B. TECH.
5Th SEMESTER
DISCRETE MATHEMATICS
(I.T & Comp. Science Engg.)

SYLLABUS

B.Tech (CSE/IT, Discrete Mathematical Structures)

Unit I

Logic: Propositional equivalence, predicates and quantifiers, Methods of proofs, proof strategy, sequences and summation, mathematical induction, recursive definitions and structural induction, program correctness.

Counting: The basics of counting, the pigeonhole principle, permutations and combinations, recurrence relations, solving recurrence relations, generating functions, inclusion-exclusion principle, application of inclusion-exclusion.

Unit II

Relations: Relations and their properties, n-array relations and their applications, representing relations, closure of relations, equivalence of relations, partial orderings.

Graph theory: Introduction to graphs, graph terminology, representing graphs and graph isomorphism, connectivity, Euler and Hamilton paths, planar graphs, graph coloring, introduction to trees, application of trees.

Unit III

Group theory: Groups, subgroups, generators and evaluation of powers, cosets and Lagrange's theorem, permutation groups and Burnside's theorem, isomorphism, automorphisms, homomorphism and normal subgroups, rings, integral domains and fields.

Unit IV

Lattice theory: Lattices and algebras systems, principles of duality, basic properties of algebraic systems defined by lattices, distributive and complimented lattices, Boolean lattices and Boolean algebras, uniqueness of finite Boolean expressions, prepositional calculus. Coding theory: Coding of binary information and error detection, decoding and error correction.

Text Books:

*1) K.H. Rosen: Discrete Mathematics and its application, 5th edition, Tata McGraw Hill.*Chapter 1(1.1-1.5), Chapter 3(3.1-3.4,3.6), Chapter 4(4.1-4.3,4.5), Chapter 6(6.1,6.2,6.4-6.6) Chapter 7(7.1-7.6), Chapter 8(8.1-8.5,8.7,8.8)

2. *C. L. Liu: Elements of Discrete Mathematics*, 2nd edition, TMH 2000.

Chapter 11(11.1 – 11.10 except 11.7), Chapter 12(12.1 – 12.8)

3.*B.Kalman: Discrete Mathematical Structure*, 3rd edition, Chapter 11(11.1,11.2)

References:

1. "Discrete Mathematical Structures": Tremblay and Manohar, Tata McGraw Hill
2. "Discrete Mathematics": 1st edition by Maggard Thomson
3. "Discrete Mathematics": Semyour Lipschutz, Varsha Patil IInd Edition Schaum's Series, TMH
4. "Discrete Mathematical Structures": Kolman, Busby and Ross, Prentice Hall India, Edition 3
5. "Discrete Mathematics and its application" – Mott Kendle
6. "Discrete Mathematical Structure" : G. Shankar Rao, New Age Publisher.
7. "Fundamental Approach to Discrete Mathematics" Acharjaya D. P. Sreekumar, New Age Publisher.

Disclaimer

This document does not claim any originality and cannot be used as a substitute of prescribed text books. The information presented here is merely a collection by the committee members for their respective teaching assignments. Various sources as mentioned references at the beginning of the document as well as freely available materials from the internet were constituted for preparing this document. The ownership of the information lies with respective authors or institutions. Further this document is not intended to be used for commercial purposes and the committee members are not accountable for any issues, legal or otherwise, arising out of this document. The committee members make no representations or warranties with respect to the accuracy or completeness of the contents of the document and disclaim any implied warranties of merchantability or fitness for a particular purpose. The committee members shall not be liable for any loss or profit or any other commercial, incidental, consequential or any other damages.

Acknowledgement

The committee members gratefully acknowledge Google, NPTEL and different reference books for getting help for preparation of this lecture note. The committee members also want to express their gratitude to the persons those who thinks knowledge should be free and be accessible and sharable without any restrictions so that every individual on this world has the same opportunity to explore and become enlightened by the collective gift of mankind.

This lecture note being first draft so there may be some error. Also detail proofs and some graphs are omitted; however details discussion has been made in the class. Thus apart from this lecture note students/readers are strongly recommended following the mentioned books in the references and above all conferring with the faculty members for thorough knowledge in the subject.

Justification of Learning the Subject:

What is **Discrete Mathematics?**

Consider an **analog clock (**One with hands that continuously rotate and show time in continuous fashion) and a **digital clock (**It shows time in discrete fashion). The former one gives the idea of **Continuous Mathematics** whereas the later one gives the idea of **Discrete Mathematics**. Thus, Continuous Mathematics deals with continuous functions, differential and integral calculus etc. whereas discrete mathematics deals with mathematical topics in the sense that it analyzes data whose values are separated (such as integers: Number line has gaps)

Example of continuous math – Given a fixed surface area, what are the dimensions of a cylinder that maximizes volume?

Example of Discrete Math – Given a fixed set of characters, and a length, how many different passwords can you construct? How many edges in graph with n vertices? How many ways to choose a team of two people from a group of n?

Why do you learn Discrete Mathematics?

This course provides some of the mathematical foundations and skills that you need in your further study of Information Technology and Computer Science & Engineering. These topics include: Logic, Counting Methods, Relation and Function, Recurrence Relation and Generating Function, Introduction to Graph Theory And Group Theory, Lattice Theory and Boolean Algebra etc.

.

Unit I

PROPOSITIONAL LOGIC AND COUNTING THEORY

OBJECTIVES:

After going through this unit, you will be able to :

- Define proposition & logical connectives.
- To use the laws of Logic.
- Describe the logical equivalence and implications.
- Define arguments & valid arguments.
- To study predicate and quantifier.
- Test the validity of argument using rules of logic.
- Give proof by truth tables.
- Give proof by mathematical Induction.
- Discuss Fundamental principle of counting.
- Discuss basic idea about permutation and combination.
- Define Pigeon hole principle.
- Study recurrence relation and generating function.

INTRODUCTION :

Mathematics is assumed to be an exact science. Every statement in Mathematics must be precise. Also there can't be Mathematics without proofs and each proof needs proper reasoning. Proper reasoning involves logic. The dictionary meaning of 'Logic' is the science of reasoning. The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid & invalid mathematical arguments.

In addition to its importance in mathematical reasoning, logic has numerous applications in computer science to verify the correctness of programs & to prove the theorems in natural & physical sciences to draw conclusion from experiments, in social sciences & in our daily lives to solve a multitude of problems.

The area of logic that deals with propositions is called the propositional calculus or propositional logic. The mathematical approach to logic was first discussed by British mathematician George Boole; hence the mathematical logic is also called as Boolean logic.

In this chapter we will discuss a few basic ideas.

PROPOSITION (OR STATEMENT)

A proposition (or a statement) is a declarative sentence that is either true or false, but not both.

A proposition (or a statement) is a declarative sentence which is either true or false but not both.

Imperative, exclamatory, interrogative or open sentences are not statements in logic.

Example 1 : For Example consider, the following sentences.

(i) VSSUT is at Burla.

(ii) $2 + 3 = 5$

(iii) The Sun rises in the east.

(iv) Do your home work.

(v) What are you doing?

(vi) $2 + 4 = 8$

(vii) $5 < 4$

(viii) The square of 5 is 15.

(ix) $x + 3 = 2$

(x) May God Bless you!

All of them are propositions except (iv), (v),(ix) & (x) sentences (i), (ii) are true, whereas (iii),(iv), (vii) & (viii) are false.

Sentence (iv) is command, hence not a proposition. (v) is a question so not a statement. (ix) is a declarative sentence but not a statement, since it is true or false depending on the value of x. (x) is a exclamatory sentence and so it is not a statement.

Mathematical identities are considered to be statements. Statements which are imperative, exclamatory, interrogative or open are not statements in logic.

Compound statements:

Many propositions are composites that are, composed of sub propositions and various connectives discussed subsequently. Such composite propositions are called compound propositions.

A proposition is said to be primitive if it cannot be broken down into simpler propositions, that is, if it is not composite.

Example 2 : Consider, for example following sentences.

a. "The sun is shining today and it is colder than yesterday"
b. "Sita is intelligent and she studies every night."

Also the propositions in Example 1 are primitive propositions.

LOGICALOPERATIONS OR LOGICAL CONNECTIVES :

The phrases or words which combine simple statements are called logical connectives. There are five types of connectives. Namely, 'not', 'and', 'or', 'if…then', iff etc. The first one is a unitary operator whereas the other four are binary operators.
In the following table we list some possible connectives, their symbols & the nature of the compound statement formed by them.

Sr. No.	Connective	Symbol	Compound statement
1	AND	$\wedge$	Conjunction
2	OR	$\vee$	Disjunction
3	NOT	$\neg$	Negation
4	If....then	$\rightarrow$	Conditional or implication
5	If and only if (iff)	$\leftrightarrow$	Biconditional

Now we shall study each of basic logical connectives in details.

Basic Logical Connectives:

Conjunction (AND):

If two statements are combined by the word "and" to form a compound proposition (statement) then the resulting proposition is called the conjunction of two propositions.

Symbolically, if P & Q are two simple statements, then 'P $\wedge$ Q' denotes the conjunction of P and Q and is read as 'P and Q.

Since, $P \wedge Q$ is a proposition it has a truth value and this truth value depends only on the truth values of P and Q.

Specifically, if P & Q are true then $P \wedge Q$ is true; otherwise $P \wedge Q$ is

false.

The truth table for conjunction is as follows.

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

Example 3:

Let P: In this year monsoon is very good.
Q: The rivers are flooded.

Then, $P \wedge Q$: In this year monsoon is very good and the rivers are flooded.

Disjunction (OR) :

Any two statements can be connected by the word 'or' to form a compound statement called disjunction.

Symbolically, if P and Q are two simple statements, then $P \vee Q$ denotes the disjunction of P and Q and read as 'P or Q'.

The truth value of $P \vee Q$ depends only on the truth values of P and Q. Specifically if P and Q are false then $P \vee Q$ is false, otherwise $P \vee Q$ is true.

The truth table for disjunction is as follows.

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

Example 4:

P: Paris is in France
Q $2+3=6$
then $P \vee Q$: Paris is in France or 2 + 3 = 6.
Here, $P \vee Q$ is true since P is true & Q is False.

Thus, the disjunction $P \vee Q$ is false only when P and Q are both false.

Negation (NOT)

Given any proposition P, another proposition, called negation of P, can be formed by modifying it by "not". Also by using the phrase "It is not the case that or" "It is false that" before P we will able to find the negation.

Symbolically, $\neg P$ Read as "not P" denotes the negation of P. the truth value of $\neg P$ depends on the truth value of P

If P is true then $\neg P$ is false and if P is false then $\neg P$ is true. The truth table for Negation is as follows:

P	$\neg P$
T	F
F	T

Example 5:

Let P: 3 is a factor of 12.
Then Q = $\neg P$: 3 is not a factor of 12.
Here P is true & $\neg P$ is false.

Conditional or Implication: (If…then)

If two statements are combined by using the logical connective 'if…then' then the resulting statement is called a conditional statement.

If P and Q are two statements forming the implication "if P then Q" then we denotes this implication $P \to Q$.

In the implication $P \to Q$,

P is called antecedent or hypothesis

Q is called consequent or conclusion.

The statement $P \to Q$ is true in all cases except when P is true and Q is false.

The truth table for implication is as follows.

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

Since conditional statement play an essential role in mathematical reasoning a variety of terminology is used to express $P \to Q$.

i) If P then Q
ii) P implies Q
iii) P only if Q
iv) Q if P
v) P is sufficient condition for Q
vi) Q when P
vii) Q is necessary for P
viii) Q follows from P
ix) if P, Q
x) Q unless $\neg P$

Converse, Inverse and Contra positive of a conditional statement :

We can form some new conditional statements starting with a conditional statement $P \to Q$ that occur so often. Namely converse, inverse, contra positive. Which are as follows:

1. **Converse:** If $P \to Q$ is an implication then $Q \to P$ is called the converse of $P \to Q$.

2. **Contra positive :** If $P \to Q$ is an implication then the implication $\neg Q \to \neg P$ is called it's contra positive.

3. **Inverse:** If $P \to Q$ is an implication then $\neg P \to \neg Q$ is called its inverse.

Example 6:

Let P: You are good in Mathematics.
Q: You are good in Logic.

Then, $P \to Q$: If you are good in Mathematics then you are good in Logic.

1) Converse: $(Q \to P)$
   If you are good in Logic then you are good in Mathematics.
2) Contra positive: $\neg Q \to \neg P$
   If you are not good in Logic then you are not good in Mathematics.
3) Inverse: $(\neg P \to \neg Q)$
   If you are not good in Mathematics then you are not good in Logic.

Biconditional Statement: Let P and Q be propositions. The biconditional statement $P \leftrightarrow Q$ is the proposition "P if and only if Q". The biconditional statement is true when P and Q have same truth values and is false otherwise.

Biconditional statements are also called bi-implications. It is also read as p is necessary and sufficient condition for Q.

The truth table for biconditional statement is as follows.

P	Q	$P \leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 7 : Let P : Ram can take the flight.
Q : Ram buy a ticket.
Then $P \leftrightarrow Q$ is the statement.
"Ram can take the flight iff Ram buy a ticket".

Precedence of Logical Operators:

We can construct compound propositions using the negation operator and the logical operators defined so far. We will generally use parentheses to specify the order in which logical operators in a compound proposition are to be applied. In order to avoid an excessive number of parentheses.

We sometimes adopt an order of precedence for the logical connectives. The following table displays the precedence levels of the logical operators.

Operator	Precedence
$\neg$	1
$\wedge$	2
$\wedge$	3
$\rightarrow$	4
$\leftrightarrow$	5

LOGICAL EQUIVALANCE:

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

Definition: The compound propositions P and Q are said to be logically equivalent if $P \leftrightarrow Q$ is a tautology. The notation $P \equiv Q$ denotes that P and Q are logically equivalent.

Some equivalence statements are useful for deducing other equivalence statements. The following table shows some important equivalence.

Logical Identities or Laws of Logic:

Name	Equivalence
1. Identity Laws	$P \wedge T \equiv P$ $P \vee F \equiv P$
2. Domination Laws	$P \vee T \equiv T$ $P \wedge F \equiv F$
3. Double Negation	$\neg(\neg P) \equiv P$
4. Idempotent Laws	$P \vee P \equiv P$ $P \wedge P \equiv P$
5. Commutative Laws	$P \vee Q \equiv Q \vee P$ $P \wedge Q \equiv Q \wedge P$
6. Associative Laws	$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$

7. Distributive Laws	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
8. De Morgan's Laws	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
9. Absorption Laws	$P \vee (P \wedge Q) \equiv P$ $P \wedge (P \vee Q) \equiv P$
10. Negation Laws (Inverse / Complement)	$P \vee \neg P \equiv T$ $P \wedge \neg P \equiv F$
11. Equivalence Law	$P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$
12. Implication Law	$P \rightarrow Q \equiv \neg P \vee Q$
13. Biconditional Property	$P \leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$
14. Contra positive o f Conditional statement	$P \rightarrow Q \equiv \neg Q \rightarrow \neg P$

Note that while taking negation of compound statement 'every' or 'All' is interchanged by 'some' & 'there exists' is interchanged by 'at least one' & vice versa.

Example 8: If P: "This book is good."
Q: "This book is costly."
Write the following statements in symbolic form.

a) This book is good & costly.
b) This book is not good but costly.
c) This book is cheap but good.
d) This book is neither good nor costly.
e) If this book is good then it is costly.

Answers:

a) $P \wedge Q$
b) $\neg P \wedge Q$
c) $\neg Q \wedge P$
d) $\neg P \wedge \neg Q$
e) $P \rightarrow Q$

Logical Equivalence Involving Implications :

Let P & Q be two statements.

The following table displays some useful equivalences for implications involving conditional and biconditional statements.

Sr. No.	Logical Equivalence involving implications
1	$P \to Q \equiv \neg P \vee Q$
2	$P \to Q \equiv \neg Q \to \neg P$
3	$P \vee Q \equiv \neg P \to Q$
4	$P \wedge Q \equiv \neg(P \to \neg Q)$
5	$\neg(P \to Q) \equiv P \wedge \neg Q$
6	$(P \to Q) \wedge (P \to r) \equiv P \to (Q \wedge r)$
7	$(P \to r) \wedge (Q \to r) \equiv (P \vee Q) \to r$
8	$(P \to Q) \vee (P \to r) \equiv P \to (Q \vee r)$
9	$(P \to r) \vee (Q \to r) \equiv (P \wedge Q)r$
10	$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$
11	$P \leftrightarrow Q \equiv \neg P \leftrightarrow \neg Q$
12	$P \leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$
13	$\neg(P \leftrightarrow Q) \equiv P \leftrightarrow \neg Q$

All these identities can be proved by using truth tables.

NORMAL FORM AND TRUTH TABLES :

Well ordered Formulas:

A compound statement obtained from statement letters by using one or more connectives is called a statement pattern or statement form. thus, if P, Q, R, … are the statements (which can be treated as variables) then any statement involving these statements and the logical connectives $\neg, \wedge, \vee, \to, \leftrightarrow$ is a statement form or a well ordered formula or statement pattern.

Definition: A propositional variable is a symbol representing any proposition. Note that a propositional variable is not a proposition but can be replaced by a proposition.

Any statement involving propositional variable and logical connectives is a well formed formula.

Note: A wof is not a proposition but we substitute the proposition in place of propositional variable, we get a proposition.

E.g. $\neg(P \vee Q) \wedge (\neg Q \wedge R) \rightarrow Q, \neg(P \rightarrow Q)$ etc.

Truth table for a Well Formed Formula:

If we replace the propositional variables in a formula α by propositions, we get a proposition involving connectives. If α involves n propositional constants, we get 2n possible combination of truth variables of proposition replacing the variables.

Example 9: Obtain truth value for $\alpha = (P \rightarrow Q) \wedge (Q \rightarrow P)$.

Solution: The truth table for the given well formed formula is given below.

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	α
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Tautology:

A tautology or universally true formula is a well formed formula, whose truth value is T for all possible assignments of truth values to the propositional variables.

Example 10 : Consider $P \vee \neg P$, the truth table is as follows.

P	$\neg P$	$P \vee \neg P$
T	F	T
F	T	T

$P \vee \neg P$ always takes value T for all possible truth value of P, it is a tautology.

Contradiction or fallacy:

A contradiction or (absurdity) is a well formed formula whose truth value is false (F) for all possible assignments of truth values to the propositional variables.

Thus, in short a compound statement that is always false is a contradiction.

Example 11 : Consider the truth table for $P \wedge \neg P$.

P	$\neg P$	$P \wedge \neg P$
T	F	F
F	T	F

$\therefore P \wedge \neg P$ always takes value F for all possible truth values of P, it is a Contradiction.

Contingency:

A well formed formula which is neither a tautology nor a contradiction is called a contingency.

Thus, contingency is a statement pattern which is either true or false depending on the truth values of its component statement.

Example 12: Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent

.

Solution : The truth tables for these compound proposition is as follows.

1	2	3	4	5	6	7	8
P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$	$6 \leftrightarrow 7$
T	T	F	F	T	F	F	T
T	F	F	T	T	F	F	T
F	T	T	F	T	F	F	T
F	F	T	T	F	T	T	T

We can observe that the truth values of $\neg(p \vee q)$ and $\neg p \wedge \neg q$ agree for all possible combinations of the truth values of p and q.

It follows that $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$ is a tautology; therefore the given compound propositions are logically equivalent.

Example 13: Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Solution : The truth tables for these compound proposition as follows.

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

As the truth values of $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Example 14 : Determine whether each of the following form is a tautology or a contradiction or neither :

i) $(P \wedge Q) \rightarrow (P \vee Q)$

ii) $(P \vee Q) \wedge (\neg P \wedge \neg Q)$

iii) $(\neg P \wedge \neg Q) \rightarrow (P \rightarrow Q)$

iv) $(P \rightarrow Q) \wedge (P \wedge \neg Q)$

v) $\left[P \wedge (P \rightarrow \neg Q) \rightarrow Q\right]$

Solution:

i) The truth table for $(p \wedge q) \rightarrow (p \vee q)$

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

Here all the entries in the last column are 'T'.

$\therefore (p \wedge q) \rightarrow (p \vee q)$ is a tautology.

ii) The truth table for $(p \vee q) \wedge (\neg p \wedge \neg q)$ is

1	2	3	4	5	6	
p	q	$p \vee q$	$\neg p$	$\neg q$	$\neg P \wedge \neg q$	$3 \wedge 6$
T	T	T	F	F	F	F
T	F	T	F	T	F	F
F	T	T	T	F	F	F
F	F	F	T	T	T	F

The entries in the last column are 'F'. Hence $(p \vee q) \wedge (\neg p \wedge \neg q)$ is a contradiction.

iii) The truth table is as follows.

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$p \to q$	$(\neg p \wedge \neg q) \to (p \to q)$
T	T	F	F	F	T	T
T	F	F	T	F	F	T
F	T	T	F	F	T	T
F	F	T	T	T	T	T

Here all entries in last column are 'T'.

$\therefore$ $(\neg p \wedge \neg q) \to (p \to q)$ is a tautology.

iv) The truth table is as follows.

p	q	$\neg q$	$p \wedge \neg q$	$p \to q$	$(p \to q) \wedge (p \wedge \neg q)$
T	T	F	F	T	F
T	F	T	T	F	F
F	T	F	F	T	F
F	F	T	F	T	F

All the entries in the last column are 'F'. Hence it is contradiction.

v) The truth table for $\left[p \wedge (p \rightarrow \neg q) \rightarrow q\right]$

p	q	$\neg q$	$p \rightarrow \neg q$	$p \wedge (p \rightarrow \neg q)$	$\left[p \wedge (p \rightarrow \neg q) \rightarrow q\right]$
T	T	F	F	F	T
T	F	T	T	T	F
F	T	F	T	F	T
F	F	T	T	F	T

The last entries are neither all 'T' nor all 'F'.

$\therefore$ $\left[p \wedge (p \rightarrow \neg q) \rightarrow q\right]$ is a neither tautology nor contradiction. It is a Contingency.

PREDICATES AND QUANTIFIERS

Predicates: A predicate is a function from universe of discourse to truth values. Consider a sentence: x is greater than 2. Here is greater than 2 is the predicate and x is the subject or variable.

If values are assigned to all the variables, the resulting sentence is a proposition.

e.g. 1. $x < 9$ is a predicate

2. $4 < 9$ is a proposition

Propositional Function:

A propositional function (or an open sentence) defined on A is a predicate together with subjects. It is denoted by the expression P(x) which has the property that P(a) is true or false for each $a \in A$.

The set A is called domain of P(x) and the set T_p of all elements of A for which P (a) is true is called the truth set of P(x).

Propositional functions can be converted to proposition by two aspects

(i) By assigning exact value to the variable and (ii) using quantification.

e.g. Let A = {x / x is an integer < 8}

Here P(x) is the sentence "x is an integer less than 8".

The common property is "an integer less than 8".

$\therefore$ P(1) is the statement "1 is an integer less than 8".

