RAJIV GANDHI UNIVERSITY OF KNOWLEDGE TECHNOLOGIES

DEPARTMENT OF MATHEMATICS

IIIT-SRIKAKULAM

BRANCH(CSE-SEM-2)

DISCRETE MATHEMATICS

Dr.B.BHASKARA RAO

ASSISTANT PROFESSOR(C)

DEPARTMENT OF MATHEMATICS

RGUKT-SRIKAKULAM

CSE-E-1-SEM-2

Course Code	Course Name	Course Category	L – T - P	Credits
20MA1202	Discrete Mathematics (CSE)	B.Sc	3-1-0	4

COURSE LEARNING OBJECTIVES

The objective of this course is to

- Develop mathematical maturity of students to build the ability to understand and create mathematical arguments and to teach them how to think logically and mathematically.
- Prove theorems and Mathematical arguments by using different methods. Provide the mathematical foundations for many computer science courses including data structures, algorithms, database theory, automata theory, formal languages, compiler theory, computer security and operating systems.
- Learn the basic properties of sets and how to work with discrete structures, which are abstract mathematical structures used to represent discrete objects and relationship between these objects.
- Introduce basic techniques of counting so that they develop the ability to enumerate.
- Learn the concepts of graphs and its properties, solving real world problems by using graphs.
- Learn the concepts of Euler Paths, graph coloring, trees.

COURSE CONTENT

Unit – I **(10 Contact hours)**

PROPOSITIONAL LOGIC: Propositions and Connectives, well-formed formulas, Logical Equivalence and laws of logic, Normal forms, PCNF, PDNF.

Unit - II **(10 Contact hours)**

PROOF TECHNIQUES: Tautological implications and rules of inferences, Methods of proofs (Forward proof, proof by contradiction, contra positive proofs, proof of necessity and sufficiency, Proof by Mathematical induction).

Unit - III **(12 Contact hours)**

SETS, RELATIONS AND FUNCTIONS: Sets, Relations, Equivalence Relations and compatibility relations, Transitive closure, Posets, Finite and infinite sets, countable and uncountable sets (definitions), Functions.

Unit - IV **(12 Contact hours)**

INTRODUCTION TO COUNTING: Counting Principles, Pigeon-hole Principle, Permutations and Combinations, Recurrence Relations, Linear Recurrence relations, Generating functions.

Unit - V **(9 Contact hours)**

INTRODUCTION TO GRAPH THEORY: Graphs and their basic properties, Special types of graphs and representations of graphs, Isomorphism's, connectivity.

Unit – VI **(7 Contact hours)**

GRAPH THEORY (Continuation): Euler and Hamiltonian Paths, Planar Graphs, Graph coloring, Trees

LEARNING RESOURCES

TEXT BOOK

Kenneth H. Rosen,*'Discrete Mathematics and its Applications'*, Tata McGraw-Hill, 7th Edition.

REFERENCE BOOKS

- Trembley and Manohar, '*Discrete Mathematical Structures to Computer Science'*, by Mc - Graw Hill (1997).
- Kolman, Busby and Ross, *'Discrete Mathematical Structures'* PHI (2009), Sixth Edition.
- Thomas Koshy, '*Discrete Mathematics with Applications'*, Elsevier Academic press.

WEB RESOURCES

- NPTEL Lectures by Prof. Kamala Krithivasan, Dept of CSE,IIT Madras
  URL: https://www.youtube.com/watch?v=xlUFkMKSB3Y&list=PL0862D1A947252D20
- MIT open course ware: Mathematics for Computer Science, Fall 2010. Instructor: Tom Leighton
  URL 1: **https://www.youtube.com/watch?v=L3LMbpZIKhQ&list=PLB7540DEDD482705B**
  URL 2:http://ocw.mit.edu/6-042JF10
- Discrete Mathematics for GATE. IIT lecture
  URL: https://www.youtube.com/watch?v=E6uhC0pT9J8&list=PLEJxKK7AcSEGD7ty8DB1aU0xVG_P_hs_0
- RGUKT Course Content

COURSE OUTCOMES: At the end of the course, the student will be able to

CO 1	Read, comprehend and construct mathematical argument
CO 2	Prove theorems and mathematical statements in different techniques.
CO 3	Deal with set, relation, countability and functions.
CO 4	Apply permutation, combination, pigeon-hole principle, recurrence relation and generating functions to enumerate objects.
CO 5	Understand and apply concepts of graph in many computer science courses.
CO 6	Deal with Euler paths in graphs and coloring of graphs

Assessment method for Theory courses only

Course Nature	**Theory**			
Assessment Method				
Assessment Tool	Weekly tests	Monthly tests	End Semester Test	Total
Weightage (%)	10%	30%	60%	100%

UNIT-1

Propositional Logic

MODULE-1

Propositions and Connectives

1.1

Propositions and Connectives

Logic is concerned with all kinds of reasoning, whether they be legal arguments or mathematical proofs or conclusions in a scientific theory based on a set of hypotheses. An aim of logic is to provide rules by which one can determine whether any particular argument or reasoning is valid (correct). Due to the diversity of their application, these rules, called ***rules of inference***, must be stated in general terms and must be independent of any particular language used in the arguments. The theory of inference is formulated in such a way that we should be able to decide the validity of the argument by following the rules mechanically and independently of our own feelings about the argument.

We require a language to state rules. Natural languages are not suitable for this purpose since they are not precise and are ambiguous. It is therefore necessary to develop a formal language called **object language**. A formal language is one in which the *syntax* is well defined. In order to avoid ambiguity, we use symbols which have been clearly defined in the object language. An advantage of the use of symbols is that they are easy to write and manipulate. Because of the use of symbols, the logic that we shall study is also called **symbolic logic**.

The study of object language requires the use of a natural language (and we choose English in our case). This natural language will then be called ***meta language.***

Propositions:

A ***declarative sentence*** is a sentence that declares a fact. We begin by assuming that the object language contains a set of declarative sentences which cannot be further broken down or analysed into simpler sentences. These are ***primary declarative sentences***. Only those declarative sentences will be admitted in the object languages which have one and only one of two possible values called ***truth values***. The two truth values are ***true*** and ***false*** which are denoted by the symbols T and F respectively. Occasionally T and F are respectively denoted by 1 and 0 .

Since only two possible truth values are admitted, our logic is sometimes called a ***two-valued logic***.

Declarative sentences in the object language are of two types. The first type includes those declarative sentences which are considered to be primitive in the object language. The declarative sentences of the second type are obtained from the primitive declarative sentences by using certain symbols called ***connectives (logical operators***) and certain punctuation marks, such as parentheses to join primitive declarative sentences. In any case, all the declarative sentences to which it is possible to assign one and only of the two truth values are called ***propositions*** (or ***statements***).

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

Example 1:

(i) Delhi is the capital of India
(ii) $2 + 3 = 4$
(iii) What is it?
(iv) $x + y = z$
(v) This statement is false

(i) and (ii) are declarative sentences and they are propositions. Proposition (i) is true and the proposition (ii) is false. Sentence (iii) is not a proposition since it is not a declarative sentence. Sentence (iv) is not a proposition, since it is neither true nor false. Note that the sentence (iv) can be turned into a proposition if we assign values to the variables. Sentence (v) is not a proposition since we cannot properly assign a definite truth value. If we assign the value true then (v) implies that the sentence (v) is false. On the other hand, if we assign it the value false then (v) implies that the sentence (v) is true. This example illustrates a ***semantic paradox***.

A ***proposition variable*** (or ***statement variable***) is a variable that represents a proposition. The propositional variables are denoted by lowercase letters. The conventional letters used for propositional variables are $p, q, r, s, \ldots$

The area of logic that deals with propositions is called ***propositional calculus*** or ***propositional logic***. It was first developed systematically by the Greek philosopher Aristotle more than 2300 years ago.

A proposition which does not contain any connectives is called a **atomic** (or **primary** or **simple**) ***proposition***. A proposition which contains one or more atomic propositions as well as some connectives is called a ***molecular*** (or ***compound*** or ***composite***) ***proposition***.

Negation:

Let p be a proposition. The negation of p, denoted by $\sim p$ (also denoted by $\neg\, p$ or $\bar{p}$), is the proposition " it is not the case that p". The proposition $\sim p$ is read as "not p". The truth value of $\sim p$ is the opposite of the truth value of p.

The truth table of $\sim p$ is a tabular form in which the truth values of $\sim p$ are given for arbitrary truth values of p.

Truth table for $\sim p$	
p	$\sim p$
T	F
F	T

Consider the proposition p : Delhi is a city

Then $\sim p$ is the proposition $\sim p$: It is not the case that Delhi is a city

The above proposition can also be written as $\sim p$: Delhi is not a city

Note that the two propositions "It is not the case that Delhi is a city" and "Delhi is not a city" are not identical but we have denoted both of them by $\sim p$. The reason to denote them by the same $\sim p$ is that they mean the same in English (meta language).

Note: A given proposition in object language is denoted by a symbol and it may correspond to several statements in meta language. This multiplicity happens because in a meta language one can express oneself in a variety of ways.

Note that the negation constructs a new proposition from a single existing proposition. We will now introduce connectives (***and***, ***or***, ***if…then*** … and ***if and only if)*** that are used to form new propositions from two or more existing propositions.

Conjunction:

If p and q are propositions, then the conjunction of p and q is the compound proposition "p and q" denoted by $p \wedge q$. The connective **and** is denoted by the symbol $\wedge$.

The compound proposition $p \wedge q$ is true when both p and q are true and is false otherwise.

The truth table of a compound proposition is a tabular form in which the truth values of the compound proposition are given interms of its component parts.

Truth table for $p \wedge q$		
p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Note that in logic the word "but" sometimes is used instead of "and" in a conjunction. (In meta language, there is a difference in meaning between "and" and "but"; we will not be concerned with this nuance here.)

Disjunction:

If p and q are propositions, the disjunction of p and q is the compound statement "p **or** q" denoted by $p \vee q$. The connective **or** is denoted by the symbol $\vee$.

The compound proposition $p \vee q$ is true if at least one of p or q is true and is false otherwise.

Truth table for $p \vee q$		
p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Note: In English the word "or" is commonly used in two distinct ways. It is used (i) in the *inclusive* sense, i.e., "p or q or both", and (ii) in the *exclusive* sense, i.e., "p or q but not both". For example, "He will go to Harvard University or Yale University" uses "or" in the exclusive sense. In logic $p \vee q$ always means "p and/or q".

Example 2:

Let p and q be propositions given by

p : Sam is rich $\qquad$ q : Sam is happy

Write each of the following in symbolic form:

a. Sam is poor but happy.
b. Sam is either rich or unhappy.
c. Sam is neither rich nor happy.

Solution:

a. $\sim p \wedge q$

b. $p \vee \sim q$
c. $\sim p \wedge \sim q$

Conditional propositions:

If p and q are propositions, then the compound statement "if p, then q" ("if p, q") denoted by $p \to q$, is called a ***conditional proposition*** or ***implication***.

In $p \to q$, the proposition p is called ***antecedent*** (or ***hypothesis***) and the proposition q is called ***consequent*** (or ***conclusion***). The connective ***if … then …*** is denoted by $\to$.

The proposition $p \to q$ has a truth value F when q has truth value F and p has truth value T and has truth value T otherwise.

Truth table for $p \to q$		
p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Note:

(i) According to the definition, it is not necessary that there be any kind of relation between p and q in order to form $p \to q$.
(ii) It is customary to represent any one of the following expressions by $p \to q$:

q is necessary for p
p is sufficient for q
q if p
p only if q
q whenever p
q when p
a necessary condition for p is q
q unless $\sim p$
a sufficient condition for q is p
q follows from p

(iii) In mathematics “if p then q” and “p implies q” are used interchangeably, but in this text we use the word implies in different way.

The **converse** of the implication $p \to q$ is the implication $q \to p$.

The **inverse** of the implication $p \to q$ is the implication $\sim p \to \sim q$ (read as if not p then not q).
The **contra positive** of the implication $p \to q$ is the implication $\sim q \to \sim p$.

Truth tables for converse, inverse and contrapositive of $p \longrightarrow q$

p	q	$Conditional$ $p \longrightarrow q$	$Converse$ $q \longrightarrow p$	$\sim p$	$\sim q$	$Inverse$ $\sim p \longrightarrow \sim q$	$Contrapositive$ $\sim q \longrightarrow \sim p$
T	T	T	T	F	F	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Example 3:

Write the converse, inverse and contrapositive of the implication “If today is Sunday, then I will go for a walk”.

Solution: Let p and q be propositions

p : Today is Sunday $\qquad$ q : I will go for a walk

Then the given proposition is written as $p \longrightarrow q$.

The converse of this implication is

$q \longrightarrow p$: If I will go for a walk, then Today is Sunday

The inverse of the above implication is

$\sim p \longrightarrow \sim q$: If Today is not Sunday then I will not go for a walk

The contrapositive of $p \longrightarrow q$ is

$\sim q \longrightarrow \sim p$: If I will not go for a walk, then Today is not Sunday

Biconditional Propositions:

If p and q are propositions, then the compound statement "p if and only if q", denoted by $\boldsymbol{p \leftrightarrow q}$ **(**or $\boldsymbol{p \rightleftarrows q}$), is called a **biconditional proposition**. The connective ***if and only if*** is denoted by the symbol $\leftrightarrow$ (or $\rightleftarrows$).

The proposition $p \leftrightarrow q$ can also be stated as "p is necessary and sufficient condition for q" (or "if p then q, and conversely" or "p iff q")

The proposition $p \leftrightarrow q$ has truth value T whenever both p and q have identical truth values.

Truth table for $p \leftrightarrow q$		
p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 4:

Construct the truth tables for $\boldsymbol{p \wedge \sim p}$ and $\boldsymbol{p \vee \sim p}$

Truth table for $p \wedge \sim p$		
p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

Truth table for $p \vee \sim p$		
p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

P1:

Which of the following are propositions?

a. **2 is an even integer.**
b. **Why should we study discrete structures?**
c. **There is an integer x such that $x^2 = 3$.**
d. **Please be quiet.**
e. **Dogs can fly.**
f. **There will be snow in December.**
g. **What a beautiful evening!**
h. **Get up and do your exercises.**

Solution:

a. This is a declarative sentence and its truth value is T. Therefore, it is a proposition.
b. This is not a declarative sentence. Therefore, it is not a proposition.
c. This is a declarative sentence, since there is no integer x such that $x^2 = 3$. Its truth value is F. Therefore, it is a proposition.
d. This is not a declarative sentence. Therefore, it is not a proposition.
e. This is a declarative sentence and its truth value is F.
f. This is a declarative sentence and it is either true or false but not both. Therefore, it is a proposition.
g. This is not a declarative sentence. Therefore, it is not a proposition.
h. This is not a declarative sentence. Therefore, it is not a proposition.

P2:

If p and q are the following propositions:

p : 2 is an even integer **q : -3 is a negative integer**

then write the following propositions interms of p, q and logical connectives and find their truth values:

a. **2 is an even integer and -3 is a negative integer.**
b. **2 is not an even integer and -3 is a negative integer.**
c. **2 is not an even integer and -3 is not a negative integer.**
d. **If 2 is not an even integer, then -3 is not a negative integer.**
e. **If 2 is an even integer, then -3 is not a negative integer.**
f. **2 is an even integer if and only if -3 is a negative integer.**
g. **2 is not an even integer if and only if -3 is a negative integer.**

Solution:

First, note that the truth value of p is T and the truth value of q is T.

a. $p \wedge q$, T
b. $\sim p \wedge q$, F
c. $\sim p \wedge \sim q$, F
d. $\sim p \longrightarrow \sim q$, T
e. $p \longrightarrow \sim q$, F
f. $p \leftrightarrow q$, T
g. $\sim p \leftrightarrow q$, F

P3:

Write the converse, the inverse and the contrapositive of the following conditional proposition

"The home team wins whenever it is raining"

Solution:

The given proposition can be rewritten as "If it is raining, then the home team wins". It is written in symbolic form as $p \longrightarrow q$ where

p : It is raining $\qquad$ q : The home team wins

The converse of $p \longrightarrow q$ is $q \longrightarrow p$, i.e., "If the home team wins, then it is raining".

The inverse of $p \longrightarrow q$ is $\sim p \longrightarrow \sim q$, i.e., "If it is not raining, then the home team does not win".

The contrapositive of $p \longrightarrow q$ is $\sim q \longrightarrow \sim p$, i.e., "If the home team does not win, then it is not raining".

P4:

Construct the truth tables for $\sim p \vee q$ and $\sim p \vee \sim q$.

Solution:

Truth table for $\sim p \vee q$			
p	q	$\sim p$	$\sim p \vee q$
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Truth table for $\sim p \vee \sim q$				
p	q	$\sim p$	$\sim q$	$\sim p \vee \sim q$
T	T	F	F	F
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

P5:

Construct the truth tables for $\sim p \wedge q$ and $p \wedge \sim q$.

Solution:

Truth table for $\sim p \wedge q$			
p	q	$\sim p$	$\sim p \wedge q$
T	T	F	F
T	F	F	F
F	T	T	T
F	F	T	F

Truth table for $p \wedge \sim q$			
p	q	$\sim q$	$p \wedge \sim q$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	T	F

P6:

Determine the truth values of the following propositions:

a. If Paris is in France then $2+2=4$
b. If Paris is in France then $2+2=5$
c. If Paris is in England then $2+2=4$
d. If Paris is in England then $2+2=5$

Solution:

Note that the proposition "If p, then q" is false only when p is true and q is false. Therefore, the truth values of the above are

a. T b. F c. T d. T

P7:

Determine the truth values of the following propositions:

a. Paris is in France if and only if $2 + 2 = 4$
b. Paris is in France if and only if $2 + 2 = 5$
c. Paris is in England if and only if $2 + 2 = 4$
d. Paris is in England if and only if $2 + 2 = 5$

Solution:

The propositions (a) and (d) are true since the primary (atomic) propositions are both true in (a) and both false in (d). On the other hand (b) and (d) are false since their atomic propositions have opposite truth values.

P8:

Let p, q be primitive propositions for which the implication $p \longrightarrow q$ is false. Determine truth values for

a. $p \wedge q$
b. $\sim p \vee q$
c. $q \longrightarrow p$
d. $\sim q \longrightarrow \sim p$
e. $p \leftrightarrow q$
f. $\sim p \longrightarrow \sim q$

Answers:

Note that the proposition "If p then q" is false only when p is true and q is false. Therefore, the truth values of the above are

a. F
b. F
c. T
d. F
e. F
f. T

1.1. Propositions and Connectives

Exercises:

1. Which of the following sentences are propositions? What are the truth values of those that are propositions?
   a. Kharagpur is in Andhra Pradesh
   b. Answer this question
   c. $5 + 8 = 13$
   d. $x + 2 = 9$

2. What is the negation of each of these propositions?
   a. Today is Monday
   b. There is no pollution in Jaipur
   c. $2 + 5 = 7$

3. Let p and q be propositions, where

   p : It is below freezing $\qquad$ q : It is snowing

Write the following propositions using p and q and connectives:

   a. It is below freezing and snowing
   b. It is below freezing but not snowing
   c. It is not below freezing and it is not snowing
   d. It is either snowing or below freezing (or both)
   e. If it is below freezing, it is also snowing
   f. That it is below freezing is necessary and sufficient for it to be snowing

4. Let p and q be propositions, where

   p : Swimming at the New Jersey shore is allowed

   q : Sharks have been spotted near the shore

Express each of these compound propositions as an English sentence.

   a. $\sim q$

b. $p \wedge q$
c. $\sim p \vee q$
d. $p \longrightarrow \sim q$
e. $\sim q \longrightarrow p$
f. $\sim p \longrightarrow \sim q$
g. $p \leftrightarrow \sim q$

5. Determine whether the following conditional propositions are true of false.
   a. If $1 + 1 = 2$ then $2 + 2 = 5$
   b. If $1 + 1 = 3$ then $2 + 2 = 4$
   c. If $1 + 1 = 3$ then $2 + 2 = 5$
   d. If monkey can fly then $1 + 1 = 3$

6. Determine whether the following biconditionals are true or false:
   a. $2 + 2 = 4$ if and only if $1 + 1 = 2$
   b. $1 + 1 = 2$ if and only if $2 + 3 = 4$
   c. $1 + 1 = 3$ if and only if monkeys can fly
   d. $0 > 1$ if and only if $2 > 1$

7. Construct the truth tables for following:
   a. $p \vee \sim q$
   b. $\sim p \wedge \sim q$

MODULE-2

Well-formed formulas

1.2. Well – formed Formulas

A ***well-formed formula*** (***wff***) is defined recursively as follows:

(i) *A proposition variable alone is a wff*
(ii) *If a is a wff then $\sim a$ is a wff*
(iii) *If a and b are wffs, then $(a \wedge b)$, $(a \vee b)$, $(a \longrightarrow b)$ and $(a \leftrightarrow b)$ are wffs.*
(iv) *A string of symbols containing the proposition variables, connectives and parentheses is a wff if and only if it can be obtained by finitely many applications of the above rules (i), (ii) and (iii).*

By the above definitions the following are wffs:

$$(p \wedge q) , ((p \wedge q) \longrightarrow q), \Big(((p \longrightarrow q) \wedge (q \longrightarrow r)) \leftrightarrow (p \longrightarrow r)\Big)$$

We use parentheses to avoid ambiguity. For the sake of convenience we shall omit the outer parentheses. Thus we write the above wffs respectively as

$$p \wedge q , (p \wedge q) \longrightarrow q, \big((p \longrightarrow q) \wedge (q \longrightarrow r)\big) \leftrightarrow (p \longrightarrow r)$$

Since we deal with only wffs, we refer wffs as *formulas*.

The following are not formulas

$$p \vee q \wedge r , \ (p \longrightarrow q) \longrightarrow (\wedge r), (p \wedge q) \longrightarrow q)$$

Note:

(i) In the construction of formulas, the parentheses will be used in the same sense in which they are used in elementary algebra or some times in a programming language.

(ii) The following is the hierarchy of operations and parentheses:

1. Connectives within parentheses; among parentheses innermost first
2. Negation $\sim$
3. $\wedge$ and $\vee$
4. $\longrightarrow$
5. $\leftrightarrow$

Truth tables of well-formed Formulas

If there are $\boldsymbol{n}$ distinct variables in a formula, then we need to consider $\mathbf{2}^{\boldsymbol{n}}$ possible combinations of truth values in order to obtain the truth table of the formula.

Construction of truth tables

There are **two** methods of construction of truth tables.

The first columns of the table are for the proposition variables $p, q, r, \ldots$ and create enough number of rows ($i.e.$, 2^n rows if there are n *variables*) in the table for all possible combinations of T and F for the variables.

Method – 1

Devote a column for each elementary stage of the construction of the formula. The truth value at each step is determined from the previous stages by the definition of connectives. Finally the truth value of the formula is given in the last column.

Method – 2

Write the formula on the top row to the right of its variables. A column is drawn for each variable as well as for the connectives that appear in the formula. The truth values are entered step by step. The step numbers at the bottom of the table show the sequence followed in arriving the final step.

Example 1:

Construct the truth table for the formula

$$(p \vee q) \longrightarrow \big((r \vee p) \wedge (\sim r \vee q)\big)$$

Solution:

Method- 1

Let β be $(r \vee p) \wedge (\sim r \vee q)$. Then the given formula is $(p \vee q) \longrightarrow \beta$.

Truth table for $(p \vee q) \longrightarrow ((r \vee p) \wedge (\sim r \vee q))$								
p	q	r	$p \vee q$	$r \vee p$	$\sim r$	$\sim r \vee q$	β	$(p \vee q) \longrightarrow \beta$
T	T	T	T	T	F	T	T	T
T	T	F	T	T	T	T	T	T
T	F	T	T	T	F	F	F	F
T	F	F	T	T	T	T	T	T
F	T	T	T	T	F	T	T	T
F	T	F	T	F	T	T	F	F
F	F	T	F	T	F	F	F	T
F	F	F	F	F	T	T	F	T

Method- 2

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$(\boldsymbol{p}$	$\vee$	$\boldsymbol{q})$	$\longrightarrow$	$((\boldsymbol{r}$	$\vee$	$\boldsymbol{p})$	$\wedge$	$(\sim$	$\boldsymbol{r}$	$\vee$	$\boldsymbol{q}))$
T	T	T	T	T	T	T	T	T	T	T	F	T	T	T
T	T	F	T	T	T	T	F	T	T	T	T	F	T	T
T	F	T	T	T	F	F	T	T	T	F	F	T	F	F
T	F	F	T	T	F	T	F	T	T	T	T	F	T	F
F	T	T	F	T	T	T	T	T	F	T	F	T	T	T
F	T	F	F	T	T	F	F	F	F	F	T	F	T	T
F	F	T	F	F	F	T	T	T	F	F	F	T	F	F
F	F	F	F	F	F	T	F	F	F	F	T	F	T	F
1	**1**	**1**	**1**	**2**	**1**	**7**	**1**	**3**	**1**	**6**	**4**	**1**	**5**	**1**

Step 7 is the final step and it gives the truth values of the given formula

Tautology

A wff is said to be a ***tautology*** *(a* ***universally valid formula*** *or* ***logical truth****) if its truth value is* T *for all possible assignments of truth values to the proposition variables of the formula.*

Note:

(i) If p is any proposition then the formula $p \vee \sim p$ is a tautology
(ii) The conjunction of two tautologies is also a tautology

The proof of the above result (ii) is given below:

Let a and b be formulas which are tautologies. For all possible assignments of truth values to the variables of a and b, the truth values of both a and b will be T and hence the truth value of $a \wedge b$ will be T. Thus $a \wedge b$ is a tautology.

Contradiction

*A wff is said to be a **contradiction** (or **absurdity**) if its truth value is F for all possible assignments of truth values of the proposition variables of the formula.*

Note:

(i) If p is any proposition then the formula $p \wedge \sim p$ is a contradiction
(ii) The negation of a contradiction is a tautology

Contingency

*A wff is said to be **satisfiable** or **contingency** if it is neither a tautology nor a contradiction.*

Ex: If p and q are propositions then $p \wedge q$ and $p \vee q$ are satisfiable (contingency).

Example 2:

Show that the formula $\big(p \longrightarrow (q \longrightarrow r)\big) \longrightarrow \big((p \longrightarrow q) \longrightarrow (p \longrightarrow r)\big)$ is a tautology.

Solution:

Method-1

Let α be the formula $\big(p \longrightarrow (q \longrightarrow r)\big)$ and β be the formula $(p \longrightarrow q) \longrightarrow (p \longrightarrow r)$. Then the given formula is $\alpha \longrightarrow \beta$.

Truth table for $\alpha \longrightarrow \beta$								
p	q	r	$q \longrightarrow r$	α	$p \longrightarrow q$	$p \longrightarrow r$	β	$\alpha \longrightarrow \beta$
T	T	T	T	T	T	T	T	T
T	T	F	F	F	T	F	F	T
T	F	T	T	T	F	T	T	T
T	F	F	T	T	F	F	T	T
F	T	T	T	T	T	T	T	T
F	T	F	F	T	T	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	T	T	T	T

It is a tautology since its truth value is T for all possible assignments of truth values to the proposition variables of the formula.

Method- 2

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$(\boldsymbol{p}$	$\longrightarrow$	$(\boldsymbol{q}$	$\longrightarrow$	$\boldsymbol{r}))$	$\longrightarrow$	$((\boldsymbol{p}$	$\longrightarrow$	$\boldsymbol{q})$	$\longrightarrow$	$(\boldsymbol{p}$	$\longrightarrow$	$\boldsymbol{r}))$
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	F	T	T	T	T	F	T	F	F
T	F	T	T	T	F	T	T	T	T	F	F	T	T	T	T
T	F	F	T	T	F	T	T	T	T	F	F	T	T	F	F
F	T	T	F	T	T	T	T	T	F	T	T	T	F	T	T
F	T	F	F	T	T	F	T	T	F	T	T	T	F	T	F
F	F	T	F	T	F	T	T	T	F	T	F	T	F	T	T
F	F	F	F	T	F	T	T	T	F	T	F	T	F	T	F
1	**1**	**1**	**1**	**3**	**1**	**2**	**1**	**7**	**1**	**4**	**1**	**6**	**1**	**5**	**1**

Step 7 is the final step and it has truth values of T's only. Hence the given formula is a ***tautology***.

Example 3:

Show that the formula $\sim(p \vee q \vee \sim r) \wedge \big((r \longrightarrow p) \vee (r \longrightarrow q)\big)$ is a contradiction.

Solution:

We show this by constructing truth table.

p	q	r	$\sim$	$(p$	$\vee$	q	$\vee$	$\sim$	$r)$	$\wedge$	$((r$	$\longrightarrow$	$p)$	$\vee$	$(r$	$\longrightarrow$	$q))$
T	T	T	F	T	T	T	T	F	T	F	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T	T	F	F	F	T	T	T	F	T	T
T	F	T	F	T	T	F	T	F	T	F	T	T	T	T	T	F	F
T	F	F	F	T	T	F	T	T	F	F	F	T	T	T	F	T	F
F	T	T	F	F	T	T	T	F	T	F	T	F	F	T	T	T	T
F	T	F	F	F	T	T	T	T	F	F	F	T	F	T	F	T	T
F	F	T	T	F	F	F	F	F	T	F	T	F	F	F	T	F	F
F	F	F	F	F	F	F	T	T	F	F	F	T	F	T	F	T	F
1	**1**	**1**	**5**	**1**	**3**	**1**	**4**	**2**	**1**	**9**	**1**	**6**	**1**	**8**	**1**	**7**	**1**

Step 9 is the final step and it has truth values of F only. Hence the given formula is a contradiction.

Example 4:

Is the formula $(p \wedge q) \vee r \longrightarrow p \wedge (q \vee r)$ a tautology, contradiction or contingency?

Solution:

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$((\boldsymbol{p}$	$\wedge$	$\boldsymbol{q})$	$\vee$	$\boldsymbol{r})$	$\longrightarrow$	$(\boldsymbol{p}$	$\wedge$	$(\boldsymbol{q}$	$\vee$	$\boldsymbol{r}))$
T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	F	T	T	T	T	T	F
T	F	T	T	F	F	T	T	T	T	T	F	T	T
T	F	F	T	F	F	F	F	T	T	F	F	F	F
F	T	T	F	F	T	T	T	F	F	F	T	T	T
F	T	F	F	F	T	F	F	T	F	F	T	T	F
F	F	T	F	F	F	T	T	F	F	F	F	T	T
F	F	F	F	F	F	F	F	T	F	F	F	F	F
1	**1**	**1**	**1**	**2**	**1**	**3**	**1**	**6**	**1**	**5**	**1**	**4**	**1**

Step 6 is the final step and it has truth values of T and F. Hence the given formula is neither a ***tautology*** nor a ***contradiction***. Therefore, it is a ***contingency***.

Substitution instance

*Let a and b be formulas. We say that a is a **substitution instance** of b if a can be obtained from b by substituting formulas for the variables of b, with the condition that the same formula is substituted for the same variable each time it occurs.*

Example: Let b: $p \longrightarrow (q \wedge p)$. Then

a: $(r \leftrightarrow s) \longrightarrow \big(q \wedge (r \leftrightarrow s)\big)$is a substitution instance of a , since $r \leftrightarrow s$ is substituted for p in b.Note that $(r \leftrightarrow s) \longrightarrow (q \wedge p)$ is not a substitution instance of b.

Note:

1. In constructing substitution instances of a formula, substitutions are made for the atomic formula and never for the molecular formula:

Ex: $p \longrightarrow q$ is not a substitution instance of $p \longrightarrow \sim r$, since it is r which must be substituted and not $\sim r$.

2. **Any substitution instance of a tautology is a tautology**

It is known that $p \vee \sim p$ is a tautology. If we substitute any formula for p, the resulting formula will be a tautology.

Example 5:

Determine the formulas which are substitution instances of other formulas in the following list and give the substitutions.

(a) $\big(p \longrightarrow (q \longrightarrow p)\big)$
(b) $\Big(\Big(\big((p \longrightarrow q) \wedge (r \longrightarrow s)\big) \wedge (p \vee r)\Big) \longrightarrow (q \vee s)\Big)$
(c) $\Big(q \longrightarrow \big((p \longrightarrow p) \longrightarrow q\big)\Big)$
(d) $\big(p \longrightarrow \big(p \longrightarrow (q \longrightarrow p)\big) \longrightarrow p\big)$

(e) $\Big(\big(((r \longrightarrow s) \wedge (q \longrightarrow p)) \wedge (r \vee q)\big) \longrightarrow (s \vee p)\Big)$

Solution:

(i) Substitute q for p and $(p \longrightarrow p)$ for q in (a), we get (c).Therefore ,(c) is the substitution instance of (a)

(ii) Substitute $\big(p \longrightarrow (q \longrightarrow p)\big)$for q in (a), we get (d). Therefore, (d) is the substitution instance of (a)

(iii) Substitute r, s, q and p for p, q, r and s respectively in (b) we get(e). Therefore, (e) is the substitution instance of $(\ b)$.

P1:

Construct the truth table for $(\boldsymbol{p} \vee \boldsymbol{q}) \vee \sim\boldsymbol{p}$.

Solution:

Truth table for $(p \vee q) \vee \sim p$				
p	q	$p \vee q$	$\sim p$	$(p \vee q) \vee \sim p$
T	T	T	F	T
T	F	T	F	T
F	T	T	T	T
F	F	F	T	T

P2:

Construct the truth table for $(p \longrightarrow q) \wedge (q \longrightarrow p)$.

Solution:

Truth table for $(p \longrightarrow q) \wedge (q \longrightarrow p)$				
p	q	$p \longrightarrow q$	$q \longrightarrow p$	$(p \longrightarrow q) \wedge (q \longrightarrow p)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

P3:

Show that the formula $\sim(\boldsymbol{p} \wedge \boldsymbol{q}) \leftrightarrow (\sim\boldsymbol{p} \vee \sim\boldsymbol{q})$ is a tautology.

Solution:

We show this by constructing its truth table

Method- 1

Truth table for $\alpha : \sim(p \wedge q) \leftrightarrow (\sim p \vee \sim q)$							
p	q	$p \wedge q$	$\sim(p \wedge q)$	$\sim p$	$\sim q$	$(\sim p \vee \sim q)$	α
T	T	T	F	F	F	F	T
T	F	F	T	F	T	T	T
F	T	F	T	T	F	T	T
F	F	F	T	T	T	T	T

It is a tautology since its truth value is T for all possible assignments of truth values to the proposition variables of the formula.

Method- 2

$\boldsymbol{p}$	$\boldsymbol{q}$	$\sim$	$(\boldsymbol{p}$	$\wedge$	$\boldsymbol{q})$	$\leftrightarrow$	$(\sim$	$\boldsymbol{p}$	$\vee$	$\sim$	$\boldsymbol{q})$
T	T	F	T	T	T	T	F	T	F	F	T
T	F	T	T	F	F	T	F	T	T	T	F
F	T	T	F	F	T	T	T	F	T	F	T
F	F	T	F	F	F	T	T	F	T	T	F
1	**1**	**3**	**1**	**2**	**1**	**7**	**4**	**1**	**6**	**5**	**1**

Step 7 is the final step and it has truth values of T only. Hence the given formula is a ***tautology*.**

$\therefore \sim(p \wedge q) \leftrightarrow (\sim p \vee \sim q)$ is a tautology

P4:

If p, q and r are proposition variables then show that $(p \longrightarrow q) \vee (\sim p \longrightarrow r)$ is a tautology.

Solution:

We show this by constructing truth table.

Method-1

Truth Table for $(p \longrightarrow q) \vee (\sim p \longrightarrow r)$							
p	q	r	$a: p \longrightarrow q$	$\sim p$	r	$b: \sim p \longrightarrow r$	$a \vee b$
T	T	T	T	F	T	T	T
T	T	F	T	F	F	T	T
T	F	T	F	F	T	T	T
T	F	F	F	F	F	T	T
F	T	T	T	T	T	T	T
F	T	F	T	T	F	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	F	F	T

It is a tautology since its truth value is T for all possible assignments of truth values to the proposition variables of the formula.

Method-2

p	q	r	$(p$	$\longrightarrow$	$q)$	$\vee$	$(\sim$	p	$\longrightarrow$	$r)$
T	T	T	T	T	T	T	F	T	T	T
T	T	F	T	T	T	T	F	T	T	F
T	F	T	T	F	F	T	F	T	T	T
T	F	F	T	F	F	T	F	T	T	F
F	T	T	F	T	T	T	T	F	T	T
F	T	F	F	T	T	T	T	F	F	F
F	F	T	F	T	F	T	T	F	T	T
F	F	F	F	T	F	T	T	F	F	F
1	**1**	**1**	**1**	**2**	**1**	**5**	**3**	**1**	**4**	**1**

Step 5 is the final step and it has truth values of T only. Hence the given formula is a ***tautology***.

P5:

Show that the formula $(\sim q \wedge p) \wedge (p \longrightarrow q)$ is a contradiction.

Solution:

p	q	$(\sim$	q	$\wedge$	$p)$	$\wedge$	$(p$	$\longrightarrow$	$q)$
T	T	F	T	F	T	F	T	T	T
T	F	T	F	T	T	F	T	F	F
F	T	F	T	F	F	F	F	T	T
F	F	T	F	F	F	F	F	T	F
1	**1**	**2**	**1**	**3**	**1**	**5**	**1**	**4**	**1**

Step 5 is the final step and it has truth values F only. Hence the given formula is a Contradiction

P6:

Show that the formula for $(p \wedge q) \wedge \sim(p \vee q)$ is a contradiction.

Solution:

p	q	$(p$	$\wedge$	$q)$	$\wedge$	$\sim$	$(p$	$\vee$	$q)$
T	T	T	T	T	F	F	T	T	T
T	F	T	F	F	F	F	T	T	F
F	T	F	F	T	F	F	F	T	T
F	F	F	F	F	F	F	F	T	F
1	**1**	**1**	**2**	**1**	**5**	**4**	**1**	**3**	**1**

Step 5 is the final step and it has truth values F only. Hence the given formula is a Contradiction

P7:

Show that the formula $(p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow r)$ is a contingency.

Solution:

p	q	r	$(p$	$\longrightarrow$	$(q$	$\longrightarrow$	$r))$	$\longrightarrow$	$((p$	$\longrightarrow$	$q)$	$\longrightarrow$	$r)$
T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	F	T	T	T	T	F	F
T	F	T	T	T	F	T	T	T	T	F	F	T	T
T	F	F	T	T	F	T	F	T	T	F	F	T	F
F	T	T	F	T	T	T	T	T	F	T	T	T	T
F	T	F	F	T	T	F	F	F	F	T	T	F	F
F	F	T	F	T	F	T	T	T	F	T	F	T	T
F	F	F	F	T	F	T	F	F	F	T	F	F	F
1	**1**	**1**	**1**	**3**	**1**	**2**	**1**	**6**	**1**	**4**	**1**	**5**	**1**

Step 6 is the final step and it has truth values T and F. Thus it is neither a Tautology nor a contradiction. Therefore it is a contingency.

P8:

Show that the formula $(p \longrightarrow (q \vee r)) \longrightarrow ((p \wedge q) \longrightarrow r)$ is a contingency.

Solution:

p	q	r	$(p$	$\longrightarrow$	$(q$	$\vee$	$r))$	$\longrightarrow$	$((p$	$\wedge$	$q)$	$\longrightarrow$	$r)$
T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	F	F	T	T	T	F	F
T	F	T	T	T	F	T	T	T	T	F	F	T	T
T	F	F	T	F	F	F	F	T	T	F	F	T	F
F	T	T	F	T	T	T	T	T	F	F	T	T	T
F	T	F	F	T	T	T	F	T	F	F	T	T	F
F	F	T	F	T	F	T	T	T	F	F	F	T	T
F	F	F	F	T	F	F	F	T	F	F	F	T	F
1	**1**	**1**	**1**	**3**	**1**	**2**	**1**	**6**	**1**	**4**	**1**	**5**	**1**

Step 6 is the final step and it has truth values T and F. Thus it is neither a Tautology nor a contradiction. Therefore it is a contingency.

1.2. Well-Formed Formulas

Exercises:

Which of the following formulas is a tautology, contradiction, contingency?

a. $\sim\big((p \longrightarrow q) \longrightarrow \big((r \vee p) \longrightarrow (r \vee q)\big)\big)$

b. $\big(q \wedge (p \longrightarrow q)\big) \longrightarrow p$

c. $(p \vee q) \longrightarrow \big((p \vee r) \vee (r \vee q)\big)$

d. $\sim\big(p \vee (q \wedge r)\big) \leftrightarrow \big((p \vee q) \wedge (p \vee r)\big)$

e. $\big(p \vee (q \longrightarrow r)\big) \leftrightarrow \big((p \vee \sim r) \longrightarrow q\big)$

f. $p \longrightarrow \Big(q \longrightarrow \Big(r \longrightarrow \big(\sim p \longrightarrow (\sim q \longrightarrow \sim r)\big)\Big)\Big)$

g. $(p \longrightarrow \sim p) \longrightarrow \sim p$

h. $\Big(\big(p \wedge (p \longrightarrow \sim q)\big) \vee (q \longrightarrow \sim q)\Big) \longrightarrow \sim q$

i. $(p \longrightarrow q) \longrightarrow \big((p \vee r) \longrightarrow (q \vee r)\big)$

j. $\big((p \vee q) \wedge \sim r\big) \longrightarrow \sim p \vee r$

k. $\big(\sim(p \vee q \vee \sim r)\big) \wedge \big((r \longrightarrow p) \vee (r \longrightarrow q)\big)$

1.2. Well-Formed Formulas

Answers:

a. Contradiction
b. Contingency
c. Tautology
d. Contradiction
e. Contingency
f. Tautology
g. Tautology
h. Tautology
i. Tautology
j. Contingency
k. Contradiction

MODULE-3

Logical Equivalence and laws of logic

1.3

Logical Equivalence and the Laws of Logic

In this module we define the logical equivalence of wffs, state the principle of duality and prove the laws of logic.

Logical Equivalence

Let a and b be two wffs and let $p_1, p_2, \dots, p_n$ be all the propositional variables occurring in a and b.
We say that a and b are ***equivalent*** (or ***logically equivalent***) if the truth values of a and b are equal for each of the 2^n possible combinations of truth values assigned to $p_1, p_2, \dots, p_n$.

Theorem 1:

a and b are equivalent if and only if $a \leftrightarrow b$ is a tautology.

Proof: Suppose a and b are equivalent. That is, a and b have the same truth value for each of the 2^n possible combinations of truth values assigned to proposition variables $p_1, p_2, \dots, p_n$ and therefore, $a \leftrightarrow b$ is T for each of the 2^n combinations of truth values. Thus, $a \leftrightarrow b$ is a tautology. Conversely, if $a \leftrightarrow b$ is a tautology, then a and b have the same truth value for each of the 2^n combinations of truth values assigned to its n propositional variables. Thus a and b are equivalent.

Representation: We represent the equivalence of a and b by $a \Leftrightarrow b$ or $a \equiv b$,read as a is *equivalent* to b.

Note:

1. The symbol $\Leftrightarrow$ (or $\equiv$) is not a connective in the object language but a symbol in the meta language and it is a relation.
2. Note that $a \equiv b$ is same as $b \equiv a$ ($i.e.$, a and b have the same truth values for each assignment of the truth values for the proposition variables). Thus, equivalence of wffs is a *Symmetric relation*. Further, if $a \equiv b$ and $b \equiv c$ then $a \equiv c$. That is, the equivalence of wffs is a *Transitive relation.*

Duality Law (Principle of Duality)

We shall consider wffs which contain the connectives $\wedge$,$\vee$ and $\sim$. (There is no loss of generality in restricting our consideration to these three connectives since any formula containing any other connectives can be replaced by an equivalent formula containing only these three connectives). We introduce two special variables $\boldsymbol{T_0}$ and $\boldsymbol{F_0}$ denoting a tautology and contradiction respectively.

Dual of a formula

Let a be a formula containing logical connectives $\wedge$, $\vee$, $\sim$ and special variables T_0 and F_0. *The **dual** of a, denoted by a^*, is the formula obtained from a by replacing each occurrence of $\wedge$ and $\vee$ by $\vee$ and $\wedge$ respectively and each occurrence of T_0 and F_0 by F_0 and T_0 respectively.*

The connectives $\wedge$ and $\vee$ are also called *duals* of each other.

Example: The duals of $p \vee \sim p$, $p \vee T_0$ and $(p \vee \sim q) \wedge (r \vee F_0)$ are $p \wedge \sim p$, $p \wedge F_0$ and $(p \wedge \sim q) \vee (r \wedge T_0)$ respectively.

Note: $(a^*)^* = a$

The following is an interesting theorem which states that if any two formulas (containing $\wedge$, $\vee$, $\sim$, T_0 and F_0) are equivalent then their duals are also equivalent to each other.

Theorem 2: Principle of Duality

Let a and b be formulas (containing $\wedge$,$\vee$, $\sim$, $\boldsymbol{T_0}$ and $\boldsymbol{F_0}$). If $\boldsymbol{a} \equiv \boldsymbol{b}$ then $\boldsymbol{a}^* \equiv \boldsymbol{b}^*$.

Basic equivalent formulas:

Theorem 3:

If p and q are proposition variables then the following properties hold:

- *Idempotent properties*

  $p \vee p \equiv p$; $p \wedge p \equiv p$
- *Commutative properties*

  $p \vee q \equiv q \vee p$; $p \wedge q \equiv q \wedge p$

- *Absorption properties*

$$p \wedge (p \vee q) \equiv p \quad ; \qquad p \vee (p \wedge q) \equiv p$$

Proof: We prove $p \vee p \equiv p$, $p \vee q \equiv q \vee p$ and $p \vee (p \wedge q) \equiv p$ through truth tables.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p}$	$\boldsymbol{p \vee p}$	$\boldsymbol{p \vee q}$	$\boldsymbol{q \vee p}$	$\boldsymbol{p \wedge (p \vee q)}$
T	T	T	T	T	T	T
T	F	T	T	T	T	T
F	T	F	F	T	T	F
F	F	F	F	F	F	F

Note that the truth values of $p \vee p$ and p are identical. Therefore $p \vee p \equiv p$.By the same reason $p \vee q \equiv q \vee p$ and $p \wedge (p \vee q) \equiv p$. The other equivalences follow by the principle of duality.

Theorem 4: Negation properties:

If p and q are proposition variables, then the following properties hold:

- *Double negation property*

  $$\sim(\sim p) \equiv p$$

- *De Morgan's properties*

  $$\sim(p \vee q) \equiv \sim p \wedge \sim q \quad ; \qquad \sim(p \wedge q) \equiv \sim p \vee \sim q$$

proof: We prove $\sim(\sim p) \equiv p$ and $\sim(p \vee q) \equiv \sim p \wedge \sim q$ through truth tables.

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

Note that the truth values of $\sim(\sim p)$ and p are identical. Therefore $\sim(\sim p) \equiv p$. By the same reason$\sim(p \vee q) \equiv \sim p \wedge \sim q$.The other De Morgan's law follows by the principle of duality.

Theorem 5:

If p, q and r are proposition variables, then the following properties hold:

- *Associative properties*

  $p \vee (q \vee r) \equiv (p \vee q) \vee r \quad ; \quad p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$
- *Distributive properties*

  $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r) \quad ; \quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Proof: We prove $p \vee (q \vee r) \equiv (p \vee q) \vee r$ and $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ through truth tables.

p	q	r	$(p$	$\vee$	$(q$	$\vee$	$r))$	$((p$	$\vee$	$q)$	$\vee$	$r)$
T	T	T		T		T			T		T	
T	T	F		T		T			T		T	
T	F	T		T		T			T		T	
T	F	F		T		F			T		T	
F	T	T		T		T			T		T	
F	T	F		T		T			T		T	
F	F	T		T		T			F		T	
F	F	F		F		F			F		F	
1	**1**	**1**	**1**	**3**	**1**	**2**	**1**	**1**	**4**	**1**	**5**	**1**

p	q	r	$(p$	$\wedge$	$(q$	$\vee$	$r))$	$((p$	$\wedge$	$q)$	$\vee$	$(p$	$\wedge$	$r))$
T	T	T		T		T			T		T		T	
T	T	F		T		T			T		T		F	
T	F	T		T		T			F		T		T	
T	F	F		F		F			F		F		F	
F	T	T		F		T			F		F		F	
F	T	F		F		T			F		F		F	
F	F	T		F		T			F		F		F	
F	F	F		F		F			F		F		F	
1	**1**	**1**		**3**		**2**			**4**		**6**		**5**	

Note that the truth values of $p \vee (q \vee r)$ and $(p \vee q) \vee r$ are identical. Therefore $p \vee (q \vee r) \equiv (p \vee q) \vee r$. By the same reason $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$. The other equivalences follow by the principle of duality.

Theorem 6:

If p is a proposition variable, T_0 and F_0 are special variables denoting a tautology and contradiction respectively, then the following properties hold:

- *Identity properties*

  $p \wedge T_0 \equiv p \quad ; \quad p \vee F_0 \equiv p$
- *Domination properties*

  $p \vee T_0 \equiv T_0 \quad ; \quad p \wedge F_0 \equiv F_0$
- *Inverse properties*

  $p \vee \sim p \equiv T_0 \quad ; \quad p \wedge \sim p \equiv F_0$

Proof: We prove $p \wedge T_0 \equiv p$, $p \vee T_0 \equiv T_0$ and $p \vee \sim p \equiv T_0$ through the truth tables.

$\boldsymbol{p}$	$\boldsymbol{T_0}$	$\boldsymbol{F_0}$		$(\boldsymbol{p}$	$\wedge$	$\boldsymbol{T_0})$		$(\boldsymbol{p}$	$\vee$	$\boldsymbol{T_0})$		$(\boldsymbol{p}$	$\vee$	$\sim\boldsymbol{p})$
T	T	F			T				T				T	F
F	T	F			F				T				T	T
1					**2**				**3**				**4**	

Note that the truth values of $p \wedge T_0$ and p are identical. Therefore $p \wedge T_0 \equiv p$. By the same reason $p \vee T_0 \equiv T_0$ and $p \vee \sim p \equiv T_0$. The other equivalences follow by the principle of duality.

The equivalences so far given are the properties of the operators ∧,∨ and ∼ on the set of propositions in symbolic logic. The set of all propositions under the operations ∧,∨ and ∼ is an algebra called *algebra of propositions* which is a particular example of a *Boolean algebra*. The following is the list of laws for the algebra of propositions:

The laws of Logic (Logical Equivalences):

If p, q, r are any proposition variables, T_0 is any tautology and F_0 is any contradiction, then the following laws of logic are valid.

Equivalence	Name
$p \vee p \equiv p$; $p \wedge p \equiv p$	Idempotent laws
$p \vee q \equiv q \vee p$; $p \wedge q \equiv q \wedge p$	Commutative laws
$p \wedge (p \vee q) \equiv p$; $p \vee (p \wedge q) \equiv p$	Absorption laws
$\sim(\sim p) \equiv p$	Double negation law
$\sim(p \vee q) \equiv \sim p \wedge \sim q$; $\sim(p \wedge q) \equiv \sim p \vee \sim q$	De Morgan's laws
$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	Associative laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$p \wedge T_0 \equiv p$; $p \vee F_0 \equiv p$	Identity laws
$p \vee T_0 \equiv T_0$; $p \wedge F_0 \equiv F_0$	Domination laws
$p \vee \sim p \equiv T_0$; $p \wedge \sim p \equiv F_0$	Inverse laws

Note the logical equivalences in the above table, except the double negation law, are in pairs where each pair of formulas are duals of each other.

Replacement Process:

It is a process in which we replace any part of the *wff* which is itself a formula (be it *atomic* or *molecular*) by any other formula. In general, a replacement yields a new formula.

Replacement rule: Let a be a formula,b be a formula that appears in a, and let c be a formula such that $c \equiv b$. Let a_1 be the formula obtained by replacing one or more occurrences of b by c in a.Then $a_1 \equiv a$.
Further if a is a tautology then a_1 is also a tautology. That is, if we replace any part or parts of a tautology by formulas that are equivalent to these parts we again get a tautology.

Example:

I. Let a be the formula $(p \longrightarrow q) \longrightarrow r$.We have $p \longrightarrow q \equiv \sim p \vee q$.Let a_1 be the formula obtained by replacing $p \longrightarrow q$ by its equivalent formula $\sim p \vee q$
$i.e.,$ $a_1: (\sim p \vee q) \longrightarrow r$.Then $a \equiv a_1$,

$$i.e., (p \longrightarrow q) \longrightarrow r \equiv (\sim p \vee q) \longrightarrow r$$

II. Let b be the formula $p \longrightarrow (p \vee q)$.Since $p \equiv \sim(\sim p)$, the formula $b_1 : p \longrightarrow (\sim(\sim p) \vee q)$ is derived from b by replacing the second occurrence (but not the first occurrence) of p by $\sim(\sim p)$. By replacement rule $b \equiv b_1$

Equivalent formulas for conditional and Biconditional propositions :

Theorem 7: Prove that

(a) $\boldsymbol{p \longrightarrow q \equiv \sim p \vee q}$
(b) $\boldsymbol{p \leftrightarrow q \equiv (p \longrightarrow q) \wedge (q \longrightarrow p)}$
(c) $\boldsymbol{p \longrightarrow q \equiv \sim q \longrightarrow \sim p}$

Solution: We prove (a) and (b) by constructing truth tables

p	q		p	$\longrightarrow$	q		$(\sim p$	$\vee$	$q)$		p	$\leftrightarrow$	q		$(p$	$\longrightarrow$	$q)$	$\wedge$	$(q$	$\longrightarrow$	$p)$
T	T			T			F	T				T				T		T		T	
T	F			F			F	F				F				F		F		T	
F	T			T			T	T				F				T		F		F	
F	F			T			T	T				T				T		T		T	
1	**1**			**2**			**3**	**4**				**5**				**6**		**8**		**7**	

(c) We have $p \longrightarrow q \equiv \sim p \vee q$

Now, $\sim q \longrightarrow \sim p \equiv \sim(\sim q) \vee \sim p$
$\equiv q \vee \sim p$ (Double negation property, Replacement rule)
$\equiv \sim p \vee q$ (Commutative law for disjunction)
$\equiv p \longrightarrow q$

Therefore $p \longrightarrow q \equiv \sim q \longrightarrow \sim p$ (Symmetry of equivalence)

Note: A conditional proposition $p \longrightarrow q$ and its contrapositive $\sim q \longrightarrow \sim p$ are logical equivalent.

Example 1: Show that $(\boldsymbol{p} \longrightarrow \boldsymbol{q}) \wedge \big(\sim\boldsymbol{q} \wedge (\boldsymbol{r} \vee \sim\boldsymbol{q})\big) \equiv \sim(\boldsymbol{p} \vee \boldsymbol{q})$.

Solution: $(p \longrightarrow q) \wedge \big(\sim q \wedge (r \vee \sim q)\big)$

$\equiv (p \longrightarrow q) \wedge \big(\sim q \wedge (\sim q \vee r)\big)$ (Commutative law for $\vee$)

$\equiv (p \longrightarrow q) \wedge \sim q$ (Absorption law)

$\equiv (\sim p \vee q) \wedge \sim q$ $(\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$

$\equiv (\sim p \wedge \sim q) \vee (q \wedge \sim q)$ (Distributive law)

$\equiv \big(\sim(p \vee q)\big) \vee F_0$ (De Morgan's law and $q \wedge \sim q$ is a contradiction)

$\equiv \sim(p \vee q)$ (Identity law)

Example 2: Show that

$\Big((\boldsymbol{p} \vee \boldsymbol{q}) \wedge \sim\big(\sim\boldsymbol{p} \wedge (\sim\boldsymbol{q} \vee \sim\boldsymbol{r})\big)\Big) \vee (\sim\boldsymbol{p} \wedge \sim\boldsymbol{q}) \vee (\sim\boldsymbol{p} \wedge \sim\boldsymbol{r})$ **is a tautology.**

Solution:

$(\sim p \wedge \sim q) \vee (\sim p \wedge \sim r) \equiv \sim(p \vee q) \vee \sim(p \vee r)$ (De Morgan's law)

$\equiv \sim\big((p \vee q) \wedge (p \vee r)\big)$ (De Morgan's law)

$\equiv \sim\big(p \vee (q \wedge r)\big)$ (Distributive law)

and

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

$\equiv (p \vee q) \wedge \sim\big(\sim p \wedge \sim(q \wedge r)\big)$ (De Morgan's law)

$\equiv (p \vee q) \wedge \sim\Big(\sim\big(p \vee (q \wedge r)\big)\Big)$ (De Morgan's law)

$\equiv (p \vee q) \wedge \Big(\big(p \vee (q \wedge r)\big)\Big)$ (Double negation law)

$\equiv (p \vee q) \wedge \big((p \vee q) \wedge (p \vee r)\big)$ (Distributive law)

$\equiv \big((p \vee q) \wedge (p \vee q)\big) \wedge (p \vee r)$ (Associative law)

$\equiv (p \vee q) \wedge (p \vee r) \equiv p \vee (q \wedge r)$ (Idempotent law)

Now, the given formula is equivalent to $p \vee (q \wedge r) \vee \sim\big(p \vee (q \wedge r)\big) \equiv T_0$
Since it is a substitution instance of a tautology $p \vee \sim p$ (by substituting p by $p \vee (q \wedge r)$).

Example 3: Show that

(i) $\sim(\boldsymbol{p} \wedge \boldsymbol{q}) \longrightarrow \big(\sim\boldsymbol{p} \vee (\sim\boldsymbol{p} \vee \boldsymbol{q})\big) \equiv \sim\boldsymbol{p} \vee \boldsymbol{q}$

(ii) $(\boldsymbol{p} \vee \boldsymbol{q}) \wedge \big(\sim\boldsymbol{p} \wedge (\sim\boldsymbol{p} \wedge \boldsymbol{q})\big) \equiv \sim\boldsymbol{p} \wedge \boldsymbol{q}$

Solution: $\sim(p \wedge q) \longrightarrow \big(\sim p \vee (\sim p \vee q)\big)$

$\equiv \sim\big(\sim(p \wedge q)\big) \vee \big(\sim p \vee (\sim p \vee q)\big)$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$

$\equiv (p \wedge q) \vee \big((\sim p \vee \sim p) \vee q\big)$ (Double negation law and Associative law for $\vee$)

$\equiv (p \wedge q) \vee (\sim p \vee q)$ (Idempotent law)

$\equiv \big((p \wedge q) \vee \sim p\big) \vee q$ (Associative law for $\vee$)

$\equiv \big((p \vee \sim p) \wedge (q \vee \sim p)\big) \vee q$ (Distributive law)

$\equiv \big(T_0 \wedge (q \vee \sim p)\big) \vee q$ (Inverse law)

$\equiv (q \vee \sim p) \vee q$ (Identity law)

$\equiv (\sim p \vee q) \vee q$ (Commutative law for $\vee$)

$\equiv \sim p \vee (q \vee q)$ (Associative law for $\vee$)

$\equiv \sim p \vee q$ (Idempotent law)

This proves (i). Note that

$\sim(p \wedge q) \longrightarrow \big(\sim p \vee (\sim p \vee q)\big) \equiv (p \wedge q) \vee \big(\sim p \vee (\sim p \vee q)\big) \equiv \sim p \vee q$

Therefore $(p \wedge q) \vee \big(\sim p \vee (\sim p \vee q)\big) \equiv \sim p \vee q$

By the principle of duality

$$(p \vee q) \wedge \big(\sim p \wedge (\sim p \wedge q)\big) \equiv \sim p \wedge q$$

P1:

Show that $\sim(\boldsymbol{p} \vee (\sim\boldsymbol{p} \wedge \boldsymbol{q}))$ and $\sim\boldsymbol{p} \wedge \sim\boldsymbol{q}$ are logically equivalent.

Solution:

We prove this by using logical equivalences.

$\sim(p \vee (\sim p \wedge q)) \equiv \sim((p \vee \sim p) \wedge (p \vee q))$ (Distributive law)

$\equiv \sim(T_0 \wedge (p \vee q))$ ($\because$ $p \vee \sim p$ is a tautology)

$\equiv \sim(p \vee q)$ (Identity law)

$\equiv \sim p \wedge \sim q$ (De Morgan's law)

P2:

Show that $(\boldsymbol{p} \wedge \boldsymbol{q}) \longrightarrow (\boldsymbol{p} \vee \boldsymbol{q})$ is a tautology.

Solution:

We show this by using logical equivalences.

$$
\begin{aligned}
(p \wedge q) \longrightarrow (p \vee q) &\equiv \sim(p \wedge q) \vee (p \vee q) && (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta) \\
&\equiv (\sim p \vee \sim q) \vee (p \vee q) && \text{(De Morgans' law)} \\
&\equiv \big((\sim p \vee \sim q) \vee p\big) \vee q && \text{(Associative law for } \vee) \\
&\equiv \big(\sim p \vee (\sim q \vee p)\big) \vee q && \text{(Associative law for } \vee) \\
&\equiv \big(\sim p \vee (p \vee \sim q)\big) \vee q && \text{(Commutativity for } \vee) \\
&\equiv \big((\sim p \vee p) \vee \sim q\big) \vee q && \text{(Associative law for } \vee) \\
&\equiv (\sim p \vee p) \vee (\sim q \vee q) && \text{(Associative law for } \vee) \\
&\equiv T_0 \vee T_0 = T_0
\end{aligned}
$$

P3:

Show that $\sim\left(\sim\left((\boldsymbol{p} \vee \boldsymbol{q}) \wedge \boldsymbol{r}\right) \vee \sim\boldsymbol{q}\right)$ and $\boldsymbol{q} \wedge \boldsymbol{r}$ are logical equivalent.

Solution:

We prove this by using logical equivalences.

$$\sim\left(\sim\left((p \vee q) \wedge r\right) \vee \sim q\right) \equiv \sim\left(\sim\left((p \vee q) \wedge r\right)\right) \wedge \sim(\sim q) \quad \text{(De Morgan's law)}$$

$$\equiv \left((p \vee q) \wedge r\right) \wedge q \quad \text{(Double negation law)}$$

$$\equiv q \wedge \left((p \vee q) \wedge r\right) \quad \text{(Commutative law for } \wedge\text{)}$$

$$\equiv \left(q \wedge (p \vee q)\right) \wedge r \quad \text{(Associative law for } \wedge\text{)}$$

$$\equiv \left(q \wedge (q \vee p)\right) \wedge r \quad \text{(Commutative law for } \vee\text{)}$$

$$\equiv q \wedge r \quad \text{(Absorption law)}$$

P4:

Prove the following logical equivalence

$$\boldsymbol{p} \wedge \Big(\big(\sim\boldsymbol{q} \longrightarrow (\boldsymbol{r} \wedge \boldsymbol{r})\big) \vee \sim\Big(\boldsymbol{q} \vee \big((\boldsymbol{r} \wedge \boldsymbol{s}) \vee (\boldsymbol{r} \wedge \sim\boldsymbol{s})\big)\Big)\Big) \Leftrightarrow \boldsymbol{p}$$

Solution:

$$p \wedge \Big(\big(\sim q \longrightarrow (r \wedge r)\big) \vee \sim\Big(q \vee \big((r \wedge s) \vee (r \wedge \sim s)\big)\Big)\Big)$$

$$\equiv p \wedge \Big((\sim q \longrightarrow r) \vee \sim\Big(q \vee \big(r \wedge (s \vee \sim s)\big)\Big)\Big)$$

(Idempotent law and Distributive law)

$$\equiv p \wedge \Big(\big(\sim(\sim q) \vee r\big) \vee \big(q \vee (r \wedge T_0)\big)\Big)$$

($\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta$, inverse law)

$$\equiv p \wedge \big((q \vee r) \vee \sim(q \vee r)\big)$$ (Double negation law, identity law)

$$\equiv p \wedge T_0$$ (Substitution instance of a tautology)

$$\equiv p$$ (Identity law)

P5:

Show that $\left(\sim \boldsymbol{p} \wedge (\sim \boldsymbol{q} \wedge \boldsymbol{r})\right) \vee (\boldsymbol{q} \wedge \boldsymbol{r}) \vee (\boldsymbol{p} \wedge \boldsymbol{r}) \Leftrightarrow \boldsymbol{r}$

Solution:

$\left(\sim p \wedge (\sim q \wedge r)\right) \vee (q \wedge r) \vee (p \wedge r)$

$\Leftrightarrow \left(\sim p \wedge (\sim q \wedge r)\right) \vee \left((q \vee p) \wedge r\right)$ (Distributive law)

$\Leftrightarrow \left((\sim p \wedge \sim q) \wedge r\right) \vee \left((q \vee p) \wedge r\right)$ (Associative law for ∧)

$\Leftrightarrow \left((\sim p \wedge \sim q) \vee (q \vee p)\right) \wedge r$ (Distributive law)

$\Leftrightarrow \left(\sim (p \vee q) \vee (p \vee q)\right) \wedge r$ (De Morgan's law and commutativity of ∨)

$\Leftrightarrow T_0 \wedge r$ (Substitution instance of a tautology and commutativity of ∨)

$\Leftrightarrow r$ (Identity law)

P6:

Prove the following without using truth tables

(a) $\sim(\boldsymbol{p} \longrightarrow \boldsymbol{q}) \equiv \boldsymbol{p} \wedge \sim\boldsymbol{q}$
(b) $\sim(\boldsymbol{p} \leftrightarrow \boldsymbol{q}) \equiv (\boldsymbol{p} \wedge \sim\boldsymbol{q}) \vee (\sim\boldsymbol{p} \wedge \boldsymbol{q})$

Solution:

(a) $\sim(p \longrightarrow q) \equiv \sim(\sim p \vee q)$ $\quad (\because p \longrightarrow q \equiv \sim p \vee q)$

$\equiv \left(\sim(\sim p)\right) \wedge \sim q$ (De Morgan's law)

$\equiv p \wedge \sim q$ (Double negation law)

(b) $\sim(p \leftrightarrow q) \equiv \sim\left((p \longrightarrow q) \wedge (q \longrightarrow p)\right)$

$\equiv \sim\left((\sim p \vee q) \wedge (\sim q \vee p)\right)$

$\equiv \left(\sim(\sim p \vee q)\right) \vee \left(\sim(\sim q \vee p)\right)$ (De Morgan's law)

$\equiv \left((\sim(\sim p) \wedge \sim q)\right) \vee \left((\sim(\sim q) \wedge \sim p)\right)$ (De Morgan's law)

$\equiv (p \wedge \sim q) \vee (q \wedge \sim p)$ (Double negation law)

$\equiv (p \wedge \sim q) \vee (\sim p \wedge q)$ (Commutative law for conjunction)

P7:

Show that

(a) $(\boldsymbol{p} \wedge \boldsymbol{q}) \longrightarrow \boldsymbol{r} \equiv \boldsymbol{p} \longrightarrow (\boldsymbol{q} \longrightarrow \boldsymbol{r})$
(b) $(\boldsymbol{p} \vee \boldsymbol{q}) \longrightarrow \boldsymbol{r} \equiv (\boldsymbol{p} \longrightarrow \boldsymbol{r}) \wedge (\boldsymbol{q} \longrightarrow \boldsymbol{r})$

Solution:

(a) $(p \wedge q) \longrightarrow r \equiv \big(\sim(p \wedge q)\big) \vee r$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$
$\equiv (\sim p \vee \sim q) \vee r$ (De Morgan's law)
$\equiv \sim p \vee (\sim q \vee r)$ (Associative law for $\vee$)
$\equiv p \longrightarrow (\sim q \vee r)$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$
$\equiv p \longrightarrow (q \longrightarrow r)$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$

(b) $(p \vee q) \longrightarrow r \equiv \sim(p \vee q) \vee r$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$
$\equiv (\sim p \wedge \sim q) \vee r$ (De Morgan's law)
$\equiv (\sim p \vee r) \wedge (\sim q \vee r)$ (Distributive law)
$\equiv (p \longrightarrow r) \wedge (q \longrightarrow r)$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$

P8:

There are two restaurants next to each other. One has a sign that says, "*Good food is not cheap*", and the other has a sign that says, "*Cheap food is not good*". Are the signs saying the same thing?

Solution:

Let g and c respectively denote the propositions *The food is good* and *The food is cheap.*

The first sign *Good food is not cheap* can be written as $g \longrightarrow \sim c$.

The second sign *Cheap food is not good* can be written as $c \longrightarrow \sim g$.

Now, $g \longrightarrow \sim c \equiv \sim g \vee \sim c$ and $c \longrightarrow \sim g \equiv \sim c \vee \sim g$.

Then $g \longrightarrow \sim c \equiv \sim g \vee \sim c \equiv \sim c \vee g \equiv c \longrightarrow \sim g$.

$$\therefore g \longrightarrow \sim c \equiv c \longrightarrow \sim g$$

Thus, the two signs are equivalent. Therefore, they say the same thing.

1.3. Equivalence Formulas, Logical Equivalence and the Laws of Logic

Exercises:

I. Show the following equivalences:

1. $(p \vee q) \wedge \sim(\sim p \wedge q) \equiv p$
2. $p \vee q \vee \big(\sim p \wedge (\sim q \wedge r)\big) \Leftrightarrow p \vee q \vee r$
3. $\sim(p \vee q) \vee \big((\sim p \wedge q) \vee \sim q\big) \Leftrightarrow \sim(p \wedge q)$
4. $p \longrightarrow (q \vee r) \equiv (p \longrightarrow q) \vee (p \longrightarrow r)$
5. $\sim(p \leftrightarrow q) \equiv (p \vee q) \wedge \sim(p \wedge q)$
6. $\big((\sim p \vee \sim q) \longrightarrow (p \wedge q \wedge r)\big) \Leftrightarrow p \wedge q$
7. $\big((p \wedge q) \vee (p \wedge r)\big) \longrightarrow s \equiv \big(\sim p \vee (\sim q \wedge \sim r)\big) \vee s$

II. Show that the following are tautologies.

1. $(p \vee q) \longrightarrow (q \longrightarrow q)$
2. $p \longrightarrow \big(q \longrightarrow (p \wedge q)\big)$
3. $\big((p \vee q) \wedge (p \longrightarrow r) \wedge (q \longrightarrow r)\big) \longrightarrow r$

.

MODULE-4

Normal forms, PCNF, PDNF

1.4. Normal Forms

Decision problem: The problem of determining, in a finite number of steps, whether a given formula is a tautology or a contradiction or at least satisfiable is known as a ***decision problem***.

Since the construction of truth tables involves a finite number of steps, a *decision problem* has a solution in the propositional calculus. The construction of truth tables may not be practical (even with the help of a computer). We therefore look for other methods known as reduction to normal forms.

We use the words "***product***" and "***sum***" in place of "*conjunction*" and "*disjunction*" respectively for convenience.

Elementary product and Elementary sum

A *product* of the variables and their negations is called an ***elementary product***.
A *sum* of the variables and their negations is called an ***elementary sum***.

If p and q are atomic variables then

- $p, \sim p$, $p \wedge \sim p$, $\sim p \wedge q$, $\sim p \wedge \sim q \wedge p \wedge \sim p$ are some examples of elementary products of two variables.
- $p, \sim p \vee q, \sim q \vee p \vee \sim p,\ \ p \vee \sim p,\ \ q \vee p \vee \sim q$ are some examples of elementary sums of two variables.

The following statements hold for elementary sums and products.

- A necessary and sufficient condition for an *elementary product* to be identically false (contradiction) is that it contains a variable and its negation.
- A necessary and sufficient condition for an *elementary sum* to be identically true (tautology) is that it contains a variable and its negation.

Disjunctive normal form of a formula

Let α be a formula. A formula which is equivalent to α and which consist of a sum of elementary products is called a ***disjunctive normal form*** (***DNF***) of α.

Consider the formula $p \vee (q \wedge r)$. Note that the formula is already in the disjunctive normal form. We see that

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r) \equiv \big((p \vee q) \wedge p\big) \vee \big((p \vee q) \wedge r\big)$$

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

From this we say that $(p \wedge p) \vee (q \wedge p) \vee (p \wedge r) \vee (q \wedge r)$ is also a disjunctive normal form of $p \vee (q \wedge r)$.Further,

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

Thus, $p \vee (q \wedge p) \vee (p \wedge r) \vee (q \wedge r)$ is another disjunctive normal form of $p \vee (q \wedge r)$.

Example 1: Show that the formula $\sim q \wedge (p \longrightarrow q) \wedge (\sim p \longrightarrow q)$ is a contradiction.

Solution: We will first write a ***DNF*** of the formula

$$\sim q \wedge (p \longrightarrow q) \wedge (\sim p \longrightarrow q) \equiv \sim q \wedge (\sim p \vee q) \wedge (\sim(\sim p) \vee q)$$

$$\equiv \sim q \wedge (\sim p \vee q) \wedge (p \vee q) \equiv \sim q \wedge \big((\sim p \vee p) \wedge q\big)$$

$$\equiv \sim q \wedge (T_0 \wedge q) \equiv (\sim q \wedge q) \equiv F_0$$

Note:

(1) The disjunctive normal form of a given formula is not unique.
(2) Different disjunctive normal forms of a given formula are equivalent.
(3) To get a unique disjunctive normal form of a given formula, we will introduce the concept of *principle disjunctive normal form* (PDNF).
(4) A given formula is identically *false* (a contradiction) if every *elementary product* present in its disjunctive normal form is identically false (a contradiction). That is every *elementary product* has atleast a variable and its negation.

Example 2: Obtain disjunctive normal forms of

(a) $\boldsymbol{p} \wedge (\boldsymbol{p} \longrightarrow \boldsymbol{q})$

(b) $\sim(\boldsymbol{p} \vee \boldsymbol{q}) \longleftrightarrow (\boldsymbol{p} \wedge \boldsymbol{q})$.

Solution:

(a) $p \wedge (p \longrightarrow q) \equiv p \wedge (\sim p \vee q) \equiv (p \wedge \sim p) \vee (p \wedge q)$

A disjunctive normal form of $p \wedge (p \longrightarrow q)$ is $(p \wedge \sim p) \vee (p \wedge q)$

(b) $\sim(p \vee q) \leftrightarrow (p \wedge q) \equiv \big(\sim(p \vee q) \wedge (p \wedge q)\big) \vee \Big(\sim\big(\sim(p \vee q)\big) \wedge \sim(p \wedge q)\Big)$

$$\big(\because r \leftrightarrow s \equiv (r \wedge s) \vee (\sim r \wedge \sim s)\big)$$

$$\equiv \big(\sim(p \vee q) \wedge (p \wedge q)\big) \vee \big((p \vee q) \wedge \sim(p \wedge q)\big)$$

$$\equiv (\sim p \wedge \sim q \wedge p \wedge q) \vee \big((p \vee q) \wedge (\sim p \vee \sim q)\big)$$

$$\equiv (\sim p \wedge \sim q \wedge p \wedge q) \vee \big((p \vee q) \wedge \sim p\big) \vee \big((p \vee q) \wedge \sim q\big)$$

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

Conjunctive normal form of a formula:

Let α be a formula. A formula which is equivalent to α and which consists of a *product* of *elementary sums* is called a ***conjuctive normal form*** (***CNF***) of α.

Consider the formula $p \wedge (q \vee r)$. Notice that it is the dual of $p \vee (q \wedge r)$. We have already seen that

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

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

Applying the principle of duality to the above two, we get

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

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

Thus we see that

$p \wedge (q \vee r)$,$(p \vee p) \wedge (q \vee p) \wedge (p \vee r) \wedge (q \vee r)$ and $p \wedge (q \vee p) \wedge (p \vee r) \wedge (q \vee r)$ are *CNF*s of $p \wedge (q \vee r)$.

Example 3: Show that the formula $\boldsymbol{q} \vee (\boldsymbol{p} \wedge \sim\boldsymbol{q}) \vee (\sim\boldsymbol{p} \wedge \sim\boldsymbol{q})$ is a tautology.

Solution: We will first write a CNF of the formula.

$$q \vee (p \wedge \sim q) \vee (\sim p \wedge \sim q) \equiv q \vee \big((p \vee \sim p) \wedge \sim q\big)$$

$$\equiv (q \vee p \vee \sim p) \wedge (q \vee \sim q) \quad (CNF)$$

Note that each elementary sum is a tautology. Therefore the given formula is a tautology.

Note:

(1) The conjunctive normal form of a given formula is not unique
(2) Different conjunctive normal forms of a given formula are equivalent
(3) To obtain a unique *CNF* of a given formula, we will introduce the concept of a *principal conjunctive normal form* (*PCNF*)
(4) A given formula is identically *true* (a tautology) if every *elementary sum* present in its *CNF* is identically *true* (tautology). That is every *elementary sum* has atleast a variable and its negation.

Example 4: Obtain conjunctive normal forms of

(a) $\boldsymbol{p} \wedge (\boldsymbol{p} \longrightarrow \boldsymbol{q})$

(b) $\sim(\boldsymbol{p} \vee \boldsymbol{q}) \leftrightarrow (\boldsymbol{p} \wedge \boldsymbol{q})$**.**

Solution:

(a) $p \wedge (p \longrightarrow q) \equiv p \wedge (\sim p \vee q)$

$p \wedge (\sim p \vee q)$ is a conjunctive normal form of $p \wedge (p \longrightarrow q)$.

(b) $\sim(p \vee q) \leftrightarrow (p \wedge q) \equiv \big(\sim(p \vee q) \longrightarrow (p \wedge q)\big) \wedge \big((p \wedge q) \longrightarrow \sim(p \vee q)\big)$

$$(\because r \leftrightarrow s \equiv (r \longrightarrow s) \wedge (s \longrightarrow r))$$

$$\equiv \Big(\sim\big(\sim(p \vee q)\big) \vee (p \wedge q)\Big) \wedge \big(\sim(p \wedge q) \vee \sim(p \vee q)\big)$$

$$\equiv \big((p \vee q) \vee (p \wedge q)\big) \wedge \big((\sim p \vee \sim q) \vee (\sim p \wedge \sim q)\big)$$

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

which is a *CNF* of $\sim(p \vee q) \leftrightarrow (p \wedge q)$.

Principal Disjunctive Normal Forms:

Minterm: A ***minterm*** in n propositional variables $p_1, p_2, \dots, p_n$ is the formula $\boldsymbol{q_1} \wedge \boldsymbol{q_2} \wedge \dots \wedge \boldsymbol{q_n}$ where each $\boldsymbol{q_i}$ is either $\boldsymbol{p_i}$ or $\sim\boldsymbol{p_i}$.

Since each q_i has two choices p_i or $\sim p_i$, *the number of minterms in* n *propositional variables is* 2^n.

The minterms in three propositional variables p, q and r are

$p \wedge q \wedge r,\ p \wedge q \wedge \sim r, p \wedge \sim q \wedge r,\ p \wedge \sim q \wedge \sim r, \sim p \wedge q \wedge r, \sim p \wedge q \wedge \sim r,$ $\sim p \wedge \sim q \wedge r, \sim p \wedge \sim q \wedge \sim r.$

The minterms in two propositional variables p and q are

$$p \wedge q\ , p \wedge \sim q\ , \sim p \wedge q\ , \sim p \wedge \sim q$$

The following is the truth table for the above minterms.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \wedge q}$	$\boldsymbol{p \wedge \sim q}$	$\boldsymbol{\sim p \wedge q}$	$\boldsymbol{\sim p \wedge \sim q}$
T	T	T	F	F	F
T	F	F	T	F	F
F	T	F	F	T	F
F	F	F	F	F	T

Note:

(1) Each minterm has truth value T for exactly one combination of the truth values of the variables.
(2) Different minterms have truth value T for different combinations of truth values of the variables.

Principal disjunctive normal form (Sum-of-products canonical form):

Let a be a formula in n propositional variables. An equivalent formula of a consisting of disjunctions of minterms (in n variables) only is called the ***principal disjunctive normal form (PDNF)*** of a. Such a normal form is also called the ***sum -of -products canonical form***.

Note:

(1) Every formula which is not a contradiction has a unique principal disjunctive normal form.
(2) Two formulas are equivalent if and only if their principal disjunctive normal forms are identical.
(3) A formula is a tautology if and only if all minterms appear in its *PDNF*.

Finding *PDNF* through Truth table: If the truth table of any given formula is known then for every truth value T in the truth table of the formula, select the minterm which also has the truth value T for the same combination of the truth values of the variables .The disjunction of these selected minterms will be equivalent to the given formula and it is the P*DNF* of the formula.

Example 5: Obtain the *PDNF* of the formula $\boldsymbol{q \vee (p \longrightarrow q)}$ through its truth table.

Solution: The truth table of the given formula $q \vee (p \longrightarrow q)$ is given below.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \longrightarrow q}$	$\boldsymbol{q \vee (p \longrightarrow q)}$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

The formula is T for the combination of truth values TT, FT and FF.The minterms which are True for the same combination of truth values are respectively $p \wedge q, \sim p \wedge q$ and $\sim p \wedge \sim q$. Note that the disjunction of these minterms $i.e.,(p \wedge q) \vee (\sim p \wedge q) \vee (\sim p \wedge \sim q)$ is equivalent to the given formula and it is the *PDNF* of the given formula.

Procedure to obtain the PDNF of a given formula without constructing the truth table

1. Replace conditionals and biconditionals by their equivalent formulas containing ∧,∨ and ∼ .
2. Apply laws of negations to the variables using De Morgan's laws and double negation law.
3. Apply distributive laws.
4. Obtain the minterms in the disjunctions by introducing the missing variables.

Example 6: Obtain the *PDNF* of the following formulas

(a) $\boldsymbol{p} \wedge (\boldsymbol{p} \longrightarrow \boldsymbol{q})$

(b) $\sim(\boldsymbol{p} \vee \boldsymbol{q}) \leftrightarrow (\boldsymbol{p} \wedge \boldsymbol{q})$.

Solution:

(a) $p \wedge (p \longrightarrow q) \equiv p \wedge (\sim p \vee q) \equiv (p \wedge \sim p) \vee (p \wedge q)$

$$\equiv F_0 \vee (p \wedge q) \equiv (p \wedge q)$$

$\therefore (p \wedge q)$ is the *PDNF* of $p \wedge (p \longrightarrow q)$

(b) $\sim(p \vee q) \leftrightarrow (p \wedge q) \equiv \big(\sim(p \vee q) \wedge (p \wedge q)\big) \vee \Big(\sim\big(\sim(p \vee q)\big) \wedge \sim(p \wedge q)\Big)$

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

(See Example 2)

$$\equiv F_0 \vee F_0 \vee (q \wedge \sim p) \vee (p \wedge \sim q) \vee F_0 \equiv (\sim p \wedge q) \vee (p \wedge \sim q)$$

$\therefore (\sim p \wedge q) \vee (p \wedge \sim q)$ is the *PDNF* of $\sim(p \vee q) \leftrightarrow (p \wedge q)$

Example 7: Show that $\boldsymbol{p} \vee (\sim \boldsymbol{p} \wedge \boldsymbol{q})$ and $\boldsymbol{p} \vee \boldsymbol{q}$ are equivalent by obtaining their *PDNF*s.

Solution: We show that the two formulas have identical *PDNF*s.

We have $p \equiv p \wedge T_0 \equiv p \wedge (q \vee \sim q) \equiv (p \wedge q) \vee (p \wedge \sim q)$

Now, $p \vee (\sim p \wedge q) \equiv (p \wedge q) \vee (p \wedge \sim q) \vee (\sim p \wedge q)$

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

On the other hand, $q \equiv T_0 \wedge q \equiv \begin{pmatrix} p \vee \\ \sim p \end{pmatrix} \wedge q \equiv (p \wedge q) \vee (\sim p \wedge q)$

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

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

Thus, $p \vee (\sim p \wedge q) \equiv p \vee q$, since they have identical PDNFs.

Note:

The above procedure becomes *tedious* if the given formula is complicated and contains more than three variables.

Principal Conjunctive Normal Forms

Maxterm: A ***maxterm*** in n propositional variables $p_1, p_2, \dots p_n$ is the formula $\boldsymbol{q_1} \vee \boldsymbol{q_2} \vee \dots \vee \boldsymbol{q_n}$ where each $\boldsymbol{q_i}$ is either $\boldsymbol{p_i}$ or $\sim \boldsymbol{p_i}$.

Note that the maxterms are the duals of minterms and *the number of maxterms in n variables is* 2^n.

By the principle of duality, each of the maxterms has the truth value F for exactly one combination of the truth values of the variables.

Different maxterms have truth value F for different combinations of truth values of the variables.

Principal conjunctive normal form (Product-of-Sums canonical form)

Let a be a formula in n propositional variables. An equivalent formula of a consisting of conjunction of maxterms (in n variables) only is called the ***principal conjunctive normal form (PCNF)*** of a. Such a normal form is also called the **product-of- Sums canonical form**.

Note:

1. Every formula which is not a tautology has a unique principal conjunctive normal form
2. Two formulas are equivalent if and only if their principal conjunctive normal forms are identical.
3. A formula is a contradiction if and only if all max terms appear in its PCNF.
4. All assertions made for the PDNFs are also valid for the PCNFs by the principle of duality.

Example 8: Obtain the *PCNF* of the following formulas

(a) $\boldsymbol{p} \wedge (\boldsymbol{p} \longrightarrow \boldsymbol{q})$

(b) $\sim(\boldsymbol{p} \vee \boldsymbol{q}) \leftrightarrow (\boldsymbol{p} \wedge \boldsymbol{q})$.

Solution:

(a) $p \wedge (p \longrightarrow q) \equiv p \wedge (\sim p \vee q)$

Now $p \equiv p \vee F_0 \equiv p \vee (q \vee \sim q) \equiv (p \vee q) \wedge (p \vee \sim q)$

$\therefore\ p \wedge (p \longrightarrow q) \equiv p \wedge (\sim p \vee q) \equiv (p \vee q) \wedge (p \vee \sim q) \wedge (\sim p \vee q)$

$\therefore$ $(p \vee q) \wedge (p \vee \sim q) \wedge (\sim p \vee q)$ is the *PCNF* of $p \wedge (p \longrightarrow q)$

(b) $\sim(p \vee q) \leftrightarrow (p \wedge q) \equiv \big(\sim(p \vee q) \longrightarrow (p \wedge q)\big) \wedge \big((p \wedge q) \longrightarrow \sim(p \vee q)\big)$
$\equiv \big((p \vee q \vee p) \wedge (p \vee q \vee q)\big) \wedge \big((\sim p \vee \sim q \vee \sim p) \wedge (\sim p \vee \sim q \vee \sim q)\big)$

(See Example 4)

$\equiv \big((p \vee q) \wedge (p \vee q)\big) \wedge \big((\sim p \vee \sim q) \wedge (\sim p \vee \sim q)\big) \equiv (p \vee q) \wedge (\sim p \vee \sim q)$

$\therefore$ $(p \vee q) \wedge (\sim p \vee \sim q)$ *is the PCNF* of $\sim(p \vee q) \leftrightarrow (p \wedge q)$.

A notation for the representation of minterms and maxterms:

Suppose that n variables $p_1, p_2, \dots, p_n$ are given and are arranged in a particular order say $p_1, p_2, \dots, p_n$.

The 2^n minterms and 2^n maxterms corresponding to the n variables are respectively denoted by

$$\boldsymbol{m_0, m_1, m_2 \dots, m_{(2^n-1)}} \text{ and } \boldsymbol{M_0, M_1, M_2 \dots, M_{(2^n-1)}}$$

The following procedure is followed to write m_j and M_j.
Write the subscript j in binary form and add appropriate number of zeros on the left (if necessary) so that the number of digits in the binary representation of j is exactly n.

Representation of the minterm $\boldsymbol{m_j}$: If there is a $\mathbf{1}$ (0) in the i^{th} place, from left, in the binary representation of j then the $\boldsymbol{i}^{\textbf{th}}$ **variable $\boldsymbol{i.e.}$, $\boldsymbol{p_i}$** (the negation of the i^{th} variable, $.e.$, $\sim p_i$) appears in the conjunction of the minterm m_j.

Representation of the maxterm $\boldsymbol{M_j}$: If there is a $\mathbf{1}$ (0) in the i^{th} place, from left, in the binary representation of j the **negation of the $\boldsymbol{i}^{\textbf{th}}$ variable, $\boldsymbol{i.e.}$, $\boldsymbol{\sim p_i}$** (the i^{th} variable $i.e.$, p_i) appears in the disjunction of the maxterm M_j.

By this representation, each of $m_0, m_1, \dots, m_{(2^n-1)}$ ($M_0, M_1, \dots, M_{(2^n-1)}$) corresponds to a unique minterm (maxterm), which can be determined by its subscript. Conversely, given any minterm (maxterm) we can find which of $m_0, m_1, \dots, m_{(2^n-1)}$ ($M_0, M_1, \dots, M_{(2^n-1)}$) denotes it.

Minterms and maxterms in two variables:

If p and q are two variables arranged in that order, then the corresponding $2^2 = 4$ minterms and maxterms respectively are denoted by m_0, m_1, m_2, m_3 and M_0, M_1, M_2, M_3. The binary representation of the indices 0,1,2 and 3 are respectively $00, 01, 10$ and 11.

Following the above procedure we write the minterms and maxterms in two variables p, q. They are

$$m_0: \sim p \wedge \sim q\ , \quad m_1: \sim p \wedge q\ , \quad m_2: p \wedge \sim q \text{ and } \quad m_3: p \wedge q$$

$$M_0: p \vee q\ , \quad M_1: p \vee \sim q\ , \quad M_2: \sim p \vee q \text{ and } \quad M_3: \sim p \vee \sim q$$

Minterms and Maxterms in three variables:

If p, q and r are three variables arranged in that order, then the corresponding $2^3 = 8$ minterms and maxterms respectively denoted by

$$m_0, m_1, m_2, \dots, m_6, m_7 \text{ and } M_0, M_1, M_2, \dots, M_6, M_7$$

The binary representation of the indices 0,1,2,3,4,5,6 and 7 are respectively

$$000, 001, 010, 011, 100, 101, 110 \text{ and } 111$$

The corresponding minterms and maxterms are written as

$m_0: \sim p \wedge \sim q \wedge \sim r\ ,\ m_1: \sim p \wedge \sim q \wedge r\ ,\ m_2: \sim p \wedge q \wedge \sim r\ ,\ m_3: \sim p \wedge q \wedge r\ ,$

$m_4: p \wedge \sim q \wedge \sim r\ , \quad m_5 : p \wedge \sim q \wedge r\ , \quad m_6 : p \wedge q \wedge \sim r\ , m_7 : p \wedge q \wedge r$

and

$M_0: p \vee q \vee r\ ,\ M_1: p \vee q \vee \sim r\ ,\ M_2: p \vee \sim q \vee r\ ,\ M_3: p \vee \sim q \vee \sim r\ ,$

$M_4: \sim p \vee q \vee r\ ,\ M_5 : \sim p \vee q \vee \sim r\ , M_6 : \sim p \vee \sim q \vee r\ ,\ M_7 : \sim p \vee \sim q \vee \sim r.$

Note 1: If we have six variables $p_1, p_2, \dots, p_5, p_6$ (arranged in this order) then there are $2^6 = 64$ minterms denoted by $m_0, m_1, m_2, \dots, m_{63}$ and $2^6 = 64$ maxterms denoted by $M_0, M_1, M_2, \dots, M_{63}$.
To write the minterm m_{26} , we write the binary representation of 26 and find it as 011010 .Then

$$m_{26} :\ \sim p_1 \wedge p_2 \wedge p_3 \wedge \sim p_4 \wedge p_5 \wedge \sim p_6$$

Further, the maxterm M_{26} is $p_1 \vee \sim p_2 \vee \sim p_3 \vee p_4 \vee \sim p_5 \vee p_6$.

Conversely, if a minterm say $p_1 \wedge \sim p_2 \wedge \sim p_3 \wedge p_4 \wedge p_5 \wedge \sim p_6$ is given ,then it is an m_j where j is the decimal equivalent of the corresponding binary number 100110. We see that $j = 32 + 0 + 0 + 4 + 2 + 0 = 38$ and the given minterm is m_{38}.

If a maxterm, say $\sim p_1 \vee \sim p_2 \vee p_3 \vee p_4 \vee \sim p_5 \vee p_6$ is given, then it is an M_j where j is the decimal equivalent of the corresponding binary number 110010.We see that $j = 32 + 16 + 0 + 0 + 2 + 0 = 50$ and the given maxterm is M_{50}.

Note 2: In the above discussion

$$m_{26} : \sim p_1 \wedge p_2 \wedge p_3 \wedge \sim p_4 \wedge p_5 \wedge \sim p_6$$

Notice that (i) $\sim m_{26} \equiv \sim(\sim p_1 \wedge p_2 \wedge p_3 \wedge \sim p_4 \wedge p_5 \wedge \sim p_6)$

$$\equiv p_1 \vee \sim p_2 \vee \sim p_3 \vee p_4 \vee \sim p_5 \vee p_6 \equiv M_{26}$$

(ii) The dual of m_{26} $i.e.,$ $(m_{26})^*$ is $\sim p_1 \vee p_2 \vee p_3 \vee \sim p_4 \vee p_5 \vee \sim p_6$ and it is M_{37}

In general in the case of n variables **,**$\boldsymbol{\sim m_j \equiv M_j}$**,** $\boldsymbol{\sim M_j \equiv m_j}$ and

$$(\boldsymbol{m_j})^* \equiv \boldsymbol{M_{(2^n-1)-j}} \;, (\boldsymbol{M_j})^* \equiv \boldsymbol{m_{(2^n-1)-j}}$$

A representation of *PDNF* and *PCNF* of a formula:

If the *PDNF* of a given formula α is the disjunction of the minterms m_i, m_j, m_k(say), then we write the *PDNF* of α in a compact form as $\sum i, j, k$.

If the *PCNF* of a formula α is the conjunction of the maxterms M_k, M_l, M_m, M_n (say), then we write the *PCNF* of α in a compact form as $\prod k, l, m, n$.

Illustration:

The *PDNF* and *PCNF* of the formulas given in examples 6 and 8 are written in the compact form as

(a) $p \wedge (p \longrightarrow q) \equiv p \wedge q \equiv m_3 \equiv \sum 3$

and $p \wedge (p \longrightarrow q) \equiv (p \vee q) \wedge (p \vee \sim q) \wedge (\sim p \vee q) \equiv M_0 \wedge M_1 \wedge M_2 \equiv \prod 0,1,2$

(b). $\sim(p \vee q) \leftrightarrow (p \wedge q) \equiv (p \wedge \sim q) \vee (\sim p \wedge q) \equiv m_2 \vee m_1 \equiv \sum 1,2$

$\sim(p \vee q) \leftrightarrow (p \wedge q) \equiv (p \vee q) \wedge (\sim p \vee \sim q) \equiv M_0 \wedge M_3 \equiv \prod 0,3$

Example 9: Obtain the principal disjunctive normal form of

$$\boldsymbol{a} : (\boldsymbol{p} \vee {\sim}\boldsymbol{q}) \longrightarrow ({\sim}\boldsymbol{p} \wedge \boldsymbol{r}).$$

Solution:

$(p \vee {\sim}q) \longrightarrow ({\sim}p \wedge r) \equiv {\sim}(p \vee {\sim}q) \vee ({\sim}p \wedge r)$

$$\equiv \left({\sim}p \wedge {\sim}({\sim}q)\right) \vee ({\sim}p \wedge r) \equiv ({\sim}p \wedge q) \vee ({\sim}p \wedge r)$$

$({\sim}p \wedge q) \vee ({\sim}p \wedge r)$ is a *DNF* of a.

$$\equiv \left(({\sim}p \wedge q) \wedge T_0\right) \vee \left(({\sim}p \wedge r) \wedge T_0\right)$$

$$\equiv \left(({\sim}p \wedge q) \wedge (r \vee {\sim}r)\right) \vee \left(({\sim}p \wedge r) \wedge (q \vee {\sim}q)\right)$$

$$\equiv ({\sim}p \wedge q \wedge r) \vee ({\sim}p \wedge q \wedge {\sim}r) \vee ({\sim}p \wedge q \wedge r) \vee ({\sim}p \wedge {\sim}q \wedge r)$$

The *PDNF* (or sum -of -products canonical form) of a is

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

$$i.e, m_1 \vee m_2 \vee m_3 \equiv \sum 1,2,3,$$

Therefore, *PDNF* of a in compact form is given by

$$({\sim}p \vee {\sim}q) \longrightarrow ({\sim}p \wedge r) \equiv \sum 1,2,3$$

Example 10: Obtain the *PCNF* of the formula $\boldsymbol{a}$ given by $({\sim}\boldsymbol{p} \longrightarrow \boldsymbol{r}) \wedge (\boldsymbol{q} \leftrightarrow \boldsymbol{p})$

Solution:

$({\sim}p \longrightarrow r) \wedge (q \leftrightarrow p) \equiv ({\sim}({\sim}p) \vee r) \wedge \left((q \longrightarrow p) \wedge (p \longrightarrow q)\right)$

$$\equiv (p \vee r) \wedge ({\sim}q \vee p) \wedge ({\sim}p \vee q)$$

Now, $p \vee r \equiv p \vee r \vee F_0 \equiv p \vee r \vee (q \wedge {\sim}q)$

$$\equiv (p \vee r \vee q) \wedge (p \vee r \vee {\sim}q) \equiv (p \vee q \vee r) \wedge (p \vee {\sim}q \vee r)$$

${\sim}q \vee p \equiv {\sim}q \vee p \vee F_0 \equiv {\sim}q \vee p \vee (r \wedge {\sim}r)$

$$\equiv ({\sim}q \vee p \vee r) \wedge ({\sim}q \vee p \vee {\sim}r) \equiv (p \vee {\sim}q \vee r) \wedge (p \vee {\sim}q \vee {\sim}r)$$

Similarly, ${\sim}p \vee q = ({\sim}p \vee q \vee r) \wedge ({\sim}p \vee q \vee {\sim}r)$

Therefore, $(\sim p \longrightarrow r) \wedge (q \leftrightarrow p)$

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

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

The *PCNF* of α is

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

$$i.e., M_0 \wedge M_2 \wedge M_3 \wedge M_4 \wedge M_5$$

Therefore, $(\sim p \longrightarrow r) \wedge (q \leftrightarrow p) \equiv \prod 0,2,3,4,5$

Theorem 1:

1. ***If the PDNF (PCNF) of a given formula α containing n variables is known, then the PDNF (PCNF) of $\sim\alpha$ is the disjunction (conjunction) of the remaining minterms (maxterms) which do not appear in the PDNF (PCNF) of α.***
2. ***Since $\alpha \equiv \sim(\sim\alpha)$, the PCNF (PDNF) of α can be obtained by applying De Morgan's laws to PDNF (PCNF) of $\sim\alpha$.***

Illustration:

We have, the *PCNF* of the formula

$$\alpha: (\sim p \longrightarrow r) \wedge (q \leftrightarrow p)$$

is $\prod 0,2,3,4,5$. The *PCNF* of $\sim\alpha$ is the conjunction of the remaining maxterms. Therefore, the *PCNF* of $\sim\alpha$ is $\prod 1,6,7$

That is, $\sim\alpha \equiv (p \vee q \vee \sim r) \wedge (\sim p \vee \sim q \vee r) \wedge (\sim p \vee \sim q \vee \sim r)$

Now, $\alpha \equiv \sim(\sim\alpha) \equiv \sim[(p \vee q \vee \sim r) \wedge (\sim p \vee \sim q \vee r) \wedge (\sim p \vee \sim q \vee \sim r)]$

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

$\equiv (\sim p \wedge \sim q \wedge r) \vee (p \wedge q \wedge \sim r) \wedge (p \wedge q \wedge r)$ (By De Morgan's law)

Thus, the *PDNF* of α is $(\sim p \wedge \sim q \wedge r) \vee (p \wedge q \wedge \sim r) \vee (p \wedge q \wedge r)$

$$i.e, \quad m_1 \vee m_6 \vee m_7 \equiv \sum 1,6,7$$

Note:

1. In the above problem, we have $\sim a \equiv \prod 1,6,7$

   Now, $a \equiv \sim(\sim a) \equiv \sim(\prod 1,6,7) \equiv \sim(M_1 \wedge M_6 \wedge M_7) \equiv \sim M_1 \vee \sim M_6 \vee \sim M_7$

$$\equiv m_1 \vee m_6 \vee m_7 \equiv \sum 1,6,7$$

Thus, the *PDNF* of a is $\sum 1,6,7$

❖ ***In general given any formula $\boldsymbol{a}$ containing $\boldsymbol{n}$ variables and using the compact forms to represent the equivalent PDNF and PCNF, we see that all numbers between $\mathbf{0}$ and $\mathbf{2^n - 1}$ which do not appear in one principal normal form will appear in other principal normal form***

Example 11:

The truth table for a formula $\boldsymbol{a}$ is given in the following table. Find the *PDNF* and *PCNF* of $\boldsymbol{a}$.

Truth Table

p	q	r	a
T	T	T	F
T	T	F	F
T	F	T	T
T	F	F	F
F	T	T	T
F	T	F	T
F	F	T	F
F	F	F	T

Solution: The PDNF of a is the disjunction of the minterms corresponding to each truth value T of a.

The minterms corresponding to each truth value T of a are

$$p \wedge \sim q \wedge r, \sim p \wedge q \wedge r, \sim p \wedge q \wedge \sim r \text{ and } \sim p \wedge \sim q \wedge \sim r$$

Therefore, the PDNF of a is

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

$$i.e., m_5 \vee m_3 \vee m_2 \vee m_0 \equiv \sum 0,2,3,5$$

The *PCNF* of a is the conjunction of the maxterms corresponding to each truth value F of a.

