} \in H$.

$(ab^{-1})^{-1} \in H$ [H is a subgroup]

$(b^{-1})^{-1}a^{-1} \in H$

$ba^{-1} \in H$

$b \equiv a(mod\ H)$, for $a, b \in G$.

$\equiv$ is symmetric.

Suppose $a \equiv b(mod\ H)$, $b \equiv c(mod\ H)$, for $a, b, c \in G$

$ab^{-1} \in H$ and $bc^{-1} \in H$

$(ab^{-1})(bc^{-1}) \in H$ [H is a subgroup]

$a(b^{-1} b)c^{-1} \in H$

$ac^{-1} \in H$

$a \equiv c(mod\ H)$

$\equiv$ is transitive.

$\equiv$ is an equivalence relation.

Definition: The number of distinct left (right) cosets of H in G is called the index of H in G denoted by $[G:H]$

14.4 LAGRANGE'S THEOREM

Theorem 14.8: If G is a finite group, and H is any subgroup of G, then the order of H divides the order of G.

Proof: Let $°(G)=n$ and $°(H)=m$. We consider the left coset decomposition of G relative to H.

First we show that every left coset aH for $a \in G$ has exactly m elements.

Let $H=\{h_1,h_2,\ldots,h_m\}$, h_i's are distinct.

Consider $aH=\{ah_1, ah_2, \ldots, ah_m\}$

ah_i's are distinct , for if $ah_i = ah_j$ for $i \neq j$.

$\Rightarrow h_i = h_j$, $i \neq j$ which is a contradiction.

$\therefore$ Every left coset aH has exactly m elements.

Since G is finite, the number of left cosets will also be finite. Let k be the number of distinct left cosets.

Then, $G = a_1H \cup a_2H \cup ... \cup a_kH$.

$\therefore$ the number of elements in G is equal to the number of elements in the k cosets. Since each coset contains m elements and there are k cosets, we get

$$n = km$$

i.e. $m|n$.

i.e. $o(H)|o(G)$.

14.5 NORMAL SUBGROUPS

Definition: A subgroup H of a group G is called a normal subgroup of G if and only if for every $x \in G$ and $h \in H$, $xhx^{-1} \in H$.

Theorem 14.9: A subgroup H of a group G is normal if and only if $xHx^{-1}=H$, $\forall\ x \in G$.

Proof: Suppose that $xHx^{-1}=H\ \forall\ x \in G$.

$\Rightarrow xHx^{-1} \subseteq H$, $\forall x \in G$

Thus for all $h \in H$, $xhx^{-1} \in H, \forall x \in G$.

$\therefore$ H is normal.

Conversely, let H be normal,

Then, $xHx^{-1} \subseteq H$, $\forall\ x \in G$--------------------------------(1)

and

$x^{-1}H(x^{-1})^{-1} \subseteq H$, $\forall x \in G$

i.e $x^{-1}Hx \subseteq H\ \forall x \in G$-------------------------------- (2)

Hence, $x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$

i.e. $H \subseteq xHx^{-1}$--- (3)

From (1) and (3)

$xHx^{-1}=H$, $\forall x \in G$.

Theorem 14.10: A subgroup H of a group G is a normal subgroup iff each right coset of H in G is a left coset of H in G.

Proof: Let H be normal subgroup of G.

Then, $xHx^{-1}=H \ \forall\, x \in G$. [By Theorem 2.4.1]

$\therefore\ (xHx^{-1})\, x=Hx \quad \Rightarrow xH = Hx\ \forall x \in G$

$\therefore$ Every left coset is a right coset.

Conversely, let every left coset be a right coset,

i.e. $xH = Hx\ \forall\ x \in G$

i. e. $(xH)x^{-1} = (Hx)x^{-1}$

i. e. $xHx^{-1}=H,\ \forall\ x \in G$.

Therefore H is normal in G. [By Theorem 2.4.1]

Theorem 14.11: The intersection of any two normal subgroup of a group is a normal subgroup.

Proof: Let N_1 and N_2 be two normal subgroups of G.

For $x \in N_1 \cap N_2$ and $g \in G$.

$\Rightarrow x \in N_1\ \&\ x \in N_2\ ,\ g \in G.$

$\Rightarrow g\ xg^{-1} \in N_1$ and $g\ xg^{-1} \in N_2$ ($\because N_1$ & N_2 are normal) .

$\therefore\ gx\ g^{-1} \in N_1 \cap N_2$

$\therefore N_1 \cap N_2$ is normal.

Theorem 14.12: If G is an abelian group, then every subgroup of G is a normal subgroup.

Proof: Let H be a subgroup of G. Let a□G be arbitrary and $h \in H$.Then $ha=ah$, so $Ha=aH$, for every a□G, which implies that H is a normal subgroup of G.

14.6 SOLVED PROBLEMS

1. If H_1 & H_2 are subgroups of G , show that $H_1 \cap H_2$ is also a subgroup of G. Show that in general $H_1 \cup H_2$ need not be subgroup of G except when $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Solution: Let $a, b \in H_1 \cap H_2$.

$\Rightarrow a, b \in H_1$ and $a, b \in H_2$.

$\therefore\ ab^{-1} \in H_1$ and $ab^{-1} \in H_2$ [as H_1 & H_2 are subgroups].

$\therefore ab^{-1} \in H_1 \cap H_2, \ \forall \, a, b \in H_1 \cap H_2$

$\therefore H_1 \cap H_2$ is a subgroup.

We now give an example to show that $H_1 \cup H_2$ is not a subgroup of G.

Let H_1=(2Z , +) , H_2=(3Z , +) , G=(Z, +). Then H_1 and H_2 are subgroups of G.

Clearly $2 \in 2Z$ and $3 \in 3Z$

But $3-2 = 1 \notin 2Z \cup 3Z$

$\therefore 2Z \cup 3Z$ is not a subgroup.

If $H_1 \subseteq H_2 \Rightarrow H_1 \cup H_2 = H_2$, a subgroup of G

If $H_2 \subseteq H_1 \Rightarrow H_1 \cup H_2 = H_1$, a subgroup of G

Suppose that $H_1 \cup H_2$ is a subgroup and $H_1 \not\subset= H_2$ and $H_2 \not\subset= H_1$, then

$H_1 \not\subset= H_2 \Rightarrow \exists \, a \in H_1$ such that $a \notin H_2$

$H_2 \not\subset= H_1 \Rightarrow \exists \, b \in H_2$ such that $b \notin H_1$

But, $a, b \in H_1 \cup H_2$

$\Rightarrow a - b \in H_1 \cup H_2$ ($\because H_1 \cup H_2$ is a subgroup)

$\Rightarrow a\text{-}b \in H_1$ or $a\text{-}b \in H_2$

Suppose $a\text{-}b \in H_1$, then $a\text{-}b \in H_1$ and $a \in H_1$

$\Rightarrow a\text{-}(a\text{-}b) \in H_1$

$\Rightarrow b \in H_1$, a contradiction.

Suppose $a\text{-}b \in H_2$, then $a\text{-}b \in H_2$ and $b \in H_2$

$\Rightarrow (a - b) + b \in H_1$

$\Rightarrow a \in H_2$, a contradiction.

$\therefore H_1 \cup H_2$ is a subgroup iff $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$

2. Find the left cosets of H= {0, 3} in the group (Z_6 , $+_6$) .

Solution: Z_6 = {0, 1, 2, 3, 4, 5 }

Left cosets of H in G are

$0+H=H$

$1+H=\{1, 4\}$

$2+H=\{2, 5\}$

$3+H=\{3, 0\}$

$4+H = \{4, 1\}$

$5+H = \{5, 2\}$

$\therefore$ Distinct left cosets of H in G are H, $1+H$, $2+H$.