$\therefore$ P(1) is true.

Quantifiers:

Quantification is the way by which a Propositional function can be turns out to be a proposition. The expressions 'for all' and 'there exists' are called quantifiers. The process of applying quantifier to a variable is called quantification of variables.

Universal quantification:

The universal quantification of a predicate P(x) is the statement, "For all values of x, P(x) is true."

The universal quantification of P(x) is denoted by $\forall$ for all x P(x).

The symbol $\forall$ is called the universal quantifier.
e.g.

1) The sentence P(x) : - (-x) = x is a predicate that makes sense for real numbers x. The universal quantification of P(x), $\forall$ x P(x) is a true statement because for all real numbers, -(- x) = x.

2) Let Q(x) : x + 1 < 5, then $\forall$ Q(x) : x + 2 < 5 is a false statement, as Q(5) is not true. Universal quantification can also be stated in English as "for every x", "every x", or "for any x."

Existential quantification -
The existential quantification of a predicate P(x) is the statement
"There exists a value of x for which P(x) is true."
The existential quantification of P(x) is denoted $\exists xP(x)$. The symbol $\exists$ is called the existential quantifier. e.g.

1) Let $Q : x+1<4$. The existential quantification of Q(x), $\exists xQ(x)$ is a true statement, because Q(2) is true statement.
2) The statement $\exists y$, y + 2 = y is false. There is no value of y for which the propositional function y+2 = y produces a true statement.

Negation of Quantified statement :

$\neg \exists$ x $p(x) = \forall x \neg p(x)$
and $\neg \forall x\, p(x) = \exists x \neg p(x)$

This is true for any proposition p(x).

For example, The negation of all men are mortal is: There is a man who is not mortal.

Example 15 :

Express the statement using quantifiers: "Every student in your school has a computer or has a friend who has a computer."

Solution :

Let c(x) : "x has a computer"
F(x,y) : "x and y are friends"

Thus, We have

$$\forall x(c(x) \vee \exists y(c(y) \wedge F(x, y))$$

THEORY OF INFERENCE FOR THE PREDICAT CALCULAS

If an implication $P \Rightarrow Q$ is a tautology where P and Q may be compound statements involving any number of propositional variables we say that Q logically follows from P. Suppose $P(P_1, P_2 \ldots\ldots P_n) \rightarrow Q$. Then this implication is true regardless of the truth values of any of its components. In this case, we say that Q logically follows from $P_1, P_2 \ldots, P_n$.

Proofs in mathematics are valid arguments that establish the truth of mathematical statements.

To deduce new statements from statements we already have, we use rules of inference which are templates for constructing valid arguments. Rules of inference are our basic tools for establishing the truth of statements. The rules of inference for statements involving existential and universal quantifiers play an important role in proofs in Computer Science and Mathematics, although they are often used without being explicitly mentioned.

Valid Argument:

An argument in propositional logic is a sequence of propositions. All propositions in the argument are called **hypothesis** or **Premises**.The final proposition is called the **conclusion**. An argument form in propositional logic is a sequence of compound propositions - involving propositional variables.

An argument form is valid if no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Thus we say the conclusion C can be drawn from a given set of premises or the argument is valid if the conjunction of all the premises implies the conclusion is a tautology.

Rules of Inference for Propositional logic

We can always use a truth table to show that an argument form is valid. Arguments based on tautologies represent universally correct method of reasoning. Their validity depends only on the form of statements involved and not on the truth values of the variables they contain such arguments are called **rules of inference**.

These rules of inference can be used as building blocks to construct more complicated valid argument forms

e.g.
Let P: "You have a current password"
Q: "You can log onto the network".

Then, the argument involving the propositions,
"If you have a current password, then you can log onto the network".

"You have a current password" therefore: You can log onto the network" has the form …

.

$$P \rightarrow Q$$
$$\underline{P}$$
$$\therefore Q$$

Where $\therefore$ is the symbol that denotes 'therefore we know that when P & Q are proposition variables, the statement $((P \rightarrow Q) \wedge P) \rightarrow Q$ is a tautology

.

So, this is valid argument and hence is a rule of inference, called modus ponens or the law of detachment.

(Modus ponens is Latin for mode that affirms)
The most important rules of inference for propositional logic are as follows…..

	Rule of Inference	Tautology	Name
1)	P $P \rightarrow Q$ $\therefore Q$	$(P \wedge (P \rightarrow Q)) \rightarrow Q$	Modus ponens
2)	$\neg Q$ $P \rightarrow Q$ $\therefore \neg P$	$[\neg Q \wedge (P \rightarrow Q)] \rightarrow \neg P$	Modus tollens
3)	$P \rightarrow Q$ $Q \rightarrow R$ $\therefore P \rightarrow R$	$[(P \rightarrow Q) \wedge (Q \rightarrow R)] \rightarrow (P \rightarrow$	Hypothetical syllogism
4)	$P \vee Q$ $\neg P$ $\therefore Q$	$[(P \vee Q) \wedge \neg P] \rightarrow Q$	Disjunctive syllogism
5)	P $\therefore PVQ$	$P \rightarrow (P \vee Q)$	Addition
6)	$P \wedge Q$ $\therefore P$	$(P \wedge Q) \rightarrow P$	Simplification
7)	P Q $\therefore P \wedge Q$	$((P) \wedge (Q)) \rightarrow P \wedge Q$	Conjunction
8)	$P \vee Q$ $\neg P \vee R$ $\therefore Q \vee R$	$[(P \vee Q) \wedge (\neg P \vee R)] \rightarrow (Q \vee R$	Resolution

Example16:

Test the validity of the following arguments :

1. If milk is black then every crow is white.
2. If every crow is white then it has 4 legs.
3. If every crow has 4 legs then every Buffalo is white and brisk.
4. The milk is black.
5. So, every Buffalo is white.

Solution :

Let P : The milk is black

Q : Every crow is white

R : Every crow has four legs.

S : Every Buffalo is white

T : Every Buffalo is brisk

The given premises are

(i) $P \rightarrow Q$

(ii) $Q \rightarrow R$

(iii) $R \rightarrow S \wedge T$

(iv) P

The conclusion is S. The following steps checks the validity of argument.

1.	$P \rightarrow Q$	premise (1)
2.	$Q \rightarrow R$	Premise (2)
3.	$P \rightarrow R$	line 1. and 2. Hypothetical syllogism (H.S.)
4.	$R \rightarrow S \wedge T$	Premise (iii)
5.	$P \rightarrow S \wedge T$	Line 3. and 4.. H.S.
6.	P	Premise (iv)
7.	$S \wedge T$	Line 5, 6 modus ponens
8.	S	Line 7, simplification
$\therefore$	The argument is valid	

Example17 :

Consider the following argument and determine whether it is valid or not. Either I will get good marks or I will not graduate. If I did not graduate I will go to USA. I get good marks. Thus, I would not go to USA.

Solution :

Let P : I will get good marks.

Q : I will graduate.

R : I will go to USA

The given premises are

i) $P \vee \neg Q$

ii) $\neg Q \rightarrow R$

iii) P

The conclusion is $\neg R$.

What are proofs?

A proof is a clear explanation, accepted by the mathematical community, of why something is true.

Ancient Babylonian and Egyptian mathematics had no proofs, just examples and methods. Proofs in the way we use them today began with the Greeks and Euclid

Methods of Proof:

There are different methods of proof as follows:

- Direct method
- Indirect method.
- Contradiction method.
- Vacuous method.
- Method of induction etc

Already you have the idea about above mentioned methods. Let us discuss method of induction.

MATHEMATICAL INDUCTION

Here we discuss another proof technique. Suppose the statement to be proved can be put in the from P(n), $\forall\, n \geq n_0$. where n_0 is some fixed integer.

That is suppose we wish to show that P(n) is true for all integers $n \geq n_0$.

The following result shows how this can be done.

Suppose that

(a) $P(n_0)$ is true and

(b) If P(K) is true for some $K \geq n_0$, then P(K + 1) must also be true. The P(n) is true for all $n \geq n_0$.

This result is called the principle of Mathematical induction.

Thus to prove the truth of statement $\forall\, n \geq n_0$. P(n), using the principle of mathematical induction, we must begin by proving directly that the first proposition $P(n_0)$ is true. This is called the basis step of the induction and is generally very easy.

Then we must prove that $P(K) \Rightarrow P(K + 1)$ is a tautology for any choice of $K \geq n_0$. Since, the only case where an implication is false is if the antecedent

is true and the consequent is false; this step is usually done by showing that if P(K) were true, then P(K + 1) would also have to be true. This step is called induction step.

In short we solve by following steps.

1. Show that P(1) is true.
2. Assume P(k) is true.
3. Prove that P(k +1) is true using

P(k) Hence P(n) is true for every n.

Example 18 :

Using principle of mathematical induction prove that

(i) $1 + 2 + 3 + ... + n = n (n + 1) / 2$

(ii) $1^2 + 2^2 + 3^2 + ... + n^2 = n (n + 1) (2n + 1)/ 6$

(iii) $1^3 + 2^3 + 3^3 + ... + n^3 = n^2 (n + 1)^2 / 4$

(iv) $3^n > n^2$ for n = 1, n = 2

(v) $3^n > n^2$ for n a positive integer greater than 2.

(vi) For any positive integer number n , $n^3 + 2$ n is divisible by 3

Solution (i)

Let the statement P (n) be

$1 + 2 + 3 + ... + n = n (n + 1) / 2$

STEP 1: We first show that p (1) is true.

Left Side = 1

Right Side = 1 (1 + 1) / 2 = 1

Both sides of the statement are equal hence p (1) is true.

STEP 2: We now assume that p (k) is true

$1 + 2 + 3 + ... + k = k (k + 1) / 2$

and show that p (k + 1) is true by adding k + 1 to both sides of the above statement

$1 + 2 + 3 + ... + k + (k + 1) = k (k + 1) / 2 + (k + 1)$

$= (k + 1)(k / 2 + 1)$

$= (k + 1)(k + 2) / 2$

The last statement may be written as

$1 + 2 + 3 + ... + k + (k + 1) = (k + 1)(k + 2) / 2$

Which is the statement p(k + 1).

Hence , by method of induction P(n) is true for all n.

Solution (ii)

Statement P (n) is defined by

$1^2 + 2^2 + 3^2 + ... + n^2 = n (n + 1) (2n + 1)/ 2$

STEP 1: We first show that p (1) is true.

Left Side = $1^2 = 1$

Right Side = 1 (1 + 1) (2*1 + 1)/ 6 = 1

Both sides of the statement are equal hence p (1) is true.

STEP 2: We now assume that p (k) is true

$1^2 + 2^2 + 3^2 + ... + k^2 = k (k + 1) (2k + 1)/ 6$

and show that p (k + 1) is true by adding $(k + 1)^2$ to both sides of the above statement

$1^2 + 2^2 + 3^2 + ... + k^2 + (k + 1)^2 = k (k + 1) (2k + 1)/ 6 + (k + 1)^2$

Set common denominator and factor k + 1 on the right side

$= (k + 1) [k (2k + 1)+ 6 (k + 1)] /6$

Expand $k (2k + 1)+ 6 (k + 1)$

$= (k + 1) [2k^2 + 7k + 6] /6$

Now factor $2k^2 + 7k + 6$.

$= (k + 1) [(k + 2) (2k + 3)] /6$

We have started from the statement P(k) and have shown that

$1^2 + 2^2 + 3^2 + ... + k^2 + (k + 1)^2 = (k + 1) [(k + 2) (2k + 3)] /6$

Which is the statement P(k + 1).

Hence , by method of induction P(n) is true for all n.

Solution (iii)

Statement P (n) is defined by

$1^3 + 2^3 + 3^3 + ... + n^3 = n^2 (n + 1)^2 / 4$

STEP 1: We first show that p (1) is true.

Left Side = $1^3 = 1$

Right Side = $1^2 (1 + 1)^2 / 4 = 1$

hence p (1) is true.

STEP 2: We now assume that p (k) is true

$1^3 + 2^3 + 3^3 + ... + k^3 = k^2 (k + 1)^2 / 4$

add $(k + 1)^3$ to both sides

$1^3 + 2^3 + 3^3 + ... + k^3 + (k + 1)^3 = k^2 (k + 1)^2 / 4 + (k + 1)^3$

factor $(k + 1)^2$ on the right side

$= (k + 1)^2 [k^2 / 4 + (k + 1)]$

set to common denominator and group

$= (k + 1)^2 [k^2 + 4 k + 4] / 4$

$= (k + 1)^2 [(k + 2)^2] / 4$

We have started from the statement P(k) and have shown that

$1^3 + 2^3 + 3^3 + ... + k^3 + (k + 1)^3 = (k + 1)^2 [(k + 2)^2] / 4$

Which is the statement P(k + 1).

Hence , by method of induction P(n) is true for all n.

Solution (iv)

Statement P (n) is defined by

$n^3 + 2 n$ is divisible by 3

STEP 1: We first show that p (1) is true. Let n = 1 and calculate $n^3 + 2n$

$1^3 + 2(1) = 3$

3 is divisible by 3

hence p (1) is true.

STEP 2: We now assume that p (k) is true

$k^3 + 2k$ is divisible by 3

is equivalent to

$k^3 + 2k = 3M$, where M is a positive integer.

We now consider the algebraic expression $(k + 1)^3 + 2(k + 1)$; expand it and group like terms

$(k + 1)^3 + 2(k + 1) = k^3 + 3k^2 + 5k + 3$

$= [k^3 + 2k] + [3k^2 + 3k + 3]$

$= 3M + 3[k^2 + k + 1] = 3[M + k^2 + k + 1]$

Hence $(k + 1)^3 + 2(k + 1)$ is also divisible by 3 and therefore statement P(k + 1) is true.

Hence , by method of induction P(n) is true for all n.

Solution (v)

Statement P (n) is defined by

$3^n > n^2$

STEP 1: We first show that p (1) is true. Let n = 1 and calculate 3^1 and 1^2 and compare them

$3^1 = 3$

$1^2 = 1$

3 is greater than 1 and hence p (1) is true.

Let us also show that P(2) is true.

$3^2 = 9$

$2^2 = 4$

Hence P(2) is also true.

STEP 2: We now assume that p (k) is true

$3^k > k^2$

Multiply both sides of the above inequality by 3

$3 * 3^k > 3 * k^2$

The left side is equal to 3^{k+1}. For k >, 2, we can write

$k^2 > 2k$ and $k^2 > 1$

We now combine the above inequalities by adding the left hand sides and the right hand sides of the two inequalities

$2k^2 > 2k + 1$

We now add k^2 to both sides of the above inequality to obtain the inequality

$3k^2 > k^2 + 2k + 1$

Factor the right side we can write

$3 * k^2 > (k + 1)^2$

If $3 * 3^k > 3 * k^2$ and $3 * k^2 > (k + 1)^2$ then

$3 * 3^k > (k + 1)^2$

Rewrite the left side as 3^{k+1}

$3^{k+1} > (k + 1)^2$

Which proves that P(k + 1) is true

Hence , by method of induction P(n) is true for all n.

Solution (vi)

Statement P (n) is defined by

$n! > 2^n$

STEP 1: We first show that p (4) is true. Let n = 4 and calculate 4 ! and 2^n and compare them

4! = 24

$2^4 = 16$

24 is greater than 16 and hence p (4) is true.

STEP 2: We now assume that p (k) is true

$k! > 2^k$

Multiply both sides of the above inequality by k + 1

$k! (k + 1) > 2^k (k + 1)$

The left side is equal to (k + 1)!. For k >, 4, we can write

$k + 1 > 2$

Multiply both sides of the above inequality by 2^k to obtain

$2^k (k + 1) > 2 * 2^k$

The above inequality may be written

$2^k (k + 1) > 2^{k + 1}$

We have proved that $(k + 1)! > 2^k (k + 1)$ and $2^k (k + 1) > 2^{k + 1}$ we can now write

$(k + 1)! > 2^{k + 1}$

We have assumed that statement P(k) is true and proved that statement P(k+1) is also true.

Hence , by method of induction P(n) is true for all n.

COUNTING:

Broadly speaking combinatory(counting) is the branch of mathematics dealing with order and patterns without regard to the intrinsic properties of the objects under consideration.

FUNDAMENTAL PRINCIPLE COUNTING (FPC):

The two main counting rules: The **Multiplication Rule** states that if one can do a job by doing two tasks one after the other, and there are 'm' ways to do the first task and then 'n' ways to do the second, then there are 'mn' ways to do the whole job.

For Example, suppose there are 3 routes from Burla to Sambalpur and 4 routes from Sambalpur to Cuttack, then by FPC the total number of ways for performing journey from Burla to Cuttack is 12.

The **Addition Rule,** states that if one can do a job by doing one or the other (but not both) of two tasks, and there are m ways to do then first task and n ways to do the second, then there are m+n ways to do the whole job.

PERMUTATIONS AND COMBINATIONS:

Permutation is the arrangement of objects with ordering, whereas combination is the selection of objects without ordering.

Permutation Formula:

(i) The permutation of n – things taken r at a time without repetition is

$P(n, r) = n!/(n - r)!$

n = the total number of items you have from which to take

r = the number you are actually going to use.

(ii) The permutation of n – things taken r at a time with repetition is

$P(n, r) = n^r$

(iii) The permutation of n – things taken all at a time with repetition is

$P(n,n) = n!$

Factorial Rule: For *n* items, there are *n*! (pronounced n factorial) ways to arrange them.

$n! = (n)(n - 1)(n - 2). . . (3)(2)(1)$

For example:

$3! = (3)(2)(1) = 6$

$4! = (4)(3)(2)(1) = 24$

$5! = (5)(4)(3)(2)(1) = 120$

6! = (6)(5)(4)(3)(2)(1) = 720

Note: 0!=1

Example 2:

Let's say you have four friends, but only need to text three of them when order matters. Find the number of ways to text your friends.

Solution:

$$P(4,3) = \frac{4!}{(4-3)!} = \frac{24}{1!} = 24$$

There are 24 ways to test three out of your four friends if order matters.

Combination Formula:

The permutation of n – things taken r at a time is:

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

n = the total number of items you have from which to choose

r = the number you are actually going to use.

Example 3:

The art club has 4 members. They want to choose a group of three to compete in a regional competition. How many ways can three members be chosen?

Solution:

$$C(4,3) = \frac{4!}{3!(4-3)!} = \frac{24}{6} = 4$$

There are 4 ways to chose 3 people for the competition when order is not important

The pigeonhole principle (PHP):

The general rule states when there are k pigeonholes and there are k+1 pigeons, then they will be 1 pigeonhole with at least 2 pigeons. A more advanced version of the principle will be the following: If mn + 1 pigeons are placed in n pigeonholes, then there will be at least one pigeonhole with m + 1 or more pigeons in it.

For **Example**, 13 people are involved in a survey to determine the month of their birthday. As we all know, there are 12 months in a year, thus, even if the first 12 people have their birthday from the month of January to the month of December, the 13^{th} person has to have his birthday in any of the month of January to December as well. Thus, by PHP we are right to say that there are at least 2 people who have their birthday falling in the same month.

In fact, we can view the problem as there are 12 pigeonholes (months of the year) with 13 pigeons (the 13 persons). Of course, by the Pigeonhole Principle, there will be at least one pigeonhole with 2 or more pigeons.

PRINCIPLE OF INCLUSION-EXCLUSION:

The **Principle of Inclusion and Exclusion** allows us to find the cardinality of a union of sets by knowing the cardinalities of the individual sets and all possible intersections of them.

The basic version of the Principle of Inclusion and Exclusion is that for two finite sets A and B, is

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

The result generalizes to three finite sets (in fact it generalizes to any finite number of finite sets):

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

Example :

In a room of 50 people whose dresses have either red or white color, 30 are wearing red dress, 16 are wearing a combination of red and white. How many are wearing dresses that have only white color?

Solution

Number of people wearing a red dress = 30

i.e., n(R) = 30

Number of people wearing a combination of red and white = 16

i.e., n (R $\cap$ W) = 16

The total number of people in the room = number of people who are wearing dresses that have either red or white colour = n (R $\cup$ W) = 50.

We know,

n (R $\cup$ W) = n(R) + n(W) - n(R $\cap$ W)

50 = 30 + n(W) - 16

50 - 14 = n(W) - 16

n(W) = 36

i.e., the number of people who are wearing a white dress = 36.

Therefore, number of people who are wearing white dress only = n(W) - n(R $\cap$ W) =

36 - 16 = 20

Example :

How many members of {1, 2, 3, ……., 105} have nontrivial factors in common with 105?

Solution

105 = 3 . 5. 7, so a number shares factors with 105 if and only if it is divisible by 3, 5, or 7.

Let A, B, and C be the members of {1, 2, 3, ……., 105} divisible by 3, 5, and 7 respectively.

Clearly |A| = 35, |B| = 21, and |C| = 15. Furthermore, A $\cap$B consists of those numbers divisible by both and 5, i.e., divisible by 15. Likewise, A $\cap$ C and B $\cap$ C contain multiples of 21 and 35

respectively, so |A $\cap$ B| = 7, |A $\cap$C| = 5, and |B $\cap$ C|= 3. Finally, A $\cap$ B$\cap$ C consists only of the number 105, so it has 1 member total. Thus,

|A U B U C| = 35 + 21 + 15 - 7 - 5 - 3 + 1 = 57

Example:

At Sunnydale High School there are 28 students in algebra class,30 students in biology class, and 8 students in both classes. How many students are in either algebra or biology class?

Solution:

Let A denote the set of students in algebra class and B denote the set of students in biology class. To find the number of students in either class, we first add up the students in each class:

$$|A| + |B|$$

However, this counts the students in both classes twice. Thus we have to subtract them once:$|A \cap B|$

This shows

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

$$|AUB|=28 + 30 - 8 = 50$$

so there are 50 students in at least one of the two classes.

Example:

At Sunnydale High School there are 55 students in either algebra, biology, or chemistry class 28 students in algebra class, 30 students in biology class, 24 students in chemistry class, 8 students in both algebra and biology, 16 students in both biology and chemistry, 5 students in both algebra and chemistry. How many students are in all three classes?

Solution:

Let A, B, C denote the set of students in algebra, biology, and chemistry class, Respectively. Then A U BU C is the set of students in one of the three classes, A∩B is the set of students in both algebra and biology, and so forth. To count the number of Students in all three classes, i.e. count | A U BU C |, we can first add all the number of students in all three classes:

$$|A| + |B|+|C|$$

However, now we've counted the students in two classes too many times. So we subtract out the students who are in each pair of classes:

$$-|A \cap B|-|A \cap C|-|B \cap C|$$

For students who are in two classes, we've counted them twice, then subtracted them once, so they're counted once. But for students in all three classes, we counted them 3 times, then subtracted them 3 times. Thus we need to add them again:$|A \cap B \cap C|$

Thus

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

$$55 = 28 + 30 + 24 - 8 - 16 - 5 + |A \cap B \cap C|$$

Thus $|A \cap B \cap C| = 2$, i.e. there are 2 students in all three classes.