The maxterms corresponding to each truth value F of a are

$$\sim p \vee \sim q \vee \sim r, \sim p \vee \sim q \vee r, \sim p \vee q \vee r, p \vee q \vee \sim r$$

Here a maxterms is written by including the variable if its truth value is F and its negation if its truth value is T.Therefore the *PCNF of* a is

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

$$i.e, M_7 \wedge M_6 \wedge M_4 \wedge M_1 \equiv \prod 1,4,6,7$$

P1:

Obtain a DNF of $\boldsymbol{p} \vee \left(\sim\boldsymbol{p} \longrightarrow (\boldsymbol{q} \vee (\boldsymbol{q} \longrightarrow \sim\boldsymbol{r}))\right)$

Solution: $p \vee \left(\sim p \longrightarrow (q \vee (q \longrightarrow \sim r))\right)$

$\equiv p \vee \left(\sim p \longrightarrow (q \vee (\sim q \vee \sim r))\right)$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$

$\equiv p \vee \left(\sim p \longrightarrow (q \vee \sim q \vee \sim r)\right)$

$\equiv p \vee \left(\sim(\sim p) \vee (q \vee \sim q \vee \sim r)\right)$ $\quad (\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta)$

$\equiv p \vee p \vee q \vee \sim q \vee \sim r$ $\quad$ (Double negation law)

Thus, $p \vee p \vee q \vee \sim q \vee \sim r$ is a DNF of the given formula

Note:

1. $p \vee p \vee q \vee \sim q \vee \sim r$ is also a *CNF* of the given formula
2. $p \vee \left(\sim p \longrightarrow (q \vee (q \longrightarrow \sim r))\right) \equiv p \vee p \vee q \vee \sim q \vee \sim r \equiv T_0 (\because\ q \vee \sim q \equiv T_0)$
3. Since the given formula is a tautology, all minterms will appear in its *PDNF*. Thus $p \vee \left(\sim p \longrightarrow (q \vee (q \longrightarrow \sim r))\right) \equiv \sum 0,1,2,3,4,5,6,7$

P2:

Obtain *CNF* of $\left(\boldsymbol{p} \wedge \sim(\boldsymbol{q} \wedge \boldsymbol{r})\right) \vee (\boldsymbol{p} \leftrightarrow \boldsymbol{q})$

Solution: $\left(p \wedge \sim(q \wedge r)\right) \vee (p \leftrightarrow q)$

$$\equiv \left(p \wedge (\sim q \vee \sim r)\right) \vee \left((\sim p \vee q) \wedge (p \vee \sim q)\right)$$

$$(r \leftrightarrow s \equiv (\sim r \vee s) \wedge (r \vee \sim s))$$

$$\equiv \left(p \vee \left((\sim p \vee q) \wedge (p \vee \sim q)\right)\right) \wedge \left((\sim q \vee \sim r) \vee \left((\sim p \vee q) \wedge (p \vee \sim q)\right)\right)$$

$$\equiv \left(\left(p \vee (\sim p \vee q)\right) \wedge \left(p \vee (p \vee \sim q)\right)\right) \wedge \left((\sim q \vee \sim r \vee \sim p \vee q) \wedge (\sim q \vee \sim r \vee p \vee \sim q)\right)$$

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

Thus, $(p \vee \sim p \vee q) \wedge \ (p \vee p \vee \sim q) \wedge (\sim q \vee \sim r \vee \sim p \vee q) \wedge (\sim q \vee \sim r \vee p \vee \sim q)$

is the *CNF* of $\left(p \wedge \sim(q \wedge r)\right) \vee (p \leftrightarrow q)$

Note: The *PCNF* of the given formula is

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

$$\equiv T_0 \wedge \ (p \vee \sim q) \wedge T_0 \wedge (p \vee \sim q \vee \sim r)$$

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

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

$i.e., M_2 \wedge M_3 \equiv \prod 2,3$

P3:

Obtain the principal disjunctive normal forms of

(a) $\sim\boldsymbol{p} \vee \boldsymbol{q}$

(b) $(\boldsymbol{p} \wedge \boldsymbol{q}) \vee (\sim\boldsymbol{p} \wedge \boldsymbol{r}) \vee (\boldsymbol{q} \wedge \boldsymbol{r})$ **.**

Solution:

(a) $\sim p \equiv \sim p \wedge T_0 \equiv \sim p \wedge (q \vee \sim q) \equiv (\sim p \wedge q) \vee (\sim p \wedge \sim q)$ (Distributive law)

$q \equiv T_0 \wedge q \equiv (p \vee \sim p) \wedge q \equiv (p \wedge q) \vee (\sim p \wedge q)$ (Distributive law)

Now, $\sim p \vee q \equiv (\sim p \wedge q) \vee (\sim p \wedge \sim q) \vee (p \wedge q) \vee (\sim p \wedge q)$

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

Thus the *PDNF* of $\sim p \vee q \equiv (\sim p \wedge \sim q) \vee (\sim p \wedge q) \vee (p \wedge q)$

The *PDNF of* $\sim p \vee q$ in compact form *is* $m_0 \vee m_1 \vee m_3 \equiv \sum 0,1,3$

(b) $p \wedge q \equiv p \wedge q \wedge T_0 \equiv p \wedge q \wedge (r \vee \sim r) \equiv (p \wedge q \wedge r) \vee (p \wedge q \wedge \sim r)$

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

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

Now,

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

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

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

Thus, the *PDNF* of the given formula is

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

$$i.e., m_1 \vee m_3 \vee m_6 \vee m_7$$

The *PDNF* of the given formula in compact form is $\sum 1,3,6,7$

P4:

Obtain the *PDNF* of $\boldsymbol{p \longrightarrow \big((p \longrightarrow q) \wedge \sim(\sim q \vee \sim p)\big)}$

Solution: $p \longrightarrow \big((p \longrightarrow q) \wedge \sim(\sim q \vee \sim p)\big)$

$$\equiv p \longrightarrow \Big((\sim p \vee q) \wedge \big(\sim(\sim q) \wedge \sim(\sim p)\big)\Big)$$

($\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta$ and De Morgan's law)

$$\equiv \sim p \vee \big((\sim p \vee q) \wedge (q \wedge p)\big)$$

($\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta$ and Double negation formula)

$$\equiv \sim p \vee \big((\sim p \wedge q \wedge p) \vee (q \wedge q \wedge p)\big) \qquad \text{(Distributive law)}$$

$$\equiv \sim p \vee F_0 \vee (p \wedge q) \equiv \sim p \vee (p \wedge q) \equiv \big(\sim p \wedge (q \vee \sim q)\big) \vee (p \wedge q)$$

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

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

$$\equiv m_0 \vee m_1 \vee m_3 \equiv \sum 0,1,3$$

P5:

Obtain the product-of-sums canonical form (*PCNF*) of

$$\boldsymbol{a} : (\boldsymbol{p} \wedge \boldsymbol{q} \wedge \boldsymbol{r}) \vee (\sim\boldsymbol{p} \wedge \boldsymbol{r} \wedge \boldsymbol{q}) \vee (\sim\boldsymbol{p} \wedge \sim\boldsymbol{q} \wedge \sim\boldsymbol{r}).$$

Solution:

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

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

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

$\equiv \big(T_0 \wedge (q \wedge r)\big) \vee (\sim p \wedge \sim q \wedge \sim r)$

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

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

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

$\equiv (\sim p \vee q) \wedge T_0 \wedge (q \vee \sim r) \wedge (\sim p \vee r) \wedge (\sim q \vee r) \wedge T_0$

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

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

The product-of-sums canonical form of a is

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

$$i.e., M_4 \wedge M_5 \wedge M_1 \wedge M_6 \wedge M_2 \equiv \prod 1,2,4,5,6$$

Aliter:

Notice that a itself is in the *PDNF*, and the *PDNF* of a is $\sum 0,3,7$

Then the *PDNF* of $\sim a$ is the disjunction of the remaining minterms, therefore the *PDNF* of $\sim a$ is $\sum 1,2,4,5,6$

Now, $a \equiv \sim(\sim a) \equiv \sim(\sum 1,2,4,5,6) \equiv \sim(m_1 \vee m_2 \vee m_4 \vee m_5 \vee m_6)$

$$\equiv \sim m_1 \wedge \sim m_2 \wedge \sim m_4 \wedge \sim m_5 \wedge \sim m_6$$

$$\equiv M_1 \wedge M_2 \wedge M_4 \wedge M_5 \wedge M_6$$

$$\equiv \prod 1,2,4,5,6$$

Thus the *PCNF* of a is $\prod 1,2,4,5,6$

P6:

Obtain the sum -of- products canonical form of

$$\boldsymbol{a} : \boldsymbol{p} \vee (\sim\boldsymbol{p} \wedge \sim\boldsymbol{q} \wedge \boldsymbol{r})$$

Solution: Notice that a is in the *DNF* and $\sim p \wedge \sim q \wedge r$ is a minterm. We will introduce the missing variables

$$p \equiv p \wedge T_0 \equiv p \wedge (q \vee \sim q) \equiv (p \wedge q) \vee (p \wedge \sim q)$$

$$\equiv \big((p \wedge q) \wedge T_0\big) \vee \big((p \wedge \sim q) \wedge T_0\big)$$

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

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

Therefore

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

Thus, the sum -of- products canonical form (or *PDNF*) of a is

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

$$i.e., m_1 \vee m_4 \vee m_5 \vee m_6 \vee m_7 \equiv \sum 1,4,5,6,7$$

P7:

Find the *PDNF* and *PCNF* of $\boldsymbol{a} : (\boldsymbol{p} \longrightarrow (\boldsymbol{q} \longrightarrow \boldsymbol{r})) \longrightarrow ((\boldsymbol{p} \longrightarrow \boldsymbol{q}) \longrightarrow \boldsymbol{r})$ through its Truth table.

Solution:

p	q	r	$(p$	$\longrightarrow$	$(q$	$\longrightarrow$	$r))$	$\longrightarrow$	$((p$	$\longrightarrow$	$q)$	$\longrightarrow$	$r)$
T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	F	T	T	T	T	F	F
T	F	T	T	T	F	T	T	T	T	F	F	T	T
T	F	F	T	T	F	T	F	T	T	F	F	T	F
F	T	T	F	T	T	T	T	T	F	T	T	T	T
F	T	F	F	T	T	F	F	F	F	T	T	F	F
F	F	T	F	T	F	T	T	T	F	T	F	T	T
F	F	F	F	T	F	T	F	F	F	T	F	F	F
1	1	1	1	3	1	2	1	6	1	4	1	5	1

Notice that the given formula a is T when the combination of truth values TTT, TTF, TFT, TFF, FTT and FFT for pqr.

The minterms corresponding to each truth value T of a are

$p \wedge q \wedge r, p \wedge q \wedge \sim r, p \wedge \sim q \wedge r, p \wedge \sim q \wedge \sim r, \sim p \wedge q \wedge r$ and $\sim p \wedge \sim q \wedge r$

The *PDNF* of a is the disjunction of minterms corresponding to each truth value T of a. Therefore, the PDNF of a is

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

$$i.e., m_7 \vee m_6 \vee m_5 \vee m_4 \vee m_3 \vee m_1 \equiv \sum 1,3,4,5,6,7$$

Notice that the given formula a is F when the combination of truth values FTF and FFF for pqr.

The maxterms corresponding to each truth value F of a are $p \vee \sim q \vee r$ and $p \vee q \vee r$. (A maxterm is written by including the variable if its truth value is F and its negation if its truth value is T).

The *PCNF* of a is the conjunction of maxterms corresponding to each truth value F of a. Therefore the *PCNF* of a is $(p \vee \sim q \vee r) \wedge (p \vee q \vee r)$.

$$i.e., M_2 \wedge M_0 \equiv \prod 0,2$$

P8:

Find the *PDNF* and *PCNF* of $\boldsymbol{a}$: $\boldsymbol{(p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow r)}$ without constructing its truth table.

Solution**:** We obtain first the PDNF of a.

$(p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow r)$

$\equiv (p \longrightarrow (\sim q \vee r)) \longrightarrow ((\sim p \vee q) \longrightarrow r)$

$\equiv (\sim p \vee (\sim q \vee r)) \longrightarrow (\sim(\sim p \vee q) \vee r)$

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

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

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

Now $p \wedge \sim q \equiv (p \wedge \sim q) \wedge T_0 \equiv (p \wedge \sim q) \wedge (r \vee \sim r)$

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

$r \equiv T_0 \wedge r \equiv (q \vee \sim q) \wedge r \equiv (q \wedge r) \vee (\sim q \wedge r)$

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

Therefore,

$(p \longrightarrow (q \longrightarrow r)) \longrightarrow ((p \longrightarrow q) \longrightarrow r)$

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

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

$$i.e., \; m_7 \vee m_6 \vee m_5 \vee m_4 \vee m_3 \vee m_1 \equiv \sum 1,3,4,5,6,7$$

The above is the *PDNF* of a.

Now, the *PDNF* of $\sim a$ is the disjunction of the remaining minterms, namely $\sum 0,2$

Now, $a \equiv \sim(\sim a) \equiv \sim(\sum 0,2) \equiv \prod 0,2$ (substantiate!)

1.4 Normal forms

EXERCISES

1. Obtain *DNF* of the following formulas:
   i. $(\sim p \vee q) \leftrightarrow (p \wedge q)$
   ii. $p \longrightarrow \big((p \longrightarrow q) \wedge \sim(\sim q \vee \sim p)\big)$
2. Obtain *CNF* of the following formulas:
   i. $\big((p \longrightarrow q) \wedge \sim q\big) \longrightarrow \sim p$
   ii. $\big((p \longrightarrow q) \wedge \sim p\big) \longrightarrow \sim q$
3. Obtain *PDNF* of the formulas: $\sim\big((p \vee q) \wedge r\big) \wedge (p \vee r)$
4. Obtain *PCNF* of the formulas:
   i. $(p \wedge q) \vee (\sim p \wedge q) \vee (p \wedge \sim q)$
   ii. $(p \wedge q) \vee (\sim p \wedge \sim q \wedge r)$
5. Obtain the *PCNF* and *PDNF* of the following formulas:
   i. $p \vee \Big(\sim p \longrightarrow \big(q \vee (\sim q \longrightarrow r)\big)\Big)$
   ii. $(\sim p \vee \sim q) \longrightarrow (p \leftrightarrow \sim q)$
   iii. $\big(p \longrightarrow (q \wedge r)\big) \wedge \big(\sim p \longrightarrow (\sim q \wedge \sim r)\big)$
   iv. $q \wedge (p \vee \sim q)$
   v. $q \vee (p \wedge \sim q)$
   vi. $(q \longrightarrow p) \wedge (\sim p \wedge q)$
   vii. $p \longrightarrow \big(p \wedge (q \longrightarrow p)\big)$
6. Obtain the product of sums canonical form (*PCNF*) of the formula

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

1.4. Normal forms

Answers:

1.

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

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

2.

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

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

3. $\sum 1,4,6$

4.

   i. $\prod 0$

   ii. $\prod 0,2,4,5$

5. *PDNF* ; *PCNF*

   i. $\sum 1,2,34,5,6,7$; $\prod 0$

   ii. $\sum 1,2,3$; $\prod 0$

   iii. $\sum 0,7$; $\prod 1,2,3,4,5,6$

   iv. $\sum 3$; $\prod 0,1,2$

   v. $\sum 1,2,3$; $\prod 0$

   vi. No *PDNF* ; $\prod 0,1,2,3$

   vii. $\sum 0,1,2,3$; No *PCNF*

6. $\prod 0,1,2,3,4,7,8,11,13,14,15$

.

UNIT-2

PROOF TECHNIQUES

MODULE-1

Tautological implications and rules of inferences

1.6

Tautological Implications and Rules of Inference

We have already noted that $p \wedge q, q \wedge p$ are equivalent and $p \vee q, q \vee p$ are equivalent. That is,

$$p \wedge q \equiv q \wedge p \text{ and } p \vee q \equiv q \vee p$$

Also, $p \leftrightarrow q \equiv (p \longrightarrow q) \wedge (q \longrightarrow p) \equiv (q \longrightarrow p) \wedge (p \longrightarrow q) \equiv q \leftrightarrow p$

On the other hand $p \longrightarrow q \not\equiv q \longrightarrow p$ ($i.e.$, $p \longrightarrow q$ is not equivalent to $q \longrightarrow p$), since $p \longrightarrow q, q \longrightarrow p$ are F, T respectively when p is T and q is F.

Tautological implication

Let a and b be *wffs*. We say that ***a* *tautologically imply*** $\boldsymbol{b}$ if and only if $\boldsymbol{a} \longrightarrow \boldsymbol{b}$ ***is a tautology***. *If* a tautologically imply b**,** then we write as $\boldsymbol{a} \Longrightarrow \boldsymbol{b}$ and it is read as $\boldsymbol{a}$ ***tautologically implies*** $\boldsymbol{b}$ or simply $\boldsymbol{a}$ ***implies*** $\boldsymbol{b}$.

Note that $\Longrightarrow$ is not a connective and $a \Longrightarrow b$ is not proposition formula.

To show that $a \Longrightarrow b$*, it is sufficient to show that the assignment of the truth value* T *to the* antecedent a *leads to the truth value* T *for the* consequent .This procedure guarantees that the conditional proposition $a \longrightarrow b$ is a tautology.

Another method to show $a \Longrightarrow b$*, is to assume that the* consequent b *has the truth value* F *and then show that this assumption leads to the truth value* F *for the* antecedent a.

The following tautological implications have important applications:

(1) $p \wedge q \Longrightarrow p$; $p \wedge q \Longrightarrow q$

If the antecedent $p \wedge q$ is T then both p and q are T.Consequently the consequent is also T.Hence the result.

(2) $p \Longrightarrow p \vee q$; $q \Longrightarrow p \vee q$

If the antecedent p is true then the consequent $p \vee q$ is T for whatever truth value of q. This proves $p \Longrightarrow p \vee q$. Similarly the other follows.

(3) $(p \longrightarrow q) \wedge (q \longrightarrow r) \Longrightarrow p \longrightarrow r$

Suppose that the consequent $p \longrightarrow r$ is F. Then p is T and r is F. Now q can have truth value T or F. If q is T then $p \longrightarrow q$ is T and $q \longrightarrow r$ is F and consequently the antecedent is F. On the other hand if q is F then $p \longrightarrow q$ is F and $q \longrightarrow r$ is T and consequently, the antecedent is F. This proves the result.

(4) $(p \longrightarrow q) \wedge (r \longrightarrow s) \wedge (p \vee r) \Longrightarrow (q \vee s)$

Suppose that antecedent is true then $p \longrightarrow q,\ r \longrightarrow s$ and $p \vee r$ are true. Then q and s must be true. Therefore, the consequent $q \vee s$ is true. Thus the implication is valid.

(5) $(p \longrightarrow q) \wedge (r \longrightarrow s) \wedge (\sim q \vee \sim s) \Longrightarrow (\sim p \vee \sim r)$

Suppose that the consequent is false then both p and r are true. For any combination of truth values of q and s the antecedent is F. Thus, the implication is valid.

Theorem 1: *$a \Leftrightarrow b$ if and only if $a \Longrightarrow b$ and $b \Longrightarrow a$.*

$\boldsymbol{i.e.}$, $a \equiv b$ if and only if $a \Longrightarrow b$ and $b \Longrightarrow a$.

Proof: We have $a \longleftrightarrow b$ is equivalent to $(a \longrightarrow b) \wedge (b \longrightarrow a)$

$$i.e., a \longleftrightarrow b \Leftrightarrow (a \longrightarrow b) \wedge (b \longrightarrow a).$$

Suppose that $a \Longrightarrow b$ and $b \Longrightarrow a$. Then $a \longrightarrow b$ is a tautology and $b \longrightarrow a$ is a tautology. Therefore, $(a \longrightarrow b) \wedge (b \longrightarrow a)$ is a tautology (since the conjunction of two tautologies is a tautology).Thus, $a \longleftrightarrow b$ is a tautology. Hence a, b are equivalent $i.e.$, $a \Leftrightarrow b$.

Conversely, suppose that $a \Leftrightarrow b$. Therefore, $a \longleftrightarrow b$ is a tautology. Since $a \longleftrightarrow b \Leftrightarrow (a \longrightarrow b) \wedge (b \longrightarrow a)$, $(a \longrightarrow b) \wedge (b \longrightarrow a)$ is a tautology. If any one of $a \longrightarrow b, b \longrightarrow a$ is not a tautology then their conjugation is not a tautology. Thus, both $a \longrightarrow b$ and $b \longrightarrow a$ are tautologies. This proves $a \Longrightarrow b$ and $b \Longrightarrow a$.
Hence the result.

The following are some important facts about tautological implication and equivalence:

* If a formula is equivalent to a tautology, then it must be a tautology ($i.e.$, if $a \Leftrightarrow T_0$, then a must be a tautology)
* If a formula is implied by a tautology, then it is a tautology ($i.e.$, if $T_0 \Longrightarrow a$, then a is a tautology)
* Equivalence of formulas is transitive ($i.e.$, if $a \Leftrightarrow b$ and $b \Leftrightarrow c$ then $a \Leftrightarrow c$).
* Tautological implication of formulas is also transitive ($i.e.$, if $a \Longrightarrow b$ and $b \Longrightarrow c$ then $a \Longrightarrow c$).

Suppose $a \Longrightarrow b$ and $b \Longrightarrow c$. Then $a \longrightarrow b$ and $b \longrightarrow c$ is a tautology. Therefore $(a \longrightarrow b) \wedge (b \longrightarrow c) \Longrightarrow (a \longrightarrow c)$ and thus $(a \longrightarrow c)$ is implied by a tautology. This proves $a \longrightarrow c$ is a tautology and hence $a \Longrightarrow c$.Thus if $a \Longrightarrow b$ and $b \Longrightarrow c$ then $a \Longrightarrow c$.This proves the tautological implication is transitive.

Note:

(1) If $a \Leftrightarrow b$ and $b \Longrightarrow c$ then $a \Longrightarrow c$
(2) If $a \Longrightarrow b$ and $b \Leftrightarrow c$ then $a \Longrightarrow c$
(3) If $a \Longrightarrow b$ and $a \Longrightarrow c$ then $a \Longrightarrow b \wedge c$.(If a is true then b is true and c is true. Thus, $b \wedge c$ is true. This shows that $a \longrightarrow (b \wedge c)$ is a tautology . Hence $a \Longrightarrow b \wedge c$).

The following are some more tautological implications which have important applications:

(6) $\sim p \Longrightarrow p \longrightarrow q$; $q \Longrightarrow p \longrightarrow q$

We have $p \Longrightarrow p \vee q, i.e., p \longrightarrow (p \vee q)$ is a tautology. Substituting $\sim p$ for p we get $\sim p \longrightarrow (\sim p \vee q)$ and it is a tautology (since the substitution instance of a tautology is also a tautology).Thus $\sim p \Longrightarrow (\sim p \vee q)$.But $\sim p \vee q \equiv p \longrightarrow q$. Therefore, $\sim p \Longrightarrow p \longrightarrow q$. The other result follows from the facts $q \Longrightarrow \sim p \vee q$ and $\sim p \vee q \equiv p \longrightarrow q$.

(7) $\sim(p \longrightarrow q) \Rightarrow p$; $\sim(p \longrightarrow q) \Rightarrow \sim q$

$\sim(p \longrightarrow q) \Leftrightarrow \sim(\sim p \vee q) \Leftrightarrow \sim(\sim p) \wedge \sim q \Leftrightarrow p \wedge \sim q \Rightarrow p$

and $\sim(p \longrightarrow q) \Leftrightarrow p \wedge \sim q \Rightarrow \sim q$
Thus $\sim(p \longrightarrow q) \Rightarrow p$ and $\sim(p \longrightarrow q) \Rightarrow \sim q$

(8) $\sim p \wedge (p \vee q) \Rightarrow q$

$\sim p \wedge (p \vee q) \Leftrightarrow (\sim p \wedge p) \vee (\sim p \wedge q) \Leftrightarrow F_0 \vee (\sim p \wedge q) \Leftrightarrow (\sim p \wedge q) \Rightarrow q$

Thus, $\sim p \wedge (p \vee q) \Rightarrow q$

(9) $p \wedge (p \longrightarrow q) \Rightarrow q$; $\sim q \wedge (p \longrightarrow q) \Rightarrow \sim p$
$p \wedge (p \longrightarrow q) \Leftrightarrow p \wedge (\sim p \vee q) \Leftrightarrow (p \wedge \sim p) \vee (p \wedge q) \Leftrightarrow F_0 \vee (p \wedge q) \Leftrightarrow p \wedge q \Rightarrow q.$
Thus, $p \wedge (p \longrightarrow q) \Rightarrow q$.

$\sim q \wedge (p \longrightarrow q) \Leftrightarrow (\sim q) \wedge (\sim p \vee q) \Leftrightarrow (\sim q \wedge \sim p) \vee (\sim q \wedge q) \Leftrightarrow$
$(\sim p \wedge \sim q) \vee F_0 \Leftrightarrow \sim p \wedge \sim q_0 \Rightarrow \sim p.$
Thus $\sim q \wedge (p \longrightarrow q) \Rightarrow \sim p$.

Let $p_1, p_2, \dots, p_m$ be formulas. These formulas jointly imply a particular formula q ($i.e.$, $p_1, p_2, \dots, p_m \Rightarrow q$) means $p_1 \wedge p_2 \wedge \dots \wedge p_m \Rightarrow q$.

The theory of Inference for propositional calculus

The logic is mainly to provide rules of inference or principles of reasoning. The theory related to the rules of inference is known as the ***inference theory*** since it is concerned with the inferring of a conclusion from certain premises.

The process of deriving a conclusion from a set of premises by using the accepted rules of reasoning is known as a ***deduction*** or ***formal proof***.

In a formal proof every rule of inference that is used at any stage in the derivation is acknowledged. In mathematics we are concerned with the conclusion that is obtained by the rules of logic. This conclusion, called a ***theorem*** ,can be inferred from a set of premises, called the ***axioms** of the theory* and the truth value plays no part in the theory.

In any argument, a conclusion is admitted to be true provided that (i) the premises (assumptions, axioms, hypotheses) are accepted as true and (ii) the reasoning used in deriving the conclusion from the premises following a certain accepted rules of logical inference. Such an argument is called *sound*. In any argument we are always concerned with its soundness.

In logic we concentrate on the study of rules of inference by which conclusions are derived from premises. Any conclusion that is derived by following these rules is called a ***valid conclusion*** and the argument is called a ***valid argument***.

In logic we are concerned with the validity of the argument but not (necessarily) its soundness.

Let a and b be two wffs. We say that **b logically follows from a** or **b is a valid conclusion (consequence) of the premise a** iff a tautologically implies b, $(i.e., a \Rightarrow b)$.Further, we say that a conclusion c logically follows from a set of premises $\{h_1, h_2, \dots, h_m\}$ iff $h_1 \wedge h_2 \wedge \dots \wedge h_m \Rightarrow c$.

Validity using truth tables

Given a set of premises and a conclusion, we can determine whether the conclusion logically follows from the given premises by constructing truth tables as follows:

Let $p_1, p_2, \dots, p_n$ be all atomic variables appearing in the premises $h_1, h_2, \dots, h_m$ and the conclusion c. For all possible combinations of truth values of $p_1, p_2, \dots, p_n$ find the truth values of $h_1, h_2, \dots, h_m$ and c and enter them in the truth table. If for every row in which $h_1, h_2, \dots, h_m$ have the value T, the conclusion c also has value T, then

$$h_1 \wedge h_2 \wedge \dots \wedge h_m \Rightarrow c$$

Alternatively if for every row in which c has value F, at least one of $h_1, h_2, \dots, h_m$ has value F, then

$$h_1 \wedge h_2 \wedge \ldots \wedge h_m \Longrightarrow c$$

This method of determining the validity of a conclusion from a given set of premises is called ***Truth table technique***.

Example 1: Determine whether the conclusion c follows logically from the premises h_1, h_2 … by truth table technique

a) $\boldsymbol{h_1: p \longrightarrow q, h_2: \sim p, c: q}$
b) $\boldsymbol{h_1: \sim p \vee q, h_2: \sim(q \wedge \sim r), h_3: \sim r, c: \sim p}$

Solution:

a) We first construct the truth tables.

p	q	$h_1: p \longrightarrow q$	$h_2: \sim p$	$c: q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	F

Notice that in Table, h_1 and h_2 are true in the third and fourth rows but the conclusion $c: q$ is true only in the third row and not in the fourth row. Therefore, the conclusion is not valid.

b) We first construct the truth table

p	q	r	$h_1: \sim p \vee q$	$h_2: \sim(q \wedge \sim r)$	$h_3: \sim r$	$c: \sim p$
T	T	T	T	T	F	F
T	T	F	T	F	T	F
T	F	T	F	T	F	F
T	F	F	F	T	T	F
F	T	T	T	T	F	T
F	T	F	T	F	T	T
F	F	T	T	T	F	T
F	F	F	T	T	T	T

Observe that the last row is the only row in which h_1, h_2 and h_3 have truth value T. The conclusion c also has the truth value T in that row. Therefore, c logically follows from the given premises h_1, h_2 and h_3.

Note: It is possible to determine in a finite number of steps whether a conclusion follows from a given set of premises through the truth table technique. However, this method becomes tedious when the number of atomic variables present in all the premises and conclusion is large.

Rules of Inference

In the process of derivation to demonstrate a particular formula is a consequence of a given set of premises, we take the following two rules of inference called **rule P** and **rule T**

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

Rule **T**: A formula s may be introduced in a derivation ,if s follows logically from any one or more of the preceding formulas in the derivation.

The following is the list of important implications and equivalences that will be referred frequently. These are not independent of one another.

Table 1 Implications

$p \Rightarrow p \vee q\,; q \Rightarrow p \vee q$ $\sim p \Rightarrow p \longrightarrow q\,; q \Rightarrow p \longrightarrow q$	Disjunctive Addition
$p \wedge q \Rightarrow p\,; p \wedge q \Rightarrow q$ $\sim(p \longrightarrow q) \Rightarrow p\,; \sim(p \longrightarrow q) \Rightarrow \sim q$	Simplification
$p, q \Rightarrow p \wedge q$	Conjunctive Addition
$\sim p, p \vee q \Rightarrow q$	Disjunctive Syllogism
$p, p \longrightarrow q \Rightarrow q$	Modus ponens^*
$\sim q, p \longrightarrow q \Rightarrow \sim p$	Modus tollens^{**}
$p \longrightarrow q, q \longrightarrow r \Rightarrow p \longrightarrow r$	Hypothetical Syllogism
$p \longrightarrow q\,, r \longrightarrow s, p \vee r \Rightarrow q \vee s$	Constructive Dilemma
$p \longrightarrow q\,, r \longrightarrow s, \sim q \vee \sim s \Rightarrow \sim p \vee \sim r$	Destructive Dilemma

$*$ Latin meaning: Method of affirming.

$**$ Latin meaning: Method of denying.

Table 2 Equivalences

$p \vee p \equiv p$; $p \wedge p \equiv p$	Idempotent laws
$p \vee q \equiv q \vee p$; $p \wedge q \equiv q \wedge p$	Commutative laws
$p \wedge (p \vee q) \equiv p$; $p \vee (p \wedge q) \equiv p$	Absorption laws
$\sim(\sim p) \equiv p$	Double negation law
$\sim(p \vee q) \equiv \sim p \wedge \sim q$; $\sim(p \wedge q) \equiv \sim p \vee \sim q$	Demorgan's laws
$p \vee (q \vee r) \equiv (p \vee q) \vee r$; $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	Associative laws
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$; $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$p \wedge T_0 \equiv p$; $p \vee F_0 \equiv p$	Identity laws
$p \vee T_0 \equiv T_0$; $p \wedge F_0 \equiv F_0$	Domination laws
$p \vee \sim p \equiv T_0$; $p \wedge \sim p \equiv F_0$	Inverse laws
$p \longrightarrow q \equiv \sim p \vee q$	
$\sim(p \longrightarrow q) \equiv p \wedge \sim q$	
$p \longrightarrow q \equiv \sim q \longrightarrow \sim p$	
$p \longrightarrow (q \longrightarrow r) \equiv (p \wedge q) \longrightarrow r$	
$p \leftrightarrow q \equiv (p \longrightarrow q) \wedge (q \longrightarrow p)$	
$p \leftrightarrow q \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$	
$\sim(p \leftrightarrow q) \equiv p \leftrightarrow \sim q$	

Example 2: Show that s is a valid inference from the premises:

$\boldsymbol{p \longrightarrow q}$, $\boldsymbol{p \longrightarrow r}$, $\boldsymbol{\sim(q \wedge r)}$ **and** $\boldsymbol{s \vee p}$

Solution:

(1)	$p \longrightarrow q$	**P**
(2)	$p \longrightarrow r$	**P**
(3)	$(p \longrightarrow q) \wedge (p \longrightarrow r)$	**T**; (1), (2), Conjunctive Addition
(4)	$\sim(q \wedge r)$	**P**
(5)	$\sim q \vee \sim r$	**T**; (4), De Morgan's law
(6)	$\sim p \vee \sim p$	**T**; (3),(5), Destructive dilemma
(7)	$\sim p$	**T**; (6), Idempotent law
(8)	$s \vee p$	**P**
(9)	s	**T**; (7), (8), Disjunctive syllogism

Thus, s is a valid inference from the given premises.

Notation: The numbers in the first column designate the line of derivation and the formula. In the second column $\mathbf{P}$ or $\mathbf{T}$ represent the rule of inference, followed by a comment showing from which formulas and tautology that particular formula has been obtained.

Example 3: "If there was a ball game, then travelling was difficult. If they arrived on time, then travelling was not difficult. They arrived on time. Therefore, there was no ball game". Show that these statements constitute a valid argument.

Solution: We first symbolize the given statements and then use the method of derivation.

Let p: There was a ball game.

q: Travelling was difficult.

r: They arrived on time.

Required to show that the conclusion $\sim p$ follows from the premises $p \longrightarrow q, r \longrightarrow \sim q$ and r. The derivation is given below

(1) r	$\mathbf{P}$	
(2) $r \longrightarrow \sim q$	$\mathbf{P}$	
(3) $\sim q$	$\mathbf{T}$	; (1), (2), Modus ponens
(4) $p \longrightarrow q$	$\mathbf{P}$	
(5) $\sim p$	$\mathbf{T}$	; (3), (4), Modus tollens

Thus, the argument is valid.

Third Inference Rule

The following is the basis for the third inference rule

Theorem 2:* *If $p_1, p_2, \dots, p_m$ and p imply q, then $p_1, p_2, \dots, p_m$ imply $p \longrightarrow q$.
i.e., if $(p_1 \wedge p_2 \wedge \dots \wedge p_m \wedge p) \Longrightarrow q$ then $(p_1 \wedge p_2 \wedge \dots \wedge p_m) \Longrightarrow (p \longrightarrow q)$.

Proof: We have $p_1, p_2, \dots, p_m$ and p imply q.

$$i.e., (p_1 \wedge p_2 \wedge \dots \wedge p_m \wedge p) \Rightarrow q.$$

$i.e.$, $(p_1 \wedge p_2 \wedge \dots \wedge p_m \wedge p) \longrightarrow q$ is a tautology.

We have the following result on equivalences:

$$(p_1 \wedge p_2) \longrightarrow p_3 \Leftrightarrow p_1 \longrightarrow (p_2 \longrightarrow p_3)$$

Therefore $(p_1 \wedge p_2 \wedge \dots \wedge p_m \wedge p) \longrightarrow q \Leftrightarrow (p_1 \wedge p_2 \wedge \dots \wedge p_m) \longrightarrow (p \longrightarrow q)$.

Since $(p_1 \wedge p_2 \wedge \dots \wedge p_m \wedge p) \longrightarrow q$ is tautology, $(p_1 \wedge p_2 \wedge \dots \wedge p_m) \longrightarrow (p \longrightarrow q)$ is a tautology. Thus $(p_1 \wedge p_2 \wedge \dots \wedge p_m) \Rightarrow (p \longrightarrow q)$.
Hence the theorem.

The third inference rule is known **as Rule CP** or R**ule of conditional proof.**

Rule CP: If we can derive s from r and a set of premises ,then we can derive $r \longrightarrow s$ from the set of premises alone.

The Rule **CP** is also known as the ***deduction theorem*** and is generally used if the conclusion is of the form $r \longrightarrow s$. In such cases, r is taken as an additional premise and s is derived from the given premises and r.

Example 4: Derive the following ,using rule CP:

$$\boldsymbol{p \longrightarrow (q \longrightarrow r), q \longrightarrow (r \longrightarrow s) \Rightarrow p \longrightarrow (q \longrightarrow s)}$$

Solution: We introduce p as an additional premise and show that $q \longrightarrow s$ follows.

(1) $p \longrightarrow (q \longrightarrow r)$	**P**
(2) p	**P** (additional Premise)
(3) $q \longrightarrow r$	**T** ; (1), (2), Modus ponens
(4) $\sim q \vee r$	**T** ; (3), $\alpha \longrightarrow \beta \Leftrightarrow \sim\alpha \vee \beta$
(5) $\sim q \vee r \vee s$	**T** ; (4), Disjunctive Addition
(6) $\sim q \vee s \vee r$	**T** ; (5), commutativity
(7) $q \longrightarrow (r \longrightarrow s)$	**P**

(8) $\sim q \vee (\sim r \vee s)$ **T** ; (7), $\alpha \longrightarrow \beta \Leftrightarrow \sim\alpha \vee \beta$
(9) $\sim q \vee s \vee \sim r$ **T** ; (8), Commutativity
(10) $(\sim q \vee s \vee r) \wedge (\sim q \vee s \vee \sim r)$ **T** ; (6), (9), Conjunctive Addition
(11) $(\sim q \vee s) \vee (r \wedge \sim r)$ **T** ; (10), Distributive law
(12) $\sim q \vee s$ **T** ; (11), $r \wedge \sim r = F_0$ and $a \vee F_0 \equiv a$
(13) $q \longrightarrow s$ **T** ; $\alpha \longrightarrow \beta \Leftrightarrow \sim\alpha \vee \beta$
(14) $p \longrightarrow (q \longrightarrow s)$ **CP**

Thus, $p \longrightarrow (q \longrightarrow s)$ follows from the given premises.

The above method of derivation provides a partial solution to the decision problem, because if an argument is valid, then it is possible to show by this method that the argument is valid. On the other hand, if an argument is not valid, then it is difficult to decide after a finite number of steps that this is so.

Example 5: If A works hard, then either B or C will enjoy themselves. If B enjoys himself, then A will not work hard. If D enjoys himself, then C will not. Therefore if A works hard, D will not enjoy himself. Show that these statements constitute a valid argument.

Solution: Let a: A works hard

b: B will enjoy himself

c: C will enjoy himself

d: D will enjoy himself

We have to show that

$a \longrightarrow \sim d$ follows from $a \longrightarrow b \vee c$, $b \longrightarrow \sim a$ and $d \longrightarrow \sim c$

Since the conclusion is in the form of a conditional $a \longrightarrow \sim d$, include a as an additional premise and show that $\sim d$ follows logically from all the premises including a. The result follows by the rule **CP.** The following is the derivation.

(1) a Assumed premise
(2) $a \longrightarrow b \vee c$ **P**
(3) $b \vee c$ **T** ; $(1), (2)$, Modus ponens

(4)	$b \longrightarrow \sim a$	**P**
(5)	$a \longrightarrow \sim b$	**T** ; (4), $b \longrightarrow \sim a \equiv \sim(\sim a) \longrightarrow \sim b \equiv a \longrightarrow \sim b$
(6)	$\sim b$	**T** ; $(1), (5)$, Modus ponens.
(7)	$(\sim b) \wedge (b \vee c)$	**T** ; $(3), (6)$, Conjunctive Addition
(8)	$\sim b \wedge c$	**T** ; (7), Distributive law
(9)	c	**T,**Simplification
(10)	$d \longrightarrow \sim c$	**P**
(11)	$\sim d$	**T** ; $(9), (10)$, Modus tollens
(12)	$a \longrightarrow \sim d$	**CP**

Consistency of Premises and Indirect Method of Proof

A set of formulas $h_1, h_2, \dots, h_m$ is said to be ***consistent*** if their conjunction has truth value T for *some* assignment of the truth values to the atomic variables appearing in $h_1, h_2, \dots, h_m$.

If for *every* assignment of the truth values to the atomic variables, at least one of the formulas $h_1, h_2, \dots, h_m$ is false (so that their conjunction is identically false) then the formulas $h_1, h_2, \dots, h_m$ are called ***inconsistent***.

Alternatively, a set of formulas $h_1, h_2, \dots, h_m$ is inconsistent if their conjunction implies a contradiction, $i.e.$, $h_1 \wedge h_2 \wedge \dots \wedge h_m \Longrightarrow r \wedge \sim r$, where r is any formula.

The notion of inconsistency is used in a procedure called ***proof by contradiction*** or ***reduction absurdum*** or ***indirect method of proof.***

To show that c follows logically from the premises $h_1, h_2, \dots, h_m$,we assume that c is false and consider $\sim c$ as an additional premise. If the new set of premises ($i.e.$, $h_1, h_2, \dots, h_m$ and $\sim c$) is in consistent, then the assumption $\sim c$ is true does not hold simultaneously with $h_1, h_2, \dots, h_m$ being true. Therefore c is true whenever $h_1, h_2, \dots, h_m$ are true. Thus, c follows logically from the premises $h_1, h_2, \dots, h_m$.

Example 6: Show that the following premises are inconsistent

1. **If Jack misses many classes through illness, then he fails high school.**
2. **If Jack fails high school, then he is uneducated**
3. **If Jack reads a lot of books, then he is not educated**
4. **Jack misses many classes through illness and reads a lot of books.**

Solution: We first symbolize the given statements and then use the method of derivation.

Let m: Jack misses many classes

f: Jack fails high school

r: Jack reads a lot of books

u: Jack is uneducated

The given premises are

$m \longrightarrow f,\ \ f \longrightarrow u,\ \ r \longrightarrow \sim u$ and $m \wedge r$

Derivation:

(1)	$m \longrightarrow f$	$\mathbf{P}$
(2)	$f \longrightarrow u$	$\mathbf{P}$
(3)	$m \longrightarrow u$	$\mathbf{T}$; (1), (2),Hypothetical syllogism
(4)	$r \longrightarrow \sim u$	$\mathbf{P}$
(5)	$u \longrightarrow \sim r$	$\mathbf{T}$; (4), equivalence of contrapositive
(6)	$m \longrightarrow \sim r$	$\mathbf{T}$; (3), (5),Hypothetical syllogism
(7)	$\sim m \vee \sim r$	$\mathbf{T}$; $(6), p \longrightarrow q\ \equiv \sim p \vee q$
(8)	$\sim(m \wedge r)$	$\mathbf{T}$; (7), DeMorgan's law
(9)	$m \wedge r$	$\mathbf{P}$
(10)	$(m \wedge r) \wedge \sim(m \wedge r)$	$\mathbf{T}$; (8), (9) Conjunctive Addition
(11)	F_0	$\mathbf{T}$; (10), Contradiction.

Thus, the given premises are inconsistent.

Example 7 :Using indirect method ,show that

$$\boldsymbol{\sim(p \longrightarrow q) \longrightarrow \sim(r \vee s),\ \big((q \longrightarrow p) \vee \sim r\big),\ r \Rightarrow p \leftrightarrow q}$$

Solution: We introduce $\sim(p \leftrightarrow q)$ as an additional premise and to show that the given premises and additional premise leads to a contradiction.

(1)	r	$\mathbf{P}$
(2)	$(q \longrightarrow p) \vee \sim r$	$\mathbf{P}$
(3)	$q \longrightarrow p$	$\mathbf{T}$; $(1), (2)$, Disjunctive syllogism
(4)	$\sim(p \leftrightarrow q)$	$\mathbf{P}$ (Additional premise)
(5)	$\sim(p \longrightarrow q) \vee \sim(q \longrightarrow p)$	$\mathbf{T}$; (4), $\sim(p \leftrightarrow q) \equiv \sim\big((p \longrightarrow q) \wedge (q \longrightarrow p)\big)$ $\equiv \sim(p \longrightarrow q) \vee \sim(q \longrightarrow p)$
(6)	$\sim(p \longrightarrow q)$	$\mathbf{T}$; $(3), (5)$, Disjunctive syllogism
(7)	$\sim(p \longrightarrow q) \longrightarrow \sim(r \vee s)$	$\mathbf{P}$
(8)	$\sim(r \vee s)$	$\mathbf{T}$; $(6), (7)$,Modus Ponens
(9)	$\sim r \wedge \sim s$	$\mathbf{T}$; (8), De Morgan's law
(10)	$r \wedge (\sim r \wedge \sim s)$	$\mathbf{T}$; $(1), (9)$, Conjunctive Addition
(11)	F_0	$\mathbf{T}$; (10) Contradiction.

Thus , $(p \leftrightarrow q)$ follows from the given premises.

Note: See annexure for some more solved problems.

P1:

Determine whether the conclusion $\mathbf{c}$ follows logically from the premises $\boldsymbol{h_1, h_2}$ by truth table technique

a) $\boldsymbol{h_1: \sim p, h_2: p \leftrightarrow q, c: \sim(p \wedge q)}$
b) $\boldsymbol{h_1: p \longrightarrow (q \longrightarrow r), h_2: r, c: p}$

Solution:

a) We first construct the truth table

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{h_1: \sim p}$	$\boldsymbol{h_2: p \leftrightarrow q}$	$\boldsymbol{c: \sim(p \wedge q)}$
T	T	F	T	F
T	F	F	F	T
F	T	T	F	T
F	F	T	T	T

Observe that the fourth row is the only row in which both h_1 and h_2 have the truth value T. The conclusion $c: \sim(p \wedge q)$ also has the truth value T in that row. Therefore, the conclusion is valid

b) We first construct the truth table

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{q \longrightarrow r}$	$\boldsymbol{h_1: p \longrightarrow (q \longrightarrow r)}$	$\boldsymbol{h_2: r}$	$\boldsymbol{c: p}$
T	T	T	T	T	T	T
T	T	F	F	F	F	T
T	F	T	T	T	T	T
T	F	F	T	T	F	T
F	T	T	T	T	T	F
F	T	F	F	T	F	F
F	F	T	T	T	T	F
F	F	F	T	T	F	F

Observe that h_1 and h_2 are true in the first, third, fifth and seventh rows, but the conclusion c is true only first and third row and not in the fifth and seventh rows. Therefore, the conclusion does not logically follow from the given premises.

P2:

Show that $\boldsymbol{s \vee r}$ is tautologically implied by the premises

$$(\boldsymbol{p} \vee \boldsymbol{q}) \wedge (\boldsymbol{p} \longrightarrow \boldsymbol{r}) \wedge (\boldsymbol{q} \longrightarrow \boldsymbol{s})$$

Solution:

(1) $p \vee q$	$\mathbf{P}$
(2) $\sim p \longrightarrow q$	$\mathbf{T}$; $\sim p \longrightarrow q \Leftrightarrow \sim(\sim p) \vee q \Leftrightarrow p \vee q$
(3) $q \longrightarrow s$	$\mathbf{P}$
(4) $\sim p \longrightarrow s$	$\mathbf{T}$; (2), (3), Hypothetical syllogism
(5) $\sim s \longrightarrow p$	$\mathbf{T}$; (4), $\sim p \longrightarrow s \Leftrightarrow \sim s \longrightarrow \sim(\sim p) \Leftrightarrow \sim s \longrightarrow p$
(6) $p \longrightarrow r$	$\mathbf{P}$
(7) $\sim s \longrightarrow r$	$\mathbf{T}$; (5), (6), Hypothetical syllogism
(8) $s \vee r$	$\mathbf{T}$; (7), $\sim s \longrightarrow r \Leftrightarrow \sim(\sim s) \vee r \Leftrightarrow s \vee r$

Thus, $s \vee r$ is tautologically implied by the given set of premises.

P3:

Show that $\boldsymbol{r} \vee \boldsymbol{s}$ is a valid inference from the premises

$$\boldsymbol{c} \vee \boldsymbol{d}, (\boldsymbol{c} \vee \boldsymbol{d}) \longrightarrow \sim \boldsymbol{h}, \sim \boldsymbol{h} \longrightarrow (\boldsymbol{a} \wedge \sim \boldsymbol{b}) \text{ and } (\boldsymbol{a} \wedge \sim \boldsymbol{b}) \longrightarrow \boldsymbol{r} \vee \boldsymbol{s} \text{ .}$$

Solution:

(1) $c \vee d \longrightarrow \sim h$ **P**
(2) $\sim h \longrightarrow (a \wedge \sim b)$ **P**
(3) $c \vee d \longrightarrow (a \wedge \sim b)$ **T** ; (1), (2) Hypothetical syllogism
(4) $(a \wedge \sim b) \longrightarrow r \vee s$ **P**
(5) $c \vee d \longrightarrow r \vee s$ **T** ; (3), (4) Hypothetical syllogism
(6) $c \vee d$ **P**
(7) $r \vee s$ **T** ; (5), (6) ,Modus ponens

Thus, $r \vee s$ follows logically from the given set of premises.

P4:

Derive the following, using CP rule:

$$\sim p \lor q, \quad \sim q \lor r, r \longrightarrow s \Longrightarrow p \longrightarrow s$$

Solution: we will introduce p as an additional premise and show that s follows.

(1) $\sim p \lor q$	**P**
(2) $p \longrightarrow q$	**T** ; (1) and (2), $\alpha \longrightarrow \beta \equiv \sim\alpha \lor \beta$
(3) p	**P** (assumed premise)
(4) q	**T** ; (1), (2), (3), Modus ponens
(5) $\sim q \lor r$	**P**
(6) r	**T** ; (4), (5), Disjunctive syllogism
(7) $r \longrightarrow s$	**P**
(8) s	**T** ; (6), (7), Modus ponens
(9) $p \longrightarrow s$	**CP**

Thus, $p \longrightarrow s$ follows from the given premises.

P5:

Show that $r \longrightarrow s$ can be derived from the premises

$$p \longrightarrow (q \longrightarrow s), \sim r \vee p \text{ and } q$$

Solution: Instead of deriving $r \longrightarrow s$, we include r as an additional premise and show that s follows.

(1) $\sim r \vee p$	**P**
(2) $r \longrightarrow p$	**T** ; (1), $\alpha \longrightarrow \beta \equiv \sim\alpha \vee \beta$
(3) r	**P** ; Assumed premise
(4) p	**T** ; (2), (3), Modus ponens
(5) $p \longrightarrow (q \longrightarrow s)$	**P**
(6) $q \longrightarrow s$	**T** ; (4), (5), Modus ponens
(7) q	**P**
(8) s	**T** ; (6), (7), Modus ponens
(9) $r \longrightarrow s$	**CP**

P6:

Show that the following set of premises is inconsistent:

$$\boldsymbol{p \longrightarrow (q \longrightarrow r)\,,\, q \longrightarrow (r \longrightarrow s)\,,\, p \wedge q \wedge \sim s}$$

Solution:

(1)	$p \wedge q \wedge \sim s$	$\mathbf{P}$
(2)	p	$\mathbf{T}$; (1), simplification
(3)	$p \longrightarrow (q \longrightarrow r)$	$\mathbf{P}$
(4)	$q \longrightarrow r$	$\mathbf{T}$; $(2), (3)$, Modus ponens
(5)	q	$\mathbf{T}$; (1), simplification
(6)	r	$\mathbf{T}$; $(4), (5)$, Modus ponens
(7)	$q \longrightarrow (r \longrightarrow s)$	$\mathbf{P}$
(8)	$r \longrightarrow s$	$\mathbf{T}$; $(5), (7)$, Modus ponens
(9)	s	$\mathbf{T}$; $(6), (8)$, Modus ponens
(10)	$\sim s$	$\mathbf{T}$; (1), simplification
(11)	$s \wedge \sim s$	$\mathbf{T}$; $(9), (10)$, Conjunctive Addition
(12)	F_0	$\mathbf{T}$; (11), contradiction

Thus, the given premises are inconsistent.

P7:

Show that the following set of premises is inconsistent:

$$\boldsymbol{p \longrightarrow q\ ,p \longrightarrow r\ ,q \longrightarrow \sim r\ ,p}$$

Solution:

(1) $p \longrightarrow q$	$\mathbf{P}$
(2) p	$\mathbf{P}$
(3) q	$\mathbf{T}$; $(1), (2)$, Modus ponens
(4) $p \longrightarrow r$	$\mathbf{P}$
(5) r	$\mathbf{T}$; $(2), (4)$, Modus ponens
(6) $q \wedge r$	$\mathbf{T}$; $(3), (5)$, Conjunctive Addition
(7) $q \longrightarrow \sim r$	$\mathbf{P}$
(8) $\sim q \vee \sim r$	$\mathbf{T}$; $(7), \alpha \longrightarrow \beta \Leftrightarrow \sim\alpha \vee \beta$
(9) $\sim(q \wedge r)$	$\mathbf{T}$; (8), DeMorgan's law
(10) $(q \wedge r) \wedge \sim(q \wedge r)$	$\mathbf{T}$; $(6), (9)$, Conjunctive addition
(11) F_0	$\mathbf{T}$; (10), Contradiction

Thus, the given premises are inconsistent.

Aliter:

(1) p	$\mathbf{P}$
(2) $p \longrightarrow q$	$\mathbf{P}$
(3) q	$\mathbf{T}$; $(1), (2)$, Modus ponens
(4) $q \longrightarrow \sim r$	$\mathbf{P}$
(5) $\sim r$	$\mathbf{T}$; $(3), (4)$, Modus ponens
(6) $p \longrightarrow r$	$\mathbf{P}$
(7) r	$\mathbf{T}$; $(1), (6)$, Modus ponens
(8) $r \wedge \sim r$	$\mathbf{T}$; $(5), (7)$, Conjunctive addition
(9) F_0	$\mathbf{T}$; (8), contradiction

Thus, the given premises are inconsistent.

P8:

Using indirect method show that

$$\boldsymbol{r \longrightarrow \sim q\ , r \vee s, s \longrightarrow \sim q, p \longrightarrow q \Rightarrow \sim p}$$

Solution: We introduce $\sim(\sim p) \equiv p$ as an additional premise and show the given premises and additional premise leads to a contradiction.

(1) $p \longrightarrow q$	$\mathbf{P}$
(2) p	$\mathbf{P}$ (additional premise $\sim(\sim p)$)
(3) q	$\mathbf{T}$; $(1), (2)$, Modus ponens
(4) $s \longrightarrow \sim q$	$\mathbf{P}$
(5) $\sim s$	$\mathbf{T}$; $(3), (4)$, Modus tollens
(6) $r \vee s$	$\mathbf{P}$
(7) r	$\mathbf{T}$; $(5), (6)$, Disjunctive Syllogism
(8) $r \longrightarrow \sim q$	$\mathbf{P}$
(9) $\sim q$	$\mathbf{T}$; $(7), (8)$, Modus ponens
(10) $q \wedge \sim q$	$\mathbf{T}$; $(3), (9)$, Conjunctive Addition
(11) F_0	$\mathbf{T}$; (10), contradiction

Thus, $\sim p$ follows from the given premises.

1.6. Tautological Implications and Rules of Inference

Exercise:

1. Show that the conclusions c follows from the premises h_1 and h_2 in the following cases:
   a. $h_1 : \sim q \; ; h_2 : p \longrightarrow q \;\; , \;\; c : \sim p$
   b. $h_1 : p \longrightarrow q \; ; h_2 : q \longrightarrow r \;\; , \;\; c : p \longrightarrow r$

2. Determine whether the conclusion c is valid in the following, when h_1 , h_2 … are the premises.
   a. $h_1 : p \vee q \;\; ; \;\; h_2 : p \longrightarrow r \; ; h_3 : q \longrightarrow r \quad , c : r$
   b. $h_1 : \sim p \quad ; \;\; h_2 : p \vee q \quad , c : p \wedge q$

3. Show that the validity of the following arguments, for which the premises are given on the left and conclusion on the right.
   a. $p \longrightarrow q \, , (\sim q \vee r) \wedge \sim r \, , \sim(\sim p \wedge s) \;\; : \quad \sim s$
   b. $b \wedge c \, , (b \leftrightarrow c) \longrightarrow (h \vee g) \qquad : \quad g \vee h$

4. Derive the following, using rule **CP.**

   a. $p, p \longrightarrow \big(q \longrightarrow (r \wedge s)\big) \Rightarrow q \longrightarrow s$
   b. $(p \vee q) \longrightarrow r \Rightarrow (p \wedge q) \longrightarrow r$

5. Show that the following sets of premises are inconsistent.
   a. $a \longrightarrow (b \longrightarrow c) \, , d \longrightarrow (b \wedge \sim c) \, , a \wedge d$
   b. $p \longrightarrow q \, , q \vee r \longrightarrow s, s \longrightarrow \sim p, \;\; p \wedge \sim r$

6. Show the following using indirect method.
   a. $p \longrightarrow (q \longrightarrow \sim r) \, , \sim s \longrightarrow q \, , \sim t \wedge (p \vee t) \Rightarrow (r \longrightarrow s)$
   b. $(p \vee q) \longrightarrow (r \wedge s) \, , r \longrightarrow \sim s \Rightarrow \sim p$

7. Test the validity of the following arguments.

a. If Ram has completed B.E.Computer Science or MBA, then he is assured of a good job. If Ram is assured of a good job, he is happy. Ram is not happy. So Ram has not completed MBA

b. If US tightens visa restrictions, then the demand for BPO will increase. Either US tightens visa restrictions or some computer companies in India close down. The demand for BPO will not increase. Therefore some computer companies in India will close down.

c. If the advertisement is successful, then the sales of the product will go up. Either the advertisement is successful or the production of the product will be stopped. The sales of the product will not go up. Therefore the production of the product will be stopped.

d. If Ram is clever, then Prem is well-behaved. If Joe is good, then Sam is bad and prem is not well-behaved. If Lal is educated, then Joe is good or Ram is clever. Hence, if Lal is educated and Prem is not well-behaved ,then Sam is bad.

1.6

Tautological Implications and Rules of Inference

Annexure:

1. Show that r is tautologically implied by the premises $p \longrightarrow q, q \longrightarrow r$ and p

Solution:

(1) p Rule $\mathbf{P}$
(2) $p \longrightarrow q$ Rule $\mathbf{P}$
(3) q Rule $\mathbf{T}$; (1), (2) and modus ponens
(4) $q \longrightarrow r$ Rule $\mathbf{P}$
(5) r Rule **T** ; (3), (4) and modus ponens

Thus, r is a valid inference from the premises $p \longrightarrow q, q \longrightarrow r$ and p

2.

a. q is a valid inference from the premises: $p \longrightarrow q$, $p \vee q$ and $\sim q$.
b. $r \wedge (p \vee q)$ is a valid inference from the premises

$$p \vee q, q \longrightarrow r, p \longrightarrow m \text{ and } \sim m$$

a. *Solution:*

(1) $p \longrightarrow q$ $\mathbf{P}$
(2) $\sim q$ $\mathbf{P}$
(3) $\sim p$ $\mathbf{T}$; $(1), (2)$, Modus tollens
(4) $p \vee q$ $\mathbf{P}$
(5) q $\mathbf{T}$; $(3), (4)$, disjunctive syllogism.

Thus, q is a valid inference from the given premises.

b. *Solution:*

(1) $p \longrightarrow m$ $\mathbf{P}$
(2) $\sim m$ $\mathbf{P}$
(3) $\sim p$ $\mathbf{T}$; (1), (2), modus tollens
(4) $p \vee q$ $\mathbf{P}$
(5) q $\mathbf{T}$; (3), (4), disjunctive syllogism
(6) $q \longrightarrow r$ $\mathbf{P}$
(7) r $\mathbf{T}$; (5), (6), modus ponens
(8) $r \wedge (p \vee q)$ $\mathbf{T}$; (4), (7), Conjunctive addition

Thus, $r \wedge (p \vee q)$ is a valid conclusion that can be drawn from the given set of premises .

3. Show that $\sim(\boldsymbol{p} \wedge \boldsymbol{q})$ follows from $\sim\boldsymbol{p} \wedge \boldsymbol{q}$

Solution: We introduce $\sim\big(\sim(p \wedge q)\big)$ as an additional premise and show that this leads to a contradiction.

Derivation:

(1)	$\sim\big(\sim(p \wedge q)\big)$	$\mathbf{P}$ (assumed)
(2)	$p \wedge q$	$\mathbf{T}$; (1), double negation law
(3)	p	$\mathbf{T}$; (2), simplification
(4)	$\sim p \wedge \sim q$	$\mathbf{P}$
(5)	$\sim p$	$\mathbf{T}$; (4), simplification
(6)	$p \wedge \sim p$	$\mathbf{T}$; (3), (5), conjunctive addition.
(7)	F_0	$\mathbf{T}$; (6) contradition

MODULE-2

Methods of proofs

1.7 & 1.8

Methods of Proof

A **theorem** is a statement that can be shown to be true. We demonstrate that a theorem is true through a sequence of statements that form an argument, called **proof**. To construct proofs, methods are needed to derive new statements from old ones. The statements used in a proof can include **axioms** or **postulates**, which are underlying assumptions about mathematical structures, the hypotheses of the theorem and previously proved theorems. The **rules of inference**, which are the means used to draw conclusions from other assertions, tie together the steps of a proof. In this module, we discuss the various methods that are commonly used to prove theorems.
The methods of proof discussed in this module are not only important for their use to prove mathematical theorems but are also important for their many applications in computer science. These applications include verifying that computer programs are correct, establishing that operating systems are secure, making inferences in the area of artificial intelligence and so on.

We proved several theorems. We now examine the methodology of constructing proofs and describe how different types of statements are proved.

Vacuous Proof

Suppose that the hypothesis of the conditional $h \longrightarrow c$ is false. Then $h \longrightarrow c$ is true regardless of whether c is true or false. Thus, if the hypothesis h can be shown to be false, then the theorem $h \longrightarrow c$ is true. Such a proof is called a **Vacuous Proof**. (Vacuous proofs are rare and are necessary to handle the special cases).

Example: If $\mathbf{1 = 2}$ then $\mathbf{3 = 4}$
(A conditional with a false hypothesis is guaranteed to be true)

Example: Let $\boldsymbol{P(n)}$ be the proposition "If $\boldsymbol{n}$ is an integer and $\boldsymbol{n} > 1$, then $\boldsymbol{n}^2 > n$". Show that the proposition $\boldsymbol{P(0)}$ is true.

Solution: We have $P(0)$: If $0 > 1$,then $0^2 > 0$. Since the hypothesis is false, $P(0)$ is true by vacuous proof.

Trivial proof

Suppose that the conclusion c of the conditional $h \longrightarrow c$ is true. Then $h \longrightarrow c$ is true irrespective of the truth value of h. If the conclusion c can be shown to be true, then the theorem $h \longrightarrow c$ is true. Such a proof is called **trivial proof.**

Trivial proofs are often important to prove special cases of theorems and in mathematical induction.

Example 1:
Let $P(n)$ be the proposition "if a and b are positive integers with $a \geq b$ and n is an integer, then $a^n \geq b^n$. Show that the proposition $P(0)$ is true.

Solution: We have $P(0)$: If $a \geq b$, then $a^0 \geq b^0$. Since $a^0 = b^0 = 1$, the conclusion of $P(0)$ is true. Thus $P(0)$ is true trivially. Note that in this example of trivial proof we have not used the premise $a \geq b$.

Example 2:
Let $P(n)$: If x is a positive real number and n is any nonnegative integer, then $(1+x)^n \geq 1 + nx$. Show that the proposition $P(0)$ is true.

Solution: We have $P(0)$:If x is a positive real number then $(1+x)^0 \geq 1 + 0.x$. Since $(1+x)^0 = 1 \geq 1 + 0.x$, the conclusion $P(0)$ is true. Thus $P(0)$ is true trivially. In this trivial proof, we have not used the premise $x > 0$.
Many theorems are conditionals $h_1 \wedge h_2 \wedge \ldots \wedge h_m \longrightarrow c$ .Proving such a theorem means verifying that the proposition $h_1 \wedge h_2 \wedge \ldots \wedge h_m \longrightarrow c$ is a tautology ($i.e.$, $h_1 \wedge h_2 \wedge \ldots \wedge h_m \Longrightarrow c$).Therefore the techniques for proving implications are important.

Direct Proof

The conditional $h \longrightarrow c$ can be proved by showing that if h is true, then c must also be true. (This shows that the combination h true and c false never occurs). A proof of this kind is called a **direct proof.**

In the direct proof of the theorem $h \longrightarrow c$, assume the given hypotheses in h are true .Using the laws of logic and previously known facts together with rules of inference prove the derived conclusion c as the final step of a chain of tautological implications: $h \Longrightarrow c_1,\ c_1 \Longrightarrow c_2, \dots\ c_m \Longrightarrow c$. Then by repeated application of the hypothetical syllogism, it follows that $h \Longrightarrow c$.

Example 3:

Prove the following by the direct method of proof. The product of any two odd integers is an odd integer.

Solution: Let x and y be any two odd integers. Then it is known that there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$. Thus,

$$xy = (2m + 1)(2n + 1) = 2(2mn + m + n) + 1 = 2k + 1$$

where $k = 2mn + m + n$ is an integer, since m and n are integers. This shows that xy is an odd integer.

Note: We can rewrite the proof as a chain of tautological implications.

Indirect Proof

Direct proofs lead from the hypothesis h of a theorem to the conclusion c. They begin with the premises, continue with a sequence of logical deductions and end with the conclusion. Proofs that do not start with the hypothesis and end with conclusion are called ***Indirect Proofs***. There are two useful types of indirect proofs. They are (1) **Proof by contraposition** and (2) **Proof by contradiction**.

Proof by contraposition: This proof makes use of the fact that the conditional statement $h \longrightarrow c$ is equivalent to its contrapositive, $\sim c \longrightarrow \sim h$. That is, $h \longrightarrow c$ can be proved by showing its contrapositive $\sim c \longrightarrow \sim h$ is true. Therefore, we take $\sim c$ as hypothesis and using axioms, definitions and previously proven theorems, together with rules of inference we show that $\sim h$ follows. We normally look for a proof by contraposition when we cannot find a direct proof.

Example 4: Prove that if n is an integer and $3n + 2$ *is* odd, then n is odd.

Solution: (To construct a direct proof, we assume that $3n + 2$ is an odd integer, i.e., $3n + 2 = 2k + 1$ for some integer k. We see that $3n = 2k - 1$ and a direct way to conclude that n is odd is not in sight. Therefore we look for a proof by contraposition).

Assume the negation of the conclusion. That is n is even. Therefore, $n = 2k$ for some integer k. Now $3n + 2 = 2(3k + 1)$. This shows that $3n + 2$ is even. That is, $3n + 2$ is not odd which is the negation of the hypothesis. Thus by the proof by contraposition, the given result is proved.

Proof by Contradiction: Suppose we want to prove that a proposition p is true. Further, suppose that we can find a contradiction q such that $\sim p \longrightarrow q$ is true. Since q is false, $\sim p$ is false. This means p is true.
Because the proposition $r \wedge \sim r$ is a contradiction whenever r is a proposition, we can prove p is true if we can show that $\sim p \longrightarrow (r \wedge \sim r)$ is true for some proposition r. Proofs of this type are called ***proofs by contradiction***. Since it does not prove a result directly, it is another type of indirect proof.

Example 5: Prove by contradiction: There is no largest prime number. That is, there are infinitely many prime numbers.

Solution: Notice that the theorem has no hypothesis. Suppose that the given conclusion is false; that is, there is a largest prime number say p. Therefore, we have the prime numbers 2,3,5,7, … , p. Assume that there are k such primes $p_1, p_2, p_3, \ldots, p_k$ i.e., $p_1 = 2$, $p_2 = 3, \ldots, p_k = p$.

Let $n = (2 \cdot 3 \cdot 5 \ldots p) + 1$. Clearly, $n > p$ and n is not divisible by any of these prime numbers 2,3,5, … , p. Who is n? n is either prime or n is composite. If n is prime then we have more than k primes. If n is composite then n is divisible by a prime, $q \neq p_i,\ 1 \leq i \leq k$. Thus we have more than k prime,a contradiction. Therefore, the result follows.

Proof by Contradiction to propositions $h \rightarrow c$:

Proof by contradiction can be used to prove conditional propositions $h \longrightarrow c$. In such proofs, we assume that the hypotheses h are true but the conclusion c is false. Then argue logically and reach a contradiction F_0.

Example 6: Give a proof by contradiction of the theorem: If $3n + 2$ is odd, then n is odd.

Solution: Let $h : 3n + 2$ is odd, $c : n$ is odd. Assume that h is true but c is false. Therefore, h and $\sim c$ is true. That is $3n + 2$ is odd and n is not odd. It follows that n is even and there by $3n + 2$ is even. Thus, $\sim h$ is true. This shows that h and $\sim h$ are true. This is a contradiction. By the proof by contradiction the theorem is proved.

Proof of Equivalence

To prove a theorem that is a biconditional proposition, $i.e.$, a proposition of the form $p \longleftrightarrow q$, we show that $p \longrightarrow q$ and $q \longrightarrow p$ are both true. The validity is based on the tautology

$$(p \longleftrightarrow q) \longleftrightarrow \big((p \longrightarrow q) \wedge (q \longrightarrow p)\big)$$

Example 7: Let n be a positive integer. Then n is odd if and only if n^2 is odd.

Solution: Let p: n is odd; q: n^2 is odd. This theorem is of the form: p if and only if q. To prove the theorem we show that $p \longrightarrow q$ is true and $q \longrightarrow p$ is true.

We use a direct proof to show that $p \rightarrow q$ is true .Suppose p is true .Then n is odd and so $n = 2k + 1$ for some integer k. Therefore, $n^2 = 2(2k^2 + 2k) + 1$.This shows that n^2 is also odd. Thus, $p \longrightarrow q$ is true.

To prove $q \longrightarrow p$ is true, we prove its contraposition. Assume that $\sim p$ is true. Therefore, n is even .Thus, $n = 2k$ for some integer k. Then $n^2 = 2(2k^2)$ is also even and $\sim q$ is true .This proves $\sim p \longrightarrow \sim q$ is true. By proof by contraposition $q \longrightarrow p$ is true. Thus, $p \longleftrightarrow q$ is true.

Note: Some times a theorem states that several propositions $p_1, p_2, \dots, p_n$ are equivalent. This can be written as $p_1 \Leftrightarrow p_2 \Leftrightarrow p_3 \Leftrightarrow \cdots \Leftrightarrow p_n$ and it states that all n propositions have the same truth values, and that consequently, $p_i \Leftrightarrow p_j$ for i and j with $1 \leq i, j \leq n$. One way to prove that these are mutually equivalent is to use the tautology

$$(p_1 \Leftrightarrow p_2 \Leftrightarrow p_3 \Leftrightarrow \cdots \Leftrightarrow p_n) \longrightarrow \big((p_1 \longrightarrow p_2) \wedge (p_2 \longrightarrow p_3) \wedge \ldots \wedge (p_n \longrightarrow p_1)\big)$$

This shows that if the conditional propositions $p_1 \longrightarrow p_2,\ p_2 \longrightarrow p_3,$ $\ldots, p_{n-1} \longrightarrow p_n, p_n \longrightarrow p_1$ are true, then the propositions $p_1, p_2, \ldots, p_n$ are all equivalent.

Example 8: Show that the statements about the integer n

p_1: n is even,

p_2: $n - 1$ is odd,

p_3: n^2 is even

are equivalent.

Solution: We will show that these statements are equivalent by showing that the conditionals $p_1 \longrightarrow p_2,\ p_2 \longrightarrow p_3, p_3 \longrightarrow p_1$ are true.

We use a direct proof to show that $p_1 \longrightarrow p_2$ is true. Suppose n is even. Then $n = 2k$ for some integer k and $n - 1 = 2(k - 1) + 1$. This shows that $n - 1$ is odd. Thus, $p_1 \longrightarrow p_2$ is true.

We use a direct proof to show $p_2 \longrightarrow p_3$ is true. Suppose that $n - 1$ is odd. Then $n - 1 = 2k + 1$ for some integer k. Then $n = 2k + 2$ and $n^2 = 2[2(k + 1)^2]$. This shows that n^2 is even. Thus, $p_2 \longrightarrow p_3$ is even.
To prove $p_3 \longrightarrow p_1$, we prove by contraposition. That is, if n is not even, then n^2 is not even. That is, if n is odd then n^2 is odd. This is true. (We have already proved). Thus, $p_3 \longrightarrow p_1$ is true. Therefore p_1, p_2, p_3 are equivalent.

Proofs by Cases

It is a method of proof that can be used to prove a theorem by considering different cases separately. To prove a conditional statement of the form

$$(h_1 \vee h_2 \vee \dots \vee h_m) \longrightarrow c$$

the equivalence $(h_1 \vee h_2 \vee \dots \vee h_m) \longrightarrow c \Leftrightarrow (h_1 \longrightarrow c) \wedge (h_2 \longrightarrow c) \wedge \dots \wedge (h_m \longrightarrow c)$ can be used as a rule of inference.

This shows that the conditional statement with a hypothesis made up of a disjunction of the propositions $h_1, h_2, \dots, h_m$ can be proved by proving each of the n conditional statements $h_i \longrightarrow c$, $1 \leq i \leq n$, is true individually. Such an argument is called a **proof by cases**.

Note: Some times to prove a conditional statement $h \longrightarrow c$ is true, it is convenient to use a disjunction $h_1 \vee h_2 \vee \dots \vee h_m$ instead of h if h is equivalent $h_1 \vee h_2 \vee \dots \vee h_m$.

Example 9: Prove that if n is an integer, then $n^2 \geq n$.

Solution: We prove the conclusion by considering three cases, when $n = 0, n \geq 1$ and $n \leq -1$.

Case (i): When $n = 0$, we have $n^2 \geq 0$, since $0^2 \geq 0$. The conclusion is true in this case.

Case (ii): When $n \geq 1$, we have $n^2 = n \cdot n \geq n \cdot 1 = n$. The conclusion is true in this case.

Case (iii): When $n \leq -1$, we have $n^2 \geq 0$.Thus $n^2 \geq n$. The conclusion is true in this case also.

Thus, the conclusion is true in all the three cases. Therefore $n^2 \geq n$, if n is an integer (by proof by cases).

Note: A proof by cases is considered if it is not possible to consider all cases of a proof at the same time.

Exhaustive proof: Some theorems can be proved by examining a relatively small number of particular cases. Such proofs are called **exhaustive proofs,** because these proofs exhaust all possibilities.

Note: An exhaustive proof is a special type of proof by cases where each case is a single particular case.

Example 10: Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

Solution: We use a proof by exhaustion. We need to check whether the inequality $(n+1)^3 \geq 3^n$ is true for $n = 1,2,3,4$.
For $n = 1$, we have $(n+1)^3 = 8 \geq 3^1 = 3^n$; for $n = 2$, we have $(n+1)^3 = 27 \geq 3^2 = 3^n$; finally for $n = 4$, we have $(n+1)^3 = 125 \geq 3^4 = 3^n$.
In each case the inequality is true. Thus, the result is true.

Note: We can carry out exhaustive proofs when it is necessary to check only a relatively small number of instances of a statement.

Predicate

Declarative sentences involving variables such as $x > 3$; $x = y + 3$; $x + y = z$ and *computer x is functioning properly* are often found in mathematical assertions, in computer programs and in system specifications. These are neither true nor false when the values of the variables are not specified.
The declarative sentence "*x is greater than 3*" has two parts. The first part, the variable x, is the subject of the sentence. The second part, "is greater than", is the property of the subject and it is called the **predicate**. That is, the part of a declarative sentence that attributes a property to the subject is called the **predicate**. We denote the sentence "x is greater than 3" by $P(x)$ where P denotes the predicate "is greater than 3" and x is the variable. $P(x)$ is also said to be the value of the **propositional function** $\boldsymbol{P}$ at x. Once a value is assigned to x, the $P(x)$ becomes a proposition and has a truth value.
A declarative sentence of the form $P(x_1, x_2, \ldots, x_n)$ is the value of the proposition function P at the n-tuple $(x_1, x_2, \ldots, x_n)$ and P is also called an ***n-ary predicate*** or ***n-place predicate***.
Propositional functions occur in computer programs.

Quantifiers

Quantification is a way to create a proposition from a proposition function and it expresses the extent to which a predicate is true over a range of elements. We deal with two types of quantification here: (i) *Universal quantification*, which says that a predicate is true for every element under consideration and (ii) *existential quantification*, which says that there is one or more elements under consideration for which the predicate is true. The area of logic that deals with predicates and quantifiers is called the **predicate calculus**.

The Universal quantifier: Many mathematical statements assert that a property is true for all values of a variable in a particular domain, called **domain of discourse** or **universe of discourse** or often just referred as the **domain**. The universal quantification of $P(x)$ for a particular domain is the proposition that asserts that $P(x)$ is true for all x in this domain.

The universal quantification of $P(x)$ is the statement "$P(x)$ *for all* x *in the domain*". The notation $\forall x\ P(x)$ (read as for all $x\ \ P(x)$) denotes universal quantification of $P(x)$. Here $\forall$ is called **universal quantifier**. An element for which $P(x)$ is false is called a **counter example**.

Example 11: Let $P(x): x + 1 > x$ and the domain is the set of real numbers. Since $P(x)$ is true for all real numbers x, the quantification is $\forall x\ P(x)$.

The existential quantifier: Many mathematical statements assert that there is an element with a certain property. Such statements are expressed using existential quantification .With existential quantification, we form a proposition that is true if and only if $P(x)$ is true for at least one value of x in the domain.

The *existential quantification* of $P(x)$ is the proposition "*There exists an element* x *in the domain such that* $P(x)$".The notation $\exists x\ P(x)$ (read as there exists $x\ P(x)$) is used for the existential quantification of $P(x)$. Here $\exists$ is called the **existential quantifier**.

Existence Proofs

Many theorems are assertions that elements of particular type exist. A theorem of this type is a proposition of the form $\exists x\, P(x)$, where P is a predicate. A proof of a proposition of the form $\exists x\, P(x)$ is called an **existence proof**.

There are two kinds of existence proofs :(i) **the constructive existence proof** and (ii) **nonconstructive existence proof**.

Constructive existence proof: In this method of proof we find an element a such that $P(a)$ is true.

Example 12: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Solution: All that we need is to produce an element a that has the required properties. After considerable trying we find that

$$a = 1729 \text{ , since } 1729 = 1^3 + 12^3 = 9^3 + 10^3$$

Thus, the assertion is shown.

Nonconstructive existence proof: In this method we do not find an element a such that $P(a)$ is true but rather prove that $\exists x\, P(x)$ is true in some other way.

A method of a nonconstructive existence proof is to use a proof by contradiction and that the negation of the existential quantification leads to a contradiction.

Example 13: Show that there exist irrational numbers x and y such that x^y is rational.

Solution: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ such that x^y is rational. On the other hand, if $\sqrt{2}^{\sqrt{2}}$ is irrational then we have irrational numbers $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ such that $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$, a rational number.

Note that we have not found irrational numbers x and y such that x^y is rational. Rather, we have shown that either the pair $x = \sqrt{2}, y = \sqrt{2}$ or the pair $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$ have the desired property, but we do not know which of these pairs works.

Counter Example

To show that a statement of the form $\forall x P(x)$ is false, we need to find a *counter example*, i.e., an example x for which $P(x)$ is false.

If statement of the form $\forall x P(x)$, resisted all proof attempts and we believe it to be false then we look for a counter example.

Example 14: Is the statement "Every positive integer is the sum of the squares of three integers" true ?

Solution: We try to find a counter example. We observe the following:

$1 = 0^2 + 0^2 + 1\,; \quad 2 = 0^2 + 1^2 + 1^2; \quad 3 = 1^2 + 1^2 + 1^2;$

$4 = 0^2 + 0^2 + 2^2\,; \quad 5 = 0^2 + 1^2 + 2^2\,; \quad 6 = 1^2 + 1^2 + 2^2;$

Can we write 7 as the sum of three squares? We note that the only possible squares not exceeding 7 are $0, 1$ and 4 and no three of which add up to 7. Thus 7 is a counter example. Therefore, the statement is false.

Conjectures and Open Problems

A **conjecture** is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence or the intuition (of an expert). When a proof of a conjecture is found, the conjecture becomes a theorem. Many conjectures are shown to be false.

Number theory is noted as a subject for which it is easy to formulate conjectures, some of which are disproved, some are difficult to prove and others have remained open problems for many years.

It would be useful to have a function $f(n)$ such that $f(n)$ is prime for all the integers n. If we had such a function, we could find large primes for use of cryptography and other applications.
Number theorists dream of finding formulas that generate prime numbers. One such formula was given as a conjecture by the Swiss mathematician Leonard Euler, but his conjecture was disproved. The following is his conjecture.

"The formula $E(n) = n^2 - n + 41$ generates a prime number for every positive integer n"

Example 15: Is the statement "The formula $E(n) = n^2 - n + 41$ generates a prime for every positive integer n" true ?

Solution: Notice that it yields a prime for $n = 1, 2, 3, 4, \dots, 40$ but for $n = 41$, we see that $E(41) = 41^2 - 41 + 41 = 41^2$ is not a prime. Therefore, 41 is a counter example and it disproves the claim.

Example 16: Fermat conjectured (in 1640) that numbers of the form $f(n) = 2^{2^n} + 1$ are prime numbers for all nonnegative integers n. Note that $f(0) = 3, f(1) = 5,\ f(2) = 17, f(3) = 257$ and $f(4) = 65,537$ are all primes. Euler established the falsity of Fermat's conjecture by producing a counter example. He showed that $f(5) = 2^{2^5} + 1 = 641 \times 67{,}00{,}417$, is a composite number.

Prime numbers of the form $2^{2^n} + 1$ are called ***Fermat primes***.

Many problems about primes still await ultimate resolution. A few of the most accessible and better known of these problems are given below:

Goldbach's Conjecture: The conjecture "Every even integer $n, n > 2$ is the sum of two primes" is known as Goldbach's conjecture.

We can check this conjecture for small even numbers. It was verified by hand calculations for numbers up to the millions prior to the advent of computers. The conjecture has been checked with computers for all even integers up to 2×10^{17} (This information is up to the year 2006).

Note: Although no proof of this conjecture has been found, most mathematicians believe it is true.

The Twin Prime Conjecture: Twin primes are primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19; $4{,}967$ and $4{,}969$ and so on. The twin prime conjecture asserts that: *there are infinitely many twin primes*. The world's record for twin primes, as early 2006, consists of the numbers

$$1{,}68{,}69{,}98{,}73{,}39{,}975 \times 2^{1{,}71{,}960} \pm 1$$

with $51{,}779$ digits.

Mathematical Induction

Mathematical induction is an important proof technique (method of proof) that can be used to prove theorems of the type $\forall n \ P(n)$, where P is a predicate and the domain of the predicate is the set of natural numbers. This method is used extensively to prove results about a large variety of discrete objects. (For example, it is used to prove results about the complexity of algorithms, the correctness of certain types of computer programs, theorems about graphs and trees, as well as a wide range of identities and inequalities).

In this section, we will describe how mathematical induction can be used and why it is a valid proof technique.

Note: Mathematical induction can be used only to prove results obtained in some other way. *It is not a tool for discovering formulae or theorems*.

Principle of Mathematical induction:

To prove that $P(n)$ is true for all natural numbers n, where $P(n)$ is a propositional function, we complete two steps.
Basis step: we verify that $P(1)$ is true.
Inductive step: We show that the conditional statement $P(k) \longrightarrow P(k+1)$ is true for any arbitrary natural number k.

The assumption that $P(k)$ is true is called the **inductive hypothesis**. To complete the inductive step we assume that $P(k)$ is true for an arbitrary natural number k and show that $P(k+1)$ is also true.

Note: Some times we need to show that $P(n)$ is true for $n = a, a+1, a+2, \ldots$ where a is an integer other than 1. We can use mathematical induction to accomplish this as long as we change the basis step: Verify that $P(a)$ is true.

Example 17: Use mathematical induction to show that

a) $\boldsymbol{1+2+3+\cdots+n = \frac{n(n+1)}{2}}$ **, for all natural numbers**
b) $\boldsymbol{1+3+5+\cdots+(2n-1) = n^2}$ **, for all natural numbers**
c) $\boldsymbol{1+2+2^2+\cdots+2^n = 2^{n+1}-1}$ **, for all non-negative integers**

Solution: *Left as exercise.*

Mathematical induction can be used to prove a variety of inequalities that hold for all natural numbers greater than a natural number.

Example 18: Use mathematical induction to prove that $\boldsymbol{2^n < n!}$ for every natural number $\boldsymbol{n}$ with $\boldsymbol{n \geq 4}$.

Solution: Let $P(n)$ be the proposition: $2^n < n!$. The domain of the propositional function is the set of natural numbers $n, n \geq 4$

Basis step: The basis step is $P(4)$.Note that $P(4)$ is true, since $2^4 = 16 < 24 = 4!$
Inductive step: We assume that $P(k)$ is true for the natural number k with $k \geq 4$. That is, $2^k < k!$ is true. Then

$$2^{k+1} = 2.2^k < 2.k! \text{ (by the inductive step)}$$

$$< (k+1).k! \text{ (since } 2 < k+1 \text{ when } k \geq 4)$$

$$= (k+1)!$$

Thus, $2^{k+1} < (k+1)!$. This shows that $P(k+1)$ is true when $P(k)$ is true. Therefore by the principle of mathematical induction $P(n)$ is true for all natural numbers n with $n \geq 4$. That is, $2^n < n!$ for all $n \in \boldsymbol{N}, n \geq 4$.

Mathematical induction can be used to the prove divisibility results about integers.

Example19: Use mathematical induction to prove that $n^3 - n$ is divisible by 3, when n is a natural number.

Solution: Let $P(n)$ be the proposition: $n^3 - n$ is divisible by 3. The domain of the propositional function is the set of natural numbers.
Basis step: Note that $1^3 - 1 = 0$ is divisible by 3. Therefore, $P(1)$ is true.
Inductive step: We assume that $P(k)$ is true. That is, $k^3 - k$ is divisible by 3.
Therefore, $k^3 - k = 3m$ for some natural number m. Then

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

$$= (k^3 - k) + 3(k^2 + k)$$

$$= 3m + 3(k^2 + k) \text{ (by inductive step)}$$

This shows that $(k+1)^3 - (k+1)$ is divisible by 3.Thus $P(k+1)$ is true when $P(k)$ is true.
By the principle of mathematical induction $P(n)$ is true for all natural numbers n.
That is, $n^3 - n$ is divisible by 3 whenever n is a natural number.

Mathematical induction can be used to prove many results about sets.

Example 20: The number of subsets of a finite set

Use mathematical induction to show that if S is a finite set with n elements where n is a non negative integer, then S has 2^n subsets.

Solution: Let $P(n)$ be the proposition: *A set with n elements has 2^n subsets*.
The domain of the propositional function is the set of nonnegative integers.
Basis step: $P(0)$ is true, since a set with no elements , $i.e.$, the empty set, has exactly $1 = 2^0$ subset (namely itself).
Inductive step: Assume that $P(k)$ is true for an arbitrary nonnegative integer k, $i.e.$, every set with k elements has 2^k subsets. Let T be a set with $k+1$ elements.
Then it is possible to write $T = S \cup \{a\}$, where a is one of the elements of T and $S = T - \{a\}$. Note that S has k elements and by induction hypothesis S has 2^k

subsets. The subsets of T can be obtained in the following way:
For each subset X of S there are exactly two subsets of T. They are X and $X \cup \{a\}$. These constitute all the subsets of T and they are all distinct. Since S has 2^k subsets of there are $2 \cdot 2^k = 2^{k+1}$ subsets of T, thus $P(k+1)$ is true when $P(k)$ is true. This proves the inductive step.

By the principle of mathematical induction $P(n)$ is true for all positive integers n. That is, a set with n elements has 2^n subsets, whenever n is a nonnegative integers n.

Validity of Mathematical Induction

The validity follows from an axiom, called **the well-ordering property**, for the set of natural numbers.
The well-ordering property*:* Every non empty subset of natural numbers has a least element.
Suppose that $P(1)$ is true and that the proposition $P(k) \longrightarrow P(k+1)$ is true for an arbitrary natural number k. To show that $P(n)$ is true for all natural numbers n , assume that there is atleast one natural number for which $P(n)$ is false. Let S be the set of all those natural numbers for which $P(n)$ is false. Clearly, S is non empty. By well-ordering property, S has a least element, say m. Note that $P(m)$ is false. Surely $m \neq 1$, since $P(1)$ is true. Therefore, $m > 1$ and $m-1$ is a natural number. Since $m - 1 < m, m-1$ is not in S. Therefore , $P(m-1)$ must be true. Since the conditional proposition $P(m-1) \longrightarrow P(m)$ is true, it follows that $P(m)$ is true. This contradicts the choice of m. Therefore, (by proof by contradiction) $P(n)$ is true for every natural number n.This shows that the mathematical induction is a valid method of proof.

P1:

Give a direct proof of the theorem: If m and n are both perfect squares, then mn is also a perfect square.

Solution:

We recall a definition: An integer a is a perfect square if there is an integer b such that $a = b^2$. To produce a direct proof, we first assume the hypothesis of the conditional statement is true. That is , m and n are perfect squares. Therefore by definition, there are integers s and t such that $m = s^2$ and $n = t^2$. Now $mn = (st)^2$. This shows that mn is also a perfect square.

P2:

Prove by a proof by contraposition that if $\boldsymbol{n = ab}$, where $\boldsymbol{a}$ and $\boldsymbol{b}$ are positive integers, then $\boldsymbol{a \leq \sqrt{n}}$ or $\boldsymbol{b \leq \sqrt{n}}$.

Solution:

We furnish a proof by contraposition. Assume that the conclusion of the conditional is false. That is, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ is false. Therefore, $a \leq \sqrt{n}$ is false and $b \leq \sqrt{n}$ is false. Thus, $a > \sqrt{n}$ and $b > \sqrt{n}$. From this it follows $ab > \sqrt{n} \cdot \sqrt{n} = n$. This shows that $n \neq ab$, which says that the hypothesis of the conditional is false. By the proof by contraposition the given conditional statement is true. Hence the result.

P3:

Prove by proof by contradiction that $\sqrt{2}$ is an irrational number.

Solution:

We prove it by a proof by contradiction. Let p be the proposition: $\sqrt{2}$ is a irrational number. To prove by the proof by contradiction, suppose that $\sim p$ is true. That is $\sqrt{2}$ is a rational number. We show that this leads to a contradiction. Thus, there exists integers a and b such that they have no common factors and $\sqrt{2} = \frac{a}{b}$ .Squaring both sides, it gives $2b^2 = a^2$. From this it follows that a^2 is even and there by a is even. Therefore, $a = 2c$ for some integer c. Thus $2b^2 = 4c^2$ and $b^2 = 2c^2$. From this it follows that b is even. This shows that a and b have common factor 2, a contradiction. Thus, the assumption $\sim p$ is true leads to a contradiction. Therefore, $\sim p$ is false and therefore p is true.

P4:

Using a proof by cases, show that $|xy| = |x||y|$, where x and y are real numbers.

Solution:

Let a be a real number. Recall that, $|a|$ denotes the absolute value of a and it is defined as

$$|a| = \begin{cases} a & if \quad a \geq 0 \\ -a & if \quad a < 0 \end{cases}$$

Since $|x|$ and $|y|$ occur in the formula to be proved, we consider the following four cases:

(i) x and y both non-negative, (ii) x is non-negative and y is negative,
(iii) x is negative and y is nonnegative, and (iv) x and y both negative.

Case (i) : If $x \geq 0$ and $y \geq 0$ then $xy \geq 0$. Therefore, $|xy| = xy = |x||y|$. The conclusion is true in this case.

Case (ii) : If $x \geq 0$ and $y < 0$ then $xy \leq 0$. Therefore,
$|xy| = -xy = x(-y) = |x||y|$. The conclusion is true in this case.

Case (iii) : If $x < 0$ and $y \geq 0$ then $xy \leq 0$. Therefore,
$|xy| = -xy = (-x)y = |x||y|$. The conclusion is true in this case.

Case (iv) : If $x < 0$ and $y < 0$ then $xy > 0$. Therefore
$|xy| = xy = (-x)(-y) = |x||y|$. The conclusion is true in this case also .
The result follows by the proof by cases.

P5:

Using a proof by exhaustion, show that there are no solutions in integers $\boldsymbol{x}$ and $\boldsymbol{y}$ of $\boldsymbol{x^2 + 3y^2 = 8}$.

Solution:

We can eliminate all but a few cases. An integer x is not a solution if $x^2 > 8$, $i.e.$, if $|x| \geq 3$ and an integer y is a solution if $3y^2 > 8$, $i.e.$, if $|y| \geq 2$. This leaves the case when x takes one of the values $-2, -1, 0, 1$, or 2 and y takes one of the values $-1, 0$, or 1 . For any of these values x^2 takes one of the values 0, 1, 4 and $3y^2$ takes one of the values 0,3. Note that the largest value for $x^2 + 3y^2$ is 7.Thus the equation $x^2 + 3y^2 = 8$ has no integer solutions for $x$and y.

P6:

Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

Solution:

To show that the statement is false, we look for a counter example, i.e., an integer which is not the sum of the squares of two integers. Note that the only perfect squares not exceeding 3 are $0^2 = 0,\ 1^2 = 1$ and their sum is at most 1. Thus, there is no way to express 3 as the sum of the squares of two integers. Therefore, the given statement is false.

P7:

Use mathematical induction to show that $2n^3 + 3n^2 + n$ is divisible by 6 for every natural number n.

Solution:

Let $P(n)$ be the proposition: $2n^3 + 3n^2 + n$ is divisible by 6.The domain of the propositional function is the set of natural numbers.

Basis step: $P(1)$ is true, since $2.1^3 + 3.1^2 + 1 = 6$, which is divisible by 6.
Inductive step: Assume that $P(k)$ is true for an arbitrary natural number k, i.e., assume that $2k^3 + 3k^2 + k$ is divisible by 6.Therefore $2k^3 + 3k^2 + k = 6m$ for some natural number m. Then

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

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

$$= 6m + 6(k^2 + 2k + 1) \quad \text{(By inductive hypothesis)}$$

$$= 6(m + k^2 + 2k + 1)$$

This shows that $P(k+1)$ is true when $P(k)$ is true. By the principle of mathematical induction, $P(n)$ is true for all natural number n, $i.e.$, $2n^3 + 3n^2 + n$ is divisible by 6 for every natural number n.

P8:

Use mathematical induction to prove the following generalization of De Morgan's law for propositions:

$$\boldsymbol{\sim(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \equiv \sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_n}$$

for all $\boldsymbol{n \in N,\ n \geq 2.}$

Solution:

Let $P(n)$ be the indentity for n proposition.The domain of the propositional function is the set of natural numbers $n,\ n \geq 2$.

Basis step:$P(2)$ is true, since $\sim(p_1 \wedge p_2) \equiv \sim p_1 \vee \sim p_2$ by De Morgan's law.

Inductive step: We assume that $P(k)$ is true for an arbitrary natural number $k, k \geq 2$. That is $\sim(p_1 \wedge p_2 \wedge \ldots \wedge p_k) \equiv \sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_k$.

Then,

$$\begin{aligned}\sim(p_1 \wedge p_2 \wedge \ldots \wedge p_k \wedge p_{k+1}) &\equiv \sim\big((p_1 \vee p_2 \vee \ldots \vee p_k) \wedge p_{k+1}\big) \\ &\equiv \sim(p_1 \wedge p_2 \wedge \ldots \wedge p_k) \vee \sim p_{k+1} \\ &\equiv (\sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_k) \vee \sim p_{k+1} \\ &\equiv \sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_k \vee \sim p_{k+1}\end{aligned}$$

This, shows that $P(k+1)$ is true when $P(k)$ is true. By the principle of mathematical induction $P(n)$ is true for all $n \in \boldsymbol{N}$, $n \geq 2$. That is

$\sim(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \equiv \sim p_1 \vee \sim p_2 \vee \ldots \vee \sim p_n$, for all $n \in \boldsymbol{N}$, $n \geq 2$.

1.7. Methods of Proof

Exercise:

1. Prove by direct proof that, if an integer a is such that $a-2$ is divisible by 3, then a^2-1 is divisible by 3.

2. Prove by proof by contraposition that for any non-negative integers x, y, if $\sqrt{xy} \neq \frac{(x+y)}{2}$, then $x \neq y$.
3. Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.
4. Show that if n is an integer and n^3+5 is odd, then n is even ,using
   a. A proof by contraposition b. A proof by contradiction.

5. Use a proof by contradiction to show that there is no rational number r for which $r^3+r+1=0$. [Hint: Assume that $r=a/b$ is a root, where a and b are integers and a/b is in lowest terms. Obtain an equation involving integers by multiplying by b^3. Then look at whether a and b are each odd or even.]

6. Show that these statements about the integer x are equivalent:
   (a) $3x+2$ is even,(b) $x+5$ is odd, (c) x^2 is even.

7. Use the mathematical induction to prove that
$$1^2+3^2+5^2+\cdots+(2n+1)^2=\frac{(n+1)(2n+1)(2n+3)}{3}$$
   whenever n is a nonnegative integer.
8. Use the mathematical induction to prove that for every positive integer n,
$$1\cdot 2+2\cdot 3+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}$$
9. Prove that 5 divides n^5-n whenever n is a nonnegative integer.
10. Prove that if $A_1, A_2, \dots A_n$ are subsets of a universal set U, then
$$\left(\bigcup_{k=1}^{n} A_k\right)' = \bigcap_{k=1}^{n} (A_k)'$$
    Where A' denotes the complement of the set A

UNIT-3

SETS RELATIONS AND FUNCTIONS

MODULE-1

SETS

Unit-2 SETS AND RELATIONS

2.1

SETS

In this unit we study the fundamental discrete structure on which all other discrete structures are built, namely, *the set*. The following are some discrete structures built from sets: *combinations*, *unordered collection of objects used extensively in counting*; *relations*, *sets of ordered pairs that represent relationships between objects*; *graphs*, sets *of vertices and edges that connect vertices*; *finite state machines*, *used to model computing machines*.

The concept of a set is fundamental and it unifies mathematics. It has revolutionized mathematical thinking and it enables us to express ourselves in clear and concise terms.
The foundation of set theory was laid by the eminent German mathematician *Georg Cantor* (1845-1918).
An axiomatic approach of development of the set theory and questions of a philosophical nature are avoided. The presentation is informal, formal proofs are indicated which use the notation and the rules of inference of the predicate calculus.
Set: A ***set*** is a well-defined collection of objects. The objects of a set are called ***elements*** or ***members*** of a set. A collection (of objects) is well-defined if there is no ambiguity in determining whether or not a given object (what so ever) belongs to the collection.
Sets are denoted by capital letters and their elements by lowercase letters. If an object x is an element of a set A, then we write $x \in A$; otherwise $x \notin A$.

There are two methods of defining sets
Listing method: A set can sometimes be described by listing its elements within braces.
Example 1: The set V of all Vowels in the English alphabet is given by
$\boldsymbol{V = \{a, e, i, o, u\}}$

A set with a large number of elements that follow a definite pattern often described using ellipses (…) by listing a few elements at the beginning. For example, the set O of odd positive integers can be listed as $\{1,3,5, \dots, \dots\}$.

Set builder notation: Another way of describing a set by using the set builder notation. We characterize all those elements in the set by stating the property or properties they must have to be members.

Example 2: Let M be the set of all months of the year with exactly 30 days. Then $\boldsymbol{M}$ in set builder notation is

$$M = \{x|x \text{ is a month of the year with exactly 30 days}\}$$

Also, M in the listing method is

$$M = \{\text{April}, \text{June}, \text{September}, \text{November}\}$$

The following sets, each denoted by a bold faced letter, play an important role in discrete mathematics;

$\boldsymbol{N} = \{1,2,3, \dots, \dots\}$, the set of ***natural numbers***

$\boldsymbol{Z} = \{\dots, \dots, -2, -1,0,1,2, \dots, \dots\}$, the set of ***integers***

$\boldsymbol{Q} = \left\{\frac{p}{q} |p, q \in \boldsymbol{Z}, q \neq 0\right\}$, the set of ***rational numbers***

$\boldsymbol{R}$: The set of ***real number***

In general a set can be defined or characterized by a predicate .If $P(x)$ is the predicate then $\{x|P(x)\}$ defines a set. An element a belongs to the set $\{x|P(x)\}$ if $P(a)$ is true; otherwise a does not belongs to the set. This statement is written symbolically as

$$\forall y(P(y) \Leftrightarrow y \in \{x|P(x)\})$$

If $A = \{x|P(x)\}$, then the set A is called an ***extension* of $(\boldsymbol{x})$** , (and A is said to be specified by the predicate $P(x)$) and $\forall y(y \in A \Leftrightarrow y \in \{x|x \in A\})$

Let $P(x)$ and $Q(x)$ be any two predicates defined over a common universe of discourse denoted by U. If for every assignment of values to x from U, the resulting propositions have the same truth values, then the predicates $P(x)$ and $Q(x)$ are said to be ***equivalent to each other over E***. Then we write $P(x) \Leftrightarrow Q(x)$. The definition of the (tautological) implication can be extended in the same way.

All the implications and equivalences of the propositional calculus given in module 1.3 can be considered as implications and equivalences of the predicate calculus.

Throughout this module the proofs of set identities are established using the implications and equivalences of predicate calculus, assuming that sets are specified by predicates.

Equality of sets: Two sets A and B are ***equal*** (***extensionally equal***, written $A = B$) if they have the same elements. That is, $A = B$ if and only if $\forall x(x \in A \leftrightarrow x \in B)$.

Let the sets A and B be extensions of the predicates $P(x)$ and $Q(x)$ respectively. If $P(x) \Leftrightarrow Q(x)$, then $A = B$, that is if two predicates are equivalent then they have the same extension and the two sets specified by equivalent predicates are equal. *This is the analogy between the equality of sets and the equivalence of predicates*.

Note:

1. The sets $\{1,3,5\}, \{3,5,1\}$ and $\{1,3,3,5,1,5,5,5\}$ are all equal, because they have the same elements.
2. The order in which the elements of a set are listed does not matter and also it does not matter if an element of set is listed more than once.

There are two special sets, one of which includes every set *under discussion* while the other is included in every set *under discussion*.

Universal set: It is always possible to choose a special set U such that every set under discussion is a subset of U. Such a set is called a **Universal set**. Thus, $A \subseteq U$ for every set A.That is, every element $x \in U$, $i.e.$, $\forall\, x\ (x \in U)$ is identically true.

Further, U can be specified as $U = \{x | P(x) \lor \sim P(x)\}$, where $P(x)$ is any predicate.

Empty set: The set containing no elements is called an **empty set** or **null set** and is denoted by ϕ.
It follows from the definition of an empty set $\emptyset$, for any $x, x \in \emptyset$ is a contradiction, $i.e.$, $\forall x(x \in \emptyset)$ is a contradiction.
Further, $\emptyset$ can be specified as $\emptyset = \{x | P(x) \land \sim P(x)\}$ where $P(x)$ is any predicate. It is easy to see that, all such sets are equal to $\emptyset$. This shows that there is a unique empty set.

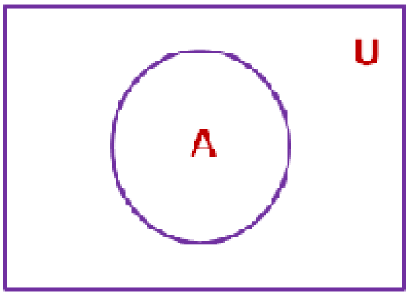
Example 3: The set of all positive integers that are greater than their squares is the empty set.

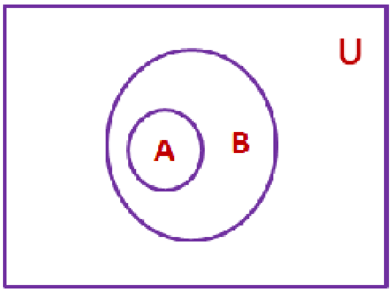
A set with one element is called a **singleton set.**

Subset: Let A and B be sets. The set A is said to be a **subset** of B
or A *is* **included** in B (written as $A \subseteq B$ and called as **inclusion**) if and only if every element of A is also an element of B.
We see that $A \subseteq B$ if and only if the quantification $\forall x(x \in A \longrightarrow x \in B)$ is true.

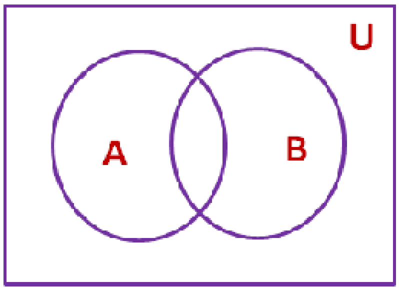
Venn diagrams: Sets and relationships between sets can be represented graphically using Venn diagrams, named after the English mathematician *John Venn* (1845 – 1918).

In Venn diagrams the universal set U which contains all the objects under consideration is represented by a rectangle. (Note that the universal set varies depending on the context).Inside this rectangle, circles (or other closed geometrical figures) are used to represent sets.





$A \subseteq B$



A and B may have common elements

Theorem 1: For every set $\boldsymbol{S}$,

$$\text{(i) } \boldsymbol{\phi \subseteq S} \;\; \textbf{and} \;\; \textbf{(ii) } \boldsymbol{S \subseteq S}$$

Proof: Let S be a set.

(i) To show that $\phi \subseteq S$, we must show that $\forall x(x \in \phi \longrightarrow x \in S)$ is true. Since ϕ has no elements, $x \in \phi$ is always false. Recall that a conditional with a false hypothesis is guaranteed to be true. Therefore, $\forall x(x \in \phi \longrightarrow x \in S)$ is true. Thus, $\phi \subseteq S$, i.e., ***empty set is a subset of every set.***

Note: This is an example of a vacuous proof.

(ii) Note that $\forall x(x \in S \longrightarrow x \in S)$ is true. Therefore, $S \subseteq S$, i.e., ***every set is a subset of itself.***

Theorem 2: For any sets $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$, $(\boldsymbol{A \subseteq B}) \wedge (\boldsymbol{B \subseteq C}) \Longrightarrow (\boldsymbol{A \subseteq C})$

Proof: We have,

$(A \subseteq B) \wedge (B \subseteq C)$ if and only if $\forall x(x \in A \longrightarrow x \in B) \wedge \forall x(x \in B \longrightarrow x \in C)$

We now use the following (tautological) implication of the predicate calculus

$\forall x(x \in A \longrightarrow x \in B) \wedge \forall x(x \in B \longrightarrow x \in C) \Longrightarrow \forall x(x \in A \longrightarrow x \in C)$

(by hypothetical syllogism) ,Thus, $(A \subseteq B) \wedge (B \subseteq C) \Longrightarrow (A \subseteq C)$

Note: The set inclusion is reflexive and transitive

Theorem 3: For any sets $\boldsymbol{A}$ and $\boldsymbol{B}$, $\boldsymbol{A} = \boldsymbol{B} \Leftrightarrow \big((\boldsymbol{A} \subseteq \boldsymbol{B}\,) \wedge (\boldsymbol{B} \subseteq \boldsymbol{A})\big)$

Proof: Let A and B be sets specified by the predicates $P(x)$ and $Q(x)$ respectively. We have the equivalence from the predicate calculus

$$\forall x\big((P(x) \longrightarrow Q(x)) \wedge (Q(x) \longrightarrow P(x))\big) \Leftrightarrow \forall x(P(x) \leftrightarrow Q(x))$$

Therefore

$$A = B \Leftrightarrow \forall x(x \in A \leftrightarrow x \in B) \Leftrightarrow \forall x\big((x \in A \longrightarrow x \in B) \wedge (x \in B \longrightarrow x \in A)\big)$$

$$\Leftrightarrow \big((A \subseteq B\,) \wedge (B \subseteq A)\big)$$

Proper subset: Let A and B be sets. The set A is said to be a **proper subset** of B, written as $A \subset B$ if $A \subseteq B$ and there must exist an element x of B that is not an element of A. That is, $A \subset B$ iff $\forall x(x \in A \to x \in B) \wedge \exists x(x \in B \wedge\ x \notin A)$ is true. $A \subset B$ is also called a **proper inclusion**.

Note: A proper inclusion is not reflexive; however, it is transitive, $i.e.$,

$$(A \subset B) \wedge (B \subset C) \Longrightarrow (A \subset C)$$

Cardinality of a set: Let S be a set. If there are exactly n distinct elements in S, where n is a nonnegative integer, then we say that S is a ***finite*** **set** and that n is the *cardinality* of S. The cardinality is denoted by $|\boldsymbol{S}|$ or $\boldsymbol{n}(\boldsymbol{S})$ or $\boldsymbol{k}(\boldsymbol{S})$

A set is said to be ***infinite*** if it is not finite.

Example 4: If $\boldsymbol{S}$ is the set of letters in the English alphabet, then $\boldsymbol{S}$ in finite and $|\boldsymbol{S}| = \boldsymbol{26}$.

Note that $|\emptyset| = 0$.

The power set: Given a set S, the power set of S is the set of all subsets of the set S. The power set of S is denoted by $\boldsymbol{P}(\boldsymbol{S})$ or $\boldsymbol{2^{s}}$.

The following theorem is well known and its proof is already given under mathematical induction.

Theorem 4: If S is a finite set with n element, then its power set $P(S)$ has 2^n elements.

Note: $P(\emptyset) = \{\emptyset\}$, $P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

$$P\left(P(P(\emptyset))\right) = \left\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\right\}$$

Indexed set: Let $\boldsymbol{I} = \{i_1, i_2, i_3, \dots, \dots\}$. If A be a family of sets $A = \{A_{i_1}, A_{i_2}, A_{i_3}, \dots, \dots\}$ such that for any $i_j \in \boldsymbol{I}$ there exists a set $A_{i_j} \in A$ and $A_{i_j} = A_{i_k}$ iff $i_j = i_k$ then A is called ***indexed set, $\boldsymbol{I}$*** is the ***index set*** and any subscript i_j in A_{i_j} is called an ***index***.

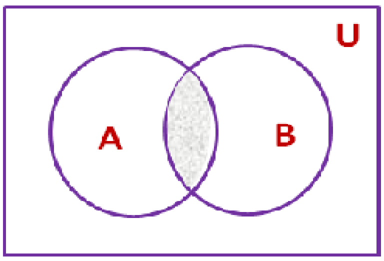
An indexed family of sets can also be written as $A = \{A_i\}_{i \in \boldsymbol{I}}$

Set Operations

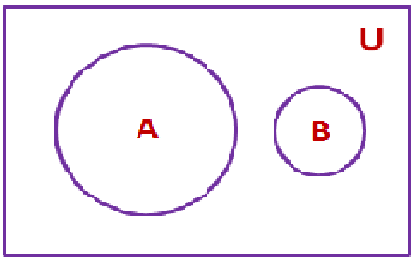
Sets can be combined in several ways to get new sets. Note that we find a close relationship between logic operations and set operations.