3. Find the left cosets of $\{P_1, P_5, P_6\}$ in the group $\langle S_3, \bullet \rangle$

Solution: $S_3 = \{ P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$

$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$

Let $H = \{P_1, P_5, P_6\}$

Now left cosets of H in S_3 are,

$P_1 \bullet H = \{ P_1 \bullet P_1, P_1 \bullet P_5, P_1 \bullet P_6\}$

$= \{P_1, P_5, P_6\} = H$

$P_2 \bullet H = \{P_2 \bullet P_1, P_2 \bullet P_5, P_2 \bullet P_6\}$

$= \{P_2, P_3, P_4\}$

$P_3 \bullet H = \{P_3 \bullet P_1, P_3 \bullet P_5, P_3 \bullet P_6\}$

$= \{P_3, P_4, P_2\}$

$P_4 \bullet H = \{P_4 \bullet P_1, P_4 \bullet P_5, P_4 \bullet P_6\}$

$= \{P_4, P_2, P_3\}$

$P_5 \bullet H = \{P_5 \bullet P_1, P_5 \bullet P_5, P_5 \bullet P_6\}$

$= \{P_1, P_6, P_1\}$

$P_6 \bullet H = \{P_6 . P_1, \mathrm{P}_6 \bullet P_5, P_6 \bullet P_6\}$

$= \{P_6, P_1, P_5\}$

Therefore, the distinct left cosets of H in S_3 are H, $P_2 \bullet H$

4. Let $(Z_6, +)$ be a group and $H = \{0, 3\}$ be a subgroup. Is H a normal subgroup?

Solution: W.k.t. $Z_6 = \{0, 1, 2, 3, 4, 5\}$

Left cosets of H in G are

$0+H = H$

$1+H = \{1,4\}$

$2+H = \{2,5\}$

$3+H = \{3,0\}$

$4+H = \{4,1\}$

$5+H = \{5,2\}$

$\therefore$ Distinct left cosets of H in G are H, $1+H$, $2+H$.

Since $(Z_6, +)$ is an abelian group,

$a+H = H+a$ i.e. left coset is equal to right coset.

Thus, H is a Normal subgroup.

14.7 SUMMARY

Definition: Let H be a subgroup of G and $a \in G$. Then the set, $Ha = \{ha \,/\, h \in H\}$ is called the right coset of H generated by a. Similarly the set $aH = \{ah \,/\, h \in H\}$ is called the left coset of H generated by a.

Theorem: There is one-to-one correspondence between any two right cosets of a subgroup H of a group G.

Theorem: Any two left (right) cosets of a subgroup are either disjoint or identical.

Theorem: Let H be a subgroup of a group G. Then G is equal to the union of all right cosets of H in G i.e. $G = \bigcup_{a \in G} Ha$

Definition: If H is a subgroup of a group G and a, b are two elements of G such that $ab^{-1} \in H$. Then we say that a is congruent to b modulo H, and write as $a \equiv b \; mod(H)$.

Theorem: If H is a subgroup of G with a, b□G then $a \equiv b \; mod(H)$ if and only if ab^{-1}□H is an equivalence relation.

Definition: The number of distinct left (right) cosets of H in G is called the index of H in G denoted by $[G:H]$.

14.8 KEYWORDS

Coset, subgroup, normal subgroup.

14.9 QUESTIONS

1. Is the set of +ve rationals a subgroup of the group of numbers under the operation of addition?

   Solution: Not a subgroup

2. Let G be the non zero integers under the operation of multiplication and let $H=\{3^{n} \mid n \in R\}$.Is H a subgroup of G?
3. Let $G=Z_8$, for each of the following subgroups H of G, determine all the left cosets of H in G, a) $H = \{[0],[4]\}$ b) $H = \{[0],[2],[4],[6]\}$.
4. Let G be the group of all non zero real numbers under the operation of multiplication and consider the subgroup $H=\{3^{n} \mid n \in R\}$ of G. Determine all the left cosets of H in G.
5. Let N be a subgroup of group G, Prove that N is a normal subgroup of G if and only if $a^{-1}Na \square N$ for all $a \in G$.
6. Find the right cosets of $H= \{0, 3\}$ in the group $(Z_6 , +_6)$.
7. Let $(Z_6, +)$ be a group and $H=\{0, 3\}$ be a subgroup. Is H a normal subgroup?

14.10 REFERENCES

1. Discrete mathematics for computer science, by Kolman, Busby and Ross, PHI publications.
2. Discrete Mathematical Structures, by N. G. Goudru, Himalaya Publishing House.
3. Discrete mathematical structures with applications to computer science, by Tremblay and Manohar (McGraw-Hill publications).
4. Topics in Algebra, by I. N. Herstein, Wiley eastern Ltd.

UNIT-15: ISOMORPHISM AND ALGEBRAIC SYSTEM

Structure

15.0 Objectives

15.1 Introduction

15.2 Homomorphism and Isomorphism

15.3 Group Homomorphism

15.4 Kernel of a homomorphism

15.5 Algebraic system with two binary operations

15.6 Solved Problems

15.7 Summary

15.8 Keywords

15.9 Questions

15.10 References

15.0 OBJECTIVES

When you go through this unit, you will be able to

✓ Explain homomorphism and isomorphism;

✓ Analyse the procedure to establish isomorphism;

✓ Explain an algebraic system with two binary operations;

15.1 INTRODUCTION

The concept of isomorphism shows that two algebraic systems which are isomorphic to one another are structurally indistinguishable and that the results of operations in one system can be obtained from those of the other by simply relabeling the names of the elements and symbols for operations. This concept has useful applications in the sense that the results of one system permit an identical interpretation in the other system.

The algebraic systems with one binary operation like semigroups, monoids, groups are not adequate to describe the system of real numbers. We shall therefore consider an abstract algebraic system called a ring, which is a special case of a group on which an additional binary operation satisfying certain properties could be defined. Other algebraic systems with two binary operations will be obtained by imposing further restrictions on rings.

15.2 HOMOMORPHISM AND ISOMORPHISM

An isomorphism between two mathematical structures of the same type should preserve the distinguishing features of the structures.

Definition: Let $(S\ ,\ *)$ & $(T\ ,\ \bullet)$ be two Semigroups. A mapping $\varphi : (S, *) \rightarrow (T, \bullet)$ is called a semigroup homomorphism if $\varphi(a * b) = \varphi(a) \bullet \varphi(b),\ \forall\ a, b \in S$

Further φ is called an isomorphism if φ is one-one and onto.

Procedure to establish isomorphism:

To show that the semigroups $(S,*)$ and $(T, \bullet)$ are isomorphic

Step1: Define a mapping $\varphi : S \rightarrow T$ with Dom(φ)=S.

Step 2: Show that $\varphi(a*b) = \varphi(a) \bullet \varphi(b)$.

Step3: Show that φ is one to one.

Step 4: Show that φ is onto.

Example 1: Let Z be the set of integers and 2Z be the set of even integers. Show that the semigroups (Z, +) and (2Z, +) are isomorphic.

Solution: We follow the above procedure to show that (Z, +) and (2Z, +) are isomorphic.

Step1: Define a function φ :Z→2Z by $\varphi(a) = 2a$.

Step 2: We have, $\varphi(a + b) = 2(a + b)$

$$= 2a+2b$$

$$= \varphi(a) + \varphi(b).$$

Step 3: We show that φ is one-one, suppose that $\varphi(a_1) = \varphi(a_2)$. Then $2a_1 = 2a_2$, so $a_1=a_2$.

Step4: We show that φ is onto

Suppose that b is any even integer

Then $a = b/2 \in\ z$ and

$\varphi\ (a) = \varphi\ (b/2) = 2b/2 = b$

So φ is onto

Hence $(Z, +)$ and $(2Z, +)$ are isomorphic semigroups.

Definition: Let $(S, *, e_S)$ and $(T, \bullet, e_T)$ be two monoids, where e_S and e_T are identity elements of S and T with respect to the corresponding binary operations $*$ and $\bullet$ respectively. A mapping $\varphi : S \rightarrow T$ is called a monoid homomorphism if

$$\varphi(a * b) = \varphi(a) \bullet \varphi(b),\ \forall\ a, b \in S \text{ and}$$

$$\varphi(e_S) = e_T\,.$$

Further φ is called an isomorphism if φ is one-one and onto.