RECURRENCE RELATION:

We are familiar with some problem solving techniques for counting, such as principles for addition, multiplication, permutations, combinations etc. But there are some problems which cannot be solved or very tedious to solve, using these techniques. In some such problems, the problems can be represented in the form of some relation and can be solved accordingly. We shall discuss some such examples before proceeding further.

The expression of higher terms in terms of combination of lower terms is known as recurrence relation

Example: The number of bacteria, double every hour, then what will be the population of the bacteria after 10 hours? Here we can represent number of bacteria at the n^{th} hour be a_n. Then, we can say that $a_n = 2a_{n-1}$.

Example: Consider the Fibonacci sequence

1, 1, 2, 3, 5, 8, 13,…

The recurrence relation is given by:

$$a_n = a_{n-1} + a_{n-2}, a_0 = a_1 = 1$$

Example : ***Towers of Hanoi*** is a popular puzzle. There are three pegs mounted on a board, together with disks of different sizes. Initially, these discs are placed on the first peg in order of different sizes, with the largest disc at the bottom and the smallest at the top. The task is to move the discs from the first peg to the third peg using the middle peg as auxiliary. The rules of the puzzle are:

- Only one disc can be moved at a time.
- No disc can be placed on the top of a smaller disc.

This is a popular puzzle and we shall discuss its solution, using the one of the techniques discussed in this chapter.

With these illustrations, we define recurrence relation now.

Definition: A recurrence relation for the sequence $\{a_n\}$ is an equation, that expresses a_n in terms of one or more of the previous terms of the sequence, namely, a_0, a_1, ..., a_{n-1}, for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer.

Example : $a_n = 1.06a_{n-1}$, with $a_0 = 0.5$.

Example : $a_n = 2a_{n-1} + 5$, with $a_0 = 1$.

The term a_0, given in the above two examples, specify **initial condition** to solve the recurrence relation completely.

FORMULATION OF RECURRENCE RELATION:

Before we proceed with discussing various methods of solving recurrence relation, we shall formulate some recurrence relation. The first example of formulation that we discuss is the problem of Tower of Hanoi as above.

Example: With reference to above Example, let H_n denote the number of moves required to solve the puzzle with n discs. Let us define H_n recursively.

Solution: Clearly, $H_1 = 1$.

Consider top $(n-1)$ discs. We can move these discs to the middle peg using H_{n-1} moves. The n^{th} disc on the first peg can then moved to the third peg. Finally, $(n-1)$ discs from the middle peg can be moved to the third peg with first peg as auxiliary in H_{n-1} moves. Thus, total number of moves needed to move n discs are: $H_n = 2H_{n-1} + 1$. Hence the recurrence relation for the Tower of Hanoi is:

$H_n = 1$ if $n = 1$.

$H_n = 2H_{n-1} + 1$ otherwise.

Example: Find recurrence relation and initial condition for the number of bit strings of length n that do not have two consecutive 0s.

Solution: Let a_n denote the number of bit strings of length n that do not contain two consecutive 0s. Number of bit strings of length one that follow the necessary rule are: string 0 and string 1. Thus, $a_1 = 2$. The number of bit strings of length 2 is: string 01, 10 and 11. Thus, $a_2 = 3$. Now we shall consider the case $n \geq 3$. The bit strings of length n that do not have two consecutive 0s are precisely those strings length n–1 with no consecutive 0s along with a 1 added 1 at the end of it (which is a_{n-1} in number) and bit strings of length n–2 with no consecutive 0s with a 10 added at the end of it (which is a_{n-2} in number). Thus, the recurrence relation is:

$a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$ with $a_1 = 2$ and $a_2 = 3$.

METHODS OF SOLVING RECURRENCE RELATION :

Now, in this section we shall discuss a few methods of solving recurrence relation and hence solve the relations that we have formulated in the previous section.

Backtracking Method:

This is the most intuitive way of solving a recurrence relation. In this method, we substitute for every term in the sequence in the form of previous term (i.e. a_n in the form of a_{n-1}, a_{n-1} in the form of a_{n-2} and so on) till we reach the initial condition and then substitute for the initial condition. To understand this better, we shall solve the recurrence relations that we have come across earlier.

Example: Solve the recurrence relation $a_n = 1.06a_{n-1}$, with $a_0 = 0.5$.

Solution: Given recurrence relation is $a_n = 1.06a_{n-1}$, with $a_0 = 0.5$. From this equation, we have $a_n = 1.06a_{n-1} = 1.06 \times 1.06\ a_{n-2} = 1.06 \times 1.06 \times 1.06\ a_{n-3}$ Proceeding this way, we have $a_n = (1.06)^n a_0$. But, we know that $a_0 = 0.5$.Thus, explicit solution to the given recurrence relation is $a_n = 0.5 \times (1.06)^n$ for $n \geq 0$.

Method for solving linear homogeneous recurrence relations with constant coefficients:

In the previous subsection, we have seen a backtracking method for solving recurrence relation. However, not all the equations can be solved easily using this method. In this subsection, we shall discuss the method of solving a type of recurrence relation called linear homogeneous recurrence relation. Before that we shall define this class of recurrence relation.

Definition : A ***linear homogeneous recurrence relation of degree k*** with constant coefficients is a recurrence relation of the form: $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$, where c_1, c_2, ..., c_k are constant real numbers with $c_k \neq 0$.

Example : Fibonacci sequence is also an example of a linear homogeneous recurrence relation of degree 2.

Example: The recurrence relation $a_n = a_{n-1}$ not linear (due to $+ an$-square term), whereas the relation $H_n = 2H_{n-1} + 1$ is not homogeneous (due to constant 1).

The basic approach for solving a linear homogeneous recurrence relation to look for the solution of the form $a_n = r^n$, where r is constant. Note that, r^n is a solution to the linear homogeneous recurrence relation of
degree k, if and only if;

$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \ldots + c_k r^{n-k}$. When both the sides of the equation are

divided by r^{n-k} and right side is subtracted from the left side, we obtain an equation, known as characteristic equation of the recurrence relation as
follows:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \ldots - c_{k-1} r - c_k = 0 .$$

The solutions of the equation are called as characteristic roots of the recurrence relation.

In this subsection, we shall focus on solving linear homogeneous recurrence relation of degree 2 that is: $a_n = c_1 a_{n-1} + c_2 a_{n-2}$.

The characteristic equation of this relation is $r^2 - c_1 r - c_2 = 0$. This is a quadratic equation and has two roots. Two cases arise.

(i) Roots are distinct, say s_1 and s_2. Then, it can be shown that $a_n = us_1^n + vs_2^n$ is a solution to the recurrence relation, with $a_1 = us_1 + vs_2$ and $a_2 = us_1^2 + vs_2^2$.

(ii) Roots are equal, say s. Then it can be shown that a_n solution to the recurrence relation is $a_n = (u + vn)s^n$

We shall use above results to solve some problems

Example : Solve the recurrence relation $b_n + 3b_{n-1} + 2b_{n-2} = 0$, with $b_1 = -2$ and $b_2 = 4$.

Solution: The characteristic equation to the given recurrence relation is $x^2 + 3x + 2 = 0$. Roots of this equation are $s_1 = -2$ and $s_2 = -1$. Hence the solution to the relation is:

$b_n = u(-1)^n + v(-2)^n$. $b_1 = -2 = -u - 2v$ and $b_2 = 4 = u + 4v$. Solving these two equations simultaneously, we get, $u = 0$ and $v = 1$. Thus, explicit solution to the given recurrence relation is $b_n = (-2)^n$

Method for solving linear non-homogeneous recurrence relations with constant coefficients:

The method is similar to the solution differential equation by method of undermined co-efficient.

GENERATING FUNCTION:

Let $a_0, a_1, ...a_n$ be a sequence, and then the corresponding generating function is given by:

$$A(x) = a_0 x^0 + a_1 x^1 + ... + a_n x^n$$

For **Example**, if 1, 1, 1,…. be a sequence then the corresponding generating function is given by:

$$A(x) = 1 + x + x^2 + ... = 1/(1-x)$$

From a given sequence we can find the corresponding generating function and vice versa.

Unit II

INTRODUCTION TO RELATIONS AND GRAPH THEORY

OBJECTIVES:

After going through this unit, you will be able to know:

- Definition of Relation.
- Representation of Relations
- Types of Relations
- Equivalence of relations
- Relations and Partition
- Definition and examples of partial order relation
- Representation of posets using Hasse diagram
- Closure of relations.
- Introduction to graphs
- Graph terminology
- Graph isomorphism
- Connectivity
- Euler and Hamilton paths
- Planar graphs
- Graph colouring
- Introduction to trees

INTRODUCTION :

Relationships between elements of sets occur in many contexts. We deal with many relationships such as student's name and roll no., teacher and her specialization, a person and a relative (brother – sister, mother – child etc.). In this section, we will discuss mathematical approach to the relation. These have wide applications in Computer science (e.g. relational algebra)

RELATIONS:

Relationship between elements of sets is represented using a mathematical structure called relation. The most intuitive way to describe the relationship is to represent in the form of ordered pair. In this section, we study the basic terminology and diagrammatic representation of relation.

Definition :

Let A and B be two sets. A **binary relation** from A to B is a subset of $A \times B$.

Note : If A, B and C are three sets, then a subset of $A \times B \times C$ is known as ternary relation. Continuing this way a subset of $A_1 \times A_2 \times ... \times A_n$ is known as n – ary relation.

Note: Unless or otherwise specified in this chapter a relation is a binary relation.

Let A and B be two sets. Suppose R is a relation from A to B (i.e. R is a subset of $A \times B$). Then, R is a set of ordered pairs where each first element comes from A and each second element from B. Thus, we denote it with an ordered pair (a, b), where $a \in A$ and $b \in B$. We also denote the relationship with $a\ R\ b$, which is read as a related to b. The ***domain*** of R is the set of all first elements in the ordered pair and the ***range*** of R is the set of all second elements in the ordered pair.

Example 1: Let $A = \{ 1, 2, 3, 4 \}$ and $B = \{ x, y, z \}$. Let $R = \{(1, x), (2, x), (3, y), (3, z)\}$. Then R is a relation from A to B.

Example 2: Suppose we say that two countries are adjacent if they have some part of their boundaries common. Then, "is adjacent to", is a relation R on the countries on the earth. Thus, we have, (India, Nepal) $\in R$, but (Japan, Sri Lanka) $\notin R$.

Example 3: A familiar relation on the set **Z** of integers is "m divides n". Thus, we have, $(6, 30) \in R$, but $(5, 18) \notin R$.

Example 4: Let A be any set. Then $A \times A$ and ϕ are subsets of $A \times A$ and hence they are relations from A to A. These are known as universal relation and empty relation, respectively.

Note : As relation is a set, it follows all the algebraic operations on relations that we have discussed earlier.

Definition : Let R be any relation from a set A to set B. The **inverse** of R, denoted by R^{-1}, is the relation from B to A which consists of those ordered pairs, when reversed, belong to R. That is:

$$R^{-1} = \{(b, a) : (a, b) \in R\}$$

Example 5:
Inverse relation of the relation in example 1 is, $R^{-1} = \{(x,), (x, 2), (y, 3), (z, 3)\}$.

REPRESENTATION OF RELATIONS:

Matrices and graphs are two very good tools to represent various algebraic structures. Matrices can be easily used to represent relation in any programming language in computer. Here we discuss the representation of relation on finite sets using these tools.

Consider the relation in Example1.

	x	y	z
1	1	0	0
2	1	0	0
3	0	1	1
4	0	0	0

Fig. 1

Thus, if $a\ R\ b$, then we enter 1 in the cell (a, b) and 0 otherwise. Same relation can be represented pictorially as well, as follows:

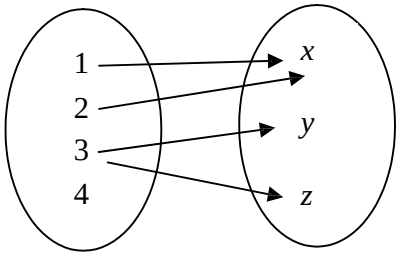


Fig 2

Thus, two ovals represent sets A and B respectively and we draw an arrow from $a \in A$ to $b \in B$, if $a\ R\ b$.

If the relation is from a finite set to itself, there is another way of pictorial representation, known as **diagraph**.

For example, let A = {1, 2, 3, 4} and R be a relation from A to itself, defined as follows:

R = {(1, 2), (2, 2), (2, 4), (3, 2), (3, 4), (4, 1), (4, 3)} Then, the diagraph of R is drawn as follows:

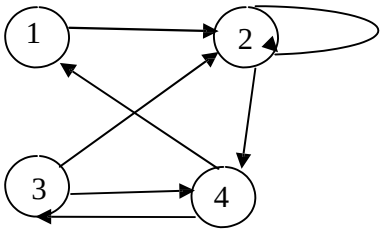


Fig 3

The directed graphs are very important data structures that have applications in Computer Science (in the area of networking).

Definition : Let A, B and C be three sets. Let R be a relation from A to B and S be a relation from B to C. Then, composite relation R°S, is a relation from A to C, defined by, a(R°S)c, if there is some b ∈ B, such that $a\ R\ b$ and $b\ S\ c$.

Example 6: Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$,$C = \{x, y, z\}$ and let $R = \{(1, a), (2, d), (3, a), (3, b), (3, d)\}$ and $S = \{(b, x), (b, z), (c, y), (d, z)\}$.

Pictorial representation of the relation in Example 6 can be shown as below (Fig 4).

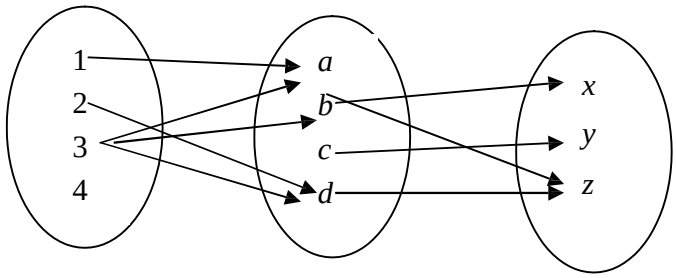


Fig.4

Thus, from the definition of composite relation and also from Fig 4, $R°S$ will be given as below.

$$R°S = \{(2, z), (3, x), (3, z)\}.$$

There is another way of finding composite relation, which is using matrices.

Example7: Consider relations R and S in Example 6. Their matrix representations are as follows.

$$M_R = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad M_S = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Consider the product of matrices M_R and M_S as follows: Observe that the non-zero entries in the product tell us which elements are related in $R \circ S$. Hence, $M_R M_S$ and $M_{R \circ S}$ have same non-zero entries.

TYPES OF RELATIONS:

In this section, we discuss a number of important types of relations defined from a set A to itself.

Definition : Let R be a relation from a set A to itself. R is said to be ***reflexive***, if for every $a \in A$, $a\ R\ a$ (a is related to itself).

Example 8: Let A = {a, b, c, d} and R be defined as follows: $R = \{(a, a), (a, c), (b, a), (b, b), (c, c), (d, c), (d, d)\}$. R is a reflexive relation.

Example 9: Let A be a set of positive integers and R be a relation on it defined as, $a\ R\ b$ if "a divides b". Then, R is a reflexive relation, as a divides to itself for every positive integer a.

Note : If we draw a diagraph of a reflexive relation, then all the vertices will have a loop. Also if we represent reflexive relation using a matrix, then all its diagonal entries will be 1.

Definition : Let R be a relation from a set A to itself. R is said to be ***irreflexive***, if for every $a \in A$, $a \not R a$

Example 10: Let A be a set of positive integers and R be a relation on it defined as, $a\ R\ b$ if "a is less than b". Then, R is an irreflexive relation, as a is not less than itself for any positive integer a.

Example 11: Let A = {a, b, c, d} and R be defined as follows: $R = \{(a, a), (a, c), (b, a), (b, d), (c, c), (d, c), (d, d)\}$.Here R is neither reflexive nor irreflexive relation as b is not related to itself and a, c, d are related to themselves.

Note : If we draw a diagraph of an irreflexive relation, then no vertex will have a loop. Also if we represent irreflexive relation using a matrix, then all its diagonal entries will be 0.

Definition : Let R be a relation from a set A to itself. R is said to be ***symmetric***, if for $a, b \in A$, if $a\ R\ b$ then $b\ R\ a$.

Definition : Let R be a relation from a set A to itself. R is said to be ***anti-symmetric***, if for $a, b \in A$, if $a\ R\ b$ and $b\ R\ a$, then $a = b$. Thus, R is not anti-symmetric if there exists $a, b \in A$ such that $a\ R\ b$ and $b\ R\ a$ but $a \neq b$.

Example 13: Let A = {1, 2, 3, 4} and R be defined as:
$R = \{(1, 2), (2, 3), (2, 1), (3, 2), (3, 3)\}$, then R is symmetric relation.

Example 14: An equality (or "is equal to") is a symmetric relation on the set of integers.

Example 15: Let $A = \{a, b, c, d\}$ and R be defined as: R = {(a, b), (b, a), (a, c), (c, d), (d, b)}. R is not symmetric, as $a\ R\ c$ but c R a . R is not anti-symmetric, because $a\ R\ b$ and $b\ R\ c$, but $a \neq b$.

.**Example 16:** The relation "less than or equal to (≤)", is an anti- symmetric relation.

Example 17: Relation "is less than (<)", defined on the set of all real numbers, is an asymmetric relation.

Definition : Let R be a relation defined from a set A to itself. R is said to ***transitive***, if for $a, b, c \in A$, $a\ R\ b$ and $b\ R\ c$, then $a\ R\ c$.

Example 18: Let $A = \{a, b, c, d\}$ and R be defined as follows: R = {(a,b), (a, c), (b, d), (a, d), (b, c), (d, c)}. Here R is transitive relation on A.

Example 19: Relation "a divides b", on the set of integers, is a transitive relation.

Definition : Let R be a relation defined from a set A to itself. If R is reflexive, symmetric and transitive, then R is called as **equivalence** relation.

Example 20: Consider the set L of lines in the Euclidean plane. Two lines in the plane are said to be related, if they are parallel to each other. This relation is an equivalence relation.

Example 21: Let m be a fixed positive integer. Two integers, a, b are said to be congruent modulo m, written as: $a \equiv b \pmod{m}$, if m divides $a - b$. The congruence relation is an equivalence relation.

Example 22 : Let $A = \{2, 3, 4, 5\}$ and let $R = \{(2, 3), (3, 3), (4, 5), (5, 1)\}$. Is R symmetric, asymmetric or antisymmetric

Solution :

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

b) R is not asymmetric since $(3,3) \in R$

c) R is antisymmetric.

Example 23 : Determine whether the relation R on a set A is reflexive, irreflexire, symmetric, asymmetric antisymmetric or transitive.

I) A = set of all positive integers, a R b iff $a - b \leq 2$.

Solution :

1) R is reflexive because $|a - a| = 0 < 2, \forall\, a \in A$

2) R is not irreflexive because $|1-1| = 0 < 2$ for $1 \in A$ ($\therefore$ A is the set of all positive integers.)

3) R is symmetric because $|a - b| \leq 2 \Rightarrow |b - a| \leq 2 \;\; \therefore a\, R\, b \Rightarrow b\, R\, a$

4) R is not asymmetric because $|5 - 4| \leq 2$ and we have $|4 - 5| \leq 2$
$\therefore 5\, R\, 4 \Rightarrow 4\, R\, 5$

5) R is not antisymmetric because $1\, R\, 2$ & $2\, R\, 1$ $1\, R\, 2 \Rightarrow |1 - 2| \leq 2$ & $2\, R\, 1 \Rightarrow |2 - 1| \leq 2$. But $1 \neq 2$

6) R is not transitive because 5 R 4, 4 R 2 but 5 $\not R$ 2

II) $A = Z^+$, $a\, R\, b$ iff $|a - b| = 2$

Solution :

As per above example we can prove that R is not reflexive, R is irreflexive, symmetric, not asymmetric, not antisymmetric & not transitive

III) Let A = {1, 2, 3, 4} and R {(1,1), (2,2), (3,3)}

1) R is not reflexive because $(4,4) \notin R$

2) R is not irreflexive because $(1,1) \notin R$

3) R is symmetric because whenever a R b then b R a.

4) R is not asymmetric because $|R| \Rightarrow |R|$

5) R is antisymmetric because $2\, R\, 2, 2\, R\, 2 \Rightarrow 2 = 2$

6) R is transitive.

IV) Let $A = Z^+$, $a\, R\, b$ iff GCD (a, b) = 1 we can say that a and b are relatively prime.

1) R is not reflexive because $(3,3) \neq 1$ it is 3. $\therefore (3,3) \notin R$

2) R is not irreflexive because (1, 1) = 1

3) R is symmetric because for $(a,b)=1 \Rightarrow (b,a)=1$. $\therefore a\ R\ b \rightarrow b\ R\ a$

4) R is not asymmetric because (a, b) = 1 then (b, a) = 1. $\therefore a\ R\ b \rightarrow b\ R\ a$

5) R is not antisymmetric because 2 R 3 and 3 R 2 but $2 \neq 3$.

6) R is not transitive because 4 R 3, 3 R 2 but 4 $\not R$ 2 because (4,2) = G.C.D. (4,2) = $2 \neq 1$.

V) A = Z a R b iff $a \leq b+1$

1) R is reflexive because $a \leq a+1 \ \forall\ a \in |\ A$.

2) R is not irreflexive because $0 \leq 0+1$ for $O \in A$.

3) R is not symmetric because for $2 \leq 5+1$ does not imply $5 \leq 2+1$.

4) R is not asymmetric because for (2,3) $\in$ R and also (3,2) $\in$ R.

5) R is not antisymmetric because 5 R 4 and 4 R 5 but $4 \neq 5$.

6) R is not transitive because (6,45) $\in$ R, (5,4) $\in$ R but (6,47) $\notin$ R.

RELATIONS AND PARTITION:

In this section, we shall know what partitions are and its relationship with equivalence relations.

Definition : A partition or a quotient set of a non-empty set *A* is a collection P of non-empty sets of *A*, such that

(i) Each element of *A* belongs to one of the sets in P.

(ii) If A_1 and A_2 are distinct elements of P, then $A_1 \cap A_2 = \phi$.

The sets in P are called the blocks or cells of the partition.

Example : Let *A* = {1, 2, 3, 4, 5}. The following sets form a partition of *A*, as *A* = $A_1 \cup A_2 \cup A_3$ and $A_1 \cap A_2 = \phi$, $A_1 \cap A_3 = \phi$, and $A_2 \cap A_3 = \phi$.
A_1 = {1, 2}; A_2 = {3, 5}; A_3 = {4}.

Example 24: Let *A* = {1, 2, 3, 4, 5, 6}. The following sets do not form a partition of *A*, as

A = $A_1 \cup A_2 \cup A_3$ but $A_2 \cap A_3 \neq \phi$.A_1 = {1, 2}; A_2 = {3, 5}; A_3 = {4, 5, 6}.

The following result shows that if P is a partition of a set A, then P can be used to construct an equivalence relation on A.