Intersection: Let A and B be sets. The *intersection* of the sets A and B, denoted by $\boldsymbol{A} \cap \boldsymbol{B}$, is the set containing elements in both A and B. That is,

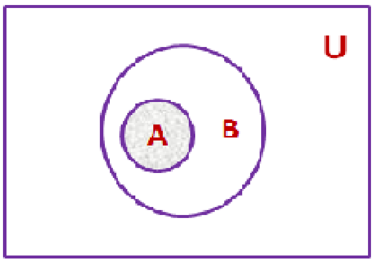
$$\boldsymbol{A} \cap \boldsymbol{B} = \{\boldsymbol{x} | \boldsymbol{x} \in \boldsymbol{A} \wedge \boldsymbol{x} \in \boldsymbol{B}\}$$



$A \cap B$



$A \cap B = \emptyset$



$A \cap B = A$

Note: It is easy to see that $A \cap B \subseteq A$ and $A \cap B \subseteq B$

Theorem 5: For any sets $\boldsymbol{A}$,$\boldsymbol{B}$ and $\boldsymbol{C}$

i) $\boldsymbol{A \cap B = B \cap A}$

ii) $\boldsymbol{A \cap A = A}$

iii) $\boldsymbol{A \cap \emptyset = \emptyset}$

iv) $\boldsymbol{A \cap (B \cap C) = (A \cap B) \cap C}$

Proof:

(i) $A \cap B = \{x |\ x \in A \wedge x \in B\}$

$= \{x |\ x \in B \wedge x \in A\}$ (by the commutativity of the predicate calculus)

$= B \cap A$

(ii) $A \cap A = \{x |\ x \in A \wedge x \in A\} = \{x |\ x \in A\} = A$

(iii) $A \cap \emptyset = \{x |\ x \in A \wedge x \in \emptyset\} = \{x |\ x \in \emptyset\} = \emptyset \qquad (\because\ p \wedge F_0 = F_0)$

(iv) $A \cap (B \cap C) = \{x |\ x \in A \wedge x \in (B \cap C)\}$

$= \{x |\ x \in A \wedge (x \in B \wedge x \in C)\}$

$= \{x |\ (x \in A \wedge x \in B) \wedge x \in C\}$

(by the associativity for the predicate calculus)

$= \{x |\ x \in (A \cap B) \wedge x \in C\}$

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

this completes the proof of the theorem.

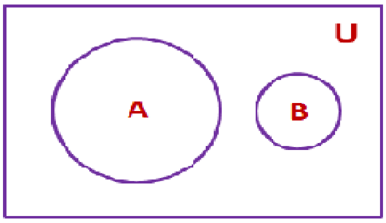
For any indexed set $A = \{A_i\}_{i \in \boldsymbol{I}}$

$$\bigcap_{i \in \boldsymbol{I}} A_i = \{x |\ x \in A_i \ for\ all\ i \in \boldsymbol{I}\ \}$$

For $\boldsymbol{I} = \boldsymbol{I_n} = \{1, 2, 3, \dots, n\}$, we write

$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i = \bigcap_{i \in \boldsymbol{I_n}} A_i$$

Disjoint sets: Two sets are said to be *disjoint* if and only if their intersection is the empty set. That is, two sets A and B are disjoint iff $A \cap B = \emptyset$



Disjoint Sets

A collection of sets is called a ***disjoint collection*** if every pair of sets in the collection are disjoint .The sets in a disjoint collection are said to be ***mutually disjoint***.

Let $A = \{A_i\}_{i \in \boldsymbol{I}}$ be an indexed set. The set A is a disjoint collection iff $A_i \cap A_j = \emptyset$ for $i, j \in \boldsymbol{I}, i \neq j$.

Example 5: Show that $\boldsymbol{A \subseteq B}$ iff $\boldsymbol{A \cap B = A}$

Solution: We have $A \subseteq B$ iff $\forall x(x \in A \longrightarrow x \in B)$

Note that for any x $(x \in A \longrightarrow x \in B) \equiv (x \in A \land x \in B) \leftrightarrow x \in A$

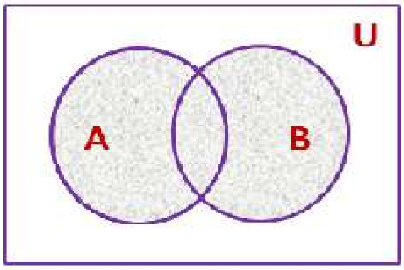
This follows from the equivalence $p \longrightarrow q \equiv ((p \land q) \leftrightarrow p)$ (verify!)

Thus, $A \subseteq B$ iff $\forall x\ ((x \in A \land x \in B) \leftrightarrow x \in A)$

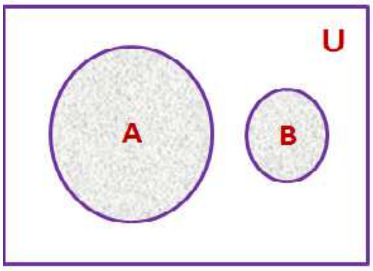
i.e., $A \subseteq B$ iff $A \cap B = A$

Union: Let A and B be sets. The *union* of the sets A and B is denoted by $\boldsymbol{A \cup B}$, is the set that contains those elements that are either in$A$ or in B or in both. That is,

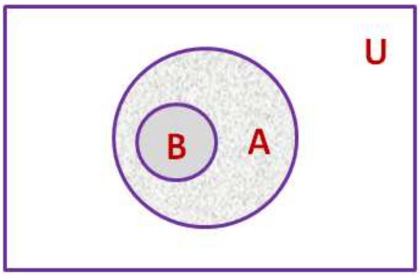
$$\boldsymbol{A \cup B = \{x \mid x \in A \lor x \in B\}}$$



$\boldsymbol{A} \cup \boldsymbol{B}$



$\boldsymbol{A} \cup \boldsymbol{B}$, where A and B are disjoint



$A \cup B = B$

Theorem 6: For any sets $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$

- **i)** $\boldsymbol{A} \cup \boldsymbol{B} = \boldsymbol{B} \cup \boldsymbol{A}$
- **ii)** $\boldsymbol{A} \cup \emptyset = \boldsymbol{A}$
- **iii)** $\boldsymbol{A} \cup \boldsymbol{A} = \boldsymbol{A}$
- **iv)** $\boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C}) = (\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C}$

Proof: Let A, B and C be any sets

i) $A \cup B = \{x |\ x \in A \vee x \in B\}$

$= \{x |\ x \in B \vee x \in A\}$ (by the commutativity of the predicate calculus)

$= B \cup A$

ii) $A \cup \emptyset = \{x |\ x \in A \vee x \in \emptyset\} = \{x |\ x \in A \vee F_0\} = \{x |\ x \in A\} = A$

iii) $A \cup A = \{x |\ x \in A \vee x \in A\}$

$= \{x |\ x \in A\}$ (by the idempotent law of the predicate calculus)

$= A$

iv) $A \cup (B \cup C) = \{x |\ x \in A \vee x \in (B \cup C)\} = \{x |\ x \in A \vee (x \in B \vee x \in C)\}$

$= \{x |\ (x \in A \vee x \in B) \vee x \in C\}$

(by the associativity of the predicate calculus)

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

Thus the theorem is proved

For any indexed set $A = \{A_i\}_{i\in \boldsymbol{I}}$

$$\bigcup_{i\in \boldsymbol{I}} A_i = \{x|\ x \in A_i\ for\ at\ least\ one\ i \in \boldsymbol{I}\ \}$$

For $\boldsymbol{I} = \boldsymbol{I_n} = \{1, 2, 3, \dots, n\}$, we write

$$A_1 \cup A_2 \cup \dots \cup A_n = \bigcup_{i=1}^{n} A_i = \bigcup_{i\in \boldsymbol{I_n}} A_i$$

Theorem 7: Distributive laws:

For any sets $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$

i) $\boldsymbol{A} \cap (\boldsymbol{B} \cup \boldsymbol{C}) = (\boldsymbol{A} \cap \boldsymbol{B}) \cup (\boldsymbol{A} \cap \boldsymbol{C})$

ii) $\boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C}) = (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$

Proof:

$A \cap (B \cup C) = \{x|\ x \in A \wedge x \in (B \cup C)\}$

$= x|x \in A \wedge (x \in B\ \vee x \in C)$

$= \{x|(x \in A\ \wedge x \in B) \vee (x\ \in A\ \wedge x \in C)\}$

(By distributivity of the predicate calculus)

$= \{x|x \in (A \cap B) \vee x \in (A \cap C)\}$

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

The other distributive law can be proved on similar lines.

Let A be a family of indexed set over an index set I such that

$$A = \{A_1, A_2, A_3, \dots, \dots\} = \{A_i\}_{i\in I}$$

The associative laws and distributive laws can be generalized in the following way

$$B \cup \left(\bigcap_{i\in I} A_i\right) = \bigcap_{i\in I} (B \cup A_i)$$

$$B \cap \left(\bigcup_{i \in I} A_i\right) = \bigcup_{i \in I} (B \cap A_i)$$

The above identities can be proved by the mathematical induction.

Theorem 8: Absorption laws: For any sets A and B

i) $\boldsymbol{A \cup (A \cap B) = A}$
ii) $\boldsymbol{A \cap (A \cup B) = A}$

Proof:

$A \cup (A \cap B) = (A \cup A) \cap (A \cup B)$ (by distributive law)

$= A \cap (A \cup B)$ (by idempotent law)

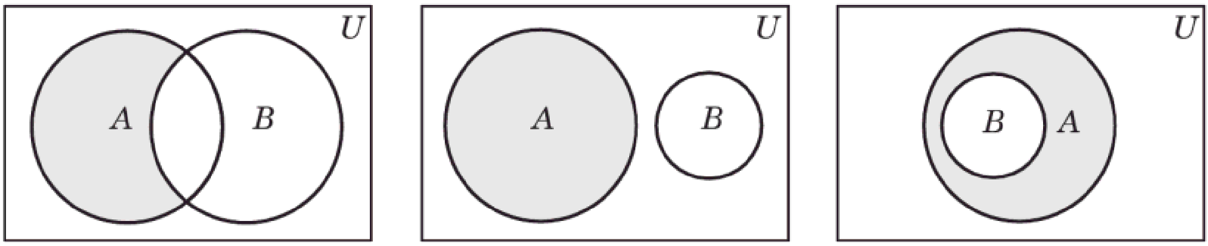
Now, $A \cup (A \cap B) = \{x | \, x \in A \vee (x \in A \wedge x \in B)\}$

$= \{x | \, x \in A\}$ (by absorption law of the predicate calculus)

Thus, $A \cap (A \cup B) = A \cup (A \cap B) = A$

Difference of two sets: Let A and B sets. The ***difference*** of A and B is denoted by $\boldsymbol{A - B}$, is the set containing those elements that are in A but not in B. The difference of $A$and B is also called the ***complement of B with respect to A***.That is,

$$\boldsymbol{A - B = \{x | x \in A \wedge x \notin B\} = \{x | x \in A \wedge \sim(x \in B)\}}$$

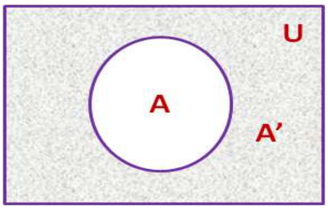


$A - B$ $\quad$ $A - B = A$ $\quad$ $A - B$

Note: It is easy to see that $A - B \subseteq A$

Complement of a set: Let U be the universal set. The ***complement*** of the set A is denoted by $'$, is the complement of A with respect to U, $i.e.$,

$$\boldsymbol{A' = U - A = \{x | x \in U \wedge x \notin A\} = \{x | x \notin A\} = \{x | \sim(x \in A)\}}.$$



Theorem 9: For any set A

i) $(A')' = A$
ii) $A \cup A' = U$
iii) $A \cap A' = \emptyset$
iv) $\emptyset' = U$ and
v) $U' = \emptyset$

Proof:

i) $(A')' = \{x \mid \sim(x \in A')\} = \{x \mid \sim(\sim(x \in A))\}$

$= \{x \mid x \in A\}$ (by double negation law of the predicate calculus)

$= A$

ii) $A \cup A' = \{x \mid x \in A \vee x \in A'\} = \{x \mid x \in A \vee \sim(x \in A)\} = U$
iii) $A \cap A' = \{x \mid x \in A \wedge x \in A'\} = \{x \mid x \in A \wedge \sim(x \in A)\} = \emptyset$
iv) $\emptyset' = \{x \mid \sim(x \in \emptyset)\} = \{x \mid x \in U\} = U$
v) $U' = (\emptyset')' = \emptyset$ (by (i))

Example 6: Show that (i) $A - B = A \cap B'$ (ii) $A \subseteq B$ iff $\sim B \subseteq \sim A$

Solution:

i) $A - B = \{x \mid x \in A \wedge x \notin B\} = \{x \mid x \in A \wedge x \in B'\} = A \cap B'$
ii) $A \subseteq B$ iff $\forall x(x \in A \longrightarrow x \in B) \equiv \forall x(\sim(x \in B) \longrightarrow \sim(x \in A))$
(the conditional and its contrapositive are equivalent)

$\equiv \forall x(x \in B' \longrightarrow x \in A')$ iff $B' \subseteq A'$

Thus $A \subseteq B$ iff $B' \subseteq A'$

Theorem 10: De Morgan's laws: For any sets $\boldsymbol{A}$ and $\boldsymbol{B}$

$$\textbf{(i)}\ (\boldsymbol{A} \cap \boldsymbol{B})' = \boldsymbol{A}' \cup \boldsymbol{B}' \qquad\qquad \textbf{(ii)}\ (\boldsymbol{A} \cup \boldsymbol{B})' = \boldsymbol{A}' \cap \boldsymbol{B}'$$

Proof:

i) $(A \cap B)' = \{x \mid x \notin (A \cap B)\}$

$= \{x \mid \sim(x \in (A \cap B))\}$

$= \{x \mid \sim(x \in A \wedge x \in B)\}$

$= \{x \mid \sim(x \in A) \vee \sim(x \in B)\}$

(by De Morgan's law of the predicate calculus)

$= \{x \mid x \in A' \vee x \in B'\}$

$= A' \cup B'$

ii) $(A \cup B)' = \{x \mid x \notin (A \cup B)\}$

$= \{x \mid \sim(x \in (A \cup B))\}$

$= \{x \mid \sim(x \in A \vee x \in B)\}$

$= \{x \mid \sim(x \in A) \wedge \sim(x \in B)\}$

(by De Morgan's law for of the predicate calculus)

$= \{x \mid x \in A' \wedge x \in B'\}$

$= A' \cap B'$

Symmetric Difference: Let A and B be two sets. The ***symmetric difference*** (or) ***Boolean sum*** of A and B is the set, denoted by $\boldsymbol{A \oplus B}$, and it is defined by

$$\boldsymbol{A \oplus B = (A - B) \cup (B - A)}$$

Note: $\boldsymbol{A \oplus B = (A - B) \cup (B - A) = (A \cap B') \cup (A' \cap B)}$

Theorem 11: For any sets $\boldsymbol{A}$, $\boldsymbol{B}$ and $\boldsymbol{C}$

i) $A \oplus B = B \oplus A$ ($\oplus$ is commutative)

ii) $A \oplus \emptyset = A$

iii) $A \oplus A = \emptyset$

iv) $A \oplus (B \oplus C) = (A \oplus B) \oplus C$ ($\oplus$ is associative)

Example 7: Show that $(\boldsymbol{A} \oplus \boldsymbol{B}) = (\boldsymbol{A} \cup \boldsymbol{B}) - (\boldsymbol{A} \cap \boldsymbol{B})$

Solution: We have $(A \oplus B) = (A' \cap B) \cup (A \cap B')$

Now $(A \cup B) - (A \cap B) = (A \cup B) \cap (A \cap B)'$

$= (A \cup B) \cap (A' \cup B')$ (Demorgan's law)

$= (A \cap A') \cup (A \cap B') \cup (B \cap A') \cup (B \cap B')$(Distributive law)

$= (A \cap B') \cup (B \cap A') = (A - B) \cup (B - A) = (A \oplus B)$

Thus, $A \oplus B = (A \cup B) - (A \cap B)$

Therefore, $\boldsymbol{A} \oplus \boldsymbol{B} = (\boldsymbol{A} - \boldsymbol{B}) \cup (\boldsymbol{B} - \boldsymbol{A}) = (\boldsymbol{A} \cup \boldsymbol{B}) - (\boldsymbol{A} \cap \boldsymbol{B})$

Set Identities

If A and B are extensions of the predicates $P(x)$ and $Q(x)$ respectively in a universal set U, then $A \cup B$ and $A \cap B$ are the extensions of $P(x) \vee Q(x)$ and $P(x) \wedge Q(x)$ respectively. Similarly A' is the extension of $\sim P(x)$. The extension of $P(x) \longrightarrow Q(x)$ and $P(x) \leftrightarrow Q(x)$ are respectively $A \cup B'$and $(A' \cup B) \cap (A \cup B')$. Thus, the new sets formed from the sets A and B can be interpreted in terms of extensions of formulas containing $P(x)$ and $Q(x)$.

The identities of set theory follow from the corresponding equivalences of predicate formulas. Also the inclusion of sets follows from the corresponding implications of predicates.
If we replace predicates by their extensions, $\wedge$ by $\cap$, $\vee$ by $\cup$ and $\sim$ by $'$ in any predicate formula then we obtain corresponding formulas of set theory. Also the equivalences and implications are replaced by equality and inclusion of sets. This technique has often been used to prove the identities other relations of set theory so far.
Some of the basic identities describe certain properties of the operations involved and are given special names. These properties describe an algebra called **set algebra** (or **algebra of sets**).We note that the propositional algebra and set algebra are particular cases of an abstract algebra called a **Boolean Algebra.**

This fact also explains the similarities between the operators in the propositional calculus and the operations of set theory.

For all identities listed in this module, the corresponding equivalences from the propositional calculus are also listed. Similar equivalences hold for the predicate calculus

Set algebra	Propositional algebra	Laws
$A \cup A = A; A \cap A = A$	$p \vee p \equiv p \quad ; p \wedge p \equiv p$	Idempotent laws
$A \cup B = B \cup A; A \cap B = B \cap A$	$p \vee q \equiv q \vee p \ ; p \wedge q \equiv q \wedge p$	Commutative laws
$A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$	$p \wedge (p \vee q) \equiv p$; $p \vee (p \wedge q) \equiv p$	Absorption laws
$(A')' = A$	$\sim(\sim p) \equiv p$	Double negation law
$(A \cup B)' = A' \cap B'$ $(A \cap B)' = A' \cup B'$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$; $\sim(p \wedge q) \equiv \sim p \vee \sim q$	De Morgan's laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	Associative laws
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	Distributive laws
$A \cap U = A; A \cup \emptyset = A$	$p \wedge T_0 \equiv p \quad ; \quad p \vee F_0 \equiv p$	Identity laws
$A \cup U = U; A \cap \emptyset = \emptyset$	$p \vee T_0 \equiv T_0 \quad ; \quad p \wedge F_0 \equiv F_0$	Domination laws
$A \cup A' = U; A \cap A' = \emptyset$	$p \vee \sim p \equiv T_0 \quad ; \ p \wedge \sim p \equiv F_0$	Inverse laws

All the identities given above are presented in pairs except the double negation law. This pairing is done because a **principle of duality**, similar to the one given for propositional calculus also holds in the case of set algebra.(In fact the principle of duality holds in Boolean Algebra).Given any identity in the set algebra, one can obtain its *dual* $i.e.$, another identity by interchanging $\cup$ with $\cap$ and U with $\emptyset$.

P1:

Prove or disprove: For any sets $\boldsymbol{A}, \boldsymbol{B} \subseteq \boldsymbol{U}$

(i) $\boldsymbol{P}(\boldsymbol{A} \cup \boldsymbol{B}) = \boldsymbol{P}(\boldsymbol{A}) \cup \boldsymbol{P}(\boldsymbol{B})$

(ii) $\boldsymbol{P}(\boldsymbol{A} \cap \boldsymbol{B}) = \boldsymbol{P}(\boldsymbol{A}) \cap \boldsymbol{P}(\boldsymbol{B})$

Solution:

(i) Let $A = \{1\}$, $B = \{2\}$

Therefore $A \cup B = \{1,2\}$, now $\{1,2\} \in P(A \cup B)$

Note that $P(A) \cup P(B) = \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}$

and $\{1,2\} \notin P(A) \cup P(B)$

hence $P(A \cup B) \neq P(A) \cup P(B)$

(ii) $X \in P(A \cap B) \Leftrightarrow X \subseteq A \cap B$

$\Leftrightarrow X \subseteq A$ and $X \subseteq B$

$\Leftrightarrow X \in P(A)$ and $X \in P(B)$

$\Leftrightarrow X \in P(A) \cap P(B)$

Therefore $P(A \cap B) = P(A) \cap P(B)$

P2:

Show that for any sets $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ and $\boldsymbol{D}$

$$(\boldsymbol{A} \cap \boldsymbol{B}) \cup \big(\boldsymbol{B} \cap \big((\boldsymbol{C} \cap \boldsymbol{D}) \cup (\boldsymbol{C} \cap \boldsymbol{D}')\big)\big) = \boldsymbol{B} \cap (\boldsymbol{A} \cup \boldsymbol{C})$$

Solution: $(A \cap B) \cup \big(B \cap \big((C \cap D) \cup (C \cap D')\big)\big)$

$= (A \cap B) \cup \big(B \cap \big(C \cap (D \cup D')\big)\big)$ (Distributive law)

$= (A \cap B) \cup \big(B \cap (C \cap U)\big)$

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

$= (B \cap A) \cup (B \cap C)$ (Commutative law)

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

P3:

Show that for any sets $\boldsymbol{A}$ and $\boldsymbol{B}$, $\boldsymbol{A} - (\boldsymbol{A} \cap \boldsymbol{B}) = \boldsymbol{A} - \boldsymbol{B}$

Solution: $A - (A \cap B) = A \cap (A \cap B)'$

$= A \cap (A' \cup B')$ (De Morgan's law)

$= (A \cap A') \cup (A \cap B')$

$= \emptyset \cup (A \cap B')$

$= A \cap B' = A - B$

P5:

Simplify, using laws of set theory.

(i) $\boldsymbol{A \cap (B - A)}$

(ii) $\boldsymbol{(A \cap B) \cup (A \cap B \cap C' \cap D) \cup (A' \cap B)}$

(iii) $\boldsymbol{(A - B) \cup (A \cap B)}$

(iv) $\boldsymbol{A' \cup B' \cup (A \cap B \cap C')}$

(v) $\boldsymbol{A' \cup (A \cap B') \cup (A \cap B \cap C') \cup (A \cap B \cap C \cap D') \cup \ldots}$

Solution:

(i) $A \cap (B - A) = A \cap (B \cap A')$

$= A \cap (A' \cap B)$ (Commutative law)

$= (A \cap A') \cap B$ (Associative law)

$= \emptyset \cap B$

$= \emptyset$

(ii) $(A \cap B) \cup (A \cap B \cap C' \cap D) \cup (A' \cap B)$

$= (A \cap B) \cup (A' \cap B)$ (Absorption law)

$= (A \cup A') \cap B$ (Distributive law)

$= U \cap B$

$= B$

(iii) $(A - B) \cup (A \cap B) = (A \cap B') \cup (A \cap B)$

$= A \cap (B' \cup B)$ (Distributive law)

$= A \cap U$

$= A$

(vi) $A' \cup B' \cup (A \cap B \cap C')$

$= (A \cap B)' \cup (A \cap B \cap C')$ (De Morgan's law)

$= \big((A \cap B)' \cup (A \cap B)\big) \cap \big((A \cap B)' \cup C'\big)$ (Distributive law)

$= U \cap (A' \cup B' \cup C')$ (De Morgan's law)

$= (A' \cup B' \cup C')$

(V) First note that

$A' \cup (A \cap B') = (A' \cup A) \cap (A' \cup B')$ (Distributive law)

$= U \cap (A' \cup B')$

$= U \cap (A \cap B)'$ (De Morgan's law)

$= (A \cap B)' ------(1)$

Now, $A' \cup (A \cap B') \cup (A \cap B \cap C')$

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

$= (A \cap B \cap C)'$ (using (1))

and $A' \cup (A \cap B') \cup (A \cap B \cap C') \cup (A \cap B \cap C \cap D')$

$= (A \cap B \cap C)' \cup (A \cap B \cap C \cap D')$

$= (A \cap B \cap C \cap D)'$ (using (1))

Continuing this process we get ,

$\boldsymbol{A' \cup (A \cap B') \cup (A \cap B \cap C') \cup (A \cap B \cap C \cap D') \cup \ldots = (A \cap B \cap C \cap D \cap \ldots)'}$.

P6:

For any sets $\boldsymbol{A}$ and $\boldsymbol{B}$

i) $\boldsymbol{A \oplus B = B \oplus A}$ (⊕ is commutative)

ii) $\boldsymbol{A \oplus \emptyset = A}$

iii) $\boldsymbol{A \oplus A = \emptyset}$

iv) $\boldsymbol{A \oplus A' = U}$

v) $\boldsymbol{A \oplus U = A'}$

Solution:

We have $A \oplus B = (A' \cap B) \cup (A \cap B')$

i) $A \oplus B = (A - B) \cup (B - A)$

$= (B - A) \cup (A - B)$ (Commutativity of ∪)

$= B \oplus A$

ii) $A \oplus \emptyset = (A' \cap \emptyset) \cup (A \cap \emptyset')$

$= \emptyset \cup (A \cap U) = \emptyset \cup A = A$

iii) $A \oplus A = (A' \cap A) \cup (A \cap A') = \emptyset \cup \emptyset = \emptyset$

iv) $A \oplus A' = (A \cap (A')') \cup (A' \cap A')$

$= (A \cap A) \cup A'$

$= A \cup A'$

$= U$

v) $A \oplus U = (A \cap U') \cup (A' \cap U)$

$= (A \cap \emptyset) \cup A'$

$= \emptyset \cup A'$

$= A'$

P7:

For any sets $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$

$$\boldsymbol{A \oplus (B \oplus C) = (A \oplus B) \oplus C} \quad \textbf{(}\oplus \textbf{ is associative)}$$

Solution: $A \oplus (B \oplus C) = \big(A' \cap (B \oplus C)\big) \cup (A \cap (B \oplus C)')$

Now $A' \cap (B \oplus C) = A' \cap \big((B' \cap C) \cup (B \cap C')\big)$

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

and $(A \cap (B \oplus C)') = A \cap \big((B' \cap C) \cup (B \cap C')\big)'$

$= A \cap \big((B' \cap C)' \cap (B \cap C')'\big)$ (De Morgan's law)

$= A \cap \big((B \cup C') \cap (B' \cup C)\big)$

(De Morgan's law and double negation law)

$= A \cap \big((B \cap B') \cup (B \cap C) \cup (C' \cap B') \cup (C' \cap C)\big)$

(Distributive law)

$= A \cap (\emptyset \cup (B \cap C) \cup (C' \cap B') \cup \emptyset)$

$= A \cap \big((B \cap C) \cup (C' \cap B')\big)$

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

Therefore,

$A \oplus (B \oplus C) = (A' \cap B' \cap C) \cup (A' \cap B \cap C') \cup (A \cap B' \cap C') \cup (A \cap B \cap C)$

Further, $(A \oplus B) \oplus C = C \oplus (A \oplus B)$ ($\because \oplus$ is commutative)

$= (C' \cap A' \cap B) \cup (C' \cap A \cap B') \cup (C \cap A' \cap B') \cup (C \cap A \cap B)$ (How ?)

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

Thus, $A \oplus (B \oplus C) = (A \oplus B) \oplus C$

P8:

Show that the sets $\boldsymbol{A}$ and $\boldsymbol{B}$.

$$(\boldsymbol{A} \oplus \boldsymbol{B})' = \boldsymbol{A} \oplus \boldsymbol{B}'$$

Solution:

$(A \oplus B)' = \big((A - B) \cup (B - A)\big)'$ (Definition of symmetric difference)

$= \big((A \cap B') \cup (B \cap A')\big)'$

$= (A \cap B')' \cap (B \cap A')'$ (De Morgan's law)

$= (A' \cup (B')') \cap (B' \cup (A')')$

$= (A' \cup B) \cap (B' \cup A)$ (Double negation law)

$= (A' \cap B') \cup (B \cap B') \cup (A' \cap A) \cup (B \cap A)$ (Distributive law)

$= (A \cap B) \cup (A' \cap B')$

$= (A \cap (B')') \cup (A' \cap B') = A \oplus B'$

2.1 .SETS

Exercise

1. Prove that $\left[\left(A \cup (B \cap C)\right) \cap \left(A' \cup (B \cap C)\right)\right] \cap (B' \cup C') = \emptyset$

2. Show that $(A \cap B) \cup \left[B \cap \left((C \cap D) \cup (C \cap D')\right)\right] = B \cap (A \cup C)$

3. If $A \cup B = A \cup C$ and $A \cap B = A \cap C$, then prove that $B = C$.

4. Prove the following
   (a) $A \cup (B - A) = A \cup B$
   (b) $(A \cup B) \cap (A \cup C) = A \cup (B' \cup C')'$
   (c) $[C \cap (A \cup B)] \cup [(A \cup B) \cap C'] = A \cup B$
   (d) $(A \cup C) \cap [(A \cap B) \cup (C' \cap B)] = A \cap B$

5. Prove the following identities:
   (a) $A - (B - C) = (A - B) \cup (A \cap C)$
   (b) $A \cup (B - C) = (A \cup B) - (C - A)$
   (c) $A \cap (B - C) = (A \cap B) - (A \cap C)$
   (d) $(A - B) - C = A - (B \cup C) = (A - C) - B$

6. Write the following sets as a disjoint union.
   (a) $A \cup B$
   (b) $A \oplus B$
   (c) $A \cup B \cup C$.

P4:

Show that for any sets $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$

$$\left(\left((\boldsymbol{A} \cup \boldsymbol{B}) \cap \boldsymbol{C}\right)' \cup \boldsymbol{B}'\right)' = \boldsymbol{B} \cap \boldsymbol{C}$$

Solution:

$$\left(\left((A \cup B) \cap C\right)' \cup B'\right)' = \left(\left((A \cup B) \cap C\right)'\right)' \cap (B')' \quad \text{(De Morgan's law)}$$

$$= \left((A \cup B) \cap C\right) \cap B \quad \text{(Double negation law)}$$

$$= (A \cup B) \cap (C \cap B) \quad \text{(Associative law of intersection)}$$

$$= (A \cup B) \cap (B \cap C) \quad \text{(Commutative law of intersection)}$$

$$= \left((A \cup B) \cap B\right) \cap C \quad \text{(Associative law of intersection)}$$

$$= B \cap C \quad \text{(Absorption law)}$$

MODULE-2

RELATIONS

2.2.

Relations

Ordered pairs and n −tuples

We first introduce the concepts of ordered pairs and ordered n tuples:
The following is an intuitive definition of an ordered pair.

An ***order pair*** consists of two objects given in a fixed order. The ordering of the two objects is important. We shall denote an ordered pair by (x, y).

A familiar example of an ordered pair is the representation of points in the 2-dimentional Cartesian plane.

The ***equality*** of two ordered pairs (x, y) and (u, v) is defined by

$$(\boldsymbol{x}, \boldsymbol{y}) = (\boldsymbol{u}, \boldsymbol{v}) \Leftrightarrow \big((\boldsymbol{x} = \boldsymbol{u}) \wedge (\boldsymbol{y} = \boldsymbol{v})\big)$$

The concept of an ordered pair can be extended to define an ordered triple, and, more generally, an n-tuple.

An ***ordered triple*** is an ordered pair whose first member is itself an ordered pair. Thus, an ordered triple can be written as $\big((x, y), z\big)$.

We can derive the equality of two ordered triples from the definition of the equality of two ordered pairs.

$$\big((x, y), z\big) = \big((u, v), w\big) \text{ iff } \big((x, y) = (u, v)\big) \wedge \ (z = w)$$

But $(x, y) = (u, v) \Leftrightarrow \big((x = u) \wedge (y = v)\big)$,

Therefore, $\big((x, y), z\big) = \big((u, v), w\big) \Leftrightarrow \big((x = u) \wedge (y = v) \wedge (z = w)\big)$

From the above definition of equality of two ordered triples, we may write an ordered triple as (x, y, z) with an understanding that $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ ***stands for*** $\big((\boldsymbol{x}, \boldsymbol{y}), \boldsymbol{z}\big)$.

Continuing in this way, an ***ordered*** $\boldsymbol{n}$***-tuple***$(\boldsymbol{n} \geq \mathbf{3})$ is defined as an ordered pair whose first member is an ordered $(n-1)$-tuple. We write an ordered n-tuple as $\big((x_1, x_2, \dots, x_{n-1}), x_n\big)$.

Further,$\big((x_1, x_2, \dots, x_{n-1}), x_n\big) = \big((u_1, u_2, \dots, u_{n-1}), u_n\big)$

$\Leftrightarrow \big((x_1 = u_1) \wedge (x_2 = u_2) \wedge \dots \wedge (x_n = u_n)\big)$

Therefore, an ordered n-tuple will be written as $(\boldsymbol{x_1}, \boldsymbol{x_2}, \dots, \boldsymbol{x_n})$.

Cartesian product

Let A and B be any two sets. The ***Cartesian product*** of A and B (in this order) is written as $A \times B$ and is defined as the set of all ordered pairs such that the first and second members of the ordered pair are respectively the elements of A and B. That is,

$$\boldsymbol{A} \times \boldsymbol{B} = \{(\boldsymbol{x}, \boldsymbol{y}) | (\boldsymbol{x} \in \boldsymbol{A}) \wedge (\boldsymbol{x} \in \boldsymbol{B})\}$$

Note:

i. If any one of A, B is the empty set $\emptyset$, then $A \times B = \emptyset = B \times A$

ii. In general, $A \times B \neq B \times A$.

iii. If A and B are finite sets with m and n elements respectively, then

$$\boldsymbol{n}(\boldsymbol{A} \times \boldsymbol{B}) = \boldsymbol{mn}$$

iv. $(A \times B) \times C \neq A \times (B \times C)$

From the definition

$$(A \times B) \times C = \big\{\big((a, b), c\big) | \big((a, b) \in A \times B\big) \wedge (c \in C)\big\}$$

$$= \{(a, b, c) | (a \in A) \wedge (b \in B) \wedge (c \in C)\}$$

and $\quad A \times (B \times C) = \big\{\big(a, (b, c)\big) | (a \in A) \wedge \big((b, c) \in B \times C\big)\big\}$

Note that $\big(a, (b, c)\big)$ is not an ordered triple, since $A \times (B \times C)$ is the set of all ordered pairs, where the first member of the ordered pair is an element of A and the second member is an ordered pair from $B \times C$.Therefore

$$(A \times B) \times C \neq A \times (B \times C)$$

A Cartesian product satisfies the following distributive properties:

Theorem 1: For any three sets $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$

i. $\boldsymbol{A} \times (\boldsymbol{B} \cup \boldsymbol{C}) = (\boldsymbol{A} \times \boldsymbol{B}) \cup (\boldsymbol{A} \times \boldsymbol{C})$
ii. $\boldsymbol{A} \times (\boldsymbol{B} \cap \boldsymbol{C}) = (\boldsymbol{A} \times \boldsymbol{B}) \cap (\boldsymbol{A} \times \boldsymbol{C})$

Proof: We prove the first and the second can be proved on similar lines.

i. $A \times (B \cup C) = \{(x, y) | (x \in A) \wedge (y \in B \cup C)\}$

$$= \{(x, y) | (x \in A) \wedge ((y \in B) \vee (y \in C))\}$$

$$= \{(x, y) | ((x \in A) \wedge (y \in B)) \vee ((x \in A) \wedge (y \in C))\}$$

(by the distributivity of the predicate calculus)

$$= \{(x, y) | ((x, y) \in A \times B) \vee ((x, y) \in A \times C)\}$$

$$= (A \times B) \cup (A \times C)$$

We now define the Cartesian product of any finite number of sets.

Let $A = \{A_i\}_{i \in I_n}$ be an indexed set and $I_n = \{1,2, \dots, n\}$. We denote the Cartesian product of the sets $A_1, A_2, \dots, A_n$ by

$$\bigtimes_{i \in I_n} A_i = A_1 \times A_2 \times A_3 \dots . \times A_n$$

and it is defined by

$$\bigtimes_{i \in I_1} A_i = A_1 \text{ and } \bigtimes_{i \in I_m} A_i = \left(\bigtimes_{i \in I_{m-1}} A_i \right) \times A_m \quad for\ m = 2,3,4, \dots, n$$

By the above definition

$$A_1 \times A_2 \times A_3 = (A_1 \times A_2) \times A_3$$

$$A_1 \times A_2 \times A_3 \times A_4 = (A_1 \times A_2 \times A_3) \times A_4$$

$$= \big((A_1 \times A_2) \times A_3\big) \times A_4$$

This definition of Cartesian product of n sets is related to the definition of n-tuples in the following way:

$$A_1 \times A_2 \times \dots \times A_n = \{(x_1, x_2, \dots, x_n) | (x_1 \in A_1) \wedge (x_2 \in A_2) \wedge \dots \wedge (x_n \in A_n)\}$$

Note:

i. We write $A \times A$ by $\boldsymbol{A^2}$, $A \times A \times A$ by $\boldsymbol{A^3}$ and so on.
ii. If $A_1, A_2, A_3, \dots, A_n$ are finite sets ,then

$$n(A_1 \times A_2 \times \dots \times A_n) = n(A_1).n(A_2) \dots .n(A_n)$$

Relations

The concept of a relation is a basic concept in everyday life as well as in mathematics. We have already come across various relations. Familiar examples in arithmetic are relations such as 'greater than', 'less than' or that of 'equality between two real numbers'. Similar examples exist for relations among more than two objects. In this module we only consider relations, called binary relations, between a pair of objects. We note that a relation between two objects can be defined by listing the two objects as an ordered pair. A set of all such ordered pairs, in each of which the first member has some definite relationship to the second, describes a particular relationship.

Relation: Any set of ordered pairs defines a ***binary relation***.

We call a binary relation simply a relation. If R is a relation and $(x, y) \in R$ then we sometimes write $\boldsymbol{xRy}$ and it is read as "**$\boldsymbol{x}$ is in relation $\boldsymbol{R}$ to $\boldsymbol{y}$**" or "**$\boldsymbol{x}$ is related to $\boldsymbol{y}$ by the relation $\boldsymbol{R}$**".

Binary relation from $\boldsymbol{A}$ to $\boldsymbol{B}$: Let A and B be any two sets. A subset S of the Cartesian product $A \times B$ is said to be a **binary relation from $\boldsymbol{A}$ to $\boldsymbol{B}$**.

Let

$$D(S) = \big\{x \in A | (\exists y)\big((x, y) \in S\big)\big\}$$

$i.e.$, $D(S)$ is the set of objects $x \in A$ such that for some $y \in B$, $(x, y) \in S$ and $D(S)$ is called the ***domain of S***. Clearly $D(S) \subseteq A$.

Let

$$R(S) = \{y \in B | (\exists x)((x, y) \in S)\}$$

$i.e.$, $R(S)$ is the set of all objects $y \in B$ such that for some $x \in A$, $(x, y) \in S$ and $R(S)$ is called the ***range of S.*** Clearly, $R(S) \subseteq B$.

Note that $A \times B \subseteq A \times B$ and $\emptyset \subseteq A \times B$. Therefore $A \times B$ itself defines a relation from A to B called the ***Universal relation*** from A to B, while the empty set defines a relation called a ***void relation*** from A to B.

Number of relations: If A and B are finite sets with m and n elements respectively, then the number of relations from A to B is 2^{mn}.

This follows from the fact that every subset of $A \times B$ is a relation and there are 2^{mn} subsets for $A \times B$.

Relation on $\boldsymbol{A}$: A relation from A to itself is called *a* ***relation on A.*** That is, R is a relation on A iff $\boldsymbol{R \subseteq A \times A}$.

Throughout this module a relation means a relation on a set A.

If R and S are relations on a set A then $R \cap S$, $R \cup S$, $R - S$ and R' define relations on A in the following way:

$$\boldsymbol{R \cap S = \{(x, y) | (x, y) \in R \wedge (x, y) \in S\}}$$

$$\boldsymbol{R \cup S = \{(x, y) | (x, y) \in R \vee (x, y) \in S\}}$$

$$\boldsymbol{R - S = \{(x, y) | (x, y) \in R \wedge (x, y) \notin S\}}$$

$$\boldsymbol{R' = \{(x, y) | (x, y) \notin R\} = A \times A - R}$$

Example 1: Let $\boldsymbol{A = \{1, 2, 3, 4\}}$. If $\boldsymbol{R}$ and $\boldsymbol{S}$ are relations on a set $\boldsymbol{A}$ defined by

$$\boldsymbol{R = \{(x, y) | x \in A \wedge y \in A \wedge (x \equiv y (mod\ 2))\}}$$

$$\boldsymbol{S = \{(x, y) | x \in A \wedge y \in A \wedge (x \leq y)\}}$$

then find $\boldsymbol{R \cap S}$, $\boldsymbol{R \cup S}$, $\boldsymbol{S'}$ and $\boldsymbol{R - S}$.

Solution: We have

$R = \{(x, y)|x \in A \wedge y \in A \wedge ((x - y)\ is\ an\ integral\ multiple\ of\ 2)\}$

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

$S = \{(x, y)|x \in A \wedge y \in A \wedge (x \leq y)\}$

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

Now,

i. $R \cap S = \{(x, y)|(x, y) \in R \wedge (x, y) \in S\} = \{(1,3), (2,4)\}$

ii. $R \cup S = \{(x, y)|(x, y) \in R \vee (x, y) \in S\}$

$R \cup S = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,1), (3,3), (3,4), (4,2), (4,4)\}$

iii. $S' = \{(x, y)|(x, y) \notin S\} = \{(x, y)|(x, y) \in A \times A \wedge (x, y) \notin S\}$

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

iv. $R - S = R \cap S' = \{(3,1), (4,2)\}$

Properties of binary relations on a set

Reflexive relation: A (binary) relation R on a set A is ***reflexive*** if for every $x \in A$, xRx, $i.e.$, $(x, x) \in R$ or

$$R \text{ is reflexive on } A \Leftrightarrow \forall x(x \in A \longrightarrow xRx)$$

Examples:

(i) The relation $\leq$ is reflexive on $\boldsymbol{R}$,the set of real numbers, since $x \leq x$, $\forall x \in \boldsymbol{R}$

(ii) The relation inclusion ($\subseteq$) is reflexive in the family of all subsets of a universal set.

(iii) The relation equality of sets is also reflexive.

The relation $<$ is not reflexive on $\boldsymbol{R}$ and the relation proper inclusion ($\subset$) is not reflexive on the family of subsets of a universal set.

Symmetric relation: A relation R on a set A is ***symmetric*** if, for every $x, y \in A$. yRx whenever xRy, $i.e.$, $(y, x) \in R$ whenever $(x, y) \in R$.
That is R is symmetric $\Leftrightarrow \forall x\ \forall y\big(x \in A \wedge y \in A \wedge (xRy \longrightarrow yRx)\big)$

The relation $\leq$ and $<$ are not symmetric on $\boldsymbol{R}$, while the relation of equality is symmetric. The relation of similarity is both reflexive and symmetric on the set of triangles in a plane.

(The relation of being a brother is not symmetric on the set of all people. However, in the set of all males it is symmetric).

Transitive relation: A relation R on a set A is ***transitive*** if for every x, y and $z \in A$

$$xRz \text{ whenever } xRy \text{ and } yRz$$

$$i.e., (x, z) \in R \text{ whenever } (x, y) \in R \text{ and } (y, z) \in R.$$

That is,
R is transitive $\Leftrightarrow \forall x\ \forall y\ \forall z\big(x \in A \wedge y \in A \wedge z \in A \wedge (xRy \wedge yRz \longrightarrow xRz)\big)$

The relations $\leq$, $<$ and $=$ are transitive on $\boldsymbol{R}$.

The relations $\subseteq$, $\subset$ and equality are transitive on the family of subsets of a universal set. The relation similarity of triangles in a plane is transitive, while the relation of being a mother is not on the set of people.

Irreflexive relation: A relation R on a set A is ***Irreflexive*** if, for every $x \in A$, $(x, x) \notin R$.$i.e.$ $\boldsymbol{x \not{R}\, x \ \ \forall x \in A}$

The relation $<$ on $\boldsymbol{R}$ is irreflexive because for no $x \in \boldsymbol{R}$ do we have $x < x$. The relation of proper inclusion on the set of all non-empty subsets of a universal set is irreflexive.

Let R, S and T be relations on $A = \{1,2,3\}$ given by

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

$$S = \{(1,1), (1,2), (3,2), (2,3), (3,3)\}$$

$$T = \{(1,1), (2,1), (2,2), (3,2), (3,3)\}$$

Here R is irreflexive, S is not reflexive and T is reflexive.

Antisymmetric relation: A relation R on a set A is ***antisymmetric*** if, for every $x, y \in A$,

$$x = y \text{ whenever } xRy \text{ and } yRx.$$

$$i.e., x = y \text{ whenever } (x, y) \in R \text{ and } (y, x) \in R.$$

That is

$$\forall x\, \forall y\, \forall z \left(x \in A \wedge y \in A \wedge \left(xRy \wedge yRx \longrightarrow (x = y)\right)\right)$$

The contrapositive of this definition is that $\boldsymbol{R}$ is antisymmetric if $\boldsymbol{x \neq y}$ then $\boldsymbol{x \not{R} y}$ or $\boldsymbol{y \not{R} x}$. It follows that $\boldsymbol{R}$ is not anti symmetric if we have $\boldsymbol{x}$ and $\boldsymbol{y}$ in ,$\boldsymbol{x \neq y}$,and both $\boldsymbol{xRy}$ and $\boldsymbol{yRx}$

Let X be the collection of subsets of a universal set. For $A, B \in X$, $A \subseteq B$ and $B \subseteq A \Longrightarrow A = B$.Thus, inclusion is an antisymmetric relation on X.

Also the relation of proper inclusion on X is antisymmetric.

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

The following are some examples of equivalence relations:

i. Equality of numbers on the set of real numbers
ii. Equality of subsets of a universal set.
iii. Similarity of triangles on the set of triangles
iv. Relation of lines being parallel on a set of lines in a plane
v. Relation of living in the same town on the set of people living in Andhra Pradesh
vi. Relation of propositions being equivalent in the set of propositions.

Congruence modulo $\boldsymbol{m}$: Let $m > 1$ be a given natural number. For any $x, y \in \boldsymbol{Z}$, $x \equiv y(mod\ m)$, read as "x is congruent to y modulo m", if $x - y$ is divisible by m. The relation is called congruence modulo m

Example 2: The relation $\boldsymbol{R}$ on $\boldsymbol{Z}$, the set of integers , defined by

$$\boldsymbol{R} = \{(\boldsymbol{x}, \boldsymbol{y}) | \boldsymbol{x} \in \boldsymbol{Z} \wedge \boldsymbol{y} \in \boldsymbol{Z} \wedge (\boldsymbol{x} \equiv \boldsymbol{y}(\boldsymbol{mod\ m}))\}$$

is an equivalence relation.

Solution:

i. For any $x \in \boldsymbol{Z}$,$x - x$ is divisible by m. Therefore, $x \equiv x(mod\ m)\ \forall x \in Z$. Thus R is reflexive.

ii. For any $x, y \in \boldsymbol{Z}$, if $x \equiv y(mod\ m)$ then $x - y$ is divisible by m. Therefore $y - x$ is also divisible by m . Thus,
$x \equiv y(mod\ m) \Longrightarrow y \equiv x(mod\ m)$.This shows that R is symmetric

iii. For , $y, z \in \boldsymbol{Z}$, if $x \equiv y(mod\ m)$ and $y \equiv z(mod\ m)$, then $x - y$ and $y - z$ are divisible by m. Therefore,
$x - z = (x - y) + (y - z)$ is also divisible by $m\ i.e.$, $x \equiv z(mod\ m)$

Thus, ***the relation congruence modulo $\boldsymbol{m}$ is an equivalence relation on the set $\boldsymbol{Z}$ of integers.***

Partial order: A relation R on a set A is called a **partial order relation** or **partial ordering relation** or **partial order** iff R is reflexive, anti symmetric and transitive.

The following are some examples of partial order relations:

i. The relation $\leq$ is a partial ordering on $\boldsymbol{R}$
ii. The relation $\geq$ is a partial ordering on $\boldsymbol{R}$
iii. Let A be any set. The relation of inclusion($\subseteq$) is a partial ordering on $P(A)$
iv. The relation "divides" is a partial ordering on the set of positive integers

Note:

(i) If R_1 and R_2 are equivalence relations on A, then $R_1 \cap R_2$ is also an equivalence relation A.

(ii) If R_1 and R_2 are partial orders on A, then $R_1 \cap R_2$ is also a partial order on A.

(iii) For any set A, $A \times A$ is an equivalence relation on A.

(iv) If $A = \{a_1, a_2, \dots a_n\}$ then the equality relation $R = \{(a_i, a_i) | i = 1, 2, \dots, n\}$ is the smallest equivalence relation on A.

(v) Let R be a relation on a set A . R is both an equivalence relation and a partial order on A if and only if R is the equality relation on A.

P1:

Write down all relations from $\boldsymbol{A} = \{\mathbf{1}, \mathbf{2}\}$ to $\boldsymbol{B} = \{\boldsymbol{a}, \boldsymbol{b}\}$.

Solution: We have $A = \{1,2\}$, $B = \{a, b\}$, and $n(A) = n(B) = 2$

Now $A \times B = \{(x, y) | x \in A \wedge y \in B\}$

$$= \{(1, a), (1, b), (2, a), (2, b)\}$$

The number of relations from a finite set A to a finite set B is $2^{n(A) \cdot n(B)} = 16$

We have to enlist all relations from A to B.

$R_1 : \phi$

$R_2 : \{(1, a)\}$

$R_3 : \{(1, b)\}$

$R_4 : \{(2, a)\}$

$R_5 : \{(2, b)\}$

$R_6 : \{(1, a), (1, b)\}$

$R_7 : \{(1, a), (2, a)\}$

$R_8 : \{(1, a), (2, b)\}$

$R_9 : \{(1, b), (2, a)\}$

$R_{10} : \{(1, b), (2, b)\}$

$R_{11} : \{(2, a), (2, b)\}$

$R_{12} : \{(1, a), (1, b), (2, a)\}$

$R_{13} : \{(1, a), (1, b), (2, b)\}$

$R_{14} : \{(1, a), (2, a), (2, b)\}$

$R_{15} : \{(1, b), (2, a), (2, b)\}$

$R_{16}: \{(1, a), (1, b), (2, a), (2, b)\}$

P2:

Let $\boldsymbol{A = \{1, 2, 3\}}$ and $\boldsymbol{B = \{1, 2, 3, 4\}}$.

If $\boldsymbol{R_1 = \{(1, 1), (2, 2), (3, 3)\}}$ and $\boldsymbol{R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}}$, then find $\boldsymbol{R_1 \cup R_2}$, $\boldsymbol{R_1 \cap R_2}$, $\boldsymbol{{R_1}'}$, $\boldsymbol{R_2 - R_1}$.

Solution:

i) $R_1 \cup R_2 = \{(x, y) | (x, y) \in R_1 \vee (x, y) \in R_2\}$

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

ii) $R_1 \cap R_2 = \{(x, y) | (x, y) \in R_1 \wedge (x, y) \in R_2\}$

$= \{(1,1)\}$

iii) $R_1' = (A \times B) - R_1$
$= \{(1,2), (1,3), (1,4), (2,1), (2,3), (2,4), (3,1), (3,2), (3,4)\}$

iv) $R_2 - R_1 = R_2 \cap R_1' = \{(1,2), (1,3), (1,4)\}$

P3:

Let $\boldsymbol{A = \{1, 2, 3, \ldots, 7\}}$ **and**

$$\boldsymbol{R = \{(x, y) | x \in A \wedge y \in A \wedge (x \equiv y (mod\ 3))\}}$$

$$\boldsymbol{S = \{(x, y) | x \in A \wedge y \in A \wedge (x \equiv y (mod\ 4))\}}$$

Find $\boldsymbol{R \cap S}$ **,** $\boldsymbol{R \cup S}$ **,** $\boldsymbol{R - S}$**.**

Solution: We have

$$R = \left\{ \begin{matrix} (1,1), (1,4), (1,7), (2,2), (2,5), (3,3), (3,6), (4,1), (4,4), \\ (4,7), (5,2), (5,5), (6,3), (6,6), (7,1), (7,4), (7,7) \end{matrix} \right\}$$

$$S = \left\{ \begin{matrix} (1,1), (1,5), (2,2), (2,6), (3,3), (3,7), (4,4), \\ (5,1), (5,5), (6,2), (6,6), (7,3), (7,7) \end{matrix} \right\}$$

$$R \cap S = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7)\}$$

$$R \cup S = \left\{ \begin{matrix} (1,1), (1,4), (1,5), (1,7), (2,2), (2,5), (2,6), (3,3), (3,6), (3,7), (4,1), \\ (4,4), (4,7)(5,1), (5,2), (5,5), (6,2), (6,3), (6,6), (7,1), (7,3), (7,4), (7,7) \end{matrix} \right\}$$

$$R - S = \{(1,4), (1,7), (2,5), (3,6), (4,1), (4,7), (5,2), (6,3), (7,1), (7,4)\}$$

$$S - R = \{(1,5), (2,6), (3,7), (5,1), (6,2), (7,3)\}$$

P4:

The relation "divides" is a partial order relation on N, the set of natural numbers.

Solution: We have $\boldsymbol{N}$ and let

$$R = \{(x, y) | x \in \boldsymbol{N} \wedge y \in \boldsymbol{N} \wedge (x|y)\}$$

(i) For any $x \in \boldsymbol{N}$, we have $x|x$. Thus xRx , $\forall x \in \boldsymbol{N}$. Therefore the relation R is reflexive.

(ii) If $x|y$ and $y|x$ then $y = kx$ and $x = ly$ for some $k, l \in \boldsymbol{N}$. Therefore, $x = klx$. Thus $kl = 1$, implying $k = l = 1$. This shows that $x = y$, proving R is antisymmetric.

(iii) If $x|y$ and $y|z$ then $y = kx$ and $z = ly$ for some $k, l \in \boldsymbol{N}$.Therefore $z = lkx$. This proves that $x|z$. Thus R is transitive.

Therefore, R is reflexive, anti symmetric and transitive. This proves R is a partial order relation on $\boldsymbol{N}$.

Note: The relation "divides" is not a partial order on $\boldsymbol{Z}$**,** the set of integers(why?)

P5:

If $\boldsymbol{R}$ is a relation on $\boldsymbol{Z} \times \boldsymbol{Z}$, where $(\boldsymbol{x}, \boldsymbol{y})\ \boldsymbol{R}\ (\boldsymbol{u}, \boldsymbol{v})$ if $\boldsymbol{x} \leq \boldsymbol{u}$. Determine whether $\boldsymbol{R}$ is reflexive, symmetric, anti symmetric or transitive

Solution:

First note that $R \subseteq (\boldsymbol{Z}\ \times \boldsymbol{Z})\ \times\ (\boldsymbol{Z}\ \times \boldsymbol{Z})$

(i) For any $x \in \boldsymbol{Z}$ we have $x \leq x$
For any $(x, y) \in\ \boldsymbol{Z}\ \times\ \boldsymbol{Z}$, we have ,$(x, y)R(x, y)$, since $x \leq x$
Thus, $(x, y)R\ (x, y)$, $\forall\ (x, y)\ \in Z\ \times Z$.
Therefore R is reflexive

(ii) If $x \leq u$ then $(x, y)R\ (u, v)$, but $(u, v) \not{R} (x, y)$,since $u \geq x$ when $x \leq u$
Therefore R is not symmetric.
If $(x, y)\ R\ (u, v)$ and $(u, v)\ R\ (x, y)$ then $x \leq u$ and $u \leq x$,
$i.e.$, $x = u$ with no restriction y and v.
Note that $(1, 2)\ R\ (1, -3)$ and $(1, -3)\ R\ (1, 2)$ without being equal. This shows that R is not anti symmetric. Thus R is neither symmetric nor anti symmetric.

Remark: Not symmetric does not mean anti symmetric.

(iii) $(x, y)\ R\ (u, v)$ and $(u, v)\ R\ (r, s) \implies x \leq u$ and $u \leq r$

$$\implies x \leq r$$

$$\implies (x, y)\ R\ (r, s)$$

This, shows that R is transitive.

Therefore, R is reflexive, transitive and neither symmetric nor anti symmetric.

P6:

Let R_1 and R_2 be relations on a set A.

(a) Prove or disprove that R_1 and R_2 reflexive $\Longrightarrow$ $R_1 \cap R_2$ is reflexive.

(b) Answer part (a) when each occurrence of "reflexive" is replaced by (i) symmetric (ii) anti symmetric and (iii) transitive.

Solution:

(a) R_1 and R_2 are reflexive $\Longrightarrow (x,x) \in R_1, \ \forall\, x \in A$ and $(x,x) \in R_2, \ \forall\, x \in A$

$$\Longrightarrow (x,x) \epsilon R_1 \cap R_2\,, \ \forall\, x \,\epsilon\, A$$

$\Longrightarrow R_1 \cap R_2$ is reflexive.

(b)

(i) We have R_1 and R_2 are symmetric.

$(x,y) \in R_1 \cap R_2 \Longrightarrow (x,y) \in R_1$ and $(x,y) \in R_2$

$\Longrightarrow (y,x) \in R_1$ and $(y,x) \in R_2$

(Since R_1 and R_2 are symmetric)

$\Longrightarrow (y,x) \in R_1 \cap R_2$

Thus, $R_1 \cap R_2$ is symmetric whenever R_1 and R_2 are symmetric.

(ii) We have R_1 and R_2 are anti symmetric

$(x,y) \in R_1 \cap R_2$ and $(y,x) \in R_1 \cap R_2$

$\Longrightarrow \big((x,y) \in R_1$ and $(x,y) \in R_2\big)$ and $\big((y,x) \in R_1$ and $(y,x) \in R_2\big)$

$\Longrightarrow \big((x,y) \in R_1$ and $(y,x) \in R_1\big)$ and $\big((x,y) \in R_2$ and $(y,x) \in R_2\big)$

$\Longrightarrow (x=y)$ and $(y=x)$ (Since R_1 and R_2 are anti symmetric).

$\Longrightarrow x=y$

Thus, $R_1 \cap R_2$ is anti symmetric whenever R_1 and R_2 are anti symmetric.

(iii) We have R_1 and R_2 are transitive

$(x, y) \in R_1 \cap R_2$ and $(y, z) \in R_1 \cap R_2$

$\Longrightarrow \big((x, y) \in R_1$ and $(x, y) \in R_2\big)$ and $\big((y, z) \in R_1$ and $(y, z) \in R_2\big)$

$\Longrightarrow \big((x, y) \in R_1$ and $(y, z) \in R_1\big)$ and $\big((x, y) \in R_2$ and $(y, z) \in R_2\big)$

$\Longrightarrow (x, z) \in R_1$ and $(x, z) \in R_2$ (Since R_1 and R_2 are transitive)

$\Longrightarrow (x, z) \in R_1 \cap R_2$

Thus, $R_1 \cap R_2$ is transitive whenever R_1 and R_2 are transitive.

P7:

What is wrong with the following argument?

Let A be a set with R a relation on A. If R is symmetric and transitive, then R is reflexive

Solution:

Let $(x, y) \in R$ .By the symmetry $(y, x) \in R$. Now $(x, y) \in R$ and $(y, x) \in R$ will imply $(x, x) \in R$, by transitivity. Hence R is reflexive.

The conclusion $(x, x) \in R$ is true for $x \in A$ only. The relation R be reflexive we need $(x, x) \in R, \forall x \in A$

There may exist an element $a \in A$ such that for all $b \in A$, neither(a, b) nor $(b, a) \in R$. The argument is not correct.

P8:

Which of the following relations on $A = \{0, 1, 2, 3\}$ are equivalent relations/partial orders? Determine the properties of an equivalence/a partial order the others lack.

$R_1 = \{(0,0), (1,1), (2,2), (3,3)\}$

$R_2 = \{(0,0), (0,2), (2,0), (2,2), (2,3), (3,2), (3,3)\}$

$R_3 = \{(0,0), (1,1), (1,2), (2,1), (2,2), (3,3)\}$

$R_4 = \{(0,0), (1,1), (1,3), (2,2), (2,3), (3,1), (3,2), (3,3)\}$

$R_5 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,2), (3,3)\}$

$R_6 = \{(0,0), (2,0), (2,2), (2,3), (3,2), (3,3)\}$

$R_7 = \{(0,0), (1,1), (1,2), (2,2), (3,3)\}$

$R_8 = \{(0,0), (1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$

Solution:

Relation	Reflexive	Symmetric	Anti symmetric	transitive	Equivalence relation	Partial order
R_1	✓	✓	✓	✓	✓	✓
R_2	×	✓	×	×	×	×
R_3	✓	✓	×	✓	✓	×
R_4	✓	✓	×	×	×	×
R_5	✓	×	×	×	×	×
R_6	×	×	×	×	×	×
R_7	✓	×	✓	✓	×	✓
R_8	✓	×	✓	✓	×	✓

2.2. Relations

Exercises

1. List the ordered pairs in the relation R from $A = \{0,1,2,3,4\}$ to $B = \{0,1,2,3\}$, where $(a, b) \in R$ if and only if
    a) $a = b$
    b) $a + b = 4$
    c) $a > b$
    d) $a|b$
    e) $gcd(a, b) = 1$
    f) $lcm(a, b) = 2$

2. Let $A = \{a, b, c\}$ and $B = \{1,2,3,4\}$.
   If $R = \{(a, 2), (a, 4), (b, 2), (b, 3), (c, 1), (c, 4)\}$
   $S = \{(a, 3), (b, 1), (b, 2), (b, 4), (c, 4), (c, 1)\}$
   Then find $R \cap S$, $R \cup S$, $R - S$, $S - R$.

3. Let $A = \{1,2,3,4\}$ and $B = \{a, b, c\}$.
   If $R = \{(1, a), (2, b), (3, c), (4, a)\}$ and $S = \{(1, b), (2, c), (3, a), (4, a)\}$
   Then find $R \cup S$, $R \cap S$, $R - S$, $S - R$.

4. Let $A = \{2,3,5,6,7\}$ and $B = \{3,4,10,12,14,15\}$. Let R and S be relations from A to B defined by:
   For all $a \in A, b \in B$
    i. $a\ R\ b$ iff $a|b$
    ii. $a\ S\ b$ iff $a \geq b$
   then find $R \cup S$ and $R \cap S$.

5. Consider the following relation on Z:

$R_1 = \{(a, b) | a \leq b\}$

$R_2 = \{(a, b) | a > b\}$

$R_3 = \{(a, b) | a = b \text{ or } a = -b\}$

$R_4 = \{(a, b) | a = b\}$

$R_5 = \{(a, b) | a = b + 1\}$

$R_6 = \{(a, b) | a + b \leq 3\}$

Decide which of these are reflexive, symmetric, anti symmetric, transitive.

6. Consider the following relation on $A = \{1,2,3,4\}$.

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

   $R_2 = \{(1,1), (1,2), (2,1)\}$

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

   $R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$

   $R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

   $R_6 = \{(3,4)\}$

   Which of these relations are reflexive, symmetric, anti symmetric, transitive?

7.
   a) How many relations are there on the set $\{a, b, c, d\}$?
   b) How many relations are there on the set $\{a, b, c, d\}$ that contain the pair (a, a)?

8. Let R be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $ad = bc$. Show that R is an equivalence relation.

9. Give an example of a relation in $\{1,2,3\}$ which is
   a) Reflexive but neither symmetric nor transitive
   b) Symmetric but neither reflexive nor transitive
   c) Transitive but neither reflexive nor symmetric
   d) Reflexive and symmetric but not transitive
   e) Reflexive and transitive but not symmetric
   f) Symmetric and transitive but not reflexive
   g) Reflexive, symmetric and transitive
   h) Not reflexive, not symmetric and not transitive

MODULE-3

Equivalence Relations and compatibility relations

2.3

Equivalence relations and Compatibility relations

We first discuss **two** methods of representing relations on a set. One method uses zero-one matrices and the other method uses directed graphs.

Relation Matrix of a Relation

Let A and B be finite sets with m and n elements respectively. Let the elements of A and B be ordered in certain order say $A = \{a_1, a_2, \dots, a_m\}$ and $B = \{b_1, b_2, \dots, b_n\}$. A relation R from A to B can be represented by an $m \times n$ matrix called the **relation matrix of $\boldsymbol{R}$**, denoted by $\boldsymbol{M_R}$ with entries $0's$ and $1's$.($i.e.$, bits) and $M_R = (m_{ij})_{m \times n}$ is defined as

$$\boldsymbol{m_{ij} = \begin{cases} 1 & if \quad a_i R \ b_j \\ 0 & if \quad a_i \not{R} \ b_j \end{cases}}$$

Example 1: If $\boldsymbol{A = \{1, 2, 3, 4\}}$, $\boldsymbol{B = \{1, 4, 6, 8, 9\}}$ and a relation $\boldsymbol{R}$ from $\boldsymbol{A}$ to $\boldsymbol{B}$ is defined by: for $\boldsymbol{a, b \in A}$, $\boldsymbol{a\ R\ b}$ iff $\boldsymbol{a|b}$.Write $\boldsymbol{R}$ and the matrix of $\boldsymbol{R}$.

Solution: We have, $R = \{(a, b) |\ a \in A\ \wedge b \in B\ \wedge\ (a|b)\}$

$R\ = \{(1,1), (1,4), (1,6), (1,8), (1,9), (2,4), (2,6), (2,8), (3,6), (3,9), (4,4), (4,8)\}$

and $M_R = (m_{ij})_{4\times 5}$ where $m_{ij} = \begin{cases} 1 & if \quad a_i \ \ | \ b_j \\ 0 & if \quad a_i \ \ \nmid b_j \end{cases}$

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

Note: The matrix of a relation from A to B depends on the ordering of the elements of A and B.

Conversely, given two sets A and B with $|A| = m$ and $|B| = n$, an $m \times n$ matrix whose entries are zeros and ones determines a relation .

Consider the matrix

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

Since M is a 3×4 matrix, we let $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4\}$ and

we write down the corresponding relation R from A to B as follows

$$\left(a_i,\ b_j\right) \in R \text{ iff } m_{ij} = 1.$$

Therefore, $R = \{(a_1, a_1),\ (a_1, b_4), (a_2, b_2), (a_2, b_3), (a_3, b_1), (a_3, b_3)\}$

Throughout this module we consider the relations on a set $A, i.e.$,The relations form A to itself.

A relation matrix M_R of a relation R on a set A reflects some of the properties of R.

a) If R is reflexive, then all the diagonal entries of M_R must be 1.
b) If R is symmetric, then M_R is a symmetric matrix.
c) If R is antisymmetric, then M_R is such that $m_{ij} = 0$ whenever $m_{ji} = 1$ for $i \neq j$.

Graph of a relation:

A relation can also be represented pictorially by drawing its graph. Although we shall introduce some of the concepts of graph theory which are discussed in a sub sequent unit, here we shall use graph only as a tool to represent relations.

Let R be a relation on a set $A = \{a_1, a_2, \dots, a_m\}$ (we order the elements of A in a certain order and keep the ordering fixed throughout the discussion). The elements of A are represented by points (or small circles) called **nodes** (or **vertices**).

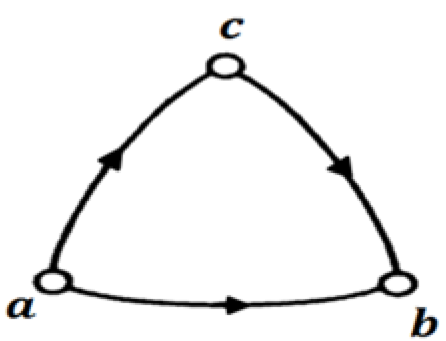
If $a_i\ R\ a_j$, $i.e.$, $\left(a_i, a_j\right) \in R$, then we connect the nodes a_i and a_j by means of an arc ,called an **edge**, and put an arrow mark on the arc form a_i to a_j. When all nodes corresponding to all the ordered pairs in R are connected by arcs with proper arrows, we get a **graph** (**directed graph** and **digraph**) of the relation R.

If $a_i\ R\ a_j$ and $a_j\ R\ a_i$, then we draw to arcs a_i to a_j and a_j to a_i. For the sake of simplicity, we may replace two arcs by one arc with arrows pointing in both directions. If $a_i R\ a_i$, we get an arc which starts from a_i and returns to a_i. Such an arc is called a **loop**.

A node $a \in A$ is said to be an **isolated node**, if $a \not{R} x$ and $x \not{R}\ a$, $for\ all\ x \in A,\ x \neq a$

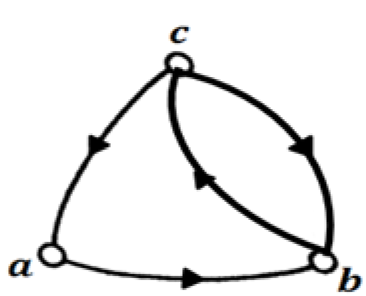
Example 2: Let $A = \{a, b, c\}$

(i) Let $R_1 = \{(a, b), (a, c), (c, b)\}$. Then its digraph and M_{R_1} are given by

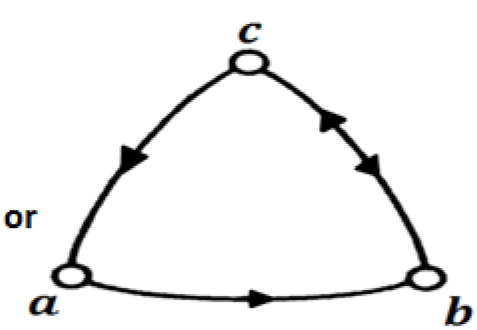


$$M_{R_1} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

(ii) Let $R_2 = \{(a, b), (c, a), (c, b), (b, c)\}$. Then

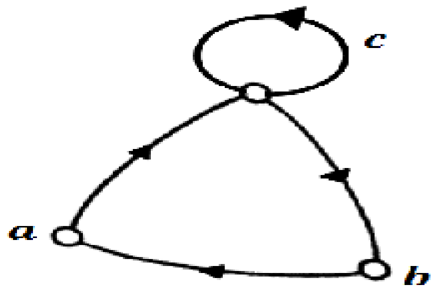


or



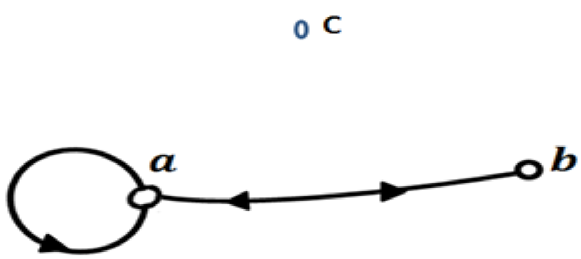
$$M_{R_2'} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

(iii) Let $R_3 = \{(a,c),(c,c),(c,b),(b,a)\}$



$$M_{R_3} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

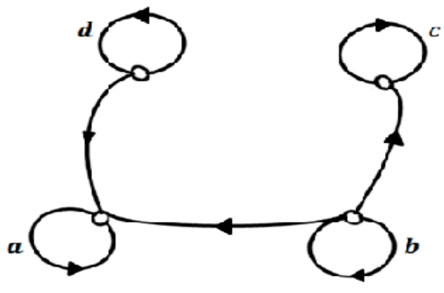
(iv) Let $R_4 = \{(a,a),(a,b),(b,a)\}$



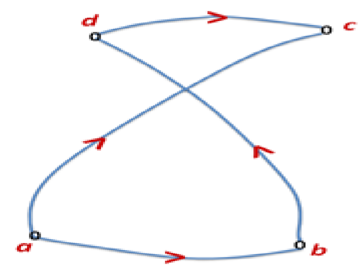
$$M_{R_4} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

From the graph of a relation it is possible to observe some of its properties

If a relation is reflexive, then there must be loops at each node. On the other hand, if the relation is irreflexive, then there is no loop at any node .



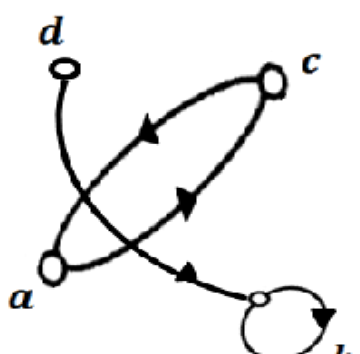
Reflexive relation



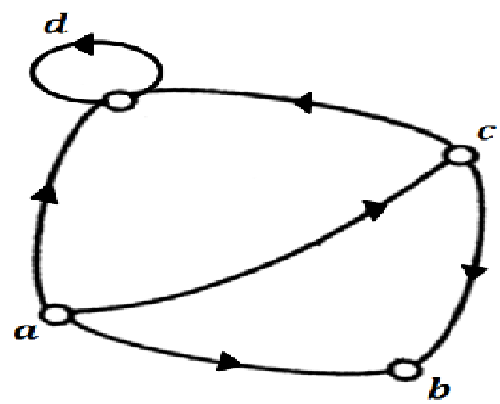
Irreflexive relation

If a relation is symmetric then there must be an arc form one node b to another node a whenever there is an arc from a to b.

If a relation is antisymmetric then an arc from one node b to another node a $(a \neq b)$ does not exist, whenever there is an arc form a to b.

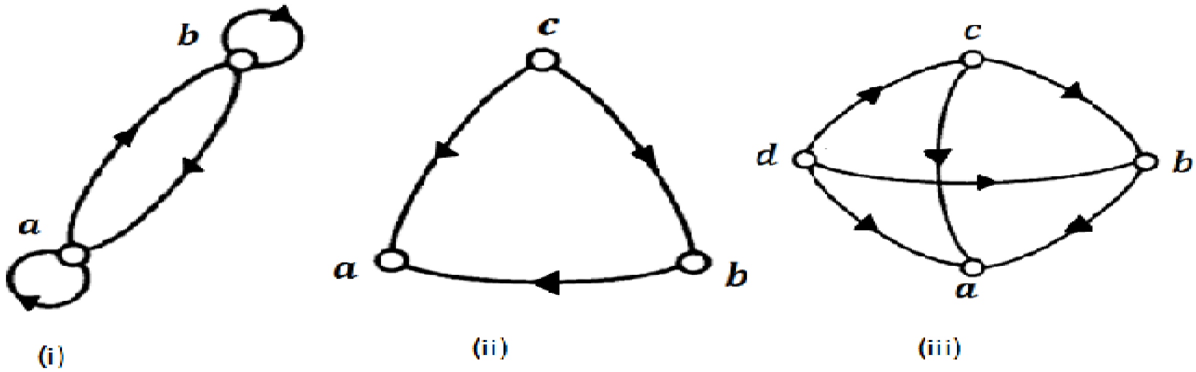


Symmetric



Antisymmetric relation

If a relation is transitive, then the situation is not so simple. In any case, its digraph must have circuits of the type shown in the following figure



Transitive

Note:

i) When the number of elements in a set A over which a relation R is defined is large, say greater than or equal to 5 or 6, both the graphical and the matrix representations of the relation become unwieldy. However, the matrix representation can be considered, since the computing machines can handle matrices well.

ii) It is easy to determine from the matrix of the relation whether the relation is reflexive or symmetric. But it is not always easy to determine from the matrix whether the relation is transitive.

iii) The entries of the relation matrix are denoted by T and F instead of 1 and 0 respectively in order to conserve storage (note that in FORTRAN only 1 byte is needed for each logical entry, but at least 2 bytes are required for an integer entry).

Partition and Covering of a set

Let A be a given set and $C = \{A_1, A_2, \dots, A_m\}$, where each $A_i, i = 1, 2, 3, \dots, m$ is a subset of A. We say that C is a ***covering*** of A if $A = \bigcup_{i=1}^{m} A_i$ and the sets $A_1, A_2, \dots, A_m$ are said to ***cover*** A.

We say that C is a **partition** of A if $A_i \cap A_j = \emptyset$, when $i \neq j$ and $A = \bigcup_{i=1}^{m} A_i$

That is C is a partition of A, if C is a covering of A and the elements of C, which are subsets of A are mutually disjoint. If C is a partition of A, then the sets $A_1, A_2, \ldots, A_m$ of C are called the ***blocks*** of the partition.

For example, Let $A = \{a, b, c\}$ and consider the following collection of subsets of A.

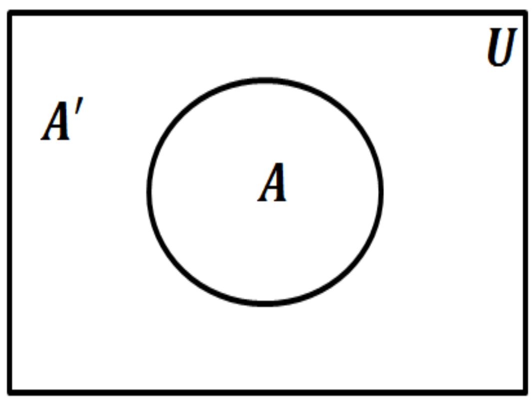
$$C_1 = \{\{a, b\}, \{b, c\}\}, C_2 = \{\{a\}, \{b, c\}\}$$

$$C_3 = \{\{a\}, \{b\}, \{c\}\}, C_4 = \{\{a\}, \{a, b\}, \{a, c\}\}$$

The sets C_1 and C_4 are coverings of A and are not partitions of A.The sets C_2 and C_3 are partitions of A.

Some partitions of the Universal set U

First consider a subset A of U. The subsets A and A' generate a partition of U, since $A \cap A' = \emptyset$ and $A \cup A' = U$.

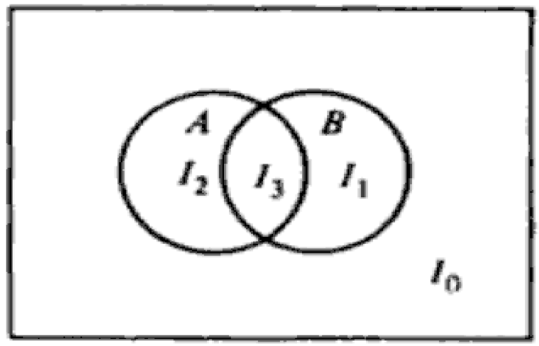


Let A and B be any two subsets of U.Consider the subsets

$$I_0 = A' \cap B', I_1 = A' \cap B, I_2 = A \cap B' \text{ and } I_3 = A \cap B$$

The sets I_0, I_1, I_2 and I_3 are called ***complete intersections*** or the ***minterms*** generated by the subsets A and B. Note that $I_i \cap I_j = \emptyset, i \neq j$ and $U = \bigcup_{i=0}^{3} I_i$.

Therefore,$P = \{I_0, I_1, I_2, I_3\}$ is a partition of U. The complete intersections or the minterms generated by A and B are the blocks of a partition of U.

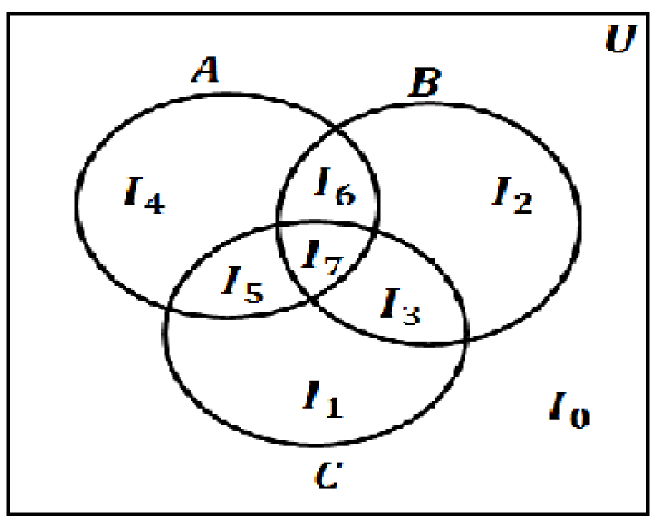


Let A, B and C be three subsets of U and let the 2^3 minterms denoted by I_i, $i = 0,1,2,\dots,7$

$I_0 = A' \cap B' \cap C'$, $I_1 = A' \cap B' \cap C$, $I_2 = A' \cap B \cap C'$, $I_3 = A' \cap B \cap C$,
$I_4 = A \cap B' \cap C'$, $I_5 = A \cap B' \cap C$, $I_6 = A \cap B \cap C'$, $I_7 = A \cap B \cap C$

The subscript of I shows indirectly the minterm under consideration as in the propositional calculus. Note that $I_i \cap I_j = \phi$, $i \neq j$ and $U = \bigcup_{i=0}^{7} I_i$

Therefore $P = \{I_0, I_1, I_2, \dots, I_7\}$ is a partition of U. The minterms generated by A, B and C are the blocks of a partition of U.



In general, if $A_1, A_2, \dots, A_n$ are n subsets of the universal set U, then the complete intersections or minterms generated by these n subsets are denoted by

$I_0, I_1, I_2, \dots, I_{2^n-1}$. These are mutually disjoint and $U = \bigcup_{i=0}^{2^n-1} I_i$

Note: Note the similarity between the minterms defined here and those given in the propositional calculus.

Equivalence relation:

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

Equivalence class: Let R be an equivalence relation on a set A. For any $x \in A$, the set $[x]_R \subseteq X$ defined by

$$[\boldsymbol{x}]_{\boldsymbol{R}} = \{\boldsymbol{y} | \boldsymbol{y} \in \boldsymbol{X} \wedge \boldsymbol{xRy}\}$$

is called an ***R*- equivalence class** generated by $x \in X$.That is, the set $[x]_R$ consists of all the ***R*-relatives** of x in the set A.
Some times $[x]_R$ is also written as x/R.

Properties of equivalence classes

1) $\boldsymbol{x \in [x]_R}$ **, for all** $\boldsymbol{x \in R}$.
   For any $x \in A$, we have xRx (since R is reflexive).Therefore $x \in [x]_R$,$\forall x \in A$.
   That is **each element of A generates an R-equivalence class $[x]_R$ which is nonempty.**
2) $\boldsymbol{[x]_R = [y]_R}$ **iff** $\boldsymbol{xRy}$.
   Suppose $[x]_R = [y]_R$.Clearly, from above $y \in [y]_R$. Therefore, $y \in [x]_R$ and this means xRy.
   Conversely, suppose xRy. If $z \in [y]_R$ then yRz. Now xRy and yRz imply xRz (since R is transitive). Thus, $z \in [x]_R$.Therefore $[y]_R \subseteq [x]_R$ when xRy.
   Further $xRy \Longrightarrow yRx$ (since R is symmetric).Therefore $[y]_R \subseteq [x]_R$.
   Thus , if xRy then $[x]_R = [y]_R$.

3) **If $\boldsymbol{x} \not{R}\, \boldsymbol{y}$ then $[\boldsymbol{x}]_{\boldsymbol{R}} \cap [\boldsymbol{y}]_{\boldsymbol{R}} = \boldsymbol{\phi}$.**
   Assume the contrary, $i.e.$, $[x]_R$ and $[y]_R$ are not disjoint. Therefore, there is at least one element $z \in [x]_R$ and $z \in [y]_R$; i.e., xRz and yRz. Since R is transitive we have xRy. This is a contradiction. The result now follows.

Theorem 1: Every equivalence relation $\boldsymbol{R}$ on a set generates a unique partition of the set. The blocks of this partition correspond to the $\boldsymbol{R}$-equivalence classes.

Proof: Let R be any equivalence relation on a set A. It is known from the properties of the equivalence classes, each element $x \in A$ generates an R- equivalence class which is non empty and any two R- equivalence classes are either disjoint or equal. Thus, the family of R-equivalence classes generated by the elements of A defines a partition P of A.That is the R-equivalence class are the blocks of this partition P. Such a partition P is unique because an R-equivalence class of any element of A is unique. Hence the theorem.

Quotient set: We shall denote the family of equivalence classes of R on A by A/R, (also written as $\boldsymbol{A}$ **modulo** $\boldsymbol{R}$ or $\boldsymbol{A}$ **mod** $\boldsymbol{R}$ (inshort)) called the **quotient set of** $\boldsymbol{A}$ **by** $\boldsymbol{R}$.

Two special equivalence relations:

Consider two special equivalence relations on a set A.

i) The relation $R_1 = A \times A$, *i.e.,* the universal relation on A. Note that every element of A is in R_1-relation to all the elements of A.In this case the quotient set of A by R_1 is the set $\{A\}$.
ii) The relation $R_2 = \{(a, a) | a \in A\}$, i.e., the equality relation or **identity relation** on A. It is an equivalence relation on A and $[a] = \{a\}$ for each $a \in A$ the quotient set of A by R_2 consists of all singleton subsets of A. Note that R_2 generates the largest partition of A.

Example 3: If $\boldsymbol{R}$ is the equivalence relation "*congruence modulo* 5" on Z, then find equivalence classes generated by the elements of Z and the quotient set $\boldsymbol{Z/R}$.

Solution:

$$[0]_R = \{y | y \in \boldsymbol{Z} \ \wedge 0Ry\} = \{y \in \boldsymbol{Z} \ | y \equiv 0(mod\ 5)\}$$

$$= \{y \in \boldsymbol{Z} \ | y = 5k \ , k \in Z\} = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$[1]_R = \{y \in \boldsymbol{Z} \ | yR1\} = \{y \in Z | y \equiv 1(mod\ 5)\}$$

$$= \{y \in \boldsymbol{Z} | y - 1 \ is\ divisible\ by\ 5\} = \{y \in \boldsymbol{Z} \ | y - 1 = 5k \ , k \in \boldsymbol{Z}\}$$

$$= \{y \in \boldsymbol{Z} \ | y = 5k + 1, k \in \boldsymbol{Z}\}$$

$$= \{\dots, -9, -4, 1, 6, 11, \dots\}$$

$$[2]_R = \{y \in \boldsymbol{Z} | y \equiv 2(mod\ 5)\} = \{y \in \boldsymbol{Z} \ | y = 5k + 2, k \in \boldsymbol{Z}\}$$

$$= \{\dots, -8, -3, 2, 7, 12, \dots\}$$

$$[3]_R = \{y \in \boldsymbol{Z} | y \equiv 3(mod\ 5)\} = \{5k + 3 \mid k \in \boldsymbol{Z}\}$$

$$= \{\dots, -7, -2, 3, 8, 13, \dots\}$$

$$[4]_R = \{y \in \boldsymbol{Z} | y \equiv 4(mod\ 5)\} = \{5k + 4 \mid k \in \boldsymbol{Z}\}$$

$$= \{\dots, -6, -1, 4, 9, 14, \dots\}$$

Therefore, the quotient $\boldsymbol{Z}/R$ is a family of an equivalence classes of R on $\boldsymbol{Z}$.
Thus, $\boldsymbol{Z}/R \ = \{[0]_R, [1]_R, [2]_R, [3]_R, [4]_R\}$

In a similar manner we can find the equivalence classes generated by an equivalence relation "*congruence relation modulo* m" on $\boldsymbol{Z}$, where $m \in \boldsymbol{N}, m > 1$.

Example 4: Let S be the set of all well-formed formulas in $\boldsymbol{n}$ proposition variables and let $\boldsymbol{R}$ be the relation given by

$$\boldsymbol{R} = \{(\boldsymbol{a}, \boldsymbol{b}) | \boldsymbol{a} \in \boldsymbol{S} \wedge \boldsymbol{b} \in \boldsymbol{S} \wedge (\boldsymbol{a} \Leftrightarrow \boldsymbol{b})\}$$

Prove that $\boldsymbol{R}$ is an equivalence relation on $\boldsymbol{S}$

Solution: For any $a, b \in S$, a is equivalent to b (written as $a \Leftrightarrow b$ or $a \equiv b$) if a and b have the same truth values in their truth tables, $i.e.$, $a \leftrightarrow b$ is a tautology.

Let R be the propositional equivalence. Let $a, b, c \in S$. Clearly R is reflexive.
If aRb, i.e., a and b have the same truth values in their truth tables then b and a also have the same truth values in their truth tables, i.e., bRa. Thus, R is symmetric.

If aRb and bRc, i.e., a, b have the same entries in their truth tables and b, c have the same entries in their truth tables, then a and c also have the same entries in their truth tables, $i.e.$, aRc. Thus, R is transitive.

Therefore, R is an equivalence relation on S and R partitions S into mutually disjoint equivalence classes.

Note that the set S of all well-formed formulas in n propositional variables is an infinite set.

Observe that there are 2^n rows in the truth table for any formula in n variables. Since each row can have any one of the truth values T or F, we have 2^{2^n} possible truth tables. Every formula in n variables will have one of these 2^{2^n} truth tables. All those formulas which have one of these truth tables are equivalent to each other and are in one R-equivalence class. Since there are 2^{2^n} distinct truth tables, there are 2^{2^n} R-equivalence classes generated by the elements of S.

Converse of Theorem 1

So far we have considered the partition of a set A generated by an equivalence relation on A. We now show that the converse of Theorem 1 is also true. That is, if we start with a definite partition P of a given set A, then we can define an equivalence relation R with $A/R = P$.

Theorem 2: If P is any partition of a set A then there is an equivalence relation R on A whose equivalence classes are the blocks of the partition P.

Proof: Let $P = \{A_1, A_2, \ldots, A_m\}$ be a partition of A. That is $A_i \cap A_j = \phi, i \neq j$ and $\bigcup_{i=1}^{m} A_i = A$. For each $x \in A$ there is a block say A_1 of P such that $x \in A_1$. Evidently x does not belong to any other block of P.

We now take all the elements of $A_1 \times A_1$ as members of a relation R. Clearly, every element of A that is in A_1 is R-related to every other element of A_1. Further, no other element of A which is not in A_1 is related to the elements of A_1. Similarly, we take other blocks A_i , $i = 2,3, \ldots, m$ and take all the elements of $A_i \times A_i$ as member of R. Then

$$R = (A_1 \times A_1) \cup (A_2 \times A_2) \cup \ldots \cup (A_m \times A_m)$$

It is straight forward to check R is an equivalence relation on A and for any $a_i \in A_i$, $i = 1,2, \ldots, m$. We see

$$[a_i]_R = \{y \in A | yRa_i\} = A_i \text{ and}$$

$$A/R = \{[a_i]_R | i = 1,2, \ldots, m\} = \{A_1, A_2, \ldots, A_m\} = P$$

Hence the theorem.

Theorem 1 and Theorem 2 together proves the following result:

An equivalence relation on a set generates a partition of the set and conversely

Example 5: Let $A = \{a, b, c, d, e\}$ and let $P = \{\{a, b\}, \{c\}, \{d, e\}\}$. Obtain the equivalence relation defined by P.

Solution: Let R be the equivalence relation defined by the partition $P = \{A_1, A_2, \ldots, A_m\}$. Then $R = (A_1 \times A_1) \cup (A_2 \times A_2) \cup \ldots \cup (A_m \times A_m)$.

The required equivalence relation is

$$R = \{\{a, b\} \times \{a, b\}\} \cup \{\{c\} \times \{c\}\} \cup \{\{d, e\} \times \{d, e\}\}$$

$= \{(a,a),(a,b),(b,a),(b,b),(c,c),(d,d),(d,e),(e,d),(e,e)\}$

Compatibility Relations

A relation R on a set A is said to be a ***Compatibility relation*** if it is reflexive and symmetric.

Let R be a compatibility relation on A and $x, y \in A$, we say that x, y are **compatible** if xRy. A compatibility relation is sometimes denoted by $\approx$.

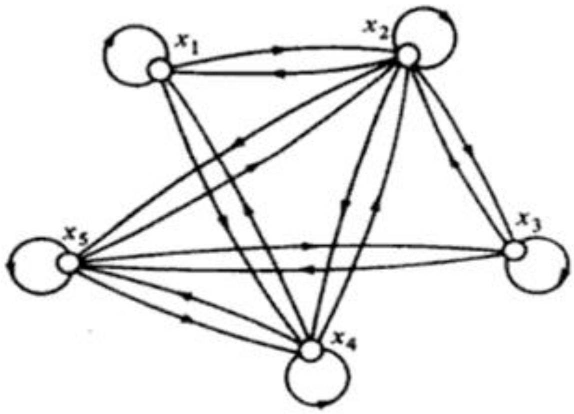
Compatibility relations are useful in solving certain minimization problems of switching theory, particularly for incompletely specified minimization problems.

Evidently all equivalence relations are compatibility relations. We are concerned with those compatibility relations which are not equivalent relations.

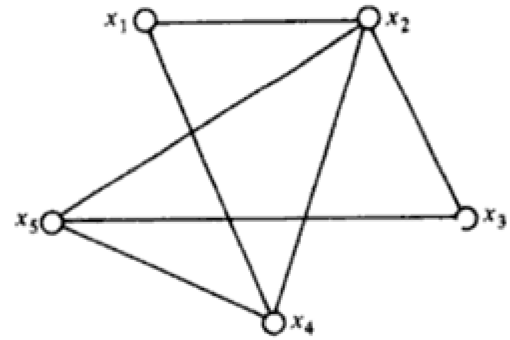
Example 6: Let $\boldsymbol{A = \{ball, bed, dog, let, egg\}}$ and let $\boldsymbol{R}$ be a relation on $\boldsymbol{X}$ given by for $\boldsymbol{x, y \in A, xRy}$ iff $\boldsymbol{x}$ and $\boldsymbol{y}$ contain some common letter.

Clearly R is reflexive. If xRy $i.e.$, x and y contain some common letter, then y and x contain the same common letter $i.e.$, yRx. This shows that R is symmetric. Thus, R is a compatibility relation on A. Note that *ball* ≈ *bed* and *bed* ≈ *egg* but *ball* ≉ *egg*. This shows that ≈ is not transitive.

Thus, R is a compatibility relation. Denote "ball", "bed" , "dog", "let" and "egg" by x_1, x_2, x_3, x_4 and x_5 respectively. The graph of the compatibility relation ≈ on A is given below.



(i)



(ii) Simplified graph of compatibility relation

Since $\approx$ is a compatibility relation, it is not necessary to draw the loops at each node nor is it necessary to draw both the arcs xRy and yRx. Thus ,we can simplify the graph of $\approx$ on A as shown in the figure (ii)

The relation matrix of a compatibility relation is symmetric and has diagonal elements unity. It is therefore, sufficient to give only the elements of the lower triangular part of the relational matrix in such a case. For this compatibility relation, the relation matrix is given below.

x_2	1			
x_3	0	1		
x_4	1	1	0	
x_5	0	1	1	1
	x_1	x_2	x_3	x_4

Note that the elements in each of the sets $\{x_1, x_2, x_4\}$ and $\{x_2, x_3, x_5\}$ are mutually compatible. Notice that the union of these two sets is A. Therefore, $\{\{x_1, x_2, x_4\}, \{x_2, x_3, x_5\}\}$ is a covering of A. It may be seen that the elements of the set $\{x_2, x_4, x_5\}$ are also mutually compatible.

An equivalence relation on a set A defines a partition of A into equivalence classes and a compatibility relation does not necessarily define a partition. However, a compatibility relation on A defines a covering of the set A.

Maximal compatibility block

Let A be a set and $\approx$ a compatibility relation on A. A subset $M \subseteq A$ is called a ***maximal compatibility block*** if any element of M is compatible to every other element of M and no element of $X - M$ is compatible to all the elements of M. From figure (ii) that the subsets $\{x_1, x_2, x_4\}, \{x_2, x_3, x_5\}$ and $\{x_2, x_4, x_5\}$ are maximal compatible blocks.

There are two procedures to find the maximal compatibility block.

Procedure 1

To find the maximal compatibility blocks corresponding to a compatibility relation R on a set A, first draw a simplified graph of R and pick from this graph the **largest complete polygons**. By a largest complete polygon we mean a polygon in which any vertex is connected to every other vertex. The set of elements of A which are the vertices of these largest complete polygons are the maximal compatibility blocks of R. In addition to these largest complete polygons, any element of A which is related only to itself forms a maximal compatibility block. Also, any two elements which are compatible to one another but not compatible to any other elements is a maximal compatibility block.

Procedure 2

This procedure is to find maximal compatibility block from the table of the relation matrix.

First delete all the elements which are only compatible to themselves and obtain the simplified table of the relation matrix, because they are in a maximal compatible block by themselves and are in no other compatibility block. Such blocks are listed at the end.

Step 1: Start in the right most column of the table and proceed to the left until a column containing at least one nonzero entry is encountered. List all the compatible pairs represented by the entries in that column.

Step 2: Proceed left to the next column that contains at least one nonzero entry.

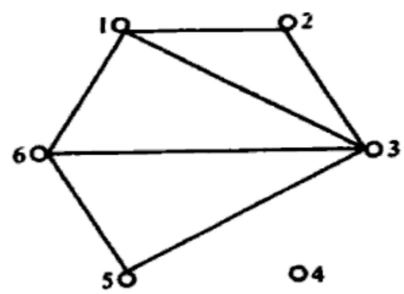
a) If any element is compatible to all the members of some previously defined compatibility class, then add this element to that class.
b) If a member is compatible to only some members of a previously defined class, then form a new class which includes all the elements that are compatible.

Next, list all the compatible pairs not included in any previously defined class.

Step 3: Repeat step 2 until all the columns are considered.

The final sets of compatibility classes including those which are isolated elements constitute the maximal compatibility classes (blocks).

Example 7: The graph of a compatibility relation is given below. Write its relation matrix and find its maximal compatibility block.



Solution: We have $A = \{1,2,3,4,5,6\}$ and Its relation matrix is

2	1				
3	1	1			
4	0	0	0		
5	0	0	1	0	
6	1	0	1	0	1
	1	2	3	4	5

Procedure 1

The largest complete polygons are $\{1,2,3\}, \{1,3,6\}, \{3,5,6\}$ and these are maximal compatibility blocks. $\{4\}$ is also a m.c.b. Note that 4 is an isolated node.

Procedure 2

We delete all the elements which are only compatible to themselves. That is we denote the element 4, because 4 is only compatible to itself. The node 4 is an isolated node. Now, the simplified table of the relation matrix is

2	1			
3	1	1		
5	0	0	1	
6	1	0	1	1
	1	2	3	5

Step 1: $(5,6)$

$(3,6), (3,5)$

Step 2: $(5,6), (3,5), (3,6)$ 2(a) Since 3 is compatible with all the elements of the previously defined class $i.e., \{5,6\}$.

$(5,6), (3,5), (3,6)$

Step 2:

$(2,3)$

$(5,6), (3,5), (3,6)$

$(2,3)$

Step 2:

$(1,2),(1,3),(1,6)$

———————————————————————

$(5,6),(3,5),(3,6)$

$(2,3),(1,2),(1,3)$

$(1,6)$

———————————————————————

$(5,6),(3,5),(3,6)$

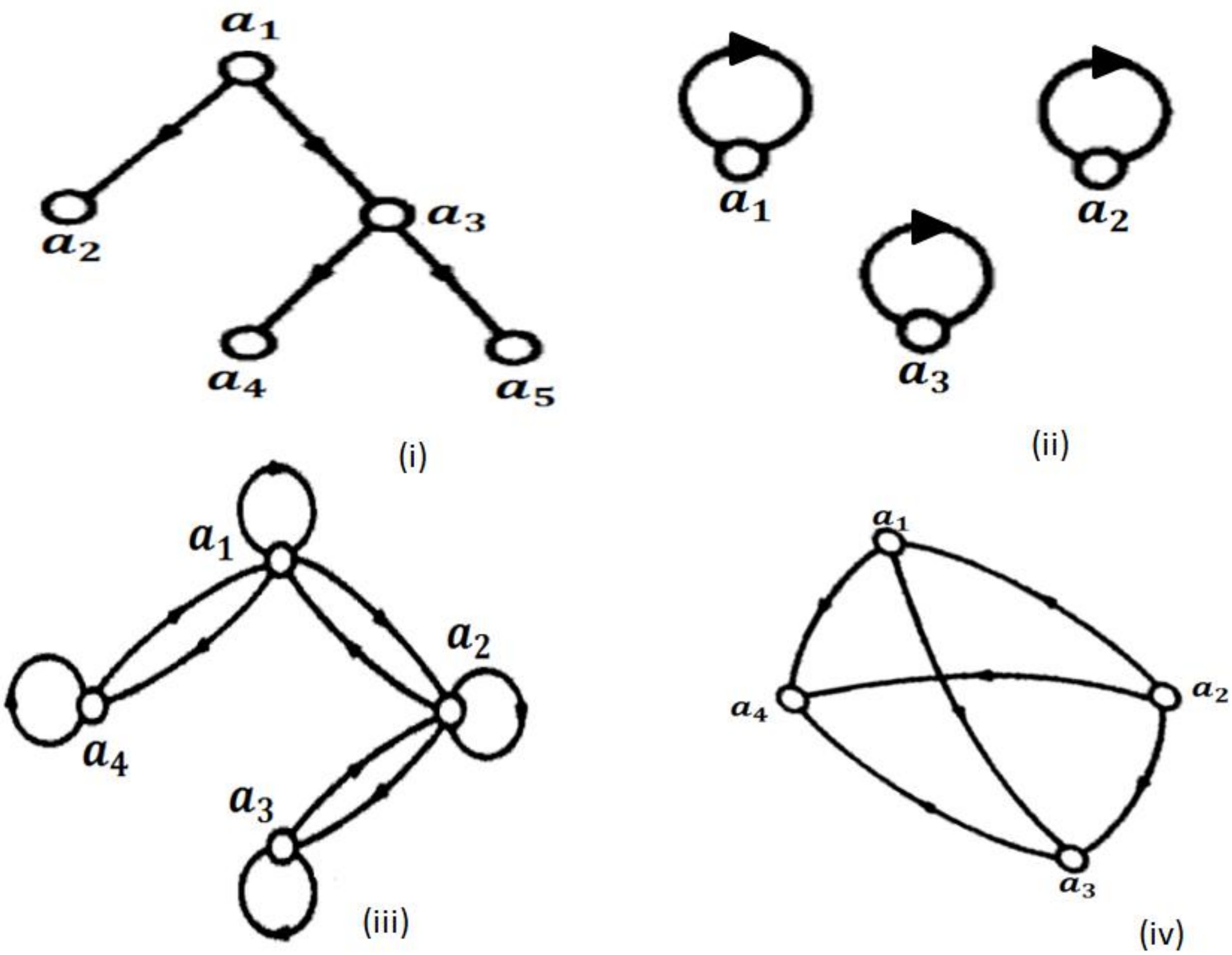
$(2,3),(1,2),(1,3)$

$(1,2),(1,3),(1,6)$ 2(b)

The m.c.bs are $\{3,5,6\}$, $\{1,2,3\}$, $\{1,3,6\}$ and $\{4\}$

P1:

Determine the property of the relations given by the following graphs and also write the corresponding relation matrices.



Solution:

i) The relation corresponding to the graph given by figure (i) is $R_1 = \{(a_1, a_2), (a_1, a_3), (a_3, a_4), (a_3, a_5)\}$ on $A = \{a_1, a_2, a_3, a_4, a_5\}$ and its corresponding relation matrix is

$$M_{R_1} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

It is irreflexive, antisymmetric and not transitive

ii) The relation corresponding to the graph given by figure (ii) is $R_2 = \{(a_1, a_1), (a_2, a_2), (a_3, a_3)\}$ on $A = \{a_1, a_2, a_3\}$ and its corresponding relation matrix is

$$M_{R_2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

It is reflexive, symmetric and transitive.

iii) The relation corresponding to the graph given by figure (iii) is

$$R_3 = \begin{Bmatrix} (a_1, a_1), (a_1, a_2), (a_1, a_4), (a_2, a_1), (a_2, a_2), (a_2, a_3), (a_3, a_2), (a_3, a_3), (a_4, a_1) \\ , (a_4, a_4) \end{Bmatrix}$$

on $A = \{a_1, a_2, a_3, a_4\}$ and its corresponding relation matrix is

$$M_{R_3} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

It is reflexive, symmetric and not transitive.

iv) The relation corresponding to the graph given by figure (iv) is $R_4 = \{(a_1, a_3), (a_1, a_4), (a_2, a_1), (a_2, a_3), (a_2, a_4), (a_3, a_4)\}$ on $A = \{a_1, a_2, a_3, a_4\}$ and its corresponding relation matrix is

$$M_{R_4} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

It is irreflexive, antisymmetric and transitive.