Theorem 15.1: If f is a homomorphism from a commutative semigroup $(S, *)$ onto a semigroup $(T, \bullet)$, then $(T, \bullet)$ is also commutative.

Proof: Let t_1 and t_2 be any elements of T. Then there exit s_1 and s_2 in S with

$$t_1 = f(s_1) \text{ and } t_2 = f(s_2)$$

Consider,

$$\begin{aligned} t_1 \bullet t_2 &= f(s_1) \bullet f(s_2) \\ &= f(s_1 * s_2) \\ &= f(s_2 * s_1) \\ &= f(s_2) \bullet f(s_1) \\ &= t_2 \bullet t_1 \end{aligned}$$

Hence, $(T, \bullet)$ is also commutative.

Theorem 15.2: Let $(S, *)$, $(T, \bullet)$ and $(V, \oplus)$ be semigroups and $g: S \rightarrow T$ & $h: T \rightarrow V$ be semigroup homomorphisms. Then $(h \bullet g): S \rightarrow V$ is a semigroup homomorphism from $(S, *)$ to $(V, \oplus)$.

Proof: Let $a,b \in S$. Then

$$\begin{aligned} (h \bullet . g)\ (a*b) &= h[g(a*b)] \\ &= h[g(a) \bullet g(b)] \end{aligned}$$

$= h(g(a)) \oplus h(g(b))$

$= (h \circ g)\,(a) \oplus (h \circ g)\,(b)$

So, $(h \bullet g)$: $S \rightarrow V$ is a semigroup homomorphism

15.3 GROUP HOMOMORPHISM

Definition: Let $(G, *)$ and $(G', \bullet)$ be two groups. Then a mapping $\varphi:(G, *)\rightarrow(G', \bullet)$ is a group homomorphism if $\varphi(a * b) = \varphi(a) \bullet \varphi(b)$, $\quad \forall\, a, b \in G$.

Further φ is called an isomorphism if φ is one-one and onto.

Theorem 15.3: If φ is a homomorphism from a group G into a group G^1, then

1. $\varphi\,(e) = e^1$, where e is the identity in G and e^1 is the identity in G^1.
2. $\varphi\,(a^{-1}) = [\varphi(a)]^{-1}$, $\forall\ a \in G$.

Proof: 1) Let $a \in G$ then $\varphi(a) \in G^1$.

Consider,

$\varphi(a)\bullet e^{\,1} = \varphi(a)$ $\qquad [\because e^1$ is identity in $G^1]$

$= \varphi(a * e)$ $\qquad [\because e$ is the identity in $G]$

$= \varphi(a)\bullet \varphi(e)$ $\qquad [\because \varphi$ is homomorphism$]$

Hence, $\varphi\,(e) = e^1$. $\qquad$ [by left cancellation law in G']

2) Let $a \in G$ be arbitrary. Since G is a group $a^{-1} \in G$ and

$aa^{-1} = e$.

$\Rightarrow\ \varphi\,(aa^{-1}) = \varphi(e)$

$\Rightarrow \varphi\,(a) \bullet \varphi\,(a^{-1}) = e^1$, $\quad [\because \varphi$ is homomorphism$]$

$\therefore \varphi\,(a^{-1})$ is the inverse of G^1.

$\therefore [\varphi\,(a)]^{-1} = \varphi\,(a^{-1})$.

Example 2: Let φ: $G \rightarrow G^1$ be mapping from group G into G^1, defined by $\varphi(a) = e^1, \forall\, a \in G$. Then φ is a homomorphism. (e^1 is the identity in G^1)

Now for $a,b \in G$

$$\varphi\ (a * b) = e^1 = e^1 \bullet e^1$$
$$= \varphi(a) \bullet \varphi(b)$$

15.4 KERNEL OF A HOMOMORPHISM

If $\varphi : G \rightarrow G^1$ is a group homomorphism then the set of all elements of G which are mapped onto the identity of G^1 is called kernel of φ.

i.e $\quad \ker \varphi = \{x \in G /\ \varphi\ (x) = e^1\}$

Theorem 15.4: The kernel K of a homomorphism φ of G into G^1 is a normal subgroup of G.

Proof: First we show that K is a subgroup of G.

For $a, b \in K$, we have $\varphi\ (a) = e^1 = \varphi\ (b)$

Consider,

$$\varphi\ (ab^{-1}) = \varphi\ (a) \bullet \varphi(b^{-1}) = \varphi(a) \bullet [\varphi(b)]^{-1}$$
$$= e^1 \bullet (e^1)^{-1} = e^1$$

$\therefore ab^{-1} \in K.$

$\therefore K$ is a subgroup of G.

For $a \in K$ and $x \in G$,

Consider, $\varphi\ (xax^{-1}) = \varphi(x) \bullet \varphi\ (a) \bullet \varphi\ (x^{-1})$ $\quad$ [$\because \varphi$ is a homomorphism]

$= \varphi\ (x) \bullet e^1 \bullet \varphi\ (x^{-1})$ $\quad$ [$\because a \in K$]

$= \varphi\ (x) \bullet \varphi\ (x^{-1})$

$= \varphi\ (xx^{-1})$ $\quad$ [$\because \varphi$ is homomorphism]

$= \varphi\ (e) = e^1$

$\therefore\ xax^{-1} \in K$

Hence, K is normal in G.

Example 3: The map $\pi: R^2 \rightarrow R$ defined by $\pi\ (x, y) = x$ is a homomorphism and $\ker \pi = R$.

Solution: Consider,

$$\pi\,[(x_1,\ y_1) + (x_2,\ y_2)] = \pi\,(x_1+x_2\,,\, y_1+y_2)$$

$$= x_1+x_2$$

$$= \pi\,(x_1, y_1) + \pi\,(x_2, y_2).$$

$\therefore$ π is a homomorphism.

$\text{Ker}\,\pi = \{(x, y) \in R^2 \,/\, \pi\,(x, y)=0\}.$

$= \{(x, y)\in R^2/x=0\}.$

$= \{(0, y) \in R^2\} = R.$

15.5 ALGEBRAIC SYSTEM WITH TWO BINARY OPERATIONS

Algebraic System:

A set with one or more n-ary operations on the set is called an algebraic system. We denote an algebraic system by $(S, f_1, f_2, \ldots)$ where S is a non-empty set and $f_1, f_2, \ldots$ are n-ary operations on S.

Example 4: Any group $(G, *)$ is an algebraic system consisting of a set G and a binary operation $*$.

Definition: An algebraic system $(S, +, \cdot\,)$ is called a ring if,

(i) $(S, +)$ is an abelian group.

(ii) $(S, \cdot)$ is a semigroup.

(iii) The operator $\cdot$ is distributive over $+$, that is for any $a, b, c\in S$

$$a\cdot(b + c)= a\cdot b + a\cdot c \quad \text{and}$$

$$(b + c)\cdot a = b\cdot a + c\cdot a.$$

Example 5: The set of all integers under operation addition +, and multiplication ·, is a ring called ring of integers.

Solution:

(i) We know that (Z, +) is an abelian group.

(ii) Again, we know that (Z, ·) is a semigroup.

(iii) Multiplication of integers is distributive with respect to addition of integers i. e. for any $a, b, c \in S,$

$a \cdot (b + c) = a \cdot b + a \cdot c$ and

$(b + c) \cdot a = b \cdot a + c \cdot a.$

Therefore (Z, +, ·) is a ring.

Special types of rings

Commutative ring: A ring R is commutative if the multiplication operation in R is commutative, that is, for all $a, b \in R$, $ab=ba$

Example: Ring of integers.

Ring with unity element : A ring R is said to be a ring with unity element if R has a multiplicative identity, i.e. if there exist an element in R denoted by 1 such that

$$1 \cdot a = a \cdot 1 = a \quad \forall a \in R.$$

Example: (i) Set of all rational numbers

(ii) Ring of integers.