Theorem: Let P be a partition of a set *A*. Define a relation *R* on *A* as *a R b* if and only if *a*, *b* belong to the same block of P then *R* is an equivalence relation on *A*.

Example 25: Consider the partition defined in Example 23. Then the equivalence relation as defined from the partition is:

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

Now, we shall define equivalence classes of R on a set A.

Theorem: Let R be an equivalence relation on a set A and let $a, b \in A$, then $a \, R \, b$ if and only if $R(a) = R(b)$, where $R(a)$ is defined as: $R(a) = \{x \in A: a \, R \, x\}$. $R(a)$ is called as **relative set** of a.

Example26: If we consider an example in 25, we observe that, $R(1) = R(2)$, $R(3) = R(5)$.

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

Earlier, we have seen that, a partition defines an equivalence relation. Now, we shall see that, an equivalence relation defines a partition.

Theorem: Let R be an equivalence relation on A and let P be the collection of all distinct relative sets R(a) for a $\in$ A. Then P is a partition of A and R is equivalence relation of this partition.

Note: If R is an equivalence relation on A, then sets $R(a)$ are called as equivalence classes of R.

Example 27: Let A = {1, 2, 3, 4} and R = {(1, 1), (1, 2), (2, 1), (2, 2), (3,4), (4, 3), (3, 3), (4, 4)}. We observe that $R(1) = R(2)$ and $R(3) = R(4)$ and hence P = { {1, 2}, {3, 4} }.

Example 28: Let A = Z (set of integers) and define R as

$R = \{(a, b) \in A \times A: a \equiv b \pmod 5\}$. Then, we have,

$R(1)$ = {.....,–14, –9, –4, 1, 6, 11, ... }

$R(2)$ = {.....,–13, –8, –3, 2, 7, 12, ... }

$R(3)$ = {.....,–12, –7, –2, 3, 8, 13, ... }

$R(4)$ = {.....,–11, –6, –1, 4, 9, 14, ... }

$R(5)$ = {.....,–10, –5, 0, 5, 10, 15, ... }.

$R(1)$, $R(2)$, $R(3)$, $R(4)$ and $R(5)$ form partition on Z with respect to given equivalence relation.

PARTIAL ORDER RELATION

We often use relation to describe certain ordering on the sets. For example, lexicographical ordering is used for dictionary as well as phone directory. We schedule certain jobs as per certain ordering, such as priority. Ordering of numbers may be in the increasing order.

In the previous chapter, we have discussed various properties (reflexive etc) of relation. In this chapter we use these to define ordering of the sets.

Definition 1: A relation R on the set A is said to be ***partial order relation***, if it is reflexive, anti-symmetric and transitive.

Before we proceed further, we shall have a look at a few examples of partial order relations.

Example 1: Let $A = \{a, b, c, d, e\}$. Relation R, represented using following matrix is a partial order relation.

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

Observe the reflexive, anti-symmetric and transitive properties of the relation from the matrix.

Example 2: Let A be a set of natural numbers and relation R be "less than or equal to relation ($\leq$)". Then R is a partial order relation on A. For any $m, n, k \in N$, $n \leq n$ (reflexive); if $m \leq n$ and $m \geq n$, then $m = n$ (anti-symmetric); lastly, if $m \leq n$ and $n \leq k$, then $m \leq k$ (transitive).

Definition : If R is a partial order relation on a set A, then A is called as partial order set and it is denoted with (A, R). Typically this set is termed as ***poset*** and the pair is denoted with $(A, \leq)$.

DIAGRAMMATIC REPRESENTATIONOF PARTIAL ORDER RELATIONS AND POSETS:

In the previous chapter, we have seen the diagraph of a relation. In this section, we use the diagraphs of the partial order relations, to represent the relations in a very suitable way where there no arrowhead and transitivity shown indirectly known as Hasse diagram.

We understand the Hasse diagram, using following example.

Example 1: Let $A = \{a, b, c, d, e\}$ and the following diagram represents the diagraph of the partial order relation on A.

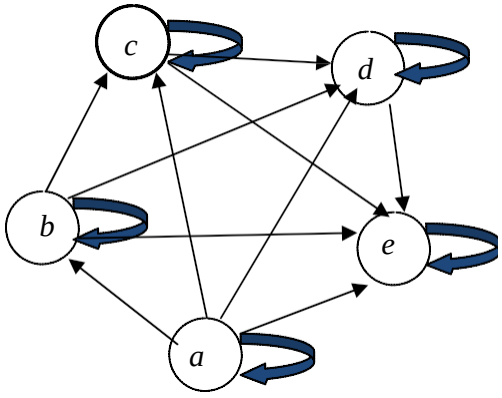


Fig.1

Now, we shall draw Hasse diagram from the above diagrams using following rules.

(i) Drop the reflexive loops

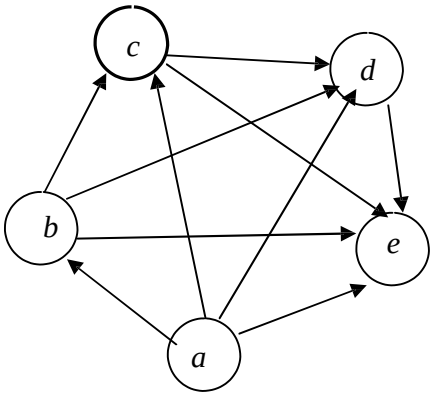


Fig. 2

(ii) Drop transitive lines

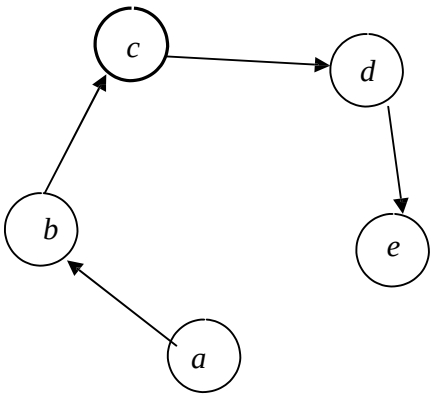


Fig. 3

(iii)Drop arrows

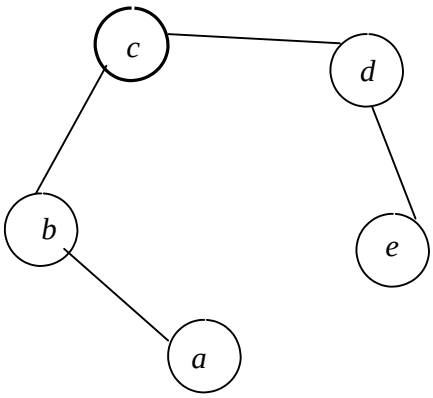


Fig.4

Note : In many cases, when the graphical representation is so oriented that all the arrow heads point in one direction (upward, downward, left to right or right to left). A graphical representation in which all the arrowheads point upwards, is known as Hasse diagram.

Example 4: `Let A = {1, 2, 3, 4, 6, 9} and relation R defined on A be " a divides b". Hasse diagram for this relation is as follows:

Note : The reader is advised to verify that this relation is indeed a partial order relation. Further, arrive at the following Hasse diagram from the diagraph of a relation as per the rules defined earlier.

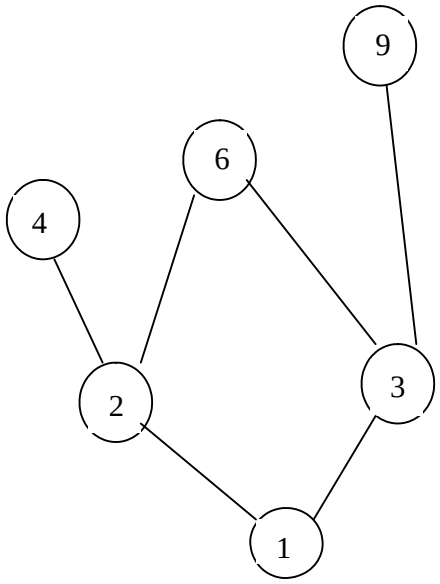


Fig.5

Example 5 : Determine the Hasse diagram of the relation on A = {1,2,3,4,5} whose M_R is given below :

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

Solution :

Reflexivity is represented by 1 at diagonal place. So after removing reflexivity R is R = {(1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5)}

Remove transitivity as

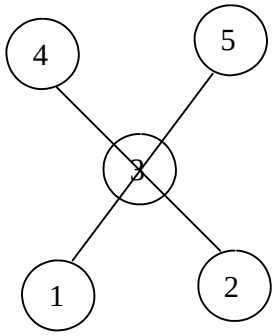
$(1,3)(3,4) \in R$

$\therefore$ remove $(1,4) \in R$

$(2,3)(3,5) \in R \ \therefore$ remove $(2,5) \in R$ and so on.

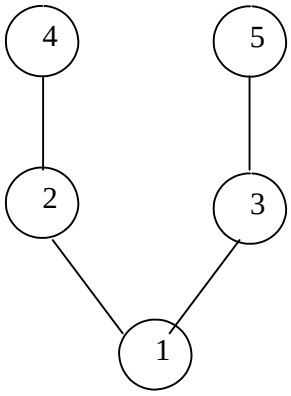
$\therefore R = \{(1,3),(2,3),(3,4),(3,5)\}$

The Hasse Diagram is



Example 6 :

Determine matrix of partial order whose Hasse diagram is given as follow -



Solution :

Here A = [1, 2, 3, 4, 5)

Write all ordered pairs (a, a) $\forall \ a \in A$ i.e. relation is reflexive.

Then write all ordered pairs in upward direction. As $(1, 2) \in R$ & $(2,4) \in R \Rightarrow (1,4) \in R$ since R is transitive.

$$\therefore R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,4), (2,4), (1,4), (1,3), (3,5), (1,5)\}$$

The matrix M_R can be written as -

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

Now, we shall have a look at certain terms with reference to posets.

Definition : Let $(A, \leq)$ be a partially ordered set. Elements $a, b \in A$, are said to be comparable, if $a \leq b$ or $b \leq a$.
E.g. In example 4, 2 and 4 are comparable, whereas 4 and 9 are not comparable.

Definition : Let $(A, \leq)$ be a partially ordered set. A subset of A is said to be a ***chain*** if every two elements in the subset are related.

Example 7: In the poset of example 4, subsets {1, 2, 4}; {1, 3, 6};{1, 2, 6} and {1, 3, 9} are chains.

Definition : A subset of a poset A is said to be ***anti-chain***, if no two elements of it are related.

Example 8: In the poset of example 4, subsets {2, 9}; {3, 4}; {4, 6, 9}are anti-chains.

Definition : A partially ordered set A is said to be ***totally ordered*** if it is chain.

Example 9: Let A = {2, 3, 5, 7, 11, 13, 17, 19} and the relation defined on A be $\leq$.
Then poset $(A, \leq)$ is a chain.

CLOSURE PROPERTIES

Consider a given set A and let R be a relation on A. Let P be a property of such relations, such as being reflexive or symmetric or transitive. A relation with property P will be called a P-relation. The P-closure of an arbitrary relation R on A, written P (R), is a P-relation such that

$$R \subseteq P(R) \subseteq S$$

for every *P*-relation *S* containing *R*. We will write

$$\text{reflexive}(R), \text{symmetric}(R), \text{and} \quad \text{transitive}(R)$$

for the reflexive, symmetric, and transitive closures of *R*.

Generally speaking, P (R) need not exist. However, there is a general situation where P (R) will always exist. Suppose *P* is a property such that there is at least one *P*-relation containing *R* and that the intersection of any *P*-relations is again a *P*-relation. Then one can prove that

$$P(R) = \cap(S \mid S \text{ is a } P\text{-relation and } R \subseteq S)$$

Thus one can obtain P (R) from the "top-down," that is, as the intersection of relations. However, one usually wants to find P (R) from the "bottom-up," that is, by adjoining elements to *R* to obtain P (R). This we do below.

Reflexive and Symmetric Closures

The next theorem tells us how to obtain easily the reflexive and symmetric closures of a relation. Here

$A = \{(a, a) \mid a \in A\}$ is the diagonal or equality relation on *A*.

Theorem: Let *R* be a relation on a set *A*. Then:

(i) $R \cup A$ is the reflexive closure of *R*.

(ii) $R \cup R^{-1}$ is the symmetric closure of *R*.

In other words, reflexive(*R*) is obtained by simply adding to *R* those elements (a, a) in the diagonal which do not already belong to *R*, and symmetric(*R*) is obtained by adding to *R* all pairs (b, a) whenever (a, b) belongs to *R*.

EXAMPLE 10 Consider the relation $R = \{(1, 1), (1, 3), (2, 4), (3, 1), (3, 3), (4, 3)\}$ on the set $A = \{1, 2, 3, 4\}$.

Then

$$\text{reflexive}(R) = R \cup \{(2, 2), (4, 4)\} \quad \text{and symmetric}(R) = R \cup \{(4, 2), (3, 4)\}$$

Transitive Closure

Let *R* be a relation on a set *A*. Recall that $R^2 = R \circ R$ and $R^n = R^{n-1} \circ R$. We define The following theorem applies:

Theorem : R^* is the transitive closure of *R*.

Suppose *A* is a finite set with *n* elements. We show

$$R* = R \cup R^2 \cup \ldots \cup R^n$$

This gives us the following theorem:

Theorem : Let *R* be a relation on a set *A* with *n* elements. Then

$$\text{transitive } (R) = R \cup R^2 \cup \ldots \cup R^n$$

EXAMPLE 11 Consider the relation R = {(1, 2), (2, 3), (3, 3)} on A = {1, 2, 3}.

Then:

$R^2 = R \circ R = \{(1, 3), (2, 3), (3, 3)\}$ and $R^3 = R^2 \circ R = \{(1, 3), (2, 3), (3, 3)\}$

Accordingly,

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

MAXIMAL, MINIMAL ELEMENTS AND LATTICES:

In this section, we discuss certain element types in the poset and hence a special kind of poset, Lattice.

To understand these types, we shall refer to the following figures, i.e. Fig.6 and Fig.7.

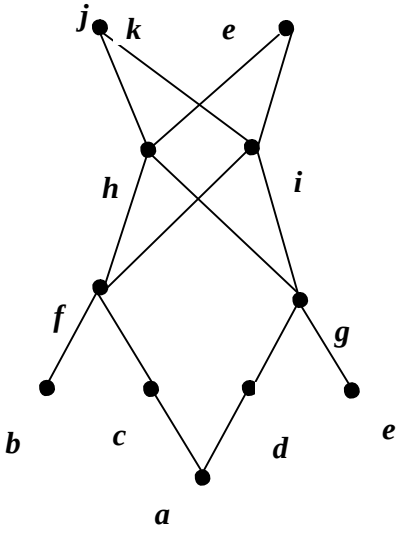


Fig. 6

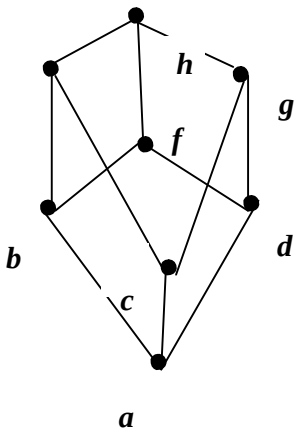


Fig. 7

Definition : Let $(A, \leq)$ be a poset. An element $a \in A$ is called a ***maximal element***, if for no $b \in A$, $a \neq b$, $a \leq b$. E.g. In Fig. 4, j and k are maximal elements.

Definition : Let $(A, \leq)$ be a poset. An element $a \in A$ is called a ***minimal element***, if for no $b \in A$, $a \neq b$, $b \leq a$. E.g. In Fig. 4.6, a, b and e are minimal elements.

Definition : Let a, b be two elements in the poset $(A, \leq)$. An element $c \in A$, is said to be an ***upper bound*** of a, b if $a \leq c$ and $b \leq c$. E.g. In Fig 7, f_1 h are upper bounds of b and d.

Definition : Let a, b be two elements in the poset $(A, \leq)$. An element $c \in A$, is said to be a ***least upper bound*** of a, b if $a \leq c$ and $b \leq c$ and if d is an upper bound of a, b, then $c \leq d$. E.g. In Fig 2, f is a least upper bound of b and d.

Definition : Let a, b be two elements in the poset $(A, \leq)$. An element $c \in A$, is said to be a ***lower bound*** of a, b if $c \leq a$ and $c \leq b$. E.g. In Fig 6, f, g are lower bounds of h and i.

Definition : Let a, b be two elements in the poset $(A, \leq)$. An element $c \in A$, is said to be a ***greatest lower bound*** of a, b if $c \leq a$ and $c \leq b$ and if d is a lower bound of a, b, then $d \leq c$. E.g. In Fig 4, c is a greatest lower bound of e and g.

Definition : A poset $(A, \leq)$ is said to be a ***lattice***, if every two elements in A have a unique least upper bound and a unique greatest lower bound.

E.g. Fig. 6 is not a lattice, because j and k are two least upper bounds of h and i, whereas Fig. 7 is a lattice.

Graph Theory

Graphs with Basic Terminology

The fundamental concept of graph theory is the graph, which (despite the name) is best thought of as a mathematical object rather than a diagram, even though graphs have a very natural graphical representation. A graph – usually denoted G(V,E) or G = (V,E) – consists of set of vertices V together with a set of edges E. Vertices are also known as nodes, points and (in social networks) as actors, agents or players. Edges are also known as lines and (in social networks) as ties or links. An edge e = (u,v) is defined by the unordered pair of vertices that serve as its end points. Two vertices *u* and *v* are *adjacent* if there exists an edge (*u*,*v*) that connects them. An edge e = (u,u) that links a vertex to itself is known as a *self-loop* or *reflexive* tie. The number of vertices in a graph is usually denoted *n* while the number of edges is usually denoted *m*.

As an example, the graph depicted in Figure 1 has vertex set V={a,b,c,d,e.f} and edge set E = {(a,b),(b,c),(c,d),(c,e),(d,e),(e,f)}.

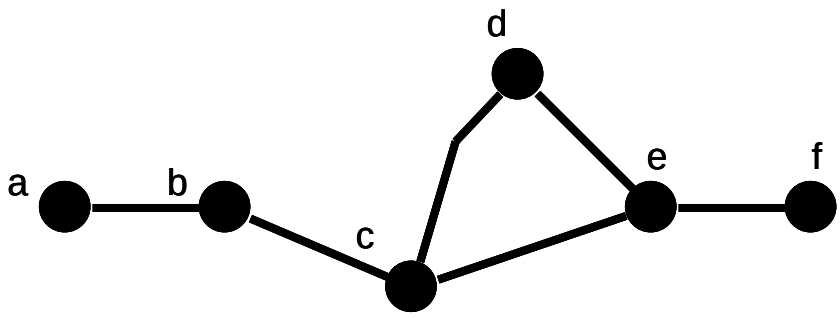


Figure 1.

When looking at visualizations of graphs such as Figure 1, it is important to realize that the only information contained in the diagram is adjacency; the position of nodes in the plane (and therefore the length of lines) is arbitrary unless otherwise specified. Hence it is usually dangerous to draw conclusions based on the spatial position of the nodes. For example, it is tempting to conclude that nodes in the middle of a diagram are more important than nodes on the peripheries, but this will often – if not usually – be a mistake.

When used to represent social networks, we typically use each line to represent instances of the same social relation, so that if *(a,b)* indicates a friendship between the person located at node a and the person located at node b, then *(d,e)* indicates a friendship between *d* and *e*. Thus, each distinct social relation that is empirically measured on the same group of people is represented by separate graphs, which are likely to have different structures (after all, who talks to whom is not the same as who dislikes whom).

Every graph has associated with it an adjacency matrix, which is a binary $n \times n$ matrix A in which $a_{ij} = 1$ and $a_{ji} = 1$ if vertex vi is adjacent to vertex vj, and aij = 0 and aji = 0 otherwise. The natural graphical representation of an adjacency matrix is a table, such as shown in Figure 2.

	a	b	c	d	e	f
a	0	1	0	0	0	0
B	1	0	1	0	0	0
c	0	1	0	1	1	0
D	0	0	1	0	1	0
e	0	0	1	1	0	1
f	0	0	0	0	1	0

Figure 2. Adjacency matrix for graph in Figure 1.

Examining either Figure 1 or Figure 2, we can see that not every vertex is adjacent to every other. A graph in which all vertices are adjacent to all others is said to be *complete*. The extent to which a graph is complete is indicated by its density, which is defined as the number of edges divided by the number possible. If self-loops are excluded, then the number possible is $n(n-1)/2$. If self-loops are allowed, then the number possible is $n(n+1)/2$. Hence the density of the graph in Figure 1 is $6/15 = 0.40$.

A *clique* is a *maximal complete subgraph*. A *subgraph* of a graph *G* is a graph whose points and lines are contained in *G*. A complete subgraph of *G* is a section of *G* that is complete (i.e., has density = 1). A maximal complete subgraph is a subgraph of *G* that is complete and is maximal in the sense that no other node of *G* could be added to the subgraph without losing the completeness property. In Figure 1, the nodes {c,d,e}

together with the lines connecting them form a clique. Cliques have been seen as a way to represent what social scientists have called primary groups.

hile not every vertex in the graph in Figure 1 is adjacent, one can construct a sequence of adjacent vertices from any vertex to any other. Graphs with this property are called *connected*. Similarly, any pair of vertices in which one vertex can reach the other via a sequence of adjacent vertices is called *reachable*. If we determine reachability for every pair of vertices, we can construct a reachability matrix R such as depicted in Figure 3. The matrix R can be thought of as the result of applying transitive closure to the adjacency matrix A.

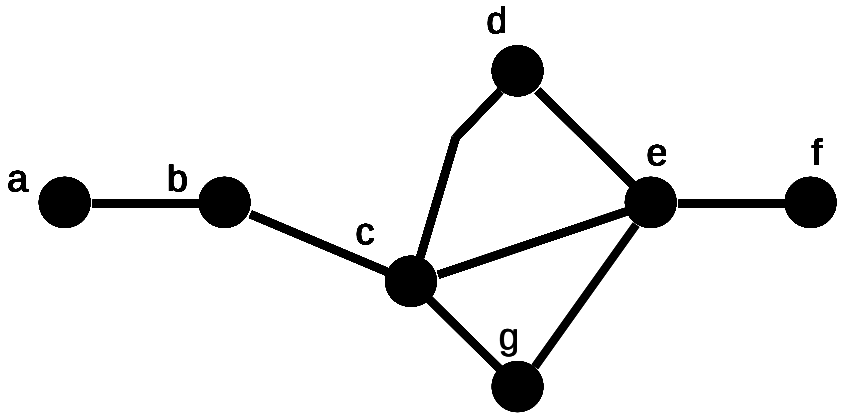


Figure 3.

A *component* of a graph is defined as a maximal subgraph in which a path exists from every node to every other (i.e., they are mutually reachable). The size of a component is defined as the number of nodes it contains. A connected graph has only one component.