P2:

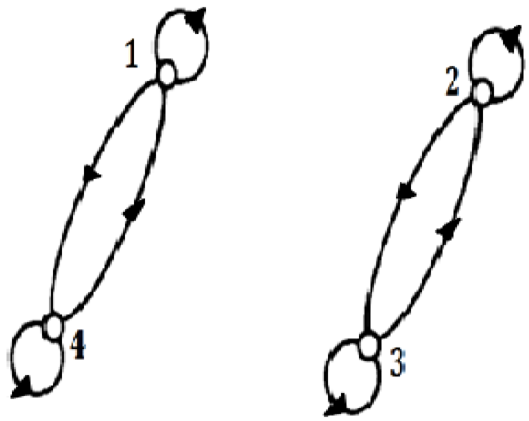
Let $A = \{1, 2, 3, 4\}$ and

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

Show that R is an equivalence relation through its relation matrix and graph.
Find the quotient set A/R for the example

Solution:

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



Note that the diagonal entries of M_R are all 1, and M_R is a symmetric matrix. Therefore, R is reflexive and symmetric. Further, it is transitive. Thus, R is an equivalence relation. The equivalence classes are

$$[1]_R = \{y | y \in A \ \wedge 1Ry\} = \{1,4\}$$

$$[2]_R = \{y | y \in A \ \wedge 2Ry\} = \{2,3\}$$

Therefore , $A/R = \{[1]_R, [2]_R\} = \{\{1,4\}, \{2,3\}\}$

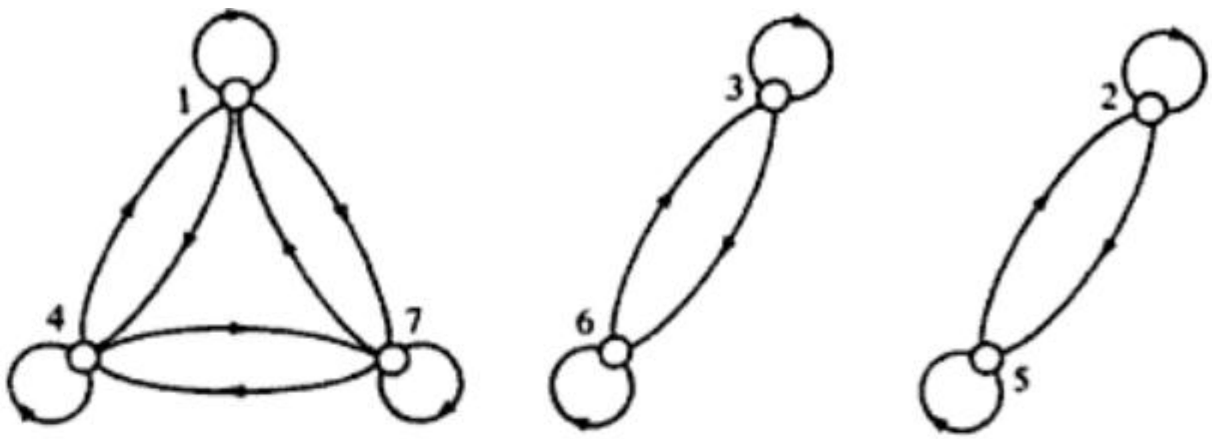
P3:

Let $A = \{1, 2, 3, \dots, 7\}$ and $R = \{(x, y) | x \equiv y (mod\ 3)\}$.

Show that R is an equivalence relation through its graph. Find the quotient set A/R for the example.

Solution: We have

$$R = \left\{ \begin{matrix} (1,1), (1,4), (1,7), (2,2), (2,5), (3,3), (3,6), (4,1), (4,4), (4,7), (5,2), (5,5), (6,3), (6,6), \\ (7,1), (7,4), (7,7) \end{matrix} \right\}$$



Clearly R is reflexive and symmetric. Further R is transitive. Thus R is an equivalence relation. The equivalence classes are

$$[1]_R = \{y | y \in A\ \wedge 1Ry\} = \{1,4,7\}$$

$$[2]_R = \{y | y \in A\ \wedge 2Ry\} = \{2,5\}$$

$$[3]_R = \{y | y \in A\ \wedge 3Ry\} = \{3,6\}$$

Therefore , $A/R = \{[1]_R, [2]_R, [3]_R\} = \{\{1,4,7\}, \{2,5\}, \{3,6\}\}$

P4:

Obtain the equivalence relation defined by the partition $\boldsymbol{P = \{A_1, A_2, A_3\}}$ of the set $\boldsymbol{A = \{1, 2, 3, 4, 5, 6\}}$, where $\boldsymbol{A_1 = \{1, 2, 3\}}$, $\boldsymbol{A_2 = \{4, 5\}}$ and $\boldsymbol{A_3 = \{6\}}$

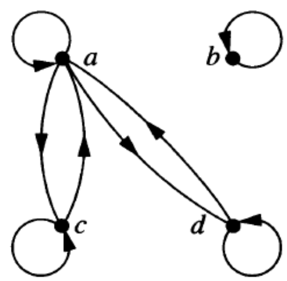
Solution:

Let R be the equivalence relation defined by the partition $P = \{A_1, A_2, A_3\}$ of A.
Then $R = (A_1 \times A_1) \cup (A_2 \times A_2) \times (A_3 \times A_3)$

$$R = \left\{ \begin{matrix} (1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), \\ (3,3), (4,4), (4,5), (5,4), (5,5), (6,6) \end{matrix} \right\}$$

P5:

Determine whether the relation R represented by the following digraph is an equivalence relation. If R is an equivalence relation then find its quotient set



Solution:

Let R be the relation on $A = \{a, b, c, d\}$ represented by the given graph and M_R be its relation matrix. Then

$$R = \{(a, a), (a, c), (a, d), (b, b), (c, a), (c, c), (d, a), (d, d)\}$$

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

From the diagraph, we see that there is a loop at every node. Therefore R is reflexive. From M_R we see that $(M_R)^T = M_R$. Therefore M_R is a symmetric matrix and thus R is a symmetric relation. Further, R is symmetric. Therefore, R is an equivalence relation. The equivalence classes are

$$[a]_R = \{x \in A | x\ R\ a\} = \{a, b, c, d\}$$

$$[b]_R = \{x \in A | x\ R\ b\} = \{b\}$$

Therefore the quotient set is

$$A/R = \{[a]_R, [b]_R\} = \{\{a, c, d\}, \{b\}\}$$

P6:

Determine the number of equivalence relations on a set with three elements.

Solution:

It is known that every equivalence relation on a set generates a unique partition of the set. Conversely if P is any partition on a set then there is an equivalence relation on the set.

That is an equivalence relation on a set generates a partition of the set and conversely.

From this it follows that the number of equivalence relation on a finite set A is the number of partitions of A:

Let $A = \{a, b, c\}$. We now list all partitions of A:

$$P_1 = \{\{a\}, \{b\}, \{c\}\}$$

$$P_2 = \{\{a\}, \{b, c\}\}$$

$$P_3 = \{\{b\}, \{a, c\}\}$$

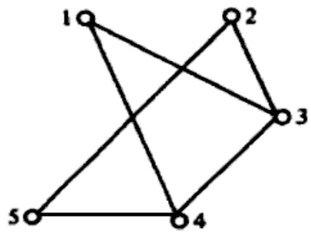
$$P_4 = \{\{c\}, \{a, b\}\}$$

$$P_5 = \{\{a, b, c\}\}$$

Thus there are five equivalence relations on a set with three elements.

P7:

The graph of a compatibility relation is given below. Write its relation matrix and find its maximal compatibility blocks.



Solution: We have $A = \{1,2,3,4,5\}$

The relation matrix is

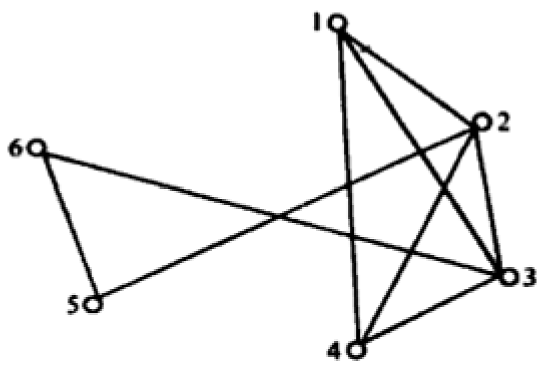
2	0			
3	1	1		
4	1	0	1	
5	0	1	0	1
	1	2	3	4

The largest complete polygon is $\{1,3,4\}$. Therefore it is maximal compatibility block. The other m.c.bs are $\{2,3\}, \{4,5\}, \{2,5\}$

Obtain the m.c.bs by procedure 2 (Do it !)

P8:

The graph of a compatibility relation is given below. Write its relation matrix and find its maximal compatibility blocks.



Solution: We have $A = \{1,2,3,4,5,6\}$

The relation matrix is

2	1				
3	1	1			
4	1	1	1		
5	0	1	0	0	
6	0	0	1	0	1
	1	2	3	4	5

The largest complete polygon is $\{1,2,3,4\}$ and it is a maximal compatibility block. The other m.c.bs are $\{2,5\}, \{3,6\}, \{5,6\}$

Obtain the m.c.bs by procedure 2 (Do it !)

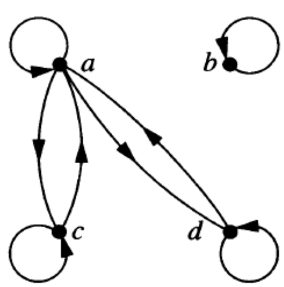
2.3. Equivalence relations and Compatibility relations

Exercise:

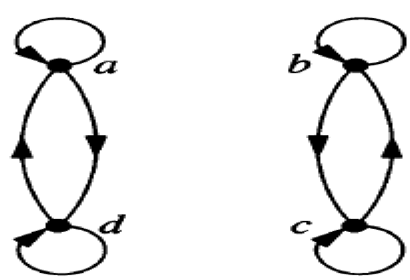
1. Show that the relation of logical equivalence on the set of all compound propositions is an equivalence relation. What are the equivalence classes of F and of T?
2. Suppose that A is a nonempty set, and f is a function that has A as its domain. Let R be the relation on A consisting of all ordered pairs (x, y) such that $f(x) = f(y)$.
   a. Show that R is an equivalence relation on A.
   b. What are the equivalence classes of R?

3. Determine whether the relation with the directed graphs shown below is an equivalence relation.

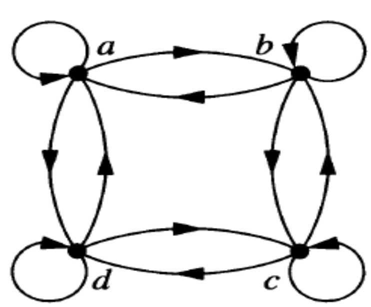
i)



ii)



iii)



4. Determine whether the relations represented by these zero-one matrices are equivalence relations.
   a. $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$
   b. $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
   c. $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

5. Which of these collections of subsets are partitions of $\{1,2,3,4,5,6\}$?
   a. $\{1,2\},\{2,3,4\},\{4,5,6\}$
   b. $\{1\},\{2,3,6\},\{4\},\{5\}$
   c. $\{2,4,6\},\{1,3,5\}$
   d. $\{1,4,5\},\{2,6\}$

6. List the ordered pairs in the equivalence relations produced by these partitions of $\{0,1,2,3,4,5\}$. Draw the corresponding digraphs.
   a. $\{0\},\{1,2\},\{3,4,5\}$
   b. $\{0,1\},\{2,3\},\{4,5\}$
   c. $\{0,1,2\},\{3,4,5\}$
   d. $\{0\},\{1\},\{2\},\{3\},\{4\},\{5\}$

7. Determine the number of different equivalence relations on a set with five elements by listing them.

.

MODULE-4

Transitive closure

2.4

Transitive closure

In this module we discuss composition of binary relation, Boolean matrices and transitive closure of a relation on a set.

Composition of Binary Relation

Let A, B and C be sets. Let R be a relation from A to B and S be a relation from B to C. Then a relation, written as $\boldsymbol{R \circ S}$, is called a **composition** of R and S is defined as

$$\boldsymbol{R \circ S = \{(x, z) | x \in A \wedge z \in C \wedge (\exists y)(y \in B \wedge (x, y) \in R \wedge (y, z) \in S)\}}$$

The operation of obtaining $R \circ S$ from R and S is called **composition** of relations.

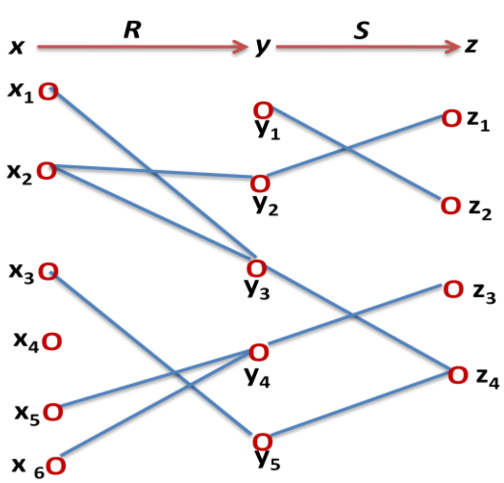
Note:

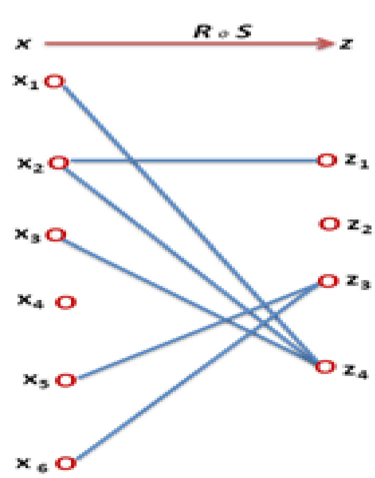
(i) $R \circ S = \phi$,if the intersection of range of R and the domain of S is empty.

(ii) $R \circ S \neq \phi$, if there exists at least one ordered pair $(x, y) \in R$ such $y \in B$ is a first component in an ordered pair in S.

(iii) Domain of $R \circ S$ is a subset of A and its range is a subset of C. In fact, the $D(R \circ S) \subseteq D(R)$ and $\boldsymbol{R}(R \circ S) \subseteq \boldsymbol{R}(S)$.

From the graphs of R and S we can easily construct the graph of $R \circ S$.





The operation of composition of relations produces a relation from two relations. Therefore, the operation of composition is a binary operation. The same operation can be applied again to produce other relations. For example let R, S and P be relations from A to B, from B to C and from C to D respectively. Then we can also form $(R \circ S) \circ P$, which is a relation from A to D. Similarly, we can also form $R \circ (S \circ P)$, which is also a relation from A to D.

Lemma: The operation of composition on relations is associative.

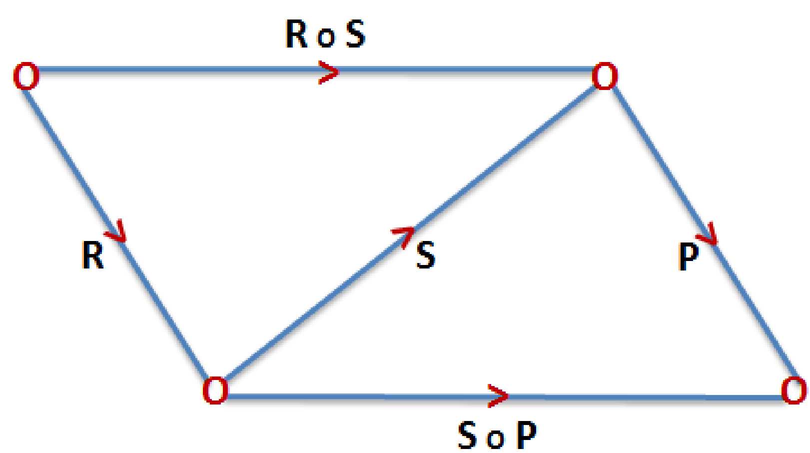
$i.e.$, if R, S and P be any relations defined above then

$$(\boldsymbol{R} \circ \boldsymbol{S}) \circ \boldsymbol{P} = \boldsymbol{R} \circ (\boldsymbol{S} \circ \boldsymbol{P})$$

Proof: Assume that $(R \circ S) \circ P$ is nonempty. Let $(x, y) \in R$, $(y, z) \in S$ and $(z, w) \in P$. This means that $(x, z) \in R \circ S$ and $(x, w) \in (R \circ S) \circ P$. Also note that $(y, w) \in S \circ P$ and $(x, w) \in R \circ (S \circ P)$.

This shows that $(R \circ S) \circ P \subseteq R \circ (S \circ P)$. In a similar manner we show that $R \circ (S \circ P) \subseteq (R \circ S) \circ P$. Thus, $(R \circ S) \circ P = R \circ (S \circ P)$. Therefore, the operation of composition on relations is associative.

The above result follows from the following partial graph:



Since the composition of relations is associative, we may delete parenthesis, so that $R \circ (S \circ P) = (R \circ S) \circ P = R \circ S \circ P$.

Example 1: Let $A = \{1, 2, 3, 4, 5\}$.Let R and S be relations on A defined by

$$\boldsymbol{R} = \{(\mathbf{1},\mathbf{2}),(\mathbf{2},\mathbf{2}),(\mathbf{3},\mathbf{4})\}$$

$$\boldsymbol{S} = \{(\mathbf{4},\mathbf{2}),(\mathbf{2},\mathbf{5}),(\mathbf{3},\mathbf{1}),(\mathbf{1},\mathbf{3})\}$$

Find $R \circ R$, $S \circ S$, $R \circ S$, $S \circ R$, $R \circ (S \circ R)$, $(R \circ S) \circ R$ and $R \circ R \circ R$.

Solution:

(i) $R \circ R = \{(1,2),(2,2),(3,4)\} \circ \{(1,2),(2,2),(3,4)\} = \{(1,2),(2,2)\}$

(ii) $S \circ S = \{(1,3),(2,5),(3,1),(4,2)\} \circ \{(1,3),(2,5),(3,1),(4,2)\}$

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

(iii) $R \circ S = \{(1,2),(2,2),(3,4)\} \circ \{(1,3),(2,5),(3,1),(4,2)\}$

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

(iv) $S \circ R = \{(1,3),(2,5),(3,1),(4,2)\} \circ \{(1,2),(2,2),(3,4)\}$

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

Note that $R \circ S \neq S \circ R$

(v) $(R \circ S) \circ R = \{(1,5),(2,5),(3,2)\} \circ \{(1,2),(2,2),(3,4)\} = \{(3,2)\}$

(vi) $R \circ (S \circ R) = \{(1,2),(2,2),(3,4)\} \circ \{(1,4),(3,2),(4,2)\}$

$= \{(3,2)\} = (R \circ S) \circ R$

(vii) $R \circ R \circ R$

$= \{(1,2),(2,2),(3,4)\} \circ \{(1,2),(2,2)\}$

$= \{(1,2),(2,2)\}$

Boolean Matrix

A matrix whose entries are bits (i.e., 0 and 1) is called a Boolean Matrix. That is $M = (m_{ij})_{m \times n}$ is a Boolean matrix if $m_{ij} = 0 \; or \; 1$ for all i and j.

Join and Meet

The ***Join*** of the Boolean matrices $M = (m_{ij})_{m\times n}$ and $N = (n_{ij})_{m\times n}$, denoted by $\boldsymbol{M} \vee \boldsymbol{N}$, is defined by $M \vee N = (m_{ij} \vee n_{ij})_{m\times n}$

The ***Meet*** of the Boolean matrices $M = (m_{ij})_{m\times n}$ and $N = (n_{ij})_{m\times n}$, denoted by $\boldsymbol{M} \wedge \boldsymbol{N}$, is defined by $M \wedge N = (m_{ij} \wedge n_{ij})_{m\times n}$

Example 2: Let $\boldsymbol{M} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}$ and $\boldsymbol{N} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} \end{bmatrix}$ then find $\boldsymbol{M} \vee \boldsymbol{N}$ and $\boldsymbol{M} \wedge \boldsymbol{N}$.

Solution: $M \vee N = \begin{bmatrix} 1 \vee 0 & 0 \vee 0 & 1 \vee 1 \\ 0 \vee 1 & 1 \vee 0 & 0 \vee 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

$$M \wedge N = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 0 & 1 \wedge 1 \\ 0 \wedge 1 & 1 \wedge 0 & 0 \wedge 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Note: If R is a relation from a finite set A to a finite set B then its relation matrix M_R is a Boolean matrix

If R and S are relations from a finite set A to a finite set B with respective relation matrices M_R and M_S then

$$\boldsymbol{M_{R\cup S}} = \boldsymbol{M_R} \vee \boldsymbol{M_S}$$

$$\boldsymbol{M_{R\cap S}} = \boldsymbol{M_R} \wedge \boldsymbol{M_S}$$

Boolean Product

The ***Boolean product*** of the Boolean matrices $P = (p_{ij})_{m\times n}$ and $Q = (q_{ij})_{n\times p}$, denoted by $\boldsymbol{P \circ Q}$ (or $\boldsymbol{P \odot Q}$)is the matrix $R = (r_{ij})_{m\times p}$, where

$$\boldsymbol{r_{ij} = (p_{i1} \wedge q_{1j}) \vee (p_{i2} \wedge q_{2j}) \vee \ldots \vee (p_{in} \wedge q_{nj}) = \bigvee_{k=1}^{n} (p_{ik} \wedge q_{kj})},$$

$$i = 1, 2, 3, \ldots, m \;\; ; \;\; j = 1, 2, 3, \ldots, p$$

where $p_{ik} \wedge q_{kj}$ and $\bigvee_{k=1}^{n}$ indicate **bit-ANDing** and **bit- ORing** respectively.

Example 3: let $P = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ and $= \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$, then find $P \circ Q$ and $Q \circ P$, if it is defined.

Solution: (i) Since the number of columns in P is equal to the number of rows of Q, $P \circ Q$ is defined.

$$P \circ Q = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 1) \vee (1 \wedge 0) & (1 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 0) \\ (0 \wedge 1) \vee (1 \wedge 1) \vee (0 \wedge 0) & (0 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 0) \end{bmatrix}$$

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

(i) Since the number of columns in Q is equal to the number of rows of P, $Q \circ P$ is defined.

$$Q \circ P = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 0) \vee (0 \wedge 1) & (1 \wedge 1) \vee (0 \wedge 0) \\ (1 \wedge 1) \vee (1 \wedge 0) & (1 \wedge 0) \vee (1 \wedge 1) & (1 \wedge 1) \vee (1 \wedge 0) \\ (0 \wedge 1) \vee (0 \wedge 0) & (0 \wedge 0) \vee (0 \wedge 1) & (0 \wedge 1) \vee (0 \wedge 0) \end{bmatrix}$$

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

Boolean Power of a Boolean Matrix

Let M be an $m \times m$ boolean matrix and n is any nonnegative integer. The $\boldsymbol{n^{th}}$ **Boolean power of $\boldsymbol{M}$**, denoted by M^n or (sometimes $M^{[n]}$) defined recursively as follows:

$\boldsymbol{M^0} = \boldsymbol{I_m}$ (where I_m is the $m \times m$ identity matrix) $\boldsymbol{M^n = M^{n-1} \circ M,\ \ if\ n \geq 1}$

Example 4: if $\boldsymbol{M} = \begin{bmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$ then compute $\boldsymbol{M^2}$ and $\boldsymbol{M^3}$

Solution:

$$M^2 = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \qquad \text{(do it!)}$$

$$M^3 = M^2 \circ M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \text{ (do it!)}$$

Note: If A, B and C are Boolean matrices then

i) $A \vee A = A$, $A \wedge A = A$
ii) $A \vee B = B \vee A$, $A \wedge B = B \wedge A$
iii) $A \vee (B \vee C) = (A \vee B) \vee C$, $A \wedge (B \wedge C) = (A \wedge B) \wedge C$
iv) $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$, $A \vee (B \wedge C) = (A \vee B) \vee (A \vee C)$
v) $A \circ (B \circ C) = (A \circ B) \circ C$

Matrix of the composite relation

Let $A = \{a_1, a_2, \ldots, a_m\}, B = \{b_1, b_2, \ldots, b_n\}$ and $C = \{c_1, c_2, \ldots, c_p\}$

Let R be a relation from A to B and S be a relation from B to C then the relation matrices M_R and M_S are $m \times n$ and $n \times p$ (zero- one) matrices. The relation matrix of the relation $R \circ S$ can be obtained from the matrices M_R and M_S in the following manner

$$\boldsymbol{M_{R \circ S} = M_R \circ M_S}$$

Example 5: Let $A = \{a_1, a_2, a_3, a_4, a_5\}$ and R, S be relations on A given by

$$\boldsymbol{R = \{(a_1, a_2), (a_2, a_2), (a_3, a_4)\}}$$

$$\boldsymbol{S = \{(a_1, a_3), (a_2, a_5), (a_3, a_1), (a_4, a_2)\}}$$

Compute $M_{R \circ S}$ and $M_{S \circ R}$

Solution:

To compute $M_{R \circ S}$ and $M_{S \circ R}$, we first write the relation matrices of R and S.

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

Now, $M_{R \circ S} = M_R \circ M_S$

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

$M_{S \circ R} = M_S \circ M_R$

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

Note: Note that $R \circ S = \{(a_1, a_5), (a_2, a_5), (a_3, a_2)\}$

$$S \circ R = \{(a_1, a_4), (a_3, a_2), (a_4, a_2)\}$$

Converse of a relation

Let R be a relation from a set A to a set B . A relation $\overline{\boldsymbol{R}}$ from B to A is called the **converse of** , the ordered pairs of $\overline{R}$ are obtained by interchanging the elements of the ordered pairs of R. That is for $x, y \in R,\ x\,R\,y \Leftrightarrow y\,\overline{R}\,x$ $i.e.,$ $(x, y) \in R$ iff $(y, x) \in \overline{R}$. From the definition it follows that $\overline{\overline{R}} = R$. The relation matrix $M_{\overline{R}}$ of $\overline{R}$ is obtained by interchanging the rows and columns of M_R. That is $M_{\overline{R}}$ is the transpose of M_R. That is, $\boldsymbol{M_{\overline{R}}} = (\boldsymbol{M_R})'$. Further, the graph of $\overline{R}$ is obtained from the graph of R by reversing the arrow on each arc.

Converse of a composite relation

Theorem: If $\boldsymbol{R}$ is a relation from $\boldsymbol{A}$ to $\boldsymbol{B}$ and $\boldsymbol{S}$ is a relation from $\boldsymbol{B}$ to $\boldsymbol{C}$ then $\overline{\boldsymbol{R} \circ \boldsymbol{S}} = \overline{\boldsymbol{S}} \circ \overline{\boldsymbol{R}}$.

Proof: Now, $R \circ S$ is a relation from A to C and its converse $\overline{R \circ S}$ is a relation from C to A. Since $\overline{S}$ is a relation form C to A, $\overline{R}$ from B to A ; $\overline{S} \circ \overline{R}$ is a relation from C to A.
Let $x \in A$ and $z \in C$ be arbitrary elements. Suppose that there is an element $y \in B$ such that xRy and ySz. Then $x(R \circ S)z$ and $z\left(\overline{R \circ S}\right)x$.
Further, $x\,R\,y$ and $y\,S\,z \implies z\,\overline{S}\,y$ and $y\,\overline{R}\,x \implies z\left(\overline{S} \circ \overline{R}\right)x$.
For any $x \in A$ and $z \in C$, $z\left(\overline{R \circ S}\right)x \implies x(R \circ S)z \implies \exists\, y \in B$ such that $x\,R\,y$ and $y\,S\,z \implies z\left(\overline{S} \circ \overline{R}\right)x$ (shown as above) .Therefore, $\overline{R \circ S} \subseteq \overline{S} \circ \overline{R}$

Conversely for any $x \in A$ and $z \in C$, $z\left(\overline{S} \circ \overline{R}\right)x \implies \exists\, y \in B$ such that $z\,\overline{S}y$ and $y\,\overline{R}\,x$

$\implies x\,R\,y$ and $y\,Sz \implies x(R \circ S)\,z \implies z\,\left(\overline{R \circ S}\right)\,x$.Therefore, $\overline{S} \circ \overline{R} \subseteq \overline{R \circ S}$

Thus, $\overline{R \circ S} = \overline{S} \circ \overline{R}$. Hence the result

The same rule can be expressed in terms of the relation matrices by saying that the **transpose of $\boldsymbol{M_{R \circ S}}$ is the same as the matrix $\boldsymbol{M_{\overline{S} \circ \overline{R}}}$** .The matrix $M_{\overline{S} \circ \overline{R}}$ can be obtained from the matrices $M_{\overline{S}}$ and $M_{\overline{R}}$, which in turn can be obtained from M_S and M_R.

Note: $\boldsymbol{M_{\overline{R \circ S}} = (M_{R \circ S})' = (M_R \circ M_S)' = M_S{}' \circ M_R{}' = M_{\overline{S}} \circ M_{\overline{R}} = M_{\overline{S} \circ \overline{R}}}$.

Example 6: If $\boldsymbol{M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}}$ **and** $\boldsymbol{M_S = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}}$

Then show that $\boldsymbol{M_{\overline{R \circ S}} = M_{\overline{S}} \circ M_{\overline{R}}}$**.**

Solution:

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

Now, $M_{\overline{R \circ S}} = (M_{R \circ S})' = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

We have, $M_{\overline{S}} = (M_S)' = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

$$M_{\overline{R}} = (M_R)' = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Now, $M_{\overline{S}} \circ M_{\overline{R}} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

Thus, $M_{\overline{R \circ S}} = M_{\overline{S} \circ \overline{R}}$.

The following hold for any relations R and S.

Theorem 1: For any relations R and S, the following hold:

(i) $\overline{\overline{R}} = R$

(ii) $R = S \Leftrightarrow \overline{R} = \overline{S}$

(iii) $R \subseteq S \Leftrightarrow \overline{R} \subseteq \overline{S}$

(iv) $\overline{R \cup S} = \overline{R} \cup \overline{S}$

(v) $\overline{R \cap S} = \overline{R} \cap \overline{S}$

Consider the following distinct relations R_1, R_2, R_3 and R_4 on a set $A = \{a, b, c\}$

$$R_1 = \{(a,b),(a,c),(c,b)\}$$

$$R_2 = \{(a,b),(b,c),(c,a)\}$$

$$R_3 = \{(a,b),(b,c),(c,c)\}$$

$$R_4 = \{(a,b),(b,a),(c,c)\}$$

Denoting the composition of a relation R by itself as

$R \circ R = R^2$, $R \circ R \circ R = R^2 \circ R = R^3, \ldots, R^{m-1} \circ R = R^m$

Now, $R_1^2 = \{(a,b)\}, R_1^3 = R_1^2 \circ R_1 = \emptyset$, $R_1^4 = R_1^3 \circ R_1 = \emptyset, \ldots$

$R_2^2 = \{(a,c),(b,a),(c,b)\}$, $R_2^3 = R_2^2 \circ R_2 = \{(a,a),(b,b),(c,c)\}$
$R_2^4 = R_2^3 \circ R_2 = R_2$, $R_2^5 = R_2^4 \circ R_2 = R_2 \circ R_2 = R_2^2 = \{(a,c),(b,a),(c,b)\}$

$R_3^2 = \{(a,c),(b,c),(c,c)\}$, $R_3^3 = R_3^2 \circ R_3 = \{(a,c),(b,c),(c,c)\} = R_3^2$

$$R_3^4 = R_3^3 \circ R_3 = R_2^3 \circ R_3 = R_3^3 = R_3^2$$

$$R_4^2 = \{(a,a),(b,b),(c,c)\}, R_4^3 = R_4^2 \circ R_4 = R_4, R_4^4 = R_4^3 \circ R_4 = R_4 \circ R_4 = R_4^2$$

Given a finite set A, containing n elements and a relation R on A, we can interpret $R^m, (m = 1, 2, 3, \ldots, \ldots)$ in terms of its graph. From the examples given above, it is possible to say that ***there are at most n distinct powers of R, for R^m, $m > n$ can be expressed in terms of $R, R^2, \ldots, R^n$***. We now construct the relation on A given by

$$\boldsymbol{R^+ = R \cup R^2 \cup R^3 \cup \ldots \cup R^n}$$

This construction requires only a finite number of powers of R and these computations can easily be performed by using M_R, (the relation matrix of R) and Boolean multiplication of these matrices. Now,

$R_1^+ = R_1 \cup R_1^2 \cup R_1^3 \ = \ R_1$

$R_2^+ = R_2 \cup R_2^2 \cup R_2^3$
$\quad = \{(a, b), (b, c), (c, a), (a\ , c), (b, a), (c, b), (a, a), (b, b), (c, c)\}$

$R_3^+ = R_3 \cup R_3^2 \cup R_3^3 \ = \ R_3 \cup R_3^2$

$\quad = \{(a, b), (b, c), (c, c), (a\ , c)\}$

$R_4^+ = R_4 \cup R_4^2 \cup R_4^3 \ = \ R_4 \cup R_4^2$

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

Notice that the relations R_1^+, R_3^+ and R_4^+ are all transitive and that

$R_i \subseteq R_i^+,\ i = 1, 2, 3, 4$

Further, we see that R_i^+ is obtained from R_i , $(i = 1, 2, 3, 4)$ by adding only those ordered pairs to R_i such that R_i^+ is transitive.

The following is the general definition R^+.

Transitive Closure: Let A be a finite set with n elements and R be a relation on A. The relation

$$\boldsymbol{R^+ = R \cup R^2 \cup R^3 \cup \ldots \cup R^n}$$

on A is called the **transitive closure** of R on A.

The properties of transitive closure of a relation on a set are highlighted in the following theorem

Theorem 2: Let $\boldsymbol{R}$ be a relation on a finite set $\boldsymbol{A}$

(i) The transitive closure $\boldsymbol{R^+}$ of $\boldsymbol{R}$ is transitive

(ii) If $\boldsymbol{P}$ is any other transitive relation on $\boldsymbol{A}$ such that $\boldsymbol{R \subseteq P}$ then $\boldsymbol{R^+ \subseteq P}$. That is $\boldsymbol{R^+}$ is the smallest transitive relation containing $\boldsymbol{R}$.

Theorem 3: Let $\boldsymbol{R}$ be a relation on a set with $\boldsymbol{n}$ elements. Let $\boldsymbol{R^+}$ be the transitive closure of . Then

$$\boldsymbol{M_{R^+} = M_R \vee M_{R^2} \vee M_{R^3} \vee \dots \vee M_{R^n} = M_R \vee (M_R)^2 \vee (M_R)^3 \vee \dots \vee (M_R)^n}$$

For an illustration see P5

Applications of transitive closure of a relation

Transitive closures of relations have important applications in the following areas: Net works, synthetic analysis, fault detection and diagnosis in switching circuits.

Note: There are five equivalence relations on the set $A = \{a, b, c\}$. They are corresponding to the following partitions

$P_1 = \{\{a\}, \{b\}, \{c\}\}$, $P_2 = \{\{a, b, c\}\}$, $P_3 = \{\{a\}, \{b, c\}\}$, $P_4 = \{\{b\}, \{a, c\}\}$

$P_5 = \{\{c\}, \{a, b\}\}$.

Let R_1, R_2, R_3, R_4 and R_5 be the equivalence relations corresponding to the partitions P_1, P_2, P_3, P_4 and P_5 respectively.

$R_1 \circ R$ is an equivalence relation where $R \in \{R_1, R_2, R_3, R_4, R_5\}$

$R_2 \circ R$ is an equivalence relation where $R \in \{R_1, R_2, R_3, R_4, R_5\}$

Further, notice that $R_i \circ R_j$ is not an equivalence relation where $i, j \in \{3, 4, 5\}, i \neq j$

P1:

Let $\boldsymbol{R}$ and $\boldsymbol{S}$ be two relations on N ,the set of Natural numbers

$$\boldsymbol{R} = \{(\boldsymbol{x}, \boldsymbol{2x}) |\ \boldsymbol{x} \in \boldsymbol{N}\} \quad , \quad \boldsymbol{S} = \{(\boldsymbol{x}, \boldsymbol{7x}) |\ \boldsymbol{x} \in \boldsymbol{N}\}$$

Find $\boldsymbol{R} \circ \boldsymbol{S}, \boldsymbol{R} \circ \boldsymbol{R}, \boldsymbol{R} \circ \boldsymbol{R} \circ \boldsymbol{R}$ and $\boldsymbol{R} \circ \boldsymbol{S} \circ \boldsymbol{R}$

Solution: We have $x \xrightarrow{\text{R}} 2x$ and $x \xrightarrow{\text{S}} 7x$

(i) $x \xrightarrow{\text{R}} 2x \xrightarrow{\text{S}} 14x$ and $R \circ S = \{(x, 14x) |\ x \in \boldsymbol{N}\}$

Further, $x \xrightarrow{\text{S}} 7x \xrightarrow{\text{R}} 14x$. Therefore, $S \circ R = \{(x, 14x) |\ x \in \boldsymbol{N}\} = R \circ S$

(ii) $x \xrightarrow{\text{R}} 2x \xrightarrow{\text{R}} 4x$. Therefore, $R \circ R = \{(x, 4x) |\ x \in \boldsymbol{N}\}$

(iii) $R \circ R \circ R = \{(x, 8x) |\ x \in \boldsymbol{N}\}$

(iv) $x \xrightarrow{R \circ S} 14x \xrightarrow{\text{R}} 28x$. Therefore, $R \circ S \circ R = \{(x, 28x) |\ x \in \boldsymbol{N}\}$

P2:

Let $\boldsymbol{E}$ be the identity relation on a set $\boldsymbol{A}$ and $\boldsymbol{R}$ be any relation on $\boldsymbol{A}$. Show that $\boldsymbol{S} = \boldsymbol{E} \cup \boldsymbol{R} \cup \overline{\boldsymbol{R}}$ is a compatibility relation.

Solution: Notice that S is a relation on A. For any $x \in A$, we have $(x, x) \in E$ and so $(x, x) \in S$. Thus S is reflexive.

If for $x, y \in A, x \neq y$, $(x, y) \in S$ then (x, y) belongs to either R or $\overline{R}$. If $(x, y) \in R$ then $(y, x) \in \overline{R}$ and so $(y, x) \in S$. A similar argument holds when $(x, y) \in \overline{R}$. This proves that $(y, x) \in S$, whenever $(x, y) \in S$. Thus S is symmetric.

Therefore, S is reflexive and symmetric. This proves S is a compatibility relation on A.

P3:

Given the relation matrix M_R of a relation R on the set $A = \{a, b, c\}$. Find the relation matrices of $\bar{R}, R \circ R \circ R$ and $R \circ \bar{R}$ on the set A, where

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

Find the matrix of the transitive closure of R

Solution: We have that R is a relation on the set $A = \{a, b, c\}$ and

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

Now, $M_{\bar{R}} = (M_R)' = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$

$$M_{R^2} = M_{R\circ R} = M_R \circ M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$M_{R^3} = M_{R\circ R\circ R} = M_{R^2\circ R} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = M_{R^2}$$

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

The matrix of the transitive closure R^+ of R is given by

$$M_{R^+} = M_R \vee M_{R^2} \vee M_{R^3} = M_R \vee M_{R^2}$$

That is $M_{R^+} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \vee \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

P4:

Two equivalence relations R and S are given by the relation matrices M_R and M_S , where $M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $M_S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

a) **Show that $R \circ S$ is not an equivalence relation**

b) **Obtain equivalence relations R_1 and R_2 on the set $A = \{1, 2, 3\}$ such that $R_1 \circ R_2$ is an equivalence relation.**

Solution:

a) We have $M_{R \circ S} = M_R \circ M_S = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

$R \circ S$ is not an equivalence relation, because $M_{R \circ S}$ is not a symmetric matrix.

b) Let R_1 be the identity relation on $A = \{1, 2, 3\}$ then $M_{R_1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Let R_2 be the universal relation on $A = \{1, 2, 3\}$ then $M_{R_2} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

It is known that the equality relation on a finite set A is the smallest equivalence relation on A and the universal relation on A is the largest equivalence relation on A. We see that

$$M_{R_1 \circ R_2} = M_{R_1} \circ M_{R_2} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = M_{R_2}$$

This shows that $R_1 \circ R_2$ is an equivalence relation.

P5:

Find the matrix of the transitive closure of the relation $\boldsymbol{R}$ with

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

Solution:

$M_{R^2} = M_{R \circ R} = M_R \circ M_R = (M_R)^2$ and $M_{R^3} = (M_R)^3$

Now, $(M_R)^2 = M_R \circ M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$

$$(M_R)^3 = (M_R)^2 \circ M_R = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = {M_R}^2$$

Now, we have

$$M_{R^+} = M_R \vee (M_R)^2 \vee (M_R)^3$$

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

2.4. Transitive closure

Exercise

1. If $A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ and $C = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ then compute

   a) $A \wedge (B \vee C)$
   b) $(A \wedge B) \vee (A \wedge C)$
   c) $A \circ (B \circ C)$
   d) $B \circ C \circ A$
   e) $A^3 \circ B^2$
   f) $B^3 \circ C^2$

2. Let R be the relation whose matrix is
$$M_R = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$
   Find the matrix representing
   (i) $\overline{R}$ (ii) R^2 (iii) R^3 (iv) $R \circ \overline{R}$ (v) $\overline{R} \circ R$

3. Let R_1 and R_2 be relations on a set A with
$$M_{R_1} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad M_{R_2} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$
   Find the matrices of the following relations

   (i) $R_1 \cup R_2$ (ii) $R_1 \cap R_2$ (iii) $R_2 \circ R_1$ (iv) $R_1 \circ R_1$

4. Find the transitive closure of the following relations on $A = \{1, 2, 3, 4\}$
   a) $R_1 = \{(1,2), (2,1), (2,3), (3,4), (4,1)\}$
   b) $R_2 = \{(2,1), (2,3), (3,1), (3,4), (4,1), (4,3)\}$
   c) $R_3 = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$
   d) $R_4 = \{(1,1), (1,4), (2,1), (2,3), (3,1), (3,2), (3,4), (4,2)\}$

MODULE-5

Posets

2.5.

Posets

We often use relations to order some or all of the elements of sets. For example (i) we order words using the relation containing pairs of words (x, y), where the word x comes before the word y in the dictionary, (ii) we schedule projects using the relation consisting of pairs (x, y), where x, y are tasks in a project such that the task x must be completed before the task y begins, (iii) we order the elements of a set of real numbers using the relation containing the pairs (x, y) where x is less than y. If we add all the pairs of the form (x, x) to these relations, we obtain the relation that is reflexive, antisymmetric and transitive. These are the properties that characterize relations used to order the elements.

Partial order and Poset

A relation R on a set A is called a ***Partial ordering*** or ***Partial order*** if it is *reflexive*, *antisymmetric* and *transitive*. A set A together with a partial order R defined on it, denoted by $(\boldsymbol{A}, \boldsymbol{R})$ is called a ***Partially ordered set*** or ***Poset*** in short.

Examples

i) The relation “less than or equal to $(\leq)$ ” and “greater than or equal to $(\geq)$“ are partial orders on any non empty subset A of $\boldsymbol{R}$. Therefore, $(A, \leq)$ and $(A, \geq)$ are posets, where A is a non empty subset of $\boldsymbol{R}$.
ii) The divisibility relation (i.e., divides (|)) is a partial order on any non empty subset A on $\boldsymbol{N}$. Therefore, $(A, |)$ is a poset, where A is a nonempty subset of $\boldsymbol{N}$.
iii) Let A be a set and $P(A)$ be its power set. The inclusion relation $(\subseteq)$ is a partial order on $P(A)$. Therefore, $(P(A), \subseteq)$ is poset, where A is a set.

Notation: Customarily a partial order is denoted by $\preccurlyeq$.

This notation is used because the relation $\leq$ is the most familiar example of a partial order on $\boldsymbol{R}$ and the symbol $\preccurlyeq$ is similar to $\leq$.

The notation $x \prec y$ denotes that $x \preccurlyeq y$ and $x \neq y$.

Note: if $(A, \preccurlyeq)$ is a poset and $x, y \in A$ then it is not necessary that either $x \preccurlyeq y$ or $y \preccurlyeq x$.

For example, in $(P(A), \subseteq)$, where $A = \{1,2,3\}$; $\{1,2\}$ is not related to $\{1,3\}$ and vice versa, because neither set is a subset of the other.

Comparability in a poset

Let $(A, \preccurlyeq)$ be a poset. Two elements $a, b \in A$ are said to be ***comparable*** if ***either*** $\boldsymbol{a \preccurlyeq b}$ ***or*** $\boldsymbol{b \preccurlyeq a}$. The elements $a, b \in A$ are ***incomparable*** if ***neither*** $\boldsymbol{a \preccurlyeq b}$ ***nor*** $\boldsymbol{b \preccurlyeq a}$.

Example 1: In the poset $(P(A), \subseteq)$, where $A = \{1,2,3\}$; $\{1\}$ and $\{1,3\}$are comparable (because$\{1\} \subseteq \{1,3\}$) and $\{1,2\}$, $\{1,3\}$ are incomparable because neither set is a subset of the other.

Note: the adjective ***partial*** in the poset mean that there may be pairs of elements which are incomparable. If every pair of elements in a poset are comparable then the ordering relation is called a ***total order***.

Totally ordered set: If $(A, \preccurlyeq)$ be a poset and every two elements of A are comparable then $(A, \preccurlyeq)$ is called a ***totally ordered set*** or ***linearly ordered set*** or ***chain*** and $\preccurlyeq$ is called a ***total order*** or a ***linear order***.

Example 2: Let A be any nonempty subset of $\boldsymbol{R}$. The poset $(A, \leq)$ is a totally ordered set because for any $a, b \in A$, we have either $a \leq b$ or $b \leq a$.

Example 3: Let $A = \{1,2,3,4\}$. The poset $(A, |)$ is not a chain because A contains elements that are incomparable such as 2 and 3.

Consider the totally ordered set $(\boldsymbol{N}, \leq)$ and $\boldsymbol{N} \times \boldsymbol{N}$. Define a relation $\preccurlyeq$ on $\boldsymbol{N} \times \boldsymbol{N}$ as follows. For any $(x_1, y_1), (x_2, y_2) \in \boldsymbol{N} \times \boldsymbol{N}$, define

$$\boldsymbol{(x_1, y_1) \preccurlyeq (x_2, y_2)} \textbf{ either if } \boldsymbol{x_1 < x_2} \textbf{ or if both } \boldsymbol{x_1 = x_2} \textbf{ and } \boldsymbol{y_1 \leq y_2}$$

Example: $(\boldsymbol{N} \times \boldsymbol{N}, \preccurlyeq)$ **is a totally ordered set** **(See P1 for solution)**

Lexicographic order

The words in a dictionary are listed in alphabetic or lexicographic order which is based on the ordering of the letters in the alphabet. This is a special case of an ordering of strings on a set constructed from a partial ordering on the set. The following is such a construction in any poset.

Let $(A_1, \preccurlyeq_1)$ and $(A_2, \preccurlyeq_2)$ be two posets. Consider the Cartesian product $A_1 \times A_2$. The ***lexicographic ordering*** $\preccurlyeq$ on $A_1 \times A_2$ is defined by

$$(\boldsymbol{x_1}, \boldsymbol{y_1}) \preccurlyeq (\boldsymbol{x_2}, \boldsymbol{y_2}) \Leftrightarrow (\boldsymbol{x_1} \prec_{\boldsymbol{1}} \boldsymbol{x_2}) \vee \big((\boldsymbol{x_1} = \boldsymbol{x_2}) \wedge (\boldsymbol{y_1} \preccurlyeq_{\boldsymbol{2}} \boldsymbol{y_2})\big)$$

It may be verified that $\preccurlyeq$ is a partial order. Therefore, $(A_1 \times A_2, \preccurlyeq)$ is a poset.

If $(A, \preccurlyeq_1)$ is an ordered set then the lexicographic ordering $\preccurlyeq$ defined on $A \times A$ is a total order and $(A \times A, \preccurlyeq)$ is a totally ordered set (chain).

Example 4: In the $(\boldsymbol{N} \times \boldsymbol{N}, \preccurlyeq)$, where $\preccurlyeq$ is the lexicographic ordering constructed from the usual $\leq$ relation on $\boldsymbol{N}$,

$(2,2) \preccurlyeq (2,1), (3,1) \preccurlyeq (1,5), (2,2) \preccurlyeq (2,2), (3,2) \preccurlyeq (1,1), (4,9) \preccurlyeq (4,11), \dots$

Generalization of Lexicographic ordering

Let $(A, \preccurlyeq_1)$ be a totally ordered set. Let n be a given natural number and

$$P = A \cup A^2 \cup A^3 \cup \dots . U A^n = \bigcup_{i=1}^{n} A^i$$

That is, P consists of strings of elements of A of length less than or equal to n. A string of length p may be considered as a p-tuple .Define a total ordering $\preccurlyeq$ on P called lexicographic ordering as follows:

Let $(a_1, a_2, \dots, a_p)$ and $(b_1, b_2, \dots, b_p, \dots, b_q)$ with $p \leq q$ be any two elements of P. Now,

$$(a_1, a_2, \dots, a_p) \preccurlyeq (b_1, b_2, \dots, b_p, \dots, b_q)$$

if any of the following hold:

i) $\left(a_1, a_2, \ldots., a_p\right) = (b_1, b_2, \ldots, b_p)$

ii) $a_1 \neq b_1$ and $a_1 \prec_1 b_1$ in $(A \preccurlyeq_1)$

iii) $a_i = b_i, i = 1,2, \ldots, k \ (k < p)$ and $a_{i+1} \neq \ b_{i+1}$ and $a_{i+1} \prec_1 b_{i+1}$ in $(A, \preccurlyeq_1)$

If none of these conditions are satisfied then

$$(b_1, b_2, \ldots, b_q) \preccurlyeq (a_1, a_2, \ldots, a_p)$$

Example 5: Let $A = \{a, b, c, \ldots, z\}$ be the lower case English alphabet and a linear ordering on A denoted by $\leq$, where $a \leq b \leq c \leq \cdots \leq z$. Let

$$P = X \cup X^2 \cup X^3 \cup X^4$$

That is , P consists of all "words" or strings of 4 or fewer than 4 letters from A. The lexicographic ordering in P is same as that used in dictionaries

For example, zerm, zero, zebra, axe, ante

ante $\preccurlyeq$ axe (by ii)

zebra $\preccurlyeq$ zero (Here "zero" and "zebra" are compared and the conditions (i), (ii) and (iii) are not satisfied)

zerm $\preccurlyeq$ zero (by (iii))

Note: Instead of using $\preccurlyeq$ to denote lexicographic ordering, it is customary to use the terminology such as "lexically less than or equal to "or "lexically greater than "

Application of lexicographic ordering

Lexicographic ordering is used in **sorting character data** on a computer

Hasse diagrams

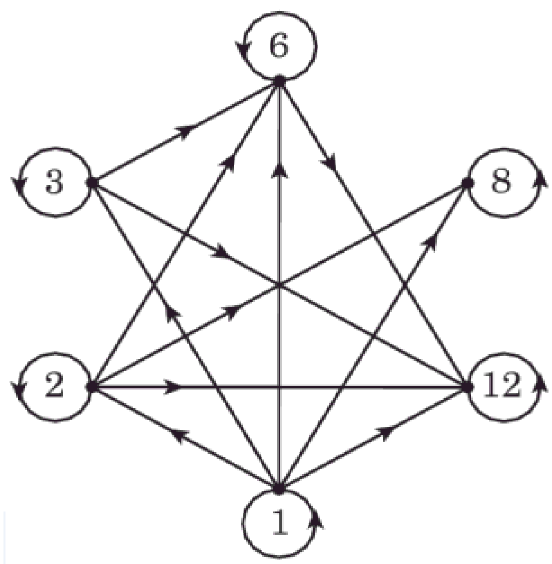
We can simplify the diagraphs of a finite poset by omitting many of its edges. For instance, since a partial order is reflexive, each vertex has a loop, which we can delete. In addition, drop all edges implied by transitivity (For example if the digraph of a poset contains edges (a, b) and (b, c) , it has the edge (a, c) , which we can omit. Finally, draw the remaining edges ***upward*** and ***drop all arrows***. The resulting is called the ***Hasse diagram*** named after the twentieth – century German mathematician **Helmut Hasse** $(1898 - 1979)$.

Example 6: Draw the Hasse diagram for the poset $(A, |)$, where $A = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{6}, \mathbf{8}, \mathbf{12}\}$ and | denotes the divisibility relation.

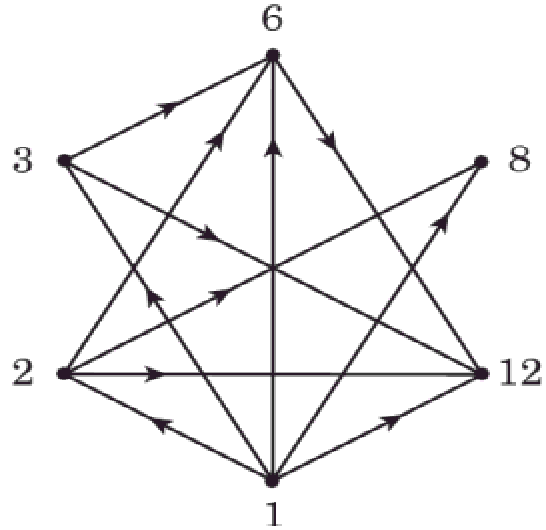
Solution: The ordered pairs in the partial order are
$(1,1), (1,2), (1,3), (1,6), (1,8), (1,12), (2,2), (2,6), (2,8), (2,12), (3,3), (3,6), (3,12)$

$(6,6), (6,12), (8,8), (12,12)$

The diagraph of the poset is

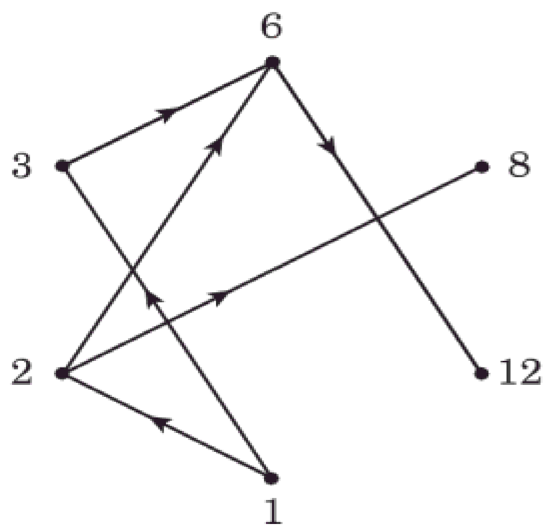


Step 1: Delete the loop at each vertex

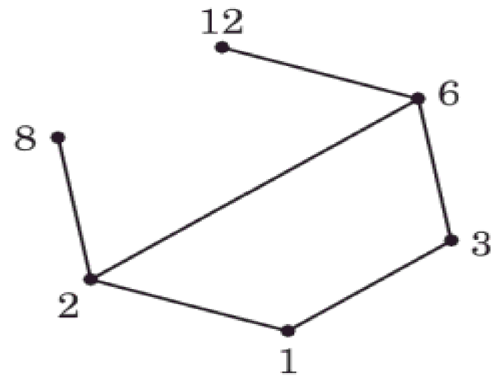


Step 2: Delete all the edges implied by transitivity. These are

$(1,6), (1,8), (1,12), (2,12), (3,12)$



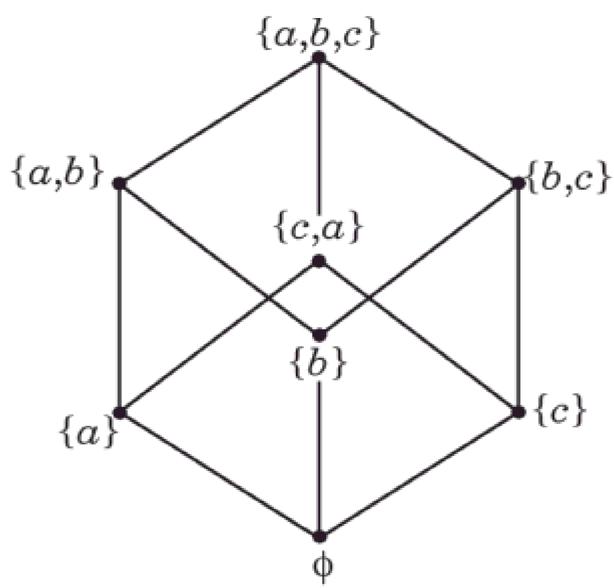
Step 3: Omit all arrows and arrange all edges, point upward to obtain the Hasse diagram.



Example 7: **Draw Hasse diagram of the poset $(\boldsymbol{P}(\boldsymbol{A}), \subseteq)$, where $\boldsymbol{A} = \{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}$**

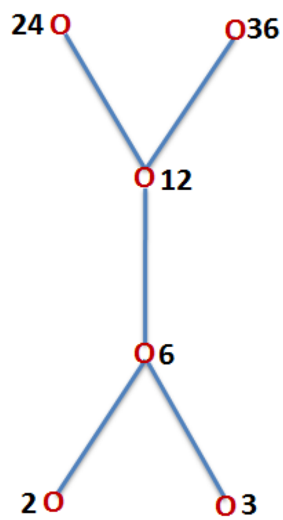
Solution: We have $A = \{a, b, c\}$ and
$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$

Following the steps 1-3, produces the Hasse diagram of the poset $(\boldsymbol{P}(\boldsymbol{A}), \subseteq)$



Example 8: Draw the Hasse diagram of the poset $(A, |)$, where $\boldsymbol{A = \{2, 3, 6, 12, 24, 36\}}$

Solution: We have $A = \{2,3,6,12,24,36\}$. Following the steps 1-3, produces the Hasse diagram of $(\boldsymbol{A}, |)$,



Hasse diagram of divides relation

Extremal elements: An element a in a poset $(A, \preccurlyeq)$ is a **maximal element**. If there is *no element* b in A such that $a \prec b$. An element a in a poset $(A, \preccurlyeq)$ is a **minimal element**. If there is no element b in A such that $b \prec a$.

The maximal and minimal elements in a finite poset are the “top” and “bottom” elements in its Hasse diagram.

The poset $(A, |)$, where $A = \{1, 2, 3, 6, 8, 12\}$ has two maximal elements 8 and 12 and one minimal element 1. The poset $(A, |)$ where $A = \{2, 3, 6, 12, 24, 36\}$ has two maximal elements 24 and 36 and two minimal elements 2 and 3.

Note:

(i) A poset may have more than one maximal element and more than one minimal element.

(ii) A poset need not have any maximal or minimal elements. For example the poset $(\boldsymbol{Z}, \leq)$ has no maximal or minimal elements.

(iii) A poset may have a maximal element but no minimal elements or a minimal element but no maximal elements. For example $(\boldsymbol{Z}^{-}, \leq)$ has a maximal element but no minimal elements, where as the poset $(\boldsymbol{N}, \leq)$ has a minimal element but no maximal elements.

Two special extremal elements are the greatest and the least elements.

Greatest and least elements: Let $(A, \preccurlyeq)$ be a poset. If there exists an element $a \epsilon A$ such that $a \preccurlyeq x$, for all $x \in A$, then a is called the **least element** of A. If these exists an element $b \in A$ such that $x \preccurlyeq b$ for all $x \in A$, then b is called the **greatest element** of A.

Note: The least element (greatest element) if exists is unique and they are the *topmost* and *bottom most* elements in the Hasse diagram of a finite poset.

The least element and the greatest element of a poset are usually denoted by 0 and 1 respectively.

The poset $(A, |)$ where $A = \{1, 2, 3, 6, 8, 12\}$ has no greatest element, but has the least element 1.

The poset $(A, |)$ where $A = \{2, 3, 6, 12, 24, 36\}$ has no least element and has no greatest element.

Although an arbitrary poset need not have a minimal element , *every non empty finite poset has at least one minimal element*. We state this result as a lemma.

Lemma 1: Every finite non empty poset $(A, \preccurlyeq)$ has at least one minimal element.

Topological Sorting

Suppose that a project is made up of n different tasks. Some tasks can be completed only after others have been finished. To find an order R for these tasks, we set up a partial order on the set of tasks so that $a\, R\, b, a \neq b$, iff the task b cannot be started until the task a has been completed. To produce a schedule for the project, we need to produce an order for all n tasks that is compatible with this partial order.

A total ordering $\preccurlyeq$ is said to be *compatible* with the partial ordering R. If

$$\boldsymbol{a \preccurlyeq b} \textbf{ whenever } \boldsymbol{aRb}$$

Constructing a compatible total ordering from a given partial ordering is called **topological sorting.**

The following is the procedure of a topological sorting and it works for any finite none empty poset.
To define a total ordering on the poset $(A,\ R)$ where A has n elements,first choose a minimal element call, it a_1 (such an element exists by Lemma 1). Now note that $(A-\{a_1\},R)$ is also a poset (where R is the restriction on $A-\{a_1\}$). If it is nonempty choose a minimal element, call it a_2 ,of this poset and we have $a_1 \ \prec a_2$.Remove a_2 form $A-\{a_1\}$, if $A-\{a_1\ a_2\}$ is nonempty continue the procedure. Because A is finite this process must terminate.

The end product is a sequence of elements $a_1, a_2, \dots, a_n$ and the derived total ordering $\preccurlyeq$ is defined by

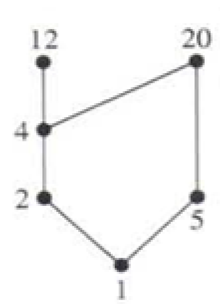
$$a_1 \prec a_2 \prec a_3 \prec a_4 \prec \cdots \prec a_n$$

This total ordering $\preccurlyeq$ is compatible with the original partial ordering R.

Application: Topological sorting has an application to the scheduling of projects.

Example 9: Topologically sort the elements of the poset $(A,|)$, where
$$\boldsymbol{A = \{1, 2, 4, 5, 12, 20\}}$$
Find a compatible total ordering for the poset $(A,|)$

Solution: The Hasse diagram of the poset $(\boldsymbol{A},|)$ is



Step 1: Choose a minimal element. This must be 1 (because 1 is the only minimal element.

Step -2: Extract 1 and obtain $A - \{1\} = \{2, 4, 5, 12, 20\}$ **.** Now, There are two minimal elements, namely 2 and 5, select 5 .

Repeat step – 2: Extract 5 and obtain $A - \{1, 5\} = \{2,4, 12, 20\}$ .The minimal element at this stage is 2.

Repeat Step – 2: Extract 2 and obtain $A - \{1, 5, 2\} = \{4, 12, 20\}$. The minimal element at this stage is 4.

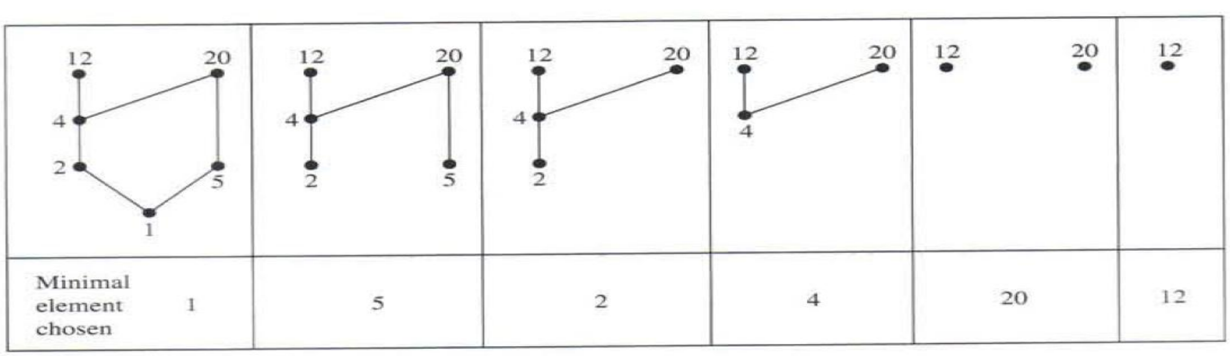
Repeat Step – 2: Extract 4 and obtain $A - \{1, 5, 2, 4\} = \{12, 20\}$**.** Either of the two can be a minimal element, select 20.

Repeat Step – 2: Extract 20 and obtain $A - \{1, 5, 2, 4, 20\} = \{12\}$ Now, it is the last element left.

This produces a total ordering $1 \prec 5 \prec 2 \prec 4 \prec 20 \prec 12$.

Note: It is one possible order for the tasks

The steps used by this sorting are illustrated in the figure.



Note:

Computer scientists use the terminology “Topological sorting” and mathematician use the terminology “Linearization of partial ordering” for the same thing. In mathematics topology deals with the geometry. In computer science, a topology is any arrangement of objects that can be connected with edges.

P1:

Consider the totally ordered set $(\boldsymbol{N}, \leq)$ and $\boldsymbol{N} \times \boldsymbol{N}$. Define a relation $\preccurlyeq$ on $\boldsymbol{N} \times \boldsymbol{N}$ as follows. For any $(\boldsymbol{x_1}, \boldsymbol{y_1}), (\boldsymbol{x_2}, \boldsymbol{y_2}) \in \boldsymbol{N} \times \boldsymbol{N}$, define

$$(\boldsymbol{x_1}, \boldsymbol{y_1}) \preccurlyeq (\boldsymbol{x_2}, \boldsymbol{y_2}) \text{ either if } \boldsymbol{x_1} < \boldsymbol{x_2} \text{ or if both } \boldsymbol{x_1} = \boldsymbol{x_2} \text{ and } \boldsymbol{y_1} \leq \boldsymbol{y_2}$$

Show that $(\boldsymbol{N} \times \boldsymbol{N}, \preccurlyeq)$ is a totally ordered set

Solution: For any $(x, y) \in \boldsymbol{N} \times \boldsymbol{N}$ **,** we have $(x, y) \preccurlyeq (x, y)$ because $x = x$ and $y \leq y$. Therefore, $\preccurlyeq$ is reflexive.

If $(x_1, y_1) \preccurlyeq (x_2, y_2)$ and $(x_2, y_2) \preccurlyeq (x_1, y_1)$ then the possibility $x_1 < x_2$ and $x_2 < x_1$ is not possible. Therefore, $(x_1 = x_2 \text{ } and \text{ } y_1 \leq y_2)$ and $(x_2 = x_1 \text{ } and \text{ } y_2 \leq y_1)$ imply $x_1 = x_2$ and $y_1 = y_2$. Thus, $(x_1, y_1) = (x_2, y_2)$. This proves that $\preccurlyeq$ is antisymmetric.

$(x_1, y_1) \preccurlyeq (x_2, y_2)$ and $(x_2, y_2) \preccurlyeq (x_3, y_3)$

$\Longrightarrow x_1 < x_2$ or $(x_1 = x_2 \text{ } and \text{ } y_1 \leq y_2)$ and $x_2 < x_3$ or $(x_2 = x_3 \text{ } and \text{ } y_2 \leq y_3)$

$\Longrightarrow x_1 < x_3$ or $(x_1 = x_3 \text{ } and \text{ } y_1 \leq y_3)$ (How ?)

$\Longrightarrow (x_1, y_1) \preccurlyeq (x_3, y_3)$

This proves that $\preccurlyeq$ is Transitive. Thus, $(\boldsymbol{N} \times \boldsymbol{N}, \preccurlyeq)$ is a poset.

Let (x_1, y_1) and (x_2, y_2) be any two elements of $\boldsymbol{N} \times \boldsymbol{N}$**.** Since $x_1, x_2 \in \boldsymbol{N}$, by law of trichotomy $x_1 < x_2$ or $x_1 = x_2$ or $x_2 < x_1$.

If $x_1 < x_2$ then $(x_1, y_1) \preccurlyeq (x_2, y_2)$

If $x_2 < x_1$ then $(x_2, y_2) \preccurlyeq (x_1, y_1)$

Let $x_1 = x_2$. For any $y_1, y_2 \in \boldsymbol{N}$, we have either $y_1 \leq y_2$ or $y_2 \leq y_1$, because $(\boldsymbol{N}, \leq)$ is a chain. If $y_1 \leq y_2$ then $(x_1, y_1) \preccurlyeq (x_2, y_2)$. If $y_2 \leq y_1$ then $(x_2, y_2) \preccurlyeq (x_1, y_1)$. This shows that any two elements of $\boldsymbol{N} \times \boldsymbol{N}$ are comparable. Thus, $\preccurlyeq$ is a total order. Therefore, $(\boldsymbol{N} \times \boldsymbol{N}, \preccurlyeq)$ is a totally ordered set.

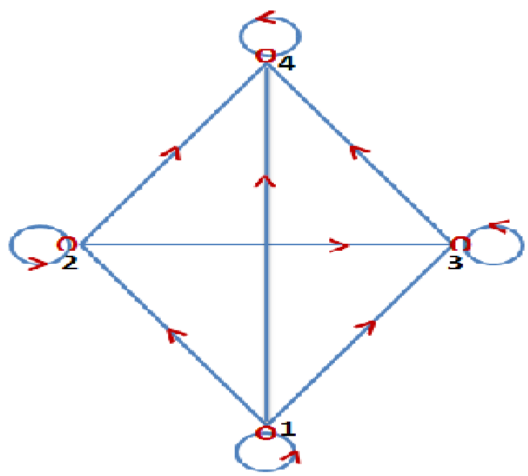
P2:

Draw the Hasse diagram for the "less than or equal to" relation defined on the set $A = \{1, 2, 3, 4\}$.

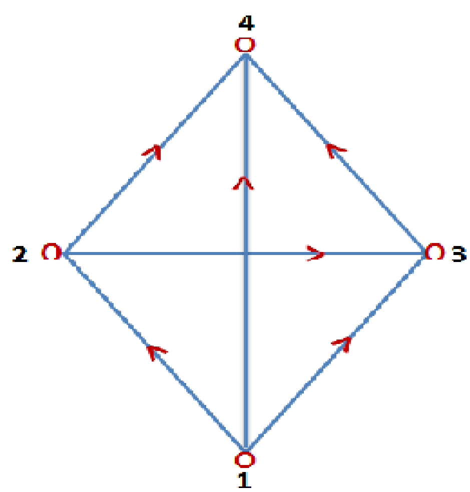
Solution: Let R be a relation "less than or equal to "on $A = \{1,2,3,4\}$. Therefore

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

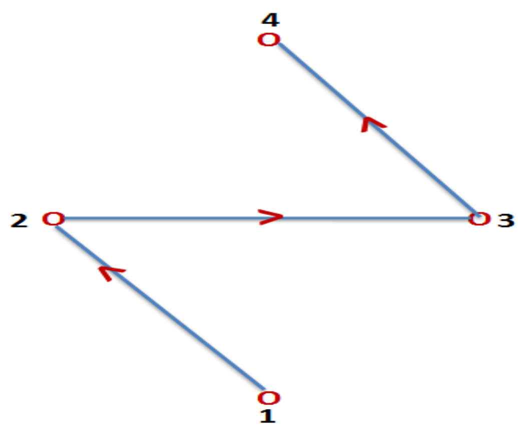
(A, R) is a poset. The diagraph of the poset is



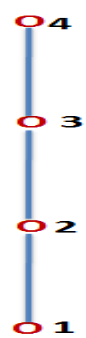
Step 1: Delete the loop at each vertex



Step 2 : Delete all the edges implied by transitivity . These are $(1,4), (1,3), (2,4)$



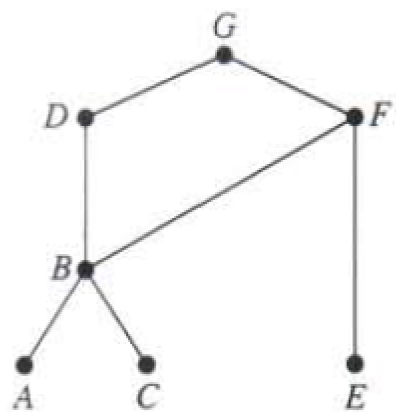
Step 3 : Omit all arrows and arrange all edges point upward to obtain the Hasse diagram.



It is a chain

P3:

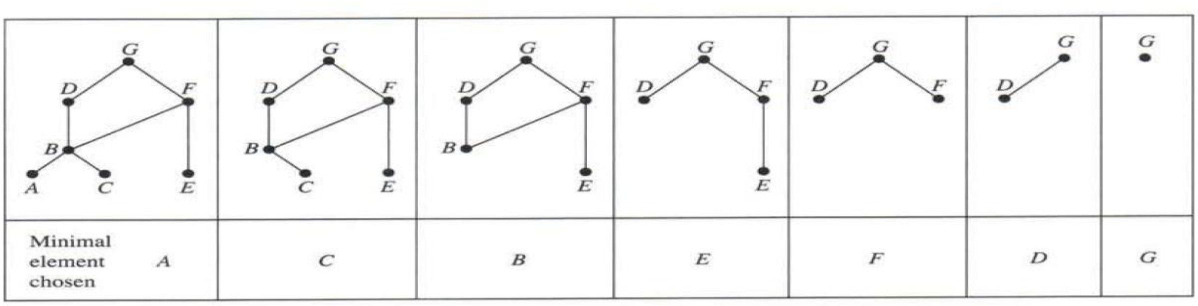
A development project at a computer company requires the completion of seven tasks. Some of these tasks can be started only after other tasks are finished. A partial ordering on tasks is set up by considering task $x \prec$ task y if task y cannot be started until task x has been completed. The Hasse diagram for the seven tasks with respect to this partial ordering is shown below.



Find an order in which these tasks can be carried out to complete the project.

Solution:

An ordering of the seven tasks can be obtained by topological sort. The steps are shown in the following figure.



The result of this sort is $A \prec C \prec B \prec E \prec F \prec D \prec G$

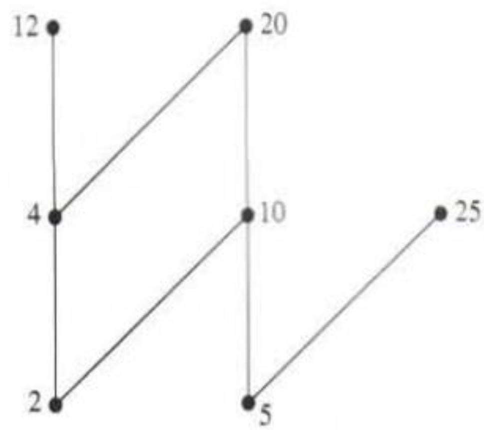
Note: It is one possible order for the tasks.

P4:

Which elements of the poset $(A, |)$ are maximal and which are minimal, defined on the set $A = \{2, 4, 5, 10, 12, 20, 25\}$.

Solution:

The Hasse diagram of the poset is



Notice that there is no $b \in A$ such that

$12 \prec b$ $i.e.,$ $12|b$, $20 \prec b$ $i.e.,$ $20|b$ and $25 \prec b$ $i.e.,$ $25|b$

Therefore, 12, 20 and 25 are maximal elements of the poset.

Further, notice that there is no $b \in A$ such that

$b \prec 2$, $i.e.,$ $b|2$ and$b \prec 5$, $i.e.,$ $b|5$

Therefore, 2 and 5 are minimal elements of the poset.

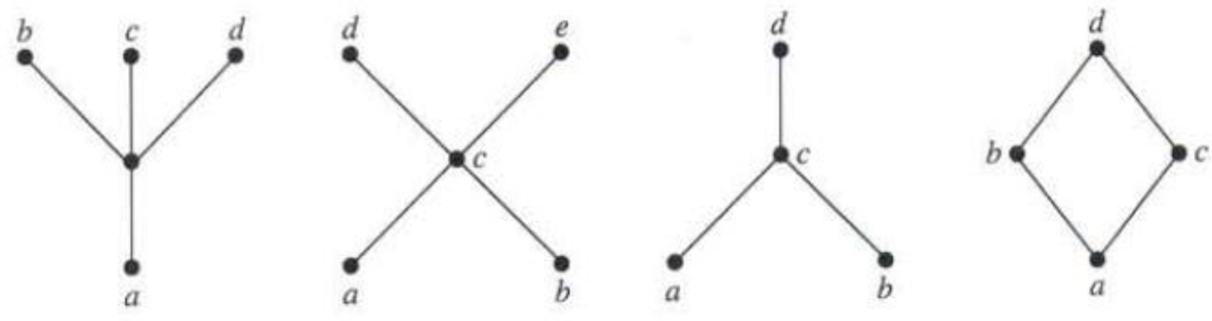
Note:

(i) There is no $a \in A$ such that $a \preccurlyeq x, \forall x \in A$, $i.e.,$ $a|x$, $\forall x \in A$. Therefore, the poset has no least element.

(ii) There is no $a \in A$ such that , $x \preccurlyeq a, \forall x \in A$, $i.e.,$ $x|a$, $\forall x \in A$. Therefore, the poset has no greatest element.

P5:

Determine whether the Posets represented by each of the following Hasse diagrams have a greatest element and least element:



(a) (b) (c) (d)

Solution:

Recall the definition of least and greatest elements.

Poset	Least element	Greatest element
(a)	a	No
(b)	No	No
(c)	No	d
(d)	a	d

P6:

Let A be a nonempty set. Determine whether there is a greatest element and a least element in $(\boldsymbol{P}(\boldsymbol{A}), \subseteq)$.

Solution:

Notice that $\phi \subseteq X$, for every subset X of A. Therefore, ϕ is the least element of the poset. Further,$X \subseteq A$, for every subset X of A. Therefore, A is the greatest element of the poset.

P7:

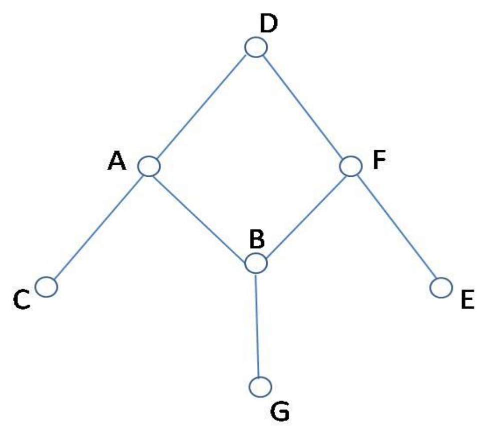
Seven tasks, A through G, comprise a project. Some of them can be started only after others are completed as indicated in the following table:

Task	Requires the completion of
A	B, C
B	G
C	None
D	A, F
E	None
F	B, E
G	None

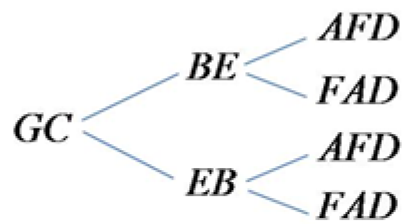
How many ways can the tasks be arranged sequentially, so that the prerequisites of each task will be completed before it started? List all of them.

Solution:

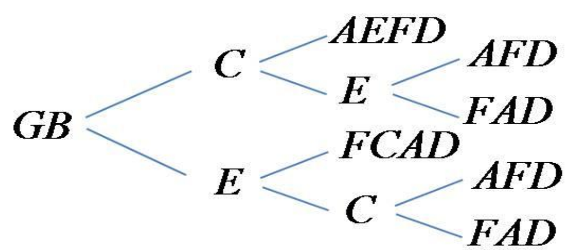
From the table, we draw the following Hasse diagram:



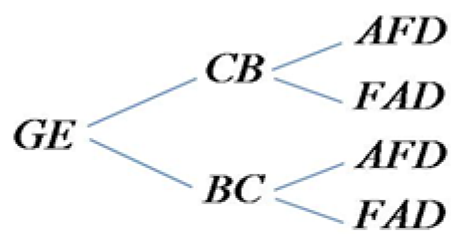
We topologically sort the elements of the poset and obtain 26 possible orders for the tasks. The following are the possible orders.


GC
BE
EB
AFD
FAD
AFD
FAD

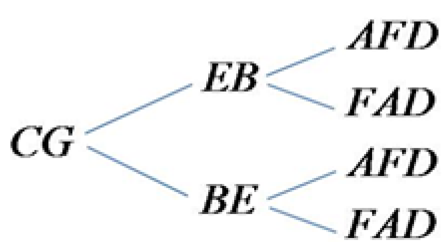
(4)


GB
C
E
AEFD
E
AFD
FAD
FCAD
C
AFD
FAD

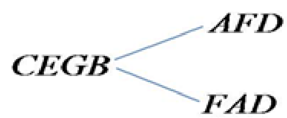
(6)


GE
CB
BC
AFD
FAD
AFD
FAD

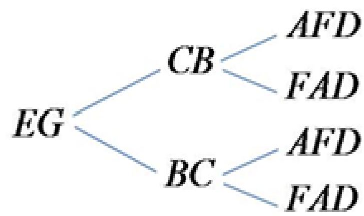
(4)


CG
EB
BE
AFD
FAD
AFD
FAD

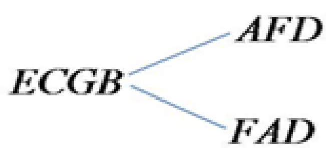
(4)



(2)



(4)

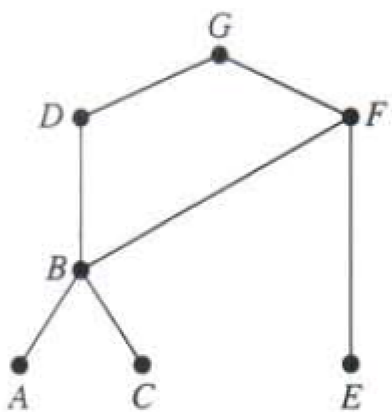


(2)

Therefore there are 26 possible orders.

P8:

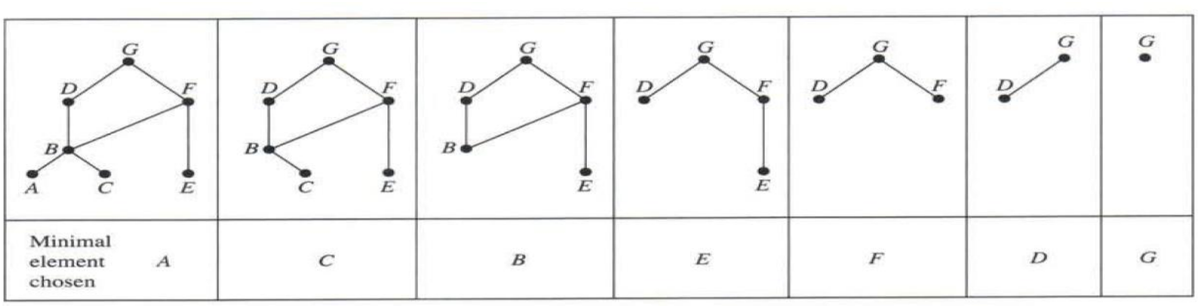
A development project at a computer company requires the completion of seven tasks. Some of these tasks can be started only after other tasks are finished. A partial ordering on tasks is set up by considering task $x \prec$ task y if task y cannot be started until task x has been completed. The Hasse diagram for the seven tasks with respect to this partial ordering is shown below.



Find an order in which these tasks can be carried out to complete the project.

Solution:

An ordering of the seven tasks can be obtained by topological sort. The steps are shown in the following figure.



The result of this sort is $A \prec C \prec B \prec E \prec F \prec D \prec G$

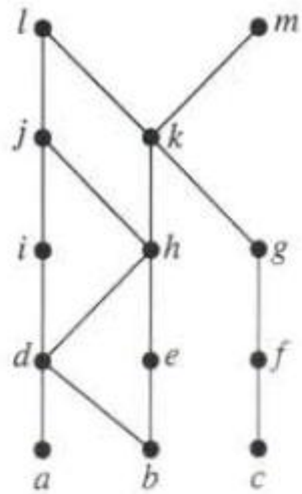
Note: It is one possible order for the tasks.

2.5. Posets

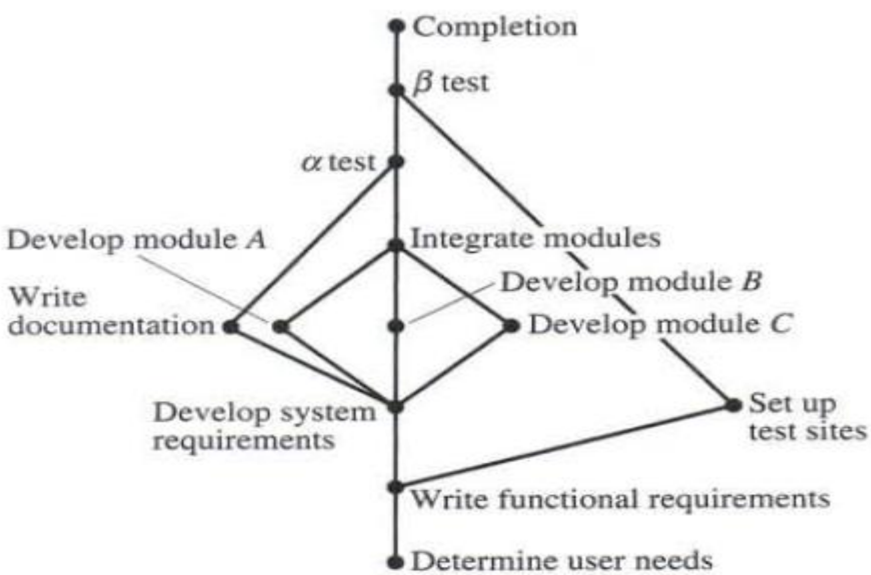
Exercise:

1. Let (S, R) be a poset. Show that $(S, \overline{R})$ is also a poset, where $\overline{R}$ is the inverse of R. The poset $(S, \overline{R})$ is called the ***dual*** of (S, R).
2. Find the duals of the following posets.
   a) $(\{0,1,2\}, \leq)$
   b) $(\boldsymbol{Z}, \geq)$
   c) $(P(\boldsymbol{Z}), \supseteq)$
   d) $(\boldsymbol{Z}^{+}, |)$
3. Which of the following pairs of elements are comparable in the poset $(\boldsymbol{Z}^{+}, |)$?
   a) $5, 15$
   b) $6, 9$
   c) $8, 16$
   d) $7, 7$
4. Find two incomparable elements in the following posets ?
   a) $(P(\{0,1,2\}), \subseteq)$
   b) $(\{1,2,4,6,8\}, |)$
5. Find the lexicographic ordering of the following n-tuples
   a) $(1,1,2), (1,2,1)$
   b) $(0,1,2,3), (0,1,3,2)$
   c) $(1,0,1,0,1), (0,1,1,1,0)$
6. Draw the Hasse diagram for divisibility on the set
   a) $\{1,2,3,4,5,6,7,8\}$
   b) $\{1,2,3,5,7,11,13\}$
   c) $\{1,2,3,6,12,24,36,48\}$
   d) $\{1,2,4,8,16,32,64\}$

7. Show that lexicographic order is a partial ordering on the Cartesian product of two sets.
8. Find a compatible total order for the poset with the Hasse diagram shown in the following figure.



9. Find a compatible total order for the divisibility relation on the set $\{1,2,3,6,8,12,24,36\}$
10. Find an ordering of the tasks of a software project if the Hasse diagram for the tasks of the project is as shown.



.

MODULE-6

countable and uncountable sets

2.6

Countable and uncountable sets

We are all familiar with a useful application of the set of natural numbers in counting. This property of natural numbers is used in measuring the *size* of a set and in comparing the *sizes* of any two sets. In the process of counting we establish a one to one correspondence between the objects to be counted and the set of natural numbers $\{1, 2, 3, \ldots, n\}$. From this correspondence we say that the number of objects is n.The following is a generalization of this concept:

Equivalent Sets

Two sets A and B are said to be ***equivalent*** or ***equipotent*** or to have the ***same cardinality*** or ***similar*** written as $A \sim B$, if and only if there is a one- to- one correspondence between the sets A and B. A one -to -one correspondence can be established by showing a **bijective** mapping $f: A \longrightarrow B$.

Example 1: $\boldsymbol{N}$, the set of natural numbers and $\boldsymbol{N_2} = \{\mathbf{2}, \mathbf{4}, \mathbf{6}, \ldots\}$, the set of even natural numbers are equivalent.

Solution: Define a map $f: \boldsymbol{N} \longrightarrow N_2$ by $f(n) = 2n$. It is easy to see that f is bijective. Thus $\boldsymbol{N} \sim N_2$.

Note: Notice that $N_2 \subset \boldsymbol{N}$

Example 2: Let $\boldsymbol{P}$ be the set of all possible real numbers and $\boldsymbol{S}$ be the subset of $\boldsymbol{P}$ given by $\boldsymbol{S} = \{\boldsymbol{x} | \boldsymbol{x} \in \boldsymbol{P} \ \wedge (\mathbf{0} < x < 1)\}$, then show that $\boldsymbol{S} \sim \boldsymbol{P}$.

Solution: Define a mapping $f: P \longrightarrow S$ by $f(x) = \frac{x}{1+x}$ for $x \in P$. Clearly, the range of f is in S. Now,

$$f(x_1) = f(x_2) \Longrightarrow \frac{x_1}{1+x_1} = \frac{x_2}{1+x_2} \Longrightarrow x_1 + x_1x_2 = x_2 + x_1x_2 \Longrightarrow x_1 = x_2$$

This shows that f is injective. Further, for any $y \in S$ there exists a $\frac{y}{1-y} \in P$, such that $f\left(\frac{y}{1-y}\right) = \frac{\frac{y}{1-y}}{1+\frac{y}{1-y}} = y$, $i.e.$, every element in S has a pre-image. Thus f is surjective. Therefore, f is bijective and $S \sim P$

Example 3: Any two closed intervals $[\boldsymbol{a}, \boldsymbol{b}]$, $\boldsymbol{a} < b$ and $[\boldsymbol{c}, \boldsymbol{d}]$, $\boldsymbol{c} < d$ are equivalent. (See P1 for solution)

Note: It is easy to see that the equivalence of sets (equipotence of sets) is an equivalence relation on a family of sets and hence partitions the family of sets into equivalence classes.(See P3)

Let F be a family of sets and let $\sim$ denotes the relation of equivalence (equipotence) on F. The equivalence classes of F under the relation $\sim$ are called **cardinal numbers**. For any set $A \in F$, the equivalence class to which A belongs is denoted by $[\boldsymbol{A}]$ or $\boldsymbol{card}(\boldsymbol{A})$ and is called the ***cardinal number* of $\boldsymbol{A}$**. For $A, B \in F, [A] = [B] \Leftrightarrow A \sim B$.

We shall first start with the empty set and denote its cardinal number by 0. For the time being, denote the cardinal number of a set A by $k(A)$, so that $k(\emptyset) = 0$. If $p \notin A$, then the cardinal number of $A \cup \{p\}$ $i.e.$, $k(A \cup \{p\})$ can be written as $k(A) + 1$. We can build sets starting with null set and building successive unions such that the cardinalities of these sets can be represented by zero and the natural numbers.

For example, Let $A_1 = \{a\}$, $A_2 = \{a, b\}$, $A_3 = \{a, b, c\}$, … . Then we have, $A_1 = \emptyset \cup \{a\}$ and $k(A_1) = k(\emptyset) + 1 = 0 + 1 = 1$.

$A_2 = \{a, b\} = A_1 \cup \{b\}$, and $k(A_2) = k(A_1) + 1 = 1 + 1 = 2$

$A_3 = \{a, b, c\} = A_2 \cup \{c\}$, and $k(A_3) = k(A_2) + 1 = 2 + 1 = 3$

and so on .In this way the cardinal number of a set containing n elements can be denoted by the natural number n.

Remark: It is not possible to represent the cardinality of every set by a natural number, because there are sets which cannot be built by successive unions, as was done above.

The following is the definition of a finite set:

Finite and infinite set: A set is said to be ***finite***, if its cardinal number is a natural number. A set is said to be ***infinite*** if it is not finite.

Denumerable set: A set A is said to be **denumerable**, if $\sim \boldsymbol{N}$ **,**$i.e.$, A is equivalent to the set of natural numbers. The cardinality of a denumerable set is denoted by the symbol $\mathcal{N}_0$ (read as *aleph null* or *aleph not*).The use of $k(A)$ is restricted to denote only the cardinality of a finite set A

Countable and uncountable sets: A set is said to be ***countable***, if it is either finite or denumerable. A set is said to be ***nondenumerable*** or ***uncountable*** if it is infinite and not denumerable.

Note: An important difference between a finite and an infinite set is that no proper subset of a finite set can be equivalent to itself, because a one-to-one correspondence between such sets is not possible.

Theorem 1: An infinite subset of a denumerable set is also denumerable.

Proof: Let A be a given denumerable set. Let S be any infinite subset of A . Since A is denumerable, $A \sim \boldsymbol{N}$ **,** that is , there exists a one-to-one correspondence between A and $\boldsymbol{N}$ **.** Let $f: \boldsymbol{N} \longrightarrow A$ be the bijective function, therefore, the elements of A can be arranged as $f(1), f(2), f(3)$, …. . Now, delete from this list those elements which are not in S. The remaining elements in the list are precisely the elements of S and they are infinite since S is infinite. Denote these elements by $f(i_1), f(i_2), f(i_3)$, …. . Define a function $g: \boldsymbol{N} \longrightarrow S$ by $g(n) = f(i_n)$. Now $g(n_1) = g(n_2) \Longrightarrow f\left(i_{n_1}\right) = f\left(i_{n_2}\right) \Longrightarrow i_{n_1} = i_{n_2}$
(since f is injective)$\Longrightarrow n_1 = n_2$. This shows that g is injective.

Let x be any element of S . Then $x = f(i_k)$ for some $i_k \in \boldsymbol{N}$ and there exists a $k \in \boldsymbol{N}$ such that $g(i_k) = f(i_k) = x$. This shows that g is surjective. Thus $g: \boldsymbol{N} \longrightarrow S$ is bijective and hence S is denumerable. Hence the theorem.

Enumeration: A sequence which is used to establish one-to-one correspondence with the elements of a set S is called an *enumeration*.

Example 4: Show that $\boldsymbol{Z}$, the set of integers is denumerable.

Proof: Define a function $f: \boldsymbol{N} \longrightarrow \boldsymbol{Z}$ by

$$f(n) = \begin{cases} \dfrac{n}{2} \quad , & if\ n\ is\ even \\ -\left(\dfrac{n-1}{2}\right), & if\ \ n\ is\ odd \end{cases}$$

This function enumerates the elements of $\boldsymbol{Z}$ as shown below:

$$\begin{array}{c} \\ f \\ \\ \end{array} \begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots\cdots.. \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots\cdots. \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & \cdots\cdots. \end{array}$$

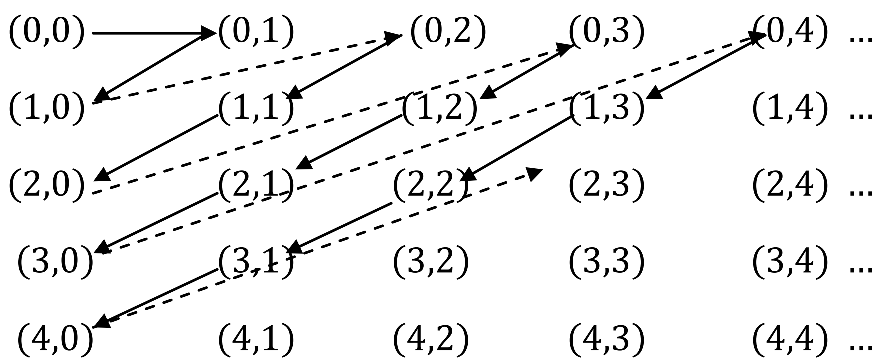
f is injective: Let $n_1, n_2 \in \boldsymbol{N}$. If n_1 is even and n_2 is odd then $f(n_1) = f(n_2) \Longrightarrow \frac{n_1}{2} = -\left(\frac{n_2-1}{2}\right) \Longrightarrow n_1 + n_2 = 1$ and this is not possible. Therefore n_1, n_2 are both even or both odd. Then $f(n_1) = f(n_2) \Longrightarrow n_1 = n_2$. This shows that f is injective.

Let x be any arbitrary element in $\boldsymbol{Z}$. Then x is either positive or nonpositive . If x is positive then there is an even number $y = 2x$ such that $f(y) = \frac{y}{2} = x$. If x is nonpositive then there is an odd natural number $y = -2x + 1$ such that $f(y) = -\left(\frac{y-1}{2}\right) = x$. In any case, each element $x \in \boldsymbol{Z}$ has a pre-image under f, showing f is surjective.

Thus, f is bijective and $\boldsymbol{Z}$ is denumerable.

Example 5: Let $\boldsymbol{W} = \{0,1,2,3,\dots\} = \boldsymbol{N} \cup \{0\}$.Show that $\boldsymbol{W} \times \boldsymbol{W}$ is denumerable.

Solution: We have $\boldsymbol{W} \times \boldsymbol{W} = \{(m,n) | m,n \in W\}$, write the elements of $\boldsymbol{W} \times \boldsymbol{W}$ as shown below:



Now, arrange the elements of $\boldsymbol{W} \times \boldsymbol{W}$ in the order shown by the arrows, namely,

$(0,0), (0,1), (1,0), (0,2), (1,1)$, $(2,0), (0,3), (1,2), (2,1), (3,0), (0,4), (1,3),$

$(2,2), (3,1), (4,0), \dots, \dots$

Define a mapping $f: \boldsymbol{W} \times \boldsymbol{W} \longrightarrow \boldsymbol{N}$ by

$$\boldsymbol{f(m,n) = \frac{1}{2}(m+n+1)(m+n) + m + 1}$$

Notice that f maps $(0,0), (0,1), (1,0), (0,2), (1,1)$, $(2,0), \dots$ onto $1,2,3,4,5,6, \dots$

respectively. Further f is bijective. Thus, $\boldsymbol{W} \times \boldsymbol{W}$ is denumerable.

Example 6: Show that $\boldsymbol{N} \times \boldsymbol{N}$ is denumerable.

Solution: Notice that $\boldsymbol{N} \times \boldsymbol{N} \subset \boldsymbol{W} \times \boldsymbol{W}$ and $\boldsymbol{N} \times \boldsymbol{N}$ is an infinite set. Since $\boldsymbol{W} \times \boldsymbol{W}$ is denumerable, by Theorem 1, $\boldsymbol{N} \times \boldsymbol{N}$ is also denumerable.

Example 7: Show that the set $\boldsymbol{Q}^+$ of positive rational numbers is denumerable.

Solution: Obtain a subset S of $\boldsymbol{N} \times \boldsymbol{N}$ by deleting all ordered pairs (m,n) in which m and n are not relatively prime ($i.e$, m and n have a common factor greater than 1). Note that S contains at least $(1,1), (2,1), (3,1), (4,1), \dots$ .Therefore S is infinite. Since $\boldsymbol{N} \times \boldsymbol{N}$ is denumerable, and S is an infinite subset of $\boldsymbol{N} \times \boldsymbol{N}$, S is also denumerable(by Theorem 1).

We have $Q^+ = \left\{\frac{m}{n} | m, n \in \boldsymbol{N}, m \text{ and } n \text{ are relatively prime}\right\}$

Define a map $f: Q^+ \longrightarrow S$ by $f\left(\frac{m}{n}\right) = (m, n)$

Now, $f\left(\frac{m_1}{n_1}\right) = f\left(\frac{m_2}{n_2}\right) \Longrightarrow (m_1, n_1) = (m_2, n_2) \Longrightarrow m_1 = m_2, n_1 = n_2$

$$\Longrightarrow \frac{m_1}{n_1} = \frac{m_2}{n_2}$$

This shows f is injective. For any $(m, n) \in S$,(where m, n are relatively prime) there is an $\frac{m}{n} \in Q^+$ such that $f\left(\frac{m}{n}\right) = (m, n)$. This shows that f is surjective. Thus $f: Q^+ \longrightarrow S$ is bijective and $Q^+ \sim S$. Since S is denumerable $S \sim N$. Thus $Q^+ \sim S$, $S \sim \boldsymbol{N}$. Therefore $Q^+ \sim \boldsymbol{N}$ (since $\sim$ is transitive).This proves that Q^+ is denumerable.

Lemma 1: If A_1, A_2, … are a countable number of finite sets then $S = \bigcup_i A_i$ is countable.

Solution: We list the elements of A_1 ,then we list the elements of A_2 which do not belong to A_1, then we list the elements of A_3 which have not been listed in $A_1 \cup A_2$, and so on. We can always list the elements of each set, since each set is finite. Now define sets $B_1, B_2, B_3, \ldots$ as given below:

$$B_1 = A_1 \text{ and for } k \geq 2 \text{ , } B_k = A_k - (A_1 \cup A_2 \cup \ldots \cup A_{k-1})$$

Then, the sets B_i are disjoint and

$$S = \bigcup_i A_i = \bigcup_i B_i$$

Let $b_{i1}, b_{i2}, \ldots, b_{im_i}$ be all the elements of B_i. Then $S = \{b_{ij}\}$.

Now, we have two possibilities: either S is finite or infinite.

If S is infinite define a map $f: S \longrightarrow \boldsymbol{N}$ by

$$f\left(b_{ij}\right) = m_1 + m_2 + \cdots + m_{i-1} + j$$

It may be seen that f is bijective. Thus S is denumerable.

Therefore, S is either finite or denumerable, $i.e.$, S is countable.

Theorem 2: A countable union of countable sets is countable.

Proof: Suppose $A_1, A_2, \ldots$ are countable number of sets. Let $S = \bigcup_i A_i$.

If $A_1, A_2, \ldots$ are finite sets then S is countable (by the above Lemma 1…).

Suppose that the sets $A_1, A_2, \ldots$ are countable number of denumerable sets. Since A_i is denumerable, its elements can be indexed as

$$a_{i1}, a_{i2}, a_{i3}, \ldots$$

Now define sets $B_2, B_3, B_4, \ldots$ as follows:

$$B_k = \left\{a_{ij} \,|\, i + j = k\right\}$$

Note that $B_2 = \{a_{11}\}$, $B_3 = \{a_{12}, a_{21}\}$, $B_4 = \{a_{13}, a_{22}, a_{31}\}$, …. Observe that each B_k is finite and

$$S = \bigcup_i A_i = \bigcup_k B_k$$

By Lemma1, $\bigcup_k B_k$ is countable. Therefore, $S = \bigcup_i A_i$ is countable.

In any case countable union of countable sets is countable.

Example 8: The set $\boldsymbol{Q}$ of rational numbers is denumerable.

Solution: It is known that Q^+, the set of positive rational numbers is denumerable. Similarly Q^-, the set of negative rational numbers is also denumerable. Thus, $\boldsymbol{Q} = Q^- \cup \{0\} \cup Q^+$ is also denumerable (Since countable union of countable sets is countable).

Example 9: The open interval $(\mathbf{0},\mathbf{1})$ is equivalent to $\boldsymbol{R}$

Solution: Define a map $f:(0,1)\longrightarrow \boldsymbol{R}$ by

$$f(x)=\begin{cases}\dfrac{1}{2x}-1 & , \quad 0<x\leq\dfrac{1}{2}\\ \dfrac{1}{2(x-1)}+1 & , \quad \dfrac{1}{2}\leq x<1\end{cases}$$

It may be seen that f is bijective. Therefore $(0,1)\sim\boldsymbol{R}$**.**

Cantor's diagonal argument

We now show that the set of real numbers lying between 0 and 1 is not denumerable (i.e., uncountable). The proof is based on cantor's diagonal argument and the indirect method. We assume that the set $(0,1)$ is denumerable and then show that an element of the set is different from all those enumerated exists, showing that the enumeration is not exhaustive and hence arriving at a contradiction. The arrangement is called ***diagonal*** because to obtain this particular element, we move along the diagonal of an array.

The diagonal argument is used frequently in the theory of automata and other logical investigations.

This method of proof can be used for showing the nondenumerabilty of other sets also.

Theorem 3: The open interval $(\mathbf{0},\mathbf{1})$ is nondenumerable.

Solution: Assume that $(0,1)$ is denumerable. Then the elements of S can be arranged in an infinite sequence $s_1,s_2,s_3,\ldots$. It is known that every positive real number less than 1 can be expressed as $s=0.y_1y_2y_3\ldots$ where $y_i\in\{0,1,2,\ldots,9\}$ and s has an infinite number of nonzero $y_i\,'s$ .This statement is true because the real numbers such as 0.5 and 0.312 can be written as $0.49999\ldots$ and $0.311999\ldots$ respectively. In the light of this fact , we can write the elements $s_1,s_2,s_3,\ldots.$ as

$$s_1 = 0.a_{11}a_{12}a_{13} \dots a_{1n} \dots$$

$$s_2 = 0.a_{21}a_{22}a_{23} \dots a_{2n} \dots$$

$$s_3 = 0.a_{31}a_{32}a_{33} \dots a_{3n} \dots$$

$$s_4 = 0.a_{41}a_{42}a_{43} \dots a_{4n} \dots \quad \text{and so on...}$$

Construct a real number $r = 0.b_1b_2b_3 \dots b_n \dots$,where $b_j = 1$ if $a_{jj} \neq 1$ and $b_j = 2$ if $a_{jj} = 1$ for $j = 1,2,3, \dots$.Notice that r is not equal to any of the numbers $s_1, s_2, s_3, \dots$., because r differs from s_1 in the first position, from s_2 in the second position and so on. This shows that $r \notin (0,1)$ which is a contradiction . Thus the open interval $(0,1)$ is nondenumerable

Corollary: The set $\boldsymbol{R}$ of real numbers is nondenumerable.

Proof: The proof is by contradiction. Assume that $\boldsymbol{R}$ is denumerable. Note that $(0,1) \subset \boldsymbol{R}$ and $(0,1)$ is infinite. By Theorem 1, $(0,1)$ is denumerable. This is a contradiction. Thus $\boldsymbol{R}$ is nondenumerable.

Cardinality of $\boldsymbol{R}$: The cardinality of $\boldsymbol{R}$ is denoted by $\boldsymbol{c}$ and is called the **power of continuum**. That is, $\boldsymbol{card}(\boldsymbol{R}) = \boldsymbol{c}$

Note:

1. The result that the nondenumerabilty of the set of real numbers in the open interval $(0,1)$ is true for the set of real numbers in any open interval (a, b) with $a < b$.
2. The cardinality of all these sets (a, b),$a < b$ which are mutually equivalent and equivalent to $\boldsymbol{R}$, is denoted by $\boldsymbol{c}$
3. The sets $\boldsymbol{R}$,$\boldsymbol{R}^2$,$\boldsymbol{R}^3$, … are all nondenumerable and have the cardinality c

Example 10: Prove that the set of irrational numbers is nondenumerable.

Solution: It is known that $\boldsymbol{R} = \boldsymbol{Q} \cup X$, where X is the set of irrational numbers. To prove that X is nondenumerable. Assume the contrary, $i.e.$, X is denumerable. It is known that $\boldsymbol{Q}$ is denumerable. Therefore $\boldsymbol{Q} \cup X$ is also denumerable, $i.e.$, $\boldsymbol{R}$ is denumerable, a contradiction. Therefore X is nondenumerable.

We now introduce an ordering relation on the family of subsets of the universal set and a corresponding ordering on the set of cardinal numbers.

If A and B are sets such that A is equivalent to a subset of B, then we say that A is ***dominated*** by B or A **precedes** B and write $A \preccurlyeq B$.

If α and β denote the cardinal numbers of the sets A and B respectively and if $A \preccurlyeq B$, then we say that ***α is less than or equal to β***. Symbolically,

$$\boldsymbol{A \preccurlyeq B \iff \alpha \leq \beta}$$

Note: The choice of the term *less than or equal to* express the relation on the set of cardinal numbers is based on the fact that for finite sets $A \preccurlyeq B$ implies the natural number representing $k(A)$ is less than or equal to the natural number representing $k(B)$.
From the definition, it is clear that the relation $\preccurlyeq$ and $\leq$ are both reflexive and transitive. The **Schroder – Bernstein theorem** states the following:

If $\boldsymbol{A}$ and $\boldsymbol{B}$ are sets such that $\boldsymbol{A \preccurlyeq B}$ and $\boldsymbol{B \preccurlyeq A}$ then $\boldsymbol{A \sim B}$.