Ring with zero divisors: A ring R is called a ring with zero divisor if there exist elements $a \neq 0$, $b \neq 0$ in R with $ab = 0$. Then we say that a is zero divisor of b and vice versa

Example: Consider, $Z_6 = \{0, 1, 2, 3, 4, 5\}$

Clearly $2 \neq 0$, $3 \neq 0 \in Z_6$, but $2 \otimes_6 3 = 0$.

So, 2 is a zero divisor of 3.

Hence Z_6 is a ring with zero divisor.

Ring without zero divisor: A ring R is called a ring without zero divisor if for any $a, b \in R$ with $ab=0$ then either $a=0$ or $b=0$.

Example: Ring of integers

Integral domain: An integral domain is a commutative ring with unity which has no zero divisors.

Example: $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$.

Field : A commutative ring with unity in which every non-zero element has the multiplicative inverse is called a field.

Example: $(Q, +, \cdot)$, $(C, +, \cdot)$.

15.6 SOLVED PROBLEMS

1. Show that the mapping $\varphi:(Z, +) \rightarrow (2Z, +)$ defined by $\varphi(n)=2n$ is a homomorphism.

Consider

$$\varphi(n+m) = 2(n+m) \qquad \text{for } n, m \in (Z, +)$$
$$= 2n+2m$$
$$= \varphi(n) + \varphi(m).$$

2. Show that the mapping $\varphi : (Z, +)\rightarrow(2Z, +)$ defined by $\varphi(n)=2n$ is an isomorphism.

Solution: For $n, m\in Z \Rightarrow n+m\in Z$.

$$\therefore \quad \varphi(n+m)=2(n+m)$$
$$=2n+2m$$
$$= \varphi(n) + \varphi(m)$$

$\therefore\ \varphi$ is a homomorphism.

If $\varphi(x) = \varphi(y)$ for $x, y \in Z$.

$\Rightarrow 2x = 2y$

$\Rightarrow x = y$

$\therefore\ \varphi$ is one – one.

For each $y \in 2Z$, we can find an element $y/2\in Z$ such that

$$\varphi(y/2) = y$$

$\therefore\ \varphi$ is onto

Hence φ is an isomorphism.

3. Determine whether the mapping $\varphi : (R, +) \rightarrow (R^{+}, \times)$ defined by $\varphi(x)=e^{x}$ is an isomorphism.

Solution:

For $x, y \in R$

$$\varphi(x+y)= e^{x+y} = e^{x}.e^{y}$$

$$= \varphi(x).\ \varphi(y)$$

$\therefore\ \varphi$ is a homomorphism.

If $\varphi\ (x) = \varphi\ (y)$

$$e^{x} = e^{y}$$

$$\Rightarrow e^{x}.e^{-y}=1$$

$$\Rightarrow e^{x-y} =1$$

$$\Rightarrow\ x\text{-}y =0$$

$$\Rightarrow\ x = y$$

$\therefore\ \varphi$ is one-one.

For any $y\in (R^{+}, \times)$, $\exists\ \log_{e}^{y} \in R$ such that $\varphi(\log_{e}^{y}) =e^{\log y} = y$.

$\therefore\ \varphi$ is onto.

$\therefore\ \varphi$ is an isomorphism.

15.7 SUMMARY

Let $(S\ ,\ *)$ & $(T\ ,\ \bullet)$ be two semigroups. A mapping φ: $(S, *) \rightarrow (T, \bullet)$ is called a semigroup homomorphism if $\varphi(a * b) =\varphi(a) \bullet \varphi(b),\ \forall\ a, b \in S$

Further φ is called an isomorphism if φ is one-one and onto.

Theorem: Let $(S, *)$, $(T, \bullet)$ and $(V, \oplus)$ be semigroups and g: $S \rightarrow T$ & h: $T \rightarrow V$ be semigroup homomorphisms. Then $(h \bullet g)$: $S \rightarrow V$ is a semigroup homomorphism from $(S, *)$ to $(V, \oplus)$.

Theorem: If φ is a homomorphism from a group G into a group G^{1}, then

1. $\varphi\ (e) = e^{1}$, where e is the identity in G and e^{1} is the identity in G^{1}.
2. $\varphi\ (a^{-1}) = [\varphi(a)]^{-1},\ \forall\ a \in G$.

Definition: If $\varphi : G \rightarrow G^1$ is a group homomorphism then the set of all elements of G which are mapped onto the identity of G^1 is called kernel of φ.

Definition: A set with one or more n-ary operations on the set is called an algebraic system.

Definition: An algebraic system $(S, +, \cdot)$ is called a ring if,

(iv) $(S, +)$ is an abelian group.

(v) $(S, \cdot)$ is a semigroup.

(vi) The operator $\cdot$ is distributive over +.

15.8 KEYWORDS

Homomorphism, isomorphism, algebraic system.

15.9 QUESTIONS

1. What are the steps to be followed to check whether 2 semigroups $(S,*)$ and $(T,*)$ are isomorphic. Show that $(Z, +)$ and $(T, *)$ are isomorphic , where Z is the set of all even integers.
2. Let G be a group and let a be a fixed element of G. Then show that the function $f : G \rightarrow G$ defined by $f(x)=axa^{-1}$, where x□G, is an isomorphism.
3. Let $(S,*)$ and $(T,*)$ be monoids with identities e and e^1 respectively, Let $f : S \rightarrow T$ be an isomorphism. Then prove that $f(e)= e^1$.
4. Let G be a group under addition and G^1 be a group under multiplication. Let $f : G \rightarrow G^1$ be defined by $f(x)=e^x$. Show that f is an isomorphism.
5. Let $(S_1,*)$, $(S_2,*^1)$, and $(S_1,*^{11})$ be semigroups and let $f : S_1$ □ S_2 and $g : S_2$ □ S_3 be isomorphisms. Show that $gof : S_1$ □ S_3 is an isomorphism.
6. Prove that the set of all reals, rationals, complex numbers forms a ring under usual addition and multiplication.
7. Prove that set M_n of all $n \times n$ matrices is a ring with respect to the addition and multiplication of matrices when the elements in matrices are numbers which are members of any ring of numbers.

15.10 REFERENCES

1. Discrete mathematics for computer science, by Kolman, Busby and Ross, PHI publications.
2. Discrete Mathematical Structures, by N. G. Goudru, Himalaya Publishing House.
3. Discrete mathematical structures with applications to computer science, by Tremblay and Manohar (McGraw-Hill publications).
4. Topics in Algebra, by I. N. Herstein, Wiley eastern Ltd.

UNIT-16: INTRODUCTION TO CODING THEORY

Structure

16.0 Objectives

16.1 Introduction

16.2 Encoding functions

16.3 Hamming distance

16.4 Group codes

16.5 Decoding and Error correction

16.6 Solved Problems

16.7 Summary

16.8 Keywords

16.9 Questions

16.10 References

16.0 OBJECTIVES

When you go through this unit, you will be able to

- ✓ Explain the Group codes;
- ✓ Differentiate between encoding and decoding functions;
- ✓ Analyse the procedure of detecting errors in communication;
- ✓ Analyse the procedure of correcting errors in communication

16.1 INTRODUCTION

Error-detection and correction techniques have become increasingly important in the design of computer systems. Most systems contain telephone and communication lines which cause transmitted messages to be corrupted by the presence of noise. Peripheral equipment associated with such systems is by far the most unreliable component of these systems and both error detection and error correction are frequently performed. Algebraic structures have been the basis of the most important codes which have been designed.

Communication plays an important role. It takes place in a variety of ways. The three essential parts in an ideal communication system are transmitter, channel and receiver.

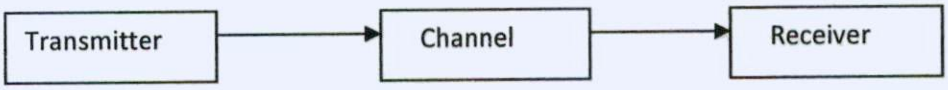


Fig 16.1

In practice, the transmission channel may suffer disturbances, which are called noise, due to weather interference, electrical problems and so on. The important task of a communication system is to minimize the errors in transmission.