A sequence of adjacent vertices $v_0,v_1,\ldots,v_n$ is known as a *walk*. In Figure 3, the sequence *a,b,c,b,a,c* is a walk. A walk can also be seen as a sequence of *incident* edges, where two edges are said to be incident if they share exactly one vertex. A walk in which no vertex occurs more than once is known as a *path*. In Figure 3, the sequence *a,b,c,d,e,f* is a path. A walk in which no edge occurs more than once is known as a *trail*. In Figure 3, the sequence *a,b,c,e,d,c,g* is a trail but not a path. Every path is a trail, and every trail is a walk. A walk is closed if $v_o = v_n$. A *cycle* can be defined as a closed path in which $n >= 3$. The sequence *c,e,d* in Figure 3 is a cycle. A *tree* is a connected graph that contains no cycles. In a tree, every pair of points is connected by a unique path. That is, there is only one way to get from A to B.

The length of a walk (and therefore a path or trail) is defined as the number of edges it contains. For example, in Figure 3, the path *a,b,c,d,e* has length 4. A walk between two vertices whose length is as short as any other walk connecting the same pair of vertices

is called a *geodesic*. Of course, all geodesics are paths. Geodesics are not necessarily unique. From vertex *a* to vertex *f* in Figure 1, there are two geodesics: *a,b,c,d,e,f* and *a,b,c,g,e,f*.

The *graph-theoretic distance* (usually shortened to just "distance") between two vertices is defined as the length of a geodesic that connects them. If we compute the distance between every pair of vertices, we can construct a distance matrix *D* such as depicted in Figure 4. The maximum distance in a graph defines the graph's *diameter*. As shown in Figure 4, the diameter of the graph in Figure 1 is 4. If the graph is not connected, then there exist pairs of vertices that are not mutually reachable so that the distance between them is not defined and the diameter of such a graph is also not defined.

	a	B	c	d	e	f	G
a	0	1	2	3	3	4	3
b	1	0	1	2	2	3	2
c	2	1	0	1	1	2	1
d	3	2	1	0	1	2	2
e	3	2	1	1	0	1	1
f	4	3	2	2	1	0	2
g	3	2	1	2	1	2	0

Figure 4. Distance matrix for graph in Figure 3.

The powers of a graph's adjacency matrix, A^p, give the number of walks of length *p* between all pairs of nodes. For example, A^2, obtained by multiplying the matrix by itself, has entries a_{ij}^2 that give the number of walks of length 2 that join node v_i to node v_j. Hence, the geodesic distance matrix *D* has entries $d_{ij} = p$, where *p* is the smallest *p* such that $a_{ij}^p > 0$. (However, there exist much faster algorithms for computing the distance matrix.)

The *eccentricity e(v)* of a point *v* in a connected graph G(V,E) is max d(u,v), for all $u \in V$. In other words, a point's eccentricity is equal to the distance from itself to the point farthest away. The eccentricity of node *b* in Figure 3 is 3. The minimum eccentricity of all points in a graph is called the radius r(G) of the graph, while the maximum eccentricity is the diameter of the graph. In Figure 3, the radius is 2 and the diameter is 4. A vertex that is least distant from all other vertices (in the sense that its eccentricity

equals the radius of the graph) is a member of the *center* of the graph and is called a *central point*. Every tree has a center consisting of either one point or two adjacent points.

Directed Graphs

As noted at the outset, the edges contained in graphs are unordered pairs of nodes (i.e., *(u,v)* is the same thing as *(v,u)*). As such, graphs are useful for encoding directionless relationships such as the social relation "sibling of" or the physical relation "is near". However, many relations that we would like to model are not directionless. For example, "is the boss of" is usually anti-symmetric in the sense that if *u* is the boss of *v*, it is unlikely that *v* is the boss of *u*. Other relations, such as "gives advice to" are simply non-symmetric in the sense that if *u* gives advice to *v*, *v* may or may not give advice to *u*.

To model non-symmetric relations we use *directed graphs*, also known as *digraphs*. A digraph *D(V,E)* consists of a set of nodes *V* and a set of ordered pairs of nodes *E* called *arcs* or directed lines. The arc *(u,v)* points from *u* to *v*.

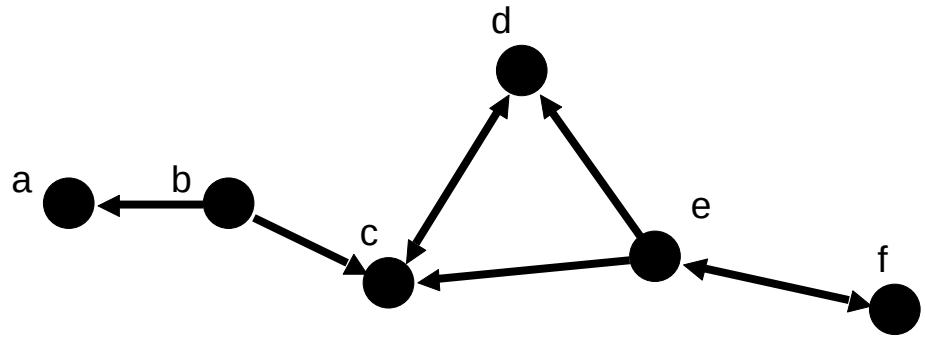


Figure 5a

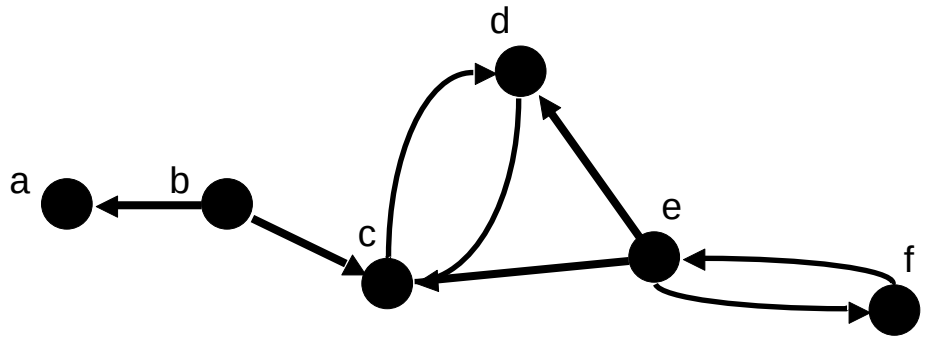


Figure 5b

Digraphs are usually represented visually like graphs, except that arrowheads are placed on lines to indicate direction (see Figure 5). When both arcs *(u,v)* and *(v,u)* are present in a digraph, they may be represented by a double-headed arrow (as in Figure 5a), or two separate arrows (as shown in Figure 5b).

In a digraph, a *walk* is a sequence of nodes $v_o,v_1,\ldots v_n$ in which each pair of nodes v_i, v_i+1 is linked by an arc (v_i,v_i+1). In other words, it is a traversal of the graph in which the flow of movement follows the direction of the arcs, like a car moving from place to place via one-way streets. A *path* in a digraph is a walk in which all points are distinct. A *semiwalk* is a sequence of nodes $v_o,v_1,\ldots v_n$ in which each pair of nodes v_i, v_i+1 is linked by either the arc (v_i,v_i+1) or the arc (v_i+1,v_i). In other words, in a semiwalk, the traversal need not respect the direction of arcs, like a car that freely goes the wrong way on one-way streets. By analogy, we can also define a *semipath*, *semitrail*, and *semicycle*.

Another way to think of semiwalks is as walks on the *underlying graph*, where the underlying graph is the graph *G(V,E)* that is formed from the digraph *D(V,E')* such that $(u,v) \in E$ if and only if $(u,v) \in E'$ or $(v,u) \in E'$. Thus, the underlying graph of a digraph is basically the graph formed by ignoring directionality.

A digraph is *strongly connected* if there exists a path (not a semipath) from every point to every other. Note that the path from *u* to *v* need not involve the same intermediaries as the path from *v* to *u*. A digraph is unilaterally connected if for every pair of points there is a path from one to the other (but not necessarily the other way around). A digraph is *weakly connected* if every pair of points is mutually reachable via a semipath (i.e., if the underlying graph is connected).

A *strong component* of a digraph is a maximal strongly connected subgraph. In other words, it is a subgraph that is strongly connected and which is as large as possible (there is no node outside the subgraph that is strongly connected to all the nodes in the subgraph). A *weak component* is a maximal weakly connected subgraph.

The number of arcs originating from a node *v* (i.e., outgoing arcs) is called the *outdegree* of *v*, denoted *od(v)*. The number of arcs pointing to a node *v* (i.e., incoming arcs) is called the *indegree* of *v*, denoted *id(v)*. In a graph representing friendship feelings

among a set of persons, *outdegree* can be seen as indicating gregariousness, while *indegree* corresponds to popularity. The average *outdegree* of a digraph is necessarily equal to the average *indegree*.

The *adjacency matrix* A of a digraph is an $n \times n$ matrix in which $a_{ij} = 1$ if $(v_i,v_j) \in E$ and $a_{ij} = 0$ otherwise. Unlike the adjacency matrix of an undirected graph, the adjacency matrix of a directed graph is not constrained to be symmetric, so that the top right half need not equal the bottom left half (i.e., $a_{ij} <> a_{ji}$). If a digraph is acyclic, then it is possible to order the points of D so that the adjacency matrix upper triangular (i.e., all positive entries are above the main diagonal).

Some notations

K_n : the complete graph on n vertices.

C_n : the n-cycle graph.

$K_{m,n}$: the complete bipartite graph on m+n vertices and mn edges..

$K_{1,n}$: the star graph on n+1 vertices.

mK_n : m disjoint copies of K_n.

Paths and Circuits

- *chain* : A sequence of vertices $[v_0, v_1, v_2, \ldots v_l]$ is a chain of length *l* in *G* if $v_{i-1}v_i \in E \text{ or } v_iv_{i-1} \in E$ for *i*=1,2, ...,*l*.
- *path* : A sequence of vertices $[v_0, v_1, v_2, \ldots v_l]$ is a *path from v_0 to v_l of length l* in *G* if $v_{i-1}v_i \in E$ for *i*=1,2, ...,*l*.
- *simple* path: It does not include the same edge twice.
- *elementary* path(or chain): A path or chain in *G* is called *elementary* if no vertex occurs more than once.
- *connected graph* : A graph *G* is *connected* if between any two vertices there exists a path in *G* joining them.
- strongly *connected graph* : A graph *G* is *strongly connected* if for any two vertices *x* and *y* there exists a path in *G* from *x* to *y*.
- *elementary cycle(circuit)* : A *cycle* $[v_0, v_1, v_2, \ldots v_l, v_0]$ is a *elementary cycle* if $v_i \neq v_j$ for $i \neq j$.

- *chordless cycle* : A simple cycle $[v_0, v_1, v_2, \ldots v_l, v_0]$ is *chordless* if $v_i\, v_j \notin E$ for i and j differing by more than 1 mod l+1.
- **Theorem :** In a (directed or undirected) graph with n vertices, if there is a path from vertex v_1 to vertex v_2, then there is a path of no more than n-1 edges from v_1 to vertex v_2.
- *bipartite graph* : An undirected graph $G=(V,E)$ is bipartite if its vertices can be partitioned into two disjoint stable sets $V=S_1+S_2$.

complete bipartite graph : A bipartite graph $G=(S_1,S_2,E)$ is *complete* if for every $x \in S_1$ and $y \in S_2$ we have $xy \in E$, i.e., every possible edge that could exist does exist.

Eulerian Paths and Circuits

- L. Euler, the father of the graph theorysolved the Königsberg's bridge problem, 1736
- Eulerian path problem : a path that traverses each edge in the graph once and only once.
- **Theorem:** An undirected graph possess an Eulerian path if and only if it is connected and has either zero or two vertices of odd degree.

Proof. ($\Rightarrow$) Suppose that the graph possess an Eulerian path. It must be connected.

When the eulerian path is traced, we observe that every time the path meets a vertex, it goes through two edges which are incident with the vertex and have not been traced before.

Thus, except for the two vertices at the ends of the path, the degree of any vertex in the graph must be even.

($\Leftarrow$) omitted.

- **Theorem:** An undirected graph possess an Eulerian circuit if and only if it is connected and has no vertices of odd degree.
- **Theorem :** An directed graph possess an Eulerian circuit if and only if it is connected and the incoming degree of every vertex is equal to its outgoing degree.
- An directed graph possess an eulerian path if and only if it is connected and the incoming degree of every vertex is equal to its outgoing degree with the possible exception of two vertices. For these two vertices, the incoming degree of one is one larger than its outgoing degree, and the incoming degree of the other is one less than its outgoing degree.

Hamiltonian Paths and Circuits

- *Hamiltonian path* : A path that passes through each of the vertices in a graph exactly once.
- No simple necessary and sufficient condition is known for graph to have a Hamiltonian path or circuit.
- **Theorem :** *Let G be a <u>linear</u> graph of n vertices. If the sum of the degrees for each pair of vertices in G is n - 1 or larger, then there exists a hamiltonian path in G.*

Proof. (1) *G* is connected:

Suppose *G* has two or more disconnected components. Let v_1 be a vertex in one component that has n_1 vertices and v_2 be a vertex in another component that has n_2 vertices.

Since the degree of v_1 is at most $n_1 - 1$ and the degree of v_2 is at most $n_2 - 1$, the sum of their degrees is at most $n_1 + n_2 - 2 < n - 1$, contradicts to the assumption.

(2) Construct a hamiltonian path:

- ✓ Let there be a **length *p-1 (p < n)* path**, ($v_1, v_2, v_3, \ldots, v_p$). Both v_1 *and* v_p are adjacent only to the vertices that are in the path.
- ✓ *There is a cycle containing exactly the vertices* $v_1, v_2, v_3, \ldots, v_p$.
  - ✧ Assume v_1 is adjacent to $V_{i_1}, V_{i_2}, \ldots, V_{i_k}$, where $1 < i_j < p$.
  - ✧ If v_p is adjacent to one of $V_{i_1-1}, V_{i_2-1}, \ldots, V_{i_k-1}$, then we have the cycle.
  - ✧ If v_p is not adjacent to any one of $V_{i_1-1}, V_{i_2-1}, \ldots, V_{i_k-1}$, then v_p is adjacent to at most *p-k-1* vertices. Contradicts to the assumption.
- ✓ Pick a vertex v_x that is not in the cycle. Because *G* is connected, there is a vertex v_k that is not in the cycle with an edge between v_x and v_k for some v_k in $\{v_1, v_2, v_3, \ldots, v_p\}$.
- ✓ We now **have the path ($v_x, v_k, v_{k+1}, \ldots, v_{j-1}, v_p, v_{p-1}, \ldots, v_j, v_1, v_2, v_3, \ldots, v_{k-1}$), which contains *p* edges.**
- ✓ Repeat the foregoing construction until we have a path with *n - 1* edges.

- **Theorem :** *There is always a hamiltonian path in a directed complete graph.*

  Proof. Let there be a length *p-1 (p < n)* path, $(v_1, v_2, v_3, \ldots, v_p)$. *Let* v_x be a vertex that is not included in this path, and there is no edge from v_x *to* v_1. However, $(v_1, v_x) \in G$.

  Suppose that (v_x, v_2) is also an edge in the path. Replace the edge (v_1, v_2) in the original path with the two edges (v_1, v_x) *and* (v_x, v_2) so that the vertex v_x will be included in the argument path.

  If there is no edge from v_x to v_2, then there must be an edge (v_2, v_x) in the path and we can repeat the argument.

  If we find that it is not possible to include vertex v_k in any augment path by replacing an edge (v_k, v_{k+1}) in the original path with two edges (v_k, v_x) and $(v_x, v_{k+1})$with $1 \leq k \leq p-1$, then we conclude that there must be an edge (v_p, v_x) in the graph.

  We can repeat the argument until all vertices in the graph are included in the argumented path.

- There is no general method of solution to the problem of proving the non-existence of a hamiltonian path or circuit in a graph.

Planar Graphs

- *planar* graph : A graph is said to be planar if it can be drawn on a plane is such a way that no edges cross one another, except, of course, at common vertices.
- *Region* : A region of a planar graph is defined to be an area of the plane that is bounded be edges and is not further divided into subareas. A region is said to be *finite* if this area is finite, and is said to be *infinite* if its area is infinite. Clearly, a planar graph has exactly one infinite region.
- **Theorem :** *For a connected planar graph,* $\boldsymbol{v - e + r = 2}$ *(Euler's formula)*

  where ***v, e,*** and ***r*** are the number of vertices, edges, and regions of the graph, respectively.

- Application of Euler's formula : *In any connected planar graph that has no loops and has two or more edges,* $\boldsymbol{e \leq 3v - 6.}$

- **Theorem** (**Kuratowski**): *A graph is planar if and only if it does not contain any subgraph that is isometric to o either* K_5 *or* $K_{3,3}$.

- **Tree**: A part of a graph that is connected and contains no cycles.
- **Theorem**: A connected graph possesses a tree iff there is exactly one path in between every pair of vertices.
- **Theorem**: A tree with n vertices has exactly n – 1 vertices.
- **Spanning Tree**: A tree containing all the vertices with exactly n – 1 edges.
- There are two algorithms namely Kruskal's and Prim' algorithms to find the MST.

Unit III

GROUP THEORY

OBJECTIVES:

After going through this unit, you will be able to know:

- Binary Operation
- Definition of Group, semi group, Monoid
- Permutation groups
- Cosets and Lagrange's theorem
- Homomorphism, Isomorphism and Automorphism of Groups
- Rings, integral domains and field.

INTRODUCTION:

In this chapter, we will study, binary operation as a function, and two more algebraic structures, semigroups and groups. They are called an algebraic structure because the operations on the set define a structure on the elements of that set. We also define the notion of a hornomorphism and product and quotients of groups and semigroup.

BINARY OPERATION

A binary operation on a set A is an everywhere defined function $f : A \times A \to A$, generally the operation is denoted by * on A, then $a * b \in A \ \forall a, b \in A.$

Properties of binary operation : Let $*$ be a binary operation on a set A, Then $*$ satisfies the following properties, namely

- Closure property
- Associative property
- Identity Property
- Inverse property
- Commutative property etc.

SEMIGROUP

A non-empty set S together with a binary operation $*$ is called as a semigroup if –

i) binary operation $*$ is closed

ii) binary operation $*$ is associative

we denote the semigroup by (S, $*$)

Commutative Semigroup :- A semigroup (S, $*$) is said to be commutative if $*$ is commutative i.e. $a * b = b * a \forall a \in S$

Examples : 1) (z, +) is a commutative semigroup

2) The set P(S), where S is a set, together with operation of union is a commutative semigroup.

3) (Z, –) is not a semigroup
The operation subtraction is not associative

IDENTITY ELEMENT :

An element e of a semigroup (S, $*$) is called an identity element if $e * a = a * e = a \; a \in S$

Monoid A non-empty set M together with a binary operation *defined on it, is called as a monoid if –

i) binary operation $*$ is closed

ii) binary operation $*$ is associative and

iii) (M, $*$) has an identity.

i.e. A semi group that has an identity is a monoid.

A a non-empty set G together with a binary operation $*$ defined on it is called a group if

(i) binary operation $*$ is close,

(ii) binary operation $*$ is associative,

(iii) (G, $*$) has an identity,

(iv) every element in G has inverse in G,

We denote the group by (G, $*$)

Commutative (Abelian Group : A group (G, $*$) is said to be commutative if $*$ is commutative. i.e. $a * b = b * a \;\; \forall a, b \in G$.

Cyclic Group : If every element of a group can be expressed as the power of an element of the group, then that group is called as cyclic group.

The element is called as generator of the group.

If G is a group and a is its generator then we write $G =< a >$

For example consider

$G = \{1, -1, i, -i\}$. G is a group under the binary operation of multiplication. Note that $G =< i >$. Because $a = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$

SUBSEMI GROUP :

Let (S, $*$) be a semigroup and let T be a subset of S. If T is closed under operation $*$, then (T, $*$) is called a subsemigroup of (S, $*$).

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

Subgroup : Let (G, $*$) be a group. A subset H of G is called as subgroup of G if (H, $*$) itself is a group.

Necessary and Sufficient Condition for subgroup : Let (G; $*$) be a group. A subset H of G is a subgroup of G if and only if $\forall a, b \in H \; a * b^{-1} \in H$

PERMUTATION GROUP

Definition : A permutation on n symbols is a bijective function of the set $A = \{1, 2, ...n\}$ onto itself. The set of all permutations on n symbols is denoted by S_n. If α is a permutation on n symbols, then α is completely determined by its values $\alpha(1), \alpha(2).....\alpha(n)$. We use following notation to denote $\alpha \begin{pmatrix} 1 & 2 & 3 & ..... & n \\ \alpha(1) & \alpha(1) & \alpha(3) & ..... & \alpha(n) \end{pmatrix}$.

For example $\alpha \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$ denotes the permutation on the 5 symbols (1,2,3,4,5). α maps 1 to 5, 2 to 3, 3 to 1, 4 to 2 and 5 to 4.

Product of permutation : - Let A = {1,2,3,4}

Let $\alpha \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ and $\beta \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

Then $\alpha O \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

Cycle - an element $\alpha \in S_n$ is called a cycle of lingth r if $\exists$ r symbols

$i_1, i_2 \ldots i_n \alpha(i_1) = i_2, \alpha(i_2) = i_3 \ldots \alpha(i_n) = i_1.$

Example : Consider following permutation

i) $\alpha\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$. It can be expressed as a product of cycles -

$$\alpha\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 6 & 5 \end{pmatrix} = (1\ 2\ 3\ 4)(5\ 6)$$

Transposition :

A cycle of length two is called transposition.

For example following permutation can be expressed as a product of transpositions.

$$\alpha(1837)(25)(46)$$
$$\therefore \alpha(18)(13)(17)(25)(46)$$

Even (odd) Permutation -

Let A {1, 2, ….n). A permutation $\alpha \in S_n$ is even or odd according to whether it can be expressed as the product of an even number of transpositions or the product of an odd number of transpositions respectively.

For example we can consider following permutation :

$$\alpha = (1\ 4\ 5)(2\ 3)$$
$$\alpha = (1\ 4)(1\ 5)(2\ 3)$$

= odd no. of transpositions so α is odd permutation

Example 1 : Show that $*$ defined as $x * y = x$ is a binary operation on the set of positive integers. Show that $*$ is not commutative but is associative.

Solution : Consider two positive integers x and y. By definition $x * y = x$ which is a positive integer. Hence $\cdot$ is a binary operation.

For commutativity : $x * y = x$ and $y * x = x$. Hence $x * y \neq y * x$ in general $\therefore$ $*$ is not commutative.

But $x * (y * z) = x * y = x$ and $(x * y) * z = x * z = x$. Hence $x * (y * z) = (x * y) * z$. $\therefore$ $*$ is associative

Example 2 : Let I be the set of integers and Z_m be the set of equivalence classes generated by the equivalence relation "congruent modulo m" for any positive integer m.

a) Write the sets Z_3 and Z_6

b) Show that the algebraic systems $(Z_m, +_m)$ and $(Z_m, \times_m)$ are monoids.

c) Find the inverses of elements in Z_3 and Z_4 with respect to $+_3$ and $\times_4$ respectively.