Associated with the relations $\preccurlyeq$ and $\leq$, we have the relations $\prec$ and $<$ given by

$$A \prec B \iff A \preccurlyeq B \text{ and } A \nsim B.$$

$$\alpha < \beta \iff \alpha \leq \beta \text{ and } \alpha \neq \beta.$$

Since $\boldsymbol{N}$ is a proper subset of real numbers, we have $\boldsymbol{N} \preccurlyeq \boldsymbol{R}$. Further $\boldsymbol{N} \nsim \boldsymbol{R}$, since $\boldsymbol{N}$ is denumerable and $\boldsymbol{R}$ is nondenumerable. Therefore, $\boldsymbol{N} \preccurlyeq \boldsymbol{R}$ and $\boldsymbol{N} \nsim \boldsymbol{R} \Longrightarrow \boldsymbol{N} \prec \boldsymbol{R}$. From this it follows that $card\ \boldsymbol{N} < card\ \boldsymbol{R}$, i.e., $\mathcal{N}_0 < \boldsymbol{c}$.

For a given set, can we find another set whose cardinality greater than that of the given set? For finite sets, such a construction is easy. For infinite sets, a theorem due to Cantor shows the existence of such sets.

Theorem 4 (Cantor): Power Set Theorem

For any set A, $A \prec 2^A$ where 2^A is the power set of A. If α is the cardinality of A and 2^α denotes the cardinality of 2^A, then $\alpha < 2^\alpha$.

(See P8 for proof)

Remark: The cardinality of 2^N is c. That is $\mathbf{2^{\mathcal{N}_0} = c}$.

P1:

Any two closed intervals $[\boldsymbol{a}, \boldsymbol{b}]$, $\boldsymbol{a} < b$ and $[\boldsymbol{c}, \boldsymbol{d}]$, $\boldsymbol{c} < d$ are equivalent.

Solution:

Define a map f: $[a, b] \longrightarrow [c, d]$ by

$$f(x) = c + \frac{d-c}{b-a}(x-a)$$

Notice that $f(a) = c$, $f(b) = d$

Let $\alpha, \beta \in [a, b]$ such that $f(\alpha) = f(\beta)$. Then

$$c + \frac{d-c}{b-a}(\alpha - a) = c + \frac{d-c}{b-a}(\beta - a)$$

$\Longrightarrow$ $\alpha - a = \beta - a$ $\Longrightarrow$ $\alpha = \beta$. This proves f is injective.

Let β be any element in $[c, d]$.

Do we have a α such that $f(\alpha) = \beta$? If so then $c + \frac{d-c}{b-a}(\alpha - a) = \beta$,

i.e., $\alpha = a + \frac{b-a}{d-c}(\beta - c)$ (solve for α)

Clearly $a \leq \alpha \leq b$. Thus β has a pre-image. This shows that f is surjective.

Therefore, $[a, b] \sim [c, d]$. Thus, any two closed intervals are equivalent.

P2:

If A and B are sets with the same cardinality and; C and D are sets with the same cardinality, then $A \times C$ and $B \times D$ have the same cardinality.

Solution:

Given that A and B have the same cardinality and; C and D have the same cardinality. That is, $A \sim B$ and $C \sim D$.

Let f and g be the bijections from A to B and from C to D respectively, *i.e.,* $f: A \longrightarrow B$ and $g: C \longrightarrow D$ are bijections. Required to prove that $A \times C \sim B \times D$

Define a map $h: A \times C \longrightarrow B \times D$ by $h(a,c) = \big(f(a), g(c)\big)$.

h is injective:

$$h(a_1,c_1) = h(a_2,c_2) \Longrightarrow \big(f(a_1), g(c_1)\big) = \big(f(a_2), g(c_2)\big)$$

$\Longrightarrow f(a_1) = f(a_2)$ and $g(c_1) = g(c_2)$

$\Longrightarrow a_1 = a_2$ and $c_1 = c_2$ (since f, g are injective)

$\Longrightarrow (a_1,c_1) = (a_2,c_2)$

Thus, h is injenctive.

h is surjunctive:

Let (b,d) be any element of $B \times D$. That is, b and d are arbitrary elements of B and D respectively. Since f is surjective, there exists an element $x \in A$ such that $f(x) = b$. Similarly, there exists an element $y \in C$ such that $g(y) = d$.Thus, there is an element $(x,y) \in A \times C$ such that

$$h(x,y) = \big(f(x), g(y)\big) = (b,d)$$

This shows that h is surjective. Therefore, $h : A \times C \longrightarrow B \times D$ is bijective.

Thus, $A \times C \sim B \times D$ and so $A \times C$ and $B \times D$ have the same cardinality.

P3:

The relation of equivalence (or equipotence) of sets on any family of sets is an equivalence relation.

Solution:

Let F be a family of sets and let $\sim$ denotes the relation of equivalence of sets on F.

Recall that, for any $A, B \in F$, $A \sim B$ iff there is a bijection between A and B.

(i) *$\sim$ is reflexive:*

Let A be any sets in F. We have an identify function $i : A \longrightarrow A$ defined by $i(x) = x$, $\forall x \in A$. It is known that the identity function is bijective. Thus, $A \sim A$, for every $A \in F$. Therefore, the relation $\sim$ is reflexive.

(ii) *$\sim$ is symmetric:*

Let $A, B \in F$ and $A \sim B$.

$A \sim B \Longrightarrow$ There exists a bijective function $f : A \longrightarrow B$. It is known that the inverse of a bijective function exists and it is bijective.

$\Longrightarrow f^{-1} : B \longrightarrow A$ exists and f^{-1} is bijective $\Longrightarrow B \sim A$

Thus, $A \sim B \Longrightarrow B \sim A$. Therefore, the relation $\sim$ is symmetric.

(iii) *$\sim$ is transitive:*

Let $A, B, C \in F, A \sim B$ and $B \sim C$.

$A \sim B$ and $B \sim C \Longrightarrow$ There exist bijections $f : A \longrightarrow B$ and $g : B \longrightarrow C$.

$\Longrightarrow g \circ f : A \longrightarrow C$ is bijective (∵The composition of two bijective functions is also bijective)

$\Longrightarrow A \sim C$

Therefore, the relation $\sim$ is transitive.

Thus, the relation $\sim$ (equivalence of sets) defined on F is an equivalence relation.

P4:

Determine whether each of these sets is countable or uncountable. For those that are countable, exhibit a one-to-one correspondence between the set of natural numbers and the set of

a) the negative integers
b) the odd integers
c) the real numbers between $\mathbf{0}$ and $\frac{\mathbf{1}}{\mathbf{2}}$

Solution:

a) We have $\boldsymbol{Z}^{-} = \{\dots, -4, -3, -2, -1\}$. Clearly, $\boldsymbol{Z}^{-}$ infinite.
Define a map $f: \boldsymbol{N} \longrightarrow \boldsymbol{Z}^{-}$ by $f(n) = -n,\ n \in \boldsymbol{N}$.
It is injective and surjective (show!)

Thus, $\boldsymbol{Z}^{-} \sim \boldsymbol{N}$. Thus, $\boldsymbol{Z}^{-}$ is denumerable. Therefore, $\boldsymbol{Z}^{-}$ is countable.

b) We have $A = \{\dots, -5, -3, -1, 1, 3, 5, \dots\} = B \cup C$, where $= \{1, 3, 5, \dots\}$, the set of positive odd integers and $C = \{\dots, -5, -3, -1\}$, the set of negative odd integers. Required to show that A is countable.

Clearly, both B and C are infinite sets. Define a map $f: \boldsymbol{N} \longrightarrow B$ by $f(n) = 2n - 1$. It is bijective (show!). Thus, $\boldsymbol{N} \sim B$. Therefore, $B \sim \boldsymbol{N}$ (why?), B is denumerable and B is countable.

Notice that $B \sim C$. Therefore, $C \sim B$ and $B \sim \boldsymbol{N} \Longrightarrow C \sim \boldsymbol{N}$ (why?) .This shows that C is countable.

Since B and C are countable; $A = B \cup C$ is also countable (*because countable union of countable sets is countable*).

c) We have $\left(0, \frac{1}{2}\right)$, $i.e.$, $\left\{x \mid x \in \boldsymbol{R} \wedge \left(0 < x < \frac{1}{2}\right)\right\}$. It is uncountable, because the set of real numbers in any open interval (a, b) with $a < b$, is uncountable.

P5:

Determine whether each of these sets is countable or uncountable. For those that are countable, exhibit a one-to-one correspondence between the set of natural numbers and the set of

a) **the integers that are multiples of 7**
b) **the integers not divisible by 3**
c) **all rational numbers that cannot be written with denominators less than 4**

Solution:

a) We have $\boldsymbol{Z_7}$, $i.e$, the set of integers that are multiples of 7

$$= \{\dots, -21, -14, -7, 0, 7, 14, 21, \dots\}$$

Clearly $\boldsymbol{Z_7}$ is infinite.

First note that $\boldsymbol{Z} \sim \boldsymbol{Z_7}$**.** Define a map $f : \boldsymbol{Z} \longrightarrow \boldsymbol{Z_7}$ by $f(n) = 7n, n \in \boldsymbol{Z}$. It is easy to see that f is bijective. Therefore, $\boldsymbol{Z} \sim \boldsymbol{Z_7}$

Now, $\boldsymbol{Z_7} \sim \boldsymbol{Z}$ and $\boldsymbol{Z} \sim \boldsymbol{N}$ ($\because Z$ is denumerable) $\Longrightarrow \boldsymbol{Z_7} \sim \boldsymbol{N}$ ($\because \sim$ is transitive)

$\Longrightarrow \boldsymbol{Z_7}$ is denumerable. Therefore, $\boldsymbol{Z_7}$ is countable

b) We have $\boldsymbol{Z_3} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$, $\boldsymbol{Z} - \boldsymbol{Z_3}$ is the set of all integers not divisible by 3 and it is an infinite set. Note that Z is denumerable and $\boldsymbol{Z} - \boldsymbol{Z_3} \subset \boldsymbol{Z}$. Therefore, $\boldsymbol{Z} - \boldsymbol{Z_3}$ is denumerable (*by Theorem: Every infinite subset of a denumerable set is denumerable*). Thus $\boldsymbol{Z} - \boldsymbol{Z_3}$ is countable.

c) We have $\boldsymbol{Q}$, the set of rational numbers. Let A be the set of all rational numbers which are written with the denominator less than 4. That is

$$A = \left\{\frac{p}{1} \mid p \in \boldsymbol{Z}\right\} \cup \left\{\frac{p}{2} \mid p \in \boldsymbol{Z}\right\} \cup \left\{\frac{p}{3} \mid p \in \boldsymbol{Z}\right\}$$

Clearly, A is infinite. Now, $\boldsymbol{Q} - \boldsymbol{A}$ is the set of all rational numbers. That cannot be written with denominator less than 4. Note that $\boldsymbol{Q}$ is denumerable and $\boldsymbol{Q} - \boldsymbol{A} \subset \boldsymbol{Q}$. Therefore, $\boldsymbol{Q} - \boldsymbol{A}$ is denumerable (*by Theorem: Every infinite subset of a denumerable set is denumerable*). Thus, $\boldsymbol{Q} - \boldsymbol{A}$ is countable.

P6:

If A is uncountable and $A \subseteq B$ then B is uncountable.

Proof:

We have that A is an uncountable set and $A \subseteq B$. Required to prove that B is uncountable.

Now, A is uncountable $\Longrightarrow$ A is infinite and A is not denumerable. Since A is infinite, $A \subseteq B$; B must be an infinite set.

Assume that B is denumerable. Since A is infinite, $A \subseteq B$ and B is denumerable, A must be denumerable (*by Theorem: Every infinite subset of a denumerable set is denumerable*).This is a contradiction to the nondenumerabilty of A. Therefore, B is not denumerable. Thus, B is uncountable.

P7

If A is an uncountable set and B is a countable set then $A - B$ is uncountable.

Solution:

We have that A is an uncountable set and B is a countable set. Required to prove that $A - B$ is uncountable.

Assume the contrary, $i.e.$, Assume that $A - B$ is countable. Then

$$A = (A - B) \cup B$$

is countable, because countable union of countable sets is countable. This is a contradiction to the uncountability of A. The result now follows.

P8:

Theorem (Cantor): Power Set Theorem

For any set A, $A \prec 2^A$ where 2^A is the power set of A. If α is the cardinality of A and 2^α denotes the cardinality of 2^A, then $\alpha < 2^\alpha$.

Solution:

Let $f: A \longrightarrow 2^A$ be defined by $f(a) = \{a\}$ for every $a \in A$. If $f(a) = f(b)$ then $\{a\} = \{b\}$ and $a = b$. This shows that f is injective. Thus A is equivalent to a (proper) subset of 2^A. Therefore $A \preccurlyeq 2^A$.

To show that $A \prec 2^A$, we have to show that $A \nsim 2^A$, we show this by indirect method of proof.

Assume that $A \sim 2^A$. Let g: $A \longrightarrow 2^A$ be a bijection. For any $a \in A$, $g(a)$ is a subset of A (because $g(a)$ is an element of 2^A). We call a an *interior member* of A if $a \in g(a)$; otherwise a is called an *exterior member* of A.

Let B be the set of all exterior members of A, that is,

$$B = \{x|(x \in A) \wedge (x \notin g(x))\}$$

Clearly $B \subseteq A$. Therefore, $B \in 2^A$. Since g is onto, B has a pre-image say $b \in A$. That is, there exists an element $b \in A$ such that $g(b) = B$.

Now, we have two cases: either $b \in B$ or $b \notin B$.

(i) If $b \in B$ then $b \in A$ and $b \notin g(b)$. Since $g(b) = B$; $b \notin B$. This is a contradiction.

(ii) If $b \notin B$ then $b \in g(b)$. Since $g(b) = B$; $b \in B$. Again we arrive a contradiction.

This argument shows that $A \nsim 2^A$. Therefore $A \prec 2^A$.

If $ard(A) = \alpha$, then $card(2^A) = 2^\alpha$.Now, $\alpha < 2^\alpha$, since $A \prec 2^A$.

Hence the theorem.

MODULE-7

FUNCTIONS

2.7

Functions

In this section we study a particular class of relations called functions. We are primarily concerned with discrete functions which transform a finite set into another finite set. There are several such transformations involved in the computer implementation of any program. Computer output can be considered as function of input. A complier transforms a program into a set of machine language instructions (the object program). After introducing the concept of functions in general, we discuss unary and binary operations which form a class of functions. Such operations have important applications in the study of algebraic structures. Also discussed is a special class of functions known as hashing functions that are used in organizing files on a computer, along with other techniques associated with such organizations.

Function: Let A and B be two sets. A relation f from A to B is called a function if for every $a \in A$ there is a unique element $b \in B$ such that $(a, b) \in f$.

Note: A relation must satisfy the following two additional conditions to qualify to be a function.

(i) The domain of f must be A (not merely a subset of A)

(ii) The second requirement of uniqueness can be expressed as

$$\big((\boldsymbol{x}, \boldsymbol{y}) \in \boldsymbol{f}\big) \wedge \big((\boldsymbol{x}, \boldsymbol{z}) \in \boldsymbol{f}\big) \Rightarrow \boldsymbol{y} = \boldsymbol{z}$$

Terms such as *map* (or *mapping*), *operation*, *transformation* and *correspondence* are used as synonyms for *function*.

The notations $\boldsymbol{f} : \boldsymbol{A} \longrightarrow \boldsymbol{B}$ or $\boldsymbol{A} \xrightarrow{\boldsymbol{f}} \boldsymbol{B}$ are used to express f as a function from A to B.

For a function $\boldsymbol{f}: \boldsymbol{A} \longrightarrow \boldsymbol{B}$ if $(x, y) \in f$, then x is called the **argument** and the corresponding y is called the **image of $\boldsymbol{x}$ under $\boldsymbol{f}$**.

Instead of writing $(x, y) \in f$, it is customary to write $y = f(x)$ and to call $\boldsymbol{y}$ as the **value of the function $\boldsymbol{f}$ at $\boldsymbol{x}$**. The domain of f is denoted by $\boldsymbol{D_f}$ and $D_f = A$.The range of f is denoted by $\boldsymbol{R_f}$ and

$$\boldsymbol{R_f = \{y \in B | (\exists x \in A) \wedge (y = f(x))\}}$$

Note that $R_f \subseteq B$ and B is called the **codomain** of f.

Since a function is a relation, we can write a relation matrix or draw a graph to represent it when its domain and co domain are finite sets.

Note: From the definition of a function it follows that every row of its relation matrix have only one entry 1 and all other entries in the rows are 0's.

When the domain and co domain of a function f are infinite, the correspondence can be expressed more easily by a rule.

For example, $f(x) = x^2$, $x \in \boldsymbol{R}$ represents a function $\{(x, x^2) | x \in \boldsymbol{R}\}$ where $\boldsymbol{R}$ is the set of real numbers and $f : \boldsymbol{R} \longrightarrow \boldsymbol{R}$**.**

Note: A program written in a high-level language is transformed (or mapped) into a machine language by a compiler. Similarly, the output from a computer is a function of its input**.**

Restriction of a function: If $\boldsymbol{f : A \longrightarrow B}$ and $X \subseteq A$, then $f \cap (X \times B)$. (i.e., the intersection of the ordered pairs of f and $X \times B$) is a function from X to B called the **restriction of $\boldsymbol{f}$ to $\boldsymbol{X}$** and is written as $\boldsymbol{f/X}$. If g is the restriction of f then f is called the **extension** of g.

Note: Notice that $\boldsymbol{(f/X): X \longrightarrow B}$ is such that for any $x \in X$, $(f/X)(x) = f(x)$. The domain of f/X is X, while that of f is A.

If g is a restriction of f then $D_g \subseteq D_f$ and $g(x) = f(x)$, $\forall x \in D_g$ and as relations $g \subseteq f$.

Example 1: Let $\boldsymbol{f : R \longrightarrow R}$ be given by $\boldsymbol{f(x) = x^2}$. We have $\boldsymbol{N \subset R}$ and

$$\boldsymbol{f/N = \{(1, 1), (2, 4), (3, 9), (4, 16), \ldots\}}$$

Equality of functions: Equality of functions can be defined in terms of the equality of sets, since functions are sets of ordered pairs. Note that this definition also requires that equal functions have the same domain and the same range.

It is known that not all possible subsets of $A \times B$ are functions from A to B.

We know that not all relations from A to B are functions from A to B. The collection of all those relations from A to B which are functions from A to B is denoted by $\boldsymbol{B^A}$.

Example 2: Let $\boldsymbol{A = \{a, b, c\}}$ and $\boldsymbol{B = \{0, 1\}}$. Write all functions from $\boldsymbol{A}$ to $\boldsymbol{B}$

Solution: We have $A \times B = \{(a, 0), (a, 1), (b, 0), (b, 1), (c, 0), (c, 1)\}$

and there are 2^6 relations from A to B. Of these, only the following 2^3 relations are function from A to B:

$f_0 = \{(a, 0), (b, 0), (c, 0)\}$

$f_1 = \{(a, 0), (b, 0), (c, 1)\}$

$f_2 = \{(a, 0), (b, 1), (c, 0)\}$

$f_3 = \{(a, 0), (b, 1), (c, 1)\}$

$f_4 = \{(a, 1), (b, 0), (c, 0)\}$

$f_5 = \{(a, 1), (b, 0), (c, 1)\}$

$f_6 = \{(a, 1), (b, 1), (c, 0)\}$

$f_7 = \{(a, 1), (b, 1), (c, 1)\}$

The number of function from $\boldsymbol{A}$ to $\boldsymbol{B}$ when $\boldsymbol{A}$, $\boldsymbol{B}$ are finite

Let A and B be finite sets with m and n elements respectively. Since the domain of any function from A to B is A, there are exactly m ordered pairs in each of the functions. Further, any element $x \in A$ can have any one of the n elements of B as its image; therefore, there are $n \times n \times \ldots \times n$ (m times)$= n^m$ possible distinct functions.

Note: The number n^m explains why the notation B^A is used to represent the set of all functions from A to B. The same notation is used even when A or B are infinite sets.

A mapping $f : A \longrightarrow B$ is called **onto** (**surjective** or **surjection**) if the range $\boldsymbol{R_f = B}$; otherwise, it is called an **into function**.

A mapping $f : A \longrightarrow B$ is called **one-to-one** (**injective** or **1-1**) if distinct elements of A are mapped into distinct elements of B. In other words, f is one-to-one if

$$\boldsymbol{x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)}$$

or equivalently

$$\boldsymbol{f(x_1) = f(x_2) \Rightarrow x_1 = x_2}$$

Note: Let A and B be finite sets. A mapping $f : A \longrightarrow B$ is one-to-one only if $|\boldsymbol{A}| \leq |\boldsymbol{B}|$.

A mapping $f : A \longrightarrow B$ is called **bijective** if it is both *injective* and *surjective*. Such a mapping is also called a **one-to-one correspondence** between A and B.

Note: For $f : A \longrightarrow B$ to be bijective, when A, B are finite, requires that $|A| = |B|$.

Composition of functions

The operation of composition of relations can be extended to functions.

Let $\boldsymbol{f : A \longrightarrow B}$ and $\boldsymbol{g : B \longrightarrow C}$ be two functions. The **composite relation** $g \circ f$ such that

$$\boldsymbol{g \circ f = \{(x, z) | (x \in A) \wedge (z \in C) \wedge (\exists y)\big(y \in B \wedge y = f(x) \wedge z = g(y)\big)\}}$$

is called the **composition** of functions (or **relative product** of functions f and g. More precisely, $g \circ f$ is called the **left composition** of g with f.Note that, **if $\boldsymbol{R_f \subseteq D_g}$ then $\boldsymbol{g \circ f}$ is nonempty, otherwise $\boldsymbol{g \circ f}$ is empty .**

$\boldsymbol{g \circ f}$ is a function from $\boldsymbol{A}$ to $\boldsymbol{C}$: Assume that $g \circ f$ is not a function. Suppose that $g \circ f$ is not empty. That is assume that (x, z_1) and (x, z_2) are both in $g \circ f$. That is there is an element $y \in B$ such that $y = f(x)$ and $z_1 = g(y)$; also $z_2 = g(y)$. This shows that $(y, z_1) \in g$ and $(y, z_2) \in g$. Since g is a function, this is not possible. Thus, $g \circ f$ is a functioin.

Any function g for which $g \circ f$ can be formed is said to be **left-composable** with the function f. In such a case, $\boldsymbol{(g \circ f)(x) = g\big(f(x)\big)}$, where x is in the domain of $g \circ f$.

Associativity of the composition of functions: Let $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$. Then the composite functions $g \circ f : A \longrightarrow C$ and $h \circ g : B \longrightarrow D$ can be formed. Other composite functions such as $h \circ (g \circ f) : A \longrightarrow D$ and $(h \circ g) \circ f : A \longrightarrow D$ can also be formed. Since each function is a relation and the composition of relations is associative; the composition of functions is also associative. Therefore, $\boldsymbol{h \circ (g \circ f) = (h \circ g) \circ f}$.

Since the composition of functions is associative we may drop parenthesis in writing the associativity, $i.e.$,

$$\boldsymbol{h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f}$$

Example 3: Let $\boldsymbol{A = \{1, 2, 3\}}$, $\boldsymbol{B = \{p, q\}}$ and $\boldsymbol{C = \{a, b\}}$. Let $\boldsymbol{f : A \longrightarrow B}$ be $\boldsymbol{f = \{(1, p), (2, p), (3, q)\}}$ and $\boldsymbol{g : B \longrightarrow C}$ be $\boldsymbol{g = \{(p, b), (q, b)\}}$. Find $\boldsymbol{g \circ f}$.

Solution: We have $A \xrightarrow{f} B \xrightarrow{g}$, $A \xrightarrow{g \circ f} C$

$$\boldsymbol{g \circ f = \{(1, b), (2, b), (3, b)\}}$$

Example 4: Let $\boldsymbol{A = \{1, 2, 3\}}$ and $\boldsymbol{f, g, h}$ and $\boldsymbol{s}$ be functions on $\boldsymbol{A}$ given by

$\boldsymbol{f = \{(1, 2), (2, 3), (3, 1)\}}$, $\boldsymbol{g = \{(1, 2), (2, 1), (3, 3)\}}$

$\boldsymbol{h = \{(1, 1), (2, 2), (3, 1)\}}$, $\boldsymbol{s = \{(1, 1), (2, 2), (3, 3)\}}$. Find $\boldsymbol{f \circ g}$, $\boldsymbol{g \circ f}$, $\boldsymbol{f \circ h \circ g}$, $\boldsymbol{s \circ g}$, $\boldsymbol{g \circ s}$, $\boldsymbol{s \circ s}$ and $\boldsymbol{f \circ s}$.

Solution:

$f \circ g = \{(1,3), (2,2), (3,1)\}$, $g \circ f = \{(1,1), (2,3), (3,2)\}$

Note that $f \circ g \neq g \circ f$.

$f \circ h \circ g = \{(1,3), (2,2), (3,2)\}$

$s \circ g = \{(1,2), (2,1), (3,3)\} = g = g \circ s$

Note that $s \circ s = s$, $f \circ s = s$.

Example 5: Let $f(x) = x + 2$, $g(x) = x - 2$ and $h(x) = 3x$ for $x \in R$. Find $g \circ f, f \circ g, g \circ g, f \circ h, h \circ g, h \circ f$ and $f \circ h \circ g$.

Solution:

(i) We have $(g \circ f)(x) = g\big(f(x)\big) = g(x+2) = (x+2) - 2 = x$.
Therefore, $g \circ f = \{(x,x) | x \in \boldsymbol{R}\}$

(ii) $(f \circ g)(x) = f\big(g(x)\big) = f(x-2) = (x-2) + 2 = x$.
Therefore, $f \circ g = \{(x,x) | x \in \boldsymbol{R}\} = g \circ f$.

(iii) $f \circ f = \{(x, x+4) | x \in \boldsymbol{R}\}$

(iv) $g \circ g = \{(x, x-4) | x \in \boldsymbol{R}\}$

(v) $(f \circ h)(x) = f\big(h(x)\big) = f(3x) = 3x + 2$

(vi) $(h \circ g)(x) = h\big(g(x)\big) = h(x-2) = 3(x-2) = 3x - 6$
Therefore, $h \circ g = \{(x, 3x-6) | x \in \boldsymbol{R}\}$.

(vii) $(h \circ f)(x) = h\big(f(x)\big) = h(x+2) = 3(x+2) = 3x + 6$
Therefore, $h \circ f = \{(x, 3x+6) | x \in \boldsymbol{R}\}$.

(viii) $\big((f \circ h) \circ g\big)(x) = (f \circ h)\big(g(x)\big) = f\big(h(x-2)\big) = f(3x-6)$
$= 3x - 6 + 2 = 3x - 4$
Therefore, $(f \circ h) \circ g = \{(x, 3x-4) | x \in \boldsymbol{R}\} = (f \circ h) \circ g = f \circ h \circ g$.

**Example 6: Let $f : R \longrightarrow R$ be given by $f(x) = -x^2$ and $g : R^+ \longrightarrow R^+$ be given by $(x) = \sqrt{x}$, where R^+ is the set of non-negative real numbers. Find $f \circ g$.
Is $g \circ f$ defined.**

Solution:

(i) Note that $R_g = \boldsymbol{R}^+ \subseteq \boldsymbol{R} = D_f$. Therefore, $f \circ g$ is defined and
$(f \circ g)(x) = f\big(g(x)\big) = f\big(\sqrt{x}\big) = -x$, for $x \in \boldsymbol{R}^+$.

(ii) Note that R_f is the set of nonpositive real numbers and it is not included in domain of g. Therefore, $g \circ f$ is not defined.

Inverse function

The converse of a relation R from A to B is defined to be a relation $\bar{R}$ from B to A such that $(y,x) \in \bar{R} \Leftrightarrow (x,y) \in R, i.e.$, the ordered pairs of $\bar{R}$ are obtained from those of R by simply interchanging the components.

Let $\bar{f}$ be the converse of f, where $\boldsymbol{f : A \longrightarrow B}$ is considered as a relation from A to B. Now $\bar{f}$ may not be a function, because the $D_{\bar{f}}$ may not be B but only a subset of B.

$\bar{f}$ may not be a function from R_f to A because it may not satisfy the uniqueness condition. For example, (x_1, y) and (x_2, y) may be in f, so that (y, x_1) and (y, x_2) will be in $\bar{f}$.

For a function $f : A \longrightarrow B$, $\bar{f}$ is a function only if f is one-to-one. But this condition does not guarantee that $\bar{f}$ will be a function from B to A. However, if is bijective then $\bar{f}$ is a function from B to A. In such case $\bar{f}$ is written as $\boldsymbol{f^{-1}}$ so that $\boldsymbol{f^{-1} : B \longrightarrow A}$ and $\boldsymbol{f^{-1}}$ is called the **inverse** of the function f. If f^{-1} exists then f is said to be **invertible**.

Note: If f is a bijective function from A to B then $\boldsymbol{f^{-1} : B \longrightarrow A}$ exists and f^{-1} is also bijective.

A map $\boldsymbol{I_A : A \longrightarrow A}$ is called an **identity map** if $I_A = \{(x,x) | x \in A\}$.

Theorem 1:

(a) **For any function $\boldsymbol{g : A \longrightarrow A}$, the function $\boldsymbol{I_A \circ g = g \circ I_A = g}$.**
For any $x \in A$, $(I_A \circ g)(x) = I_A\big(g(x)\big) = g(x)$.Therefore $I_A \circ g = g$.
Similarly $g \circ I_A = g$.

(b) **If $\boldsymbol{f : A \longrightarrow B}$ and $\boldsymbol{g : B \longrightarrow A}$, then $\boldsymbol{g = f^{-1}}$ only if $\boldsymbol{g \circ f = I_A}$ and $\boldsymbol{f \circ g = I_B}$.**

(c) **If $\boldsymbol{f : A \longrightarrow B}$ is invertible then $\boldsymbol{f^{-1} \circ f = I_A}$ and $\boldsymbol{f \circ f^{-1} = I_B}$.**

(d) **If $\boldsymbol{f : A \longrightarrow B}$ and $\boldsymbol{g : B \longrightarrow A}$ are bijective then $\boldsymbol{(g \circ f)^{-1} = f^{-1} \circ g^{-1}}$**

Theorem 2: Let $\boldsymbol{F_A}$ be the collection of all bijective function on a nonempty set $\boldsymbol{A}$. Then the following properties hold:

i) **For any , $\boldsymbol{g} \in \boldsymbol{F_A}$, $\boldsymbol{f \circ g}$ and $\boldsymbol{g \circ f}$ are also in $\boldsymbol{F_A}$.**
This is called ***closure property*** of the operation of composition.

ii) **For any $\boldsymbol{f, g, h} \in \boldsymbol{F_A}$,$(\boldsymbol{f} \circ \boldsymbol{g}) \circ \boldsymbol{h} = \boldsymbol{f} \circ (\boldsymbol{g} \circ \boldsymbol{h})$**
$i.e.$, the composition is associative.

iii) **There exists a function $\boldsymbol{I_A} \in \boldsymbol{F_A}$ called the *identity map* such that $\boldsymbol{I_A} \circ \boldsymbol{f} = \boldsymbol{f} \circ \boldsymbol{I_A} = \boldsymbol{f}$ for all $\boldsymbol{f} \in \boldsymbol{F_A}$.**

iv) **For every $\boldsymbol{f} \in \boldsymbol{F_A}$ there exists an inverse $\boldsymbol{f^{-1}} \in \boldsymbol{F_A}$ such that**

$$\boldsymbol{f} \circ \boldsymbol{f^{-1}} = \boldsymbol{f^{-1}} \circ \boldsymbol{f} = \boldsymbol{I_A}.$$

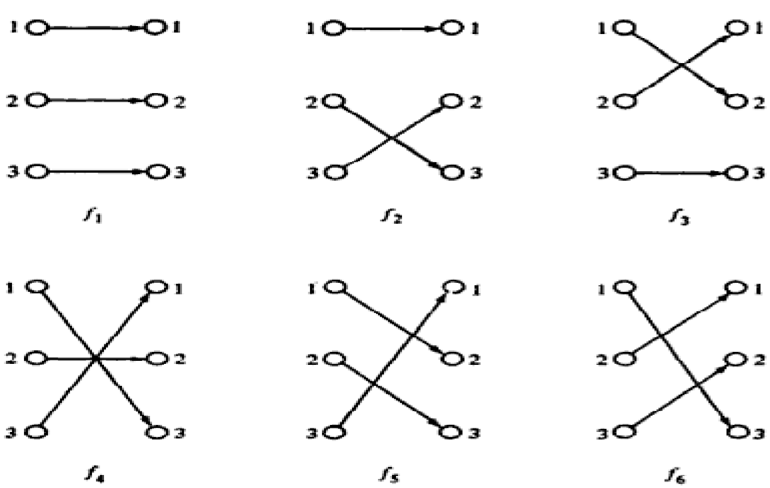
Note:

(1) Closure and associative properties of the composition of maps hold for all the functions of $\boldsymbol{A^A}$ (i.e., for all function on A) and not only for the functions of F_A.

(2) If A is a finite set with n elements $|F_A| = n!$

Example 7: Let $\boldsymbol{A = \{1, 2, 3\}}$. Find all elements of $\boldsymbol{F_A}$ and find the inverse of each element.

Solution: The following are the $3! = 6$ functions $f_1, f_2, \dots, f_6$ of F_A, where $A = \{1,2,3\}$.



Note that

(a) f_1 is the identity map of F_A. Therefore, $f_1 \circ f_i = f_i \circ f_1 = f_i$, for $i = 1,2,\dots,6$.

(b) $f_2 \circ f_2$ maps 1,2 and 3 onto 1,2 and 3 respectively; Therefore, $f_2 \circ f_2 = f_1$. Thus, ${f_2}^{-1} = f_2$, similarly ${f_3}^{-1} = f_3$, ${f_4}^{-1} = f_4$.

(c) $f_5 \circ f_6 = f_1$ and $f_6 \circ f_5 = f_1$. Thus ${f_5}^{-1} = f_6$ and ${f_6}^{-1} = f_5$

For example, $f_4 \circ f_3$ is done in the following way

$$(f_4 \circ f_3)(1) = f_4\big(f_3(1)\big) = f_4(2) = 2$$
$$(f_4 \circ f_3)(2) = f_4\big(f_3(2)\big) = f_4(1) = 3$$
$$(f_4 \circ f_3)(3) = f_4\big(f_3(3)\big) = f_4(3) = 1$$

Thus $f_4 \circ f_3 = f_5$.

Other compositions of elements of F_A are given in the following table, in which $f_i \circ f_j$ is entered at the intersection of the i^{th} row and j^{th} colum:

Table 1

$*$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

Binary operations

We now restrict our discussion to functions from a set $A \times A$ to A, or more generally to a function from $A^n = A \times A \times \dots \times A(n \text{ times})$ to A where n is a given fixed natural number.

Let A be non-empty set and f be a mapping

$$\boldsymbol{f : A \times A \longrightarrow A}$$

Then f is called a **binary operation** on A.

In general, a mapping $\boldsymbol{f : A^n \longrightarrow A}$ is called an $\boldsymbol{n}$**-ary** operation on A and n is called the **order** of the operation.

For $n = 1$, $\boldsymbol{f : A \longrightarrow A}$ is called a **unary** operation.

The operations of addition, subtraction, and multiplication are binary operations on $\boldsymbol{Z}$ and also on $\boldsymbol{R}$. The operation of division is not a binary operation on these sets.
The operations of set union and intersections are binary operations on the set of subsets of a universal set. They are binary operations on the power set of any set. The operation of complementation is a unary operation on these sets.

The composition of bijective functions from a set A to itself (i.e., on F_A) is a binary operation.

The operations of conjunction and disjunction are binary operations on the set of propositions as well as of the set of well-formed formulas in propositional logic. The operation of negation is a unary operation on these sets.

Sometimes a binary operation can be conveniently specified by a table called **composition table.**(for example see Table 1).

Example 8: Construct the composition tables for the binary operations union and intersection for the power set $\boldsymbol{P(A)}$, where $\boldsymbol{A = \{a, b\}}$.

Solution: We have $A = \{a, b\}$ and $P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$

Let $B_0 = \phi$, $B_1 = \{b\}$, $B_2 = \{a\}$, $B_3 = \{a, b\} = A$. Then $P(A) = \{B_0, B_1, B_2, B_3\}$.

The composition tables for ∪ and ∩ are given below:

Table 2

∪	B_0	B_1	B_2	B_3
B_0	B_0	B_1	B_2	B_3
B_1	B_1	B_1	B_3	B_3
B_2	B_2	B_3	B_2	B_3
B_3	B_3	B_3	B_3	B_3

Table 3

∩	B_0	B_1	B_2	B_3
B_0	B_0	B_0	B_0	B_0
B_1	B_0	B_1	B_0	B_1
B_2	B_0	B_0	B_2	B_2
B_3	B_0	B_1	B_2	B_3

It is customary to denote a binary operation by a symbol (such as $+, -, \circ, *, \bigoplus, \cup, \cap, \vee, \wedge, \sim$, etc.,) **and the value of the operation (or function) by placing the operator between the two operands.**

For example, $\boldsymbol{f(x, y)}$ may be written as $\boldsymbol{xfy}$ or $\boldsymbol{x * y}$ or $\boldsymbol{x + y}$ as the case may be.

Properties of binary operations: Let A be any non-empty set. A binary operation $\boldsymbol{f : A \times A \longrightarrow A}$ is said to be

(i) **Commutative** if $f(x, y) = f(y, x)$, for all $x, y \in A$.

(ii) **Associative** if for every $x, y, z \in A$,

$$f(f(x, y), z) = f\big(x, f(y, z)\big)$$

(iii) **Distributive** if for every $x, y, z \in A$

$$f\big(x, g(y, z)\big) = g\big(f(x, y), f(x, z)\big)$$

If $*$ and $\circ$ denote the operations f and g respectively, the above properties respectively become

$$\boldsymbol{x * y = y * x}, \textbf{ for all } \boldsymbol{x, y \in A}$$

$$\boldsymbol{(x * y) * z = x * (y * z)}, \textbf{ for all } \boldsymbol{x, y, z}$$

$$\boldsymbol{x * (y \circ z) = (x * y) \circ (x * z)}$$

The operations of addition and multiplication over $\boldsymbol{R}$ are commutative and associative.

The operation of union and intersection over the power set of any sets are commutative and associative.

The operation of subtraction over $\boldsymbol{R}$ is not commutative.

The operation of composition of bijective maps on a set is not commutative.

The operation of multiplication is distributive over the addition in $\boldsymbol{R}$.

Both union and intersection of sets distributive over each other on the power set of any set.

Certain distinguished elements: Given a binary operation $*$ on a set A, we now define certain distinguished elements of A associated with the operation $*$. *Such elements may or may not exist*.

Identity element: Let $*$ be a binary operation on a set A. If there exists an element $e \in A$ such that

$$\boldsymbol{e * x = x * e = x}$$

for every $x \in A$, then e is called the **identity** with respect to $*$.

The element 0 is the identity for addition and 1 the identity for multiplication over $\boldsymbol{R}$. The empty set ϕ is the identity for the operation of union and the universal set U is the identity for the operation of intersection over the set of subsets of a universal set U.

The identity map I_A is the identity w.r.t the composition of bijective functions of F_A.

A contradiction (i.e., an identically false proposition) is an identity for disjunction, while a tautology is an identity for conjunction of propositions.

Zero element: Let $*$ be a binary operation on A.If there exists an element $0 \in A$ such that

$$\boldsymbol{0 * x = x * 0 = 0} \text{ for all } x \in A$$

then 0 is called the **zero** w.r.t to $*$.
The element 0 is the zero for multiplication on $\boldsymbol{R}$**.** The empty set $\emptyset$ is the zero for intersection and the universal set U is the zero for the union of subsets of a universal set U.

Idempotent element: Let $*$ be a binary operation on A. An element $a \in A$ is called **idempotent** w.r.t $*$, if $\boldsymbol{a * a = a}$**.**

The *identity* and *zero* elements w.r.t. a binary operation are idempotent. There may be other idempotent elements besides the identity and zero elements. Note that every set is idempotent w.r.t. to the operations of union and intersection.

Invertible elements and inverse of an element: Let $*$ be a binary operation on A with the identity e. An element $a \in A$ is said to be **invertible**, if there is an element $x \in A$ such that

$$\boldsymbol{a * x = x * a = e}$$

Such an element x is called the **inverse** of a, it is denoted by a^{-1} and

$$\boldsymbol{a * a^{-1} = a^{-1} * a = e}.$$

By symmetry it follows that $\boldsymbol{(a^{-1})^{-1} = a}$

In many binary operation the identity element, if it exists, is invertible, since it is idempotent, the **identity element is its own inverse.**

The other invertible elements may or may not exist. For example, every real number $a \in \boldsymbol{R}$ has an inverse $-a \in \boldsymbol{R}$ for the operation of addition. Similarly, for the operation of multiplication, the inverse of every nonzero real number $a \in \boldsymbol{R}$ is $\frac{1}{a} \in \boldsymbol{R}$. In F_A, the set of all bijections on A ,every function is invertible for the operation of composition . Note that a zero element w.r.t. an operation is not invertible.

Cancellable element: Let $*$ be a binary operation on . An element $a \in A$ is called **cancellable** w.r.t $*$ if for every $x, y \in A$,

$$\boldsymbol{(a * x = a * y) \vee (x * a = y * a) \Longrightarrow (x = y)}$$

Lemma 1: If the operation $*$ is associative and the element $\boldsymbol{a} \in \boldsymbol{A}$ is invertible, then $\boldsymbol{a}$ is cancellable.

Proof: Let $x, y \in A$ and $a * x = a * y$ or $x * a = y * a$. Suppose that $a * x = a * y$. Since a is invertible a^{-1} exists and $a * a^{-1} = a^{-1} * a = e$. Now $a^{-1}(a * x) = a^{-1}(a * y) \Longrightarrow (a^{-1} * a) * x = (a^{-1} * a) * y$ (since $*$ is associative)

$$\Longrightarrow e * x = e * y \Longrightarrow x = y$$

Thus, a is cancellable.

Note: There are cases where an element is cancellable but not necessarily invertible. For example in $\boldsymbol{Z}$, any nonzero integer is cancellable with respect to multiplication, although the only integer which is invertible is 1

Characteristic function of a set

We shall discuss functions from the universal set U to the set $[0, 1]$.

Let U be a universal set and A be a subset of U. The function $\psi_A : E \longrightarrow [0, 1]$ defined by

$$\psi_A = \begin{cases} 1, & if\ x \in A \\ 0, & if\ x \notin A \end{cases}$$

is called the ***characteristic function*** of the set A.The following properties suggest how we can use the characteristic functions of the sets to determine set relations:

Properties of Characteristic function

Let A and B be any two subsets of a universal set U. Then the following hold for all $x \in U$

i) $\psi_A(x) = 0, \forall x \in U \Leftrightarrow A = \emptyset$
ii) $\psi_A(x) = 1, \forall x \in U \Leftrightarrow A = U$
iii) $\psi_A(x) \leq \psi_B(x), \forall x \in U \Leftrightarrow A \subseteq B$
iv) $\psi_A(x) = \psi_B(x), \forall x \in U \Leftrightarrow A = B$
v) $\psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x), \forall x \in U$
vi) $\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A\cap B}(x), \forall x \in U$
vii) $\psi_{A'}(x) = 1 - \psi_A(x), \forall x \in U$
viii) $\psi_{A-B}(x) = \psi_{A\cap B'}(x) = \psi_A(x) - \psi_{A\cap B}(x), \forall x \in U$

Note that the operations $\leq, =, +, *$ and $-$ used with the characteristic functions are arithmetic operations (because the values of the characteristic functions are always either 1 or 0). The above properties can easily be proved using the definition of characteristic functions. Following is the proof of (v):

$$\psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x), \forall x \in U$$

We have $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$. For $x \in A \cap B$, we have

$$\psi_{A\cap B}(x) = 1, \psi_A(x) = 1, \psi_B(x) = 1$$

Therefore, for $x \in A \cap B, \psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x)$

For $x \notin A \cap B$, we have $x \in (A \cap B)'$ i.e., $x \in A' \cup B'$ i.e., $x \in A' \vee x \in B'$

For $x \notin A \cap B$, we have $\psi_{A\cap B}(x) = 0, \psi_A(x) = 0 \; or \; \psi_B(x) = 0$

Therefore, for $x \notin A \cap B, \psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x)$

Thus, we have $\psi_{A\cap B}(x) = \psi_A(x) * \psi_B(x), \forall x \in U$.This proves (v).

Many set identities and other relations can be proved using characteristic functions and the usual arithmetic operations and relation.

Example 9: Show that $\boldsymbol{A \cap (B \cup C) = (A \cap B) \cup (A \cap C)}$

Solution: For all $x \in U$, we have

$$\psi_{A\cap(B\cup C)}(x) = \psi_A(x) * \psi_{B\cup C}(x) \quad \text{(by } (v)\text{)}$$

$$= \psi_A(x) * \left(\psi_B(x) + \psi_C(x) - \psi_{B\cap C}(x)\right) \quad \text{(by } (vi)\text{)}$$

$$= \psi_A(x) * \psi_B(x) + \psi_A(x) * \psi_C(x) - \psi_A(x) * \psi_{B\cap C}(x)$$

$$= \psi_{A\cap B}(x) + \psi_{A\cap C}(x) - \psi_{A\cap(B\cap C)}(x)$$

$$= \psi_{A\cap B}(x) + \psi_{A\cap C}(x) - \psi_{A\cap B\cap C}(x)$$

$$= \psi_{A\cap B}(x) + \psi_{A\cap C}(x) - \psi_{(A\cap B)\cap(A\cap C)}(x)$$

$$= \psi_{(A\cap B)\cap(A\cap C)}(x)$$

Thus, $\psi_{A\cap(B\cup C)}(x) = \psi_{(A\cap B)\cup(A\cap C)}(x) \;\; , \forall x \in U$

$\Longrightarrow A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ by (iv)

Example 10: **Show that $(A')' = A$.**

Solution: For all $x \in U$, $\psi_{(A')'}(x) = 1 - \psi_{A'}(x)$ (by (vii))

$= 1 - \left(1 - \psi_A(x)\right)$ (by (vii))

$= \psi_A(x)$

$\Longrightarrow (A')' = A$ (by (iv))

We can name the subsets of a finite set by using the characteristic function.

Consider $U = \{a, b, c\}$. The subsets of U are $\phi, \{a\}, \{b\}, \{a, b\}, \{a, c\}, \{b, c\}$ and $\{a, b, c\}$.

The values of the characteristic functions of these subsets are given in the following table

Table 4

x	$\varnothing$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a, b\}$	$\{a, c\}$	$\{b, c\}$	$\{a, b, c\}$
a	0	1	0	0	1	1	0	1
b	0	0	1	0	1	0	1	1
c	0	0	0	1	0	1	1	1

The values of the characteristic function of any of the subsets of U are binary triples.

Let $B = \{000, 001, 010, 011, 100, 101, 110, 111\}$. Now Table 4 can be considered as a function from powerset of U to B. Clearly this function is bijective and therefore describes a one-to-one correspondence between the sets of $P(U)$ and B. The elements of B will be used to denote the corresponding subsets. That is $B_0 = \phi, B_1 = \{c\}, B_2 = \{b\}, B_3 = \{b, c\}, B_4 = \{a\}, B_5 = \{a, c\}, B_6 = \{a, b\}$, $B_7 = \{a, b, c\}$.

Note: The characteristic functions are associated with sets in the same way as the principle of specification (given in earlier module in unit 1). We have seen that a one-to-one correspondence can be established between these characteristic functions and the sets. With the use of these characteristic functions, statements about sets and their operations can be represented in terms of *binary numbers* and so their manipulation on a computer becomes easier.

Hashing functions

Any transformation which maps the internal bit representation of a set of keys to a set of addresses is called a **hashing function**.

Various hashing functions are available. One commonly used hashing function is the **division method** (mod function)

Note that every key has a binary representation, which may be treated as a binary number. Let the numerical value of a key be denoted by k. Let n be a fixed positive integer (preferably a prime number), which is suitably chosen. The hashing function h defined by the division method is

$$\boldsymbol{h(k) = k(\mathbf{mod}\; n)}$$

i.e., $h(k)$ is the remainder of dividing k by n. Therefore, $h(k)$ is an element of the set $\{0,1,2, \dots, n-1\}$. Thus the hashing function maps the set of keys to the set of n addresses, $\{0,1,2, \dots, n-1\}$, which is called the **address set**.

Clearly, a hashing function maps different keys to the set of n addresses. Thus the set of records is partitioned into n equivalence classes. Those records which are mapped to the same address are in the same equivalence class.

It is therefore necessary to provide storage space for and also a method of finding the *collision* of or *overflow* records when more than one record has the same address. There are many techniques, called *collision resolution techniques* for this purpose.

Recursively defined functions

Sometimes it is difficult to define an object explicitly. However, it may be easy to define this object in terms of itself. This process is called **recursion**.

We use two steps to define a function f with the set of non-negative integers $W = \{0,1,2,3, \dots\}$ as its domain.

Let $a \in W$ and $A = \{a, a+1, a+2, \dots\}$. The **recursive** definition of a function f with domain A, consists of the following two parts, where $k \geq 1$.

Basis step: A few initial values of the function $f(a), f(a+1), \dots, f(a+k-1)$ are specified. An equation that specifies such initial values is an **initial condition**.

Recursive step: A formula to compute $f(n)$ from k preceding functional values $f(n-1), f(n-2), \dots, f(n-k)$ is made. Such a formula is a **recurrence relation** (or **recursion formula**).

Thus recursive definition of f consists of one or more (a finite number of) initial conditions and a recurrence relation.

Recursively defined functions are **well-defined**. That is, given any positive integer we can use the two parts of the definition to find the value of the function at that integer and that we obtain the same value no matter how we apply the two parts of the definition.

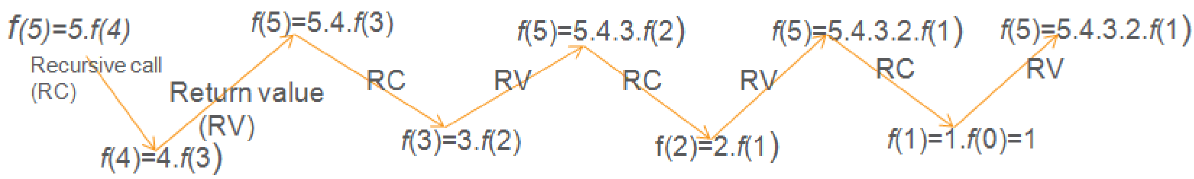
Example 11: Define recursively the factorial function f.

Solution: Recall that the factorial function f is defined by $f(n) = n!$, where $f(0) = 1$. Since $n! = n(n-1)!$, f can be defined recursively as follows:

$$\boldsymbol{f(0) = 1} \qquad - \textbf{Initial condition}$$

$$\boldsymbol{f(n) = n \cdot f(n-1)\ , n \geq 0} \qquad - \textbf{Recurrence relation}$$

Suppose we would like to compute $f(5)$ using recursive definition. We then continue to apply the recurrence relation until the initial condition is reached, as shown below:



P1:

List all possible functions from $\boldsymbol{A = \{a, b, c\}}$ and $\boldsymbol{B = \{0, 1\}}$ and indicate in each case whether the function is one-to-one and is onto.

Solution: We have $A = \{a, b, c\}$, $B = \{0,1\}$.

The number of functions from A to B is $|B|^{|A|} = 2^3 = 8$.

Since $|A| \nleq |B|$, none of these functions is one-to-one. The functions are

$f_0 = \{(a, 0), (b, 0), (c, 0)\}$, into

$f_1 = \{(a, 0), (b, 0), (c, 1)\}$, onto

$f_2 = \{(a, 0), (b, 1), (c, 0)\}$, onto

$f_3 = \{(a, 0), (b, 1), (c, 1)\}$, onto

$f_4 = \{(a, 1), (b, 0), (c, 0)\}$, onto

$f_5 = \{(a, 1), (b, 0), (c, 1)\}$, onto

$f_6 = \{(a, 1), (b, 1), (c, 0)\}$, onto

$f_7 = \{(a, 1), (b, 1), (c, 1)\}$, onto

P2:

Let $\boldsymbol{f}: \boldsymbol{A} \longrightarrow \boldsymbol{B}$, $\boldsymbol{g} : \boldsymbol{B} \longrightarrow \boldsymbol{C}$ and $\boldsymbol{g} \circ \boldsymbol{f} \neq \boldsymbol{\phi}$.

i. **If $\boldsymbol{f}, \boldsymbol{g}$ are one-to-one then so is $\boldsymbol{g} \circ \boldsymbol{f}$.**
ii. **If $\boldsymbol{f}, \boldsymbol{g}$ are onto then so is $\boldsymbol{g} \circ \boldsymbol{f}$.**
iii.**If $\boldsymbol{f}, \boldsymbol{g}$ are bijective then so is $\boldsymbol{g} \circ \boldsymbol{f}$.**

Solution: We have $f: A \longrightarrow B$, $g : B \longrightarrow C$ and $g \circ f \neq \phi$.

(i) Suppose f, g are one-to-one. Now

$$\begin{aligned} (g \circ f)(x) = (g \circ f)(y) &\Longrightarrow g\big(f(x)\big) = g\big(f(y)\big) \\ &\Longrightarrow f(x) = f(y) \qquad \text{(since } g \text{ is one-to-one)} \\ &\Longrightarrow x = y \qquad \text{(since } f \text{ is one-to-one)} \end{aligned}$$

Thus, $g \circ f$ is one-to-one when f, g are one-to-one.

(ii) Suppose f, g are onto.

Let c be any element C. Since g is onto there exists an element $b \in B$ such that $g(b) = c$. Since f is onto, for the $b \in B$, there exists an element $a \in A$ such that $f(a) = b$. Thus, for any $c \in C$ there exists an element $a \in A$ such that

$$(g \circ f)(a) = g\big(f(a)\big) = g(b) = c$$

This shows that $g \circ f$ is onto.

(iii) Suppose f, g are bijective, $i.e.$, f, g are one-to-one and onto.

$\Longrightarrow g \circ f$ is one-to-one and onto$\Longrightarrow g \circ f$ is bijective.

P3:

Show that there exists a one–to – one mapping from $\boldsymbol{A} \times \boldsymbol{B}$ to $\boldsymbol{B} \times \boldsymbol{A}$. Is it also onto?

Solution:

We have nonempty sets A and B. Define a map $\boldsymbol{f}: \boldsymbol{A} \times \boldsymbol{B} \longrightarrow \boldsymbol{B} \times \boldsymbol{A}$ by $f(x, y) = (y, x)$

(i) *f is one – to – one:*

$$f(x_1, y_1) = f(x_2, y_2) \implies (y_1, x_1) = (y_2, x_2)$$
$$\implies y_1 = y_2 \text{ and } x_1 = x_2$$
$$\implies (x_1, y_1) = (x_2, y_2)$$

Thus, f is one – to – one.

(ii) *f is onto:*

Let (b, a) be any element of $B \times A$, i.e., $b \in B$ and $a \in A$. Clearly, $(a, b) \in A \times B$ and $f(a, b) = (b, a)$. This shows f is onto.

Note: There is a one – to – one correspondence between $A \times B$ and $B \times A$.

P4:

How many distinct binary operations are there on the set $\{0, 1\}$? Can you determine the number of distinct binary operations on any finite set?

Solution:
Let A be a nonempty finite set. A binary operation on A is a mapping $\boldsymbol{A} \times \boldsymbol{A} \longrightarrow \boldsymbol{A}$.

The number of distinct binary operations on A.

$=$ The number of distinct functions from $A \times A$ to A

$= |A|^{|A\times A|}$ (Since number of functions from X to Y is $|Y|^{|X|}$)

$= |A|^{|A|.|A|} = |A|^{|A|^2}$

The number of distinct binary operations on the set $A = \{0,1\}$ is
$|A|^{|A|^2} = 2^{2^2} = 16$

P5:

Let A and B be subsets of a universal set U. Then

$$\boldsymbol{\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A\cap B}(x), x \in U}$$

Solution:

Case (*a*)

$x \in A \cup B$. Then $\Psi_{A\cup B}(x) = 1$

$x \in A \cup B \Longrightarrow (x \in A,\ x \notin A \cap B)$ or $(x \in B,\ x \notin A \cap B)$ or $(x \in A \cap B)$

If $x \in A,\ x \notin A \cap B$, then $\psi_A(x) = 1$, $\psi_B(x) = 0$, $\psi_{A\cap B}(x) = 0$

and $\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A\cap B}(x)$

Similarly, in the case of $x \in B, x \notin A \cap B$.

If $x \in A \cap B$, then $x \in A,\ x \in B,\ \psi_A(x) = \psi_B(x) = \psi_{A\cap B}(x) = 1$ and
$\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) - \psi_{A\cap B}(x)$.

Case (b)

$x \notin A \cup B$. Then $\psi_{A\cup B}(x) = 0$

$x \notin A \cup B \Longrightarrow x \notin A$ and $x \notin B$ (De Morgan's law)

i.e., $\psi_{A\cup B}(x) = 0$, $\psi_A(x) = \psi_B(x) = 0$

Further, we have $\psi_{A\cap B}(x) = \psi_A(x).\psi_B(x) = 0$

Therefore$\psi_{A\cup B}(x) = \psi_A(x) + \psi_B(x) = -\psi_{A\cap B}(x)$, for all $x \in U$.

P6:

Let A and B be subsets of a universal set U. Then

(i) $\boldsymbol{\psi_{A}(x) = 1 - \psi_{A}(x)}$ **, for all $x \in U$**

(ii) $\boldsymbol{\psi_{A \oplus B}(x) = \psi_{A}(x) + \psi_{B}(x) - 2\, \psi_{A \cap B}(x)}$

Solution:

(i) Let $x \in A'$. Then $\psi_{A'}(x) = 1$

$x \in A' \implies x \notin A \implies \psi_{A}(x) = 0$

Thus, $\psi_{A'}(x) = 1 - \psi_{A}(x)$

Let $\notin A'$. Then $\psi_{A'}(x) = 0$

$x \notin A' \implies x \in A \implies \psi_{A}(x) = 1$

Thus, $\psi_{A'}(x) = 1 - \psi_{A}(x)$

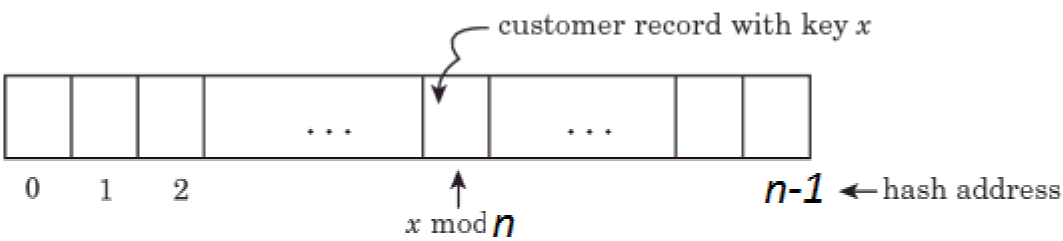
Therefore, $\psi_{A}(x) = 1 - \psi_{A}(x)$ for all $x \in U$

(ii) For all $x \in U$

$$
\begin{aligned}
\psi_{A \oplus B} &= \psi_{(A-B) \cup (B-A)}(x) \\
&= \psi_{A-B}(x) + \psi_{B-A}(x) \quad \text{(since } A-B,\ B-A \text{ are disjoint)} \\
&= \psi_{A \cap B'}(x) + \psi_{B \cap A'}(x) \\
&= \psi_{A}(x)\ \psi_{B'}(x) + \psi_{B}(x)\, \psi_{A'}(x) \\
&= \psi_{A}(x)\left(1 - \psi_{B}(x)\right) + \psi_{B}(x)\left(1 - \psi_{A}(x)\right) \\
&= \psi_{A}(x) - \psi_{A}(x)\psi_{B}(x) + \psi_{B}(x) - \psi_{A}(x)\, \psi_{B}(x) \\
&= \psi_{A}(x) + \psi_{B}(x) - 2\, \psi_{A}(x)\, \psi_{B}(x).
\end{aligned}
$$

P7:

Banks use nine – digit account numbers to create and maintain customer accounts. Customer records are stored in an array in a computer and can be accessed easily and quickly using their unique **keys**, which in this case are the account numbers. Access is often accomplished using the hashing function. $\boldsymbol{h(x) = k\ (mod\ n)}$, where x denotes the key ($i.e.$, account number in this case) and n is the number of cells in the array $(n \in \{0, 1, 2, \dots, n-1\})$ and $h(x)$ denotes the **hash address** of the customer record with key x.



Let $n = 1009$ (prime number) and $x = 20763074$ (account number) .The corresponding record is stored in the location.

$$h(207630764) = (207630764)\ (mod\ 1009) = 762$$

Similarly $h(307620765) = 307620765(mod\ \ 1009) = 881$

Since the hashing function is not injective, theoretically different customer records can be assigned to the same location. For example

$$h(207630764) = 762 = h(208801204)$$

This results in a **collision**.

You will learn how to resolve collisions in a different topic in CSE.

P8:

The Hand shake problem:

There are $\boldsymbol{n}$ guests at a party. Each person shakes hands with everybody else exactly once. Define recursively the number of handshakes $\boldsymbol{h(n)}$ that occur.

Solution:

Clearly, $h(1) = 0$. Let $n \geq 2$.

Let x be one of the guests. By definition, the number of handshakes made by the remaining $n-1$ guests among themselves is $h(n-1)$. Now the guest x shakes hand with each of these $n-1$ guests, yielding $n-1$ additional handshakes. Therefore, the total number of handshakes made is $h(n-1)+(n-1), n \geq 2$

Thus, $h(n)$ can be defined recursively as follows:
$\boldsymbol{h(1) = 0}$ -- **initial condition**
$\boldsymbol{h(n) = h(n-1)+(n-1)}$--**recurrence relation**

MODULE-1

Counting Principles

Unit-4

Counting

4.1

Counting Principles

Combinatorics, the study of arrangements of objects, is an important part of discrete structures. Enumeration, the counting of objects with certain properties, is an important part of Combinatorics. Counting is used to determine the complexity of algorithms and it is also required whether there are enough internet protocol addresses to meet the demand. Further, counting techniques are extensively used when probabilities of events are computed.

In this module we introduce the basic methods of counting. These methods serve as the foundation for almost all counting techniques.

Basic counting principles There are two basic counting principles: (i) the ***product rule*** and (ii) *the **sum rule**.*

The product rule applies when a procedure is made up of separate tasks.

The Product Rule: Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are n_1n_2 ways to do the procedure.

An extended version of the product rule is often useful.
Suppose that a procedure is carried out by performing the tasks $T_1, T_2, \dots, T_m$ in sequence. If each task T_i , $i = 1,2, \dots, n$, can be done is n_i ways, (regardless of how the previous tasks were done), then there are $n_1n_2 \dots n_m$ ways to carry out the procedure.

This can be proved by mathematical induction from the product rule of two tasks.

Example 1: How many bit strings of length seven are there?

Solution: Each of the seven bits can be chosen in two ways, because each bit is either 0 or 1. Therefore, by the product rule there are $\underbrace{2 \times 2 \times \ldots \times 2}_{7\ times} = 2^7 = 128$ different bit strings of length seven.

Example: **Counting Functions**

How many functions are there from a set with $\boldsymbol{m}$ elements to another set with $\boldsymbol{n}$ elements.

Solution: A function corresponds to a choice of one of the n elements in the codomain for each of the m elements in the domain. By product rule there are $\underbrace{n \cdot n \cdot \ldots \cdot n}_{m\ times} = n^m$ functions from a set with m elements to a set with n elements.

Example 2: **Counting one-to-one Functions**

How many one-to-one functions are there from a set with $\boldsymbol{m}$ elements to another set with $\boldsymbol{n}$ elements?

Solution: First note that there are no one-to-one functions when $m > n$.
Let $m \leq n$. Let the elements of the domain be $a_1, a_2, \ldots, a_m$. There are n ways to choose the value of the function at a_1. Since the function is one-to-one, the value of the function at a_2 can be chosen in $n - 1$ ways. In general, the value of the function at a_k, having chosen the values of $a_1, a_2, \ldots, a_{k-1}$, can be chosen in $n - (k - 1) = n - k + 1$ ways. By the product rule, there are

$$n(n - 1)(n - 2) \ldots (n - m + 1)$$

one-to-one functions from a set with m elements to another set with n elements.

Note: The product rule is often phrased in terms of sets as given below:
If $A_1, A_2, \ldots, A_m$ are finite sets, then the number of elements in the Cartesian product of these sets is the product of the number of elements in each set. To relate this to the product rule, note that the task of choosing an element in the

Cartesian product $A_1 \times A_2 \times \ldots \times A_m$ is done by choosing an element in A_1, an element in A_2 , …, and an element in A_m.

The product rule,

$$|A_1 \times A_2 \times \ldots \times A_m| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_m|$$

We now introduce the sum rule.

Sum Rule: If a task can be done in either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

The following is the extended version of the sum rule: Suppose that a task can be done in one of n_1 ways, in one of n_2 ways,…,or in one of n_m ways, where none of the set of n_i ways of doing the task is the same as any of the set of n_j ways, for all i and j with $1 \leq i < j \leq m$. Then the number of ways to do the task is

$$n_1 + n_2 + \cdots + n_m.$$

Example 3: A student can choose a computer project from one of three lists. The three lists contain 23,15 and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

Solution: The student can choose a project by selecting from the first list, the second list, or the third list. Because no project is on more than one list, by sum rule there are 23+15+19=57 ways to choose a project.

Note: The sum rule is often phrased in terms of sets.
If $A_1, A_2, \ldots, A_m$ are pairwise disjoint finite sets, then the number of elements in the union of the sets is the sum of the number of elements in the sets. To relate this to the sum rule, note that there are $|A_i|$ ways to choose an element from A_i , $i = 1,2, \ldots, m$. Because the sets are disjoint, when we select an element from one of the sets A_i , we do not also select an element from a different set A_j. By sum rule (because we cannot select an element from two of these sets at the same time) the number of ways to choose an element from one of the sets,

which is the number of elements in the union, is

$$|A_1 \cup A_2 \cup \ldots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|.$$

Many counting problems can be solved using both of the above rules in combination.

Example 4: In a version of the computer language *BASIC*, the name of a variable is a string of one or two alphanumeric characters, where uppercase and lowercase letters are not distinguished. Moreover, a variable name must begin with a letter and must be different from five strings of two characters that are reserves for programming use. How many different variable names are there in this version of BASIC?

(An alphanumeric character is either one of 26 English letters or one of 10 digits)

Solution: Let v be the number of variable names in this version of BASIC. Let v_1 and v_2 be number of variable names of one character long and two characters long respectively. By the sum rule, $v = v_1 + v_2$.

Note that $v_1 = 26$, because a one character variable name must be a letter.

Further, by the product rule there are $26 \cdot 36$ strings of length two that begin with a letter and end with an alphanumeric character. However, five of these are excluded, so $v_2 = 26 \cdot 36 - 5 = 931$.

Therefore, there are $v = v_1 + v_2 = 26 + 931 = 957$ different names of variables in this version of BASIC.

The Inclusion-Exclusion Principle

Suppose that a task can be done in n_1 or n_2 ways, but that some of the set of n_1 ways to do the task are the same as some of n_2 ways to do the task. In this situation, we cannot use the sum rule to count the number of ways to do the task. Adding the number of ways to do the tasks in these two ways leads to an overcount, because the ways to do the task in the two ways that are common are counted twice. To correctly count the number of ways to do the task, we add the number of ways to do it in one way and the number of ways to do it in the other way, and then subtract the number ways to do the task in both among the set of n_1 ways and the set of n_2 ways. This technique is called the ***principle of inclusion -exclusion*** or ***subtraction principle for counting***.

We can phrase this principle in terms of sets.
Let A and B be finite sets. There are $|A|$ and $|B|$ ways to select an element from A and B respectively. The number of ways to select an element from $A \cup B$ is the sum of the number of ways to select an element from A and B, minus the number of ways to select an element from $A \cap B$. That is

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

Example 5: How many bit strings of length eight either start with a 1 bit or end with the two bits 00?

Solution: Let A and B be the set of bit strings of length eight that start with 1 and end with 00 respectively. Then $A \cap B$ consists of all bit strings that start with 1 and end with 00. Required to find $|A \cup B|$.

Note that, we can construct a bit string of length eight that starts with 1 in $2^7 = 128$ ways. This follows by the product rule, because the first bit can be chosen in one way and each of the other seven bits can be choosen in two ways. Thus, $|A| = 128$.

We can construct a bit string of length eight that ends with 00 in $2^6 = 64$ ways. This follows by the product rule, because each of the first six bits can be chosen in two ways and the last two bits in only one way. Thus, $|B| = 64$.

We can construct a bit string of length eight that begins with 1 and ends with 00 in $2^5 = 32$ ways. This follows by the product rule, because the first bit, the last two bits can be chosen in only one way and each of the five bits in between first bit and last two bits can be chosen in two ways. Thus, $|A \cap B| = 32$.

By the principle of inclusion- exclusion

$$|A \cup B| = |A| + |B| - |A \cap B| = 128 + 64 - 32 = 160$$

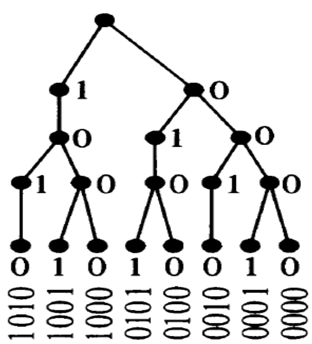
Thus, the number of bit strings of length eight that begin with 1 or that end with 00 is 160.

Tree Diagrams

Counting problems can be solved using ***tree diagrams***. A tree consists of a root, a number of branches leaving the root, and possible additional branches leaving the end points of other branches. To use trees in counting, we use a branch to represent each possible choice. We represent the possible outcomes by the leaves.

Example 6: How many bit string lengths of four do not have two consecutive 1s?

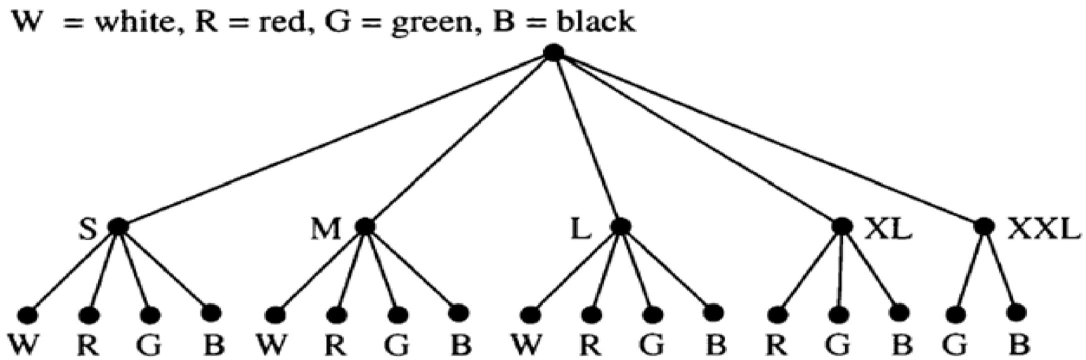
Solution:



The tree diagram displays all bit strings of length four without two consecutive 1s. There are eight bit strings of length four without two consecutive 1s.

Example 7: Suppose that **I love India** T-shirts come in five different sizes: S, M, L, XL and XXL. Suppose that each size comes in four colors, white, red, green and black, except for XL, which comes only in red, green and black, and XXL, which comes only in green and black. How many different T shirts does a souvenir shop have to stock to have at least one of each available size and color of the T-shirt?

Solution:



The tree diagram displays all possible size and color pairs. The shop owner need to stock 17 different T-shirts.

Example 8: How many positive integers not exceeding 1000 are divisible by 7 or 11

Solution: Let A be the set of positive integers not exceeding 1000 that are divisible by 7 and let B be the set of positive integers not exceeding 1000 that are divisible by 11. Then $A \cup B$ is the set of positive integers not exceeding 1000 that are divisible by 7 or 11, and $A \cap B$ is the set that are divisible by 7 and 11. Then

$$|A| = \left\lfloor \frac{1000}{7} \right\rfloor = 142 \qquad ; \qquad |B| = \left\lfloor \frac{1000}{7} \right\rfloor = 90$$

Note that the positive integers divisible by 7 and 11 are divisible by $7 \cdot 11$, because 7 and 11 are relatively prime. Therefore,

$$|A \cap B| = \left\lfloor \frac{1000}{7 \cdot 11} \right\rfloor = 12$$

By the principle of inclusion-exclusion

$$|A \cup B| = |A| + |B| - |A \cap B| = 142 + 90 - 12 = 220$$

There are 220 positive integers not exceeding 1000 that are divisible by 7 or 11.

Note: The number of positive integers not exceeding 1000 that are not divisible 7 and not divisible 11 are $1000 - 220 = 780$.

The principle of inclusion-exclusion for three finite sets is given below

Theorem 1: If $\boldsymbol{A}, \boldsymbol{B}$ and $\boldsymbol{C}$ are three finite sets, then

$$|\boldsymbol{A} \cup \boldsymbol{B} \cup \boldsymbol{C}| = |\boldsymbol{A}| + |\boldsymbol{B}| + |\boldsymbol{C}| - |\boldsymbol{A} \cap \boldsymbol{B}| - |\boldsymbol{A} \cap \boldsymbol{C}| - |\boldsymbol{B} \cap \boldsymbol{C}| + |\boldsymbol{A} \cap \boldsymbol{B} \cap \boldsymbol{C}|$$

Proof: $|A \cup B \cup C| = |A \cup (B \cup C)| = |A| + |B \cup C| - |A \cap (B \cup C)|$

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

(By the principle of inclusion- exclusion and distributive law)

Now, $|(A \cap B) \cup (A \cap C)| = |A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)|$

(By the principle of inclusion- exclusion)

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

Thus,

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

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

Hence the result.

Example 9: A total of $\mathbf{1232}$ students who have taken a course in Spanish, $\mathbf{879}$ have taken a course in French, and $\mathbf{114}$ have taken a course in Russian. Further, $\mathbf{103}$ have taken courses in both Spanish and French, $\mathbf{23}$ have taken courses in both Spanish and Russian, and $\mathbf{14}$ have taken courses in both French and Russian. If $\mathbf{2092}$ students have taken at least one of Spanish, French and Russian, then how many students have taken a course in all three languages?

Solution: Let S, F and R be the sets of students who have taken Spanish, French and Russian. Then, $|S| = 1232$, $|F| = 879$, $|R| = 114$. Further,

$|S \cap F| = 103$, $|S \cap R| = 23$, $|F \cap R| = 14$ and $|S \cup F \cup R| = 2092$.

By the principle of inclusion- exclusion,

$$|S \cup F \cup R| = |S| + |F| + |R| - |S \cap F| - |S \cap R| - |F \cap R| + |S \cap F \cap R|$$

i.e., $2092 = 1232 + 879 + 114 - 103 - 23 - 14 + |S \cap F \cap R|$

and $|S \cap F \cap R| = 2092 - 2085 = 7$.

Therefore, there are seven students who have taken courses in all the three languages.

Theorem 2: The principle of inclusion-exclusion for n finite sets

If $A_1, A_2, \ldots, A_n$ be finite sets then

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$$

(The result follows by mathematical induction)

An alternate form of the principle of inclusion - exclusion

This form can be used to solve problems that ask for the number of elements in a set A that have none of n properties $P_1, P_2, \ldots, P_n$.

Let A_i be the subset of A containing the elements that have the property P_i , $1 \le i \le n$.

The number of elements of A with all the properties $P_{i_1}, P_{i_2}, \ldots, P_{i_k}$ is denoted by $N\left(P_{i_1} P_{i_2} \ldots P_{i_k}\right)$. That is

$$\left|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}\right| = N\left(P_{i_1} P_{i_2} \ldots P_{i_k}\right)$$

If the number of elements with none of the properties $P_1, P_2, \ldots, P_n$ is denoted by $N(P_1{}' P_2{}' \ldots P_n{}')$ and the number of elements in A by N then

$$N(P_1{}' P_2{}' \ldots P_n{}') = |A| - |A_1 \cup A_2 \cup \ldots \cup A_n|$$

$$= N - \left[\sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n| \right]$$

$$= N - \sum_{1 \le i \le n} N(P_i) + \sum_{1 \le i < j \le n} N(P_i P_j) - \sum_{1 \le i < j < k \le n} N(P_i P_j P_k) + \cdots + (-1)^n N(P_1 P_2 \ldots P_n)$$

Application 1: The principle of inclusion – exclusion can be used to find the *number of primes not exceeding a specified positive integer.*

Example 10: Find the number primes not exceeding 100.
Recall that a composite number is divisible by a prime not exceeding its square root. Therefore, to find the number of primes not exceeding 100, first note the composite integers not exceeding 100 must have a prime factor not exceeding $\sqrt{100} = 10$.

Because the only primes less that 10 are 2,3,5, and 7; the primes not exceeding 100 are: these four primes and the number of those primes greater 1 and not exceeding 100 that are divisible by none of 2,3,5,7. Now, we have to consider $A = \{2,3,5, \ldots, 100\}$, since 1 is neither prime nor composite and $N = |A| = 99$.

Let P_1 be the property that an integer is divisible by 2 let P_2 be the property that an integer is divisible by 3 ,let P_3 be the property that an integer is divisible by 5 , andlet P_4 be the property that an integer is divisible by 7.

Thus, the number of primes not exceeding 100 is given by $4 + N(P_1{}'P_2{}'P_3{}'P_4{}')$.

By the principle of inclusion – exclusion

$$N(P_1{}'P_2{}'P_3{}'P_4{}') = N - [N(P_1) + N(P_2) + N(P_3) + N(P_4)] + N(P_1P_2) + N(P_1P_3) + N(P_1P_4) + N(P_2P_3) + N(P_2P_4) + N(P_3P_4) - [N(P_1P_2P_3) + N(P_1P_2P_4) + N(P_1P_3P_4) + N(P_2P_3P_4)] + N(P_1P_2P_3P_4)]$$

$$= 99 - \left[\left\lfloor\frac{100}{2}\right\rfloor + \left\lfloor\frac{100}{3}\right\rfloor + \left\lfloor\frac{100}{5}\right\rfloor + \left\lfloor\frac{100}{7}\right\rfloor\right] + \left\lfloor\frac{100}{2\cdot 3}\right\rfloor + \left\lfloor\frac{100}{2\cdot 5}\right\rfloor + \left\lfloor\frac{100}{2\cdot 7}\right\rfloor + \left\lfloor\frac{100}{3\cdot 5}\right\rfloor + \left\lfloor\frac{100}{3\cdot 7}\right\rfloor + \left\lfloor\frac{100}{5\cdot 7}\right\rfloor - \left[\left\lfloor\frac{100}{2\cdot 3\cdot 5}\right\rfloor + \left\lfloor\frac{100}{2\cdot 3\cdot 7}\right\rfloor + \left\lfloor\frac{100}{2\cdot 5\cdot 7}\right\rfloor + \left\lfloor\frac{100}{3\cdot 5\cdot 7}\right\rfloor\right] + \left\lfloor\frac{100}{2\cdot 3\cdot 5\cdot 7}\right\rfloor$$

$$= 99 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 - 3 - 2 - 1 - 0 + 0$$

$$= 21$$

Thus, there are $4 + 21 = 25$ primes not exceeding 100.

Note: The ***Sieve of Eratosthenes*** is used to find all primes not exceeding a specified positive integer.

Application 2: The principle of inclusion-exclusion can also be used to determine the number of onto functions from a set with m elements to a set with n elements.

We first consider the following example:

Example 11: How many onto functions are there from a set A with six elements to a set B with four elements.

Solution: Let $B = \{b_1, b_2, b_3, b_4\}$. Let F be the set of all function from A to B. Clearly $|F| = |B|^{|A|} = 4^6$.

Let P_1, P_2, P_3 and P_4 be the properties that b_1, b_2, b_3 and b_4 are not in the range of the function, respectively. Now, a function is onto iff it has none of the properties P_1, P_2, P_3 or P_4. The number of onto functions is given by $N(P_1{}'P_2{}'P_3{}'P_4{}')$ and by the principle of inclusion-exclusion.

$$\begin{aligned} N(P_1{}'P_2{}'P_3{}'P_4{}') &= |F| - [N(P_1) + N(P_2) + N(P_3) + N(P_4)] \\ &+ [N(P_1P_2) + N(P_1P_3) + N(P_1P_4) + N(P_2P_3) + N(P_2P_4) \\ &+ N(P_3P_4)] - [N(P_1P_2P_3) + N(P_1P_2P_4) + N(P_1P_3P_4) + N(P_2P_3P_4)] \\ &- N(P_1P_2P_3P_4) \end{aligned}$$

Note that $N(P_i)$ is the number of functions that do not have b_i in their range, for $i = 1,2,3,4$.

Therefore, $N(P_i) = 3^6$ for all $i = 1,2,3,4$ and there are ${}^4C_1$ terms of this kind.

Further, $N(P_iP_j) = 2^6$ for $1 \le i < j \le 4$ and there are ${}^4C_2$ terms of this kind.

Similarly, $N(P_iP_jP_k) = 1^6$ for $1 \le i < j < k \le 4$ and there are ${}^4C_3$ terms of this kind and $N(P_1P_2P_3P_4) = 0$ because this term is the number of functions that have none of b_1, b_2, b_3, b_4 in their range. Clearly there are no such functions. Therefore, the number of onto functions from a set A with six elements to a set B with four elements is given by

$$N(P_1'P_2'P_3'P_4') = 4^6 - {}^4C_1 \cdot 3^6 + {}^4C_2 \cdot 2^6 - {}^4C_3 . 1^6 + {}^4C_4 \cdot 0$$

$$= 4096 - 4 \cdot 729 + 6 \cdot 64 - 4$$

$$= 4096 - 2916 + 384 - 4 = 1560$$

The following is the general result related to the number of onto functions from a set with m elements to the set with n elements, where $m \ge n$.

Theorem 3: Let $\boldsymbol{m}$ and $\boldsymbol{n}$ be positive integers with $\boldsymbol{m} \ge \boldsymbol{n}$.The number of onto functions from a set with $\boldsymbol{m}$ elements to a set with $\boldsymbol{n}$ elements is

$$\boldsymbol{n^m} - {}^nC_1(\boldsymbol{n}-\boldsymbol{1})^{\boldsymbol{m}} + {}^nC_2(\boldsymbol{n}-\boldsymbol{2})^{\boldsymbol{m}} - \cdots + (-\boldsymbol{1})^{\boldsymbol{n}-\boldsymbol{1}}\, {}^nC_{n-1}\boldsymbol{1}^{\boldsymbol{m}}$$

Example 12: How many ways are there to assign five different jobs to four different employees if every employee is assigned at least one job?

Solution: Consider the assignment of jobs as a function from the set of five jobs to the set of four employees. An assignment where every employee gets at least one job is the same as an onto function from the set of jobs to the set of employees. *By Theorem* 3 there are

$$4^5 - {}^4C_1 . 3^5 + {}^4C_2 . 2^5 - {}^4C_3 . 1^5 = 1024 - 972 + 192 - 4 = 240$$

ways to assign the jobs so that each employee is assigned at least one job.

Derangements

The principle of inclusion-exclusion can be used to count the permutations of n objects that leave no objects in their original positions.

A ***derangement*** is a permutation of objects that leaves no object in its original position.

The permutation $2\ 1\ 4\ 5\ 3$ is a derangement of $1\ 2\ 3\ 4\ 5$, because no number is left in its original position. The permutation $2\ 1\ 5\ 4\ 3$ is not a derangement of $1\ 2\ 3\ 4\ 5$, because this permutation leaves 4 fixed.
Let $\boldsymbol{D_n}$ be the number of derangement of n objects.

For example, $D_3 = 2$, because the derangements of $1\ 2\ 3$ are $2\ 3\ 1$ and $3\ 1\ 2$.

We will now derive a formula for D_n using the principle of inclusion-exclusion.

Theorem 4: The number of derangements of a set with $\boldsymbol{n}$ elements is

$$\boldsymbol{D_n = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right]}$$

Proof: Let P be the set of all permutations of the set with n elements.Clearly $|P| = n!$. Let P_i be the property of fixing an element i in a permutation of P, $i = 1,2, \dots, n$. The number of derangements is the number of permutations of P having none of the properties P_i , for $i = 1,2, \dots, n$. That is

$$D_n = N(P_1{}'P_2{}' \dots P_n{}')$$

By the principle of inclusion-exclusion

$$\begin{aligned} D_n &= N(P_1{}'P_2{}' \dots P_n{}') \\ &= |P| - \sum_{1 \le i \le n} N(P_i) + \sum_{1 \le i < j \le n} N\big(P_i P_j\big) - \sum_{1 \le i < j < k \le n} N\big(P_i P_j P_k\big) + \cdots \\ &+ (-1)^n N(P_1 P_2 \dots P_n) \end{aligned}$$

Note that $N(P_i)$ is the number of permutations that fix the element i. If the element i is left in its original position, the remaining $n-1$ positions can be filled is $(n-1)!$ ways. Therefore, $N(P_i) = (n-1)!$. Similarly $N(P_i P_j) = (n-2)!$. In general $N(P_{i_1} P_{i_2} \dots P_{i_m}) = (n-m)!$.

Because there are ${}^{n}C_{m}$ ways to choose m elements from n elements,

$$\sum_{1 \le i \le n} N(P_i) = {}^{n}C_{1}(n-1)!$$

$$\sum_{1 \le i < j \le n} N(P_i P_j) = {}^{n}C_{2}(n-2)!$$

In general $(P_{i_1} P_{i_2} \dots P_{i_m}) = {}^{n}C_{m}(n-m)!$. Thus,

$$D_n = n! - {}^{n}C_{1}.(n-1)! + {}^{n}C_{2}.(n-2)! - \cdots + (-1)^n \, {}^{n}C_{n}.0!$$

$$= n! - \frac{n!}{1!(n-1)!}(n-1)! + \frac{n!}{2!(n-2)!}(n-2)! - \cdots + (-1)^n \frac{n!}{1!0!} 0!$$

$$= n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right]$$

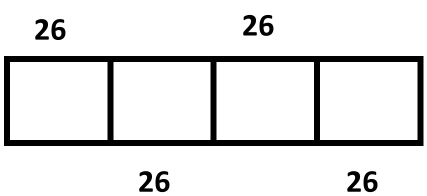
P1:

How many strings are there of lowercase English letters of length four or less?

Solution:

Number of strings of length 4

There are 26 choices for each of four places



By product rule there are $26 \times 26 \times 26 \times 26 = 4{,}56{,}976$ strings of length 4.

Similarly, there are

$26 \times 26 \times 26 = 17{,}576$ strings of length three

$26 \times 26 = 676$ strings of length two

26 strings of length one

Note that there is one string of length zero called empty string:

It is customary to take this empty string in the counting when we want to find the number of strings of length n or less.

The number of strings of length four or less of lower case English letters
$= 4{,}56{,}976 + 17{,}576 + 6{,}756 + 26 + 1 = 4{,}75{,}255.$

P2:

Each user on a computer system has a password, which is six to eight character long, where each character is an uppercase English letter (A – Z) or a digit (0 – 9). Each password must contain at least one digit. How many possible passwords are there?

Solution:

Let P be the total number of possible passwords, and let P_6, P_7 and P_8 denote the number of passwords of length 6, 7, and 8 respectively. By the sum rule

$$P = P_6 + P_7 + P_8$$

To find P_6 , find the number of strings x of uppercase letters and digits that are six characters long and subtract from this, the number of strings y with no digits. By the product rule we see $x = 36^6$ and $y = 26^6$. Thus, $P_6 = 36^6 - 26^6$.

Similarly, $P_7 = 36^7 - 26^7$ and $P_8 = 36^8 - 26^8$.

Therefore $P = P_6 + P_7 + P_8 = 36^6 + 36^7 + 36^8 - (26^6 + 26^7 + 26^8)$

$$= 26{,}84{,}48{,}30{,}63{,}360$$

P3

How many positive integers between 100 and 999 inclusive

a. **are divisible by 3 or 4**
b. **are not divisible by either 3 or 4**
c. **are divisible by exactly one of 3 and 4**

Solution:

Let $U = \{100,101, \dots ,999\}$. Then $|U| = 900$.

Let A, B be the set of positive integers between 100 and 999 (both inclusive), which are divisible by 3, 4 respectively.

$$|A| = 300\,, |B| = 225$$

The set $A \cap B$ is the set of positive integers divisible by 3 and 4. Since 3 and 4 are relatively prime.

$$|A \cap B| = 75$$

a. The set $A \cup B$ is the set of positive integers divisible by 3 or 4.
   By the principle of inclusion- exclusion
$$|A \cup B| = |A| + |B| - |A \cap B| = 300 + 225 - 75 = 450$$

b. The set of positive integers which are not divisible by either 3 or 4 is $(A \cup B)'$.
   We have
$$(A \cup B)' = |U| - |A \cup B| = 900 - 450 = 450$$

c. The set of positive integers which are divisible by exactly one of 3 and 4 is given by
$$(A - B) \cup (B - A)\; i.e., A \oplus B$$

   Now $|A \oplus B| = |A| + |B| - 2|A \cap B|$

$$= 300 + 225 - 2 \cdot 75 = 375$$

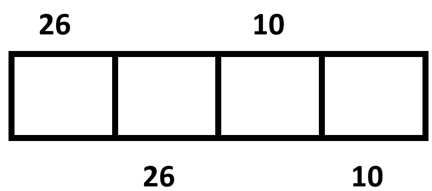
P4:

How many license plates can be made using either two or three letters followed by either two or three digits?

Solution:

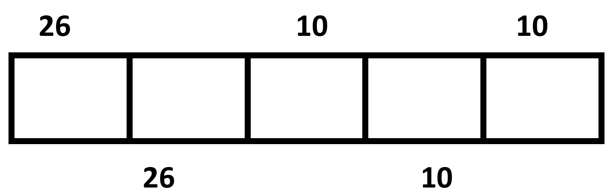
The following are four types of license plates:

(i) T_1: Two letters followed by two digits



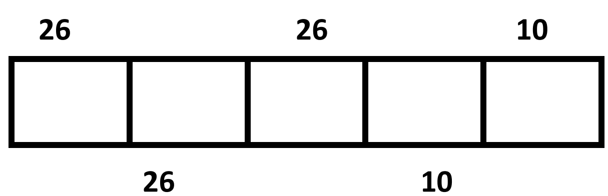
By product rule, $|T_1| = 26 \times 26 \times 10 \times 10 = 67600$

(ii) T_2: Two letters followed by three digits



By product rule, $|T_2| = 26 \times 26 \times 10 \times 10 \times 10 = 676000$

(iii) T_3: Three letters followed by two digits



By product rule, $|T_3| = 26 \times 26 \times 26 \times 10 \times 10 = 1757600$

(iv) T_4: Three letters followed by three digits

26	26	26	10	10	10

By product rule, $|T_4| = 26 \times 26 \times 26 \times 10 \times 10 \times 10 = 17576000$

The required number of license plates is

$|T_1 \cup T_2 \cup T_3 \cup T_4| = |T_1| + |T_2| + |T_3| + |T_4|$ (By sum rule)

Note that $T_i \cap T_j = \phi \,, i \neq j$

$$= 57600 + 576000 + 1757600 + 17576000$$

$$= 2{,}00{,}77{,}200$$

P5:

How many functions are there from the set $\{1, 2, 3, \dots, n\}$, where n is a positive integer, to the set $\{0, 1\}$

a. **that are one-to-one**
b. **that assign 0 to both 1 and n**
c. **that assign 1 to exactly one of the positive integers less than n**

Solution:

The number of one-to-one function from a set with m elements to a set with n-elements is

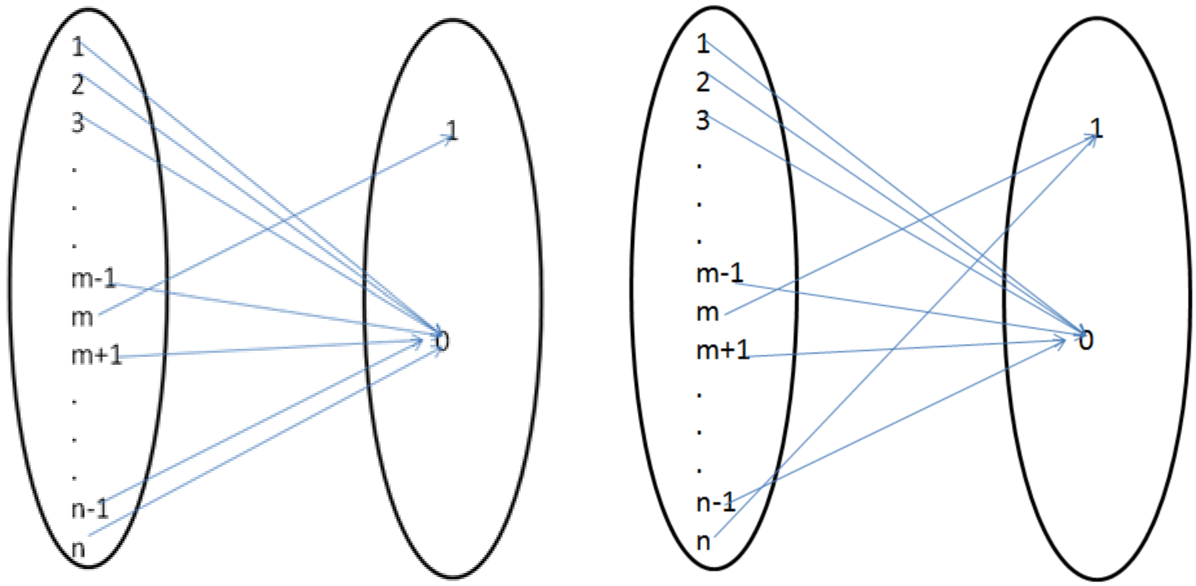
$$\begin{array}{ll} n(n-1)(n-2)\dots(n-m+1) & \text{if } m \leq n \\ 0 & \text{if } m > n \end{array}$$

(a) The number of one-to-one function from the set $\{1,2,\dots,n\}$ to a set $\{0,1\}$ is

$$\begin{array}{ll} 0 & \text{if } n > 2, i.e., n \geq 3 \\ 2 & \text{if } n = 1,2 \end{array}$$

(b) The number of functions that map 1 and n to 0 is equal to the number functions from the set $\{2,3,4,\dots,n-1\}$ to the set $\{0,1\}$ is 2^{n-2} if $n > 1$. If $n = 1$ then the number functions that map 1 to 0 is 1.

(c) Notice that there are $n-1$ positive integers less n in $\{1,2,3,4,\ldots,n\}$. Suppose that we select one of positive integer less than n, say m. If only m is mapped to 1 and no others less than n then $1,2,\ldots,m-1,m+1,\ldots n-1$ must be mapped to 0 and n can be mapped either to 0 or 1.



Thus, we have two such functions. Since m can chosen in $n-1$ ways, the number of such functions is $2(n-1)$, (by product rule).

P6:

Palindrome: A **palindrome** is a string whose reversal is identical to the string**.**

Example: How many bit strings of length n are palindromes.

Solution:

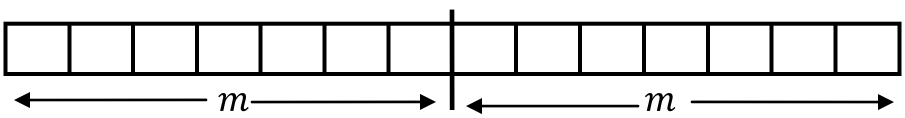
A palindrome is a string whose reversal is identical to the string.

For example, the bit string 0110110 of length 7 is a palindrome. The bit string 101101 of length 6 is a palindrome

Consider bit strings of length n.

We have two cases (i) n is even (ii) n is odd.

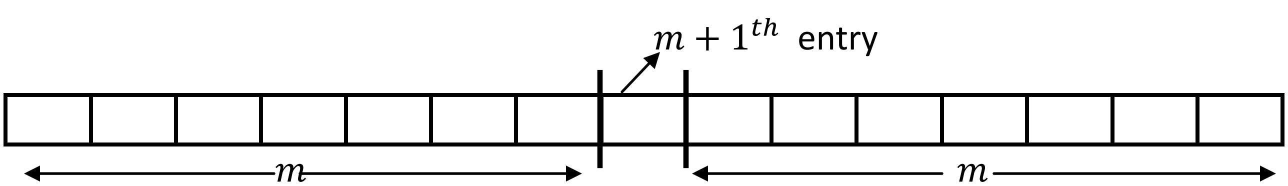
Case (i) Suppose that n is even say $n = 2m$, for some positive integer m.



$$n = 2m$$

A string of length $n = 2m$ can be seen as two strings of length m arranged side by side. If a (bit) string of length m in the left part is written in reverse order in the right part then we get a palindrome of length $n = 2m$. Thus, the number of palindromes of length $n = 2m$ is equal to the number of bit strings of length m, $i.e.$, 2^m that $2^{\frac{n}{2}}$,where n is even.

Case (ii) Suppose that n is odd, say $n = 2m + 1$, for some positive integer m.



A string of length $n = 2m + 1$ can be seen as two strings of length m arranged on either side of $(m + 1)^{\text{th}}$ entry, if the string of length m on the left side of

$(m+1)^{\text{th}}$ entry is written in the reverse order on the right side of the $(m+1)^{\text{th}}$ entry then we get a palindrome of length $n = 2m+1$. Thus,

The palindromes of length $n = 2m+1$

$$= 2 \times (\text{the number of bit strings of length } m)$$

$$= 2 \times 2^m = 2^{m+1} = 2^{\frac{n-1}{2}+1} = 2^{\frac{n+1}{2}}$$

Note: In the case of bit strings, the alphabet is $\{0,1\}$. If the alphabet is of order k then the number of palindromes of length n is

$k^{\frac{n}{2}}$ if n is even

$k^{\frac{n+1}{2}}$ if n is odd

P7:

How many positive integers not exceeding 100 are divisible either by 4 or by 6?

Solution:

Let A be the set of positive integers not exceeding 100 which are divisible by 4.

Let B be the set of positive integers not exceeding 100 which are divisible by 6.

Then

$$|A| = \left\lfloor \frac{100}{4} \right\rfloor = 25 \quad ; \qquad |B| = \left\lfloor \frac{100}{6} \right\rfloor = 16$$

The set of positive integers not exceeding 100 divisible by 4 and 6 is $A \cap B$. Then

$$|A \cap B| = \left\lfloor \frac{100}{lcm\{4,6\}} \right\rfloor = \left\lfloor \frac{100}{12} \right\rfloor = 8$$

By the principle of inclusion-exclusion, we have

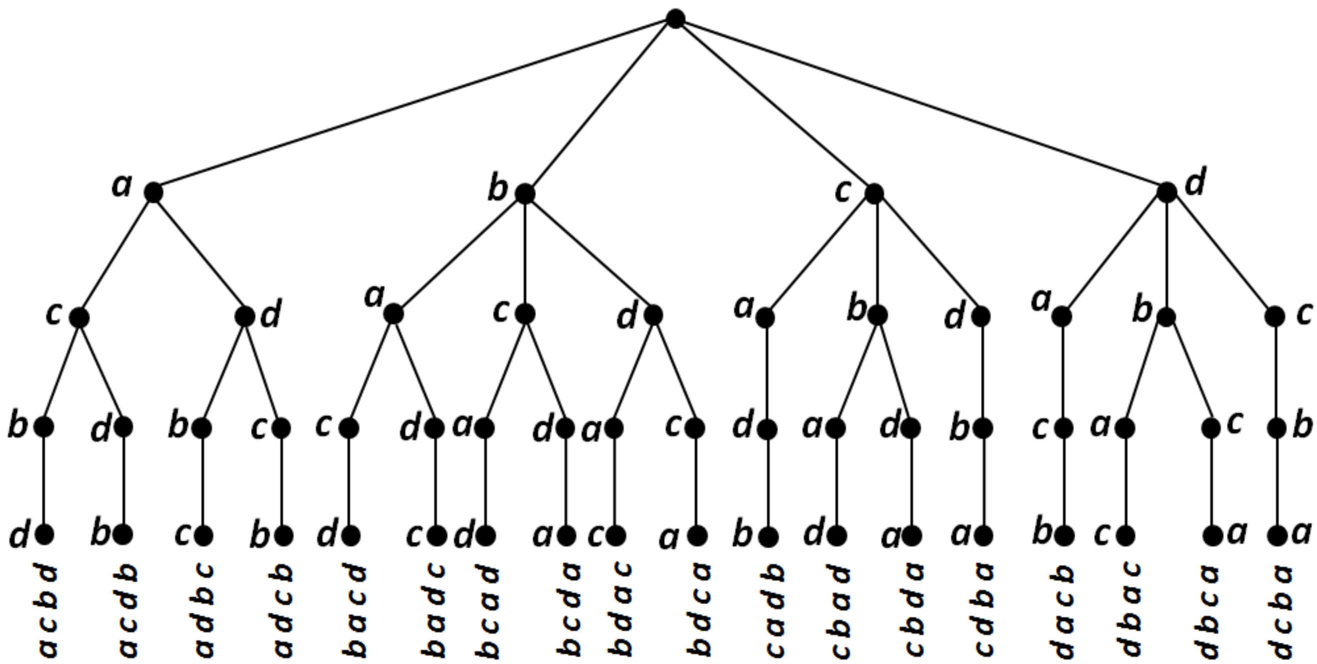
$$|A \cup B| = |A| + |B| - |A \cap B| = 25 + 16 - 8 = 33$$

Thus, the number of positive integers not exceeding 100 are divisible either by 4 or by 6 is 33.

P8:

Use a tree diagram to fine the number of ways to arrange the letters $\boldsymbol{a, b, c}$ and $\boldsymbol{d}$ such that $\boldsymbol{a}$ is not followed immediately by $\boldsymbol{b}$.

Solution:



The tree diagram displays arrangements of the letters a, b, c and d such that a is not followed immediately by b. There are 18 such arrangements.

4.1. Counting Principles.

Exercise:

1. How many different three-letters initials can people have?
2. How many different three-letters initials with none of the letters repeated can people have?
3. How many different three-letter initials are there that begin with an A?
4. How many bit stings are there of length eight?
5. How many bit strings of length ten both begin and end with a 1?
6. How many bit strings are there of length six or less?
7. How many bit strings with length not exceeding n, where n is a positive integer, consist entirely of $1's$?
8. How many strings are there of lowercase letters of length four or less?
9. How many strings are there of four lowercase letters that have the letter x in them?
10. How many positive integers less than 1000
    a. are divisible by 7?
    b. are divisible by 7 but not by 11?
    c. are divisible by both 7 and 11?
    d. are divisible by either 7 or 11?
    e. are divisible by exactly one of 7 and 11?
    f. are divisible by neither 7 nor 11?
    g. have distinct digits?
    h. have distinct digits and are even?

11. How many positive integers between 1000 and 9999 inclusive
    a. are divisible by 9?
    b. are even?
    c. have distinct digits?
    d. are not divisible by 3?
    e. are divisible by 5 or 7?
    f. are not divisible by either 5 or 7?

g. are divisible by 5 but not by 7?
h. are divisible by 5 and 7?

12. How many license plates can be made using either three digits followed by three letters or three letters followed by three digits?
13. How many license plates can be made using either two letters followed by four digits or two digits followed by four letters?
14. How many license plates can be made using either three letters followed by three digits or four letters followed by two digits?
15. How many strings of eight English letters are there
    a. that contain no vowels, if letters can be repeated?
    b. that contain no vowels, if letters cannot be repeated?
    c. that start with a vowel, if letters can be repeated?
    d. that start with a vowel, if letters cannot be repeated?
    e. that contain at least one vowel, if letters can be repeated?
    f. that contain exactly one vowel, if letters can be repeated?
    g. that start with X and contain at least one vowel, if letters can be repeated?
    h. that start and end with X and contain at least one vowel, if letters can be repeated?
16. How many different functions are there from a set with 10 elements to sets with the following number of elements?
    a. 2 $b.3$ $c.4$ $d.5$
17. How many one-to-one functions are there from a set with five elements to sets with the following number of elements?
    $a.4$ $b.5$ $c.6$ $d.7$
18. How many functions are there from the set $\{1,2,3, \dots, n\}$, where n is a positive integer, to the set $\{0,1\}$?
19. How many bit strings of length seven either begin with two $0's$ or end with three$1's$?
20. How many bit strings of length 10 either begin three $0's$ or end with two $0's$?

21. Use a tree diagram to find the number of bit strings of length four with no three consecutive $0's$.

MODULE-2

Pigeon-hole Principle

4.2

Pigeon hole Principle

Suppose that a flock of 20 pigeons flies into a set of 19 pigeonholes to roost. Because there are 20 pigeons but only 19 pigeonholes, at least one of these 19 pigeonholes must have at least two pigeons in it. If each pigeonhole had at most one pigeon in it, at most 19 pigeons, one per hole, could be accommodated. This illustrates a general principle called the **pigeonhole principle**, which states that if there are more pigeons than pigeonholes, then there must be at least one pigeonhole with at least two pigeons in it.

Theorem 1: The Pigeonhole Principle

If k is a positive integer and $k + 1$ or more objects are placed in k boxes, then there is at least one box containing two or more objects.

Proof: We give the proof by contraposition. Suppose that none of the k boxes contains more than one object. Then the total number of objects would be at most k. This is a contradiction, because there are at least $k + 1$ objects. Hence the theorem.

The pigeonhole principle is also called the **Dirichlet drawer principle**. It is named after the nineteenth century German mathematician Dirichlet (1805-1859), who often used this principle in his work.

The pigeonhole principle can be used to prove a useful result about functions.

Theorem 2: A function f from a set with $k + 1$ or more elements to a set with k elements is not one-to-one.

Proof: Suppose that for each element b in the codomain of f we have a box that contains all elements x of the domain of f such that $f(x) = b$. Thus, we have k boxes and $k + 1$ or more elements of the domain are to be placed in these k boxes. By the pigeonhole principle at least one box receives two or more elements of the domain. That is f cannot be one – to – one.