A device used to improve the efficiency of communication channel is an encoder. Decoder is a device used to transform the encoded message into original form.

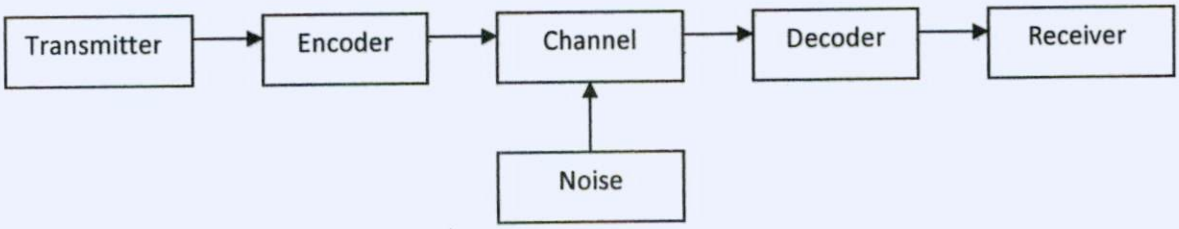


Fig 16.2

16.2 ENCODING FUNCTION

Message: Message is a basic unit of information. It is a finite sequence of characters from a finite alphabet.

Word: Let $B= \{0, 1\}$ be the alphabet we choose. Every symbol, we want to transmit is represented as a sequence of m elements from B. Thus, word is a basic unit of information and is a sequence of m 0's &1's.

The set B is a group under the binary operation + mod2.

A group structure can be given to the set of all words, that is, binary strings of length m.

Let $B^m = B \times B \times B \ldots \times B$ (m factors) is a group under the operation $\oplus$ defined by

$$(x_1, x_2, \ldots., x_m) \oplus (y_1, y_2, \ldots..y_m) = (x_1+y_1, x_2+y_2, \ldots, x_m+y_m).$$

i) For $(x_1, x_2, \ldots, x_m)$, $(y_1, y_2, \ldots..y_m) \in B^m$,

$$(x_1, x_2, \ldots., x_m) \oplus (y_1, y_2, \ldots..y_m) = (x_1+y_1, x_2+y_2, \ldots, x_m+y_m) \in B^m$$

$(B^m, \oplus)$ satisfies closure axiom.

ii) $(B^m, \oplus)$ satisfies associative axiom.

iii) $0=(0,0,0\ldots,0)$ is the identity element.

iv) Every element is its own inverse.

Hence $(B^m, \oplus)$ is a group.

Note:

1) An element in B^m is written as $(b_1, b_2, \ldots, b_m)$ or simply as $b_1\, b_2 \ldots b_m$.

2) B^m has 2^m number of elements.

Definition: An (m, n) encoding function is a one to one function e: $B^m \rightarrow B^n$ with $n>m$. For every $b \in B^m$ there exists a distinct $e(b) \in B^m$ called the codeword representing b.

Definition: Let e be an encoding function. We say that the code word $x=e(b)$ has been transmitted with k or fewer errors if the received message x_t and x differ in at least one but no more than k positions.

Definition: Let e: $B^m \rightarrow B^n$ be an (m, n) encoding function. We say that e detects k or fewer errors if whenever $x=e(b)$ is transmitted with k or fewer errors, then x_t is not a code word.

Definition: If $x \in B^n$, then the number of 1's in x is called the weight of x and is denoted by $|x|$.

Example 1: Find the weight of each of the following words in B^7: a) x=010001 b) x= 1110000 c) x=0000000 d) x=1111111.

Solution: a) $|x|=2$ b)$|x|=3$ c) $|x|=0$ d)$|x|=7$

Example 2: Parity check code: The following encoding function e: $B^m \rightarrow B^{m+1}$ is called the parity (m, m+1) check code:

If $b=b_1,b_2,\ldots b_m \in B^{m,}$ define $e(b)= b_1,b_2,\ldots b_m\ b_{m+1}$

where $b_{m+1} = b_{m+1} = \begin{cases} 0\ if\ |\ b\ |\ \ is\, even \\ 1\ if\ |\ b\ |\ \ is\, odd \end{cases}$

To illustrate this encoding function, let m=2, Then,

e(00)=000, e(01)= 011, e(10)=101, e(11)=110

Let m=2, Then e:$B^2 \rightarrow B^3$

B^2={00,01,10,11}

To find the elements in B^3

B^3= 0 if $|b|$ is even

1 if $|b|$is odd

Weight of the word 00 = |00|=0, even, so e(00)=000

Weight of the word 01 = |01|=1, odd, so e(01)=011

Weight of the word 10 = |10|=1, odd, so e(10)=101

Weight of the word 11 = |11|=2, even, so e(11)=110

The code words in B^3 are {000,011,101,110}

Let m=3, Then e: $B^3 \rightarrow B^4$

B^3= {000,001,010,011,100,101,110,111}

For b € $B^{3,}$ B_4= 0 if $|b|$ is even

1 if $|b|$is odd

e(000)=0000, e(001)=0011, e(010)=0101

e(011)=0110, e(100)=1001, e(101)=1010

e(110)=1100, e(111)=1111

The code words in B^4 are {0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111}

Parity (m, 3m) check code

Consider the encoding function $e:B^{m}\rightarrow B^{3m}$ If $b=(b_1, b_2,\dots, b_m) \in B^{m}$. Define $e(b) = e(b_1,b_2,\dots b_m) = b_1b_2\dots b_m\ b_1b_2\dots b_m\ b_1b_2\dots b_m$.

Example 3: Determine the code words for the parity check code $(m, 3m)$ where $m=2$,

Solution: We know that, $B^2=\{00,01,10,11\}$

Code words

$e(00)=000000$

$e(10)=101010$

$e(01)=010101$

$e(11)=111111$

16.3 HAMMING DISTANCE

Definition: Let x and y be words in B^{m}. The hamming distance $H(x, y)$ between x and y is the weight, $|x\oplus y|$ of $x\oplus y$. Thus the distance between $x= x_1x_2\dots x_m$ and $y=y_1y_2\dots y_m$ is the number of positions in which x and y differ.

Example 4: Find the Hamming distance between x and y.

a) $x = 000101$, $y=010110$.

b) $x = 110110$, $y = 001100$.

Solution: a) $x\oplus y = 010011$, so $|x\oplus y|=3$.

b) $x\oplus y = 111010$, so $|x\oplus y|=4$.

Theorem 16.1: (Properties of Distance Function)

Let x, y and z are the elements of B^m. Then,

a) $H(x, y) = H(y, x)$

b) $H(x, y) \geq 0$

c) $H(x, y) = 0$ if and only if $x = y$.

d) $H(x, y) \leq H(x, z) + H(z, y)$

Proof:

a) Let $x, y \in B^m$ so $x = (x_1, x_2, \ldots.., x_m)$ and $y = (y_1, y_2, \ldots\ldots., y_m)$

$$H(x, y) = |x \oplus y|$$
$$= |(x_1, x_2, \ldots, x_m) \oplus (y_1, y_2, \ldots, y_m)|$$
$$= |x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_m \oplus y_m|$$
$$= |y_1 \oplus x_1, y_2 \oplus x_2, \ldots, y_m \oplus x_m|$$
$$= |y \oplus x|$$

b) $H(x, y) = |x \oplus y|$ is the distance between $x = x_1\, x_2 \ldots x_m$ and $y = y_1\, y_2 \ldots\, y_m$. Such that $x_i \neq y_i$. i.e., the number of positions in which x and y differ. Since $x_i, y_i \in \{0,1\}$,

$$H(x,y) = |x \oplus y| \geq 0$$
$$\Rightarrow H(x,y) \geq 0$$

c) If $x_i = y_i$

Let $x_i, y_i \in \{0\}$,then $|x \oplus y| = |(0,0,\ldots.,0) \oplus (0,0, \ldots, 0)|$

$$= |(0,0,\ldots,0)|$$
$$= 0.$$
$$\Rightarrow \quad H(x, y) = 0.$$

Let $x_i, y_i \in \{1\}$ then

$|x \oplus y| = |(1, 1, \ldots,1) \oplus (1, 1, \ldots,1)|$ using mod 2 addition

$$= |(0,0,\ldots,0)|$$
$$= 0.$$
$$\Rightarrow \quad H(x, y) = 0.$$

d) For x and y in B^m,

$|x \oplus y| \leq |x| \oplus |y|$

If $z \in B^m$, then $z \oplus z = \bar{O}$, the identity element in B^m.

$$H(x, y) = |x \oplus y|$$
$$= |x \oplus \bar{O} \oplus y|$$
$$= |x \oplus z \oplus z \oplus y|$$
$$\leq |x \oplus z| + |z \oplus y|$$

$H(x, y) \leq H(x, z) + H(z, y)$

Minimum distance:

The minimum distance of an encoding function $e : B^m \to B^n$ is the minimum of the distances between all distinct pairs of code words; that is

$$\text{Min } \{ H(e(x), e(y)) \,/\, x, y \in B^m \}$$

Theorem 16.2: An (m, n) encoding function $e : B^m \longrightarrow\rightarrow B^n$ can detect k or fewer errors if and only if its minimum distance is at least $k + 1$.