Solution : a) Z_3 for $(Z_3, +_3) = \{[0], [1], [2]\}$
Z_6 for $(Z_6, +_6) = \{[0], [1], [2], [3], [4], [5]\}$
Z_3 for $(Z_3, \times_3) = \{[0], [1], [2]\}$
Z_6 for $(Z_6, \times_6) = \{[0], [1], [2], [3], [4], [5]\}$

Example 3 : Determine whether the following set together with the binary operation is a semigroup, a monoid or neither. If it is a monoid, specify the identity. If it is a semigroup or a monoid determine whether it is commutative.

i) A = set of all positive integers.
$a * b = \max\{a, b\}$ i.e. bigger of a and b

ii) Set S = {1, 2, 3, 6, 12} where $a * b = G.C.D.(a, b)$

iii) Set S ={1,2,3,6,9,18) where $a * b = L.C.M.(a, b)$

iv) Z, the set of integers, where $a * b = a + b - ab$

v) The set of even integers E, where $a * b = \frac{ab}{2}$

vi) Set of real numbers with $a * b = a + b + 2$

vii) The set of all m×n matrices under the operation of addition.

Solution :

i) A = set of all positive integers. $a * b = \max\{a, b\}$ i.e. bigger of a and b.

Closure Property: Since Max {a, b} is either a or b $\therefore\ a * b \in A$. Hence closure property is verified.

Associative Property :

Since $a * (b * c) = \max\{\{a, b\}, c\} = \max\{a, b, c\}$

= Max{a,{b, c} } = (a.b).c

$\therefore\ *$ is associative.

$\therefore$ (A, $*$) is a semigroup.

Existence of identity : $1 \in A$ is the identity because

1.a = Max{ 1,a}= a $\quad \forall\ a \in A$

$\therefore$ (A, $*$) is a monoid.

Commutative property : Since Max{a, b) = max{b, a) we have $a * b = b * a$ Hence $*$ is commutative.

Therefore A is commutative monoid.

ii) Set S = { 1,2,3,6,12} where $a * b = G.C.D.(a, b)$

*	1	2	3	6	12
1	1	1	1	1	1
2	1	2	1	2	2
3	1	1	3	3	3
6	1	2	3	6	6
12	1	2	3	6	12

Closure Property : Since all the elements of the table $\in$ S, closure property is satisfied.

Associative Property : Since

$a * (b * c) = a * (b * c) = a * GCD\{b, c\} = GCD\ \{a, b, c\}$

And $(a * b) * c = GCD\{a, b\} * c = GCD\{a, b, c\}$

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

$\therefore\ *$ is associative.

$\therefore$ (S, $*$) is a semigroup.

Existence of identity: From the table we observe that 12 $\in$ S is the identity

$\therefore$ (S, $*$) is a monoid.

Commutative property : Since GCD{a,b}= GCD{b,a) we have $a * b = b * a$. Hence $*$ is commutative.

Therefore A is commutative monoid

(iii) Set S ={ 1,2,3,6,9, 18} where $a * b$ =L.C.M. (a,b)

*	1	2	3	6	9	18
1	1	2	3	6	9	18
2	2	2	6	6	18	18
3	3	6	3	6	9	18
6	6	6	6	6	18	18
9	9	18	9	18	9	18
18	18	18	18	18	18	18

Closure Property : Since all the elements of the table $\in$ S, closure property is satisfied.

Associative Property : Since $a * (b * c) = a * LCM\{b, c\} = LCM\{a, b, c\}$

And $(a * b) * c = LCM\{a, b\} * c = LCM\{a, b, c\}$

$\therefore\quad a * (b * c) = (a * b) * c$

$\therefore\quad *$ is associative.

$\therefore\quad$ (S, $*$) is a semigroup.

Existence of identity : From the table we observe that $1 \in S$ is the identity.

$\therefore$ $(S, *)$ is a monoid.

Commutative property : Since LCM{a, b} = LCM{b, a} we have $a * b = b * a$. Hence $*$ is commutative.

Therefore A is commutative monoid.

(iv) Z, the set of integers where - a * b = a + b - ab

Closure Property : - $a, b \in z$ then $a + b - ab \in z \ \forall a, b$ so * is closure.

Associate Property : Consider $a, b \in z$

$$(a * b) * c = (a + b - ab) * c$$
$$= a + b - ab + c - (a + b - ab)c$$
$$= a + b - ab + c - ac - bc + abc \quad \textbf{(1)}$$
$$= a + b + c - ab - ac - bc + abc$$

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

(2) From 1 & 2

$$(a * b) * c = a * (b * c) \quad \forall a, b, c \in z$$

$\therefore$ * is associative

$\therefore$ (z, &) is a semigroup.

Existence of Identity : Let e be the identity element a * e = q

a + e - q.e = a

a + e - a.e = a

e (1-a) = 0

e = 0 or a = 1

But $a \neq 1$

E = 0

$\therefore$ $O \in Z$ is the identity element.

$\therefore$ (Z, *) is monoid.

Commutative property : $\forall a, b \in z$

a * b = a + b - ab

= b + a - ba

= b * a

$\therefore$ * is commutative

$\therefore$ (Z, *) is commutative monoid.

$O \in Z$ is the identity

v) E = set of even integers. $a * b = \frac{ab}{2}$

Closure Property : Since

$\frac{ab}{2}$ is even for a and b even. $\therefore\ a * b \in E$. Hence

closure property is verified.

Property : Since $a * (b * c) = q * \left(\frac{bc}{2}\right) = \frac{abc}{4} = \frac{ab}{2} * c = (a * b) * c$

$\therefore$ $*$ is associative. $\therefore (E, *)$ is a semigroup.

Existence of identity : $2 \in$ E is the identity because $2 * a = \frac{2a}{2} =$ a $\forall$ a $\in$ E

$\therefore$ (E, $*$) is a monoid.

Commutative property : Since $\frac{ab}{2} = \frac{ba}{2}$, we have $a * b = b * a$ Hence $*$ is commutative.

$\therefore$ (E,*) is commutative monoid.

(vi) -2 $\in$ A is identity

(vii) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in$ M is the identity

Example 4 : State and prove right or left cancellation property for a group.

Solution : Let (G, $*$) be a group.

(i) To prove the right cancellation law i.e. $a * b = c * b \Rightarrow a = c$

Let a, b, c $\in$ G. Since G is a group, every element has inverse in G.

$\therefore$ $b^{-1} \in$ G

Consider $a * b = c * b$

Multiply both sides by b^{-1} from the right.

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

$\therefore$ $a * (b * b^{-1}) = c * (b * b^{-1})$ Associative property

$\therefore$ $e * a = e * c$ $b * b^{-1} = e \in G$

$\therefore$ a = c $e \in G$ is the identity

(ii) To prove the left cancellation law i.e. $a * b = c * b \Rightarrow a = c$

Let a, b, $c \in G$: Since G is a group, every element has inverse in G.

$\therefore a^{-1} \in G$

Consider $a * b = a * c$

Multiply both sides by a^{-1} from the left

$\therefore$ $a^{-1} * (a * b) = a^{-1} * (a * c)$

$\therefore$ $(a^{-1} * a) * b = (a^{-1} * a) * c$ Associative property

$\therefore$ $e * b = e * c$ $a^{-1} * a = e \in G$

$\therefore$ b = c $e \in G$ is the identity

Example 5 : Prove the following results for a group G.

(i) The identity element is unique.

(ii) Each a in G has unique inverse a^{-1}

(iii) $(ab)^{-1} = b^{-1}a^{-1}$

Solution : (i) Let G be a group. Let e_1 and e_2 be two identity elements of G.

If e_1 is identity element then $e_1e_2 = e_2e_1 = e2$ ……(1)

If e_2 is identity element then $e_1e_2 = e_2e_1 = e_1$ ……(2)

$\therefore$ From (1) and (2) we get $e_1 = e_2$ i.e. identity element is unique.

(ii) Let G be a group. Let b and c be two inverses of $a \in G$.

lf b is an inverse of a then ab = ba = e……(1)

If c is an inverse of a then ac = ca = e……(2)

Where $e \in G$ be the identity element.

$\therefore$ From (1) and (2) we get ab = ac and ba = ca.

$\therefore$ b=c by cancellation law : i.e. inverse of $a \in G$ is unique.

$\therefore$ inverse of $a \in G$ is unique.

(iii) Let G be a group. Let a, $b \in G$.

Consider $(ab)(b^{-1}a^{-1})$

= $a(bb^{-1})a^{-1}$ Associative property

= $(ae)a^{-1}$ $bb^{-1} = e$, $e \in G$ is identity

= $(ae)a^{-1}$ Associative property

= $aa^{-1}e = a$

= $eaa^{-1} = e$

Similarly we can prove $(b^{-1}a^{-1})(ab) = e$.

Hence $(ab)^{-1} = b^{-1}a^{-1}$

Example 6 : Let G be a group with identity e. Show that if $a^2 = e$ for all a in G, then every element is its own inverse

Solution : Let G be a group.

Given $a^2 = e$ for all $a \in G$. Multiply by a^{-1}

we get $a^{-1}a^2 = a^{-1}e$

$\therefore \quad a = a^{-1}$

i.e. every element is its own inverse

Example 7 : Show that if every element in a group is its own inverse, then the group must be abelian.

OR

Let G be a group with identity e. Show that if $a^2 = e$ for all a in G, then G is abelian.

Solution : Let G be a group.

$\therefore$ For $a \in G$, $a^{-1} \in G$

$\therefore$ Consider $(ab)^{-1}$

$\therefore$ $(ab)^{-1} = b^{-1}a^{-1}$ reversal law of inverse.

$\therefore$ $ab = ba$ every element is its own inverse

$\therefore$ G is abelian.

Example 8 : Let Z_n denote the set of integers (0, 1, .. , n-1). Let $\otimes$ be binary operation on Z_n such that $a \otimes b$ = the remainder of ab divided by n.

i) Construct the table for the operation $\otimes$ for n=4.

ii) Show that $(Z_n, \otimes)$ is a semi-group for any n.

iii) Is $(Z_n, \otimes)$ a group for any n? Justify your answer.

Solution : (i) Table for the operation $\otimes$ for n = 4.

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(ii) To show that $(Z_n, \otimes)$ is a semi-group for any n.

Closure property : Since all the element in the table $\in \{0, 1, \ldots, n-1\}$, closure property is satisfied.

Assiciative property : Since multiplication modulo n is associative, associative property is satisfied.

$\therefore$ $(Z_n, \otimes)$ is a semi-group

(iii) $(Z_n, \otimes)$ is not a group for any n.

Example 9 : Consider the group G = {1,2,3,4,5,6} under multiplication modulo 7.

(i) Find the multiplication table of G

(ii) Find 2^{-1}, 3^{-1}, 6^{-1}.

(iii) Find the order of the subgroups generated by 2 and 3.

(iv) Is G cyclic?

Solution : (i) Multiplication table of G

Binary operation $*$ is multiplication modulo 7.

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

From the table we observe that $1 \in G$ is identity.

(ii) To find 2^{-1}, 3^{-1}, 6^{-1}.

From the table we get $2^{-1} = 4$, $3^{-1} = 5$, $6^{-1} = 6$

iii) To find the order of the subgroups generated by 2.

Consider $2^\circ = 1$ = Identity, $2^1 = 2$; $2^2 = 4$, $2^3 = 1$ = Identity

$< 2 > = \{2^1, 2^2, 2^3\}$

$\therefore$ Order of the subgroup generated by 2 =3

To find the order of the subgroups generated by 3.

Consider $3^\circ = 1$ = identity, $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$ = Identity

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

$\therefore$ Order of the subgroup generated by 3 = 6

(iv) G is cyclic because G = < 3 >.

Example 10 : Let G be an abelian group with identity e and let H = $\{x/x^2 = e\}$. Show that H is a subgroup of G.

Solution : Let $x, y \in H \therefore x^2 = e$ and $y^2 = e \quad \therefore x^{-1} = x$ and $y^{-1} = y$
Since G is abelian we have $xy = yx \therefore xy^{-1} = yx$

Now $(xy^{-1})^2 = (xy^{-1})(xy^{-1}) = (xy^{-1})(y^{-1}x)$
$= (xy^{-1})(yx) = x(y^{-1}y)x$
$= x(e)x$
$= x^2 = e$
$\Rightarrow xy^{-1} \in H$
$\therefore$ H is a subgroup.

Example 16 : Let G be a group and let H = $\{x/x \in G$ and $xy = yx$ for all $y \in G\}$. Prove that H is a subgroup of G.

Solution : Let $x, z \in H \therefore xy = yx$ for every $y \in G \quad \therefore x = yxy^{-1}$.
Similarly $zy = yz$ for every $y \in G \quad \therefore z = yzy^{-1}$.
Now consider $xz^{-1} = (yxy^{-1})(yzy^{-1})^{-1}$
$= yxy^{-1}yz^{-1}y^{-1} = yxz^{-1}y^{-1}$
$\Rightarrow (x.z^{-1})y = y(xz^{-1}) \in H.$
$\Rightarrow xz^{-1} \in H$
$\therefore$ H is a subgroup

Example 17 : Find all subgroups of $(Z,\oplus)$ where $\oplus$ is the operation addition modulo 5. Justify your answer.

Solution:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Example 18 : Let G be a group of integers under the operation of addition. Which of the following subsets of G are subgroups of G?

(a) the set of all even integers,

(b) the set of all odd integers. Justify your answer.

Solution:

a) Let H= set of all even integers.

We know, additive inverse of an even number is even and sum of two even integers is also even. Thus for $a,b \in H$ we have $ab^{-1} \in H$.
Hence H is a subgroup of G.

b) Let K = set of all odd integers.

We know, additive inverse of an odd number is odd and sum of two odd integers is even.

Thus for $a,b \in K$ we have $ab^{-1} \notin K$.

Hence K is not a subgroup of G.

Example 19 : Let $(G, *)$ be a group and H be a non-empty subset of G. Show that $(H, *)$ is a subgroup if for any a and b in H, ab^{-1} is also in H.

Solution :

(i) Let $a, a \in H \quad \therefore a\,a^{-1} \in H$. i.e. $e \in H$

$\therefore$ The identity element $\in$ H.

(ii) Let $e, a \in H \quad \therefore ea^{-1} \in H$. i.e. $a^{-1} \in H$

$\therefore$ Every element has inverse $\in$ H.

(iii) Let $a, b \in H$. $\therefore b^{-1} \in H$. $\therefore a(b^{-1})^{-1} \in H$. i.e. $ab \in H$.

$\therefore$ Closure property is satisfied.

(iv) Every element in H is also in G. And G is a group. So associative property is satisfied by the elements of H. Hence associative property is satisfied by the elements of H.

Hence H is a group. But H is a subset of G. $\therefore$ H is a subgroup of G.

Example 20 : Let H and K be subgroups of a group G. Prove that $H \cap K$ is a subgroup of G.

Solution : If H is a subgroups of a group G, then for any $a, b \in H$, $ab^{-1} \in H$.

Similarly, if K is a subgroups of a group G, then for any $a, b \in K$, $ab^{-1} \in K$.

Now if $a, b \in H \cap K$, $a, b \in H$ and $a, b \in K$. $\therefore ab^{-1} \in H$ and $ab^{-1} \in K$. Hence $ab^{-1} \in H \cap K$.

$\therefore$ $H \cap K$ is a subgroup of G.

HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM OF SEMIGROUPS

Homomorphism : Let (S, $*$) and (T, $*'$) be two semigroups. An everywhere defined function

f : S$\to$T is called a homomorphism from (S, $*$) to (T, $*'$) if

$f(a*b) = f(a) *' f(b) \quad \forall a, b \in S$

Isomorphism : Let (S, $*$) and (T, $*'$) be two semigoups. A function

f : S $\to$ T is called a isomorphism from (S, $*$) to (T, $*'$) if

(i) it is one-to-one correspondence from S to T (ii) $f(a*b) = f(a) *' f(b) \quad \forall a, b \in S$

(S, $*$) and (T, $*'$) are isomorphic' is denoted by $S \cong T$.

Automorphism : An isomorphism from a semigroup to itself is called an automorphism of the semigoup. An isonorptism $f : s \to s$ I is called automorphism.

HOMOMORPHISM, LSOMORPHISM AND AUTOMORNHISM OF MONOIDS :

Homomorphism : Let (M, $*$) and (M', $*'$) be two monoids. An everywhere defined function f : M $\to$ M' is called a homomorphism from (M, $*$) to (M', $*'$) if $f(a * b) = f(a) *' f(b) \quad \forall a, b \in M$

Isomorphism : Let (M, $*$) and (M', $*'$) be two monoids. A function

f : M $\to$ M' is called a isomorphism from (M, $*$) to (M', $*'$) if

(i) it is one-to-one correspondence from M to M' (ii) f is onto.

(iii) $f(a*b = f(a) *' f(b) \quad \forall a, b \in M$

'(M $*$) and (M', $*'$) are isomorphic is denoted by M $\cong$ M'.

Automorphism : An isomorphism from a monoid to itself is called an automorphism of the monoid. An isomorphism $f : M \to M$ is called automorphism of monoid.

HOMOMORPHISM, ISOMORPHISM AND AUTOMORPHISM O F GROUPS :

Homomorphism : Let (G, $*$) and (G', $*$') be two groups. An everywhere defined function f : G $\rightarrow$ G' is called a homomorphism from (G, $*$) to (G', $*$') if

f (a $*$ b) = f (a) $*$' f (b) $\forall$ a, b $\in$ G

Isomorphism : Let (G, $*$) and (G', $*$') be two groups. A function f : G$\rightarrow$G' is called a isomorphism from (G, $*$) to (G', $*$') if

(i) it is one-to-one correspondence from G to G' (ii) f is onto.

(iii) f(a $*$ b) = f (a) $*$' f (b) $\forall$ a, b$\in$G

'(G, $*$) and (G', $*$') are isomorphic' is denoted by G $\cong$ G'.

Automorahism: An isomorphism from a group to itself is called an automorphism of the group. An isomorphism $f : G \rightarrow G$ is called Automorphism

Theorem : Let (S, $*$) and (T, $*$') be monoids with identity e and e', respectively. Let f : S $\rightarrow$ T be an isomorphism. Then f(e) = e'.

Proof : Let b be any element of T. Since f is on to, there is an element a in S such that f(a) = b

Then $a = a * e$

$$b = f(a) = f(a * e) = f(a) * f(e) = b *' f(e)$$ (f is isomorphism)

Similarly, since $a = e * a$,

$$b = f(a) = f(e * a) f(e * a) = f(e) *' (a)$$

Thus for any ,b$\in$T,

$$b = b *' f(e) = f(e) *' b$$

which means that f(e) is an identity for T.

Thus since the identity is unique, it follows that f(e)=e'

Theorem : Let f be a homomorphism from a semigroup (S, $*$) to a semigroup (T, $*$'). If S' is a subsemigroup of (S, $*$), then F(S') = {t $\in$ T | t = f (s) for some s $\in$ S},The image of S' under f, is subsemigroup of (T, $*$').

Proof : If t_1, and t_2 are any elements of F(S'), then there exist s_1 and s_2 in S' with t_1= f(s_1) and t_2 = f(s_2). Therefore,

$$t_1 * t_2 = f(s_1) * f(s_2) = f(s_1 * s_2) = f(s_2 * s_1) = f(s_2) * f(s_1) = t_2 * t_1$$

Hence (T, $*$') is also commutative.

Example 1 : Let G be a group. Show that the function f : G $\rightarrow$ G defined by f(a) = a^2 is a homomorphism iff G is abelian.

Solution :

Step-1 : Assume G is abelian. Prove that f : G $\rightarrow$ G defined by f(a) = a^2 is a homomorphism.

Let a,b$\in$G. $\therefore$ f(a) = a^2 , f(b) = b^2 and f(ab) = $(ab)^2$ by definition of f.

$\therefore$ f(ab)=$(ab)^2$

= (ab)(ab).

= a(ba)b associativity

= a(ab)b G is abelian

= (aa)(bb) associativity

= a^2b^2

= f(a)f(b) definition of f

$\therefore$ f is a homomorphism.

Step 2 :

$\forall\, y = a^2 \in G \;\; \exists\, a \in G \; s\, t$

$f(a) = y = a^2$

$\therefore$ f is onto.

Step-3 : Assume, f : G $\rightarrow$ G defined by f(a) = a^2 s a homomorphism. Prove that G is abelian.

Let a,b$\in$G. $\therefore$ f(a) = a^2 , f(b) = b^2 and f(ab) = $(ab)^2$ by definition of f.

$\therefore$ f(ab) = f(a)f(b) f is homomorphism

$\therefore$ $(ab)^2 = a^2 b^2$ definition of f

$\therefore$ (ab)(ab) = (aa)(bb)

$\therefore$ a(ba)b = a(ab)b associativity

$\therefore$ ba = ab left and right cancellation taws

$\therefore$ G is abelian.

Example 3 : Let G be a group and let a be a fixed element of G. Show that the function $f_a : G \rightarrow G$ defined by $f_a(x) = axa^{-1}$ for x$\in$G is an isomorphism.

Solution :

Step-1: Show that f is 1-1.

$f_a(x) = axa^{-1}$

Consider $f_a(x) = f_a(y)$ for x, y $\in$G

$\therefore$ $axa^{-1} = aya^{-1}$ definition of f

$\therefore$ x = y left and right cancellation laws

$\therefore$ f is 1- 1

Step 2 :

$\forall\, y = axa^{-1} \in G \;\exists\; x \in G$ s.t.

$f_a(x) = a\,xa^{-1}$

$\therefore$ f is onto.

Step-3 : Show that f is homomorphism.

For x, y$\in$G

$f(x) = a * x * a^{-1}$, $f(y) = a * y * a^{-1}$ and $f(x * y) = a * (x * y) * a^{-1}$

Consider $f(x * y) = a * (x * y) * a^{-1}$ for x, y$\in$G

$\therefore$ $f(x * y) = a * (x * e * y) * a^{-1}$ e$\in$G is identity

$= a * (x * a^{-1} * a * y) * a^{-1}$ $a^{-1} * a = e$

$= (a * x * a^{-1}) * (a * y * a^{-1})$ associativity

$\therefore \quad * f(x * y) = f(x) * f(y)$

$\therefore$ f is homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Example 2 : Let G be a group. Show that the function f : G $\rightarrow$ G defined by f(a) = a^{-1} is an isomorphism if and only if G is abelian.

Solution :

Step-1: Assume G is abelian. Prove that f : G $\rightarrow$ G defined by f(a) = a^{-1} is an isomorphism.

i) Let f(a)=f(b)

$\therefore a^{-1} = b^{-1} \quad \therefore a = b \quad \therefore$ f is 1- l.

ii) $\forall a \in G \Rightarrow a^{-1} \in G$

$\therefore x^1 \in G$

$\Rightarrow f(x) = x^{-1}$

$\therefore$ f is onto.

iii) Let a,b$\in$G. $\therefore$f(a) = a^{-1}, f(b) = b^{-1} and f(ab) = $(ab)^{-1}$ by definition of f.