Example 1: Show that for every positive integer n there is a multiple of n that has only $0s$ and $1s$ in its decimal expansion.

Solution: Let n be a positive integer. Consider that $n+1$ integers

$$1,\ 11,\ \ 111,\dots,111\dots1$$

where the last integer in this list is the integer with $n+1, 1s$ in its decimal expansion. First note that the difference of any two in this list has a decimal expansion consisting entirely of $0s$ and $1s$. It is known that there are n possible remainders, $0,1,2,\dots,n-1$, when an integer is divided by n. Because there are $n+1$ integers in the list, by the pigeonhole principle there must be two integers say p,q in the list with the same remainder say $r \in \{0,1,\dots,n-1\}$ when divided by n. Let $p<q$. Then

$$q=tn+r,\ \ p=sn+r$$

for some positive integer $t,\ s$ and $q-p=(t-s)n$

Thus, a multiple of n has only $0s$ and $1s$ in its expansion. Hence the result.

The following example shows how the pigeonhole principle is used:

Example 2: In any group of 27 English words there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.

The generalized Pigeonhole Principle:

The pigeonhole principle states that there must be at least two objects in the same box when there are more objects than boxes. However, even more can be said when the number of objects exceed a multiple of the number of boxes.

The Generalized Pigeonhole Principle:

If N objects are palced into k boxes, then there is at least one box receiving at least $\lceil N/k \rceil$ objects.

Proof: The proof is given by the method of contradiction. Suppose that none of the boxes receives more than $\lceil N/k \rceil - 1$ objects. Then, the total number of objects is at most

$$k\left(\left\lceil\frac{N}{k}\right\rceil - 1\right) < k\ \left(\left(\frac{N}{k} + 1\right) - 1\right) = N\ ,$$

where the inequality $\left\lceil\frac{N}{k}\right\rceil < \frac{N}{k} + 1$ is used in the above. This is a contradiction, because there are a total of N objects. Hence the theorem.

Example 3: What is the minimum number of students required in a discrete structures class to be sure that at least six will receive the same grade, if there are five possible grades $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D}$ and $\boldsymbol{E}$?

Solution: The minimum number of students required to ensure that at least six students receive the same grade is the smallest positive integer N such that $\left\lceil\frac{N}{5}\right\rceil = 6$, The smallest such integer is $N = 5.5 + 1 = 26$. Thus, 26 is the minimum number of students required to ensure that at least six students will receive the same grade.

Example 4: During a month of $\mathbf{30}$ days, a baseball team plays at least one game a day, but no more than $\mathbf{45}$ games. Show that there must be a period of some number of consecutive days during which the team must play exactly $\mathbf{14}$ days.

Solution: Let a_j be the number of games played on or before the j^{th} day of the month. Then $a_1, a_2, \dots, a_{30}$ is an increasing sequence of distinct positive integers, with $1 \le a_j \le 45$. Notice that $a_1 + 14,\ \ a_2 + 14, \dots, a_{30} + 14$ is an increasing sequence of distinct positive integers with $15 \le a_j + 14 \le 59$. Now, we have 60 positive integers

$$a_1, a_2, \dots, a_{30}, a_1 + 14, a_2 + 14, \dots, a_{30} + 14$$

which are less than or equal to 59. By pigeonhole principle , two of these integers are equal. Because $a_j,\ \ j = 1, 2, \dots, 30$ are all distinct and $a_j + 14,\ \ j = 1, 2, \dots, 30$ are all distinct, there must be indices i and j with

$$a_i = a_j + 14,\ i.e.,\ a_i - a_j = 14$$

This means that exactly 14 games were played from $(j+1)^{th}$ day to i^{th} day. Hence the result.

Example 5: Show that among $n+1$ positive integers not exceeding $2n$ there must be an integer that divides one of the other integers.

Solution: Let the $n+1$ positive integers, not exceeding $2n$, be $a_1, a_2, \dots, a_{n+1}$. Let $a_j = 2^{k_j} q_j,\ j = 1, 2, \dots, n+1$, where k_j is a nonnegative integer and q_j is an odd positive integer. Thus, we have $n+1$ odd positive integers $q_1, q_2, \dots, q_{n+1}$ less than $2n$. Because there are only n odd positive integers less than $2n$, by pigeonhole principle, two of these $q_1, q_2, \dots, q_{n+1}$ must be equal. Therefore, there are integers i and j such that $q_i = q_j$. Then $a_i = 2^{k_i} q_i$ and $a_j = 2^{k_j} q_i$. If $k_i < k_j$, then $a_i | a_j$; while if $k_i > k_j$, then $a_j | a_i$

Before going to the next theorem, we review some definitions.

Suppose that $a_1, a_2, \dots, a_N$ is a sequence of real numbers. A **subsequence** of this sequence is a sequence of the form $a_{i_1}, a_{i_2}, \dots, a_{i_m}$, where

$$1 \le i_1 < i_2 < \cdots < i_m \le N.$$

A sequence is called **strictly increasing** if each term is larger than the one that precedes it and is called **strictly decreasing** if each term is smaller than the one that precedes it.

Theorem 3: Every sequence of n^2+1 distinct real numbers contains a subsequence of length $n+1$ that is either strictly increasing or strictly decreasing.

Proof: Let $a_1, a_2, \dots, a_{n^2+1}$, be a sequence of n^2+1 distinct real numbers. We associate with each term a_k an ordered pair (i_k, d_k), where i_k is the length of the longest increasing subsequence starting at a_k and d_k is the length of the longest decreasing subsequence starting at a_k. Notice that there are n^2+1 ordered pairs (i_k, d_k).

Assume the contrary. That is, assume that there are no increasing or decreasing subsequence of length $n+1$. Then i_k and d_k are both positive integers less than or equal to n, for $k = 1, 2, \dots, n^2+1$. By product rule there are n^2 possible ordered pairs (i_k, d_k). By the pigeonhole principle, two of these n^2+1 ordered pairs are equal. That is, there exist terms a_s and a_t, with $s < t$ such that $i_s = i_t$ and $d_s = d_t$. We will now show that this leads to contradictions. Because the terms of the sequence are distinct, we have either

$$a_s < a_t \text{ or } a_s > a_t$$

Let $a_s < a_t$. There is an increasing subsequence of length i_t beginning at a_t. Because, $a_s < a_t$, we have an increasing subsequence of length $i_t + 1 > i_s$ starting at a_s -a contradiction.
Let $a_s > a_t$. There is a decreasing subsequence of length i_s beginning at a_s. Because, $a_s > a_t$, we have a decreasing subsequence of length $i_s + 1 > i_t$ starting at a_t - a contradiction. Hence the theorem.

Example 6: Let (x_i, y_i, z_i), $i = 1, 2, \dots, 9$ be a set of nine distinct points with integer coordinates in xyz-space. Show that the midpoint of at least one pair of these points has integer coordinates.

Solution: Two integers x and y are said to be of the **same parity** if either both x and y are odd or both x and y are even.

The midpoint of the line segment joining the points (a, b, c) and (p, q, r) is $\left(\frac{a+p}{2}, \frac{b+q}{2}, \frac{c+r}{2}\right)$. It has integer coordinates if and only a and p have same parity, b and q have same parity, and c and r have same parity.

Note that there are eight possible triples of parity,

$$(e,e,e), (e,e,o), (e,o,e), (e,o,o), (o,e,e), (o,e,o), (o,o,e), (o,o,o),$$

where e and o respectively denote even and odd and each point (x_i, y_i, z_i), $i = 1, 2, \dots, 9$ has a parity triple. By the pigeonhole principle, at least two of the nine points have the same triple of partities. Thus, the midpoint of the line segment joining such points has integer coordinates.

Example 7:

a) **Show that if five integers are selected from the first eight positive integers, then there must be a pair of these integers with a sum equal to 9.**
b) **Is the conclusion in part (a) true if four integers are selected rather than five?**

Solution: Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$

a) Partition the set A into 4 subsets $\{1, 8\}, \{2, 7\}, \{3, 6\}$ and $\{4, 5\}$. Each consisting of two integers whose sum is 9. If five integers are selected from A then by pigeonhole principle, at least two must be from the same subset and the sum of these two integers is 9.
b) The conclusion in part (a) is false if four integers are selected. Take $A = \{1, 2, 3, 4\}$. Then the conclusion is false.

Example 8: In any group of six people each pair of individuals consists of two friends or two enemies. Prove that there are either 3 mutual friends or 3 mutual enemies.

Solution: Let A, B, C, D, E and F be six people. Consider A. Of the remaining five other people B, C, D, E and F, there are either three or more who are friends of A or three or more who are enemies of A. This follows from the generalized pigeon hole principle, because when five objects are divided into two sets, one of these sets has at least $\left\lceil \frac{5}{2} \right\rceil = 3$ objects.

In the first case, suppose that $B, C$and D are friends of A. If any two of these three are friends say B, C then A, B and C are mutual friends. Otherwise (*i.e.,* no two of B, C and D are friends) B, C and D are mutual enemies.

In the second case, suppose that that $B, C$and D are enemies of A. if any two of these three are enemies say B, C then A, B and C are mutual enemies. Otherwise (*i.e.,* no two of B, C and D are enemies) B, C and D are mutual friends.

Hence the result

Example 9: Show that in a group of 10 people (where any two people are either friends or enemies) there are either three mutual friends or four mutual enemies and there are either three mutual enemies or four mutual friends.

Solution: By symmetry we need to prove only the first statement,$i.e$, there are either 3 mutual friends or 4 mutual enemies.

Let A be one of the ten people. Of the remaining 9 other people, there are $\left\lceil \frac{9}{2} \right\rceil = 5$ or more who are enemies of A. Suppose that A has at most 5 enemies and at most 3 friends. Then the total people are $5 + 3 = 8$ people, which is a contradiction, because we have 9 people.Therefore A has at least 4 friends or at least 6 enemies in the remaining 9 people.

Case (i): Suppose that A has 4 friends, say B, C, D and E. If any two of these say, B, C ,are friends then we have found three (A,B and C) mutual friends. Otherwise $\{\mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}\}$ is a set of four mutual enemies.

Case(ii): Let $\{\mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}, \mathrm{G}\}$ be the set of 6 enemies of A. It is known that among any six people there are either three mutual friends or three mutual enemies. These three mutual enemies form with A, a set of four mutual enemies. Hence the result.

MODULE-3

Permutations and Combinations

4.3

Permutations and Combinations

Many counting problems can be solved by finding the number of ways to arrange a specified number of distinct elements of a set of a particular size, where the order of these elements matters. Many other counting problems can be solved by finding the number of ways to select a particular number of elements from a set of particular size where the order does not matter. In this module we will develop methods for such counting problems through permutations and combinations.

Permutations

A **permutation** of a set A of distinct objects is an ordered arrangement of the objects of A.

The following is the concept of an ordered arrangement of some elements of a set.

An ordered arrangement of r elements of a set A is called an $\boldsymbol{r}$ **− permutation** of A.

The number of $r -$ permutation of a set with n elements is denoted by ${}^nP_r$ or $P(n, r)$. We can find ${}^nP_r$ using the product rule.

Theorem1: If $\boldsymbol{n}$ is a positive integer and $\boldsymbol{r}$ is an integer with $\boldsymbol{1 \leq r \leq n}$, then there are

$${}^nP_r = n(n-1)(n-2)\ldots(n-r+1)$$

$\boldsymbol{r} -$ **Permutations of a set with $\boldsymbol{n}$ elements**.

Proof: The first element of the $r -$ permutation can be chosen in n ways, because there are n elements in the set. The second element can be chosen in $n - 1$ ways, because there are $n - 1$ elements left in the set after using the element in the first position. Similarly, there are $n - 2$ ways to chose the third element, and so on, until there are exactly $n-(r-1)=n-r+1$ ways to choose the r^{th} element. By the product rule, there are

$$n(n-1)(n-2)\dots(n-r+1)$$

$r-$ permutations of the set. Thus,

$$^{n}P_{r}=n(n-1)(n-2)\dots(n-r+1)$$

Note:

1. $^{n}P_{n}=n(n-1)(n-2)\dots3.2.1=n!$, where n is a positive integer.

2. $^{n}P_{0}=1$, when n is a nonnegative integer, because there is exactly one way to order zero elements. That is, there is exactly one list with no elements in it, namely the empty set.

Corollary 1: If $\boldsymbol{n}$ and $\boldsymbol{r}$ are integers with $\boldsymbol{0\le r\le n}$, then

$$^{n}P_{r}=\frac{n!}{(n-r)!}$$

Proof: When n and r are integers with $1\le r\le n$, by Theorem 1, we have

$$^{n}P_{r}=n(n-1)(n-2)\dots(n-r+1)$$

$$=\frac{n(n-1)(n-2)\dots(n-r+1).(n-r).(n-r-1).(n-r-2)\dots.3.2.1}{(n-r).(n-r-1).(n-r-2)\dots.3.2.1}$$

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

We see that $^{n}P_{0}=\frac{n!}{(n-0)!}=\frac{n!}{n!}=1$, where n is a nonnegative integer. Thus, the formula for $P(n,r)$ also holds when $r=0$.

Example 1: How many permutations of the letters $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$, $\boldsymbol{E}$, $\boldsymbol{F}$, $\boldsymbol{G}$ and $\boldsymbol{H}$ contain the string . (See **P1**)

Example 2: How many ways are there to select a first – prize winner, a second – prize winner, and a third – prize winner from $\mathbf{100}$ different people who have entered a contest. (See **P1**)

Example 3: A group contains $\boldsymbol{n}$ men and $\boldsymbol{n}$ women. How many ways are there to arrange these people in a row if the men and women alternate? (See **P2**)

Combinations

We now discuss the counting of unordered selections of objects. Many counting problems can be solved by finding the number of subsets of a particular size of a set with n elemens, where n is a positive integer.

$\boldsymbol{r} -$ **Combination:** An $\boldsymbol{r} -$ **Combination** of elements of a set A is an unordered selection of r elements from the set A. That is, an r −combination of a set is simply a subset of the set with r elements.

The number of r −combinations of a set with n distinct elements is denoted by ${}^{n}C_{r}$ or $\binom{n}{r}$ or $C(n,r)$ and is called a **binomial coefficient**.

Theorem 2: The number of $\boldsymbol{r}$ −combinations of a set with $\boldsymbol{n}$ elements, where $\boldsymbol{n}$ is a nonnegative integer and $\boldsymbol{r}$ is an integer with $\mathbf{0} \le \boldsymbol{r} \le \boldsymbol{n}$ is given by

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

Proof: The r −permutation of the set can be obtained by forming ${}^{n}C_{r}$ r −combinations of the set, and then ordering the elements of each r −combination, which can be done in ${}^{r}P_{r}$ ways. Therefore, ${}^{n}P_{r} = {}^{n}C_{r} . {}^{r}P_{r}$.

This implies that

$$^{n}C_{r}=\frac{^{n}P_{r}}{^{r}P_{r}}=\frac{\frac{n!}{(n-r)!}}{\frac{r!}{(r-r)!}}=\frac{n!}{r!(n-r)!}$$

$$i.e., \; \boldsymbol{^{n}C_{r}=\frac{n!}{r!(n-r)!}} \text{ or } \boldsymbol{^{n}C_{r}=\frac{n(n-1)(n-2)\ldots(n-r+1)}{r!}}$$

Corollary 2: Let n and r be nonnegative integers with $r \le n$ then $^{n}C_{r} = {}^{n}C_{n-r}$

Proof: From Theorem 2, we have

$$^{n}C_{r}=\frac{n!}{r!(n-r)!} \quad ; \quad ^{n}C_{n-r}=\frac{n!}{(n-r)!(n-(n-r))!}=\frac{n!}{r!(n-r)!}$$

Therefore, $^{n}C_{r}={}^{n}C_{n-r}$.

A ***combinatorial proof*** of an identity is a proof that uses counting arguments to prove that both sides of the identity count the same objects but in different ways.

Many identities involving binomial coefficients can be proved using combinatorial proofs. The following is a combinatorial proof of Corollary 2:

Proof: let S be a set with n elements. Every subset A of S with r elements corresponds to a subset of S with $n-r$ elements, namely $A'(=S-A)$ Consequently, the number of subsets of S with r elements $(0 \le r \le n)$ is equal to the number of subsets of with $n-r$ elements. Thus,

$$^{n}C_{r}={}^{n}C_{n-r}$$

Example 4: How many bit strings of length n contain exactly r 1s?

Solution: The position of r 1s in a bit string of length n form an r- combination of the set $\{1, 2, \dots, n\}$. Hence there are ${}^{n}C_{r}$ bit strings of length n that contain exactly r 1s.

Example 5: How many bit strings of length 10 contain

(a) Exactly four 1s **(b) at most four 1s**

(c) at least four 1s **(d) an equal number of 0s and 1s**

(See **P3**)

Theorem 3: Binomial Theorem

Let x and y be variables and let n be a nonnegative integer. Then

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$$

$$= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{r}x^{n-r}y^r + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$

Proof: We give a combinatorial proof.

First we note that $(x+y)^n = \underbrace{(x+y)(x+y)\dots(x+y)}_{n\ times}$

The terms in the product when it is expanded are of the form $x^{n-r}y^r$ for $r = 0, 1, 2, \dots, n$. Note that to obtain such a term it is necessary to choose $n-r$ xs so that the other r terms in the product are ys. The number of such terms is $\binom{n}{n-r}$ which is same as $\binom{n}{r}$. Thus the coefficient of $x^{n-r}y^r$ is $\binom{n}{r}$.

This proves the theorem.

We can prove some useful identities using the binomial theorem.

Corollary 3: Let n be a nonnegative integer. Then

$$\sum_{r=0}^{n} \binom{n}{r} = 2^n$$

Proof: Using binomial theorem with $x = 1$ and $y = 1$, we see that

$$2^n = (1+1)^n = \sum_{r=0}^{n} \binom{n}{r} 1^{n-r} 1^r = \sum_{r=0}^{n} \binom{n}{r}$$

Hence the result

Corollary 4: Let n be a positive integer. Then

$$\sum_{r=0}^{n} (-1)^r \binom{n}{r} = 0$$

Proof: Let n be a positive integer. Using binomial theorem with $x = 1$ and $y = -1$, we see that

$$0 = 0^n = (1 + (-1))^n = \sum_{r=0}^{n} \binom{n}{r} 1^{n-r} (-1)^r = \sum_{r=0}^{n} (-1)^r \binom{n}{r}$$

Hence the result

Note: From this corollary it follows that

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$$

Corollary 5: Let n be a nonnegative integer. Then

$$\sum_{r=0}^{n} 2^r \binom{n}{r} = 3^n$$

Proof: Using binomial theorem with $x = 1$ and $y = 2$, we see that

$$3^n = (1+2)^n = \sum_{r=0}^{n} \binom{n}{r} 1^{n-r} 2^r = \sum_{r=0}^{n} 2^r \binom{n}{r}$$

Hence the result

Pascal's identity

The binomial coefficients satisfy many different identities. The following is the one of the most important identity.

Theorem 4: Pascal's identity

Let $\boldsymbol{n}$ and $\boldsymbol{r}$ be positive integers with $\boldsymbol{r \leq n}$. Then

$$\binom{\boldsymbol{n}}{\boldsymbol{r}} + \binom{\boldsymbol{n}}{\boldsymbol{r-1}} = \binom{\boldsymbol{n+1}}{\boldsymbol{r}}$$

Proof: let T be a set containing $n+1$ elements. Let a be an element of T and let $S = T - \{a\}$. Clearly, there are $\binom{n+1}{r}$ subsets of T with r elements. Note that a subset of T with r elements either contains a together with $r-1$ elements of S or contains r elements of S and does not contain a.

Because there are $\binom{n}{r-1}$ subsets each containing $r-1$ elements, there are $\binom{n}{r-1}$ subsets of T containing a and each containing r elements. Further, there are $\binom{n}{r}$ subsets of T not containing a and each containing r elements and these are the subsets of S each containing r elements. Consequently,

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}$$

Note: Pascal's identity, together with the initial conditions $\binom{n}{0} = \binom{n}{n} = 1$ for all positive integers n, can be used to recursively define binomial coefficients. This recursive definition is useful in the computation of binomial coefficients because only addition, and not multiplication, of integers is needed to use this recursive definition.

Some other identities of the binomial coefficients

Theorem 5: Vandermonde's Identity

Let m, n and r be nonnegative integers with r not exceeding either m or n. Then

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$

Proof: Suppose that there are m items in one set and n items in a second set. Then the total number of ways to pick r elements from the union of these sets is $\binom{m+n}{r}$.

Another way to pick r elements from the union is to pick k elements from the first set and then $r-k$ elements from the second set, where k is an integer with $0 \le k \le r$. This can be done in $\binom{m}{k}\binom{n}{r-k}$ ways, using the product rule. Therefore, the total number of ways to pick r elements from union is

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$$

Let $j = r-k$. Then $k = r-j$ and

$$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \sum_{j=0}^{r} \binom{m}{r-j}\binom{n}{j}$$

Thus,

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$

Hence the result

Corollary 6: Let n be a nonnegative integer. Then

$$\binom{2n}{n} = \sum_{r=0}^{n} \binom{n}{r}^2$$

Proof: We have Vandermonde's identity

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$

Taking $m = n = r$, we get

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{n-k}\binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k}^2 \; , because \; \binom{n}{n-k} = \binom{n}{k}$$

$$= \sum_{r=0}^{n} \binom{n}{r}^2$$

Hence the result

Theorem 6: Let n and r be nonnegative integers with $r \leq n$ then

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$$

Proof: We give the combinatorial proof. By Example 4, the left-hand side, $\binom{n+1}{r+1}$, counts the number of bit strings of length $(n+1)$ containing $(r+1)$ 1s.

We will show that the right-side counts the same objects by considering the cases corresponding to the possible locations of the final 1 (or the last 1) in a string with $(r+1)$ 1s. This last 1 must occur at positions $r+1, r+2, \ldots,$ or $n+1$.

Further, if the last 1 is the k^{th} bit in the string then there must be r 1s among the first $k-1$ positions. By Example4, there are $\binom{k-1}{r}$ such bit strings.

Now summing over k from $r+1$ to $n+1$, we get

$$\sum_{k=r+1}^{n+1} \binom{k-1}{r}$$

bit strings of length $n+1$ containing exactly $+1$ $1s$. Therefore

$$\binom{n+1}{r+1} = \sum_{k=r+1}^{n+1} \binom{k-1}{r}$$

Let $= k-1$. Then

$$\sum_{k=r+1}^{n+1} \binom{k-1}{r} = \sum_{j=r}^{n} \binom{j}{r}$$

and

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$$

Hence the result.

Permutations and combinations with repetitions

Counting permutations when repetitions of elements are allowed can be easily be done using the product rule.

Theorem 7: The number of r −permutations of a set of n objects with repetition allowed is n^r .

The following is for $r-$ combinations:

Theorem 8: There are ${}^{n+r-1}C_r = {}^{n+r-1}C_{n-1}$, r −combinations from a set with n elements when repetition of elements is allowed.

Proof: Each r- combination of a set with n elements when repetition is allowed can be represented by a list with $n-1$ bars and r stars. The $n-1$ bars are used to mark off n different cells, with the i^{th} cell containing a star for each time the i^{th} element of the set occurs in the combination.

For instance, a 6- combination of a set with four elements is represented with $4-1=3$ bars and 6- stars. Now,

★★|★| |★★★

represents the combination containing exactly two of the first element, one of the second element, none of the third element and three of the fourth element of the set.

Thus, each different list containing $n-1$ bars and r- stars corresponding to an r- combination of the set with n- elements, when repetition is allowed. The number of such lists is ${}^{(n-1+r)}C_r$, because each list corresponding to a choice of r- positions to place the r- stars from the $n-1+r$ positions that contain r- stars and $n-1$ bars. Note that

$$ {}^{(n-1+r)}C_r = {}^{(n-1+r)}C_{(n-1+r)-r} = {}^{(n-1+r)}C_{n-1} $$

Example 6: Suppose that a cookie shop has four different kinds of cookies. How many different ways can six cookies be chosen? Assume that only the type of cookies and not the individual cookies or the order in which they are chosen, matters.

Solution: The number of ways to choose six cookies is the number of 6- combinations of a set with 4 elements. By Theorem 8, we have

$$ {}^{(4+6-1)}C_6 = {}^{9}C_6 = {}^{9}C_3 = \frac{9.8.7}{1.2.3} = 84 $$

Thus, there are 84 different ways to choose the six cookies from four different kinds of cookies.

Theorem 6 can also be used to find the number of solutions of certain linear equations where the variables are integers subject to constraints.

Example 7: How many solutions does the equation $x_1 + x_2 + x_3 = 11$ have, where x_1, x_2 and x_3 are nonnegative integers?

Solution: Note that a solution corresponds to a way of selecting 11 items from a set with three elements so that x_1 items of type1, x_2 items of type2 and x_3 items of type3. Hence the number of solutions is the number of 11 combinations with repetition allowed from a set with three elements. By Theorem 8, there are

$$^{(3+11-1)}C_{11} = {}^{13}C_{11} = {}^{13}C_2 = \frac{13.12}{1.2} = 78 \text{ solutions.}$$

Note: The number of solutions of this equation can also be found when the variables are subject to constraints.

Example 8: How many solutions does the equation $x_1 + x_2 + x_3 = 11$ have, where x_1, x_2 and x_3 are nonnegative integers with $x_1 \geq 1, x_2 \geq 2$ and $x_3 \geq 3$?

Solution: A solution to the equation subject to these constraints corresponds to a selection of 11 items with x_1 items of type1, x_2 items of type2 and x_3 items of type3, where in addition, there is at least one item of type1, two items of type2, and three items of type3. Therefore, there are one item of type1, two items of type2, and three items of type3. Thus, 6 items are already chosen. Then select 5 additional items. By Theorem 8, this can be done in

$$^{(3+5-1)}C_5 = {}^{7}C_5 = {}^{7}C_2 = \frac{7.6}{1.2} = 21 \text{ ways.}$$

Thus, there are 21 solutions of the equation subject to the given constraints.

Permutations with indistinguishable objects

Some elements may be indistinguishable in counting problems. When this is the case, care must be taken to avoid counting things more than once.

Theorem 9: The number of different permutations of n objects, where there are n_1 distinguishable objects of type1, n_2 distinguishable objects of type2, ... , and n_k distinguishable objects of type k, is

$$\frac{\boldsymbol{n}!}{\boldsymbol{n_1}!\,\boldsymbol{n_2}!\ldots\boldsymbol{n_k}!}$$

Proof: To determine the number of permutations, first note that n_1 objects of type 1 can be placed among n positions ${}^{n}C_{n_1}$ in ways, leaving $n - n_1$ positions free. Then the objects of type 2 can be placed in ${}^{(n-n_1)}C_{n_2}$ ways, leaving $n - n_1 - n_2$ positions free. Continue placing objects of type 3, … , type $k - 1$, until at the last stage, n_k objects of type k can be placed in ${}^{(n-n_1-n_2-\cdots-n_k)}C_{n_k}$ ways. Hence, by the product rule, the total number of different permutations is

$$\begin{aligned}
&{}^{n}C_{n_1} \cdot {}^{(n-n_1)}C_{n_2} \cdot \ \cdots \ \cdot {}^{(n-n_1-n_2-\cdots-n_k)}C_{n_k} \\
&\qquad = \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot \ \cdots \ \cdot \frac{(n-n_1-n_2-\cdots-n_{k-1})!}{n_k!(n-n_1-n_2-\cdots-n_k)!} \\
&\qquad = \frac{n!}{n_1!\,n_2!\,\cdots\,n_k!}
\end{aligned}$$

Example 9: How many different strings can be made from the letters in ABRACADABRA, using all the letters?

Solution: Note that the given word has 11 letters and it contains 5 A’s, 2 B’s, 2 R’s, one C and one D.

The number of different strings can be made from the letters of the given word using all the letter is

$$\frac{11!}{5!\,2!\,2!\,1!\,1!} = 83{,}160$$

Distributing objects into boxes

Many counting problems can be solved by enumerating the ways. The objects can be placed into boxes. The objects can be either distinguishable (*i.e.,* different from each other) or indistinguishable (*i.e.,* considered identical).

Theorem 10: The number of ways to distribute $\boldsymbol{n}$ distinguishable objects into $\boldsymbol{k}$ distinguishable boxes so that $\boldsymbol{n_i}$ objects are placed into box $\boldsymbol{i}$, $\boldsymbol{i = 1, 2, \ldots, k}$, equals

$$\frac{\boldsymbol{n}!}{\boldsymbol{n_1}!\,\boldsymbol{n_2}!\ldots\boldsymbol{n_k}!}$$

Note: Counting the number of ways of placing n distinguishable objects into k distinguishable boxes is same as counting the number of n- combinations for a set of k elements when repetitions are allowed.

P1:

a. **How many permutations of the letters $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$, $\boldsymbol{E}$, $\boldsymbol{F}$, $\boldsymbol{G}$ and $\boldsymbol{H}$ contain the string $\boldsymbol{ABC}$.**

b. **How many ways are there to select a first – prize winner, a second – prize winner, and a third – prize winner from $\mathbf{100}$ different people who have entered a contest.**

Solution:

a. Because ABC must occur as a block, we can find the number of permutations of six objects namely, the block ABC and the individual letter D, E, F, G and H. Because these six objects can occur in any order, there are $6! = 720$ permutations of letters $A\ B\ C\ D\ E\ F\ G\ H$ in which $A\ B\ C$ occurs as a block.

b. The number of ways to pick the three prize winners is the number of $3 -$ permutations of a set with 100 elements. Therefore,

$$^{100}P_3 = 100.(100-1).(100-2).(100-3) = 100.99.98 = 9{,}70{,}200$$

P2:

A group contains n men and n women. How many ways are there to arrange these people in a row if the men and women alternate?

Solution:

It amounts to arrange them in a row of $2n$ places in two ways.

(i) Men occupying odd positions and Women occupying even positions. This can be done in $n!\,.\,n! = (n!)^2$ (by the product rule).

(ii) Women occupying odd positions and Men occupying even positions. This can be done in $n!\,.\,n! = (n!)^2$ (by the product rule).

The number of ways to arrange these $2n$ people in a row if the men and women sit alternately is $(n!)^2 + (n!)^2 = 2(n!)^2$.

P3:

How many bit strings of length 10 contain

(a) Exactly four 1s **(b) at most four 1s**

(c) at least four 1s **(d) an equal number of 0s and 1s**

Solution: It is known that there are ${}^{n}C_{r}$ bit strings of length n that contain exactly r 1s

(a) The number of bit strings of length 10 containing exactly four 1s is

$$^{10}C_4 = \frac{10.9.8.7}{1.2.3.4} = 210$$

(b) The number of bit strings of length of length 10 containing at most four 1s is

$$^{10}C_0 + {}^{10}C_1 + {}^{10}C_2 + {}^{10}C_3 + {}^{10}C_4 = 1 + 10 + \frac{10.9}{1.2} + \frac{10.9.8}{1.2.3} + \frac{10.9.8.7}{1.2.3.4}$$
$$= 1 + 10 + 45 + 120 + 210 = 386$$

(c) The number of bit strings of length 10 containing at least four 1s is

$$\begin{aligned}
&{}^{10}C_4 + {}^{10}C_5 + {}^{10}C_6 + {}^{10}C_7 + {}^{10}C_8 + {}^{10}C_9 + {}^{10}C_{10} \\
&= {}^{10}C_4 + {}^{10}C_5 + {}^{10}C_4 + {}^{10}C_3 + {}^{10}C_2 + {}^{10}C_1 + {}^{10}C_0 \\
&= {}^{10}C_0 + {}^{10}C_1 + {}^{10}C_2 + {}^{10}C_3 + {}^{10}C_4 + {}^{10}C_4 + {}^{10}C_5 \\
&= 386 + 210 + \frac{10.9.8.7.6}{1.2.3.4.5} = 386 + 210 + 252 = 848
\end{aligned}$$

(d) The number of bit strings of length 10 containing equal number of 0s and 1s is

$^{10}C_5 = 252$

P4.

A coin is flipped 10 times where each flip comes up either heads or tails. How many possible outcomes

a) Are there in total?
b) Contain exactly two heads?
c) Contain at most three heads?
d) Contain the same number of heads and tails?

Solution:

a) The number of possible outcomes $= \underbrace{2 \times 2 \times \ldots \times 2}_{10\ times}$ (by product rule)

$$= 2^{10} = 1024$$

b) The number of possible outcomes containing exactly two heads = the number of ways of selecting 2 places out of $10 = {}^{10}C_2 = \frac{10.9}{1.2} = 45$

c) The number of possible outcomes containing at most three heads is

$$ {}^{10}C_0 + {}^{10}C_1 + {}^{10}C_2 + {}^{10}C_3 + {}^{10}C_4 = 176 $$

d) The number of possible outcomes containing the same number of heads and tails is ${}^{10}C_5 = 252$

P5:

Show that a nonempty set has the same number of subset with an odd number of elements as it does subsets with an even number of elements?

Solution: Let A be a set with n elements.

The number of subsets of A with k elements is ${}^nC_k$.

We have

$$(x+y)^n = {}^nC_0\, x^n + {}^nC_1\, x^{n-1}y + {}^nC_2\, x^{n-2}y^2 + \cdots + {}^nC_k\, x^{n-k}y^k + \cdots + {}^nC_n\, y^n$$

Put $x = 1, y = -1$. Then

$$0 = {}^nC_0 - {}^nC_1 + {}^nC_2 - {}^nC_3 + {}^nC_4 - {}^nC_5 + \cdots + (-1)^n\, {}^nC_n$$

From this we get

$${}^nC_0 + {}^nC_2 + {}^nC_4 + \cdots = {}^nC_1 + {}^nC_3 + {}^nC_5 + \cdots$$

The LHS gives the number of subsets of A with an even number of elements and the RHS gives the number of subsets of A with an odd number of elements.

4.3. Permutations and Combinations.

Exercise

1. Suppose that there are eight runners in a race. The winner receives a gold medal, the second – place finisher receivers a silver medal, and the third – place finisher receives a bronze medal. How many different ways are there to award these medals, if all possible outcomes of race can occur and there are no ties?
2. Suppose that a saleswoman has to visit eight different cities. She must begin her trip in a specified city, but she can visit the other seven cities in any order she wishes. How many possible orders can the saleswoman use when visiting these cities?
3. How many poker hands of five cards can be dealt from a standard deck of 52 cards? Also, how many are there to select 47 cards from a standard deck of 52 cards?
4. How many ways are there to select five players from a 10 member tennis team to make a trip to a match at another school?
5. Suppose that there are 9 faculty members in the mathematics department and 11 in the computer science department. How many ways are there to select a committee to develop a discrete mathematics course at a school if the committee is to consist of three faculty members from the mathematics department and four from the computer science department?
6. Find the value of each of these quantities.

   a. $P(6,3)$ b.$(6,5)$ c.$P(10,9)$ d. $P(8,5)$

7. Find the number of $5-$ permutations of a set with nine elements.
8. In how many different orders can five runners finish a race if no ties are allowed?
9. How many possibilities are there for the win, place, and show (first, second, and third) positions in a horse with 12 horses if all orders of finish are possible?

10. There are six different candidates for governor of a state. In how many different orders can the names of the candidates be printed on a ballot?

11. How many bit strings of length 12 contain
    a) Exactly three 1s ?
    b) At most three 1s?
    c) At least three 1s?
    d) An equal number of 0s and 1s?

12. A coin is flipped eight times where each flip comes up either heads or tails. How many possible outcomes
    a) Are there in total?
    b) Contain exactly three heads?
    c) Contain at least three heads?
    d) Contain the same number of head and tails?

13. How many bit strings of length 10 have
    a) Exactly three 0s?
    b) More 0s than 1s?
    c) At least seven 1s?
    d) At least three 1s?

14. How many permutations of the letters $ABCDEFG$ contain
    a) The string BCD?
    b) The string $CFGA$?
    c) The strings BA and GF?
    d) The string ABC and DE?
    e) The string ABC and CDE?
    f) The strings CBA and BED?

15. How many different strings can be made by reordering the letters of the word SUCCESS?

16. In how many different ways can five elements be selected in order from a set with three elements when repetition is allowed?

17. How many strings of six letters are there?

18. How many ways are there to assign three jobs to five employees if each employee can be given more than one job?

19. How many ways are there to select three unordered elements from a set with five elements when repetition is allowed?
20. How many solutions are there to the equation $x_1 + x_2 + x_3 + x_4 = 7$ where x_1 , x_2 , x_3 and x_4 are nonnegative integers?
21. How many different strings can be made from the letters in MISSISSIPPI, using all the letters?
22. How many different strings can be made from the letters in ABRACADABRA, using all the letters?
23. How many different strings can be made from the letters in AARDVARK, using all the letters, if all three $A\ s$ must be consective?

.

MODULE-4

Recurrence Relations

4.4

Recurrence Relations

Many counting problems cannot be solved using the methods discussed in the modules 4.1-4.3. One such problem is: How many bit strings of length n do not contain two consecutive zeros? To solve this problem, let a_n be the number of such strings of length n. An argument can be given that shows $a_{n+1} = a_n + a_{n-1}$. This equation is called a *recurrence relation* and the initial conditions $a_1 = 1$ and $a_2 = 3$ to determine the sequence $\{a_n\}$. Further, an explicit formula can be found for a_n from the equation relating the terms of the sequence. A similar technique can be used to solve many different types of counting problems.

Recurrence relation: let $\{a_n\}$ be a sequence. 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 $a_0, a_1, a_2, \dots, a_{n-1}$ for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer.

A sequence is called a ***solution*** of a recurrence relation if its terms satisfy the recurrence relation.

Note: A recurrence relation together with initial condition provide a recursive definition of the sequence.

Example 1: The number of bacteria in a colony doubles every hour. If a colony begins with five bacteria, obtain a recurrence relation for the number of bacteria in n hours.

Solution: Let a_n be the number of bacteria at the end of n hours. Because the number of bacteria doubles every hour, the relation $a_n = 2a_{n-1}$ holds whenever n is a positive integer. It is given the initial condition $a_0 = 5$. The recurrence relation is: $a_n = 2a_{n-1}$ for all positive integers n, and $a_0 = 5$

Example 2: Determine (a) whether the sequence $\{a_n\}$, where $a_n = 3n$ for every nonnegative integer n is a solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \dots$

(b) Show the sequence $\{a_n\}$, where $a_n = 2^n$ for every nonnegative integer n is a not a solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$

Solution: The given recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$

a) Suppose that $a_n = 3n$ for every nonnegative integer.
   For $n \geq 2$, we have

$$2a_{n-1} - a_{n-2} = 2[3(n-1)] - 3(n-2) = 3n = a_n$$

   Thus, $a_n = 3n$ is a solution of the recurrence relation.

b) Suppose that $a_n = 2^n$ for every nonnegative integer.
   For $n \geq 2$, we have

$$2a_{n-1} - a_{n-2} = 2.2^n - 2^{n-2} = 2^{n-2}(2^2 - 1) = 3.2^{n-2} \neq a_n$$

   Thus, $a_n = 2^n$ is not a solution of the recurrence relation

Note: If $a_n = 5$ for every nonnegative integer n, then for $n \geq 2$, we have

$$2a_{n-1} - a_{n-2} = 2.5 - 5 = 5 = a_n$$

Thus, $\{a_n\}$, where $a_n = 5$ is a solution of the recurrence relation.

We can use recurrence relations to model a wide variety of problems.

Example 3: Compound Interest

Suppose that a person deposits $Rs. 10,000$ in a savings account at a bank yielding 11% per year with interest compounded annually. How much will be in the account after 30 years?

Solution: To solve the problem, let P_n denote the amount in the account after n years. Note that the amount in the account after n years equals the amount in the account after $n-1$ years plus the interest for the n^{th}year. Thus, we see that the sequence $\{P_n\}$ satisfies the recurrence relation

$$P_n = P_{n-1} + \frac{P_{n-1} \times 1 \times 11}{100}$$

$$= P_{n-1} + 0.11P_{n-1} = (1.11)P_{n-1}$$

The initial condition is $P_0 = 10{,}000$.

We use an iterative approach to find a formula for P_n. Note that

$$P_1 = (1.11)P_0$$

$$P_2 = (1.11)P_1 = (1.11)^2 P_0$$

$$P_3 = (1.11)P_2 = (1.11)^3 P_0$$

$$\ldots \qquad \ldots \qquad \ldots$$

$$\ldots \qquad \ldots \qquad \ldots$$

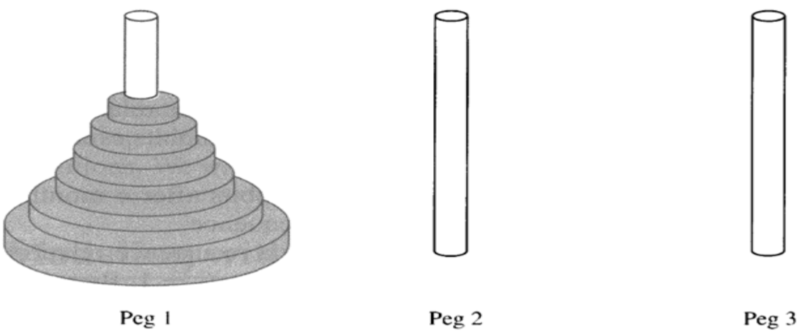
$$P_n = (1.11)P_{n-1} = (1.11)^n P_0$$

Using initial condition $P_0 = 10{,}000$, the formula $P_n = (1.11)^n 10{,}000$ is obtained.

We can use mathematical induction to establish the validity of the formula.
Putting $n = 30$, we obtain $P_{30} = (1.11)^{30} 10{,}000 = Rs.\,2{,}28{,}92{,}297$

Example 4: The Tower of Hanoi

A popular puzzle of the late nineteenth century invented by the French Mathematician Edourd Lucas, called the ***Tower of Hanoi***, consists of three pegs mounted on a board together with disks of decreasing sizes from bottom to top. Initially these disks are placed on peg 1 in order of size, with the largest on the bottom as shown below



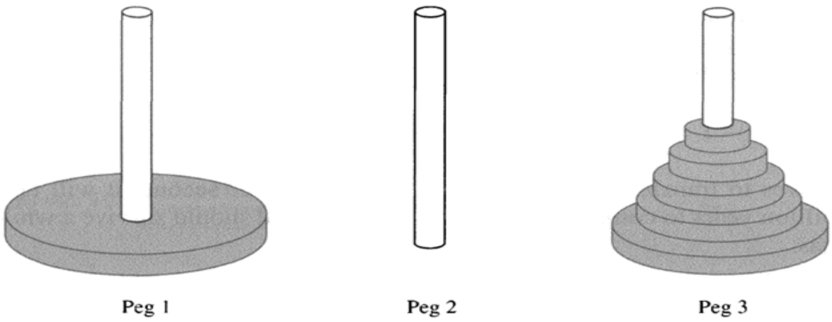
Rules: The rules of the puzzle allows disks to be moved one at a time from one peg to another as long as a disk is never placed on top of a smaller disk.

Goal: The goal of the puzzle is to have all the disks on the second peg in order of size, with the largest on the bottom.

Let H_n denote the number of moves needed to solve Tower of Hanoi problem with n disks.

Set up a recurrence relation for the sequence $\{H_n\}$.

Solution: Begin with n disks on peg 1 (as in the above figure). We can transfer the top $n-1$ disks, following the rules of the puzzle, to peg 3 using H_{n-1} moves as in the figure shown below:



We keep the largest disk fixed during these moves. Then, we use one move to transfer the largest disk to peg 2. We can transfer the $n-1$ disks on peg 3 to peg 1 using H_{n-1} additional moves, placing them on top of the largest disk, which always stays fixed on the bottom of peg 2. Further, it is easy to see that puzzle cannot be solved using fewer steps. Thus,

$$H_n = H_{n-1} + 1 + H_{n-1}$$

i.e., $H_n = 2H_{n-1} + 1$

The initial condition is $H_1 = 1$, because one disk can be transferred from peg 1 to peg 2, according to the rules of the puzzle, in one move. Therefore, the recurrence relation is

$$H_n = 2H_{n-1} + 1, \text{ for } n = 2, 3, \ldots, \text{ with the initial condition } H_1 = 1$$

Solution of the recurrence relation:

We can use an iterative approach to solve the recurrence relation. For $n \geq 2$,

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

$$= 2(2\,H_{n-2} + 1) + 1 = 2^2\,H_{n-2} + 2 + 1$$

$$= 2^2(2\,H_{n-3} + 1) + 2 + 1 = 2^3\,H_{n-3} + 2^2 + 2 + 1$$

$$\dots \quad \dots \quad \dots \quad \dots$$

$$\dots \quad \dots \quad \dots \quad \dots$$

$$= 2^{n-1}H_1 + 2^{n-2} + 2^{n-3} + \cdots + 2 + 1$$

$$= 2^{n-1} + 2^{n-2} + 2^{n-3} + \cdots + 2 + 1 \qquad \text{(Since } H_1 = 1\text{)}$$

$$= \frac{2^n - 1}{2 - 1} = 2^n - 1$$

Example 5: Codeword Enumeration

A computer system considers a string of decimal digits a valid codeword if it contains an even number of $\mathbf{0}$ digits. (For instance, $\mathbf{1230407869}$ is valid, where as $\mathbf{120987045608}$ is not valid). If $\boldsymbol{a_n}$ is the number of valid $\boldsymbol{n}$- digit code words then find a recurrence relation for $\boldsymbol{a_n}$.

Solution: Note that there are ten one - digit strings, and only one, namely 0 is not valid. Therefore, $a_1 = 9$. Let $n \geq 2$.

We can obtain a valid string with n digits from a string with $n - 1$ digits in two ways.

(i) A string of n digits can be obtained by appending a digit other than 0 to a valid string of $n - 1$ digits. This appending can be done in 9 ways. Therefore, a valid string of n digits can be obtained in this way in $9a_{n-1}$ ways.

(ii) Note that there are 10^{n-1} strings of length $n - 1$ and in this a_{n-1} are valid. Thus, we have $10^{n-1} - a_{n-1}$ invalid strings of length $n - 1$. Now, a valid string of n digits can be obtained by appending a 0 to an invalid string of length $n - 1$.

Thus, the number of valid strings of n digits obtained in this way is $10^{n-1} - a_{n-1}$.

Because all valid strings of length n are obtained in one of these two ways,

$$a_n = 9\, a_{n-1} + (10^{n-1} - a_{n-1})$$

i.e., $$a_n = 8\, a_{n-1} + 10^{n-1}$$

The recurrence relation of $\{a_n\}$ is $a_n = 8\, a_{n-1} + 10^{n-1}$ for $n \geq 2$ and $a_1 = 9$

Example 6: Solve the recurrence relation $\boldsymbol{a_n = c\, a_{n-1} + f(n)}$ for $\boldsymbol{n \geq 1}$ by iteration.

Solution: For $n \geq 1$, $a_n = c\, a_{n-1} + f(n)$

$$= c\big(c\, a_{n-2} + f(n-1)\big) + f(n) = c^2 a_{n-2} + c\, f(n-1) + f(n)$$

$$= c^2\, \big(c\, a_{n-3} + f(n-2)\big) + c\, f(n-1) + f(n)$$

$$= c^3\, a_{n-3} + c^2\, f(n-2) + c\, f(n-1) + f(n)$$

$$\ldots \qquad \ldots. \qquad \ldots.$$

$$= c^n\, a_{n-n} + c^{n-1}\, f\big(n-(n-1)\big) + c^{n-2}\, f\big(n-\ (n-2)\big) + \cdots + c\, f(n-1) + f(n)$$

$$= c^n\, a_0 + c^{n-1}\, f(1) + c^{n-2}\, f(2) + \cdots + c\, f\ (n-1) + f(n)$$

$$= c^n\, a_0 + \sum_{k=1}^{n} c^{n-k}\ f(k)$$

$$\therefore\ a_n = c^n\, a_0 + \sum_{k=1}^{n} c^{n-k}\ f(k)$$

Example 7: Show that $\{\boldsymbol{a_n}\}$ defined by $\boldsymbol{a_n = 4.2^n + 7.3^n}$ is a solution of the recurrence relation $\boldsymbol{a_n - 5\, a_{n-1} + 6\, a_{n-2} = 0}$

Solution: We have, $a_n = 4.2^n + 7\,.3^n$

$$a_{n-1} = 4.2^{n-1} + 7.3^{n-1}$$

$$a_{n-2} = 4.2^{n-2} + 7\,.3^{n-2}$$

Then $a_n - 5a_{n-1} + 6a_{n-2}$

$$= 4.2^n + 7.3^n - \ 5(4.2^{n-1} + 7.3^{n-1}) + 6(4.2^{n-2} + 7.3^{n-2})$$

$$= 4.2^{n-2}(2^2 - 5.2 + 6) + 7.3^{n-2}\,(3^2 - 5.3 + 6) = 0$$

Thus, $a_n = 4.2^n + 7.3^n$ is a solution of $a_n - 5a_{n-1} + 6 = 0$

Example 8: Find a recurrence relation for the sequence $\{a_n\}$ given by

$a_n = A.2^n + B(-3)^n$, where A, B are arbitrary constants.

Solution: The recurrence relation is obtained by eliminating A and B.

We have $a_n = A.2^n + B(-3)^n$ ... (1)

$a_{n-1} = A.2^{n-1} + B(-3)^{n-1}$ ... (2)

$a_{n-2} = A.2^{n-2} + B(-3)^{n-2}$ ... (3)

Multiplying (2) by 2 and subtracting from (1), we get

$$a_n - 2a_{n-1} = B(-3)^n - 2B(-3)^{n-1} = B(-3)^{n-1}(-3-2) = -5B(-3)^{n-1}$$

i.e., $a_n - 2a_{n-1} = -5B(-3)^{n-1}$ ... (4)

Replacing n by $n-1$ we get

$a_{n-1} - 2a_{n-2} = -5B(-3)^{n-2}$ ... (5)

From (4) we have $a_n - 2a_{n-1} = (-3)(-5B\,(-3)^{n-2})$

$= (-3)\,(a_{n-1} - 2\,a_{n-2})$ (from (5))

i.e., $a_n + 5a_{n-1} - 6a_{n-2} = 0$ is the required recurrence relation.

Example 9: A person climbs a stair case by climbing either (i) two steps in a single stride or (ii) only one step in a single stride. Find a recurrence relation for the number of ways climbing n stairs.

Solution: Let a_n denote the number of ways of climbing n stairs. In reaching n steps, the person can climb either one step or two steps in his last stride. For these two choices, the number of ways are a_{n-1} and a_{n-2} respectively.

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

Example 10: A factory makes custom sports cars at an increasing rate. In the first month only one car is made, in the second month two cars are made, and so on, with n cars made in the n^{th} month.

a) Set up a recurrence relation for the number of cars produced in the first n months by this factory.
b) Find an explicit formula for the number of cars produced in the first n months by this factory.

Solution:

(a) Let a_n be the total number of cars produced in n months. Initially $a_0 = 0$
The number of cars produced in the n^{th} month is $a_n - a_{n-1}$ and it is n.
Therefore, $a_n - a_{n-1} = n$

i.e., $a_n = a_{n-1} + n, \quad a_0 = 0$ is the recurrence relation.

(b) Now, $a_n = a_{n-1} + n$

$$= a_{n-2} + (n-1) + n$$
$$= a_{n-3} + (n-2) + (n-1) + n$$
$$\cdots \quad \cdots \quad \cdots$$
$$= a_0 + \big(n - (n-1)\big) + \cdots + (n-2) + (n-1) + n$$
$$= a_0 + 1 + 2 + \cdots + n = \frac{n\,(n+1)}{2} \qquad (\because \quad a_0 = 0)$$

4.4. Recurrence Relations

EXERCISES:

1. Is the sequence $\{a_n\}$ a solution of the recurrence relation $a_n = 8a_{n-1} - 16a_{n-2}$ if
   a) $a_n = 0$? b) $a_n = 1$? c) $a_n = 2^n$?
   d) $a_n = 4^n$? e) $a_n = n4^n$? e) $a_n = 2.4^n + 3\,n\,4^n$?
   f) $a_n = (-4^n)$? g) $a_n = n^2 4^n$?

2. Show that the sequence $\{a_n\}$ is a solution of the recurrence relation
   $a_n = a_{n-1} + 2a_{n-2} + 2n - 9$ if
   a) $a_n = -n + 2$ b) $a_n = 5(-1)^n - n + 2$
   c) $a_n = 3(-1)^n + 2^n - n + 2$ d) $a_n = 7.2^n - n + 2$

3. Find the solution to each of these recurrence relations and initial conditions. Use an iterative approach such as that used in example 5.
   a) $a_n = 3\,a_{n-1},\ \ a_0 = 2$ b) $a_n = a_{n-1} + 2,\ \ a_0 = 3$
   c) $a_n = a_{n-1} + n,\ \ a_0 = 1$ d) $a_n = a_{n-1} + 2n,\ \ 3a_0 = 4$
   e) $a_n = 2a_{n-1} - 1,\ \ a_0 = 1$ f) $a_n = 3a_{n-1} + 1,\ \ a_0 = 1$
   g) $a_n = na_{n-1},\ \ a_0 = 5$ h) $a_n = 2n\,a_{n-1},\ \ a_0 = 1$

4. A person deposits $Rs.1000$ in an account that yields 9% interest compounded annually.
   a) Set up a recurrence relation for the amount in the account at the end of n years.
   b) Find an explicit formula for the amount in the account at the end of n years
   c) How much money will the account contain after 100 years?

5.

a) Find a recurrence relation for the number of permutations of a set with n elements.
b) Use this recurrence relation to find the number of permutations of a set with n elements using iteration.

·

MODULE-5

Linear Recurrence relations

4.5

Linear Recurrence relations

A wide variety of recurrence relations occur in models. Some of these recurrence relations can be solved using iteration or some other **adhoc** technique. However, one important class of recurrence relations can be explicitly solved in a systematic way. These are recurrence relations that express terms of a sequence as linear combination of previous terms.

Linear homogeneous recurrence relation of degree k

A linear homogeneous recurrence relation of degree k is a recurrence relation of the form

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},}$$

where $c_1, c_2, \dots, c_k$ are real numbers and $c_k \neq 0$.

A recurrence relation is ***linear*** if a_n is the sum of previous terms of the sequence each multiplied by a function of n. The recurrence relation is ***homogeneous*** because no terms occur that are not multiples of the a_js. The coefficients of the terms of the sequence are all ***constants*** rather than functions n. The **degree** is k because a_n is expressed in terms of the previous k terms of the sequence.

Example 1: The recurrence relation $P_n = (1.11)P_{n-1}$ is a linear homogeneous recurrence relation of degree one. The recurrence relation $f_n = f_{n-1} + f_{n-2}$ is a linear homogeneous recurrence relation of degree two. The recurrence relation $a_n = a_{n-1} + a_{n-2}^2$ is not linear. The recurrence relation $H_n = 2H_{n-1} + 1$ is not homogeneous.

Note: A sequence $\{a_n\}$ satisfying the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

where $c_1, c_2, \dots, c_k$ are real constants, is uniquely determined whenever k initial conditions $a_0 = c_0, a_1 = c_1, \dots, a_{k-1} = c_{k-1}$ are given.

Solving linear homogeneous recurrence relations with constant coefficients

Lemma 1: ***A sequence $\{a_n\}$ defined by $a_n = r^n$ is a solution of the linear homogeneous recurrence relation of degree k with constant coefficients***

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \qquad \dots (1)$$

if and only if r is a solution of the equation

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k = 0 \qquad \dots (2)$$

Proof: A sequence $\{a_n\}$ defined by $a_n = r^n$ is a solution of equation (1) if and only if it satisfies equation (1), *i.e.,*

$$r^n - c_1 r^{n-1} - c_2 r^{n-2} - \cdots - c_{k-1} r^{n-k+1} - c_k r^{n-k} = 0$$

Because, we are looking for nonzero solutions, $r \neq 0$, cancelling r^{n-k} on both sides, we get

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r - c_k = 0 \qquad \dots (3)$$

Thus, $a_n = r^n$ is a solution of equation (1) if and only if r is a solution of equation (3).

Hence the result

The equation (3) is called the ***characteristic equation*** of the recurrence relation (1) and the roots of the equation (3) are called ***characteristic roots*** of the recurrence relation (1).

We now consider linear homogeneous recurrence relation of degree two. We consider the case when there are two distinct characteristic roots.

Theorem 1: ***Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution of the recurrence relation***

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} \qquad \dots (1)$$

if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$, $n = 0, 1, 2, \ldots$, where α_1 and α_2 are constants.

Proof: We have that r_1 and r_2 are the distinct roots of the equation $r^2 - c_1 r - c_2 = 0$, where c_1 and c_2 are real numbers. Therefore, $r_i^2 = c_1 r_i + c_2, \;\; i = 1, 2$.

Let $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$, where α_1 and α_2 are constants. Then

$$
\begin{aligned}
c_1 a_{n-1} + c_2 a_{n-2} &= c_1(\alpha_1 r_1^{n-1} + \alpha_2 r_2^{n-1}) + c_2(\alpha_1 r_1^{n-2} + \alpha_2 r_2^{n-2}) \\
&= \alpha_1 r_1^{n-2}(c_1 r_1 + c_2) + \alpha_2 r_2^{n-2}(c_1 r_2 + c_2) \\
&= \alpha_1 r_1^{n-2}.r_1^2 + \alpha_2 r_2^{n-2}.r_2^2 = \alpha_1 r_1^n + \alpha_2 r_2^n = a_n
\end{aligned}
$$

This shows that the sequence $\{a_n\}$, where $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$

Conversely, suppose that the sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1\, a_{n-1} + c_2\, a_{n-2}$.

Let $a_0 = k_0$ and $a_1 = k_1$ be the initial conditions of the recurrence relation.

We will now show that there are constants α_1 and α_2 such that the sequence $\{a_n\}$ with $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ satisfies these initial conditions.

This requires that $k_0 = a_0 = \alpha_1 + \alpha_2 \;\; ; \;\; k_1 = a_1 = \alpha_1 r_1 + \alpha_2 r_2$

Now, $\alpha_2 = k_0 - \alpha_1$ and so $k_1 = \alpha_1 r_1 + (k_0 - \alpha_1) r_2 \Longrightarrow k_1 = \alpha_1(r_1 - r_2) + k_0$

This shows that $\alpha_1 = \frac{k_1 - k_0 r_2}{r_1 - r_2}$, $(r_1 \neq r_2)$ and $\alpha_2 = k_0 - \alpha_1 = \frac{k_0 r_1 - k_1}{r_1 - r_2}$

Therefore, with these values of α_1 and α_2, the sequence $\{a_n\}$ with $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ satisfy the two initial conditions.

Now, $\{a_n\}$ and $\{\alpha_1 r_1^n + \alpha_2 r_2^n\}$ are both solutions of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, when $n = 0$ and $n = 1$. It is known that a sequence satisfying the recurrence relation is uniquely determined by initial conditions.

Therefore, a_n must be equal to $\alpha_1 r_1^n + \alpha_2 r_2^n$, for all nonnegative integers n.

Thus, a solution of equation (1) must be of the form $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$, where α_1 and α_2 are constants. Hence the theorem

Example 2: Find the solution of the recurrence relation $\boldsymbol{a_n = a_{n-1} + 2a_{n-2}}$ with $\boldsymbol{a_0 = 2}$ and $\boldsymbol{a_1 = 7}$?

Solution: The given recurrence relation is $a_n = a_{n-1} + 2a_{n-2}$

This is a linear homogeneous recurrence relation with constant coefficients of degree two. The characteristic equation is

$$r^2 = r + 2, \textit{i.e.,}\ r^2 - r - 2 = 0 \Longrightarrow (r+1)(r-2) = 0$$

The characteristic roots are $r = -1$ and $r = 2$.

Therefore, the sequence $\{a_n\}$ is a solution to the recurrence relation iff

$$a_n = \alpha_1(-1)^n + \alpha_2 2^n, \text{ where } \alpha_1 \text{ and } \alpha_2 \text{ are constants.}$$

The given initial conditions are $a_0 = 2$ and $a_1 = 7$

$$\textit{i.e.,}\ a_0 = 2 = \alpha_1 + \alpha_2\,,\ \ a_1 = 7 = -\alpha_1 + 2\alpha_2.$$

Solving for α_1, α_2 , we get $\alpha_1 = -1$ and $\alpha_2 = 3$.

The required solution is $a_n = -(-1)^n + 3.2^n$,*i.e.,* $a_n = (-1)^{n+1} + 3.2^n$, for all nonnegative integers n.

Fibonacci sequence: The sequence of Fibonacci numbers are:
$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots, \ldots.$ and they satisfy the recurrence relation:
$f_n = f_{n-1} + f_{n-2},\ n \geq 2$, with initial conditions $f_0 = 0$ and $f_1 = 1$.

Example 3: Find an explicit formula for the Fibonacci numbers.

Solution: The sequence of Fibonacci numbers satisfies the recurrence relation

$$f_n = f_{n-1} + f_{n-2},\ \ n \geq 2,\ \ f_0 = 0 \text{ and } f_1 = 1.$$

This is a linear homogenous recurrence relation with constant coefficients of degree two. Its characteristic equation is $r^2 = r + 1$, *i.e.,* $r^2 - r - 1 = 0$. Solving for r we get, $= \frac{1 \pm \sqrt{5}}{2}$. The characteristic roots are $r_1 = \frac{1+\sqrt{5}}{2}$ and $r_2 = \frac{1-\sqrt{5}}{2}$.
Therefore, the sequence $\{f_n\}$ is a solution of the recurrence relation iff

$f_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$, where α_1 and α_2 are constants.

To find α_1 and α_2, we use the initial conditions $f_0 = 0$ and $f_1 = 1$.

$$f_0 = 0 = \alpha_1 + \alpha_2 \quad ; \quad f_1 = 1 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)$$

Solving we get, $\alpha_1 = \frac{1}{\sqrt{5}}, \ \ \alpha_2 = -\frac{1}{\sqrt{5}}$.

Thus, the solution for the given recurrence relation is

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

Therefore, the Fibonacci numbers are given by

$$\boldsymbol{f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n}$$

for all nonnegative integers n

Note: Theorem 1 is not applicable when there is one characteristic root of multiplicity two. If r_0 is a root of multiplicity two of the characteristic equation then nr_0^n is another solution besides r_0^n. The following theorem shows this case.

Theorem 2: ***Let c_1 and c_2 be real numbers with $c_2 \neq 0$. Suppose that $r^2 - c_1 r - c_2 = 0$ has only one root r_0. A sequence $\{a_n\}$ is a solution of the recurrence relation***

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2}}$$

if and only if

$$\boldsymbol{a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n,}$$

for all nonnegative integers n, where α_1 and α_2 are constants.

Example 4: Find the solution of the recurrence relation

$$\boldsymbol{a_n = 6a_{n-1} - 9a_{n-2}, \quad a_0 = 1, \ a_1 = 6.}$$

Solution: The given recurrence relation is a linear homogenous recurrence relation with constant coefficients of degree two. Its characteristic equation is

$r^2 = 6r - 9,\ i.e.,\ r^2 - 6r + 9 = 0 \Longrightarrow (r-3)^2 = 0.$ The characteristic root 3 and its multiplicity is 2. Therefore, the solution of the given recurrence relation is

$$a_n = \alpha_1 3^n + \alpha_2 n 3^n \text{ , where } \alpha_1 \text{ and } \alpha_2 \text{ are constants.}$$

To evaluate α_1 and α_2 we use the initial conditions.

Take $n = 0,\ a_0 = 1 = \alpha_1$ and take $n = 1, a_1 = 6 = 3\alpha_1 + 3\alpha_2$

Solving, we get $\alpha_1 = 1$ and $\alpha_2 = 1$. Thus, the solution of the given recurrence relation with the initial conditions is $a_n = 3^n + n3^n$, for all nonnegative integers n

The following are general result when the roots are distinct.

Theorem 3: ***Let $c_1, c_2, \dots, c_k$ be real numbers. Suppose that the characteristic equation $r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$ has k distinct roots $r_1, r_2, \dots, r_k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation***

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} \quad , \ c_k \neq 0}$$

if and only

$$\boldsymbol{a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n ,}$$

for $n = 0, 1, 2, \dots$, where $\alpha_1, \alpha_2, \dots, \alpha_k$ are constants.

Example 5: Find the solution of the recurrence relation

$$\boldsymbol{a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}}$$

with the initial conditions $a_0 = 2, a_1 = 5$ and $a_2 = 15$

Solution: The given recurrence relation is a linear homogenous recurrence relation of degree 3 with constant coefficients. The characteristic equation is

$$r^3 = 6r^2 - 11r + 6 \text{ , } i.e., \ r^3 - 6r^2 + 11r - 6 = 0$$

Notice that $r = 1$ satisfies the characteristic equation and so $r - 1$ is a factor. Then$(r-1)(r^2-5r+6) = 0$ and $(r-1)(r-2)(r-3) = 0$.

The characteristic roots are $r = 1, 2, 3$ and they are all distinct. Therefore, the solutions to this recurrence relation are of the form

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

To find the constants α_1, α_2 and α_3 we use the initial conditions.

$$a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3$$

$$a_1 = 5 = \alpha_1 + 2\alpha_2 + 3\alpha_3$$

$$a_2 = 15 = \alpha_1 + 4\alpha_2 + 9\alpha_3$$

Solving these simultaneous equations we get, $\alpha_1 = 1, \alpha_2 = -1$ and $\alpha_3 = 2$. Therefore, the unique solution to the given recurrence relation and the given initial conditions is the sequence $\{a_n\}$ with

$$a_n = 1 - 2^n + 2.3^n$$

for all nonnegative integers n

The following is the most general result related to linear homogenous recurrence relation with constant coefficients, *allowing the characteristic equation to have multiple roots.*

For each root r of multiplicity m of the characteristic equation, the general solution has a summand of the form $P(n)r^n$, where $P(n)$ is a polynomial of degree $m - 1$.

Theorem 4: ***Let $c_1, c_2, \dots, c_k$ be real numbers. Suppose that the characteristic equation***

$$r^k - c_1r^{k-1} - c_2r^{k-2} - \cdots - c_kr^k = 0$$

has t disticnt roots $r_1, r_2, \dots, r_t$ with multiplicities $m_1, m_2, \dots, m_t$ respectively, so that $m_i \geq 1$ for $i = 1, 2, \dots, t$ and $m_1 + m_2 + \cdots + m_t = k$.

Then a sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

if and only if

$$a_n = (\alpha_{1,0} + \alpha_{1,1}\, n + \alpha_{1,2}\, n^2 + \cdots + \alpha_{1,m_1-1}\, n^{m_1-1}) r_1^n$$
$$+(\alpha_{2,0} + \alpha_{2,1}\, n + \alpha_{2,2}\, n^2 + \cdots + \alpha_{2,m_2-1}\, n^{m_2-1}) r_2^n$$
$$+ \cdots + (\alpha_{t,0} + \alpha_{t,1} n + \alpha_{t,2} n^2 + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n$$

***for** $n = 0, 1, 2, \ldots, \ldots$, **where** $\alpha_{i,0}$ **are constants for** $1 \le i \le t$ **and** $0 \le j \le m_i - 1$.*

Example 6: Suppose that the roots of the characteristic equation of linear homogenous recurrence relation of degree 6 with constant coefficients are $2, 2, 2, 5, 5$ and 9. What is the form of the general solution?

Solution: Given that there are three roots. The root 2 with multiplicity three, the root 5 with multiplicity two and the root 9 with multiplicity one. Therefore, the general solution is of the form

$a_n = (\alpha_{1,0} + \alpha_{1,1}\, n + \alpha_{1,2}\, n^2) 2^n + (\alpha_{2,0} + \alpha_{2,1}\, n) 5^n + \alpha_{3,0}\, 9^n$, for $n = 0, 1, 2, \ldots$

Example 7: Find the solution to the recurrence relation

$$a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$$

with initial conditions $a_0 = 1, a_1 = -2$, and $a_2 = -1$.

Solution: The given recurrence relation is a linear homogenous recurrence relation of degree 3 with constant coefficients. The characteristic equation is

$$r^3 = -3r^2 - 3r - 1$$

i.e., $r^3 + 3r^2 + 3r + 1 = 0$, *i.e.*, $(r + 1)^3 = 0$ and $r = (-1)$ (repeated thrice). Thus, the characteristic equation has only one root $r = -1$ with multiplicity three. The solutions of the given recurrence relation is of the form

$$a_n = (\alpha + \beta n + r n^2)(-1)^n$$

where α, β and γ are constants. We evaluate α, β and γ using the initial conditions.

Taking $n = 0$; $a_0 = 1 = \alpha$

Taking $n = 1$; $a_1 = -2 = -\alpha - \beta - \gamma$

Taking $n = 2$; $a_2 = -1 = \alpha + 2\beta + 4\gamma$

Solving the above three simultaneous equations we get,

$$\alpha = 1, \beta = 3 \text{ and } \gamma = -2$$

Therefore, the unique solution to the given recurrence relation with the given initial conditions is the sequence $\{a_n\}$, where $a_n = (1 + 3n - 2n^2)(-1)^n$.

Linear Nonhomogeneous Recurrence Relations with Constants Coefficients

Consider a *linear nonhomogeneous recurrence relation with constant coefficients* of the form

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),}$$

where $c_1, c_2, \dots, c_k$ are real numbers and $F(n)$ is a function, not identically zero, depending only on n.

The recurrence relation

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}}$$

is called the ***associated homogenous recurrence relation***.

Example 8: Each of the recurrence relations

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

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

$$a_n = 3a_{n-1} + n3^n$$

and $$a_n = a_{n-1} + a_{n-2} + a_{n-3} + n!$$

is a linear nonhomogeneous recurrence relation with constant coefficients. The associated homogeneous recurrence relations are

$a_n = a_{n-1}$, $a_n = a_{n-1} + a_{n-2}$, $a_n = 3a_{n-1}$ and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ respectively.

The key fact about linear nonhomogeneous recurrence relation with constant coefficients is that ***every solution is the sum a solution of the associated linear homogeneous recurrence relation and particular solution***.

Theorem 5: ***If*** $\left\{a_n^{(p)}\right\}$ ***is a particular solution of the linear nonhomogeneous recurrence relation with constant coefficients***

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)} \quad \ldots (1)$$

then every solution of (1) ***is of the form*** $\{a_n{}^{(p)} + a_n{}^{(h)}\}$***, where*** $a_n{}^{(h)}$ ***is a solution of the associated homogeneous recurrence relation***

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}} \ldots \quad \ldots (2)$$

Proof: Because $a_n^{(p)}$ is a particular solution of (1),

$$a_n^{(p)} = c_1 a_{n-1}^{(p)} + c_2 a_{n-2}^{(p)} + \cdots + c_k a_{n-k}^{(p)} + F(n) \quad \ldots (3)$$

Suppose that $\{b_n\}$ be any solution of (1). Then

$$b_n = c_1 b_{n-1} + c_2 b_{n-2} + \cdots + c_k b_{n-k} + F(n) \quad \ldots (4)$$

Subtracting (3) from (4), we get

$$b_n - a_n^{(p)} = c_1\left(b_{n-1} - a_{n-1}^{(p)}\right) + c_2\left(b_{n-2} - a_{n-2}^{(p)}\right) + \cdots + c_k\left(b_{n-k} - a_{n-k}^{(p)}\right)$$

This shows that $\left\{b_n - a_n^{(p)}\right\}$ is a solution of (2), say $a_n^{(h)}$.

That is $a_n^{(h)}$ is a solution of the associated homogeneous linear equation.
Consequently, $b_n - a_n^{(p)} = a_n^{(h)}$ *i.e.*, $b_n = a_n^{(h)} + a_n^{(p)}$

Hence the theorem

Note: We see that the key to solving (1) is finding a particular solution. Then every solution is a sum of this particular solution and a solution of (2). Although there is no general method for finding such a particular solution that works for every function $F(n)$, there are techniques that work for certain types of functions of $F(n)$, such as polynomials and powers of constants. The following is a related theorem:

Theorem 6: ***Suppose that $\{a_n\}$ satisfies the linear nonhomogeneous recurrence relation***

$$\boldsymbol{a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),} \qquad \ldots (1)$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and

$$\boldsymbol{F(n) = (b_0 + b_1 n + b_2 n^2 + \cdots + b_t n^t) s^n}$$

where $b_0, b_1, \ldots, b_t$ and s are real numbers.

(i) When s is not a root of the characterstic equation of the associated homogenous recurrence relation, there is a particular solution of (1) of the form

$$\boldsymbol{(p_0 + p_1 n + p_2 n^2 + \cdots + p_t n^t) s^n}$$

(ii) When s is a root of the characterstic equation and its multiplicity is m, there is a particular solution of (1) of the form

$$\boldsymbol{n^m (p_0 + p_1 n + p_2 n^2 + \cdots + p_t n^t) s^n}$$

Remark: Care must be taken when $s = 1$, in particular when

$$F(n) = b_0 + b_1 n + b_2 n^2 + \cdots + b_t n^t,$$

then the parameter s takes the value $s = 1$.

Example 9: a) Find all solutions of the recurrence relation $\boldsymbol{a_n = 2a_{n-1} + 3^n}$

b) Find the solution of the recurrence relation with initial condition $\boldsymbol{a_1 = 5}$

Solution: a) We have $a_n = 2a_{n-1} + 3^n$

It is a linear nonhomogeneous recurrence relation with constant coefficients. The associated homogeneous recurrence relation for a_n is

$$a_n = 2a_{n-1}$$

The characteristic equation is $r = 2$ and the characteristic root is 2.

Therefore, $a_n^{(h)} = \alpha.2^n$, where α is a constant.

We have $F(n) = 3^n$. Note that 3 is not a characteristic root. Therefore

$$a_n^{(p)} = p.3^n$$

Substituting in the given recurrence relation we get

$$p.3^n = 2.p.3^{n-1} + 3^n$$

$\Longrightarrow\ (p-1)3^n = 2p3^{n-1}\ \ \Longrightarrow 3(p-1) = 2p\ \Longrightarrow p = 3$

Thus, $a_n^{(p)} = 3.3^n = 3^{n+1}$

The general solution of the given recurrence relation is

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha.2^n + 3^{n+1}$$

b) To obtain α we use the initial condition

Taking $n = 1$; $a_1 = 5 = \alpha.2 + 3^2 \Longrightarrow 2\alpha = -4\ \Longrightarrow\ \alpha = -2.$

$\therefore$ The solution of the given recurrence relation with the given initial condition is

$$a_n = (-2).2^n + 3^{n+1} \quad \textit{i.e.,} \quad a_n = -2^{n+1} + 3^{n+1}$$

Example 10: Find all solutions of the recurrence relation

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

Solution: We have $a_n = 4a_{n-1} - 4a_{n-2} + (n+1)2^n$

It is a linear homogeneous recurrence relation with constant coefficients. The associated homogeneous recurrence relation is

$$a_n = 4a_{n-1} - 4a_{n-2}$$

The characteristic equation is $r^2 = 4a - 4$ *i.e.,* $(r-2)^2 = 0 \quad \Longrightarrow r = 2$ (twice)

Note that the characteristic root 2 has multiplicity 2.

Therefore, $a_n = (\alpha_1 + \alpha_2 n).2^n$, where α is a constant.

We have $F(n) = (n+1)2^n$.

Because 2 is a characterstic root with multiplicity $m = 2$ and $F(n) = (n+1)2^n$,

$$a_n^{(p)} = n^m(p_0 + p_1 n)2^n = n^2(p_0 + p_1 n)2^n = (p_0 n^2 + p_1 n^3)2^n$$

Substituting in the given recurrence relation we get

$$(p_0 n^2 + p_1 n^3)2^n = 4(p_0(n-1)^2 + p_1(n-1)^3)2^{n-1}$$
$$-4[p_0(n-2)^2 + p_1(n-2)^3]2^{n-2} + (n+1)2^n$$

$$\Longrightarrow\ p_0 n^2 + p_1 n^3 = 2p_0(n-1)^2 + 2p_1(n-1)^3 - p_0(n-2)^2 - p_1(n-2)^3 + n + 1$$

$$\Longrightarrow\ p_0 n^2 + p_1 n^3 = 2p_0(n^2 - 2n + 1) + 2p_1(n^3 - 3n - 1) - p_0(n^2 - 4n + 4)$$
$$-p_1(n^3 - 6n^2 + 12n - 8) + n + 1$$

Equating the coefficients of n^2 on both sides, we get

$$\Longrightarrow\ 0 = (-6p_1 + 1)n + (6p_1 - 2p_0 + 1)$$

$$\Longrightarrow\ -6p_1 + 1 = 0,\ \ 6p_1 - 2p_0 + 1 = 0$$

$$\Longrightarrow\ p_1 = \tfrac{1}{6},\ \ p_0 = 1$$

Therefore, $a_n^{(p)} = (p_0 n^2 + p_1 n^3)2^n = \left(n^2 + \frac{n^3}{6}\right)2^n$

The general solution of the given recurrence relation is

$$a_n = a_n^{(h)} + a_n^{(p)} = (\alpha_1 + \alpha_2 n)2^n + \left(n^3 + \frac{n^3}{6}\right)2^n$$

i.e., $a_n = \left(\alpha_1 + \alpha_2 n + n^2 + \frac{n^3}{6}\right)2^n$, where α_1 and α_2 are constants.

Example 11: Find the solution of the recurrence relation

$$\boldsymbol{a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3}, \textbf{ with } \boldsymbol{a_0 = 1} \textbf{ and } \boldsymbol{a_1 = 4}$$

Solution: The given recurrence relation

$$a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3$$

is a linear nonhomogeneous recurrence relation with constant coefficients. The associated homogeneous recurrence relation is

$$a_n = 4a_{n-1} - 3a_{n-2}$$

The characteristic equation is $r^2 = 4r - 3$,

i.e., $(r-1)(r-3) = 0$, *i.e.,* the characteristic roots are $r = 1$ and 3.

Therefore, $a_n^{(h)} = \alpha.1^n + \beta.3^n = \alpha + \beta.3^n$, where α and β are constants.

We have $F(n) = 2^n + n + 3$. Notice that 2 is not a characteristic root and 1 is a characteristic root of multiplicity $m = 1$. Therefore,

$$a_n^{(p)} = p.2^n + n^m\,(q + rn)1^n = p.2^n + n(q + rn)$$

$$= p.2^n + qn + rn^2$$

Substituting in the given recurrence relation we get,

$$p.2^n + qn + rn^2$$

$$= 4(p.2^{n-1} + q(n-1) + r(n-1)^2) - 3(p.2^{n-2} + q(n-2) + r(n-2)^2) + 2^n + n + 3$$

Equating the coefficient of 2^n on both sides, we get

$$p = p - \frac{3}{4}p + 1 \Longrightarrow p = -4$$

Equating the coefficient of n on both sides, we get

$$q = 4q - 8r - 3q + 12r + 1 \;\; \Longrightarrow 4r + 1 = 0 \;\; \Longrightarrow r = -\frac{1}{4}$$

Equating the constant terms on both sides we get

$$0 = -4q + 4r + 6q - 12r + 3 \;\; \Longrightarrow 2q - 8r = -3 \Longrightarrow q = -\frac{5}{2}$$

Thus, $a_n^{(p)} = -4.2^n + \frac{5}{2}n - \frac{n^2}{4}$

The general solution of the given recurrence equation is

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha + \beta.3^n - 4.2^n - \frac{5}{2}n - \frac{n^2}{4},$$

where α and β are constants. To evaluate α and β we use the initial conditions.

Taking $n = 0,\ a_0 = 1 = \alpha + \beta - 4$

Taking $n = 1,\ a_1 = 4\ = \alpha + 3\beta - 8 - \frac{5}{2} - \frac{1}{4}$

$\Longrightarrow\ \ \alpha + \beta = 5$ and $\alpha + 3\beta = \frac{59}{4}$

Solving the equations, we get $\alpha = \frac{1}{8}$ and $\beta = \frac{39}{8}$

The unique solution of the given recurrence relation is

$$a_n = \frac{1}{8} + \frac{39}{8}.3^n - 4.2^n - \frac{5}{2}n - \frac{n^2}{4}, \text{ for all nonnegative integers } n$$

P1:

Find the solution of the recurrence relation $a_n = 2a_{n-1} + 3a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$?

Solution: The given recurrence relation is $a_n = 2a_{n-1} + 3a_{n-2}$

This is a linear homogeneous recurrence relation with constant coefficients of degree two. The characteristic equation is

$$r^2 = 2r + 3, \textit{i.e.,}\ r^2 - 2r - 3 = 0 \Longrightarrow (r+1)(r-3) = 0$$

The characteristic roots are $r = -1$ and $r = 3$.

Therefore, the sequence $\{a_n\}$ is a solution to the recurrence relation iff

$$a_n = \alpha_1(-1)^n + \alpha_2 3^n, \text{ where } \alpha_1 \text{ and } \alpha_2 \text{ are constants.}$$

The given initial conditions are $a_0 = 0$ and $a_1 = 1$

$$\textit{i.e.,}\ a_0 = 0 = \alpha_1 + \alpha_2\,,\ a_1 = 1 = -\alpha_1 + 3\alpha_2.$$

Solving for α_1, α_2 , we get $\alpha_1 = -\frac{1}{4}$ and $\alpha_2 = \frac{1}{4}$.

The required solution is $a_n = -\frac{1}{4}(-1)^n + \frac{1}{4}.3^n$

$$\textit{i.e.,}\ a_n = (-1)^{n+1}\frac{1}{4} + \frac{1}{4}3^n, \text{ for all nonnegative integers } n.$$

P2:

Find the solution of the recurrence relation $\boldsymbol{a_n = -7a_{n-1} - 10a_{n-2}}$ with $\boldsymbol{a_0 = 3}$ and $\boldsymbol{a_1 = 3}$?

Solution: The given recurrence relation is $a_n = -7a_{n-1} - 10a_{n-2}$

This is a linear homogeneous recurrence relation with constant coefficients of degree two. The characteristic equation is

$$r^2 = -7r - 10, \textit{i.e.}, r^2 + 7r + 10 = 0 \Longrightarrow (r+5)(r+2) = 0$$

The characteristic roots are $r = -5$ and $r = -2$.

Therefore, the sequence $\{a_n\}$ is a solution to the recurrence relation iff

$$a_n = \alpha_1(-5)^n + \alpha_2(-2)^n, \text{ where } \alpha_1 \text{ and } \alpha_2 \text{ are constants.}$$

The given initial conditions are $a_0 = 3$ and $a_1 = 3$

$$\textit{i.e.}, a_0 = 3 = \alpha_1 + \alpha_2, \ a_1 = 3 = -5\alpha_1 - 2\alpha_2.$$

Solving for α_1, α_2 , we get $\alpha_1 = -3$ and $\alpha_2 = 6$.

The required solution is

$$a_n = -3(-5)^n + 6(-2)^n, \text{ for all nonnegative integers } n.$$

P3:

Find the solution of the recurrence relation $\boldsymbol{a_n = 10a_{n-1} - 25a_{n-2}}$ **with** $\boldsymbol{a_0 = 3,\ a_1 = 4.}$

Solution: The given recurrence relation is a linear homogenous recurrence relation is with constant coefficients of degree two. Its characteristic equation is

$$r^2 = 10r - 25,\ i.e.,\ r^2 - 10r + 25 = 0 \Longrightarrow (r-5)^2 = 0.$$

The characteristic root 5 and its multiplicity is 2. Therefore, the solution of the given recurrence relation is

$a_n = \alpha_1 5^n + \alpha_2 n\, 5^n$, where α_1 and α_2 are constants.

To evaluate α_1 and α_2 we use the initial conditions.

Take $n = 0,\ a_0 = 3 = \alpha_1$ and take $n = 1, a_1 = 4 = 5\alpha_1 + 5\alpha_2$

Solving, we get $\alpha_1 = 3$ and $\alpha_2 = -\frac{11}{5}$.

∴ The solution of the given recurrence relation with the given initial conditions is

$a_n = 3.5^n - \frac{11}{5}.n\, 5^n = \left(3 - \frac{11}{5}n\right) 5^n$, for all nonnegative integers n

P4:

Find the solution of the recurrence relation

$$\boldsymbol{a_n = 7a_{n-1} - 13a_{n-2} - 3a_{n-3} + 18a_{n-4}}\ ,$$

with $\boldsymbol{a_0 = 5},\ \boldsymbol{a_1 = 3, a_2 = 6}$ and $\boldsymbol{a_3 = -21}$

Solution: The given recurrence relation is a linear homogenous recurrence relation is with constant coefficients of degree 4. Its characteristic equation is

$$r^4 = 7r^3 - 13r^2 - 3r + 18$$

$$i.e.,\quad r^4 - 7r^3 + 13r^2 + 3r - 18 = 0 \Longrightarrow (r+1)(r-2)(r-3)^2 = 0.$$

The characteristic roots are: $-1, 2$ with multiplicity one, and 3 with multiplicity 2.

Therefore, the solution of the given recurrence relation is

$$a_n = \alpha_1(-1)^n + \alpha_2.2^n + \alpha_3.3^n + \alpha_4.n3^n\ ,$$

where $\alpha_1, \alpha_2, \alpha_3$ and α_4 are constants.

To evaluate $\alpha_1, \alpha_2, \alpha_3$ and α_4 we use the initial conditions.

Take $n = 0,\ a_0 = 5 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$

Take $n = 1, a_1 = 3 = -\alpha_1 + 2\alpha_2 + 3\alpha_3 + 3\alpha_4$

Take $n = 2, a_2 = 6 = \alpha_1 + 4\alpha_2 + 9\alpha_3 + 18\alpha_4$

Take $n = 3, a_3 = -21 = -\alpha_1 + 8\alpha_2 + 27\alpha_3 + 81\alpha_4$

Solving, we get $\alpha_1 = 2 = \alpha_3,\ \alpha_2 = 1$ and $\alpha_4 = -1$

$\therefore$ The solution of the given recurrence relation with the given initial conditions is

$$a_n = 2(-1)^n + 2^n + 2.3^n - n3^n$$, for all nonnegative integers n

P5:

Find the solution of the recurrence relation

$$\boldsymbol{a_n = 5a_{n-1} - 6a_{n-2} + 8n^2} \text{ **with initial conditions** } \boldsymbol{a_0 = 4} \text{ **and** } \boldsymbol{a_1 = 7}$$

Solution: We have $a_n = 5a_{n-1} - 6a_{n-2} + 8n^2$

It is a linear nonhomogeneous recurrence relation with constant coefficients. The associated homogeneous recurrence relation is

$$a_n = 5a_{n-1} - 6a_{n-2}$$

The characteristic equation is $r^2 = 5r - 6$ *i.e.,* $(r-2)(r-3) = 0 \Rightarrow r = 2, 3$ and the characteristic roots are $2, 3$.

Therefore, $a_n^{(h)} = \alpha_1 2^n + \alpha_2 3^n$, where α_1 and α_2 are constants.

We have $F(n) = 8n^2$. Notice that 1 is not a characteristic root.

Therefore, $a_n^{(p)} = p_0 + p_1 n + p_2 n^2$

Substituting in the given recurrence relation, we get

$$p_0 + p_1 n + p_2 n^2$$

$$= 5[p_0 + p_1(n-1) + p_2(n-1)^2] - 6[p_0 + p_1(n-2) + p_2(n-2)^2]$$

$$= (8 - p_2)n^2 + (14p_2 - p_1)n - 19p_2 + 7p_1 - p_0$$

Equating the coefficients of n^2 on both sides, we get

$$\Rightarrow\ p_2 = 8 - p_2 \Rightarrow p_2 = 4$$

Equating the coefficients of n on both sides, we get

$$\Rightarrow\ p_1 = 14p_2 - p_1 \Rightarrow p_1 = 28$$

Equating the constant terms on both sides, we get

$$\Rightarrow\ p_0 = -19p_2 + 7p_1 - p_0 \Rightarrow p_0 = 60$$

Therefore, $a_n^{(p)} = 4n^2 + 28n + 60$

The general solution of the given recurrence relation is

$$a_n = a_n^{(h)} + a_n^{(p)} = \alpha_1 2^n + \alpha_2\, 3^n + 4n^2 + 28n + 60,$$

where α_1 and α_2 are constants.

We evaluate α_1 and α_2 using the initial conditions $a_0 = 4$ and $a_1 = 7$.

Taking $n = 0$; $a_0 = 4 = \alpha_1 + \alpha_2 \ + 60 \Longrightarrow \alpha_1 + \alpha_2 = -56$

Taking $n = 1$; $a_1 = 7 = 2\alpha_1 + 3\alpha_2 \ + 4(1)^2 + 28(1) + 60 \Longrightarrow 2\alpha_1 + 3\alpha_2 = -85$

Solving the above equations, we get $\alpha_1 = -83$ and $\alpha_2 = 27$

Therefore, the unique solution to the given recurrence relation with the intial conditions $a_0 = 4$ and $a_1 = 7$ is

$$a_n = (-83)2^n + 27.3^n + 4n^2 + 28n + 60, \text{ for all nonnegative integers } n$$

P6:

Find all solutions of the recurrence relation

$$\boldsymbol{a_n = 6a_{n-1} - 9a_{n-2} + 4(n+1)3^n}.$$

Solution: We have $a_n = 6a_{n-1} - 9a_{n-2} + 4(n+1)3^n$

It is a linear nonhomogeneous recurrence relation with constant coefficients. The associated homogeneous recurrence relation is $a_n = 6a_{n-1} - 9a_{n-2}$

The characteristic equation is $r^2 = 6r - 9$ *i.e.,* $(r-3)^2 = 0 \quad \Longrightarrow r = 3$ (twice)

Note that the characteristic root 3 has multiplicity 2.

Therefore, $a_n = (\alpha_1 + \alpha_2 n)3^n$, where α is a constant.

We have $F(n) = 4(n+1)3^n$.

Because 3 is a characterstic root with multiplicity $m = 2$ and $F(n) = 4(n+1)3^n$,

$$a_n^{(p)} = n^m(p_0 + p_1 n)3^n = n^2(p_0 + p_1 n)3^n = (p_0 n^2 + p_1 n^3)3^n$$

Substitution in the given recurrence relation, we get

$$(p_0 n^2 + p_1 n^3)3^n = 6[p_0(n-1)^2 + p_1(n-1)^3]3^{n-1}$$
$$-9[p_0(n-2)^2 + p_1(n-2)^3]3^{n-2} + 4(n+1)3^n$$

$$\Longrightarrow \; p_0 n^2 + p_1 n^3 = 2p_0(n-1)^2 + 2p_1(n-1)^3 - p_0(n-2)^2 - p_1(n-2)^3 + 4n + 4$$

Equating the like terms on both sides and solving, we get

$\Longrightarrow \; p_0 = \frac{2}{3}, p_1 = 4$ (verify!)

Therefore, $a_n^{(p)} = (p_0 n^2 + p_1 n^3)3^n = \left(4n^2 + \frac{2n^3}{3}\right)3^n$

The general solution of the given recurrence relation is

$a_n = a_n^{(h)} + a_n^{(p)} = (\alpha_1 + \alpha_2 n)3^n + \left(4n^2 + \frac{2n^3}{3}\right)3^n$, where α_1 and α_2 are constants.

4.5. Recurrence relations

Exercises:

1. Solve the recurrence relation together with the initial conditions given.
   a. $a_n = 2a_{n-1}$ for $n \geq 1, , a_0 = 3$
   b. $a_n = a_{n-1}$for $n \geq 1, , a_0 = 2$
   c. $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2,\ a_0 = 1, a_1 = 0$
   d. $a_n = 4a_{n-1} - 4a_{n-2}$ for $n \geq 2,\ a_0 = 6, a_1 = 8$
   e. $a_n = -4a_{n-1} - 4a_{n-2}$ for $n \geq 2,\ a_0 = 0, a_1 = 1$
   f. $a_n = 4a_{n-2}$ for $n \geq 2, a_0 = 0, a_1 = 4$
   g. $a_n = \frac{a_{n-2}}{4}$ for $n \geq 2\ , a_0 = 1, a_1 = 0$
2. Find the solution to $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$ for $n = 3,4,5, \ldots$,

   with $a_0 = 3, a_1 = 6$ and $a_2 = 0$.
3. Find the solution to $a_n = 7a_{n-2} + 6a_{n-3}$ with $a_0 = 9, a_1 = 10$ and $a_2 = 32$.
4. Find the solution to $a_n = 5a_{n-2} - 4a_{n-4}$ with $a_0 = 3, a_1 = 2, a_2 = 6$

   and $a_3 = 8$.
5. Find the solution to $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$ with $a_0 = 7, a_1 = -4$

   and $a_2 = 8$.
6. Solve the recurrence relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with

   $a_0 = 5, a_1 = -9$ and $a_2 = 15$.
7. What is the general form of the solutions of a linear homogenous recurrence

   relation if its characteristic equation has roots $1,1,1,1,-2,-2,-2,3,3,-4$?

8. What is the general form of the particular solution guarantee to exist by Theorem 6 of the linear non homogeneous recurrence relation $a_n = 8a_{n-2} - 16a_{n-4} + F(n)$ if
   a. $F(n) = n^3$
   b. $F(n) = (-2)^n$
   c. $F(n) = n.2^n$
   d. $F(n) = n^2 4^n$
   e. $F(n) = (n^2 - 2)(-2)^n$
   f. $F(n) = n^4 2^n$
   g. $F(n) = 2$

9.
   a. Find all the solutions of the recurrence relation $a_n = 2a_{n-1} + 2n^2$
   b. Find the solutions of the recurrence relation in part(a) with the initial condition $a_1 = 4$.

10.
   a. Find all the solutions of the recurrence relation $a_n = -5a_{n-1} - 6a_{n-2} + 42.4^n$
   b. Find the solutions of this recurrence relation in with $a_1 = 56$ and $a_2 = 278$.

11. Find all solutions of the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2} + 2^n + 3n$. (Hint: Look for a particular solution of the form $qn2^n + p_1 n + p_2$, where q, p_1, p_2 are constants.
12. Find the solution of recurrence relation $a_n = 2a_{n-1} + 3.2^n$.
13. Find all solutions of the recurrence relation $a_n = 7a_{n-1} - 16a_{n-2} + 12a_{n-3} + n.4^n$.with $a_0 = -2, a_1 = 0$ and $a_2 = 5$.

.

MODULE-6

Generating functions

4.6

Generating Functions:

Generating function for a sequence: The **generating function** (or **ordinary generating function**) for the sequence $\{a_n\}_{n=0}^{\infty}, i.e., a_0, a_1, a_2, \dots, a_n, \dots$ of real number is the infinite series

$$\boldsymbol{G(x) = a_0 + a_1 x + a_2 x + \cdots + a_n x^n \dots} \qquad \dots (1)$$

$$\boldsymbol{i.e., G(x) = \sum_{n=0}^{\infty} a_n x^n}$$

Example 1: The generating functions for the sequences $\boldsymbol{\{a_n\}_{n=0}^{\infty}}$ with

i. $a_n = 3$, ii. $a_n = n + 1$ and iii. $a_n = 2^n$ are

Solution:

$$i. \sum_{n=0}^{\infty} 3x^n \quad , \quad ii. \sum_{n=0}^{\infty} (n+1) x^n \quad and \quad iii. \sum_{n=0}^{\infty} 2^n x^n$$

respectively.

Generating functions for a finite sequence:

Define the generating function of a finite sequence $a_0, a_1, a_2, \dots, a_n$ of real numbers by extending it by setting $a_k = 0$ for $k = n + 1, n + 2, \dots$.
The generating function of this infinite sequence $\{a_n\}_{n=0}^{\infty}$ is a polynomial of degree n, since no terms of the form $a_k x^k$ with $k > n$ ocuurs, $i.e.$,

$$G(x) = a_0 + a_1 x + a_2 x + \cdots + a_n x^n$$

Example 2: Write down the generating function for the finite sequence $\boldsymbol{1, 1, 1, 1, 1, 1}$.

Solution: The generating function for 1,1,1,1,1,1 is

$$G(x) = 1 + x + x^2 + x^3 + x^4 + x^5$$

Note that $\frac{x^6-1}{x-1} = 1 + x + x^2 + x^3 + x^4 + x^5$, when $x \neq 1$. Therefore, $G(x) = \frac{x^6-1}{x-1}$ is the generating function for the sequence 1,1,1,1,1,1.

Note: The RHS of the equation (1) is a formal power series in x. The letter x does not represent any thing. The various powers x^n of x are simply used to keep track of the corresponding terms a_n of the sequence. The convergence/divergence of the series is of no interest to us (at present).

Example 3: Let $\boldsymbol{m}$ be a positive integer and let $\boldsymbol{a_k} = {}^{m}C_k$, $\boldsymbol{k = 0, 1, 2, \dots, m}$. What is the generating function for the sequence $\boldsymbol{a_0, a_1, \dots a_m}$?

Solution: The generating function for the finite sequence $a_0, a_1, a_2, \dots, a_n$ is

$$G(x) = a_0 + a_1x + a_2x^2 + \dots + a_mx^m$$

$$= {}^{m}C_0 + {}^{m}C_1\,x + {}^{m}C_2\,x^2 +, \dots + {}^{m}C_m\,x^m$$

$$= (1 + x)^m$$

Example 4:

i. $f(x) = 1 + 2x + 3x^2 + \dots + (n+1)x^n + \cdots$ is the generating function for the sequence $\{n\}_{n=1}^{\infty}$ of positive integers.

ii. The function $g(x) = \frac{1}{1-x}$ is the generating function for the sequence 1,1,1, … since $\frac{1}{1-x} = 1 + x + x^2 + \cdots$ for $|x| < 1$.

iii. The function $h(x) = \frac{1}{1-ax}$ is the generating function for the sequence $1, a, a^2, a^3, \dots$,since $\frac{1}{1-ax} = 1 + ax + a^2x^2 + a^3x^3 + \cdots$ when $|ax| < 1$ or $|x| < \frac{1}{|a|}, a \neq 0$.

Equality of generating functions:

Two generating functions $f(x) = \sum_{n=0}^{\infty} a_n x^n$ and $g(x) = \sum_{n=0}^{\infty} b_n x^n$ are **equal** if $a_n = b_n \; \forall n = 0,1,2, \ldots$

Addition and Multiplication of generating functions:

Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ and $g(x) = \sum_{n=0}^{\infty} b_n x^n$ be two generating functions. Then

$$\boldsymbol{f(x) + g(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n}$$

$$\boldsymbol{f(x)g(x) = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j b_{n-j} \right) x^n}$$

Example 5: Let $f(x) = \frac{1}{(1-x)^2}$. Find the coefficients $a_0, a_1, a_2, \ldots$ in the expansion of $f(x) = \sum_{n=0}^{\infty} a_n x^n$.

Solution: We have $g(x) = \frac{1}{1-x} = 1 + x + x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n$

Now:

$$f(x) = \frac{1}{(1-x)^2} = \frac{1}{(1-x)} \cdot \frac{1}{(1-x)} = \left(\sum_{n=0}^{\infty} x^n \right) \left(\sum_{m=0}^{\infty} x^m \right)$$

$$= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} a_j b_{n-j} \right) x^n = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} 1.1 \right) x^n$$

$$= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} 1 \right) x^n = \sum_{n=0}^{\infty} (n+1) x^n \ \ (\because \sum_{j=0}^{n} 1 = n+1)$$

Therefore, the coefficients of $f(x)$ are $a_n = n+1, n = 0,1,2, \dots$

Extended binomial coefficients:

Let u be a real number and k be a nonnegative integer. Then the **extended binomial coefficients** $\binom{\boldsymbol{u}}{\boldsymbol{k}}$ is defined by

$$\binom{\boldsymbol{u}}{\boldsymbol{k}} = \begin{cases} \dfrac{\boldsymbol{u(u-1)(u-2)\dots(u-k+1)}}{\boldsymbol{k}!} & \boldsymbol{if\ k} > 0 \\ \boldsymbol{1} & \boldsymbol{if\ k \leq 0} \end{cases}$$

Example 6:

(i). $\binom{-2}{3} = \frac{(-2)(-2-1)(-2-2)}{3!} = \frac{(-2)(-3)(-4)}{3!} = -4$

(ii). $\binom{\frac{1}{2}}{4} = \frac{\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)\left(\frac{1}{2}-3\right)}{4!} = \frac{\left(\frac{1}{2}\right)\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\left(-\frac{5}{2}\right)}{4!} = -\frac{5}{128}$

The following is a useful formula for extended binomial coefficients when the top parameter is a negative integer. If the top parameter u is a negative integer then the extended binomial coefficient can be expressed in terms of an **ordinary binomial coefficient.**

Theorem 1: If n is a positive integer then

$$\binom{-\boldsymbol{n}}{\boldsymbol{r}} = (-\mathbf{1})^{\boldsymbol{r}}\ {}^{n+r-1}C_r$$

Proof:

$$\binom{-n}{r} = \frac{(-n)(-n-1)(-n-2)\ldots(-n-r+1)}{r!}$$

$$= (-1)^r \frac{n(n+1)(n+2)\ldots(n+r-1)}{r!}$$

$$= (-1)^r \frac{(n+r-1)(n+r-2)\ldots(n+1)n}{r!}$$

$$= (-1)^r \binom{n+r-1}{r}$$

$$= (-1)^r\ {}^{n+r-1}C_r$$

The extended binomial Theorem

Let x be a real number with $|x| < 1$ and let u be a real number. Then

$$(\mathbf{1}+\boldsymbol{x})^{\boldsymbol{u}} = \sum_{\boldsymbol{k}=\mathbf{0}}^{\infty} \binom{\boldsymbol{u}}{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$$

Remark: If u is a positive integer, the extended Binomial Theorem reduces to Binomial Theorem, (since $\binom{u}{k} = 0$ if $k > u$).

Example 7: Find the generating functions for $(\mathbf{1}+\boldsymbol{x})^{-\boldsymbol{n}}$ and $(\mathbf{1}-\boldsymbol{x})^{-\boldsymbol{n}}$ where $\boldsymbol{n}$ is a positive integer, using the extended Binomial theorem.

Solution: By the extended Binomial Theorem, we have

$$(1+x)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} x^k$$

$$= \sum_{k=0}^{\infty} (-1)^k \, {}^{(n+k-1)}C_k \; x^k$$

Thus, the generating function for $(1+x)^{-n}$ is

$$\sum_{k=0}^{\infty} (-1)^k \, {}^{(n+k-1)}C_k \; x^k$$

Replacing x by $-x$, we get the generating function for $(1-x)^n$. It is given by

$$\sum_{k=0}^{\infty} (-1)^k \, {}^{(n+k-1)}C_k \; (-x)^k = \sum_{k=0}^{\infty} {}^{(n+k-1)}C_k \; x^k$$

Summary of some generating functions for certain sequences

$\boldsymbol{a_k}$	$\boldsymbol{G(x)}$ **:Generating for the sequence** $\{\boldsymbol{a_k}\}_{\boldsymbol{k=0}}^{\infty}$
$\frac{1}{k!}$	$\sum_{k=0}^{\infty} \frac{x^n}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = e^x$
$\frac{(-1)^{k+1}}{k}$	$\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k!} x^k = x - \frac{x^2}{2!} + \frac{x^3}{3!} - \cdots = ln(1+x)$
1	$\sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots = \frac{1}{1-x}$
a^k	$\sum_{k=0}^{\infty} a^k x^k = 1 + ax + (ax)^2 + \cdots = \frac{1}{1-ax}$
1 if $r\|k$; 0 otherwise	$\sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots = \frac{1}{1-x^r}$
$k+1$	$\sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots = \frac{1}{(1-x)^2}$
${}^{(n+k-1)}C_k$	$\sum_{k=0}^{\infty} {}^{(n+k-1)}C_k \, x^k = 1 + {}^{n}C_1 \, x + {}^{(n+1)}C_2 \, x^2 + \cdots = \frac{1}{(1-x)^n}$

$(-1)^k \; {}^{(n+k-1)}C_k$	$\sum_{k=0}^{\infty} (-1)^n \; {}^{(n+k-1)}C_k \, x^k = 1 - {}^nC_1 \, x + {}^{(n+1)}C_2 \, x^2 - \cdots = \frac{1}{(1+x)^n}$
${}^{(n+k-1)}C_k \, x^k$	$\sum_{k=0}^{\infty} {}^{(n+k-1)}C_k \, a^k x^k = 1 + {}^nC_1 \, (ax) + {}^{(n+1)}C_2 \, (ax)^2 + \cdots = \frac{1}{(1-ax)^n}$
1 , if $k \le n$; 0 , otherwise	$\sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}$
${}^nC_k$	$\sum_{k=0}^{n} {}^nC_k \, x^k = 1 + {}^nC_1 \, x + {}^nC_2 \, x^2 + \cdots = (1+x)^n$
${}^nC_k \, a^k$	$\sum_{k=0}^{n} {}^nC_k \, a^k x^k = 1 + {}^nC_1 \, ax + {}^nC_2 \, (ax)^2 + \cdots = (1+ax)^n$

Counting problems and Generating Functions

Generating functions can be used to solve a wide variety of counting problems.

Example 8: Find the number of solutions of

$$\boldsymbol{e_1 + e_2 + e_3 = 17}$$

where $\boldsymbol{e_1, e_2}$ and $\boldsymbol{e_3}$ are nonnegative integers with $\boldsymbol{2 \le e_1 \le 5, 3 \le e_2 \le 6}$ and $\boldsymbol{4 \le e_3 \le 7}$.

Solution: The number of solutions with the given constraints is the coefficient of x^{17} in the expansion of

$$(x^2 + x^3 + x^4 + x^5)(x^3 + x^4 + x^5 + x^6)(x^4 + x^5 + x^6 + x^7)$$

This is so, since we obtain a term equal to x^{17} in the product by taking a term in the first sum x^{e_1}, a term in the second sum x^{e_2} and a term in the third sum x^{e_3}, where the exponents e_1, e_2 and e_3 satisfy the equation (1) and the given constraints.

The coefficient of x^{17} in this product is $1 + 1 + 1 = 3$
(The products $x^4x^6x^7$, $x^5x^5x^7$, $x^5x^6x^6$)

Proving Identities using Generating Functions

Example 9: Use generating function to show that

$$\sum_{k=0}^{n} \left({}^{n}C_{k}\right)^{2} = {}^{2n}C_{n}$$

where n is a positive integer?