Proof: Suppose that the minimum distance between any two code words is at least k+1. Let $b \in B^m$, and let $x = e(b) \in B^n$ be the code word representing b. Then x is transmitted and is received as x_t. If x_t were a code word different from x, then $H(x, x_t) \geq k + 1$, so x would be transmitted with k+1 or more errors. Thus, if x is transmitted with k or fewer errors, then x_t cannot be a code word. This means that e can detect k or fewer errors.

Conversely, suppose that the minimum distance between code words is $r \leq k$, and let x and y be code words with $H(x, y) = r$. If $x_t = y$, that is, if x is transmitted and is mistakenly received as y, then $r \leq k$ errors have been committed and have not been detected. Thus it is not true, that e can detect k or fewer errors.

16.4 GROUP CODES

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

$e(B^m) = \{e(b)/b \in B^m\} = \text{Ran}(e)$ is a subgroup of B^n.

Theorem 16.3: Let e: $B^m \to B^n$ be a group code. The minimum distance of e is the minimum weight of a non-zero code word.

Proof: Let m be the minimum distance of the group code and let $m = H(x, y)$, where x and y are distinct code words. Let n be the minimum weight of a non-zero code word and suppose that $n = |z|$, for a code word z.

Since, e is a group code, $x \oplus y$ is a non-zero code word.

Then $m = H(x, y) = |x \oplus y| \geq n$ ....(1)

Since the identity element $\bar{O}$ and z are distinct code words.

$n = |z| = |z \oplus \bar{O}| = H(z, \bar{O}) \geq m$ ....(2)

From (1) and (2), $m = n$.

Hence, the minimum distance of e is the minimum weight of a non-zero code word.

16.5 DECODING AND ERROR CORRECTION

Consider an (m, n) encoding function $e{:}B^m \rightarrow B^n$. Once the encoded word $x{=}e(b) \in B^n$, for $b \in B^m$, is received as the word x_t, we are faced with the problem of identifying the word b that was the original message.

An onto function d: $B^n \rightarrow B^m$ is called an (n, m) decoding function associated with e if $d(x_t){=}b'$ $\in B^m$ is such that when the transmission channel has no noise, then $b'{=}b$, that is, $d \circ e = 1_{B^m}$, where 1_{B^m} is the identity function on B^m. The decoding function d is required to be onto so that every received word can be decoded to give a word in B^m. It decodes properly received words correctly, but the decoding of improperly received words may or may not be correct.

Decoding functions:

1) Let d: $B^{m+1} \rightarrow B^m$ be a $(m+1, m)$ decoding function. If $b{=}b_1b_2b_3....b_mb_{m+1} \in B^{m+1}$, then $d(b){=}b_1b_2b_3.....b_m$. If there is no error, then

$(d \circ e)(b) = d\,(e\,(b))$

$\qquad = d(x)$

$\qquad = b.$

$d \circ e = 1_{B^m}$.

2) Let d: $B^{3m} \rightarrow B^m$ be a $(3m, m)$ decoding function.

Then, for $y = y_1, y_2 \ldots y_m, y_{m+1} \ldots y_{2m}, y_{2m+1} \ldots y_{3m}$.

$d(y) = z_1\ z_2 \ldots\ z_m$ where

$$z_i = \begin{cases} 1 \; if \; \{y_i, y_{i+m}, y_{i+2m}\} \text{ has at least two1's} \\ 0 \; if \; \{y_i, y_{i+m}, y_{i+2m}\} \text{ has less than two1's}. \end{cases}$$

That is, the decoding function d examines the i^{th} digit in each of the three blocks transmitted. The digit that occurs at least twice in these three blocks is chosen as the decoded i^{th} digit.

Maximum Likelihood Technique:

Given an (m, n) encoding function e: $B^m \to B^n$, we often need to determine an (n, m) Decoding function $d : B^n \to B^m$ associated with e. The maximum likelihood technique is to determine the decoding function d for a given e.

Since, B^m has 2^m elements, there are 2^m code words in B^m we first list that the code words in fixed order:

$x^{(1)}, x^{(2)}, \ldots\ldots\ldots\ldots x^{(2m)}$

If the received word is x_t, we compute $H(x^{(i)}, x_t)$ for $1 \leq i \leq 2^m$ and choose the first code word, say it is $x^{(s)}$, such that.

$$\underset{1 \leq i \leq 2^m}{Min}\{H(x^{(i)}, x_t)\} = H(x^{(s)}, x_t)$$

That is, $x^{(s)}$ is code word that is closest to x_t and the first in the list. If $x^{(s)} = e(b)$,we define the maximum likelihood decoding function d associated with e by $d(x_t) = b$. Observe that d depends on the particular order in which the code words in $e(B^m)$ are listed. If the code words are listed in a different order, we may obtain a different maximum likelihood decoding function d associated with e.

Theorem 16.4: Suppose that e is an (m, n) encoding function and d is a maximum likelihood decoding function associated with e. Then (e, d) can correct k or fewer errors if and only if the minimum distance of e is at least $2k+1$

Proof: Assume that the minimum distance of e is at least $2k+1$.

Let $b \in B^m$ and $x = e(b) \in B^m$. Suppose that x is transmitted with k or fewer errors, and x_t is received. This means that $H(x, x_t) \leq k$. If z is any other code word, then

$$2k+1 \leq H(x, z) \leq H(x, x_t) + H(x_t, z) \leq k + H(x_t, z).$$

Thus $H(x_t, z) \geq 2k + 1 - k = k + 1$. This means that x is the unique code word that is closest to x_t, so $d(x_t)=b$. Hence (e, d) corrects k or fewer errors.

Conversely, assume that the minimum distance between code words is $r \leq 2k$, and let $x = e(b)$ and $x^1 = e(b^1)$ be code words with $H(x, x^1) = r$. Let $x = b_1\, b_2\, b_3 \ldots b_n$, $x^1=b_1' b_2' \ldots b_n'$. Then $b_i \neq b_i'$ for exactly r integers, i between 1 and n. Assume, that $b_1 \neq b_1'$, $b_2 \neq b_2'$, …, $b_r \neq b_r'$, but $b_i = b_i'$, when $i > r$.

(a) Suppose that $r \leq k$. If x is transmitted as $x_t = x^1$, then $r \leq k$ errors have been committed but $d(x_t) = b^1$; so (e, d) has not corrected the r errors.

(b) Suppose that $k+1 \leq r \leq 2k$ and let

$y=b_1'\, b_2' \ldots\, b_{\mathrm{k}}' b_{k+1} \ldots . b_n$

If x is transmitted as $x_t=y$, then $H(x_t, x^1) = r - k \leq k$ and $H(x_t, x) \geq k$.

Thus, x^1 is at least as close to x_t as x is, and x^1 precedes x in the list of code words; so $d(x_t) \neq b$. Then we have committed k errors, which (e, d) has not corrected.