$\therefore$ f(ab) = $(ab)^{-1}$

= $b^{-1}a^{-1}$ reversal law of inverse

= $a^{-1}b^{-1}$ G is abelian

= f(a)f(b) definition of f.

$\therefore$ f is a homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Step – 2 : Assume f : G $\rightarrow$ G defined by f(a) = a^{-1} is an isomorphism. Prove that G is abelian.

Let a, b$\in$G $\therefore$f(a) = a^{-1}, f(b) = b^{-1} and f(ab) = $(ab)^{-1}$ by definition of f

$\therefore$ f(ab) = f(a)f(b) f is homomorphism

$\therefore$ $(ab)^{-1} = a^{-1}b^{-1}$ definition of f

$\therefore$ $b^{-1}a^{-1} = a^{-1}\ b^{-1}$ reversal law of inverse

G is abelian.

Example 3 : Define (Z, +) $\rightarrow$ (5Z, +) as f(x) = 5x, where 5Z=(5n : n $\in$ Z). Verify that f is an isomorphism.

Solution:

Step -1 Show that f is 1-l.

Consider f(x) = f(y) for x, y$\in$G

$\therefore$ 5x = 5y definition of f

$\therefore$ x = y $\therefore$ f is 1-1

Step 2 :

$\forall 5x \in G, \exists x \in G$

$s.t.\ f(x) = 5x$

$\therefore$ f is onto.

Step-3: Show that f is homomorphism.

For $x * y \in G$

f(x) = 5x, d(y) = 5y and f(x + y) – 5(x+y)

Consider f(x+y) = 5(x+y) for x, y $\in$G

= 5x + 5y

$\therefore$ f(x+y) = f(x) + f(y)

$\therefore$ f is homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Example 4 : Let G be a group of real numbers under addition, and let G' be the group of positive numbers under multiplication. Let f : G $\rightarrow$ G' be defined by $f(x) = e^x$. Show that f is an isomorphism from G to G'

OR

Show that the group G = (R,+) is isomorphic to G' = (R^+, x) where R is the set of real numbers and R^+ is a set of positive real numbers.

Solution :

Step 1: Show that f is 1-1.

Consider f(x) = f(y) for x,y$\in$G

$\therefore$ $e^x = e^y$ definition of f

$\therefore$ x = y $\therefore$ f is 1-1.

Step 2 : If $x \in G^1$, then $\log x \in G$ and $f(.\log x) = e^{\log x} = x$ so f is onto.

Step-3 : Show that f is homomnrphism.

For x, y∈G

$f(x) = e^x$, $f(y) = e^y$ and $f(x+y) = e^{(x+y)}$

Consider $f(x + y) = e^{(x + y)}$ for x, y ∈G

$= e^x \times e^y$

$\therefore$ $f(x + y) = f(x) \times f(y)$ f is homomorphism.

Since f is 1-1 and homomorphasm, it is isomorphism.

Example 5 : Let G = {e, a, a^2, a^3, a^4, a^5} be a group under the operation of $a^i a^j = a^r$, where $i + j \equiv r(\text{mod } 6)$. Prove that G and Z_6 are isomorphic

Solution :

Step - I : Show that f is l-I.

Let $x = a^i$, and $y = a^j$.

Consider f(x) = f(y) for x, y ∈ G

$\therefore$ $f(a^i) = f(a^j)$ definition of f

$\therefore$ $a^i = a^j$

$\therefore$ x = y f is 1-1.

Step-2 : Show that f is homomorphism.

Let x = a' and y = a' x, y ∈ G

$f(a^i) = i$, $f(a^j)$ j and $f(x + y) = f(a^i a^j)$

Consider $f(x+y) = f(a^i a^j) = f(a')$ where $i + j = r(\text{mod } 6)$

= R

= i + j

= $f(a^i) + f(a^j)$

$\therefore$ $f(x \times y) = f(x) + f(y)$ $\therefore$ f is homomorphism.

Since f is 1-1 and homomorphism, it is isomorphism.

Example 6 : Let T be set of even integers. Show that the semigroups (Z, +) and (T, +) are isomorphic.

Solution : We show that f is one to one onto .

Define $f : (Z, +) \rightarrow (T, +)$ as $f(x) = 2x$

1) Show that f is l-1

Consider f(x) = f(y)

$\therefore 2x = 2y$

$\therefore x = y$ $\therefore$ f is 1-l.

2) Show that f is onto

$y = 2x$ $\therefore x = y/2$ when y is even.

$\therefore$ for every y∈T there exists x∈Z.

$\therefore$ f is onto.

$\therefore$ f is isomorphic.

3) F is homorphism

$F(x + y) = 2(x + y)$

$= 2x + 2y$

$= f(x) + f(y)$

$\therefore$ f is honomorphism.

Example 7 : For the set A = {a,b,c} give all the permutations of A. Show that the set of all permutations of A is a group under the composition operation.

Solution : A={a,b,c}. S_3= Set of all permutations of A.

$$f_0 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \quad f_1 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \quad f_2 = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$

$$f_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \quad f_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad f_5 = \begin{pmatrix} a & b & c \\ c & a & b` \end{pmatrix}$$

Let us prepare the composition table.

0	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_4	f_5	f_2	f_3
f_2	f_2	f_3	f_0	f_4	f_3	f_1
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_3	f_1	f_2	f_5	f_0
f_5	f_5	f_2	f_3	f_1	f_0	f_4

i) **Closure Property:** Since all the elements in the composition table $\in S_3$, closure property is satisfied.

ii) **Associative Property:** Since composition of permutations is associative, associative property is satisfied.

iii) **Existance of Identity:** From the table we find that fo is the identity

iv) **Existance of Inverse:** From the composition table it is clear that

$f_0^{-1} = f_0,\ f_1^{-1} = f_1,\ f_2^{-1} = f_2,\ f_3^{-1} = f_3,\ f_4^{-1} = f_5,\ f_5^{-1} = f_4$

$\therefore$ Every element has inverse in S_3. Hence S_3 is a group.

COSET AND NORMAL SUBEROUP:

Left Coset : Let (H, $*$) be a subgroup of (G, $*$). For any a $\in$ G, the set of aH defined by $aH = \{a * h / h \in H\}$ is called the **left coset** of H in G

determined by the element $a \in G$. The element a is called the representative element of the left coset aH.

Right Coset : Let (H, $*$) be a subgroup of (G, $*$). For any $a \in G$, the set of Ha defined by

$$Ha = [h * a \mid h \in H]$$

is called the **right coset** of H in G determined by the element $a \in G$. The element a is called the representative element of the right coset Ha.

Theorem : Let (H, $*$) be a subgroup of (G, $*$). The set of left cosets of H in G form a partition of G. Every element of G belongs to one and only one left coset of H in G.

Lagrange' Theorem: The order of a subgroup of a finite group divides the order of the group.

Corollary : If (G, $*$) is a finite group of order n, then for any $a \in G$, we must have $a^n = e$, where e is the identity of the group.

Normal Subgroup : A subgroup (H, $*$) of (G, $*$) is called a normal subgroup if for any $a \in G$, aH = Ha.

Example 8 : Determine all the proper subgroups of symmetric group (S_3, o). Which of these subgroups are normal?

Solution : S = {1, 2, 3}. S_3 = Set of all permutations of S.

$S_3 = \{f_0, f_1, f_2, f_3, f_4, f_5\}$ where

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Let us prepare the composition table.

0	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_4	f_5	f_2	f_3
f_2	f_2	f_3	f_0	f_4	f_3	f_1
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_3	f_1	f_2	f_5	f_0
f_5	f_5	f_2	f_3	f_1	f_0	f_4

From the table it is clear that $\{f_0, f_1\}$, $\{f_0, f_2,\}$, $\{f_0, f_3\}$ and $\{f_0, f_4, f_5\}$ are subgroups of $(S_3, 0)$: The left cosets of $\{f_0, f_1\}$ are $\{f_0, f_1\}$, $\{f_2, f_5\}$, $\{f_3, f_4\}$. While the right cosets of $\{f_0, f_1\}$ are $\{f_0, f_1\}$, $\{f_2, f_4\}$, $\{f_3, f_5\}$. Hence $\{f_0, f_1\}$ is not a normal subgroup.

Similarly we can show that $\{f_0, f_2\}$ and $\{f_0, f_1\}$ are not normal subgroups.
On the other hand, the left and right cosets of $\{f_0, f_4, f_5\}$ are $\{f_0, f_4, f_5\}$ and $\{f_1, f_2, f_3\}$.
Hence $\{f_0, f_4, f_5\}$ is a nomal subgroup.

Example 9: Let S = {1, 2, 3}. Let G = S_3 be the group of all permutations of elements of S, under the operation of composition of permutations.

Let H be the subgroup formed by the two permutations $\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}$ and $\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$. Find the left coset of H in G. Is H a normal subgroup? Explain your notion of composition clearly.

Solution : Let

$$f_0 = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \qquad f_1 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \qquad f_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

$$f_3 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \qquad f_4 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \qquad f_5 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$$

$\therefore$ H={f_0, f_2}

Left Cosets of H in G :

$f_0H = \{f_0f_0, f_0f_2\} = \{f_0, f_2\}$ $\quad f_1H = \{f_1f_0, f_1f_2\} = \{f_1, f_4\}$

$f_2H = \{f_2f_0, f_2f_2\} = \{f_2, f_0\}$ $\quad f_3H = \{f_3f_0, f_3f_2\} = \{f_3, f_5\}$

$f_4H = \{f_4f_0, f_4f_2\} = \{f_4, f_1\}$ $\quad f_5H = \{f_5f_0, f_5f_2\} = \{f_5, f_3\}$

Right Cosets of H in G

$Hf_0 = \{f_0f_0, f_2f_0\} = \{f_0, f_2\}$ $\quad Hf_1 = \{f_0f_1, f_2f_1\} = \{f_1, f_3\}$

Since $f_1 H \neq Hf_1$, H is not a normal subgroup of G.

Example 10 : Define a normal sub-group. Let S_3 = Group of all permutations of 3 elements (say 1, 2, 3). For the following subgroups of S, find all the left cosets . Subgroup of A = {1,(1,2)}

Where I = identity permutation, (1, 2) is a transposition. Is A a normal subgroup. State a normal subgroup of the above group if it exists.

Solution : $H = \{f_0, f_3\}$

The left cosets of H in G are as follow.

$f_0H = \{f_0, f_3\}$ $\quad f_1H = \{f_1, f_5\}$ $\quad f_2H = \{f_2, f_4\}$

$f_3H = \{f_3, f_0\}$ $\quad f_4H = \{f_4, f_2\}$ $\quad f_5H = \{f_5, f_1\}$

Consider a right coset $\quad Hf_1 = \{f_1, f_4\}$

Since $f_1H \neq Hf_1$, H is not a normal subgroup of G.

RING: An algebraic structu**re (**R, +, o**)** is said to be a Ring if it satisfies :

- (R, +) is a commutative Group.
- (R, o) is a semigroup and
- **(**R, +, o**)** satisfies the distributive property.

FIELD: An algebraic structu**re (**F, +, o**)** is said to be a Field if it satisfies :

- (F, +) is a commutative Group.
- (F, o) is a commutative group and
- **(**F, +, o**)** satisfies the distributive property.

Zero Divisor: A commutative ring is said to have a zero divisor if the product of two non-zero element is zero. For example, the product of two non- zero matrices may zero.

INTEGRAL DOMAIN: A commutative without a zero divisor is called an integral domain.

THEOREM: Every finite integral domain is a field.

THEOREM: Every field is an integral domain.

Unit IV

LATTICE THEORY, BOOLEAN ALGEBRA AND CODING THEORY

OBJECTIVES:

After going through this unit, you will be able to :

- Define basic terminology associated with lattice theory.
- Boolean lattices and Boolean algebras
- Coding theory

LATTICES

BASIC TERMINOLOGY

Definition:

A poset is a **lattice** if every pair of elements has a lub (join) and a glb (meet).

Least upper bound (lub)

Let $(A, \leq)$ be a poset and B be a subset of A.

1. An element $a \in A$ is an upper bound for B iff for every element $a' \in B$, $a' \leq a$.

2. An element $a \in A$ is a least upper bound (lub) for B iff a is an upper bound for B and for every upper bound a' for B, $a \leq a'$.

Greatest lower bound (glb)

Let $(A, \leq)$ be a poset and B be a subset of A.

1. An element $a \in A$ is a lower bound for B iff for every element $a' \in B$, $a \leq a'$.

2. An element $a \in A$ is a greatest lower bound (glb) for B iff a is a lower bound for B and for every lower bound a' for B, $a' \leq a$.

Theorem:

Let $(L, \leq)$ be a lattice, For any $a, b, c \in L$,

(i) a*a = a (i') a + a = a (idempotent)

(ii) a*b=b*a (ii') a + b = b + a (Commutative)

(iii) (a*b)*c= a*(b*c) (iii') (a + b) + c = a + (b + c) (Associative)

(iv) a*(a+ b) = a (iv') a + (a*b) = a (Absorption)

Theorem:

Let (L, ≤) be a lattice for any a, b ∈ L, the following

property holds.

A ≤ b⇔a*b = a ⇔ a + b = b

Theorem:

Let (L, ≤) be a lattice, for any a, b, c ∈ L, the following

properties hold.

B ≤ c => a*b ≤ a*c, a + b≤ a + c

Theorem:

Let (L, ≤) be a lattice, For any a, b, c∈ L, the following

properties hold.

a ≤ b ^ a ≤ c => a ≤ b + c

a ≤ b ^ a ≤ c => a ≤ b*c

b ≤ a ^ c ≤ a => b*c ≤ a

b ≤ a ^ c ≤a => b + c ≤ a

Theorem:

Let (L, ≤) be a lattice, For any a, b, c∈ L, the

following inequalities hold.

a +(b*c) ≤ (a + b)*(a + c)

(a*b)+ (a*c) ≤ a*(b + c)

BOOLEAN ALGEBRA: A complemented distributive lattice is called a Boolean Algebra.

Theorem:

Let (A, *, +) be an Boolean algebra which satisfies the

1. Idempotent law, (a*a=a, a+a=a)

2. Commutative law, (a*b=b*a, a+b=b+a)

3. Associative law, ((a*b)*c= a*(b*c), (a + b) + c = a + (b + c)

4. Absorption law (a*(a + b) = a, a + (a*b) = a)

Then there exists a lattice (A, ≤), such that * is a glb, + is a lub,

and is ≤ defined as follows:

$x \leq y$ iff $x*y = x$

$x \leq y$ iff $x + y = y$

Definitions

Algebraic system :A lattice is an **algebraic system** (L, *, +) with two binary operations * and + on L which are both (1) commutative and (2) associative and (3) satisfy the absorption law.

Sublattice : Let (L, *, +) be a lattice and let S be a subset of L. The algebra (S, *, +) is a sublattice of (L, *, +) iff S is closed under both operations * and +.

Lattice homomorphism: Let (L, *, +) and (S, ^,V) be two lattice. A mapping g:L→S is called a lattice homomorphism from the lattice (L, *, +) to (S, ^ , V) if for any a, b ∈ L,

$g(a*b) = g(a) \wedge g(b)$ and $g(a + b) = g(a) \vee g(b)$.

Order-preserving : Let (P, ≤) and (Q, ≤) be two partially ordered sets, A mapping

f: P → Q is said to be order-preserving relative to the ordering ≤ in P and ≤′ in Q iff for any a, b ∈ P such that a ≤ b, f(a) ≤′ f(b) in Q.

Complete Lattice*:* A lattice is called complete if each of its nonempty subsets has a least upper bound and a greatest lower bound.

Greatest and Least elements

Let (A, ≤)> be a poset and B be a subset of A.

1. An element a ∈ B is a greatest element of B iff for every element a' ∈ B, a' ≤ a.

2. An element a ∈ B is a least element of B iff for every element a' ∈ B, a ≤ a '.

Least upper bound (lub)

Let (A, ≤) be a poset and B be a subset of A.

1. An element a ∈ A is an upper bound for B iff for every element a' ∈ B, a' ≤ a.

2. An element a ∈ A is a least upper bound (lub) for B iff a is an upper bound for B and for every upper bound a' for B, a ≤ a'.

Greatest lower bound (glb)

Let (A, $\leq$) be a poset and B be a subset of A.

1. An element a $\in$ A is a lower bound for B iff for every element a' $\in$ B, a $\leq$ a'.
2. An element a $\in$ A is a greatest lower bound (glb) for B iff a is a lower bound for B and for every lower bound a' for B, a' $\leq$ a.

Maximal and Minimal Elements: Let *(A, R)* be a poset. Then *a* in *A* is a minimal element if there does not exist an element *b* in *A* such that *bRa*. Similarly for a maximal element.

Upper and Lower Bounds

Let *S* be a subset of *A* in the poset *(A, R).* If there exists an element *a* in *A* such that *sRa* for all *s* in *S*, then *a* is called an *upper bound*. Similarly for lower bounds.

Bounds of the lattice :The least and the greatest elements of a lattice, if they exist, are called the bounds of the lattice, and are denoted by 0 and 1 respectively.

Bounded lattice: In a bounded lattice (L, *, +, 0, 1), an element b $\in$ L is called a complement of an element a $\in$ L, if a*b=0,

a + b =1.

Complemented lattice :A lattice (L, *, +, 0, 1) is said to be a complemented lattice if every element of L has at least one complement.

Distributive lattice :A lattice (L, *, +) is called a distributive lattice if for any a, b, c $\in$ L, a*(b + c) = (a*b) + (a*c) + (b*c) = (a + b)*(a + c)

EXAMPLE:

Construct the Hasse diagram of *(P({a, b, c}), $\subseteq$).*

The elements of *P({a, b, c})* are

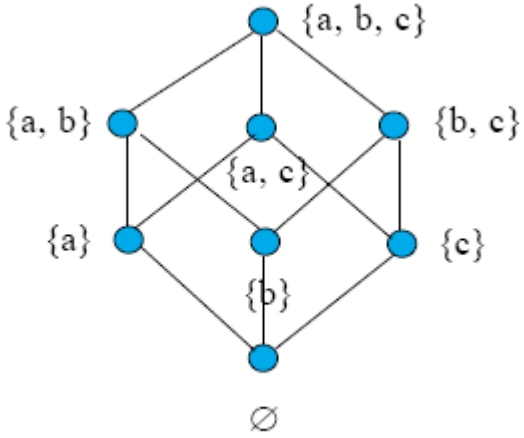
ϕ

{a}, {b}, {c}

{a, b}, {a, c}, {b, c}

{a, b, c}

The digraph is



In the above Hasse diagram, ϕ is a minimal element and *{a, b, c}* is a maximal element.

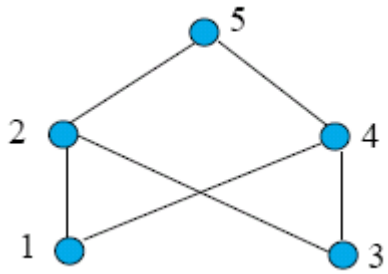
In the poset above *{a, b, c}* is the greatest element. $\not\phi$ is the least element.

In the poset above, *{a, b, c}*, is an upper bound for all other subsets. ϕ is a lower bound for all other subsets.

{a, b, c}, {a, b} {a, c} and {a} are upper bounds and {a} is related to all of them, {a} must be the lub. It is also the glb.

EXAMPLE:

In the poset *(P(S), ⊆),* lub(*A*, *B*) = $A \cup B$. What is the glb(*A*, *B*)?



Solution:

Consider the elements 1 and 3.

- Upper bounds of 1 are 1, 2, 4 and 5.
- Upper bounds of 3 are 3, 2, 4 and 5.
- 2, 4 and 5 are upper bounds for the pair 1 and 3.
- There is no lub since

- 2 is not related to 4

- 4 is not related to 2

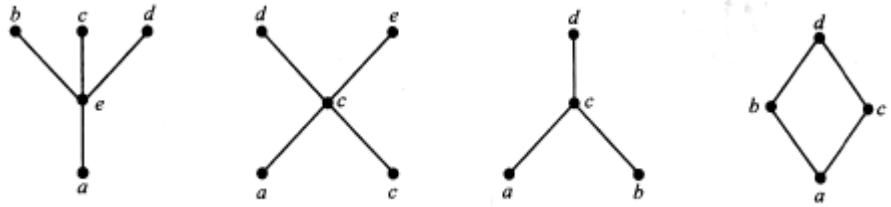
- 2 and 4 are both related to 5.

• There is no glb either.

The poset is n o t a lattice.

EXAMPLE:

Determine whether the posets represented by each of the following Hasse diagrams have a greatest element an a least element.



Solution

• The least element of the poset with Hasse diagram (a) is a. This poset has no greatest element.

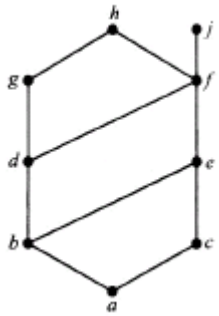
• The poset with Hasse diagram (b) has neither a least nor a greatest element.

• The poset with Hasse diagram (c) has no least element. Its greatest element is d.

• The poset with Hasse diagram (d) has least element a and greatest element d.

EXAMPLE:

Find the lower and upper bounds of the subsets {a, b, c}, {j, h}, and {a, c, d, f } and find the greatest lower bound and the least upper bound of {b, d, g}, if they exist.



Solution

The upper bounds of {a, b, c} are e, f, j, h, and its only lower bound is a.

There are no upper bounds of {j, h}, and its lower bounds are a, b, c, d, e, f .

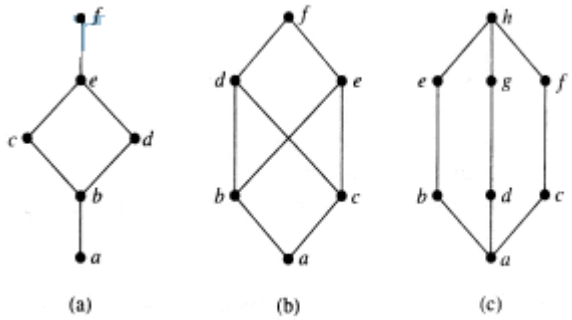
The upper bounds of {a, c, d, f } are f, h, j, and its lower bound is a.

The upper bounds of {b, d, g} are g and h. Since g _ h, g is the least upper bound.

The lower bounds of {b, d, g} are a and b. Since a _ b, b is the greatest lower bound.

EXAMPLE:

Determine whether the posets represented by each of the following Hasse diagrams are lattices.



Solution

The posets represented by the Hasse diagrams in (a) and (c) are both lattices because in each poset every pair of elements has both a least upper bound and a greatest lower bound.

On the other hand, the poset with the Hasse diagram shown in (b) is

not a lattice, since the elements b and c have no least upper bound. To see this note that each of the elements d, e and f is an upper bound, but none of these three elements precedes the other two with respect to the ordering of this poset.