Solution: Note that by the Binomial Theorem ${}^{2n}C_{n}$ is the coefficient of x^n in $(1+x)^{2n}$, now

$$(1+x)^{2n} = (1+x)^n(1+x)^n$$

$$= ({}^{n}C_{0} + {}^{n}C_{1}\,x + {}^{n}C_{2}\,x^2 + \cdots {}^{n}C_{n}\,x^n)^2$$

Equating the coefficient x^n on both sides ,we get

$$ {}^{2n}C_{n} = {}^{n}C_{0} \cdot {}^{n}C_{n} + {}^{n}C_{1} \cdot {}^{n}C_{n-1} + {}^{n}C_{2} \cdot {}^{n}C_{n-2} + \cdots + {}^{n}C_{n} \cdot {}^{n}C_{0}$$

$$= {}^{n}C_{0} \cdot {}^{n}C_{0} + {}^{n}C_{1} \cdot {}^{n}C_{1} + {}^{n}C_{2} \cdot {}^{n}C_{2} + \cdots + {}^{n}C_{n} \cdot {}^{n}C_{n}$$

$$(\because {}^{n}C_{r} = {}^{n}C_{r-1})$$

$$= \sum_{k=0}^{n} \left({}^{n}C_{k}\right)^{2}$$

Hence the result.

Solving recurrence relations using generating functions

Example 10: Solve the Fibonacci recurrence relation

$$\boldsymbol{F_n = F_{n-1} + F_{n-2},\qquad F_1 = F_2 = 1}$$

by using generating function.

Solution: We have the recurrence relation

$$F_n = F_{n-1} + F_{n-2}\quad, F_1 = F_2 = 1$$

Put $n = 2$ then $F_2 = F_1 + F_0 \Longrightarrow F_0 = 0$

Let $G(x)$ be the generating function for the sequence $\{F_n\}_{n=0}^{\infty}$, i.e,

$$G(x) = \sum_{n=0}^{\infty} F_n x^n$$

$F_n = F_{n-1} + F_{n-2} \Longrightarrow F_n x^n = F_{n-1}x^n + F_{n-2}x^n$

$$\sum_{n=2}^{\infty} F_n x^n = x\sum_{n=2}^{\infty} F_{n-1}x^{n-1} + x^2\sum_{n=2}^{\infty} F_{n-2}x^{n-2}$$

$\Longrightarrow G_n(x) - F_1 x - F_0 = x(G_n(x) - F_0) + x^2 G_n(x)$

$\Longrightarrow G_n(x) - x = xG_n(x) + x^2 G_n(x)$

$\Longrightarrow G_n(x)(1 - x - x^2) = x$

$\Longrightarrow G_n(x) = \dfrac{x}{1 - x - x^2}$

Now, $1 - x - x^2 = (1 - \alpha\, x)(1 - \beta x)$, where $\alpha + \beta = 1, \alpha\beta = -1$.

$i.e., \alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}$

$$\frac{x}{1 - x - x^2} = \frac{x}{(1 - \alpha\, x)(1 - \beta x)} = \frac{A}{1 - \alpha\, x} + \frac{B}{1 - \beta x}$$

$\Longrightarrow x = A(1-\beta x) + B(1-\alpha x) = (A+B) - (\beta A + \alpha B)x$

$\Longrightarrow A + B = 0, \qquad \beta A + \alpha B = -1$

Solving we get, $A = \frac{1}{\sqrt{5}} = -B$(do it!)

Thus,

$$G(x) = \frac{1}{\sqrt{5}}\left[\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right]$$

$i.e.,$

$$\sum_{n=0}^{\infty} F_n x^n = \frac{1}{\sqrt{5}}\left[\sum_{n=0}^{\infty} \alpha^n x^n - \sum_{n=0}^{\infty} \beta^n x^n\right] = \frac{1}{\sqrt{5}}\left(\sum_{n=0}^{\infty} (\alpha^n - \beta^n) x^n\right)$$

Equating the coefficients of x^n on both sides we get

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n)$$

$$i.e., F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

This is called **Binnet Formula for $\boldsymbol{F_n}$**.

Example 11: Solve the recurrence relation

$$\boldsymbol{a_n = 8a_{n-1} + 10^{n-1}, a_1 = 9}$$

by using generating function.

Solution: Let $G(x) = \sum_{n=0}^{\infty} a_n x^n$ be the generating function for the sequence $\{a_n\}_{n=0}^{\infty}$. Putting $n = 1$, in the given recurrence relation we get

$$a_1 = 8a_0 + 1 \Longrightarrow 9 = 8a_0 + 1 \Longrightarrow a_0 = 1$$

Multiply the given recurrence relation by x^n, we get

$$a_n x^n = 8a_{n-1}x^n + 10^{n-1}x^n$$

Sum both sides starting from $n = 1$

$$\sum_{n=1}^{\infty} a_n x^n = 8\sum_{n=1}^{\infty} a_{n-1}x^n + \sum_{n=1}^{\infty} 10^{n-1}x^n$$

$$\Longrightarrow G(x) - a_0 = 8x\sum_{n=1}^{\infty} a_{n-1}x^{n-1} + x\sum_{n=1}^{\infty} 10^{n-1}x^{n-1}$$

$$\Longrightarrow G(x) - 1 = 8x\sum_{n=0}^{\infty} a_n x^n + x\sum_{n=0}^{\infty} 10^n x^n$$

$$= 8xG(x) + x\sum_{n=0}^{\infty} 10^n x^n$$

$$= 8xG(x) + \frac{x}{1-10x}$$

$$\Longrightarrow (1-8x)G(x) = 1 + \frac{x}{1-10x} = \frac{1-9x}{1-10x}$$

$$\Longrightarrow G(x) = \frac{1-9x}{(1-8x)(1-10x)} = \frac{1}{2}\left(\frac{1}{1-8x} + \frac{1}{1-10x}\right)$$

$$= \frac{1}{2}\left(\sum_{n=0}^{\infty} 8^n x^n + \sum_{n=0}^{\infty} 10^n x^n\right)$$

$$= \sum_{n=0}^{\infty} \frac{1}{2}(8^n + 10^n)\, x^n$$

Therefore, $a_n = \frac{1}{2}(8^n + 10^n)$

Example 12: Solve the recurrence relation

$$\boldsymbol{a_n - 3a_{n-1} = n, n \in N, a_0 = 1}$$

by using generating function.

Solution: We have the generating function

$$a_n - 3a_{n-1} = n, n \in \boldsymbol{N}, a_0 = 1$$

Let $G(x)$ be the generating function for the sequence $\{a_n\}_{n=0}^{\infty}$ $i.e.,$

$$G(x) = \sum_{n=0}^{\infty} a_n x^n$$

Now,

$$a_n - 3a_{n-1} = n \Rightarrow a_n x^n - 3a_{n-1}x^n = nx^n$$

$$\Rightarrow \sum_{n=1}^{\infty} a_n x^n - 3\sum_{n=1}^{\infty} a_{n-1}x^n = \sum_{n=1}^{\infty} nx^n$$

$$\Rightarrow G(x) - a_0 - 3x\sum_{n=1}^{\infty} a_{n-1}x^{n-1} = \sum_{n=0}^{\infty} nx^n$$

$$\Rightarrow G(x) - 1 - 3xG(x) = \sum_{n=0}^{\infty} nx^n$$

$$\Rightarrow G(x)(1-3x) - 1 = x + 2x^2 + 3x^3 + \cdots = x(1 + 2x + 3x^2 + \cdots)$$

$$= x.\frac{1}{(1-x)^2}$$

$$\Rightarrow G(x) = \frac{x}{(1-3x)(1-x)^2} + \frac{1}{1-3x} \quad \ldots(1)$$

$$\frac{x}{(1-x)^2(1-3x)} = \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1-3x}$$

$\Longrightarrow x = A(1-x)(1-3x) + B(1-3x) + C(1-x)^2$

Put $x = 1$, $1 = B(-2) \Longrightarrow B = -\frac{1}{2}$

Put $x = \frac{1}{3}$, $\frac{1}{3} = C.\frac{4}{9} \Longrightarrow C = \frac{3}{4}$

Put $x = 0, 0 = A + B + C \Longrightarrow A = -(B + C) = -\frac{1}{4}$

$$\therefore \frac{x}{(1-x)^2(1-3x)} = -\frac{1}{4}\frac{1}{1-x} - \frac{1}{2}\frac{1}{(1-x)^2} + \frac{3}{4}\frac{1}{1-3x}$$

From (1)

$$G(x) = \frac{1}{4}\frac{1}{1-x} - \frac{1}{2}\frac{1}{(1-x)^2} + \frac{7}{4}\frac{1}{1-3x}$$

$$\sum_{n=1}^{\infty} a_n x^n = -\frac{1}{4}\sum_{n=1}^{\infty} x^n - \frac{1}{2}\sum_{n=1}^{\infty}\binom{2+n-1}{n} x^n + \frac{7}{4}\sum_{n=1}^{\infty} 3^n x^n$$

Equating the coefficients of x^n on both sides we get

$$a_n = -\frac{1}{4} - \frac{1}{2}\,{}^{(n+1)}C_n + \frac{7}{4}3^n = -\frac{1}{4} - \frac{(n+1)}{2} + \frac{7}{4}3^n$$

$$= -\frac{3}{4} - \frac{n}{2} + \frac{7}{4}3^n$$

Generating functions can be used to solve a system of recurrence relation.

Example 13: Solve the following system of recurrence relations using the method of generating functions

$$a_{n+1} = -2a_n - 4b_n, \qquad \dots (1)$$

$$b_{n+1} = 4a_n + 6b_n, \qquad \dots (2)$$

$n = 0,1,2, \dots; a_0 = 1, b_0 = 0.$

Solution: Let $F(x)$ and $G(x)$ be the generating functions for the sequence $\{a_n\}_{n=0}^{\infty}$and $\{b_n\}_{n=0}^{\infty}$ respectively. Form the equations (1) and (2), when $n = 0,1,2,\ldots$

$$a_{n+1}x^{n+1} = -2a_n x^{n+1} - 4b_n x^{n+1}$$

$$b_{n+1}x^{n+1} = 4a_n x^{n+1} + 6b_n x^{n+1}$$

$$\Rightarrow \sum_{n=0}^{\infty} a_{n+1}x^{n+1} = -2x\sum_{n=0}^{\infty} a_n x^n - 4x\sum_{n=0}^{\infty} b_n x^n$$

$$\sum_{n=0}^{\infty} b_{n+1}x^{n+1} = 4x\sum_{n=0}^{\infty} a_n x^n + 6x\sum_{n=0}^{\infty} b_n x^n$$

$$\Rightarrow F(x) - a_0 = -2xF(x) - 4xG(x)$$

$$G(x) - b_0 = 4xF(x) + 6xG(x)$$

$$\Rightarrow (1 + 2x)F(x) + 4xG(x) = 1 \qquad \ldots(3)$$

$$4x\, F(x) - (1 - 6x)G(x) = 0 \qquad \ldots(4)$$

Solving for $F(x)$, we get

$$F(x) = \frac{1-6x}{(1-2x)^2} \text{ (do it!)}$$

Now, $\dfrac{1-6x}{(1-2x)^2} = \dfrac{A}{1-2x} + \dfrac{B}{(1-2x)^2}$

$i.e.,$ $\quad 1 - 6x = A(1 - 2x) + B \Rightarrow A + B = 1, B = -2 \Rightarrow A = 3, B = -2$

Hence $F(x) = \dfrac{3}{1-2x} - \dfrac{2}{(1-2x)^2}$

$$= 3\sum_{n=0}^{\infty} 2^n x^n - 2\sum_{n=0}^{\infty} (n + 1)2^n x^n$$

$$= \sum_{n=0}^{\infty} (3.2^n - 2(n + 1)2^n)x^n$$

$$= \sum_{n=0}^{\infty} 2^n(1-2n)x^n = \sum_{n=0}^{\infty} a_n x^n$$

From (4), we have $G(x) = \frac{4x}{1-6x}$ $F(x) = \frac{4x}{(1-2x)^2}$

Now, $\frac{4x}{(1-2x)^2} = -\frac{2}{1-2x} + \frac{2}{(1-2x)^2}$ (do it!)

$$= -2\sum_{n=0}^{\infty} 2^n x^n + 2\sum_{n=0}^{\infty}(n+1)2^n x^n$$

$$= \sum_{n=0}^{\infty} 2^n(-2+2n+2)x^n$$

$$= \sum_{n=0}^{\infty} 2^n(2n)x^n = \sum_{n=0}^{\infty} n.2^{n+1}x^n = \sum_{n=0}^{\infty} b_n x^n$$

Thus , $a_n = 2^n(1-2n), b_n = n\ 2^{n+1}$.

UNIT-5

INTRODUCTION TO GRAPH THEORY

MODULE-1

Graphs and their basic properties

Unit-3 Graph Theory

3.1

Graphs and their basic properties

We have already studied some preliminary concepts of graph theory in Unit 2 where we discussed the digraph of a relation. We have used a digraph as a pictorial representation of a relation and it served only a limited purpose. In this unit we shall extend, and in some cases, generalize these ideas.

Graph theory is applied in such diverse areas as Social Sciences, Linguistics, Physical Sciences, Communication Engineering and others. Graph theory also plays an important role in several areas of Computer Science, such as Switching Theory and Logical design, Artificial intelligence, Formal languages, Computer graphics, Operating systems, Compiler writing, and Information organization and retrieval.

Like many important discoveries, graph theory grew out of an interesting physical problem, the celebrated **Konigsberg Bridge Puzzle**. The outstanding Swiss mathematician *Leonhard Euler* solved the puzzle in 1736, thus laying the foundation for graph theory and earning his title as the father of graph theory.

Graph: A **graph** $G = (V, E)$ consists of a nonempty set V, called the set of **nodes** (or **points** or **vertices**) of the graph and E, called the set of **edges** of the graph, which is a subset of the set of ordered or unordered pairs of element of V.

We shall assume throughout, both the sets V and E of a graph are finite.
If $\in E$, then e is an **edge**, e is **an ordered pair** $(\boldsymbol{u}, \boldsymbol{v})$ or **an unordered pair** $\{\boldsymbol{u}, \boldsymbol{v}\}$, where $u, v \in V$ and we say that the edge e *connects* or *joins* the nodes u and v. A pair of nodes are said to be **adjacent** if they are connected by an edge.

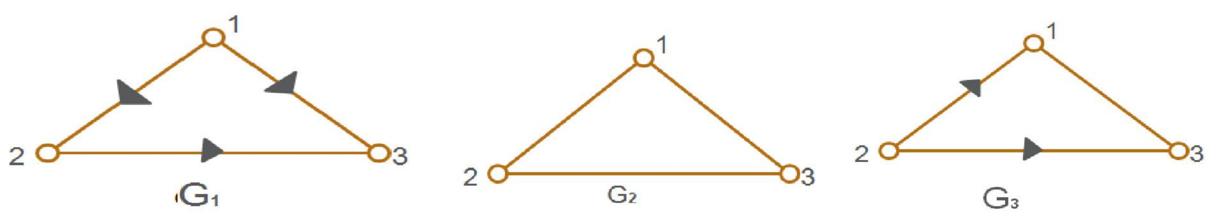
Directed, undirected and mixed graphs:

In a graph $G = (V, E)$, an edge which is an ordered pair of $V \times V$ is called a **directed edge**. An edge which is an unordered pair $\{u, v\}, u, v \in V$ is called an **undirected edge**. A graph in which every edge is directed is called a **directed graph** or **digraph**. A graph in which every edge is undirected is called a **undirected graph**. If some edges are directed and some are undirected in a graph, then the graph is called a **mixed graph**.

In the diagrams the directed edges are shown by means of arrows which also show directions.

Example 1: Let $V = \{1,2,3\}$, $E_1 = \{(1,2), (1,3), (2,3)\}$, $E_2 = \{\{1,2\}, \{1,3\}, \{2,3\}\}$ and $E_3 = \{(2,1), \{1,3\}, (2,3)\}$.

Then $G_1 = (V, E_1)$ is a digraph, $G_2 = (V, E_2)$ is an undirected graph and $G_3 = (V, E_3)$ is a mixed graph as shown below.



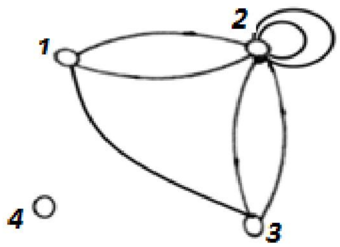
Let $G = (V, E)$ be a graph and $e \in E$ be a directed edge (u, v). Then we say that e is *initiating* or *originating* in the node u and *terminating* or *ending* in the node v. The nodes u and v are called the **initial** and **terminal** nodes of the edge e, respectively. An edge $e \in E$ which joins the nodes u and v, whether it be directed or undirected is said to be **incident** the nodes u and v.

An edge of a graph which joins a node to itself is called a **loop**. The direction of a loop is of no significance; therefore it can be considered either a directed or a an undirected edge.

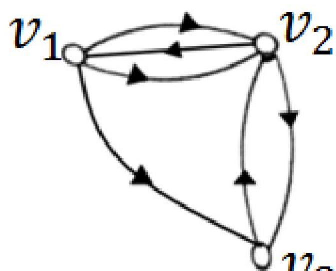
In the case of directed edges, the two possible edges (u, v) and (v, u) between a pair of nodes u, v which are opposite in direction are considered **distinct**. Two or more distinct edges between a pair of vertices are called **parallel edges**.

Any graph which contains parallel edges is called a **multigraph**.

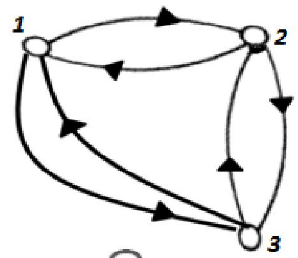
A graph is said to be **simple** if there is no more than one edge between a pair of nodes (no more than one directed edge in the case of a digraph).The graphs G_1, G_2 and G_3 are all simple graphs.



G4



G5

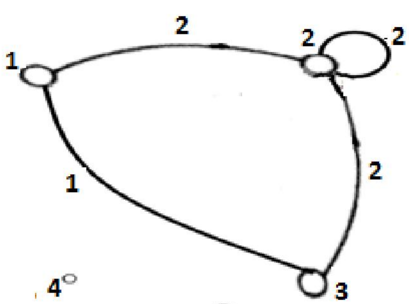


G6

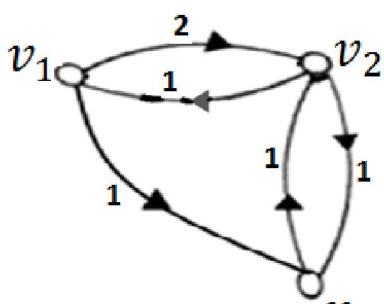
Notice that the graph G_4 , G_5 have parallel edges and so they are multigraphs. The graph G_6 is a simple graph.

If e denotes the edge joining two nodes u, v and there are n parallel edges between u, v then we say that the **multiplicity** of e is $\boldsymbol{n}$.

The multigraphs may be drawn by displaying their multiplicity on their respective multiple edges (See G_4 , G_5 below with the multiplicities on the edges).

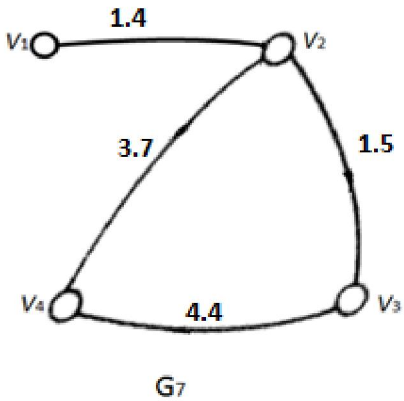


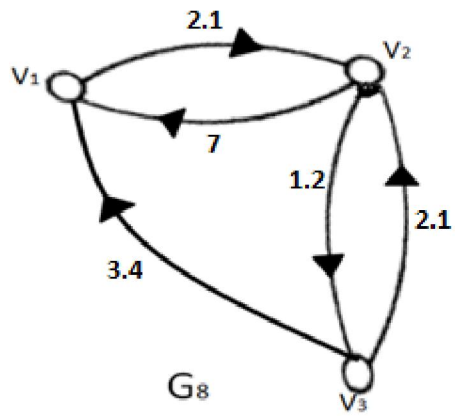
G4



G5

We may also consider the multiplicity as a **weight** assigned to an edge. This interpretation allows us to generalize the concept of weight to numbers which are not necessarily integers (See graphs G_7 and G_8)





A graph in which weights are assigned to every edge is called a **weighted graph**. The graphs G_4 , G_5 , G_7 and G_8 are all weighted graphs.

A graph representing a system of pipelines in which the weights assigned on each pipeline(i . .$e$edge) indicate the *amount of the commodity transferred* through the pipeline is an example of a weighted graph. Similarly, a graph of city streets may be assigned weights according to the *traffic density* on each street.

A node in a graph is said to be an **isolated node** if it is not adjacent to any node. In G_4 , the node 4 is an isolated node.

A graph $G = (V, E)$ is said to be a **null graph** if E is an empty set. That is, a graph containing only isolated nodes is a null graph.

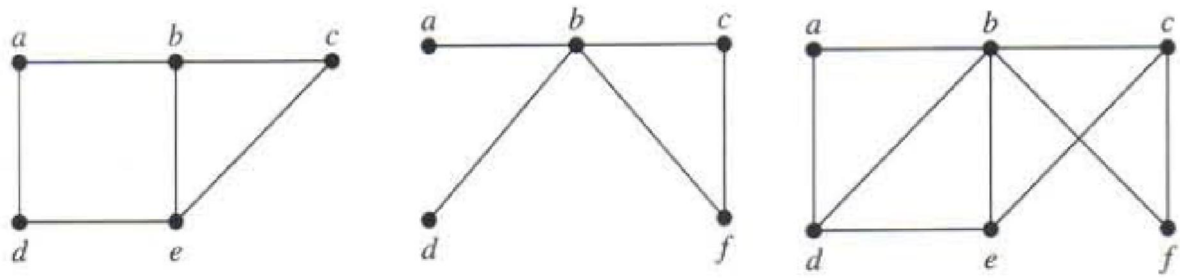
G_0: Null graph

Subgraph: When edges and vertices are removed from a graph without removing the endpoints of any remaining edges, a smaller graph is obtained such a graph is called a **Subgraph** of the original graph.

Let G and H be graphs. Let $V(G)$ and $V(H)$ be the sets of nodes of G and H respectively. The graph H is said to be a **subgraph** of the graph G

(written as $H \subseteq G$) if $V(H) \subseteq V(G)$ and every edge of H is also an edge of G. Clearly, the graph G itself, and the null graph obtained from G by deleting all the edges of G are subgraphs of G. Other subgraphs of G are obtained by deleting certain nodes and the edges incidenting with these nodes of G.

Example 2: G_1, G_2 are subgraphs of the graph G.



G_1 G_2 G

Union of graphs: The **union** of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the graph of G denoted by $G_1 \cup G_2$, where

$$G = G_1 \cup G_2 = (V, E), V = V_1 \cup V_2, \; E = E_1 \cup E_2$$

In the above diagram $G = G_1 \cup G_2$

Binary relations and simple digraphs:

Let R be a binary relation on V ($i.e$, $R \subseteq V \times V$). Then the graph of R is a digraph $G = (V, R)$. Notice that G has no parallel edges because R is a set, where the ordered pairs are enlisted only once. Therefore, the digraph G is simple. Thus, the graph of a binary relation is a simple digraph.

Conversely, let $G = (V, E)$ be a simple digraph. Then every edge of E can be expressed by means of an ordered pair of elements of V. Since G is simple, the ordered pairs corresponding to the edges of E are all distinct. Then $E \subseteq V \times V$. Therefore, E is a binary relation on V whose graph is the simple digraph G.Thus we have the following:

If $G = (V, E)$ is a simple digraph then E is a binary relation on V and conversely.

We can define the converse of a simple digraph.

The **converse** of a simple digraph $G = (V, E)$ is the graph $\bar{\boldsymbol{G}} = (\boldsymbol{V}, \bar{\boldsymbol{E}})$, where $\bar{E}$ is the converse of the relation E on V.
Note that $\bar{G}$ is also simple. The diagram of $\bar{G}$ is obtained from that of G by simply reversing the directions of the edges of G. The converse $\bar{G}$ is also called the **reversal** or **directional dual** of G.

A simple digraph $G = (V, E)$ is called **reflexive**, **transitive**, **symmetric**, **antisymmetric** if the relation E on V is respectively reflexive, transitive, symmetric, antisymmetric.

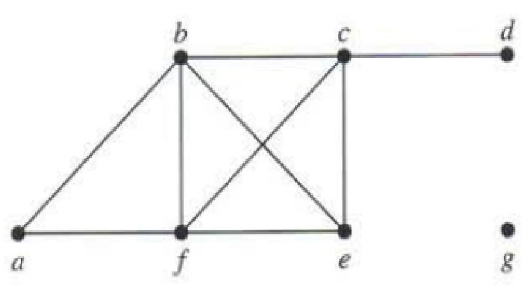
If a simple digraph $G = (V, E)$ is reflexive, symmetric and transitive, then the relation E is an equivalence relation on V and hence V is partitioned into equivalence classes. Any equivalence class of nodes along with the edges connecting them is a subgraph of G. These subgraphs are such that they are pair wise disjoint and the union of these subgraphs is the graph G. In this sense the graph G is partitional into mutually disjoint subgraphs.

Degree of a node in an undirected graph: The **degree** of a node in an undirected graph is the number of edges incident with it, except that a loop at a node contributes a count of 2 to the degree of that node. The degree of a node v is denoted by $\boldsymbol{deg}\ (\boldsymbol{v})$.

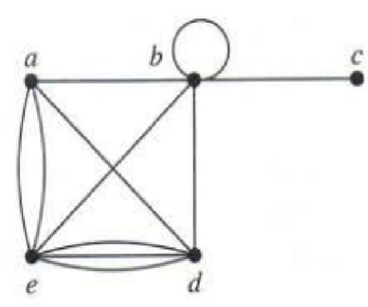
Pendant node: A node is called **pendant** iff it has degree 1.

Note: A pendant node is adjacent to exactly one other node. The degree of an isolated node is 0.

Example 3: What are the degrees of vertices in the graphs $\boldsymbol{G}$ and $\boldsymbol{H}$ given below:



G



H

Solution: In the undirected graph G,

$\deg(a) = 2$, $\deg(b) = \deg(c) = \deg(f) = 4$, $\deg(d) = 1$, $\deg(e) = 3$, $\deg(g) = 0$.

Node d is pendent and node g is an isolated node

In the undirected graph H,

$\deg(a) = 4$, $\deg(b) = 4 + 2\,(loop) = 6$, $\deg(c) = 1$, $\deg(d) = 5$, $\deg(e) = 6$

Node c in the graph H is pendant

Theorem 1: The Handshaking Theorem

Let $\boldsymbol{G} = (\boldsymbol{V}, \boldsymbol{E})$ be an undirected graph. Then

$$\sum_{v \in V} \deg(v) = 2|E|$$

*Proof***:** Note that each edge $\{a, b\}$ contributes two to the sum of the degrees of the nodes (because it contributes 1 for the degree of a and 1 for the degree of b). It is true even if $a = b$. This means that the sum of the degrees of the nodes is twice the number of edges. Hence the theorem.

Note:

i. This theorem applies even if multiple edges and loops are present.
ii. This theorem is called the Handshaking Theorem, because of the analogy between an edge having two end points and a handshake involving two hands.

The following is a consequence of the above theorem.

Theorem 2: An undirected graph has an even number of nodes of odd degree.

Proof: We have $= (V, E)$, an undirected graph. Let V_1 and V_2 be the sets of nodes of odd and even degree respectively. Clearly $V_1 \cap V_2 = \phi$ and $V_1 \cup V_2 = V$. Therefore,

$$\sum_{v \in V} \deg \ (v) = \sum_{v \in V_1} \deg v \ + \sum_{v \in V_2} \deg \ (v)$$

By Handshaking theorem

$$2|E| = \sum_{v \in V_1} \deg \ (v) + \sum_{v \in V_2} \deg \ (v)$$

Note that for each $v \in V_2, \deg(v)$ is even and so $\sum_{v \in V_2} \deg(v)$ is even. From the above, it follows that

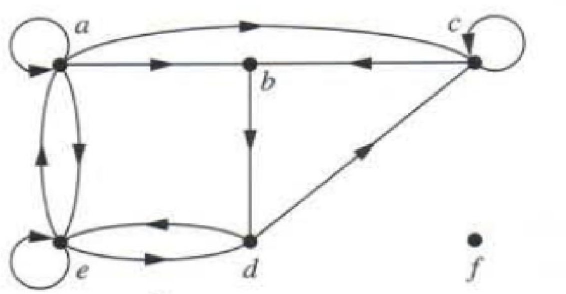
$$\sum_{v \in V_1} \deg(v) \text{ is even.}$$

If $|V_1|$ is odd then $\sum_{v \in V_1} \deg(v)$ is odd – a contradiction. Therefore $|V_1|$ must be even.Thus, the number of vertices of odd degree is even. Therefore, G has an even number of vertices of odd degree. Hence the theorem.

The definition of the degree of a node in a digraph can be refined in the following way:

In-degree, out-degree and degree of a node in a digraph: Let $G = (V, E)$ be a digraph. The **in-degree** of a node $v \in V$, denoted by $\boldsymbol{deg}^{\ -}(\boldsymbol{v})$, is the number of edges with v as their terminal node. The **outdegree** of v, denoted by $\boldsymbol{deg}^{\ +}(\boldsymbol{v})$, is the number of edges with v as their initial node. A loop at a vertex v contributes 1 to both the in-degree and the out-degree of V.The sum of the in-degree and out-degree of a node v is called the **degree** of the node v

Example 4: Find the in-degree and out-degree of each node in the digraph G given below:



G

Solution:

The in-degrees of nodes of G are:

$\deg^{-}(a) = 1 + 1(loop) = 2$, $\deg^{-}(b) = 2$, $\deg^{-}(c) = 2 + 1(loop) = 3$

, $\deg^{-}(d) = 2$, $\deg^{-}(e) = 2 + 1(loop) = 3$and $\deg^{-}(f) = 0.$

The out-degrees of nodes of G are:

$\deg^{+}(a) = 3 + 1(loop) = 4$, $\deg^{+}(b) = 1$, $\deg^{+}(c) = 1 + 1(loop) = 2$,
$\deg^{+}(d) = 2$, $\deg^{+}(e) = 2 + 1(loop) = 3$ and $\deg^{+}(f) = 0.$
Note that the sum of the in-degrees of all nodes equals to the sum of out-degrees of all nodes and each is equal to the number of edges. This is infact true in a diagraph and is proved in the following theorem.

Theorem 3: If $G = (V, E)$ is a digraph, then

$$\sum_{v \in V} \mathbf{deg}^{-}(v) = \sum_{v \in V} \mathbf{deg}^{+}(v) = |E|$$

Proof: Since each directed edge has an initial node and a terminal node, the sum of the in-degrees and the sum of the out-degrees of all nodes in a digraph are the same. Both of these sums are the number of edges in the digraph. Hence the result .

Degree sequence: The **degree sequence** of a graph is the sequence of the degrees of the vertices of the graph in nonincreasing order.

A sequence $d_1, d_2, \ldots, d_n$ is called **graphic** if it is the degree sequence of a simple graph.

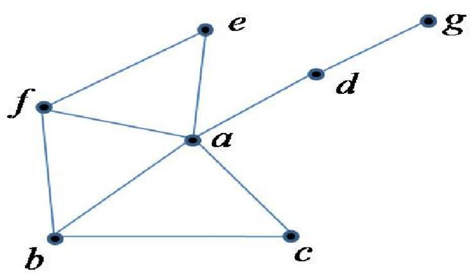
Example 5: Determine whether the degree sequence $\mathbf{5, 3, 3, 2, 2, 2, 1}$ is a graphic? If it is, how many edges does this graph have? Draw a graph having this degree sequence.

Solution: By *Handshaking theorem,* the sum of the degrees of all vertices is equal to twice the number of edges. Therefore

$$2|E| = 5 + 3 + 3 + 2 + 2 + 2 + 1 = 18$$

$$\Longrightarrow |E| = 9$$

Therefore, there are 9 edges in the graph. The diagram of such a graph is given below:



In this graph the vertex g is a pendant.

Remark: The definition of graph contains no reference to the length or the shape and positioning of the edges joining any pair of nodes, nor does it prescribe any ordering of positions of nodes. Therefore, for a given graph, there is no unique diagram which represents the graph. We can obtain a variety of diagrams by locating the nodes in an arbitrary number of different positions and also by showing the edges by arcs or lines of different shapes. Due to this arbitrariness, it can happen that two diagrams which look entirely different from one another may represent the same graph. We now has the concept of *sameness* is graph theory.

Isomorphic graphs: Two graphs are said to be **isomorphic** if there exists a one – to – one correspondence between the nodes of the two graphs which preserve adjacency of the nodes as well as the directions of the edges, if any.

Two graphs $G = (V, E)$ and $G' = (V', E')$ are said to be **isomorphic**, written as $\boldsymbol{G \cong G'}$ **,** if there exists an adjacency preserving bijective map between their vertices. That is, if there exists a bijective map $f: V \to V'$ such that

(i) $(a, b) \in E \implies \big(f(a), f(b)\big) \in E'$, for all $(a, b) \in E$ in the case of diagraphs

(ii) $\{a, b\} \in E \implies \{f(a), f(b)\} \in E'$, for all $\{a, b\} \in E$ in the case of undirected graph

In such a case, f is called an **isomorphism** between G and G'

Note: It is essential that two graphs which are isomorphic have the same number of nodes and edges, however, this is not sufficient condition for an isomorphism to exist.

Note: It is often difficult to determine whether two graphs are isomorphic. There are $n!$ possible one-to-one correspondences between the node sets of two graphs with n nodes. Testing each such correspondence to see whether it preserves adjacency is impractical if n is large.

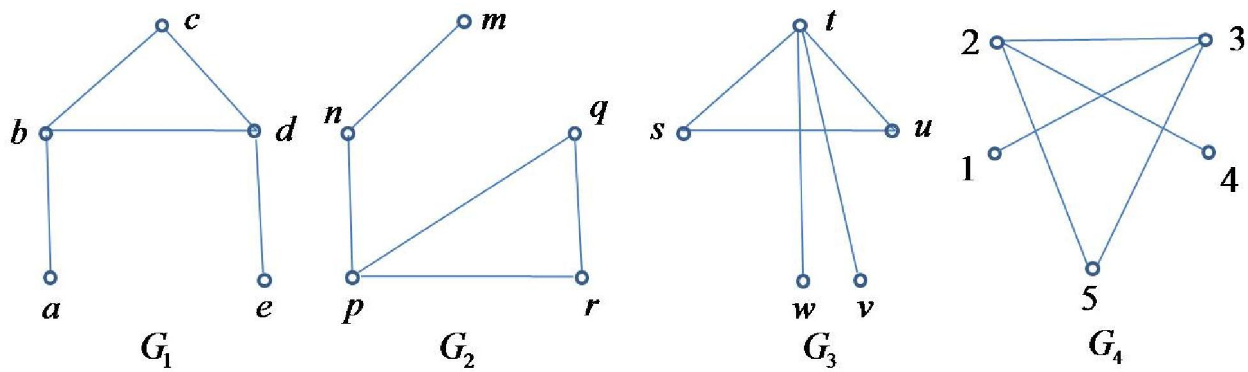
Sometimes it is not hard to show that two graphs are not isomorphic. In particular we can show that two graphs are not isomorphic if we can find a property, only one of the two graphs has, but that is preserved by isomorphism.

A property preserved by isomorphism of graphs is called a **graph invariant**.

The degrees of the nodes in isomorphic graphs G, H must be same. That is, a node v of degree d in G must correspond to a node $f(v)$ of degree d in H.

The number of nodes, number of edges and the number of vertices of each degree are all invarient under isomophism. If any of these differ in two graphs, then these graphs cannot be isomorphic. However, when these invariants are the same, it does not necessarily mean that the graphs are isomorphic.

Example 6: Which of the following graphs are isomorphic?



Solution:

All the graphs G_k , $k = 1,2,3,4$ are undirected graphs with 5 vertices and 5 edges.

The degree sequences are as follows:

$$G_1 : \ 3,3,2,1,1$$

$$G_2 : 3,2,2,2,1$$

$$G_3 : 4,2,2,1,1$$

$$G_4 : 3,3,2,1,1$$

Since the degree sequence is a graph invariant property, possibly G_1 , G_4 are isomorphic. It also confirms G_1, G_2, G_3 are pair wise nonisomorphic and G_2, G_3, G_4 are pairwise nonisomorphic.

Construction of an isomorphism f from G_1 to G_4.
The vertex sets of G_1 and G_4 are $V_1 = \{a, b, c, d, e\}$, $V_4 = \{1,2,3,4,5\}$ respectively. Now f must map c onto 5(why?). Therefore $f(c) = 5$. Since the vertex c is adjacent to vertices b, d of degree 3 in G_1 and the vertex 5 is adjacent to vertices 2,3 of degree 3 in G_4 ; we take $f(b) = 2$, $f(d) = 3$.Since b is adjacent to a of degree 1 in G_1 and 2 is adjacent to 4 of degree 1 in G_4; we take $f(a) = 4$.

We are left with the option $f(a) = 1$. Thus, we have set a bijection $f \ : V_1 \longrightarrow V_4$ in the following way

$$a \xrightarrow{f} 4$$
$$b \xrightarrow{f} 2$$
$$c \xrightarrow{f} 5$$
$$d \xrightarrow{f} 3$$
$$e \xrightarrow{f} 1$$

We see that f preserves the adjacency as shown below:

$$\{a, b\} \xrightarrow{f} \{f(a), f(b)\} = \{4,2\}$$

$$\{b, c\} \xrightarrow{f} \{2,5\}$$

$$\{b, d\} \xrightarrow{f} \{2,3\}$$

$$\{c, d\} \xrightarrow{f} \{5,3\}$$

$$\{d, e\} \xrightarrow{f} \{3,1\}$$

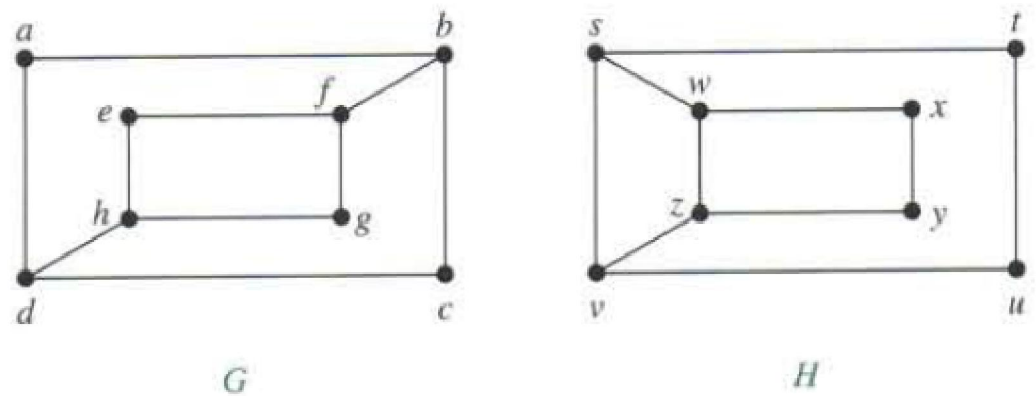
Thus, f is an isomorphism from G_1 to G_4 and $G_1 \cong G_4$.

Note: The map $g : V_1 \longrightarrow V_4$ defined by

$g(a) = 1$, $g(b) = 3$, $g(c) = 5$, $g(d) = 2$ and $g(e) = 4$

is also an isomorphism (verify!).Are these only two isomorphisms between the graphs G_1 and G_4 ? (Investigate!).

Example 7: Determine whether the following graphs are isomorphic?



Solution: Both the graphs G and H are undirected graphs; both have 8 vertices and 10 edges.

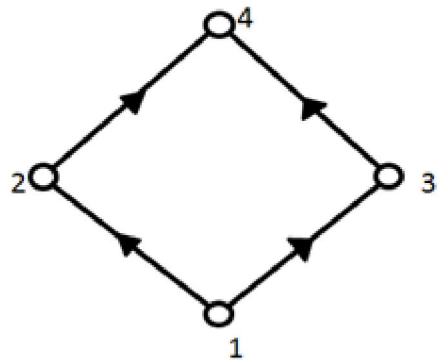
G		H	
Vertex	Degree	Vertex	Degree
a	2	s	3
b	3	t	2
c	2	u	2
d	3	v	3
e	2	w	3
f	3	x	2
g	2	y	2
h	3	z	3

The degree sequence of G : 2,2,2,2,3,3,3,3.

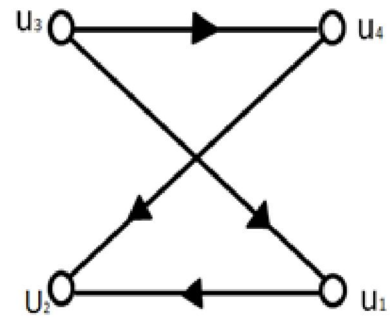
The degree sequence of H : 2,2,2,2,3,3,3,3.

Thus, all the invariants are agreeing. Note that $\deg(a) = 2$ in G and it must correspond to either t , u, $x$or y (because these are vertices of degree 2 in H). Observe that each of these four vertices t , u, x, $y$in H is adjacent to another vertex of degree 2 in H , where as a is adjacent to the vertices b, d of degree 3 and not adjacent to any vertex of degree 2 in G.This shows that G and H are not isomorphic.

Example 8: Show that the following graphs are isomorphic.



G



G'

Solution: We have digraphs

$G = (V, E)$, where $V = \{1, 2, 3, 4, \}$, $E = \{(1, 2), (1, 3), (2, 4), (3, 4)\}$

$G' = (V', E')$, where $V' = \{u_1, u_2, u_3, u_4\}$

$$E' = \{(u_1, u_2), (u_3, u_1), (u_3, u_4), (u_4, u_2)\}$$

The following are in-degree and out-degree tables for the vertices of G and G'.

G		
vertex	$\deg^-$	$\deg^+$
1	0	2
2	1	1
3	1	1
4	2	0

G'		
vertex	$\deg^-$	$\deg^+$
u_1	1	1
u_2	2	0
u_3	0	2
u_4	1	1

Since the in-degree and out-degree is in variatiant under an isomorphism, we must map 1 onto u_3 and 4 onto u_2. Now we have two possibilities
(i) $2 \longrightarrow u_1$, $3 \longrightarrow u_4$ (ii) $2 \longrightarrow u_4$, $3 \longrightarrow u_1$.

Let $f : V \longrightarrow V'$ be defined by $f(1) = u_3$, $(2) = u_1$, $f(3) = u_4$, $f(4) = u_2$.

This bijection f reserves the adjacency of nodes as shown below:

$$(1,3) \xrightarrow{\boldsymbol{f}} \big(f(1)\,, f(3)\big) = (u_3, u_4)$$

$$(1,2) \xrightarrow{\boldsymbol{f}} (u_3, u_1)$$

$$(2,4) \xrightarrow{\boldsymbol{f}} (u_1, u_2)$$

$$(3,4) \xrightarrow{\boldsymbol{f}} (u_4, u_2)$$

This shows f is an isomorphism between G and $G'$and $G \cong G'$.

Let $g : V \longrightarrow V'$ be defined by

$$g(1) = u_3\,, g(2) = u_4\,, g(3) = u_1\,, g(4) = u_2$$

It may be verified that g is also an isomorphism between G and G' and $G \cong G'$ (verify!).

Are these only two isomorphisms between the graphs G and G'? (Explore!)

P1:

How many edges are there in an undirected graph with 10 nodes each of degree six?

Solution:

We have $\sum_{v \in V} \deg(v) =$ The sum of the degrees of all nodes $= 10 \times 6 = 60.$

By Handshaking Theorem, $2|E| = \sum_{v \in V} \deg(v) = 60$. Therefore, $|E| = 30$. Thus the number of edges in the graph is 30.

P2:

Determine whether the degree sequences 1,1,1,1,1 is graphic. If it is, draw a graph having the given degree sequence.

Solution:

The given degree sequence is 1,1,1,1,1. By *Handshaking theorem*,
$2|E| =$ Sum the degrees of all the vertices

$$= 1 + 1 + 1 + 1 + 1 = 5$$

This is not possible. Therefore the given degree sequence is not a graphic.

P3:

Determine whether the degree sequences 3,2,2,1,0 is graphic. If it is, draw a graph having the given degree sequence.

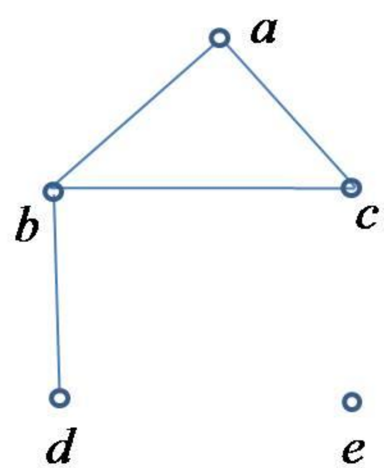
Solution:

The given degree sequence is 3,2,2,1,0.By Handshaking theorem

$2|E| =$ Sum of the degrees of all the vertices $= 3 + 2 + 2 + 1 + 0 = 8$

$\Rightarrow |E| = 4$

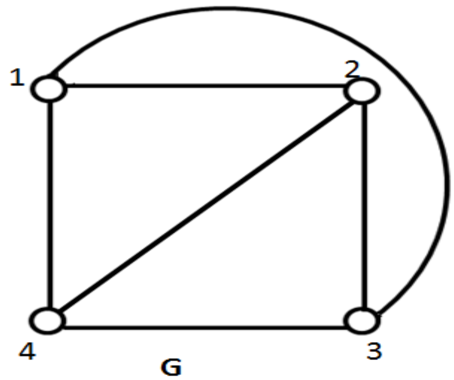
We have to draw a simple graph with 5 nodes and 4 edges with the given degree sequence.

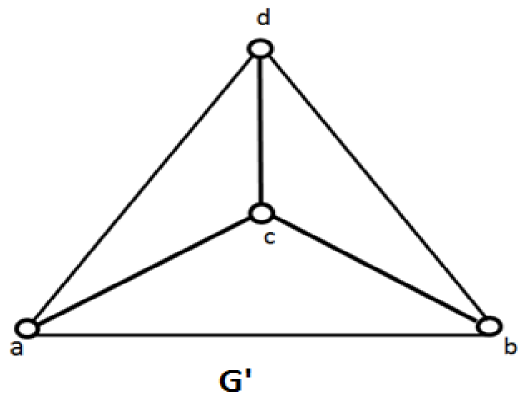


The given sequence is graphic. In the above graph d is pendant and e is an isolated node.

P4:

Show that the following graphs are isomorphic.





Solution:

The given graphs are undirected graphs.

We have, $G = (V, E)$, where $V = \{1,2,3,4\}$ and

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

$G' = (V', E')$, where $V' = V$, $E' = \{\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\},\{c,d\}\}$.

Define a map $\boldsymbol{f} : \boldsymbol{V} \longrightarrow \boldsymbol{V'}$ by , $f(1) = a\ f(2) = b$, $f(3) = c$, $f(d) = 4$.

Now, f preserves the adjacency as shown below:

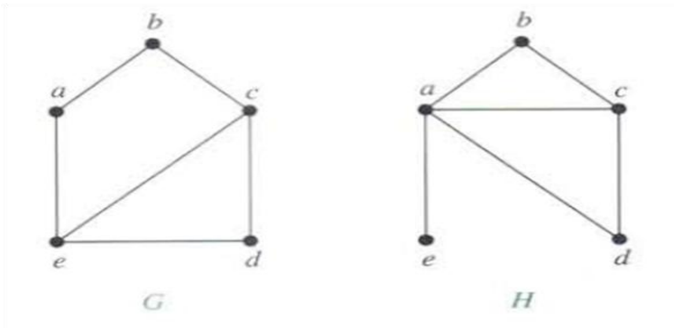
$$\{1,2\} \xrightarrow{f} \{f(1), f(2)\} = \{a,b\}$$
$$\{1,3\} \rightarrow \{a,c\}$$
$$\{1,4\} \rightarrow \{a,d\}$$
$$\{2,3\} \rightarrow \{b,c\}$$
$$\{2,4\} \rightarrow \{b,d\}$$
$$\{3,4\} \rightarrow \{c,d\}$$

Therefore f is an isomorphism from G to G' and $G \cong G'$.

Note: Every bijection from V to V' is an isomorphism(Why?)

P5:

Show that the following graphs are not isomorphic.



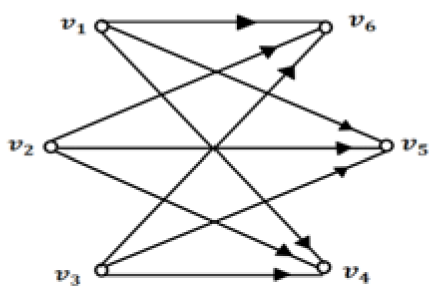
Solution:

The given graphs G and H are undirected. Both have 5 vertices and 6 edges. Note that the graph H has a vertex e of degree 1 and G has no vertices degree 1. Therefore, G and H are not isomorphic.

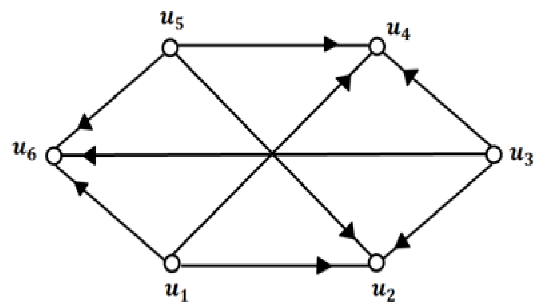
Note: The degree sequence of G is $3,3,2,2,2$ and the degree sequence of H is $4,3,2,2,1$.Therefore G and H are not isomorphic .

P6.

Show that the following diagraphs are isomorphic.



G



H

Solution:

Let $G = (V, E)$, where $V = \{v_1, v_2, v_3, v_4, v_5, v_6\}$ and
$E = \{(v_1, v_4), (v_1, v_5), (v_1, v_6), (v_2, v_4), (v_2, v_5), (v_2, v_6), (v_3, v_4), (v_3, v_5), (v_3, v_6)\}$.
Let $H = \left(V', E'\right)$, where $V' = \{u_1, u_2, u_3, u_4, u_5, u_6\}$ and
$E' = \{(u_1, u_2), (u_1, u_4), (u_1, u_6), (u_3, u_2), (u_3, u_4), (u_3, u_6), (u_5, u_2), (u_5, u_4), (u_5, u_6)\}$.

The following are the in-degree and out-degree tables:

G		
Vertex	deg^-	deg^+
v_1	0	3
v_2	0	3
v_3	0	3
v_4	3	0
v_5	3	0
v_6	3	0

H		
Vertex	deg^-	deg^+
u_1	0	3
u_2	3	0
u_3	0	3
u_4	3	0
u_5	0	3
u_6	3	0

Define a map $f: V \longrightarrow V'$ by

$$\boldsymbol{f(v_1) = u_1, f(v_2) = u_3, f(v_3) = u_5,}$$

$$\boldsymbol{f(v_4) = u_2, f(v_5) = u_4, f(v_6) = u_6}$$

f preserves the adjacency as shown below:

$(v_1, v_4) \xrightarrow{f} (u_1, u_2)$; $(v_2, v_4) \xrightarrow{f} (u_3, u_2)$; $(v_3, v_4) \xrightarrow{f} (u_5, u_2)$

$(v_1, v_5) \longrightarrow (u_1, u_4)$; $(v_2, v_5) \longrightarrow (u_3, u_4)$; $(v_3, v_5) \longrightarrow (u_5, u_4)$

$(v_1, v_6) \longrightarrow (u_1, u_6)$; $(v_2, v_6) \longrightarrow (u_3, u_6)$; $(v_3, v_6) \longrightarrow (u_5, u_6)$

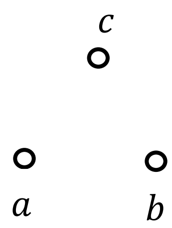
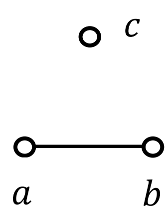
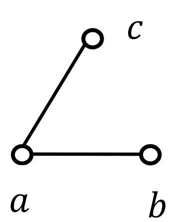
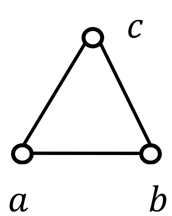
Thus, f is an isomorphism and $G \cong H$.

Note: There are 36 such isomorphisms (how? explore!)

P7.

How many nonisomorphic simple graphs (without loops) are there with 3 vertices?

Solution:

Graph	**Degree sequence**
	$0, 0, 0$
	$1, 1, 0$
	$2, 1, 1$
	$2, 2, 2$

Any simple graph with three vertices is isomorphic to one of the above four. These four are pair wise nonisomorphic. Therefore, there are four non-isomorphic simple graphs with three vertices.

3.1. **Graphs and their basic properties**

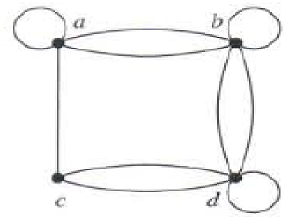
Exercise:

1. Determine whether the graphs shown below has directed or undirected edges, whether it has multiple edges, and whether it has one or more loops. Use your answer to determine the type of graph .

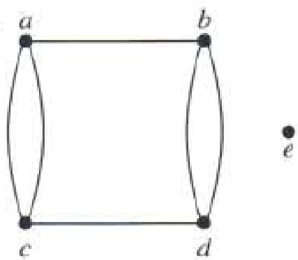
(i)

(ii)

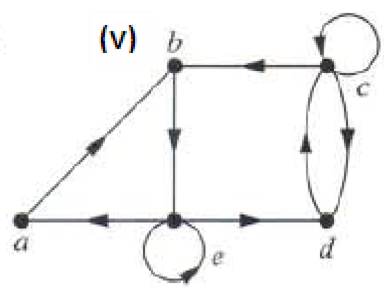
(iii)



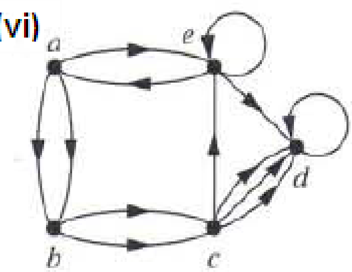
(iv)



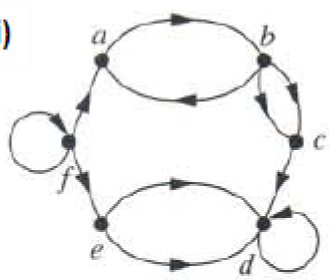
(v)



(vi)

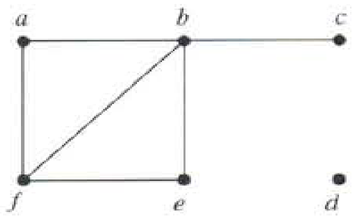


(vii)

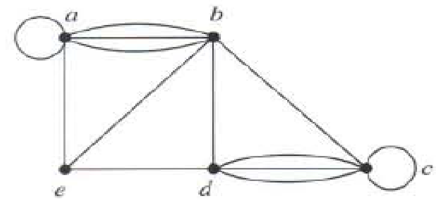


2. Find the number of vertices, the number of edges, and the degree of each vertex in the given undeircted graph. Identify all isolated and pendant vetices.

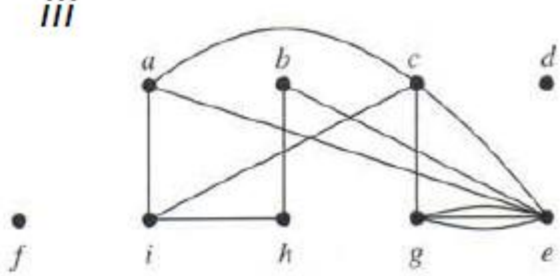
i



ii



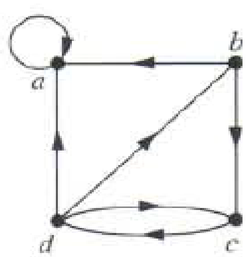
iii



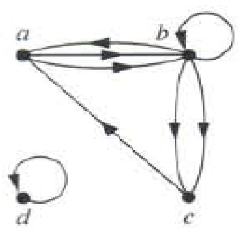
3. Can a simple graph exist with 15 vertices each of degree five?

4. Determine the number of vertices and edges and find the in – degree and out – degree of each vertex for the given directed multigraph.

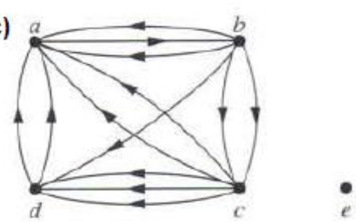
(a)



(b)



(c)

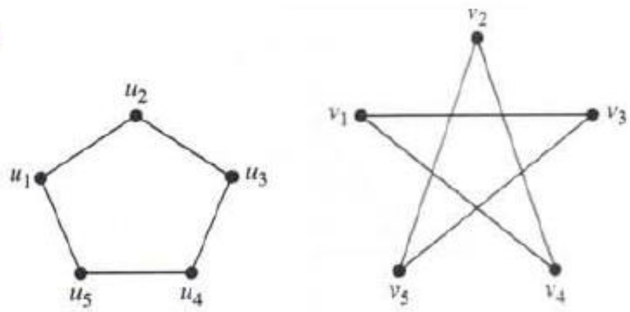


5. Determine whether each of these sequences is graphic. For those that are, draw a graph having the given degree sequence.

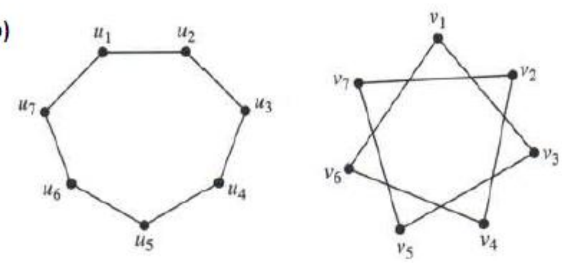
a) 3, 3, 3, 3, 2
b) 5, 4, 3, 2, 1
c) 4, 4, 3, 2, 1
d) 4, 4, 3, 3, 3

6. Determine whether the given pair of graphs is isomorphic. Exhibit an isomorphism or provide a rigorous argument that none exists.

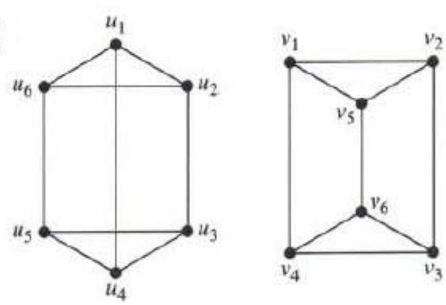
a)



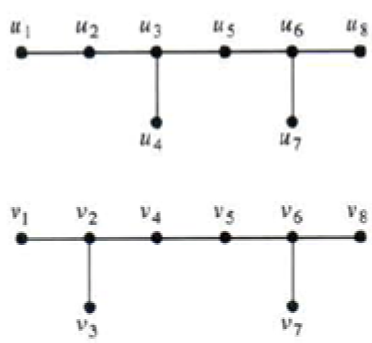
b)



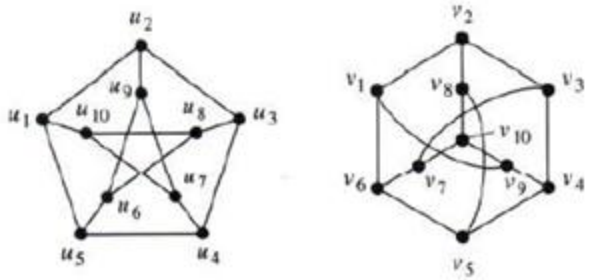
c)



d

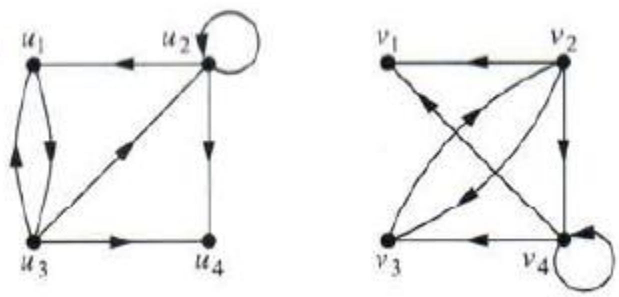


e

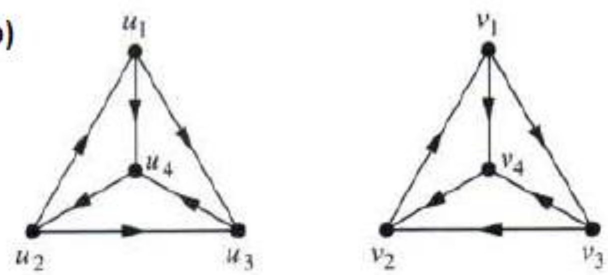


7. Determine whether the given pair of directed graphs are isomorphic.

a)



b)



MODULE-2

Special types of graphs and representations of graphs

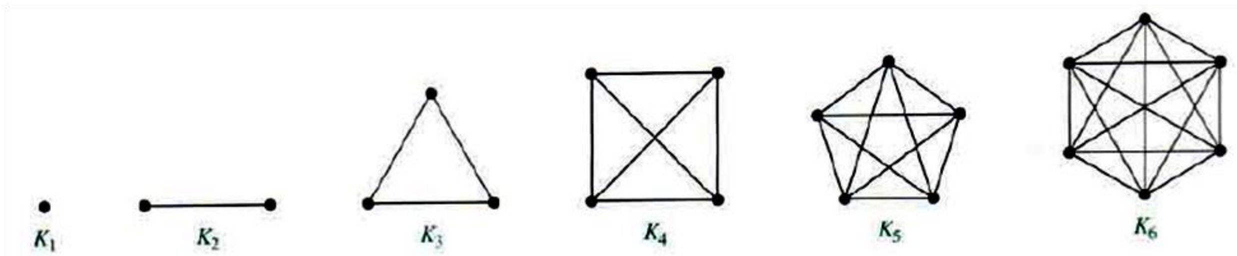
3.2

Special Types of Graphs and Representation of graphs

Some special simple Graphs

The following graphs are often used as examples and arise in many applications.

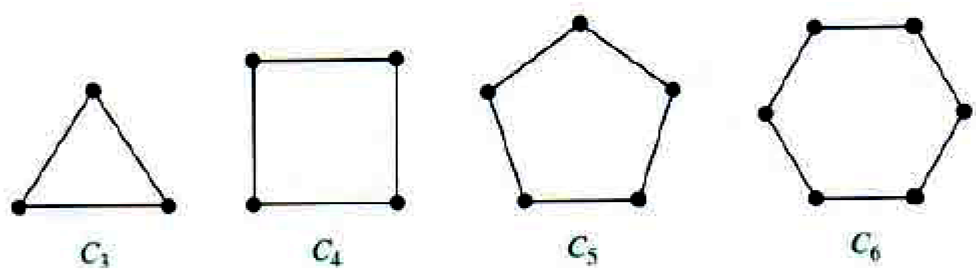
Complete Graphs: The complete graph on n vertices, denoted by K_n is the simple graph that contains exactly one edge between each pair of distinct vertices. The following are the complete graphs K_n , for $n = 1,2,3,4,5,6$:



In K_n ,the number of vertices is n, the number of edges is ${}^{n}C_2$ and the degree of each vertex is $n - 1$.

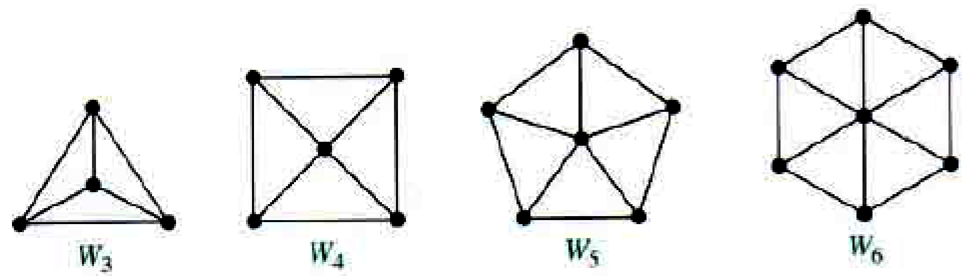
Cycles: The **cycle C_n** , $n \geq 3$, consists of n vertices $v_1, v_2, \ldots, v_n$ and edges $\{v_1, v_2\}$, $\{v_2, v_3\}$, ...$\{v_{n-1}, v_n\}$ and $\{v_n, v_1\}$.

The following are the cycles C_3 , C_4 , C_5 and C_6.



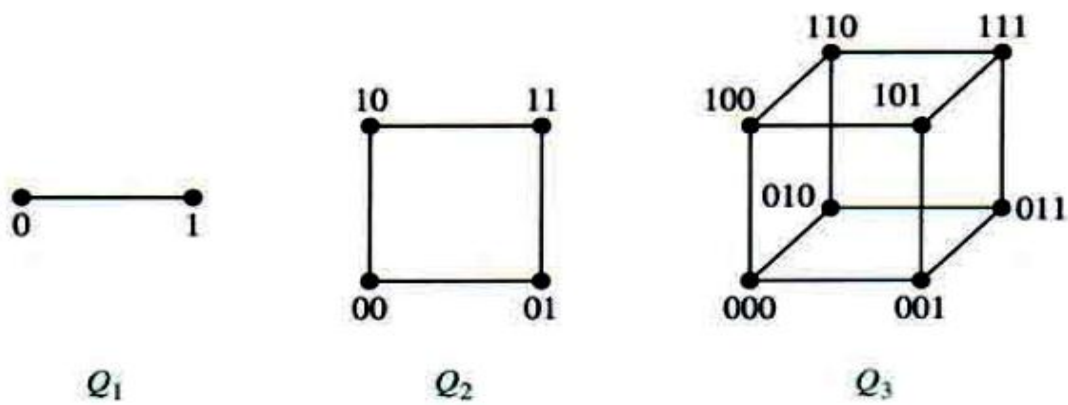
In a cycle graph C_n , $n \geq 3$; the number of vertices is n, the number of edges is n and the degree of each vertex is 2.

Wheels: We obtain the **wheel** when we add an additional vertex to the cycle C_n , for $n \geq 3$, and connect this new vertex to each of the n vertices in C_n , by new edges. The wheels W_3, W_4, W_5 , and W_6 are shown below.



In a wheel graph W_n , $n \geq 3$; the number of vertices is $n + 1$, the number of edges is $2n$ and the degree of each vertex, except the additional vertex is 3 and the degree of the additional vertex is n.

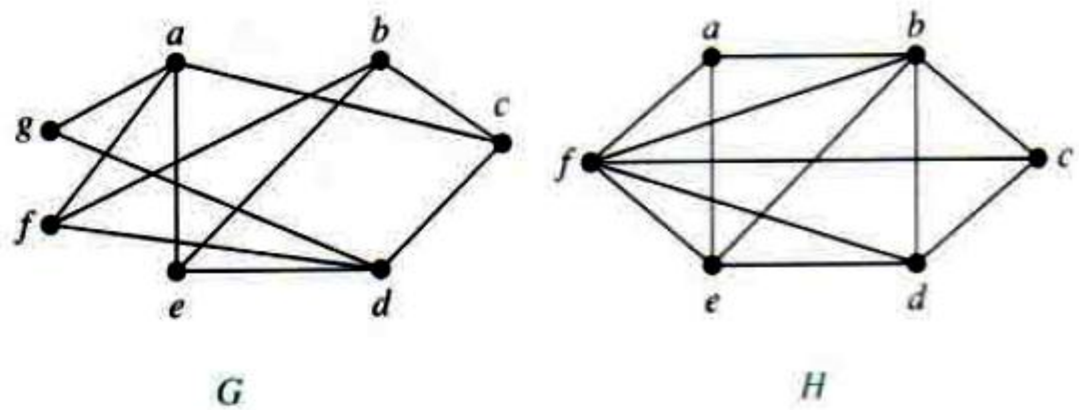
***n*-cubes:** The ***n*-cube** or the ***n*-dimensional hypercube**, denoted by Q_n; is the graph that has vertices representing the 2^n bit strings of length n. Two vertices are *adjacent* iff the strings that they represent differ in exactly one bit position. The graph Q_1, Q_2 and Q_3 are shown below:



Note: The $(n + 1) -$ cube Q_{n+1} can be constructed from the n-cube Q_n by making two copies of Q_n , prefacing the labels on the vertices with a 0 in one copy of Q_n and with a 1 in the other copy of Q_n and connecting two vertices that have labels differing only in the first bit by edges.

Bipartite graphs: A simple graph $G = (V, E)$ is called **bipartite** ,if its vertex set V can be partitioned into two disjoint sets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2). If this condition holds, then we call the pair (V_1, V_2) a **bipartition** of the vertex set V of G.

Example 1: Are the graphs G and H, shown below are bipartite?



Solution:

(i) Graph G is bipartite because its vertex set $V = \{a, b, c, d, e, f, g\}$ is the union of two disjoint sets $V_1 = \{a, b, d\}$ and $V_2 = \{c, e, f, g\}$ and each edge of G connects a vertex of V_1 to a vertex of V_2.
Note: A graph G to be bipartite it is not necessary that every vertex of V_1 be adjacent to every vertex of V_2. In this case b, g are not adjacent.

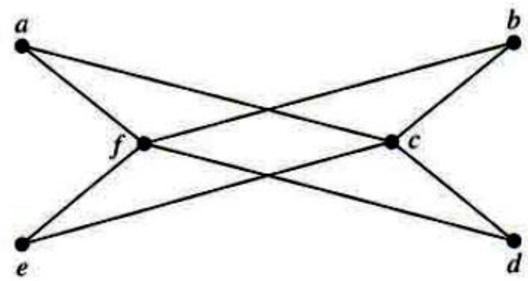
(ii) The graph H is not bipartite because its vertex set $V = \{a, b, c, d, e, f\}$ cannot be partitioned into two subsets so that edges do not connect two vertices of the same set.

The following theorem provides a useful criterion for determining whether a given simple graph is bipartite.

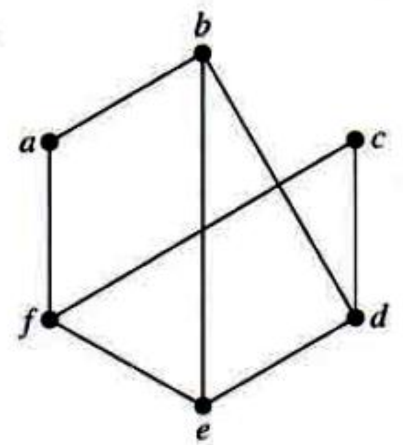
Theorem 1: A simple graph is bipartite iff it is possible to assign one of two different colours to each vertex of the graph so that no two adjacent vertices are assigned the same colour.

Note: This theorem is an example of a result in graph colourings. Graph colourings are an important part of graph theory with important applications.

Example 2: Determine whether the following graphs are bipartite using Theorem 1.



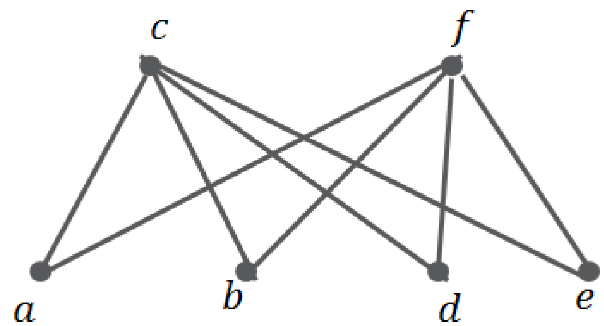
G



H

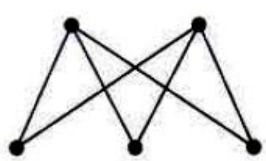
Solution:

(i) We first consider the graph G. We take two colours, **red**, **blue** and assign one of the two colours to each vertex in G. We begin and arbitrarily assign red to a. Then we must assign blue to c and f because each of these vertices is adjacent to a. We assign red to all vertices adjacent to c and f. We have now assigned colours to all vertices of G, with c and f blue and a, b, d and e are red. Note that every edge connected a red vertex and a blue vertex. Therefore, by Theorem 1, G is bipartite and it can be redrawn as

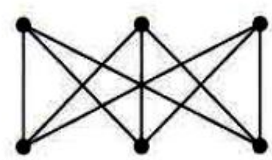


(ii) We now consider the graph H. We take two colours, red, blue and assign one of the two colours to each vertex in H. We begin and arbitrarily assign red to a. Then we must assign blue to b and f because each of these vertices is adjacent to a. Now d, e are adjacent to b, we assign red to d, e. Now note that d, e are adjacent and assigned the same colour red. Therefore, H is not bipartite by Theorem 1.

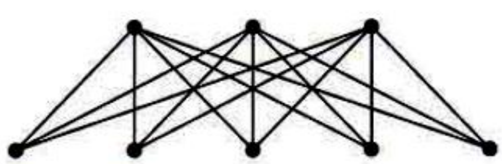
Complete bipartite graphs: The complete bipartite graph, denoted by $\boldsymbol{K_{m,n}}$, is the graph that has its vertex set partitioned into two subsets V_1 and V_2 of m and n vertices respectively. There is an edge between two vertices iff one vertex is in V_1 and the other vertex is in V_2. ($i.e.$, each vertex in V_1 is adjacent to every vertex in V_2. Therefore, there are $m + n$ vertices and mn edges in $K_{m,n}$ and $\deg(v) = n$ when $v \in V_1$, $\deg(v) = m$ when $v \in V_2$).The following are the complete bipartite graphs $K_{2,3}$, $K_{3,3}$, $K_{3,5}$ and $K_{2,6}$.



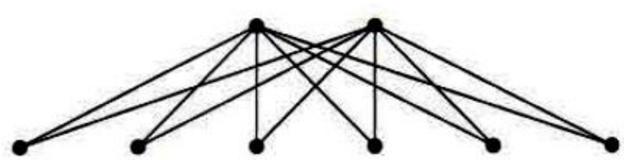
$K_{2,3}$



$K_{3,3}$



$K_{3,5}$

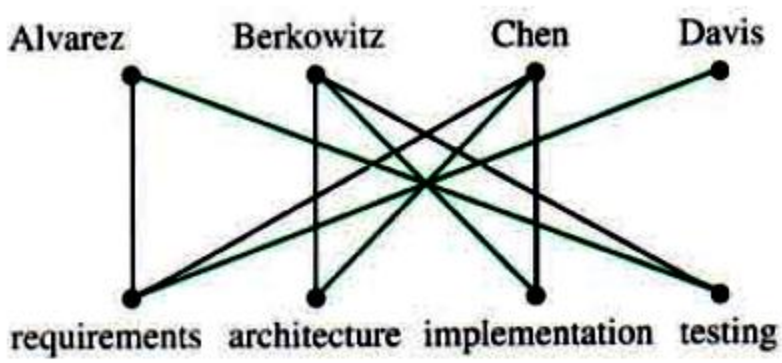


$K_{2,6}$

Some applications of special types of graphs

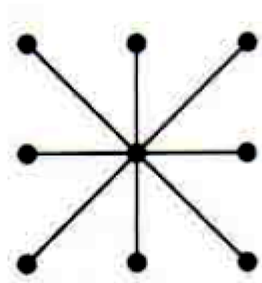
Job assignments: Suppose that there are m employees in a group and j different jobs that need to be done where $m \leq j$. Each employee is trained to do one or more of these j jobs. We represent each employee by a vertex and each job by a vertex. For each employee, we include an edge from the vertex representing that employee to the vertices representing all jobs that the employee has been trained to do.

Note that the vertex set of this graph can be partitioned into two disjoint sets, the set of vertices representing employees and the set of vertices representing the jobs, and each edge connects a vertex representing an employee to a vertex representing a job. Thus it represents a bipartite graph.



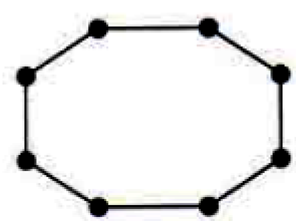
Local Area Networks (LANs)

The various computers in a building, such as minicomputers and personal computers, as well as peripheral devices such as printers and plotters can be connected using a local area network. Some of these networks are based on a star topology where all devices are connected to a central control device. A local area network can be represented using a complete bipartite graph $K_{1,n}$ as shown below:



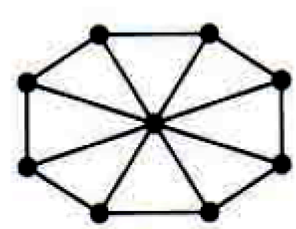
Star topology for LANs

Other local area networks are based on a ring topology, where each device is connected to exactly two others. Local area networks with a ring topology are modeled using n-cycles, C_n as shown below: Messages are sent from device to device around the cycle until the intended recipient of a message is reached.



Ring topology for LANs

Some LANs use hybrid of these two topologies. Messages may be sent around the ring, or through a central device. This redundancy makes the network more reliable. LANs with this redundancy can be modeled using wheels W_n as shown below:



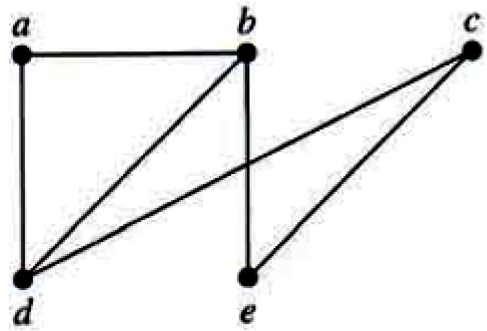
Hybrid topology for LANs

Complete graphs K_n and hypercubes Q_n have applications in interconnection networks for parallel computation.

Representation of Graphs- Adjacency Lists

One way to represent a graph without multiple edges is to list all the edges of the graph. Another way to represent a graph with no multiple edges is the use of **adjacency lists**, which specify the vertices that are adjacent to each vertex of the graph.

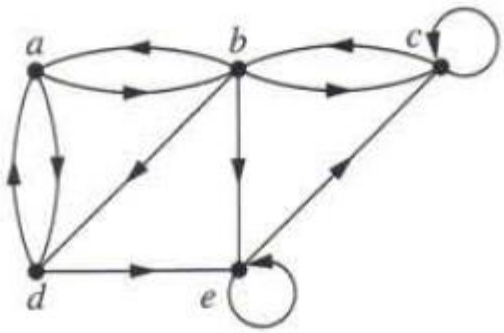
Example 3: Use an adjacency list to represent the following graph:



Solution: We list those vertices adjacent to each of the vertices of the graph.

Adjacency list of the given digraph	
Vertex	Adjacent vertices
a	b, d
b	a, d, e
c	d, e
d	a, b, c
e	b, c

Example 4: Use an adjacency list to represent the given digraph.



Solution: We represent the digraph by listing all the vertices that are the terminal nodes of edges starting at each vertex of the graph.

Adjacency list of the given digraph	
Initial vertex	Terminal vertices
a	b, d
b	a, c, d, e
c	b, c
d	a, e
e	c, e

Representation of Graphs- Adjacency Matrices

Carrying out graph algorithms using the representation of graphs by lists of edges, or by adjacency list, can be cumbersome if there are many edges in the graph. To simplify computation, graphs can be represented using matrices.

Two types of matrices are commonly used to represent the graphs. One is based on the adjacency of vertices and the other is based on the incidence of vertices and edges.

Adjacency matrix of a simple graph: Let $G = (V, E)$ be a simple undirected graph, where $|V| = n$. Suppose that the vertices of V are ordered and listed as $v_1, v_2, \dots, v_n$. The adjacency matrix of G w.r.t this ordering is the $n \times n$ zero-one matrix, denoted by $\boldsymbol{A}$ or $\boldsymbol{A_G}$ where $A = (a_{ij})_{n\times n}$ defined by

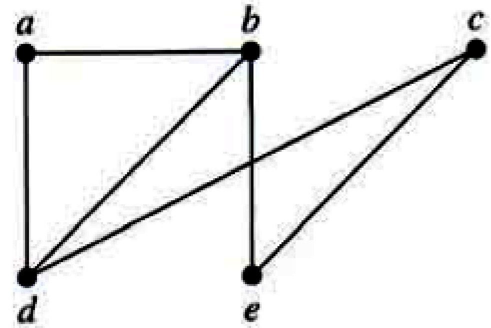
$$a_{ij} = \begin{cases} 1 & if\ \{v_i, v_j\}\ is\ an\ edge\ of\ G \\ 0 & otherwise \end{cases}$$

Note:

(i) The adjacency matrix of a simple undirected graph is a Boolean matrix and it is symmetric.

(ii) The adjacency matrix of a graph is bases on the ordering of the vertices. Therefore, there are $n!$ different adjacency matrices for a graph with n vertices, because there are $n!$ different orderings of n vertices.

Example 5: Represent the following graph with an adjacency matrix.



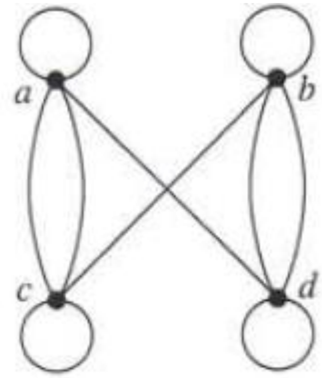
Solution: We order the vertices as a, b, c, d, e. The adjacency matrix A of the graph w.r.t. this ordering is the following Boolean matrix of order 5.

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

Adjacency matrix of multigraphs: Adjacency matrices can also be used to represent undirected graphs with loops and with multiple edges. A loop at the vertex v_i is represented by a 1 at the $(i, i)^{th}$ position of the adjacency matrix. When multiple edges are present, the adjacency matrix is no longer a zero-one matrix, because the $(i, j)^{th}$ entry of the adjacency matrix is the number of edges that are associated with the edge $\{v_i, v_j\}$.

All undirected graphs have symmetric adjacency matrices.

Example 6: Represent the following graph using an adjacency matrix.



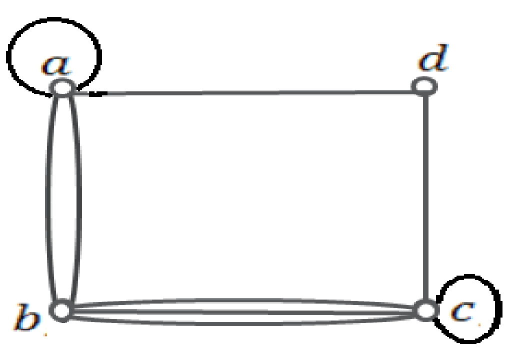
Solution: The adjacency matrix using the ordering of vertices a, b, c, d is

$$A = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}$$

Example 7: Draw an undirected graph represented by the following adjacency matrix.

$$A = \begin{bmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 3 & 0 \\ 0 & 3 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Solution: We draw the graph w.r.t the ordering of the vertices a, b, c, d.



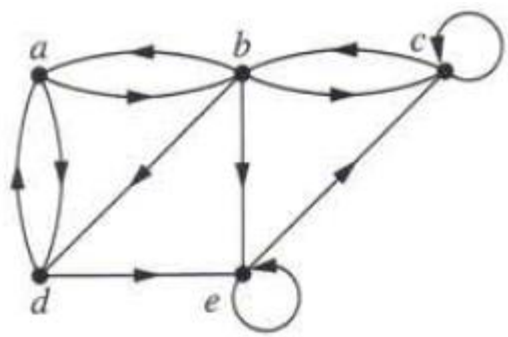
Adjacency matrix of simple digraphs:

Let $G = (V, E)$ be a simple digraph with $|V| = n$. Suppose that the vertices of V are ordered and listed as $v_1, v_2, \dots, v_n$. The $n \times n$ matrix $A = \left(a_{ij}\right)_{n\times n}$ is the adjacency matrix of the simple digraph G if

$$a_{ij} = \begin{cases} 1 & if\ \ (v_i, v_j)\ is\ an\ edge\ of\ G \\ 0 & \qquad otherwise \end{cases}$$

Note: The adjacency matrix of a simple directed graph is a Boolean matrix and it does not have to be symmetric, because there may not be an edge (v_j, v_i) when there is an edge (v_i, v_j).

Example 8: Represent the following digraph with an adjacency matrix.

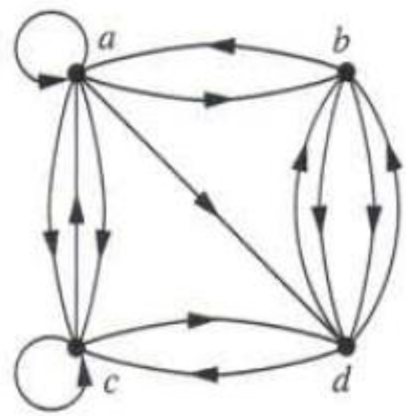


Solution: The adjacency matrix using the ordering of vertices a, b, c, d, e is

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

Adjacency matrices can also be used to represent directed multigraphs. In the adjacency matrix $A = \left(a_{ij}\right)$ for a directed multigraph, a_{ij} is the number of edges that are associated to the edge $(v_i\ , v_j)$. Such matrices are not zero-one matrices and not symmetric in general.

Example 9: Represent the following directed multigraph using an adjacency matrix:



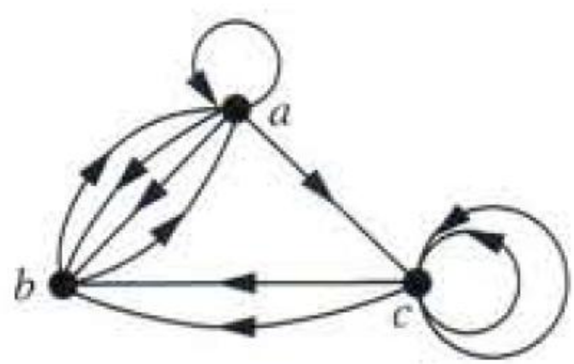
Solution: The adjacency matrix using the ordering of vertices a, b, c, d is

$$A = \begin{bmatrix} 1 & 1 & 2 & 1 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 1 & 1 \\ 0 & 2 & 1 & 0 \end{bmatrix}$$

Example 10: Draw the digraph represented by the following adjacency matrix

$$A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 0 \\ 0 & 2 & 2 \end{bmatrix}$$

*Solution***:** We draw a digraph with the given adjacency matrix w.r.t the ordering of vertices a, b, c.



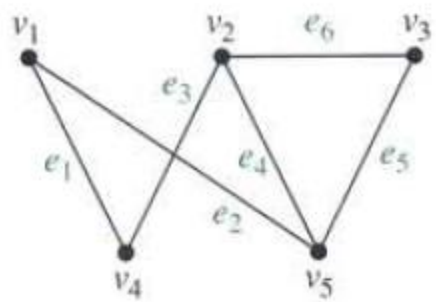
Representation of graphs-Incidence Matrices

Another common way to represent graphs is to use **incidence matrices**.

Let $G = (V, E)$ be an undirected graph. Let $v_1, v_2, \dots, v_n$ be vertices and $e_1, e_2, \dots, e_m$ be its edges. Then the incidence matrix w.r.t this ordering of vertices of V and edges of E is the $n \times m$ matrix $\boldsymbol{M} = \left(\boldsymbol{m_{ij}}\right)_{\boldsymbol{n\times m}}$, where

$$\boldsymbol{m_{ij}} = \begin{cases} \mathbf{1} & \boldsymbol{when\ edge\ e_j\ incident\ with\ vertex\ v_i} \\ \mathbf{0} & \boldsymbol{otherwise} \end{cases}$$

Example 11: Represent the following simple graph with an incidence matrix.

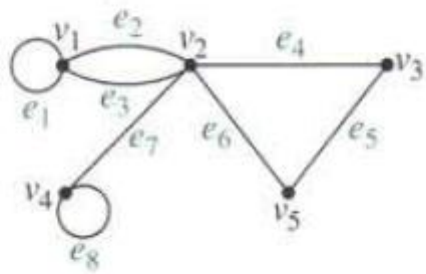


Solution: The incidence matrix using the ordering of vertices v_1, v_2, v_3, v_4, v_5 and edges $e_1, e_2, \dots, e_6$ is

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

It is easy to write column wise. For example e_1, incident with v_1 and v_4.

Example 12: Represent the following multigraph with an incidence matrix.



Solution: The incidence matrix using the ordering of vertices v_1, v_2, v_3, v_4, v_5 and edges $e_1, e_2, \dots, e_8$ is

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

Trade-offs between adjacency lists and adjacency matrices:

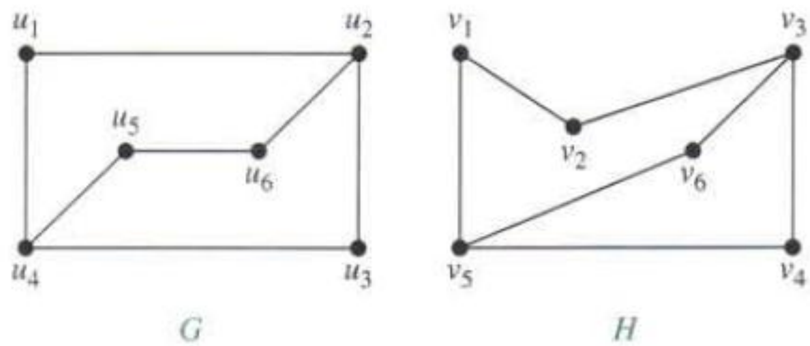
When a simple graph (with n vertices) contains relatively few edges, it is usually preferable to use adjacency lists rather than adjacency matrix to represent the graph. If each vertex has degree not exceeding c, where c is much less than n, then there are cn terms in the adjacency list of the graph. On the other hand, the adjacency matrix for the graph has n^2 entries (where cn is much less than n^2)

If a simple graph contains more than half of all possible edges then using an adjacency matrix to represent the graph is usually preferable over using the adjacency lists. This may be seen by comparing their complexities.

Isomorphic graphs and adjacency matrices:

Let $G = (V, E)$ and $G' = (V', E')$. To show that $f: V \longrightarrow V'$ is an isomorphism, we need to show that f preserves the presence and absence of edges. One helpful way to do this is to show that the adjacency matrix of G is the same as the adjacency matrix of H with rows and columns labeled by the images under f of the corresponding vertices of G.

Example 13: Determine whether the following G and H are isomorphic.



Solution: Both G and H are undirected graphs and both have six vertices and seven edges. Further, both have the degree sequence 3, 3, 2, 2, 2, 2.

Notice that in G, $deg(u_1) = 2, u_1$ is not adjacent to any other vertex of degree two and u_1 is adjacent to two vertices u_2, u_4 of degree 3.

In H the vertices with the above characters are v_4 and v_6. We arbitrarily set $f(u_1) = v_4$. Since u_2 is adjacent to u_1, the possible images of u_2 are v_3 and v_5. We arbitrarily set $f(u_2) = v_3$. Considering adjacency and degree we continue and set $f(u_3) = v_6, f(u_4) = v_5, f(u_5) = v_1, f(u_6) = v_1$.

Thus, f is a bijection from the vertex set of G to the vertex set of H. To verify whether f preserves the adjacency, we write down the adjacency matrices of G and H.

The adjacency matrix A_G of G w.r.t the ordering of the vertices $u_1, u_2, \dots, u_6$ and A_H of H w.r.t the ordering of the vertices $v_4, v_3, v_6, v_5, v_1, v_2$ are

$$A_{G=}\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} = A_H$$

This shows that f preserves the adjacency. Thus, f is an isomorphism and $G \cong H$.

Note that $f(u_1) = v_6, f(u_2) = v_3, f(u_3) = v_4, f(u_4) = v_5, f(u_5) = v_1, f(u_6) = v_2$ is also an isomorphism. Try others!

Example 14: Are the simple graphs with the following adjacency matrices isomorphic?

$a)$ $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

$b)$ $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

$c)$ $\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

Solution: Let G, H be simple graphs and let A_G, A_H be their adjacency matrices, where $A_G = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, A_H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Notice that both G, H have the 3 vertices and 4 edges. Now,

$$A_H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \xleftrightarrow{R_1 \leftrightarrow R_3} \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix} \xleftrightarrow{C_1 \leftrightarrow C_3} \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = A_G$$

(Note that for each exchange of rows, we have to immediately perform the corresponding exchange of columns: exchange of row and column operations are only to be performed)

Aliter:

a) Let the vertices of H be p, q, r. Let A_H be the adjacency matrix of H w.r.t the ordering of vertices p, q, r. Now, the adjacency matrix B of H w.r.t the ordering of the vertices r, q, p.

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

Thus, $G \cong H$.

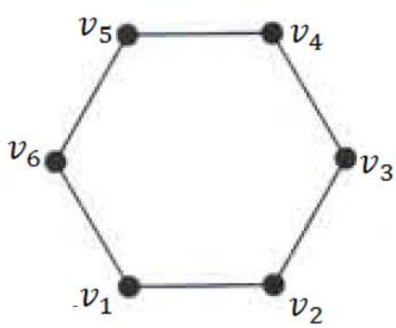
b) Notice that the first graph has 8 edges and the second graph has 10 edges. Therefore, the graphs are not isomorphic.

c) Notice that the first graph has 8 edges and the second graph has 6 edges. Therefore, the graphs are not isomorphic.

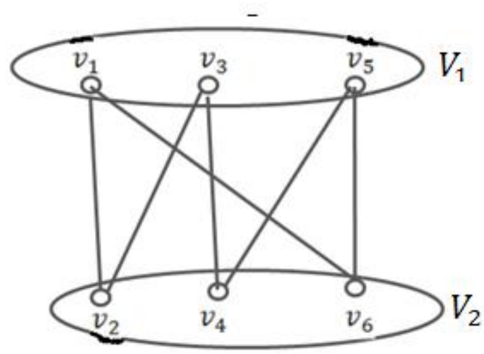
P1:

Is the Cycle C_6 bipartite?

Solution:



C_6



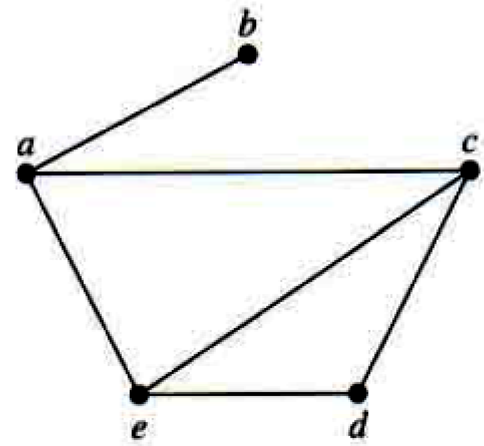
G

The vertex set $V = \{v_1, v_2, \dots, v_6\}$ can be partitioned into the sets $V_1 = \{v_1, v_3, v_5\}$ and $V_2 = \{v_2, v_4, v_6\}$.Note that edges of C_6 connects every vertex of V_1 and a vertex V_2 and no two vertices of V_1 and V_2 are adjacent (see the diagram of G). Therefore, C_6 is bipartite.

Is C_7 bipartite?

P2:

Use an adjacency list to represent the following graph:



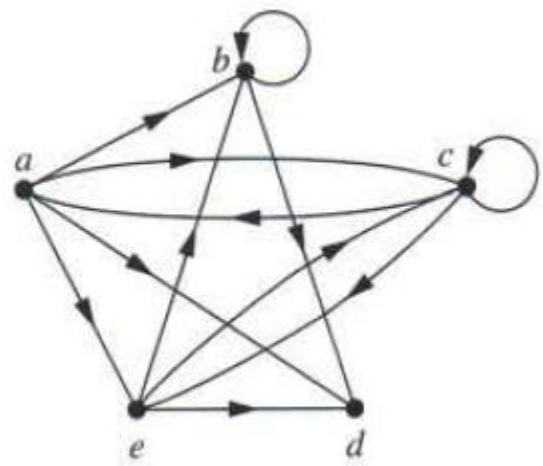
Solution:

We list those vertices adjacent to each of the vertices of the graph.

Adjacency list of the given digraph	
Vertex	Adjacent vertices
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

P3:

Use an adjacency list to represent the given digraph



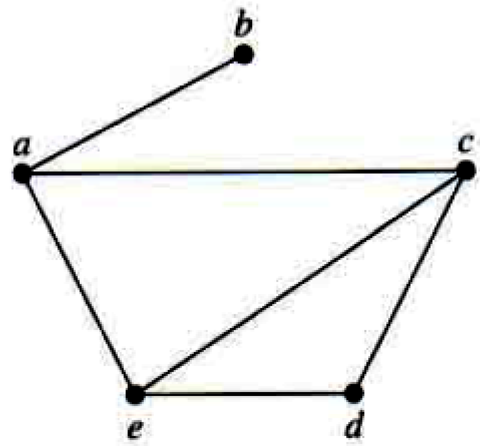
Solution:

We represent the digraph by listing all the vertices that are the terminal nodes of edges starting at each vertex of the graph.

Adjacency list of the given graph	
Initial vertex	Terminal vertices
a	b, c, d, e
b	b, d
c	a, c, e
d	$-$
e	b, c, d

P4:

Represent the following graph with an adjacency matrix



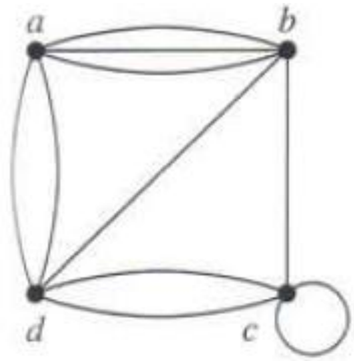
Solution:

We order the vertices as a, b, c, d, e. The adjacency matrix A of the graph w.r.t. this ordering is the following Boolean matrix of order 5.

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

P5:

Represent the following graph using an adjacency matrix.



Solution:

The adjacency matrix using the ordering of vertices a, b, c, d is

$$A = \begin{bmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 \end{bmatrix}$$

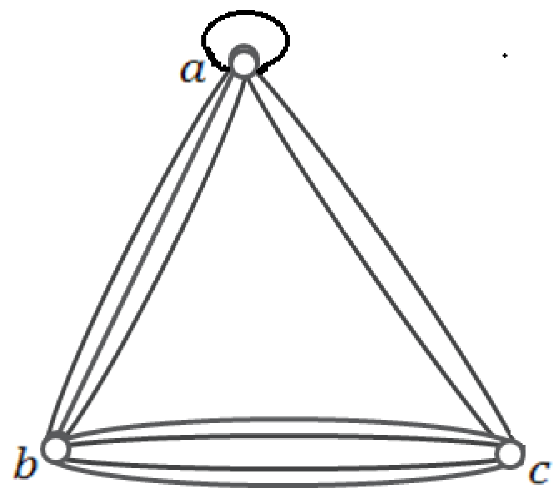
P6:

Draw an undirected graph represented by the following adjacency matrix.

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

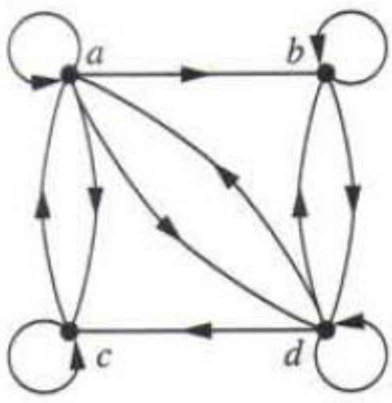
Solution:

We draw the graph w.r.t the ordering of the vertices a, b, c.



P7:

Represent the following digraph with an adjacency matrix.



Solution:

The adjacency matrix using the ordering of vertices a, b, c, d is

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

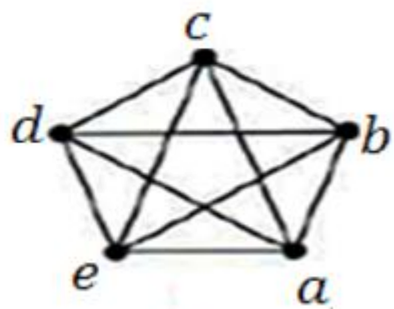
P8:

Represent each of these graphs with an adjacency matrix.

a) K_5 b) $K_{2,3}$ c) C_5 d) W_5 e) Q_3

Solution:

a) K_5

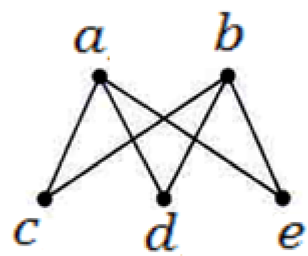


K_5

The ordering of the vertices is a, b, c, d, e. Then the adjacency matrix of K_5 is

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

b) $K_{2,3}$

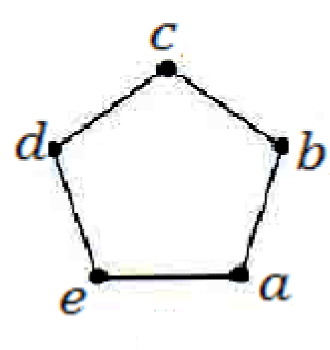


$K_{2,3}$

The vertices are ordered as a, b, c, d, e. Then the adjacency matrix w.r.t this ordering is

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

c) C_5

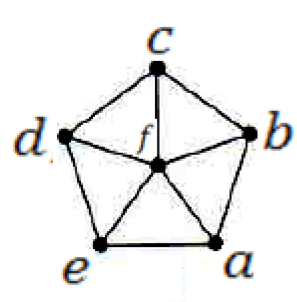


C_5

The vertices are ordered as a, b, c, d, e. The adjacency matrix w.r.t this ordering is

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

d) W_5



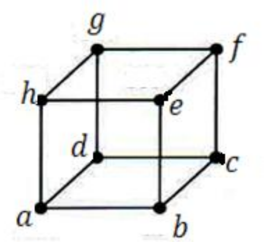
W_5

The vertices are ordered as a, b, c, d, e, f. The adjacency matrix w.r.t this ordering is

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

e) Q_3

The vertices are ordered as a, b, c, d, e, f, g, h. The adjacency matrix w.r.t this ordering is



Q_3

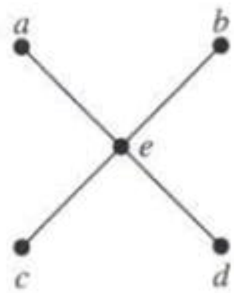
$$A = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

3.2

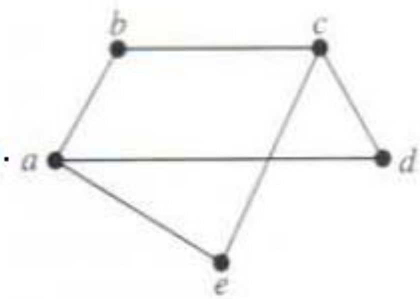
Exercise:

1. Determine whether the following graphs are bipartite by using Theorem 1.

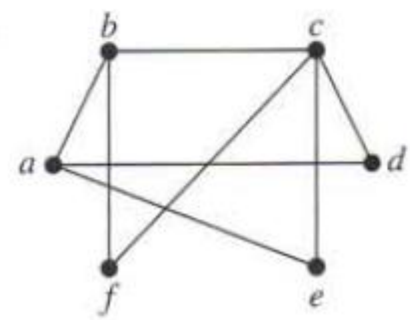
a.



b.



c.

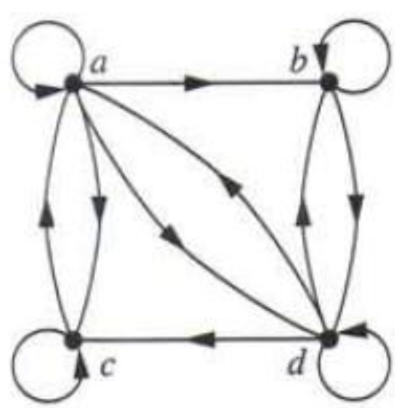


2. Draw the following graphs
   a. K_7 b. $K_{1,8}$ c. $K_{4,4}$ d. C_7 e. W_7 f. Q_4

3. Use an adjacency list to represent the given graph

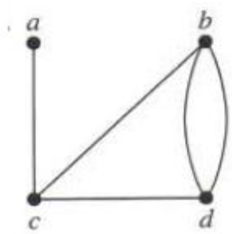
a

b

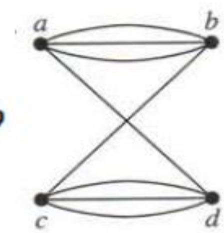


4. Represent the above graph 3 (a) & (b) with their adjacency matrices.
5. Represent the given graph using an adjacency matrix.

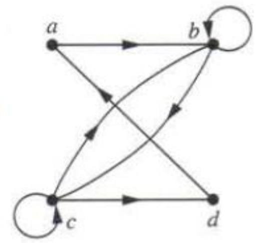
a



b



c



MODULE-3

Isomorphism's, connectivity

3.3

Connectivity

Many problems can be modeled with paths formed by travelling along the edges of graphs. Problems of efficiently planning routes for mail delivery, garbage pickup, diagnostics in computer networks can be solved using models that involve paths in graphs.

Paths

A **path** is a sequence of edges that begins at a vertex of a graph and travels from vertex to vertex along edges of the graph.

The following is a formal definition of a path in an undirected graph:

A path in an undirected graph: Let G be an undirected graph and n be a nonnegative integer. A **path of length $\boldsymbol{n}$** from a vertex u to a vertex v in G is a sequence of n edges $e_1, e_2, \dots, e_n$ of G such that e_1 is associated with $\{x_0, x_1\}$, e_2 is associated with $\{x_1, x_2\}$, and so on, finally e_n is associated with $\{x_{n-1}, x_n\}$, where $x_0 = u$ and $x_n = v$. Such a path is said to *pass through* the vertices $x_1, x_2, \dots, x_{n-1}, x_n$ or *traverse* the edges $e_1, e_2, \dots, e_n$. If the graph G is simple, then we denote this path by its sequence of vertices $x_0, x_1, x_2, \dots, x_n$.

Note that a path of length *zero* consists of a single vertex

Circuit: A path is a **circuit** if it begins and ends at the same vertex, (*i.e.*, $= v$) and the length $n > 0$.

Simple path: A path or a circuit is said to be **simple** if it does not contain the same edge more than once.