16.6 SOLVED PROBLEMS

1. Consider the (2, 3) parity check code. For each of the received words, determine whether an error will be detected a) 010 b) 110 c) 001 d) 110

Solution: Parity check code is $e: B^2 \rightarrow B^3$

a) Received word=010 $\in B^3$

Word= 01 $\in B^2$

Weight of 01 =|01|=1, odd. So, e(01)=011=code word

Since 010≠ 011, the received code word is not equal to the code word. Hence, an error detected.

b) Received word=110 $\in B^3$

Word= 11 $\in B^2$

Weight of 11 =|11|=2, even. So, e(11)=110=code word

Since 110=110, the received code word is equal to the code word. Hence, no error detected.

c) Received word=001 $\in B^3$

Word= 00 $\in B^2$

Weight of 00 =|00|=0, even .So, e(00)=000=code word

Since 001$\neq$ 000, the received code word is not equal to the code word. Hence, an error detected.

d) Received word=100 $\in B^3$

Word= 10 $\in B^2$

Weight of 10 =|10|=1, odd. So, e(10)=101=code word

Since 100$\neq$ 101, the received code word is not equal to the code word. Hence, an error detected.

2. Consider the $(m,3m)$ encoding function, where m=2, for each of the received words, determine whether an error will be detected a) 010100 b)1010101 c)111011 d)111111.

Solution: The encoding function is e: $B^2 \rightarrow B^6$

a) Received word =010100

e(01)=010101 $\neq$ 010100

The received code word is not equal to the code word.

Hence error detected.

b) Received word =101010

e(10)= 101010=101010

The received code word is equal to the code word.

Hence error cannot be detected.

3. (i) Find the minimum distances of the (2, 5) encoding function e: $B^2 \rightarrow B^5$ defined by

e(00)=00000, e(10)=00111, e(01)=01110, e(11)=11111.

(ii) How many errors will e detect?

Solution: (i). H (e(00), e(10))=|00000$\oplus$00111|=|00111|=3.

H (e(00), e(01))=|00000$\oplus$01110|=|01110|=3.

H (e(00), e(11))=|00000$\oplus$11111|=|11111|=5.

H (e(10), e(01))=|00111$\oplus$01110|=|01001|=2.

H (e(10), e(11))=|00111$\oplus$11111|=|11000|=2.

H (e(01), e(11))=|01110$\oplus$11111|=|10001|=2.

Minimum distance= min{3, 3, 5, 2, 2, 2}=2.

(ii). The minimum distance of e is 2. By Theorem 4.3.3, we have $2 \geq k+1$ or $k \leq 1$. Thus the code can detect one error.

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

Solution:- Let $N = \{00000, 01110, 10101, 11011\}$.

Let $a = 00000$, $b = 01110$, $c = 10101$, $d = 11011$.

$\oplus$	a	b	c	d
a	a	b	c	c
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Table 16.1

The identity element $a = 00000$ of B^5 belongs to N.

From the table $(N, \oplus)$ is closed.

Every element is its own inverse.

So, the encoding function is a group code.

5. Let d be the (4, 3) decoding function determine $d(y)$ for the word $y \in B^4$

(a) $y = 0110$ (b) $y = 1011$

Solution: a) $y = 0110$

By definition of $(m+1, m)$ decoding function,

$d(b) = b_1, b_2, b_3 \ldots\ldots\ldots\ldots\ldots\ldots b_m, b_{m+1} \in B_{m+1}$ where m=3

$d(b) = b_1, b_2, b_3$ where $b = d(b) = b_1, b_2, b_3, b_4$.

So $d(y) = d(0110)$ where $y = 0110 \in B^4$

$d(y) = 011$

$b)\ d(y) = d(1011)$

$d(y) = 101$

6. Let d be the (6, 2) decoding function. Determine $d(y)$ for the word y=111011 in B^6.

Solution: y=111011

The received word y has 3 equal blocks like

y =11 10 11

B_1 B_2 B_3

To find z_1, compare the first digits of B_1, B_2 and B_3.

First digit of B_1 is 1

First digit of B_2 is 1

First digit of B_3 is 1

So, first digit of B_1, B_2 and B_3 has at least two 1's. Hence, first digit of z is 1.

To find z_2

Second digit of B_1 is 1

Second digit of B_2 is 0

Second digit of B_3 is 1

So, second digit of B_1, B_2 and B_3 has at least two 1's

Hence, second digit of z is 1

Since $z = z_1z_2$, z=11.

$d(111011) = 11$

7.Let $e{:}B^2 \rightarrow B^5$ be an encoding function defined by $e(00)$=00000, $e(01)$=01110, $e(10)$=10101, $e(11)$=11011. Decode the following words relative to a maximum likelihood decoding function.

(a) 11110 (b) 10011

Solution: Let $x^{(1)}$=00000, $x^{(2)}$=01110, $x^{(3)}$=10101, $x^{(4)}$=11011

(a) Let x_r=11110

$H(x^{(1)}, x_r)$=|100000|+|111101| =|11110|=4

$H(x^{(2)},x_r)$= |101110|+|111101|=|1100001|=1

$H(x^{(3)},x_r)=|110101|+|111101|=|1010111|=3$

$H(x^{(4)},x_r)= |111011|+|111101|=|1001011|=2.$

So, minimum $(H(x^{(i)},x_r)) = \min\{4,1,3,2\}=1$

Therefore,$(H(x^{(s)},x_r)) = \min(h(x^{(s)},x_r))$

So, $x^{(s)} = x^{(2)} = e^{(b)}$

$x^{(s)} = 01110 = e^{(01)}$

Thus, maximum likelihood encoding word is b=01.

b)Let x_r=10011

$H(x^{(1)},x_r)=|00000+10011|=|10011|=3$

$H(x^{(2)},x_r)=|01110+10011|=|11101|=4$

$H(x^{(3)},x_r)=|10101+10011|=|00110|=2$

$H(x^{(4)},x_r)=|11011+10011|=|01000|=1$

so, minimum $(H(x^{(i)},x_r))=\min\{3,4,2,1\}=1$

Therefore,$(H(x^{(s)},x_r))=\min(H(x^{(4)},x_r))$

So,$x^{(s)}=x^{(4)}=e^{(b)}$

$x(s)=11011=e^{(11)}$.

Thus, maximum likelihood decoded word is b=11.

16.7 SUMMARY

Definition: An (m, n) encoding function is a one to one function e: $B^m \rightarrow B^n$ with $n>m$. For every $b \in B^m$ there exists a distinct $e(b) \in B^{m,}$ called the codeword representing b.

Definition: Let e: $B^m \rightarrow B^n$ be an (m, n) encoding function. We say that e detects k or fewer errors if whenever $x=e(b)$ is transmitted with k or fewer errors, then x_t is not a code word.

Definition: Let x and y be words in B^m. The hamming distance $H(x, y)$ between x and y is the weight, $|x\oplus y|$ of $x\oplus y$. Thus the distance between $x= x_1x_2\ldots x_m$ and $y=y_1y_2\ldots y_m$ is the number of positions in which x and y differ.

Definition: The minimum distance of an encoding function $e : B^m \rightarrow B^n$ is the minimum of the distances between all distinct pairs of code words; that is

$$\text{Min } \{\, H(e(x), e(y)) \,/\, x, y \in B^m \,\}$$

Theorem: An (m, n) encoding function $e : B^m \rightarrow B^n$ can detect k or fewer errors if and only if its minimum distance is at least $k + 1$.

Theorem: Let e: $B^m \rightarrow B^n$ be a group code. The minimum distance of e is the minimum weight of a non-zero code word.

Theorem: Suppose that e is an (m, n) encoding function and d is a maximum likelihood decoding function associated with e. Then (e, d) can correct k or fewer errors if and only if the minimum distance of e is at least $2k+1$.

16.8 KEYWORDS

Code word, group code, encoding function, decoding function.