EXAMPLE:

Determine whether $(P(S), \subseteq)$ is a lattice where S is a set.

Solution

Let A and B be two subsets of S . The least upper bound and the greatest lower bound of A and B are A U B and A $\cap$B, respectively.

Hence $(P(S), \subseteq)$ is a lattice.

CODES AND GROUP CODES

INTRODUCTION :

In today's modern world of communication, data items are constantly being transmitted from point to point.

Different devices are used for communication. The basic unit of information is message. Messages can be represented by sequence of dots and das

Let

B = {0,1}be the set of bits. Every character or symbol can be represented by sequence of elements of B. Message are coded in O's and 1's and then they are transmitted. These techniques make use of group theory. We will see a brief introduction of group code in this chapter. Also we will see the detection of error in transmitted message.

$B = \{0,1\}$ is a group under the binary operation $\oplus$ whose

The set

table is as follows :

$\oplus$	0	1
0	0	1
1	1	0

We have seen that B is a group.

It follows from theorem - "If G_1 and G_2 are groups then $G = G_1 \times G_2$ is a group with binary operation defined by $(a_1, b_1)(a_2, b_2) = (a_1, a_2, b_1, b_2)$. So $B^m = B \times B \times ... \times B$ (m factors) is a group under the operation $\oplus$ defined by $(x_1, x_2 ....x_m) \oplus (y_1, y_2 .... y_m) = (x_1 + y_1, x_2 + y_2, ... x_m + y_m)$ observe that B^m has 2^m elements. i.e. order of group B^m is 2^m.

Important Terminology :

Let us choose an integer $n > m$ and one-to-one function $e : B^m \to B^n$.

1) Encoding Function :

The function e is called an (m, n) encoding function. It means that every word in B^m as a word in B^n.

2) Code word :

If $b \in B^m$ then e(b) is called the code word

3) Weight :

For $x \in B^n$ the number of 1's in x is called the weight of x and is denoted by $|x|$.

e.g. i) $x = 10011 \in B^5 \therefore w(x) = 3$

ii) $x = 001 \in B^3 \therefore w(x) = 1$

4) $x \oplus y \rightarrow$ Let $x, y \in B^n$, then $x \oplus y$ is a sequence of length n that

has 1's in those positions x & y differ and has O's in those positions x & y are the same. i.e. The operation + is defined as 0 + 0 = 0 0 + 1 = 1 1 + 1
= 0 1 + 0 = 1

e.g. if $x, y \in B^5$

$x = 00101, y = 10110$

$\therefore x \oplus y = 10011$

$\therefore w(x \oplus y) = 3$

5) Hamming Distance :

Let $x, y \in B^m$. The Hamming Distance $\delta(x, y)$ between x and y is the weight of $x \oplus y$. It is denoted by $|x \oplus y|$. e.g. Hamming distance between x & y can be calculated as follows : if x = 110110, y = 000101 $x \oplus y$ = 110011 so $|x \oplus y|$ = 4.

6) Minimum distance :

Let $x, y \in B^n$. then minimum distance = min $\{d(x, y) / x, y \in B^n\}$. Let $x_1, x_2 - - x_n$ are the code words, let any $x_i, i = 1 - - - n$ is a transmitted word and y be the corresponding received word. Then $y = x_k$ if $d(x_k, y)$ is the minimum distane for k = 1, 2, --- n. This criteria is known as minimum distance criteria.

7) Detection of errors :

Let $e : B^m \to B^n \ (m < n)$ is an encoding function then if minimum distane of e is (k + 1) then it can detect k or fewer errors.

8) Correction of errors :

Let $e : B^m \to B^n \ (m < n)$ is an encoding function then if minimum distance of e is (2k + 1) then it can correct k or fewer errors.

Weight of a code word : It is the number of 1's present in the given code word.

Hamming distance between two code words : Let $x = x_1 x_2 \ldots x_m$ and $y = y_1 y_2 \ldots y_m$ be two code words. The Hamming distance between them, $\delta(x, y)$, is the number of occurrences such that $x_i \neq y_i$ for $i = 1, m$.

Example 1 : Define Hamming distance. Find the Hamming distance between the codes.
(a) $x = 010000, \ y = 000101$ (b) $x = 001100, \ y = 010110$

Solution : Hamming distance :
(a) $\delta(x, y) = |x \oplus y| = |010000 \oplus 000101| = |010101| = 3$
(b) $\delta(x, y) = |x \oplus y| = |001100 \oplus 010110| = |011010| = 3$

Example 2 : Let d be the $(4,3)$ decoding function defined by $d: B^4 \to B^3$. If $y = y_1\, y_2 \ldots y_{m+1}$, $d(y) = y_1\, y_2 \ldots y_m$.

Determine $d(y)$ for the word y is B^4.

(a) $y = 0110$ (b) $y = 1011$

Solution : (a) $d(y) = 011$ (b) $d(y) = 101$

Example 3 : Let $d: B^6 \to B^2$ be a decoding function defined by for $y = y_1\, y_2 \ldots y_6$. Then $d(y) = z_1\, z_2$.

where

$zi = 1$ if $\{y_1, y_{i+2}, y_{i+4}\}$ has at least two 1's.

0 if $\{y_1, y_{i+2}, y_{i+4}\}$ has less than two 1's.

Determine $d(y)$ for the word y in B^6.

(a) $y = 111011$ (b) $y = 010100$

Solution : (a) $d(y) = 11$ (b) $d(y) = 01$

Example 4 : The following encoding function $f: B^m \to B^{m+1}$ 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

$b_{m+1} = 0$ if $|b|$ is even.

$= 1$ if $|b|$ is odd.

Find $e(b)$ if (a) $b = 01010$ (b) $b = 01110$

Solution : (a) $e(b) = 010100$ (b) $e(b) = 011101$

Example 5 : Let $e : B^2 \to B^6$ is an (2,6) encoding function defined as

e(00) = 000000, e(01) = 011101
e(10) = 001110, e(11) = 111111

a) Find minimum distance.
b) How many errors can e detect?
c) How many errors can e correts?

Solution : Let $x_0, x_1, x_2, x_3 \in B^6$ where $x_0 = 000000, x_1 = 011101,$
$x_2 = 001110, x_3 = 111111$

$w(x_0 \oplus x_1) = w(011101) = 4$
$w(x_0 \oplus x_2) = w(001110) = 3$
$w(x_0 \oplus x_3) = w(111111) = 6$
$w(x_1 \oplus x_2) = w(010011) = 3$
$w(x_1 \oplus x_3) = w(100010) = 2$
$w(x_2 \oplus x_3) = w(110001) = 3$

Minimum distance = e = 2

d) Minimum distance = 2

An encoding function e can detect k or fewer errors if the minimum distance is k + 1. $\therefore k + 1 = 2 \therefore k = 1$

$\therefore$ The function can detect 1 or fewer (i.e. 0) error.

e) e can correct k or fewer error if minimum distance is 2k + 1.

$\therefore 2k + 1 = 2$

$\therefore k = \frac{1}{2}$

$\therefore$ e can correct $\frac{1}{2}$ or less than $\frac{1}{2}$ i.e. 0 errors.

GROUP CODE :

An (m, n) encoding function $e : B^m \to B^n$ is called a group code if range of e is a subgroup of B^n. i.e. (Ran (e), $\oplus$) is a group.

Since Ran (e) $\subseteq B^n$ and if (Ran (e), $\oplus$) is a group then Ran(e) is a subgroup of B^n. If an encoding function $e : B^m \to B^n$ (n < n) is a group code, then the minimum distance of e is the minimum weight of a nonzero codeword.

.

DECODING AND ERROR CORRECTION :

Consider an (m, n) encoding function $e : B^m \to B^n$, we require an (n,m) decoding function associate with e as $d : B^n \to B^m$.

The method to determine a decoding function d is called maximum likelihood technique.

Since $|B^m| = 2^m$.

Let $x_k \in B^m$ be a codeword, k = 1, 2, ---^{m} and the received word is y then. Min $1 \le k \le 2^m \{d(x_k, y)\} = d(x_i, y)$ for same i then x_i is a codeword which is closest to y. If minimum distance is not unique then select on priority

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. We now discuss a method, called the maximum likelihood techniques, for determining a decoding function d for a given e. Since B^m has 2^m elements, there are 2^m code words in B^n. We first list the code words in a fixed order.

$$x^{(1)}, x^{(2)}, ..., x^{(2^m)}$$

If the received word is x_1, we compute $\delta(x^{(i)}, x_1)$ for $1 \le i \le 2^m$ and choose the first code word, say it is $x^{(s)}$, such that

$$\min_{1 \le i \le 2^m} \{\delta(x^{(i)}, x_1)\} = \delta(x^{(s)}, x_1)$$

That is, $x^{(s)}$ is a code word that is closest to x_1, 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 $e\left(B^n\right)$ are listed. If the code words are listed in a different order, we may obtain, a different likelihood decoding function d associated with e.

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 $2k+1$.

Example : Let $m = 2, n = 5$ and $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Determine the group code $e_H : B^2 \to B^5$.

Solution : We have $B^2 = \{00, 01, 10, 11\}$. Then $e(00) = 00x_1x_2x_3$ where

$x_1 = 0.1 + 0.0 = 0$

$x_2 = 0.1 + 0.1 = 0$

$x_3 = 0.0 + 0.1 = 0$

$\therefore\ e(00) = 00000$

Now,

$e(01) = 01x_1x_2x_3$

where

$x_1 = 0.1 + 1.0 = 0$

$x_2 = 0.1 + 1.1 = 1$

$x_3 = 0.0 + 1.1 = 1$

$\therefore\ e(01) = 01011$

Next

$e(10) = 10x_1x_2x_3$

$x_1 = 1.1 + 0.0 = 1$

$x_2 = 1.1 + 1.0 = 1$

$x_3 = 1.0 + 0.1 = 0$

$\therefore\ e(10) = 10110$

$e(11) = 11101$

Example : Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. determine the $(3,6)$ group code $e_H : B^3 \to B^6$.

Solution : First find $e(000)$, $e(001)$, $e(010)$, $e(011)$, $e(100)$, $e(101)$, $e(110)$, $e(111)$.

$e(000) = 000000$ $\qquad$ $e(100) = 100100$

$e(001) = 001111$ $\qquad$ $e(101) = 101011$

$e(010) = 010011$ $\qquad$ $e(110) = 110111$

$e(100) = 011100$ $\qquad$ $e(111) = 111000$

Example : Consider the group code defined by $e : B^2 \to B^5$ such that $e(00) = 00000$ $\quad e(01) = 01110$ $\quad e(10) = 10101$ $\quad e(11) = 11011$.
Decode the following words relative to maximum likelihood decoding function.
(a) 11110 $\qquad$ (b) 10011 $\qquad$ (c) 10100

Solution : (a) $x_t = 1110$

Compute $\delta\left(x^{(1)}, x_t\right) = |\, 00000 \oplus 11110 \,| = |\, 11110 \,| = 4$

$\delta\left(x^{(2)}, x_t\right) = |\, 01110 \oplus 11110 \,| = |\, 10000 \,| = 1$

$\delta\left(x^{(3)}, x_t\right) = |\, 10101 \oplus 11110 \,| = |\, 01011 \,| = 3$

$\delta\left(x^{(4)}, x_t\right) = |\, 11011 \oplus 11110 \,| = |\, 00101 \,| = 2$

$\min\left\{\delta\left(x^{(i)}, x_t\right)\right\} = 1 = \delta\left(x^{(2)}, x_t\right)$

$\therefore$ $e(01) = 01110$ is the code word closest to $x_t = 11110$.

$\therefore$ The maximum likelihood decoding function d associated with e is defined by $d(x_t) = 01$.

(b) $x_t = 10011$

Compute $\delta\left(x^{(1)}, x_t\right) = \left| 00000 \oplus 10011 \right| = \left| 11101 \right| = 4$

$\delta\left(x^{(2)}, x_t\right) = \left| 01110 \oplus 10011 \right| = \left| 00110 \right| = 2$

$\delta\left(x^{(3)}, x_t\right) = \left| 10101 \oplus 11110 \right| = \left| 01011 \right| = 3$

$\delta\left(x^{(4)}, x_t\right) = \left| 11011 \oplus 10011 \right| = \left| 01000 \right| = 1$

$\min\left\{\delta\left(x^{(i)}, x_t\right)\right\} = 1 = \delta\left(x^{(4)}, x_t\right)$

$\therefore$ $e(11) = 11011$ is the code word closest to $x_t = 10011$.

$\therefore$ The maximum likelihood decoding function d associated with e is defined by $d(x_t) = 11$.

(c) $x_t = 10100$

Compute $\delta\left(x^{(1)}, x_t\right) = \left| 00000 \oplus 10100 \right| = \left| 10100 \right| = 2$

$\delta\left(x^{(2)}, x_t\right) = \left| 01110 \oplus 10100 \right| = \left| 11010 \right| = 3$

$\delta\left(x^{(3)}, x_t\right) = \left| 10101 \oplus 10100 \right| = \left| 00001 \right| = 1$

$\delta\left(x^{(4)}, x_t\right) = \left| 11011 \oplus 10100 \right| = \left| 01111 \right| = 4$

$\min\left\{\delta\left(x^{(i)}, x_t\right)\right\} = 1 = \delta\left(x^{(3)}, x_t\right)$

$\therefore$ $e(10) = 10101$ is the code word closest to $x_t = 10100$.

$\therefore$ The maximum likelihood decoding function d associated with e is defined by $d(x_t) = 10$.

Example : Let $H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. decode the following words relative to a maximum likelihood decoding function associated with e_H : (i) 10100, (ii) 01101, (iii) 11011.

Solution : The code words are $e(00) = 00000$, $e(01) = 00101$, $e(10) = 10011$, $e(11) = 11110$. Then $N = \{00000, 00101, 10011, 11110\}$. We implement the decoding procedure as follows. Determine all left cosets of N in B5,

as rows of a table. For each row 1, locate the coset leader ε_i, and rewrite the row in the order.

$\varepsilon_1, \varepsilon_i \oplus$

Example : Consider the $(2, 4)$ encoding function e as follows. How many errors will e detect?

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

Solution :

$\oplus$	0000	0110	1011	1100
0000	---	0110	1011	1100
0110		---	1101	1010
1011			---	0111
1100				---

Minimum distance between distinct pairs of $e = 2 \quad \therefore k + 1 = 2 \ \therefore k = 1.$
$\therefore$ the encoding function e can detect 1 or fewer errors.

Example : Define group code. Show that $(2, 5)$ encoding function $e : B^2 \to B^5$ defined by $e(00) = 0000,\ e(10) = 10101,\ e(11) = 11011$ is a group code.

Solution : Group Code

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

Since closure property is satisfied, it is a group code.

Example : Define group code. show that $(2, 5)$ encoding function $e : B^2 \to B^5$ defined by $e(00) = 00000,\ e(01) = 01110,\ e(10) = 10101,$

$e(11) = 11011$ is a group code. Consider this group code and decode the following words relative to maximum likelihood decoding function.
(a) 11110 (b) 10011.
Solution : Group Code

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

Since closure property is satisfied, it is a group code.

Now, let $x^{(1)} = 00000,\ x^{(2)} = 01110,\ x^{(3)} = 10101,\ x^{(4)} = 11011$.

(a) $x_t = 11110$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |\,00000 \oplus 11110\,| = |\,11110\,| = 4$$
$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |\,01110 \oplus 1110\,| = |\,10000\,| = 1$$
$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |\,10101 \oplus 1110\,| = |\,01011\,| = 3$$
$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |\,11011 \oplus 1110\,| = |\,00101\,| = 2$$

$\therefore$ Maximum likelihood decoding function $d(x_t) = 01$.

(b) $x_t = 10011$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |\,00000 \oplus 10011\,| = |\,10011\,| = 3$$
$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |\,01110 \oplus 10011\,| = |\,11101\,| = 4$$
$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |\,10101 \oplus 10011\,| = |\,00110\,| = 2$$
$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |\,11011 \oplus 10011\,| = |\,01000\,| = 1$$

$\therefore$ Maximum likelihood decoding function $d(x_t) = 11$.

Example : Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. Determine the $(3,6)$ group code $e_H : B^3 \to B^6$.

Solution : $B^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$e_H(000) = 000000$ $e_H(001) = 001111$ $e_H(010) = 010011$

$e_H(011) = 011100$ $e_H(100) = 100100$ $e_H(101) = 101011$

$e_H(110) = 110111$ $e_H(111) = 111000$

$\therefore$ Required group code = $\{000000, 001111, 010011, 011100, 100100, 101011, 110111, 111000\}$

Example : Show that $(2,5)$ encoding function $e : B_2 \to B_5$ defined by $e(00) = 00000$, $e(01) = 01110$, $e(10) = 10101$, $e(11) = 11011$ is a group code.

Test whether the following $(2,5)$ encoding function is a group code.

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

Solution :

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

Since closure property is satisfied, it is a group code.

Example : Show that the $(3,7)$ encoding function $e : B^3 \to B^7$ defined by

$e(000) = 0000000$ $e(001) = 0010110$ $e(010) = 0101000$

$e(011) = 0111110$ $e(100) = 1000101$ $e(101) = 1010011$
$e(110) = 1101101$ $e(111) = 1111011$ is a group code.

Solution :

$\oplus$	0000000	0010110	0101000	0111110	1000101	1010011	1101101	1111011
0000000	0000000	0010110	0101000	0111110	1000101	1010011	1101101	1111011
0010110	0010110	0000000	0111110	0101000	1010011	1000101	1111011	1101101
0101000	0101000	0111110	0000000	0010110	1101101	1111011	1000101	1010011
0111110	0111110	0101000	0010110	0000000	1111011	1101101	1010011	1000101
1000101	1000101	1010011	1101101	1111011	0000000	0010110	0101000	0111110
1010011	1010011	1000101	1111011	1101101	0010110	0000000	0111110	0101100
1101101	1101101	1111011	1000101	1010011	0101000	0111110	0000000	0010110
1111011	1111011							0000000

Since closure property is satisfied, it is a group code.

Example: Consider the $(3,8)$ encoding function $e: B^3 \to B^8$ defined by
$e(000) = 0000000$ $e(100) = 10100100$ $e(001) = 10111000$
$e(101) = 10001001$ $e(010) = 00101101$ $e(110) = 00011100$
$e(011) = 10010101$ $e(111) = 00110001$.
How many errors will e detect?

Solution :

$\oplus$	00000000	10100100	10111000	10001001	00101101	00011100	10010101	00110001
0000000	00000000	10100100	10111000	10001001	00101101	00011100	10010101	00110001
10100100	10100100	00000000	00011100	00101101	10001001	10111000	00110001	10010101
10111000	00000000	00011100	00000000	001100001	10010101	10100100	00101101	10001001
10001001	10001001	00101101	00110001	00000000	10100100	10010101	00011100	10111000
00101101	00101101	10001001	10010101	10100100	00000000	00110001	10111000	00011100
00011100	00011100	10111000	10100100	10010101	00110001	00000000	10001001	00101101
10010101	10010101	00110001	00101101	00011100	10111000	10001001	00000000	10100100
00110001	00110001	10010101	10001001	10111000	00011100	00101101	10100100	0000000

Minimum distance between pairs of $e = 3$.
$\therefore k+1 = 3$ $\therefore k = 2$ $\therefore$ The encoding function e can detect 2 or fewer errors.

Example: Consider parity check matrix H given by $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Determine the group code $e_H : B_2 \to B_5$. Decode the following words relative to a maximum likelihood decoding function associated with e_H : 01110, 11101, 00001, 11000 . [Apr-04, May-07]

Solution : $B_2 = \{00, 01, 10, 11\}$

$e_H(00) = 00x_1x_2x_3$ where $x_1 = 0.1 + 0.0 = 0$

$x_2 = 0.1 + 0.1 = 0$

$x_3 = 0.0 + 0.1 = 0$ $\therefore e_H(00) = 00000$

$e_H(01) = 01x_1x_2x_3$ where $x_1 = 0.1 + 1.0 = 0$

$x_2 = 0.1 + 1.1 = 1$

$x_3 = 0.0 + 1.1 = 1$ $\therefore e_H(01) = 01011$

$e_H(10) = 10x_1x_2x_3$ where $x_1 = 1.1 + 0.0 = 1$

$x_2 = 1.1 + 0.1 = 1$

$x_3 = 1.0 + 0.1 = 0$ $\therefore e_H(01) = 10110$

$e_H(11) = 11x_1x_2x_3$ where $x_1 = 1.1 + 1.0 = 1$

$x_2 = 1.1 + 1.1 = 0$

$x_3 = 1.0 + 1.1 = 1$ $\therefore e_H(01) = 11101$

$\therefore$ Desired group code = $\{00000, 01011, 10110, 11101\}$

(1) $x_t = 01110$

$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = |00000 \oplus 01110| = |01110| = 3$

$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = |01011 \oplus 01110| = |00101| = 2$

$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = |10110 \oplus 01110| = |11000| = 2$

$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = |11101 \oplus 01110| = |10011| = 3$

$\therefore$ Maximum likelihood decoding function $d(x_t) = 01$

(2) $x_t = 11101$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = \left| 00000 \oplus 11101 \right| = \left| 11101 \right| = 4$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = \left| 01110 \oplus 11101 \right| = \left| 10110 \right| = 3$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = \left| 10101 \oplus 11101 \right| = \left| 01011 \right| = 3$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = \left| 11011 \oplus 11101 \right| = \left| 00000 \right| = 0$$

$\therefore$ Maximum likelihood decoding function $\mathrm{d}\left(\mathrm{x_t}\right) = 11$

(3) $x_t = 00001$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = \left| 00000 \oplus 00001 \right| = \left| 00001 \right| = 1$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = \left| 01011 \oplus 00001 \right| = \left| 01010 \right| = 2$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = \left| 10110 \oplus 00001 \right| = \left| 10111 \right| = 4$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = \left| 11101 \oplus 00001 \right| = \left| 11100 \right| = 3$$

$\therefore$ Maximum likelihood decoding function $\mathrm{d}\left(\mathrm{x_t}\right) = 00$

(2) $x_t = 11000$

$$\delta\left(x^{(1)}, x_t\right) = \left| x^{(1)} \oplus x_t \right| = \left| 00000 \oplus 11000 \right| = \left| 11000 \right| = 2$$

$$\delta\left(x^{(2)}, x_t\right) = \left| x^{(2)} \oplus x_t \right| = \left| 01110 \oplus 11000 \right| = \left| 10011 \right| = 3$$

$$\delta\left(x^{(3)}, x_t\right) = \left| x^{(3)} \oplus x_t \right| = \left| 10101 \oplus 11000 \right| = \left| 01101 \right| = 3$$

$$\delta\left(x^{(4)}, x_t\right) = \left| x^{(4)} \oplus x_t \right| = \left| 11011 \oplus 11000 \right| = \left| 10000 \right| = 1$$

$\therefore$ Maximum likelihood decoding function $d\left(x_t\right) = 11$

----- *** ------