16.9 QUESTIONS

1. Consider the (2, 3) parity check code. For each of the received words, determine whether an error will be detected a) 100 b) 101 c) 001 d) 110.
2. Determine the code words for the parity check code $(m, 3m)$ where $m=3$.
3. Find the minimum distances of the (2, 4) encoding function e: $B^2 \rightarrow B^4$ defined by $e(00)=0000$, $e(10)=0011$, $e(01)=0110$, $e(11)=1111$.
4. Determine whether the (2, 5) encoding function $e : B^2 \rightarrow B^5$ defined by $e(00)=00000$, $e(01)=01110$, $e(10)=10101$, $e(11)=11011$ is a group code.
5. Let d be the (6, 2) decoding function. Determine $d(y)$ for the word $y=101011$ in B^6.
6. Let $e:B^2 \rightarrow B^5$ be an encoding function defined by $e(00)=00000$, $e(01)=01110$, $e(10)=10101$, $e(11)=11011$. Decode the following words relative to a maximum likelihood decoding function. (a)11110 (b) 10011.

16.10 REFERENCES

1. Discrete mathematics for computer science, by Kolman, Busby and Ross, PHI publications.
2. Discrete Mathematical Structures, by N. G. Goudru, Himalaya Publishing House.

3. Discrete mathematical structures with applications to computer science, by Tremblay and Manohar (McGraw-Hill publications).

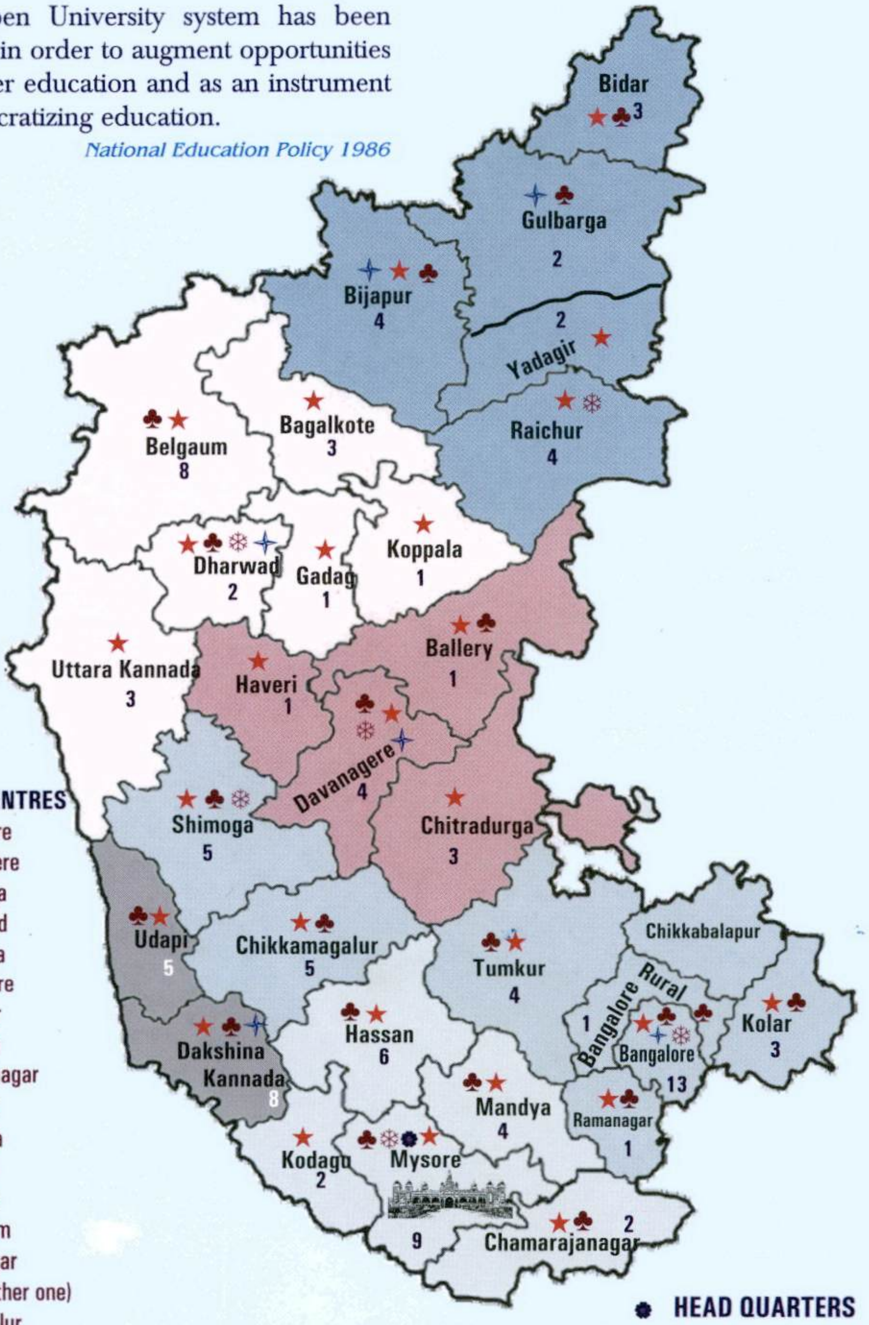
ಆದೇಶ ಸಂಖ್ಯೆ : ಕರಾಮುವಿ/ಅಸಾವಿ/2-1614/2012-13 ದಿನಾಂಕ : 02-08-2012
ಒಳಪುಟ : 60 GSM ಮಾಪ್ಲಿತೊ ಮತ್ತು ರಕ್ಷಾ ಪುಟ : 220 GSM 'ಆರ್ಟ್ ಕಾರ್ಡ್'
ಮುದ್ರಕರು : ಶ್ರೀ ಸುಬ್ರಮಣ್ಯೇಶ್ವರ ಬುಕ್ ಡಿಪೋ, ಬೆಂಗಳೂರು - 560 002, ಪ್ರತಿಗಳು - 200

Karnataka State Open University

Manasagangotri Mysore - 570 006

The Open University system has been initiated in order to augment opportunities for higher education and as an instrument of democratizing education.

National Education Policy 1986



♣ REGIONAL CENTRES

Bangalore
Davanagere
Gulbarga
Dharwad
Shimoga
Mangalore
Tumkur
Hassan
Chamarajanagar
Bellary
Mandya
Kolar
Bijapur
Belagaum
Ramanagar
Bangalore (another one)
Chikmagalur
Udupi
Karwar
Bidar
Mysore

● **HEAD QUARTERS**
★ **Total Study Centres : 123**
♣ **Regional Centres : 21**
❄ **B.Ed Study Centres : 10**
✦ **M.Ed Study Centres : 06**

KSOU

Higher Education to everyone everywhere
ಉನ್ನತ ಶಿಕ್ಷಣ ಎಲ್ಲರಿಗೂ ಎಲ್ಲೆಡೆ

Feedback : improvement, revision and launching of new programmes
Multimedia learning material
Academic and other support
Evaluation - methods and modes
INSTRUCTIONAL SYSTEM
STUDENT
Unsystematic feedback
feedback from students & academics
feedback from counsellors
feedback from public
Programme guide
course materials
assignments
supplementory material
communication etc.
Self-instructional print material
project
*audio & video cassettes at study centres
Broadcasts-radio, television & teleconferencing
Electronic media learning component
*students affairs cell
Regional Director & academic staff
Coordinator & counsellors at study centres
Optional
Obligatory
Laboratory work/practicals
Extended contact programmes
Tutor mark assignments
*Computer marked assignments
Continuous evaluation
*Examination conducted 2 times in a year
Terminal examination & project evaluation
Project
Examination results
Monitoring of assignment
Report from study centres
Rounit Programme evaluation
Special Programme evaluation
questionaires
Systematic feedback
KSOU CAMPUS
Windows 7

ಕರ್ನಾಟಕ ರಾಜ್ಯ ಮುಕ್ತ ವಿಶ್ವವಿದ್ಯಾನಿಲಯ
ಮಾನಸಗಂಗೋತ್ರಿ, ಮೈಸೂರು – 570 006

Karnataka State Open University

Manasagangotri, Mysore - 570 006 Website : www.ksoumysore.edu.in