Example 1: In the following simple undirected graph (figure 1), a, d, c, f, e is a simple path from a to e of length 4, because the edges $\{a, d\}, \{d, c\}, \{c, f\}, \{f, e\}$ are all distinct.

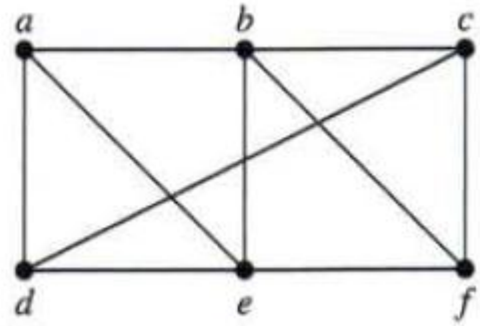


Figure 1

Notice that d, e, c, a is not a path, because $\{e, c\}$ is not an edge.

The path b, c, f, e, b is a circuit of length 4, because it is a path of length 4 that begins and ends at b.

Note that a, b, e, f, c, d, e, b is a path of length 7 and it is not simple because it has the edge $\{b, e\}$ occurs twice in the path.

The following is the definition of a path in a digraph.

A path in a digraph: Let G be a digraph and n be a nonnegative integer .A path of length n from u to v in G is a sequence of edges $e_1, e_2, \dots, e_n$ of G such that e_1 is associated with the directed edge (x_0, x_1), e_2 with (x_1, x_2), and so on, e_n is associated with (x_{n-1}, x_n), where $x_0 = u$ and $x_n = v$. When there are no multiple edges in the digraph G, this path is denoted by its vertex sequence $x_0, x_1, x_2, \dots, x_n$.

A path of length greater than zero that begins and ends at the same vertex is called a **circuit.**

A path or circuit is said to be **simple** if it does not contain the same edge more than once.

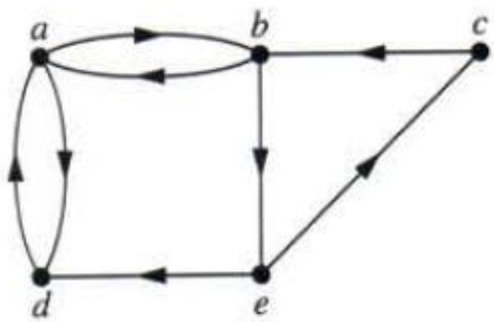
Note:

(1) The alternate terminology for path, circuit and simple path are *walk*, *closed walk* and *trail* respectively.

(2) There may be more than one path from the initial vertex u to the terminal vertex v.

(3) Paths represent useful information in many graph models.

Example 2: In the following digraph



(i) a, b, e, c, b is a path of length 4 and it is simple.

(ii) a, b, e, d, a is a circuit of length 4 and it is simple.

(iii) c, b, a, b, e, c, b is a circuit of length 6 but it is not simple, because it contains the edge (c, b) twice.

(iv) a, d, e, c is not a path, because (d, e) is not an edge in the digraph

Connectedness in undirected graphs

When does a computer network have the property that every pair of computers can share information, if messages can be sent through one or more intermediate computers? If computers are represented by vertices and communication links represent edges then the computer network represents an undirected graph and the question now becomes: Is there a path between every pair of vertices in the graph?

Undirected connected graph: An undirected graph G is said to be **connected** if there is a path between every pair of distinct vertices of G.

Thus, any two computers in the network can communicate if and only if the graph of the network is connected.

Example 3: The graph G given in figure 1 is connected, because there is a path between every pair of distinct vertices.

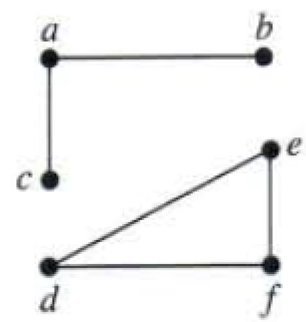
The following is a useful result:

Theorem 1: In a connected undirected graph, there is a simple path between every pair of vertices.

Connected component: A **connected component** of a graph G is a connected subgraph of G that is not a subgraph of another connected subgraph of G. That is, a connected component of a graph G is a maximal connected subgraph of G.

If a graph G is not connected then it has two or more connected components that are disjoint and have G as their union. That is, if G is not connected then G is partitioned into connected components.

Example 4: The following graph is not connected, because there is no path between the vertices a and d.



G

Its connected subgraphs are the subgraphs H_1 and H_2 , where

$$H_1 = (V_1, E_1), V_1 = \{a, b, c\}, E_1 = \{\{a, b\}, \{a, c\}\} \text{ and}$$
$$H_2 = (V_2, E_2), V_2 = \{d, e, f\}, \ E_2 = \{\{d, e\}, \{d, f\}, \{e, f\}\}.$$

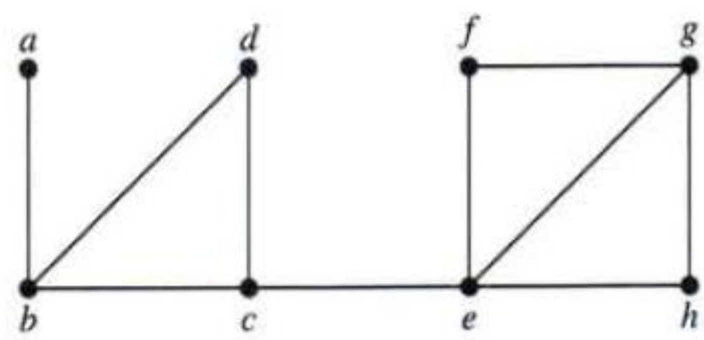
Notice that H_1 and H_2 are maximal connected sub graphs. Therefore, H_1, H_2 are components and G is partitioned into H_1 and H_2.

Cut vertex: The removal of a vertex a and all edges incident with it in a graph G produces a subgraph of G with more connected components than in G. Then such a vertex a is called a **cut vertex** or a **articulation point.**

Note that the removal of a cut vertex from a connected graph produces a subgraph that is not connected.

Cut edge: An edge whose removal produces a graph with more connected components than the original graph is called a **cut edge** or a **bridge**.

Example 5: Find all cut vertices and all cut edges in the following graph.



Solution: The removal of the vertex b and all edges that incident with b, i.e., $\{b, a\}$, $\{b, d\}$, $\{b, c\}$ disconnects the graph. (Note that remove the edges that incident with b only but not the other end vertices namely a, d and c). Therefore b is a cut vertex. Similarly c and e are also cut vertices.

Removal of the edge $\{a, b\}$ (but not the end points a, b) disconnects the graph. Therefore $\{a, b\}$ is a cut edge. Similarly $\{c, e\}$ is also a cut edge.

Connectedness in Digraphs

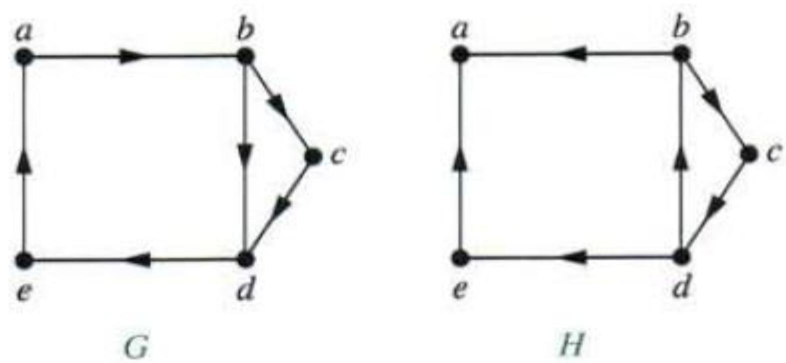
The following are two notions of connectedness in digraphs:

Weakly connectedness: A digraph G is **weakly connected** if there is a path between every pair of distinct vertices in the underlying undirected graph. That is, a digraph G is weakly connected if the undirected graph of G obtained by ignoring the directions of the edges is connected.

Strongly connectedness: A digraph G is **strongly connected** if for every two distinct vertices a and b in G, there is a path from a to b as well as a path from b to a.

Note: Every strongly connected digraph is also weakly connected, but not conversely.

Example 6: Are the following digraphs strongly connected? Are they weakly connected?



Solution: Notice the following in G:

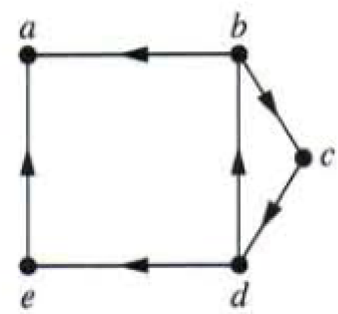
Vertex to vertex	Path
a to b	a, b
b to a	b, d, e, a
a to c	a, b, c
c to a	c, d, e, a
a to d	a, b, c, d
d to a	d, e, a
b to c	b, c
c to b	c, d, e, a, b
b to d	b, d
d to b	d, e, a, b
c to d	c, d
d to c	d, e, a, b, c

Thus for every two distinct vertices , y ;G has a path from x to y as well as a path from y to x. Thus G is strongly connected. Therefore, G is also weakly connected.

The digraph H is weakly connected, because the undirected graph derived from H by ignoring the directions of the edges of G is connected. Further, it is not strongly connected because there is no directed path from b to a

Strongly connected component: A subgraph of a digraph G that is strongly connected but not contained in a larger strongly connected subgraph ($i.e.$, maximal strongly connected subgraph) is called a **strongly connected component** or **strong component** of G

Example 7: The following graph H has three strongly connected components, consisting the vertex a; the vertex e ; and the subgraph consisting of the vertices b, c, d and edges (b, c),(c, d) and (d, b)

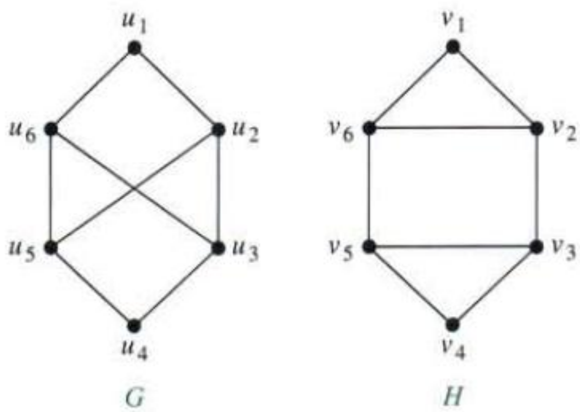


H

Paths and Isomorphism:

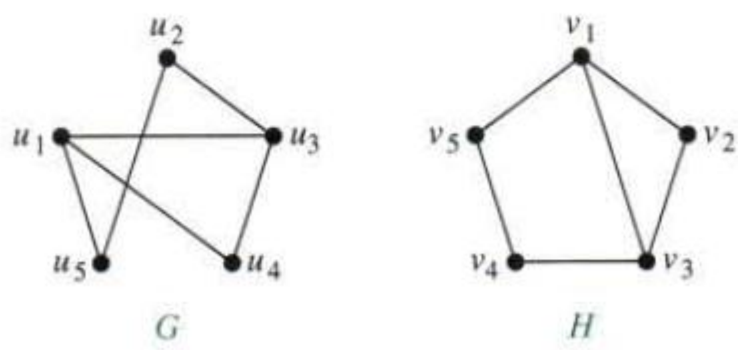
Paths and circuits can help to determine whether two graphs are isomorphic . Paths can be used to construct mapping that may be isomorphisms. A useful isomorphic invariant for simple graphs is the existence of a simple circuit of length k, where k is a natural number greater than 2.

Example 8: Determine whether the following graphs G and H are isomorphic.



Solution: Both the graphs G and H are undirected graphs with six vertices and eight edges. Both have the degree sequence 3,3,3,3,2,2. Notice that H has a simple circuit v_1, v_2, v_6, v_1 of length 3. Observe that G has no simple circuit of length 3. It may be noted that all simple circuits in G have length atleast 4. Therefore G is not isomorphic to H, because the existence of a simple circuit of length 3 is an isomorphic invariant.

Example 9: Determine whether the following graphs G and H are isomorphic.



Solution: Both the graphs G and H are undirected graphs with five vertices and six edges .Both have the degree sequence 3,3,2,2,2. Further ,both have a simple circuit of length 3, a simple circuit of length 4 and a simple circuit of length 5. Because all these isomorphic invariants agree, the graphs $G$and H may be isomorphic. Observe that the circuit of length 5 in H; $v_3, v_2, v_1, v_5, v_4, v_3$ in which the vertex v_2 of degree 2 is trapped between two vertices of degree 3, $i.e.$, $v_3$and v_1. Notice that the circuit of length 5 in G; $u_1, u_4, u_3, u_2, u_5, u_1$ in a similar circuit with the same characteristics .These paths guide us to set up the following bijection f from the vertex set of G to the vertex set of H.

$$f(u_1) = v_3, f(u_4) = v_2, f(u_3) = v_1, f(u_2) = v_5, f(u_5) = v_4$$

Let A_G and A_H be the adjacency matrices of G and H respectively, w.r.t. the ordering of the vertices.

$$u_1, u_4, u_3, u_2, u_5 \text{ in } G \text{ and } v_3, v_2, v_1, v_5, v_4 \text{ in } H$$

We notice that

$$\boldsymbol{A_G} = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{bmatrix} = \boldsymbol{A_H}$$

Thus $G \cong H$

Counting Paths Between Vertices

The number of paths between two vertices in a graph can be determined using its adjacency matrix.

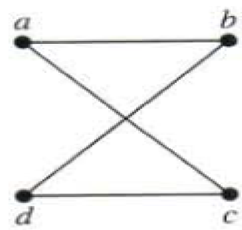
Theorem 2: Let $\boldsymbol{G = (V, E)}$ be any graph with $\boldsymbol{|V| = n}$. Let $\boldsymbol{A}$ be the adjacency matrix of $\boldsymbol{G}$ w.r.t. the ordering of vertices $\boldsymbol{v_1, v_2, v_3, \dots, v_n}$. The number of different paths of length $\boldsymbol{r}$ from $\boldsymbol{v_i}$ to $\boldsymbol{v_j}$ equals the $\boldsymbol{(i, j)}$th entry of $\boldsymbol{A^r}$ (where $\boldsymbol{r}$ is a natural number)

Proof: Follows by mathematical induction.
In the above theorem, directed or undirected edges, multiple edges and loops are allowed in G

Note:

1. In the above theorem A^r denotes the matrix multiplication $A.A.A\dots A(r\ times)$. It is not Boolean product.
2. The above theorem can be used to find the length of the shortest path between two vertices and it can be used to determine whether a graph is connected.

Example 10: How many paths of length *four* are there from a to d in the following simple graph G



Solution: The adjacency matrix of G, w.r.t. the ordering of vertices as a, b, c, d is

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

To determine the number of paths of length 4 between two vertices of G, we have to compute A^4 . Now

$$\boldsymbol{A}^2 = \begin{bmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \end{bmatrix}, \ \boldsymbol{A}^3 = \begin{bmatrix} 0 & 4 & 4 & 0 \\ 4 & 0 & 0 & 4 \\ 4 & 0 & 0 & 4 \\ 0 & 4 & 4 & 0 \end{bmatrix} \text{ and } \boldsymbol{A}^4 = \begin{bmatrix} 8 & 0 & 0 & 8 \\ 0 & 8 & 8 & 0 \\ 0 & 8 & 8 & 0 \\ 8 & 0 & 0 & 8 \end{bmatrix}$$

The number of paths of length 4 from a to d in $(1,4)^{th}$ entry in A^8, $i.e.$, 8

By inspection, we see the following 8 paths from a to d

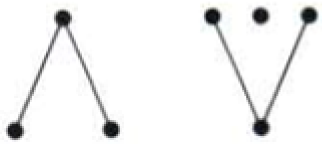
$$a, b, a, b, d \ ; \ a, b, a, c, d \ ; \ a, b, d, b, d \ ; \ a, b, d, c, d$$

$$a, c, a, b, d \ ; \ a, c, a, c, d \ ; a, c, d, b, d \ ; \ a, c, d, c, d$$

P1:

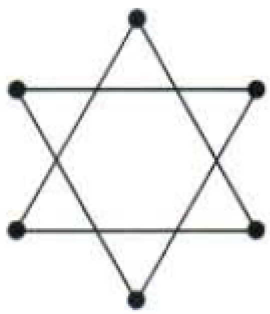
Determine whether the following graphs are connected.

i



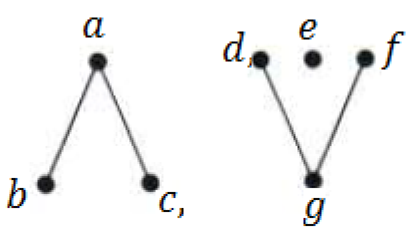
ii

iii



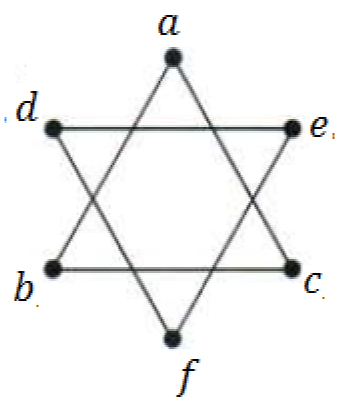
Solution:

i



It is not connected ,because there is no path between the vertices a and d.

$\boldsymbol{ii}$**.** It is connected ; because there is a path between every pair of distinct vertices



It is not connected ,because there is no path between the vertices a and d

2. **How many connected components does each of the above graphs have? For each graph ,find its connected components**.

Solution:

i. There are 3 components .They are

$H_1 = (V_1, E_1)$ where $V_1 = \{a, b, c\}$, $E_1 = \{\{a, b\}, \{a, c\}\}$

$H_2 = (V_2, E_2)$ where $V_2 = \{d, g, f\}$, $E_2 = \{\{d, g\}, \{d, f\}\}$

$H_3 = (V_3, E_3)$ where $V_3 = \{e\}$, $E_3 = \emptyset$

ii. There is one connected component $i.e$, the whole graph , because it is connected

iii. There are two connected components . They are

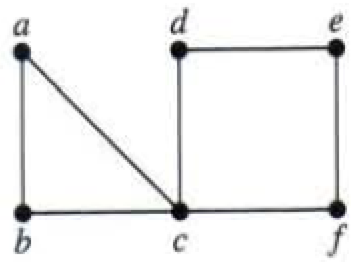
$H_1 = (V_1, E_1)$ where $V_1 = \{a, b, c\}$, $E_1 = \{\{a, b\}, \{a, c\}, \{b, c\}\}$

$H_2 = (V_2, E_2)$ where $V_2 = \{d, e, f\}$, $E_2 = \{\{d, e\}, \{d, f\}, \{e, f\}\}$

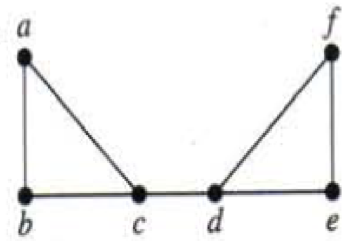
P2:

Find all cut vertices and cut edges of the following graphs

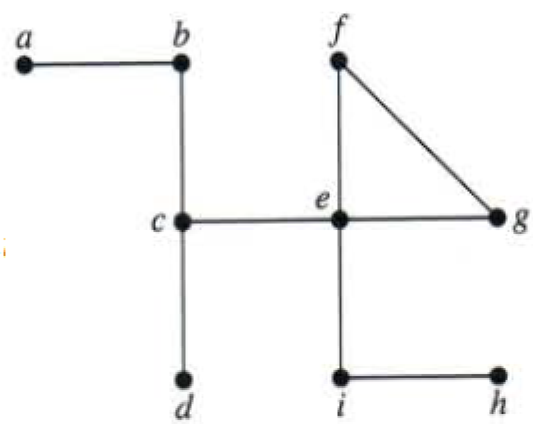
i



ii



iii.



Solution:

$\boldsymbol{i}$. The removal of the vertex c and all edges that incident with c disconnects the graph. Therefore, c is the cut vertex. Further , it is the only cut vertex. Note that the removal of any edge in this graph is not producing a graph with more connected components than the original graph. Therefore , there are no cut edges(bridges) in this graph.

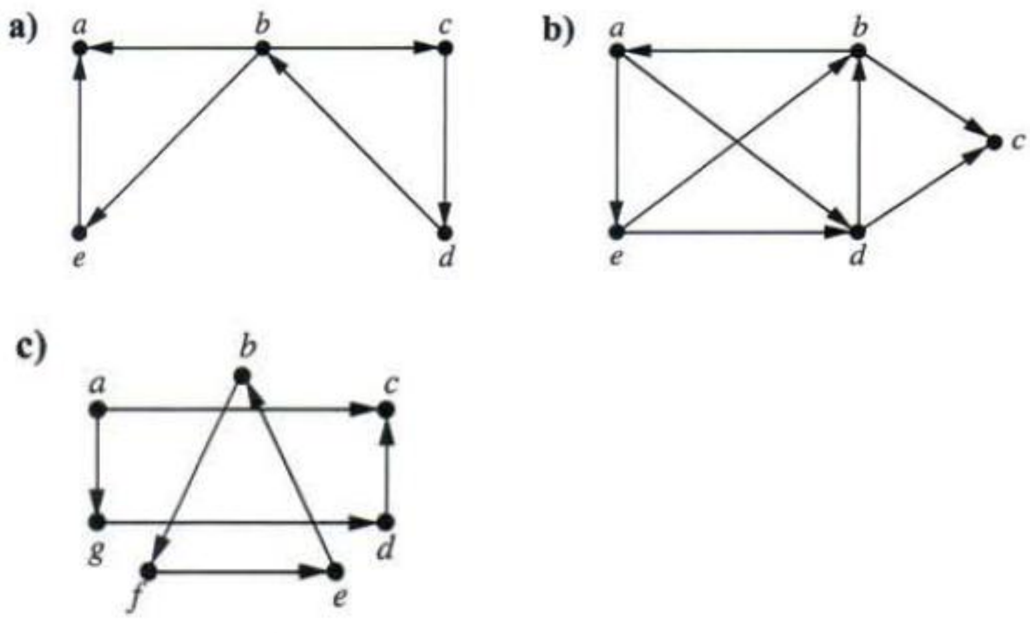
$\boldsymbol{ii}$. The cut vertices are c, d.The cut edge is $\{c, d\}$. The removal of the edge $\{c, d\}$ (not the vertices c and d) disconnects the graph into two connected components.

$\boldsymbol{iii}$. The cut vertices are :b, c, e, i and the cut edges are:

$$\{a, b\}, \{b, c\}, \{c, d\}, \{c, e\}, \{e, i\}, \{i, h\}$$

P3:

Determine whether each of these graphs is strongly connected and if not , whether it is weakly connected.



Solution:

a) The undirected graph derived from this graph by ignoring the directions of the edges is connected. Therefore it is a weakly connected graph. Notice that there is a path from a to b but there is no path from b to a. Therefore it is not strongly connected. Thus, it is a weakly connected graph, but not strongly connected.

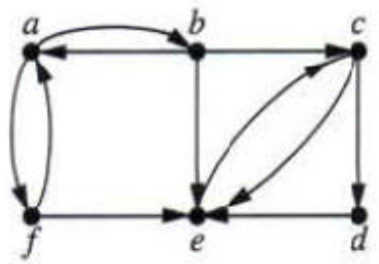
b) It is weakly connected, because the undirected graph derived from it by ignoring the directions of edges is connected. Notice that there is path from a to ; a , $d, c,$ but there is no path from c to a. Therefore, this graph is not strongly connected. Thus, it is a weakly connected graph, but not strongly connected.

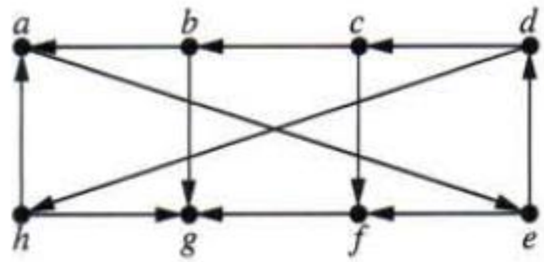
c) Notice that the undirected graph derived from this graph by ignoring the directions of the edges is not connected (because it is portioned into two connected components, one is a rectangle a, c, d, g and the other is a triangle b, e, f. Therefore, it is not weakly connected. Consequently it is not strongly

connected (If it is strongly connected, then it is weakly connected
a contradiction(because every strongly connected graph is a weakly connected).).It is neither weakly connected nor strongly connected.

P4:

Find the strongly connected components of each of these graphs.

a) 

b) 

Solution:

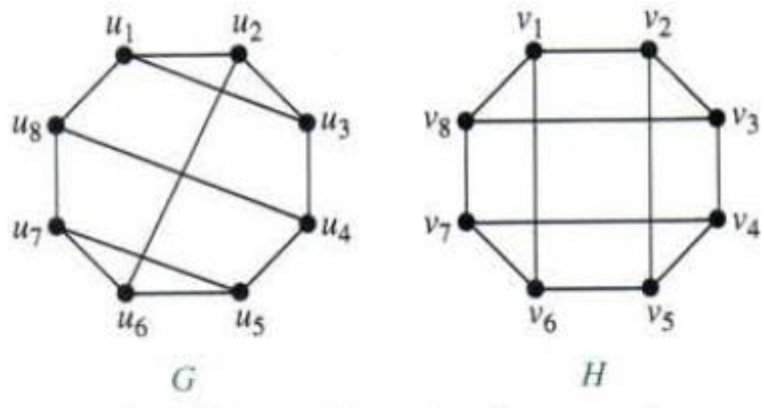
a) First note that there is a path from a to c ,but there is no path from c to a. Therefore it is not strongly connected.
Recall that a strongly connected component of a graph G is a maximal strongly connected subgraph of G
Notice that there are two strongly connected components H_1, H_2 in this graph, where
$H_1 = (V_1, E_1), V_1 = \{a, b, f\}$ and $E_1 = \{(a, b), (b, a), (a, f), (f, a)\}$
$H_2 = (V_2, E_2), V_2 = \{c, d, e\}$ and $E_2 = \{(c, e), (e, c), (c, d), (d, e)\}$

b) Notice that there is no path from g to any vertex. Therefore, $H_1 = (V_1, E_1)$, where $V_1 = \{g\}$ and $E_1 = \emptyset$ is a strongly connected component. Similarly $H_2 = (V_2, E_2)$,where $V_2 = \{f\}$ and $E_2 = \emptyset$ is a strongly connected component.
Notice that a, e, d, c, b, a is a simple circuit and a, e, d, h, a is another simple circuit; there is a interconnecting path a, e, d between these circuits. Thus every two vertices in these circuits are connected. This shows that the subgraph $H_3 = (V_3, E_3)$ is a strongly connected component where

$$V_3 = \{a, b, c, d, e, h\} \text{ and}$$
$$E_3 = \{(a, e), (e, d), (d, c), (c, b), (b, a), (d, h), (h, a)\}$$

P5:

Use paths either to show that these graphs are not isomorphic or to find an isomorphism between them.

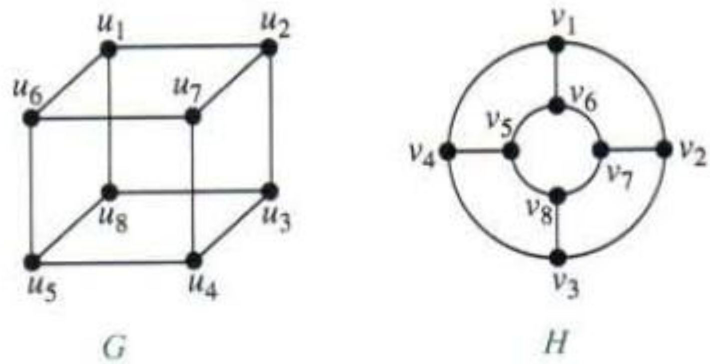


Solution:

Both the graphs G and H are undirected graphs with 8 vertices and 12 edges. Both have the degree sequence 3,3,3,3,3,3,3,3. Notice that G has two simple circuits of length 3 $(u_1, u_2, u_3, u_1$ and $u_5, u_6, u_7, u_5)$. Observe that H has no simple circuit of length 3. Therefore, G is not isomorphic to H,because the existence of a simple circuit of length 3 is an isomorphic invariant.

P6:

Use paths either to show that these graphs are not isomorphic or to find an isomorphism between them.



Solution:

Both the graphs G and H are undirected graphs with 8 vertices and 12 edges. Both have the degree sequence 3,3,3,3,3,3,3,3. Observe that the graphs G and H has the following circuit of length 8 respectively,

$$u_1, u_2, u_7, u_6, u_5, u_4, u_3, u_8, u_1$$

$$v_1, v_2, v_3, v_4, v_5, v_8, v_7, v_6, v_1$$

These circuits guide us to set up the following bijection f from the vertex set of G to the vertex set of H:

$$f(u_1) = v_1, f(u_2) = v_2, f(u_3) = v_7, f(u_4) = v_8, f(u_5) = v_5$$

$$f(u_6) = v_4, f(u_7) = v_3, f(u_8) = v_6$$

Let A_G and A_H be the adjacency matrices of G and H respectively, w.r.t. the ordering of the vertices.

$$u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8 \text{ in } G$$

$$v_1, v_2, v_7, v_8, v_5, v_4, v_3, v_6 \text{ in } H$$

We notice that

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

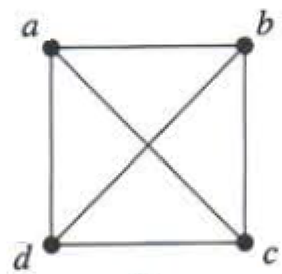
Thus , $G \cong H$

P7:

Find the number of paths of length 3 between two different vertices in K_4

Solution:

We have K_4



K_4

The adjacency matrix of K_4 w.r.t. the ordering of vertices a, b, c, d is

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

To determine the number of paths of length 3 between two vertices of K_4, we have to compute A^3. Now

$$A^2 = \begin{bmatrix} 3 & 2 & 2 & 2 \\ 2 & 3 & 2 & 2 \\ 2 & 2 & 3 & 2 \\ 2 & 2 & 2 & 3 \end{bmatrix}, \qquad A^3 = \begin{bmatrix} 6 & 7 & 7 & 7 \\ 7 & 6 & 7 & 7 \\ 7 & 7 & 6 & 7 \\ 7 & 7 & 7 & 6 \end{bmatrix}$$

The number of paths of length 3 between two different vertices in K_4 is 7

The number of circuits of length 3, from a to a is 6.They are

$$a, b, c, a \;;\quad a, c, b, a \;;\; a, d, c, a$$

$$a, c, d, a \;;\; a, d, b, a \;;\quad a, b, d, a$$

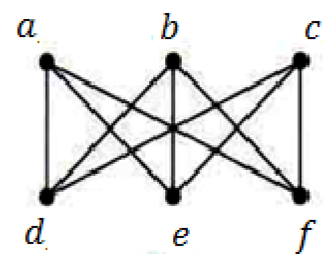
P8:

Find the number of paths of length 3 in $K_{3,3}$

- **i. between any two adjacent vertices**
- **ii. between any two nonadjacent vertices**

Solution:

We have $k_{3,3}$



The adjacency matrix of $K_{3,3}$, w.r.t. the ordering of vertices a, b, c, d, e, f.

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

To determine the number of paths of length 3 between two vertices of $K_{3,3}$, we have to compute A^3.Now

$$A^2 = \begin{bmatrix} 3 & 3 & 3 & 0 & 0 & 0 \\ 3 & 3 & 3 & 0 & 0 & 0 \\ 3 & 3 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 3 & 3 \\ 0 & 0 & 0 & 3 & 3 & 3 \\ 0 & 0 & 0 & 3 & 3 & 3 \end{bmatrix}, \quad A^3 = \begin{bmatrix} 0 & 0 & 0 & 9 & 9 & 9 \\ 0 & 0 & 0 & 9 & 9 & 9 \\ 0 & 0 & 0 & 9 & 9 & 9 \\ 9 & 9 & 9 & 0 & 0 & 0 \\ 9 & 9 & 9 & 0 & 0 & 0 \\ 9 & 9 & 9 & 0 & 0 & 0 \end{bmatrix}$$

Each vertex of $\{a, b, c\}$ is adjacent to each vertex of $\{d, e, f\}$ and no two vertices of $\{a, b, c\}$ are adjacent and no two vertices of $\{d, e, f\}$ are adjacent.

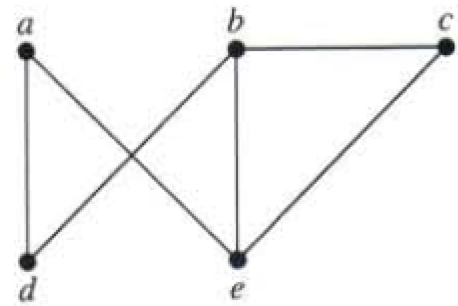
Now the number of paths of length 3 in $K_{3,3}$, between any two adjacent vertices is 0 and the number of paths of length 3 in $K_{3,3}$ between any two non adjacent vertices is 9

3.3

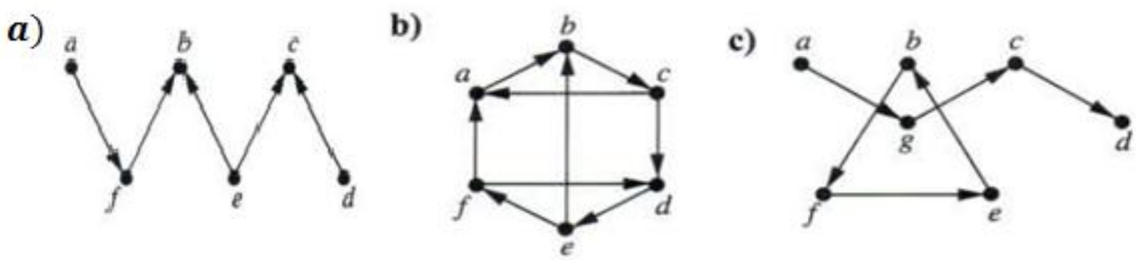
Exercise:

1. Does each of these lists of vertices form a path in the following following graph? Which paths are simple? Which are circuits? What are the lengths of those that are paths?

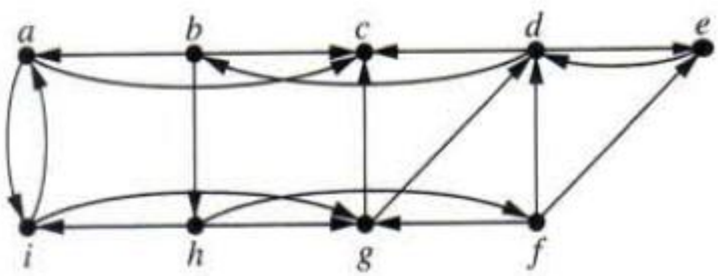
   a) a, e, b, c, b b) a, e, a, d, b, c, a c) e, b, a, d, b, e d) c, b, d, a, e, c



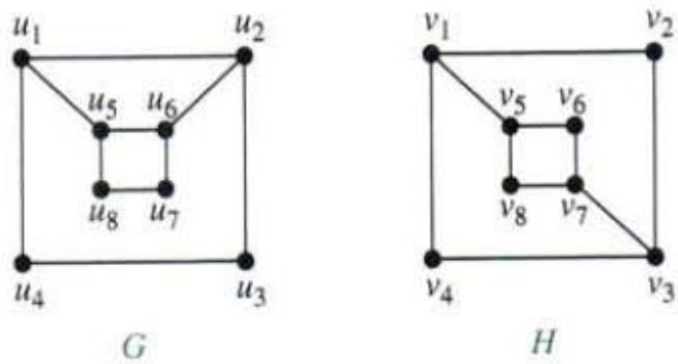
2. Determine whether each of these graphs is strongly connected and if not, whether it is weakly connected.

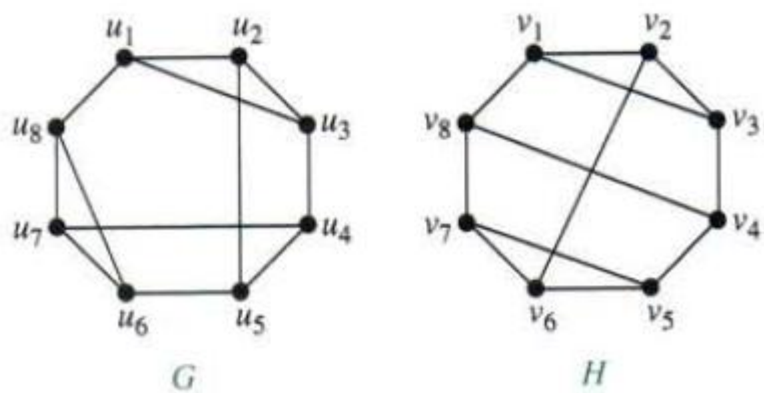


3. Find the strongly connected components of the following graph.



4. Use paths either to show that these graphs are not isomorphic or to find an isomorphism between these graphs

a) 

b) 

5. Find the number of paths of length n between two different vertices in K_4 if n is

a) 2 b) 4 c)5

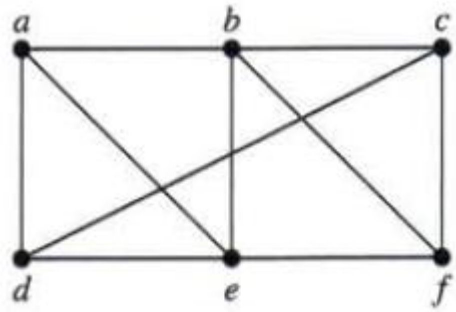
6. Find the number of paths of length n between any two adjacent vertices in $K_{3,3}$ if n is

a) 2 b) 4 c)5

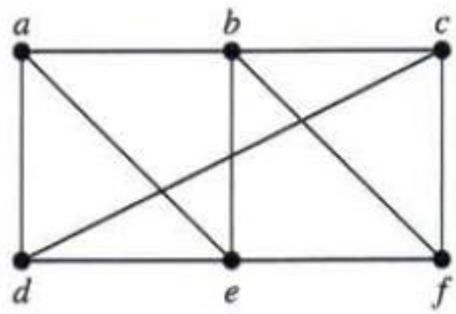
7. Find the number of paths of length n between any two non adjacent vertices in $K_{3,3}$ if n is

b) 2 b) 4 c)5

8. Find the number of paths between c to d in the following graph of length
   a) 2 b) 3 c)4 d)5 e)6 f)7



9. Find the number of paths from a to e in the following directed graph of length
   b) 2 b) 3 c)4 d)5 e)6 f)7



·

UNIT-6

GRAPH THEORY (Continuation)

MODULE-1

Euler and Hamiltonian Paths

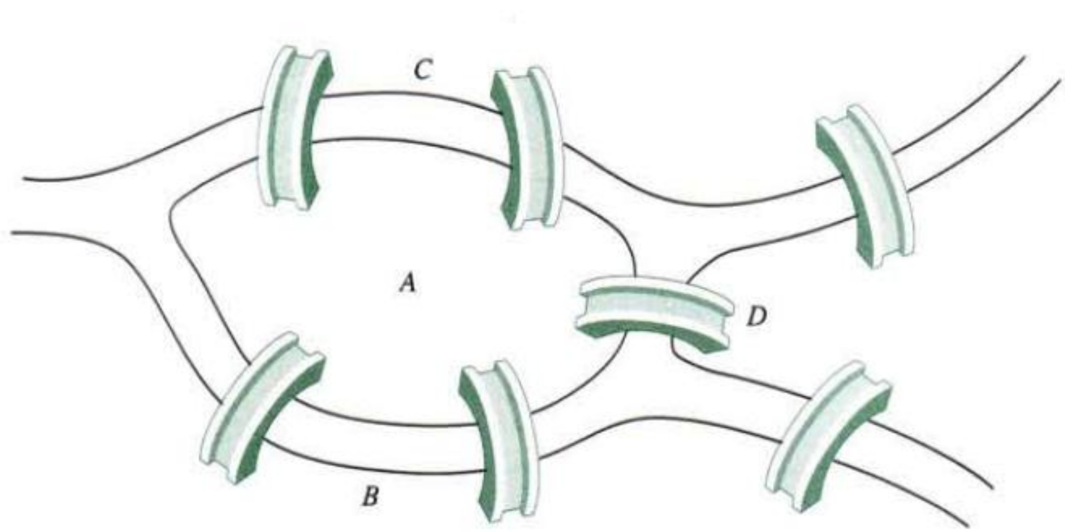
3.4

Euler and Hamilton Paths

Can we travel along the edges of a graph starting at a vertex and returning to it by traversing each edge exactly once? Similarly, can we travel along the edges of a graph starting at a vertex and returning to it by visiting each vertex of the graph exactly once? The first one gives the concept of **Euler circuit** (or **Eulerian circuit**) and the second one leads to the concept of **Hamilton circuit** (or **Hamiltonian circuit**). Although both questions have many practical applications in many different areas, both arose in old puzzles.

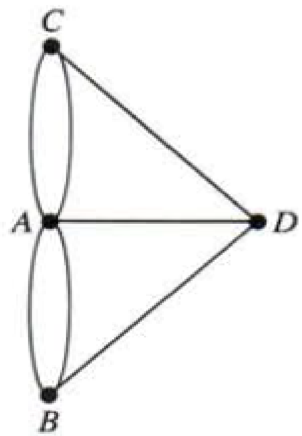
Konigsberg seven bridges problem: The town of Konigsberg, Prussia (now called Kaliningrad and part of Russian republic) was divided into four sections by the branches of the Pregel River. These four sections included the two regions on the banks of Pregel (marked as B, C), Kneiphof Island (marked as A), and the regions between the two branches of the Pregel (marked as D).

In the 18th century seven bridges connected these regions. The following figure depicts these regions and bridges.



The townspeople wondered whether it was possible to start at some location in the town, travel across all the bridges without crossing any bridge twice, and return to the starting point.

The Swiss mathematician **Leonard Euler** solved this problem, published his solution in *1736* and it was the first use of graph theory. *Euler* studied this problem and depicted the four regions as vertices A, B, C, D and the bridges as the edges, thus obtaining a multigraph as shown below:

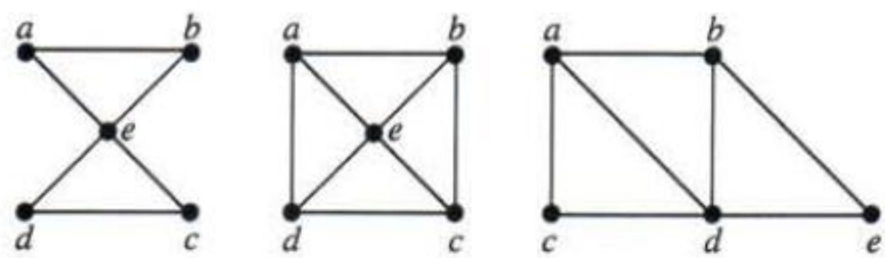


The question that the townspeople asked is:

Is there a simple circuit in this multigraph that contains every edge?

Euler Path and Euler Circuit: Let G be a graph.
An **Euler path** in G is a simple path containing every edge of G.
An **Euler circuit** in G is a simple circuit containing every edge of G.

Example 1: Which of the following undirected graphs have an Euler Circuit? Of those that do not, which have an Euler path?



G_1 G_2 G_3

Solution: The graph G, has an Euler circuit

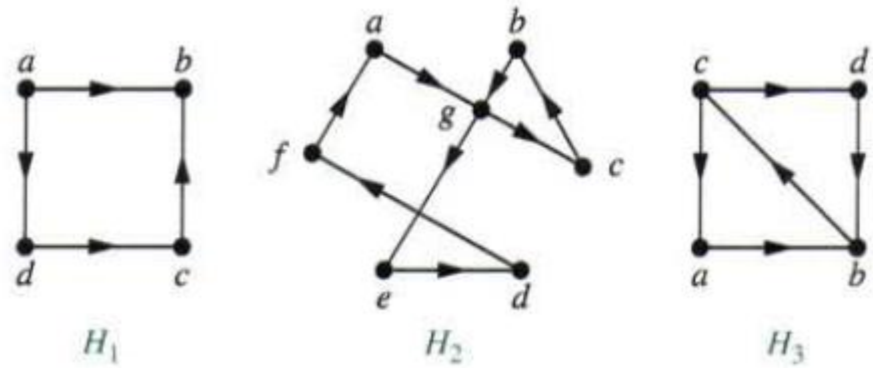
$$a, e, c, d, e, b, a$$

Neither G_2 nor G_3 has an Euler circuit (verify!). The graph G_3 has an Euler path

$$a, c, d, e, b, d, a, b$$

The graph G_3 does not have an Euler path (verify!)

Example 2: Which of the following digraphs have an Euler circuit? Of those that do not, which have an Euler path?



Solution: The digraph H_2 has an Euler circuit

$$a, g, c, b, g, e, d, f, a$$

Neither H_1 nor H_3 has an Euler circuit (verify!).The digraph H_3 has an Euler path

$$c, a, b, c, d, b$$

The digraph H_1 does not have an Euler path (verify!).

Necessary and sufficient conditions for Euler circuits and paths in an undirected graph

Let G be an undirected connected graph with at least two vertices.

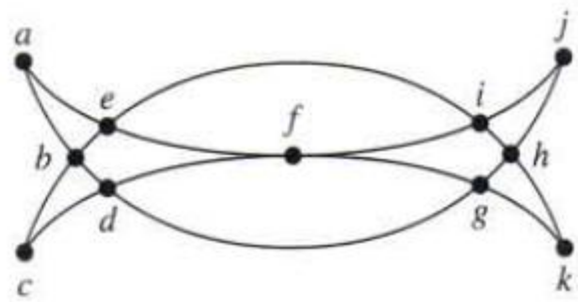
Theorem 1: The graph G has an Euler circuit if and only if each of its vertices has even degree.

Theorem 2: The graph G has an Euler path if and only if it has exactly two vertices of odd degree.

Note: The Euler path of the above theorem is from one of the two vertices of odd degree to the other.

Many puzzles ask you to draw a picture in a continuous motion without lifting the pencil so that no part of the picture is retraced. We can solve such puzzles using Euler paths and circuits.

Example 3: Can the following graph (called Mohammed's Scimitars) be drawn in the above manner, where the drawing begins and ends at the same point?



G

Solution: Note that the graph is connected and the degree sequence of the graph is 4,4,4,4,4,4,4,4,2,2,2,2. Observe that each of its vertices has even degree. By Theorem 1 , it has an Euler circuit. We will now construct an Euler circuit in the following way:

First we form a simple circuit starting at a:

$$a, b, d, g, h, j, i, f, e, a$$

Now, delete the edges in this circuit and obtain the subgraph H (some vertices may become isolated, in this case the vertices a, j become isolated).

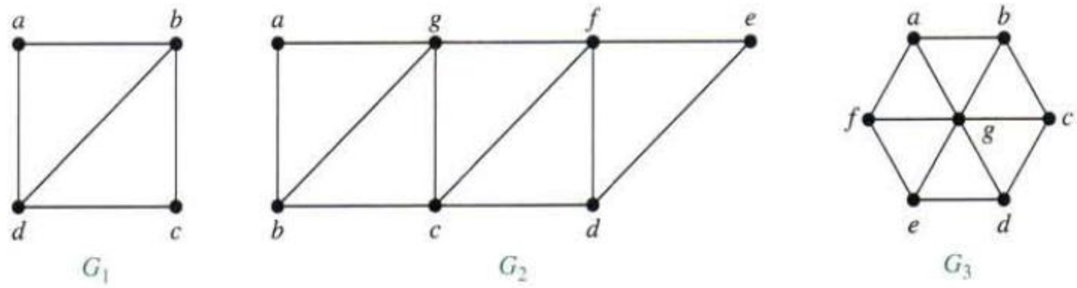
Now, form a simple circuit starting at a vertex which is common to the above circuit and H, say b. Form a simple circuit starting at b with the edges of H.

$$b, e, i, h, k, g, f, d, c, b$$

Observe that we have used all edges in the given graph. Join this new circuit in the first circuit at b we get the following Euler circuit:

$$a, b, e, i, h, k, g, f, d, c, b, d, g, h, j, i, f, e, a$$

Example 4: Which of the following graphs have an Euler path?



Solution: First note that all graphs G_1 , G_2 and G_3 are connected.

(i) The degree sequence of G_1 is 3,3,2,2. It contains exactly two vertices b, d of odd degree. By Theorem 2, G_1 has an Euler path (and it must have b and d as its end points). First start at one of the vertices of odd degree and reach the other tracing the edges exactly once. The following is a simple path starting at b and ending at d.

$$b, a, d$$

Now delete the edges in this path and obtain the sub graph H. Now every vertex in H has even degree. In H form a simple circuit with the edges of H starting at d:

$$d, b, c, d$$

Now splice(join) the two, we get an Euler path:

$$b, a, d, b, c, d$$

(ii) The degree sequence of G_2 is 4,4,4,3,3,2,2. It contains exactly two vertices b, d of odd order. By Theorem 2 G_2 has an Euler path from b to d or from d to b. We will construct the Euler path as in (i).

The first simple path is : b, c, d

Simple circuit at c : c, f, g, c

(not to traverse the edges which are already included in the earlier path)

Join : b, c, f, g, c, d

Simple circuit at g : g, b, a, g

Join : $b, c, f, g, b, a, g, c, d$

Simple circuit at f : f, e, d, f

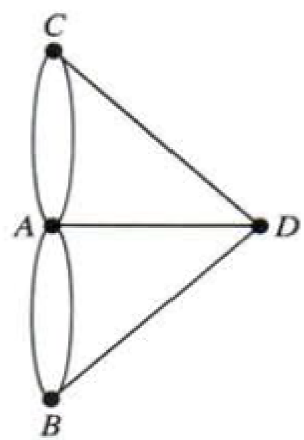
Join : $b, c, f, e, d, f, g, b, a, g, c, d$

We have traversed each edge exactly once and so the above is an Euler path.

(iii) The degree sequence of G_3 is 6,3,3,3,3,3,3. Notice that the degree of each vertex is not even and it does not have exactly two vertices of odd degree. Therefore, by Theorem 1, G_3 has no Euler circuit and by Theorem 2, G_3 has no Euler path. Thus, G_3 has neither an Euler circuit nor an Euler path.

Solution of Konigsberg Seven bridges problem:

The question can now be rephrased as: **Is there is an Euler circuit in this multigraph?**



The degree sequence of this graph is 5,3,3,3. Notice that the degree of each vertex is not even. Therefore, by Theorem 1 there is no Euler circuit in this graph.

Thus, Euler answered that it was not possible reaching the starting point by crossing each bridge exactly once.

Note that this graph does not have exactly two vertices of odd degree. By Theorem 2, there is no Euler path in this graph.

Necessary and sufficient conditions for Euler circuits and paths in a digraph

Theorem 3: **A digraph possesses an Euler circuit if and only if it is weakly connected and the in-degree of every vertex is equal to its out-degree.**

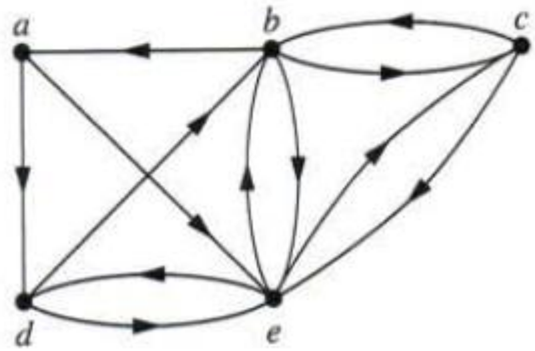
Theorem 4: **A digraph possesses an Euler path if and only if it is weakly connected and in-degree of every vertex is equal to its out-degree with the exception of two vertices $\boldsymbol{a}$, $\boldsymbol{b}$ with**

$$\boldsymbol{deg^-(a) = deg^+(a) + 1}$$

$$\boldsymbol{deg^-(b) = deg^+(b) - 1}$$

Note: The Euler path will be from b to a.

Example 5: **Determine whether the following digraph has an Euler circuit. Construct an Euler circuit if one exists. If no Euler circuit exists, determine whether the digraph has an Euler path, construct an Euler path if one exists.**



Solution: The following is the in-degree and out-degree table for vertices:

Vertex x	$\deg^-(x)$	$\deg^+(x)$
a	1	2
b	3	3
c	2	2
d	2	2

e	4	3

Notice that the given graph is weakly connected and the in-degree of every vertex is equal to its out-degree with the exception of two vertices a, e with

$$deg^{-}(e) = deg^{+}(e) + 1$$

$$deg^{-}(a) = deg^{+}(a) - 1$$

Therefore by Theorem 4, the given digraph has an Euler path (from a to e). Further, by Theorem 3 the digraph has no Euler circuit.

Construction of an Euler path:

Step 1: Take a simple path from a to e

a, d, e

Step 2: Circuit at d : d, b, e, d

(not to traverse the edges which are already included in the earlier path)

Step 3: Join : a, d, b, e, d, e

Step 4: Circuit at b b, a, e, b

Step 5: Join : $a, d, b, a, e, b, e, d, e$

Step 6: Circuit at b : b, c, b

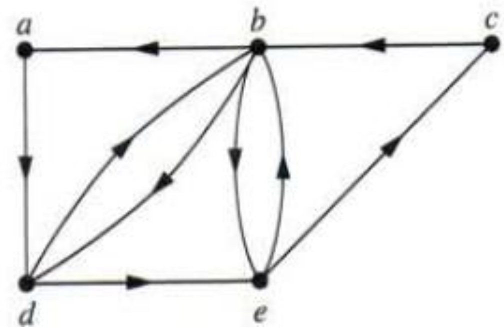
Step 7: Join : $a, d, b, c, b, a, e, b, e, d, e$

Step 8: Circuit at c : c, e, c

Step 9: Join : $a, d, b, c, e, c, b, a, e, b, e, d, e$

We have traversed each directed edge exactly once and so the above is an Euler path.

Example 6: **Determine whether the following digraph has an Euler circuit. Construct an Euler circuit if one exists. If no Euler circuit exists, determine whether the digraph has an Euler path, construct an Euler path if one exists.**



Solution: The given digraph is weakly connected. The in-degree and out-degree of each vertex is given in the following table:

Vertex x	$\deg^{-}(x)$	$\deg^{+}(x)$
a	1	1
b	3	3
c	1	1
d	2	2
e	2	2

Notice that in-degree of every vertex is equal to its out-degree. By Theorem 3 this graph has an Euler circuit. By Theorem 4 this graph has no Euler path.

The following is the construction of Euler circuit:

Step 1: Take a circuit (at any vertex): a, d, b, a

Step 2: Circuit at d : d, e, b, d

(not to traverse the edges which are already included in the earlier path)

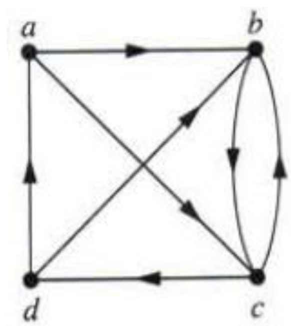
Step 3: Join : a, d, e, b, d, b, a

Step 4: Circuit at b : b, e, c, b

Step 5: Join : $a, d, e, b, d, b, e, c, b, a$

An Euler circuit is $a, d, e, b, d, b, e, c, b, a$

Example 7: **Determine whether the following digraph has an Euler circuit. Construct an Euler circuit if one exists. If no Euler circuit exists, determine whether the digraph has an Euler path, construct an Euler path if one exists.**



Solution: The given digraph is weakly connected and the in-degree and out-degree of each vertex is given in the following table.

Vertex x	$\deg^-(x)$	$\deg^+(x)$
a	1	2
b	3	1
c	2	2
d	1	2

From the table it is clear that the in-degree and out-degree of vertices are satisfying neither the conditions of Theorem 3 nor the conditions of Theorem 4. Therefore, neither an Euler circuit nor an Euler path exists in the given digraph.

Hamilton Paths and circuits

Let G be a graph.

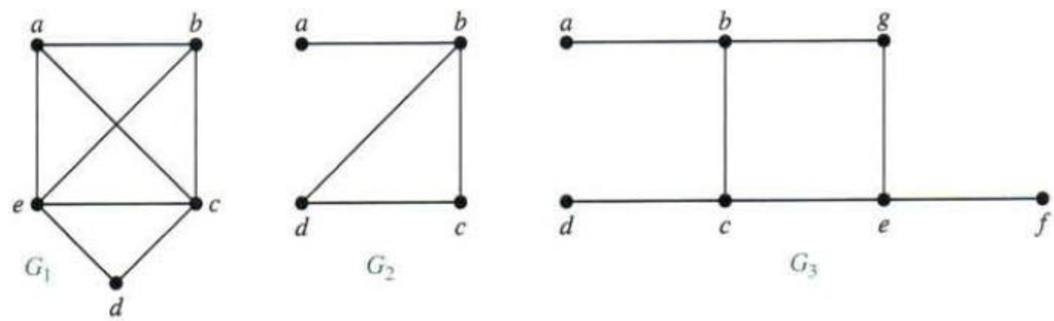
A simple path in G that passes through every vertex of G exactly once is called a **Hamilton path**.

A simple circuit in G that passes through every vertex of G exactly once is called a **Hamilton circuit**.

Note: If a graph has a Hamilton circuit, then it has a Hamilton path. This Hamilton path can be obtained from the Hamilton circuit by dropping an edge in it. However, the existence of a Hamilton path does not guarantee a Hamilton circuit.

These concepts and terminology comes from a game called **Icosian puzzle** invented in 1857 by the Irish mathematician ***Sir William Rowan Hamilton***.

Example 8: Which of the following simple graphs have a Hamilton circuit or, if not, a Hamilton path?



Solution:

(i) The graph G_1, has a Hamilton circuit a, b, c, d, e, a

(ii) The graph G_2 has no Hamilton circuit (It may be seen that every circuit containing every vertex must contain b twice), but it has a Hamilton path: a, b, c, d.

(iii) The graph G_3 has neither a Hamilton path nor a Hamilton circuit. (Note that every path containing all vertices must visit one of the vertices b, c, e more than once).

There are no known simple necessary and sufficient criteria for the existence of Hamilton paths/circuits. However, many theorems are known that give sufficient conditions for the existence of Hamilton circuits. Also certain properties can be used to show that a graph has no Hamilton circuit.

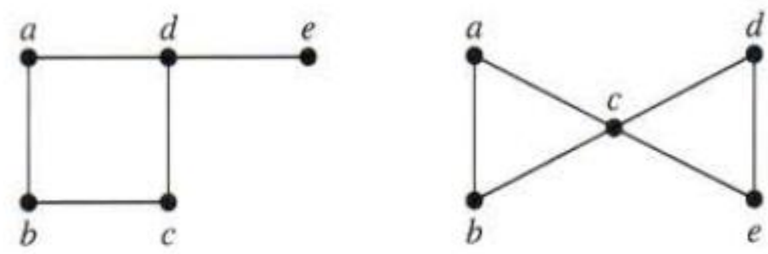
Note:

(i) A graph with a vertex of degree 1 cannot have a Hamilton circuit (because each vertex incident with two edges in a Hamilton circuit).

(ii) If a vertex in a graph has degree two, then both the edges that incident with this vertex must be part of any Hamilton circuit.

(iii) A Hamilton circuit cannot contain a smaller circuit within it.

Example 9: Show that neither graph given below has a Hamilton circuit.



G H

Solution: The graph G has no Hamilton circuit because G has a vertex e of degree one.

Notice that the degrees of the vertices a, b, d and e in H are all two. Therefore, every edge incident with these vertices must be a part of any Hamilton circuit. Now any Hamilton circuit must contain the four edges incident with c and this is not possible. Therefore, H has no Hamilton circuit.

Example 10: Every complete graph K_n has a Hamilton circuit whenever $n \geq 3$.

Solution: A Hamilton circuit in K_n can be formed by starting at any vertex and visiting vertices in any order. This is possible because every pair of vertices are adjacent in K_n.

Although no useful necessary and sufficient conditions for the existence of Hamilton circuits are known, quite a few sufficient conditions have been found.

Note: Adding edges, but not vertices, to a graph with a Hamilton circuit produces a graph with the same Hamilton circuit.

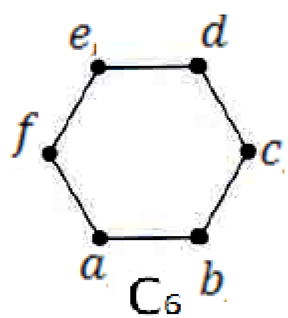
The following are the most important sufficient conditions for the existence of a Hamilton circuit.

Theorem 5 (Dirac's Theorem): If G is a simple graph with n vertices, $n \geq 3$ such that the degree of every vertex is at least $\frac{n}{2}$, then G has a Hamilton circuit.

Theorem 6(Ore's Theorem): If G is a simple graph with n vertices, $n \geq 3$ such that deg(u) + deg(v) $\geq n$ for every pair of nonadjacent vertices u and v in G, then G has a Hamilton circuit.

Both Ore's Theorem and Dirac's Theorem provide sufficient conditions for a connected simple graph to have a Hamilton circuit. However, these theorems do not provide necessary conditions for the existence of a Hamiltonian circuit.

Counter example: Consider the cycle graph C_6.



Note that C_6 has a Hamilton cycle: a, b, c, d, e, f, a. In this graph, the degree of every vertex x is 2, and thus $\deg(x)$ is atleast $\frac{n}{2} = \frac{6}{2} = 3$ is not satisfied but, C_6 has a Hamilton circuit. Further, $\deg(u) + \deg(v) = 4 \ngeq n = 6$ for every pair of non adjacent vertices u and v of C_6 , but C_6 has a Hamiltonian circuit. That is, the graph C_6 has a Hamilton circuit but does not satisfy the hypothesis of Ore's Theorem and Dirac's Theorem.

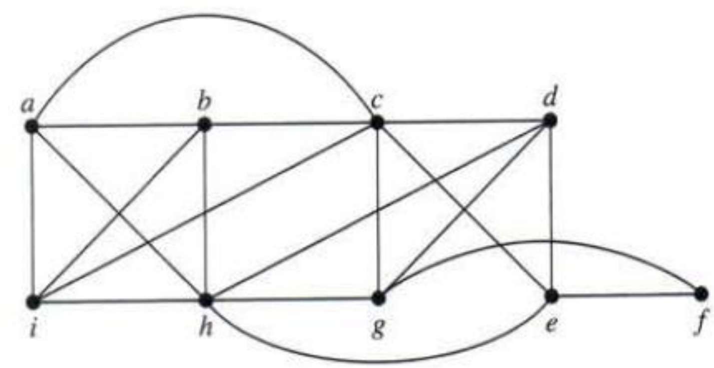
Applications:

Hamilton paths and circuits can be used to solve practical problems. For example, many applications ask for a path or circuit that visits *each road intersection in a city, each place pipelines intersection in a utility grid*, or *each node in a* *communications network exactly once*. Finding a Hamilton path or circuit in the appropriate graph model can solve such problems.

The famous **Travelling Salesman Problem** asks for the shortest route a travelling salesman should take to visit a set of cities. This problem reduces to finding a Hamilton circuit in a complete graph such that the total weight of its edges is as small as possible.

P1:

Determine whether the given graph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.



Solution:

The degrees of the vertices of the graph G are

vertex x	a	b	c	d	e	f	g	h	i
$\deg(x)$	4	4	6	4	4	2	4	6	4

Observe that the degree of each vertex of G is even. By Theorem 1, G has an Euler circuit.

Now Construction of an Euler circuit:

Take a circuit (at any vertex) : a, c, e, h, a

Simple circuit at e : e, f, g, d, e

(not to traverse the edges which are already included in the earlier path)

Join : $a, c, e, f, g, d, e, h, a$

Simple circuit at c : c, d, h, b, c

Join : $a, c, d, h, b, c, e, f, g, d, e, h, a$

Simple circuit at b : b, i, a, b

Join : $a, c, d, h, b, i, a, b, c, e, f, g, d, e, h, a$

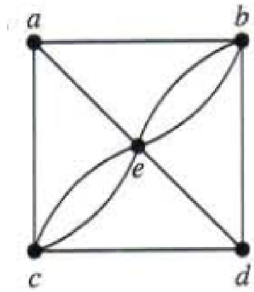
Simple circuit at i : i, c, g, h, i

Join : $a, c, d, h, b, i, c, g, h, i, a, b, c, e, f, g, d, e, h, a$

The above is the Euler circuit in G.

P2:

Determine whether the given graph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.



Solution:

The degree sequence of the given graph G is 6,4,4,3,3. The graph G has exactly two vertices a, d of odd degree. By Theorem 1, G has an Euler path (either from a to d or from d to a).

Construction of an Euler path:

Take a simple path from a to d : a, b, d

Simple circuit at b : b, e, c, e, b

(not to traverse the edges which are already included in the earlier path)

Join : a, b, e, c, e, b, d

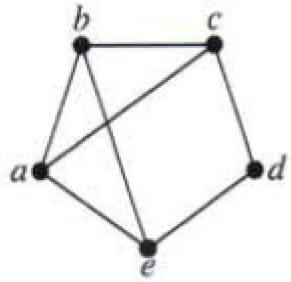
Simple circuit at c : c, a, e, d, c

Join : $a, b, e, c, a, e, d, c, e, b, d$

The above is an Euler path.

P3:

Determine whether the given graph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.

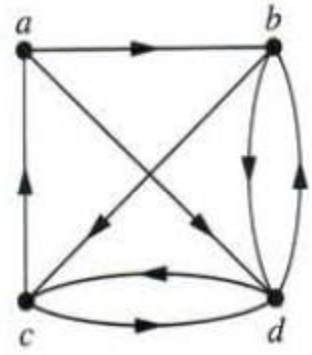


Solution:

The degree sequence of the given graph G is 3,3,3,3,2. Notice that the degree of each vertex is not even and it does not have exactly two vertices of odd degree. Therefore, by Theorem 1, G has no Euler circuit and by Theorem 2, G has no Euler path. Thus, G has neither an Euler circuit nor an Euler path.

P4:

Determine whether the given digraph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.



Solution:

The given digraph G is weakly connected. The in-degree and out-degree of each vertex is given in the following table.

$vertex$ x	$\deg^-(x)$	$\deg^+(x)$
a	1	2
b	2	2
c	2	2
d	3	2

Notice that in-degree of every vertex is equal to its out-degree with exception of two vertices a, d with

$$\deg^-(d) = \deg^+(d) + 1$$

$$\deg^-(a) = \deg^+(a) - 1$$

Therefore, by Theorem 4, the digraph G has an Euler path from a to d.

Take a simple path from a to d : a, b, d

Simple Circuit at b : b, c, a, d, b

(not to traverse the edges which are already included in the earlier path)

Join : a, b, c, a, d, b, d

Simple circuit at d : d, c, d

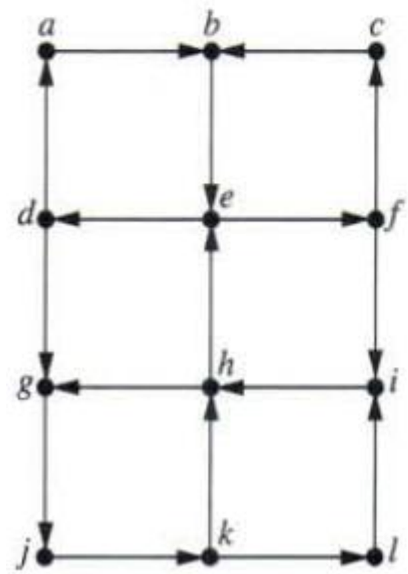
Join : $a, b, c, a, d, c, d, b, d$

An Euler path in the digraph is

$$a, b, c, a, d, c, d, b, d$$

P5:

Determine whether the given digraph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.

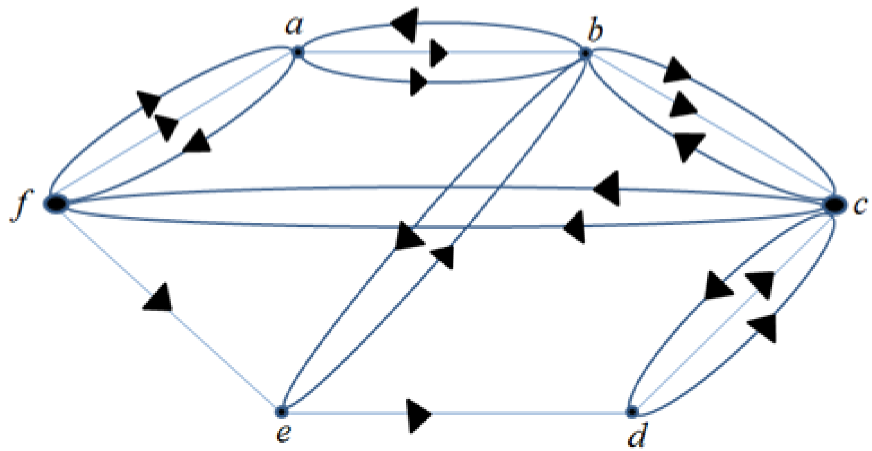


Solution:

Notice that there are 6 vertices b, d, f, g, i and k each of degree 3 and 3 is to be divided between its in-degree and out-degree. Thus this digraph has 6 vertices with unequal in-degree and out-degree. This shows that the condition of Theorem 4 and Theorem 5 are not satisfied. Therefore, neither an Euler circuit nor an Euler path exists in this digraph.

P6:

Determine whether the given digraph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.



Solution:

The given digraph G is weakly connected. The in-degree and out-degree of each vertex is given in the following table.

$vertex$ x	$\deg^-(x)$	$\deg^+(x)$
a	3	3
b	3	3
c	4	4
d	2	2
e	2	2
f	3	3

Notice that the in-degree of each vertex is equal to its out-degree. By Theorem 3, this digraph has an Euler circuit.

Construction of an Euler circuit

(1) Take a circuit at any vertex : a, b, c, d, c, f, a

(2) Circuit at d : d, c, f, e, d

(not to traverse the edges which are already included in the earlier path)

(3) Join : $a, b, c, d, c, f, e, d, c, f, a$

(4) Circuit at c : c, b, a, f, a, b, c

(5) Join : $a, b, c, b, a, f, a, b, c, d, c, f, e, d, c, f, a$

(6) Circuit at b : b, e, b

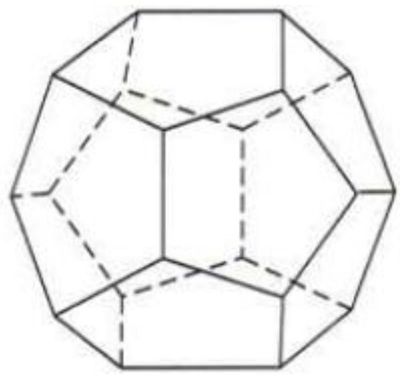
(7) Join : $a, b, e, b, c, b, a, f, a, b, c, d, c, f, e, d, c, f, a$

The path given in (7) is an Euler circuit.

P7:

A puzzle called **Icosian puzzle** (“***A voyage round the world” puzzle***) was posed by the Irish mathematician **Sir William Rowan Hamilton** in 1859 and this puzzle led to the concepts of Hamilton circuit and Hamilton path.

Hamilton devised a toy consisting of a wooden regular dodecahedron (a polyhedron with 20 vertices, 30 edges and 12 regular pentagons as faces) and sold it to a toy manufacturer in Dublin.

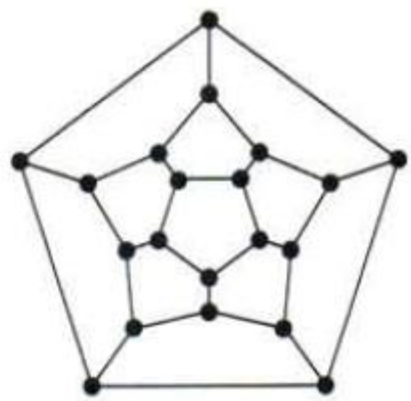


The 20 vertices were labeled with different cities in the world and 30 edges represent routes connecting the cities.

The aim of the puzzle was to start at a city, say a, and travel along the edges, visiting each of the other cities exactly once and coming back to the first city a.

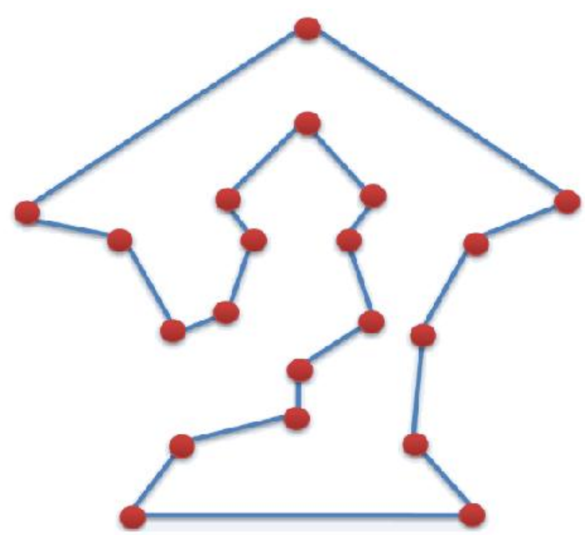
The following is an equivalent question:

Is there a circuit in the graph shown below that passes through each vertex exactly once?



This solves the puzzle because this graph is isomorphic to the graph consisting of vertices and edges of the dodecahedron.

A solution of Hamilton's puzzle is shown below



P8:

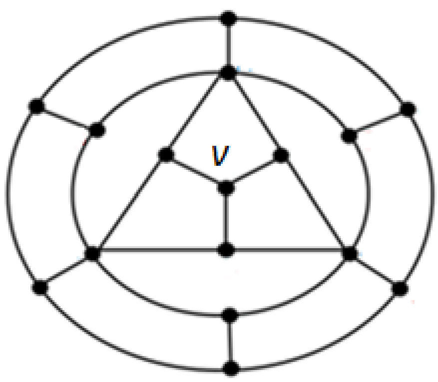
Labeling technique for the existence/nonexistence of a Hamilton circuit

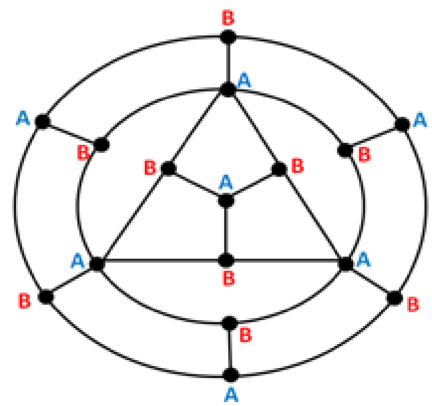
Solution:

we assign a label say A to some vertex v in G. All vertices adjacent to v with label A are labeled with B. All the vertices adjacent to vertices with label B are assigned the label A. The process is continued until all the vertices are labeled.

If there is a Hamilton circuit/path it must pass through the vertices with label A and vertices with label B alternately. In this case **the number of vertices with label A and the number of vertices with label B must differ by at most 1**. Otherwise the given graph has no Hamilton circuit/path.

Example: Determine whether the following graph has a Hamilton circuit/path.





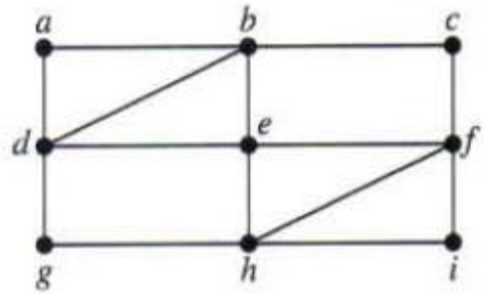
We use labeling technique. Assign label A to the center v of the graph. Assign label B to all the vertices adjacent to v. Continue the process till all the vertices are labeled. Notice that we have 7 vertices with label A and 9 vertices with label B. If there is a Hamilton circuit or path it must pass through the vertices with label A and the vertices with label B alternately and this is not possible. Thus the given graph has no Hamilton circuit. Further, there is no Hamilton path also.

3.4. Euler and Hamilton paths

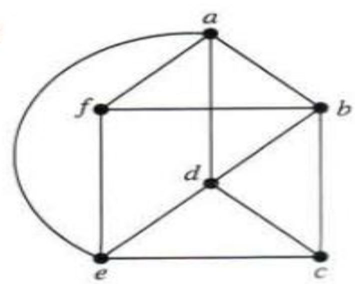
Exercise:

1. Determine whether the given graph has an Euler circuit. Construct such circuit when one exists. If no Euler circuit exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists**.**

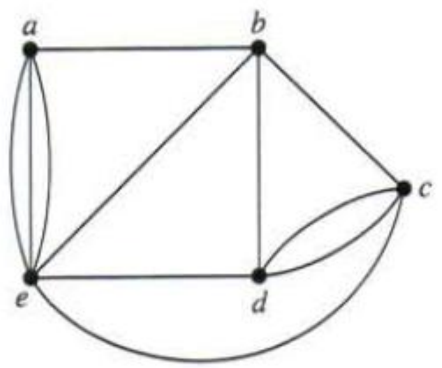
i



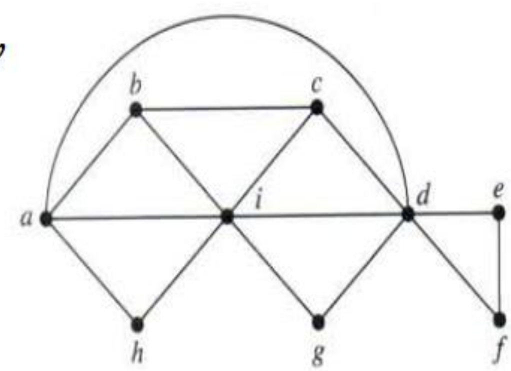
ii



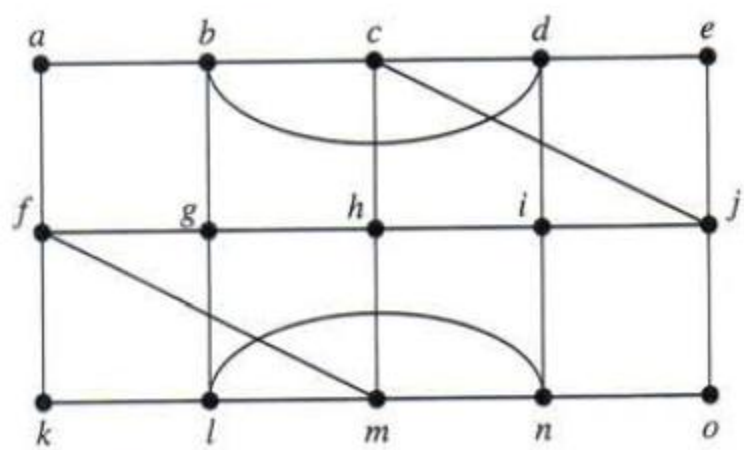
iii



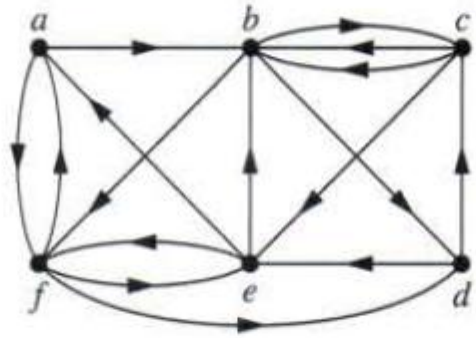
iv



v

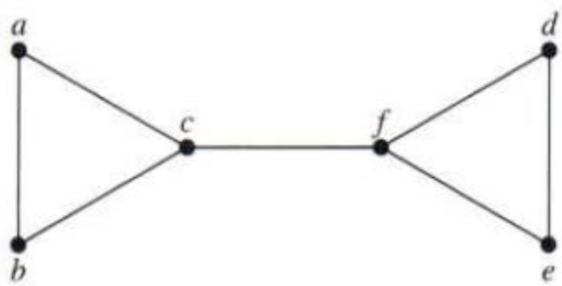


2. Determine whether the directed graph shown has an Euler circuit. Construct an Euler circuit if one exists. If no Euler circuit exists,determine whether the directed graph has an Euler path. Construct an Euler path if one exists.

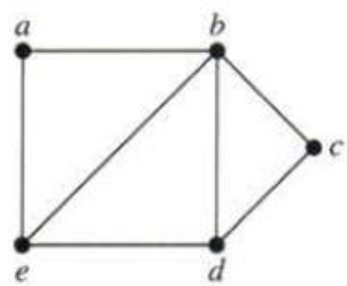


3. Determine whether the given graph has a Hamilton circuit. If it does,find such a circuit. If it does not, give an argument to show that an argument to show why no such circuit exists.

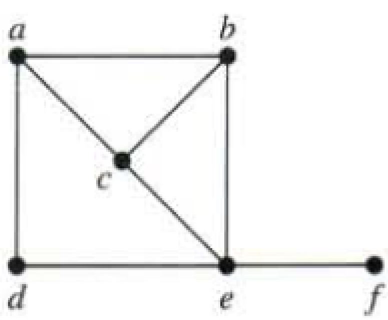
i



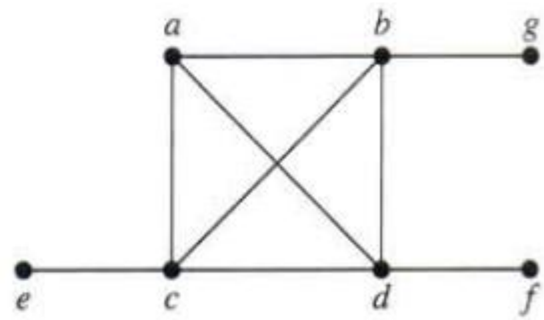
ii



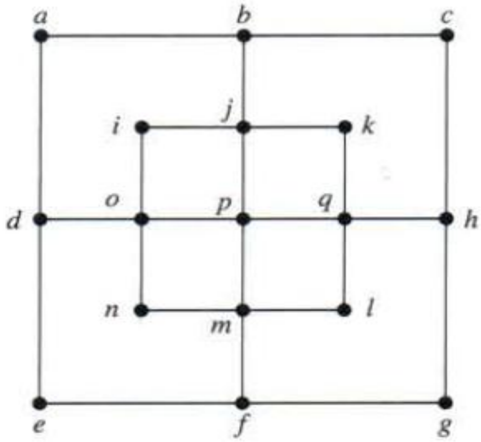
iii



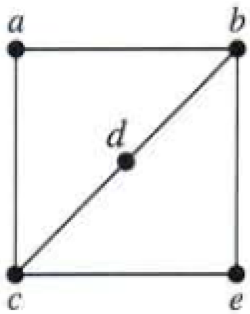
iv



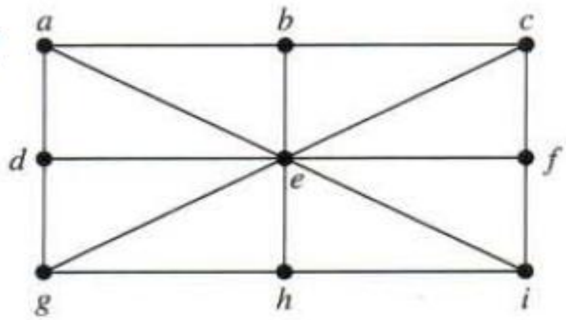
v



vi



vii



MODULE-2

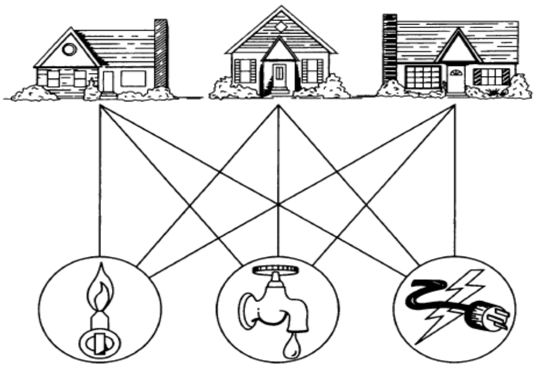
Planar Graphs

3.5

PLANAR GRAPHS

Three houses and three utilities problem:

Consider the problem of joining three houses to each of three separate utilities as shown below: **Is it possible to join these houses and utilities so that none of the connections cross?**



Three houses and three utilities

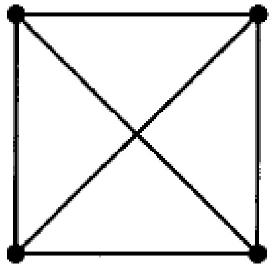
This problem can be modeled using the complete bipartite graph $K_{3,3}$. The above question is rephrased as: **Can $K_{3,3}$ be drawn in the plane so that no two of its edges cross?**

In this module we study the question of whether a graph can be drawn in the plane without edges crossing.

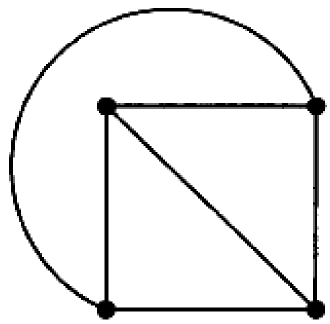
Planar graph: A graph is said to be **planar** if it can be drawn in the plane without any edges crossing. Such a drawing is called a **planar representation** of the graph.

A graph may be planar even if it is usually drawn with crossings, because it may be possible to draw it in a different way without crossings.

For example, K_4 drawn as below is planar, because it can be drawn without crossings as shown below.

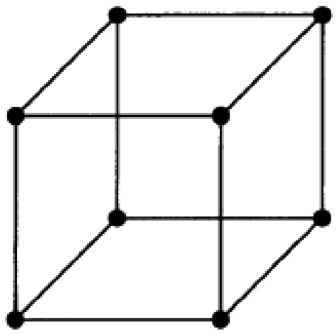


K_4 with a crossing

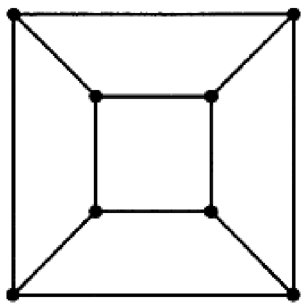


Planar representation of K_4

Example 1: Q_3 is planar

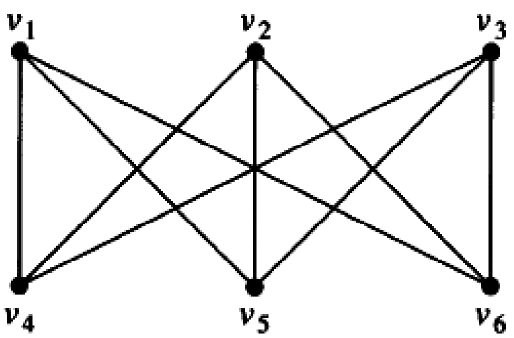


Q_3



Planar representation of Q_3

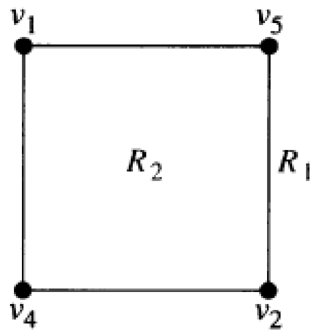
Example 2: $K_{3,3}$ is not planar.



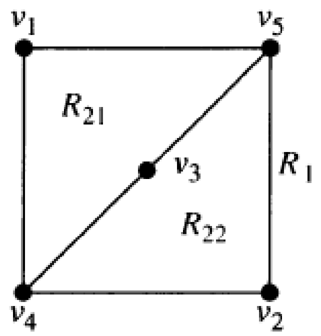
Solution: First notice that any attempt to draw $K_{3,3}$ in the plane with no edges crossing is failed.

A reason for this is given below:

In any planar representation of $K_{3,3}$ the vertices v_1 and v_2 must be connected to both the vertices v_4 and v_5 . These four edges form a closed curve that splits the plane into two regions R_1 and R_2 as shown below:



Now, the vertex v_3 is in either R_1 or R_2 .Suppose that v_3 is in R_2.The edges between v_3 , v_4 and v_3 , v_5 separate R_2 into two subregions R_{21} and R_{22} as shown below



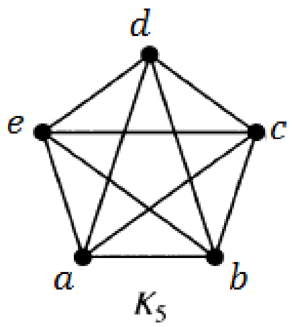
If v_6 is in R_1 , then the edge between v_6 and v_3 can not be drawn with a crossing. If v_6 is in R_{21} , then the edge between v_6 and v_2 can not be drawn without a crossing. If v_6 is in R_{22} , then the edge between v_6 and v_1 can not be drawn without a crossing. This shows that $K_{3,3}$ can not be drawn without a crossing in this case. We obtain the same conclusion if v_3 is in R_1.

Thus $K_{3,3}$ is not planar:

From the above result, we have: **The three houses and three utilities cannot be connected in the plane without a crossing.**

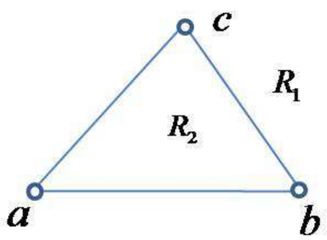
Example 3: Show that K_5 is nonplanar

Solution: We have K_5

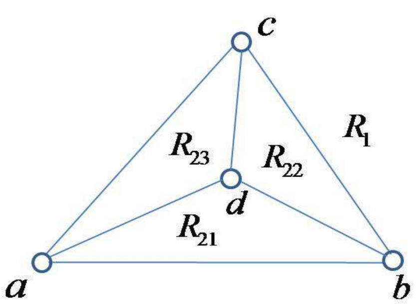


K_5

Solution: First notice that any attempt to draw K_5 in the plane with no edges crossing is failed. Assume that it has a planar representation. First, a triangle is formed by the planar representation of the subgraph of K_5 consisting of the edges connecting a, b and c; and this triangle splits the plane into two regions R_1 and R_2.



Now, the vertex d is in either R_1 or R_2. Suppose that the vertex d is in R_2 ($i.e.$, the inside of the closed curve) then the edges between d, a ; d, b and d, c separate R_2 into three subregions as shown below:



Note that there is no way to place the vertex e without forcing a crossing. If e is in R_1 , then the edge between e and d cannot be drawn without a crossing. If e is in R_{21} , then the edge between e and c can not be drawn without a crossing. If e is in R_{22} , then the edge between e and a can not be drawn without a crossing. If e is in R_{23} , then the edge between e and b can not be drawn without a crossing.

This shows that K_5 cannot be drawn without a crossing in this case. We obtain the same conclusion if the vertex d is in R_1.

Thus, K_5 is nonplanar.

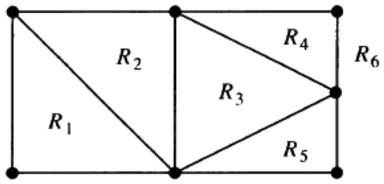
Planarity of graphs play an important role in the design of electronic circuits. We can model an electronic circuit with a graph by representing components of the electronic circuit by vertices and connections between them by edges. If the graph representing electronic circuit is planar, then we can print it on a single board with no connections crossing. If the graph is not planar then we must turn to more expensive options. For example, we can partition the vertices in the graph representing the electronic circuit into planar subgraphs. We then construct the circuit using multiple layers.

We can construct the electronic circuit using insulated wires whenever connections cross. In this case, drawing the graph with the fewest possible crossings is important.

Euler's Formula

A planar representation of a graph splits the plane into **regions**, including an unbounded region.

For example, the planar representation of the graph shown below splits the plane into six regions.



The region R_6 is the unbounded region, because it is not bounded by the edges.

Euler found a relation among the number of regions, the number of vertices, and the number of edges of a planar graph.

Theorem Euler's formula: Let G be any connected planar graph with v vertices and e edges. Let r be the number of regions in a planar representation of G. Then

$$\boldsymbol{v - e + r = 2}$$

Example 4: Suppose that a connected planar graph has 20 vertices, each of degree 3. Into how many regions does a representation of this planar graph split the plane?

Solution: The planar graph G has 20 vertices, each of degree 3. The sum of the degrees of the vertices is $20 \cdot 3 = 60$. By Handshaking theorem we have $2e = 60$, *i.e.,* $e = 30$. By Euler's formula we have, $v - e + r = 2$.
Therefore, $r = e - v + 2 = 30 - 20 + 2 = 12$.

Euler's formula can be used to prove some inequalities that must be satisfied by planar graphs.

Corollary1: Let G be a connected planar simple graph with no loops. If G has e edges and v vertices, $v \geq 3$, then

$$\boldsymbol{e \leq 3v - 6}$$

Corollary 2: If G is a connected planar simple graph with no loops then G has a vertex of degree not exceeding five.

Proof: If G has one or two vertices, then the result is true. If G has atleast three vertices then by Corollary 1, $e \leq 3v - 6$, so $2e \leq 6v - 12$. Assume the contrary. That is, assume that the degree of every vertex is at least six. By Handshaking Theorem, $2e = \sum_{x \in V} deg\, x \geq 6v$. This contradicts the inequality $2e \leq 6v - 12$.
Therefore, our assumption is false. Thus, there is a vertex of degree not exceeding five.

Corollary3: Let G be a connected planar simple graph with no circuits of length 3 $(i.e.$, every region is bounded by four or more edges). If G has e edges and v vertices, $v \geq 3$, then

$$e \leq 2v - 4$$

Example 5: K_5 is nonplanar.

Solution: Notice that K_5 is a connected simple graph with no loops. It has $v = 5$ vertices and $e = 10$ edges. Assume that K_5 is planar then by Corollary 1, $e \leq 3v - 6$, *i.e.,* $10 \leq 3 \cdot 5 - 6 = 9$ - a contradiction. Thus, K_5 is nonplanar.

Example 6: $K_{3,3}$ is nonplanar.

Solution: First note that $K_{3,3}$ is a connected simple graph with $v = 6$ vertices and $e = 9$ edges. Note that it has no loops and it satisfies the inequality $e \leq 3v - 6$. This does not imply $K_{3,3}$ is nonplanar. Observe that $K_{3,3}$ has no circuit of length 3. Now assume that $K_{3,3}$ is nonplanar. By Corollary 3, $e \leq 2v - 4$, $i.e.$, $9 \leq 2 \cdot 6 - 4 = 8$, a contradiction. Thus $K_{3,3}$ is nonplanar.

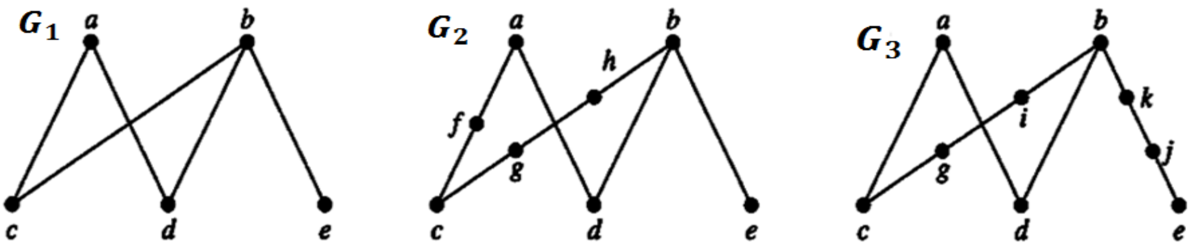
Kuratowski's Theorem

It is known that $K_{3,3}$ and K_5 are nonplanar. Clearly, a graph is not planar if it contains either of these two graphs $K_{3,3}$, K_5 as a subgraph.

Elementary subdivision: If a graph is planar, so will be any graph obtained by removing an edge $\{u, v\}$ and adding a new vertex w together with edges $\{w, u\}$ and $\{w, v\}$. Such an operation is called an ***elementary subdivision.***

Homeomorphic graphs: Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are said to ***homeomorphic*** if they can be obtained from the same graph by a sequence of elementary subdivisions.

Example 7: Show that the following graphs G_1, G_2 and G_3 are all homeomorphic.



Solution: We show that all the three graphs can be obtained from G_1 by elementary subdivisions.

First note that G_1 can be obtained from itself by an empty sequence of elementary subdivisions.

We obtain G_2 from G_1 by the following sequence of elementary subdivisions:

(i) Remove the edge $\{a, c\}$, add the vertex f, and add the edges $\{f, a\}$ and $\{f, c\}$
(ii) Remove the edge $\{b, c\}$, add the vertex g, and add the edges $\{g, b\}$ and $\{g, c\}$
(iii) Remove the edge $\{b, g\}$, add the vertex h, and add the edges $\{h, b\}$ and $\{b, g\}$

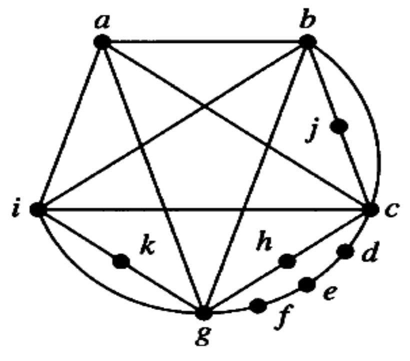
Similarly, we obtain G_3 from G_1 by a sequence of elementary subdivisions.

The Polish mathematician Kazimierz Kuratowski proved the following theorem in 1930. This theorem characterizes planar graphs using the concept of graph homeomorphism.

Theorem (Kuratowski): A graph is nonplanar if and only if it contains a subgraph homeomorphic to $K_{3,3}$ or K_5.

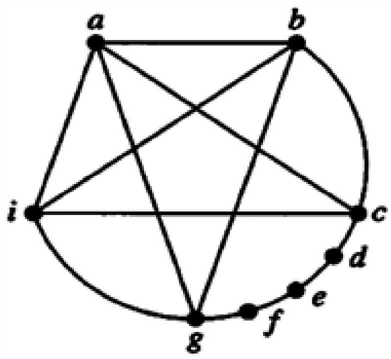
It is clear that a graph containing a subgraph homeomorphic to K_5 or $K_{3,3}$ is nonplanar. However, the proof of the converse, namely that every nonplanar graph contains a subgraph homeomorphic to $K_{3,3}$ or K_5 is complicated and it is out of scope of this course.

Example 8: Determine whether the following graph G is planar.



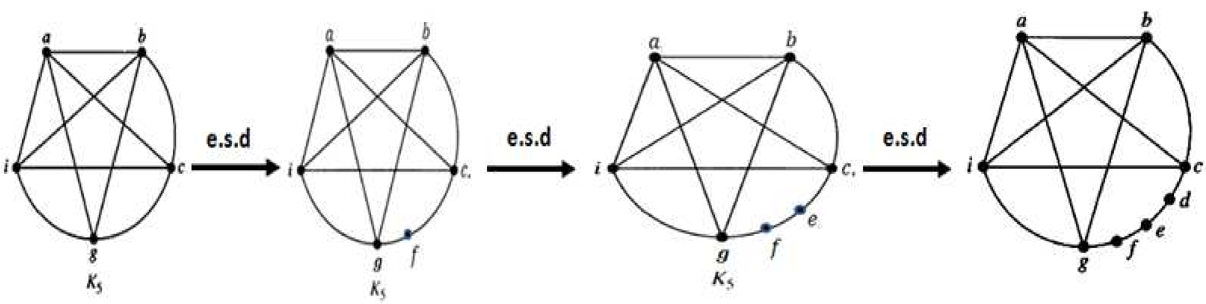
G

Solution: Let H be the subgraph of G obtained by deleting the vertices h, j and k and all edges incident with them.



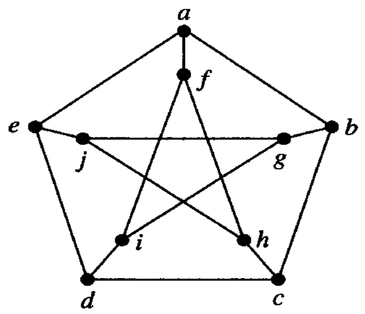
H

Now consider K_5 with vertices a, b, c, g and i. We obtain H from K_5 by the following sequence of elementary subdivisions (e.s.d) as shown below.



Thus, H is homeomorphic to K_5. This shows, that G has a subgraph homeomorphic to K_5. Therefore, by Kuratowski theorem G is nonplanar.

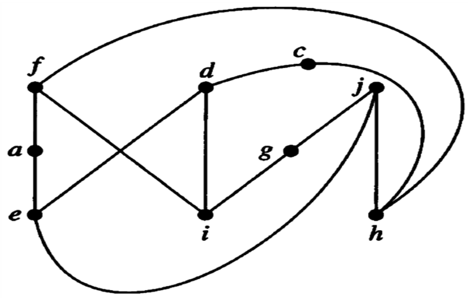
Petersen Graph: The Danish mathematician Julis Petersen studied this graph in 1891. It is often used to illustrate various theoretical properties of graphs.



$Peterson\ Graph$

Example 9: Is Petersen graph, shown above, planar?

Solution: Let H be the subgraph of the Petersen graph obtained by deleting the vertex b and all the edges incident with b.



H

Now, consider $K_{3,3}$ with vertex set $\{f, d, j\}$ and $\{e, i, h\}$, $(i.e.$, a bipartition).

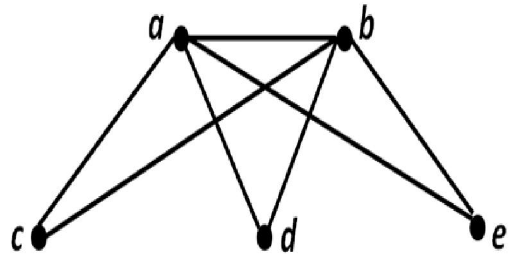
We obtain H from $K_{3,3}$ by a sequence of elementary subdivisions:

deleting $\{d, h\}$ and adding $\{c, h\}$ and $\{c, d\}$: deleting $\{e, f\}$ and adding $\{a, e\}$ and $\{a, f\}$ and deleting $\{i, j\}$ and adding $\{g, i\}$ and $\{g, j\}$

Thus, H is homeomorphic to $K_{3,3}$. This shows that the Petersen graph has a subgraph Homeomorphic to $K_{3,3}$. Therefore, by Kuratowski theorem, the Petersen graph is nonplanar.

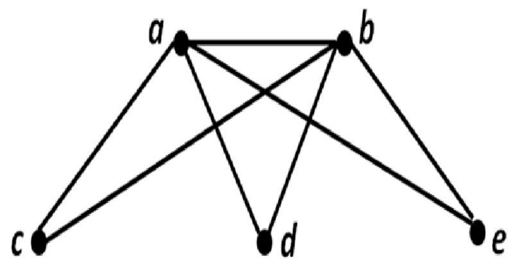
P1.

Draw the given planar graph without any crossings

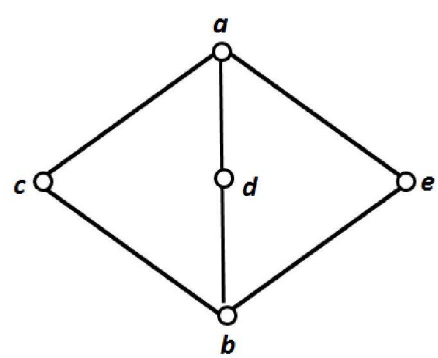


Solution:

The given planar graph is



It is $K_{2,3}$. Its planar representation is

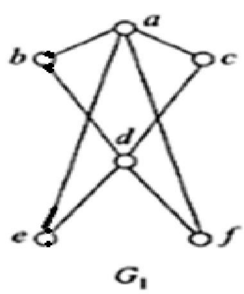


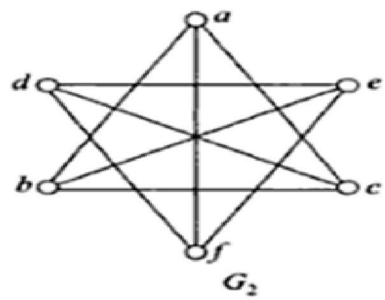
Remark:

(i) $K_{2,3}$ is planar
(ii) $K_{3,3}$ is nonplanar

P2.

Draw the given planar graph without any crossings.



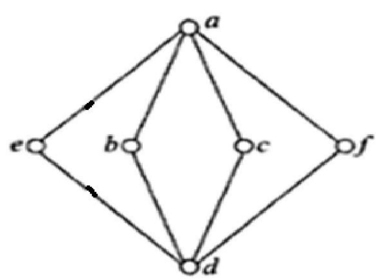


Solution:

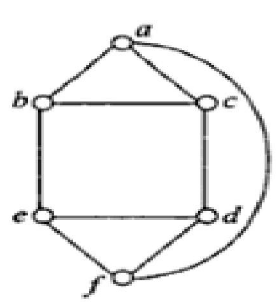
Notice that these are two simple circuits

a, c, d, b, a and a, f, d, e, a in G_1

The planar representation of G_1 can now be drawn as



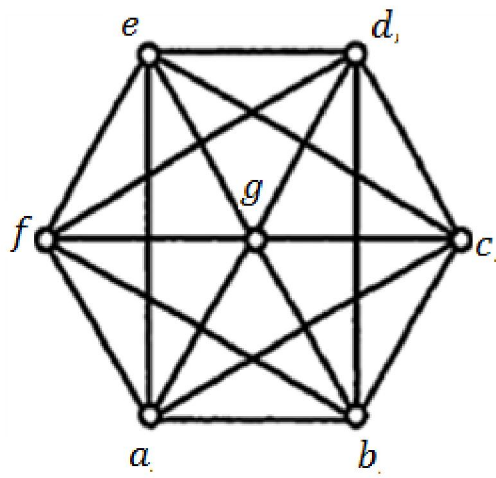
Notice that G_2 has a circuit a, b, c, d, e, f, a .The remaining edges can be drawn as shown below:



The planar representation of G_2

P3.

Show that the following graph is nonplanar.



Solution:

Notice that the graph is a connected simple graph with no loops and
$v = 7, e = 18$

Assume that the graph is planar. By Corollary 1,

$e \leq 3v - 6$, i.e., $18 \leq 3(7) - 6 = 15$, a contradiction

Therefore, the given graph is nonplanar.

P4.

Suppose that a connected planar graph has six vertices, each of degree four. Into how many regions is the plane divided by a planar representation of this graph.

Solution:

The planar graph G has 6 vertices, each of degree 4. The sum of the degrees of all the vertices is $6(4) = 24$.
By Hand shaking theorem, we have $2e = 24$, $i.e.,\quad e = 12$

By Euler's formula, we have

$v - e + r = 2,\quad i.e.,\ 6 - 12 + r = 2,\quad i.e.,\quad r = 8$

P5.

Which of these nonplanar graphs have the property that the removal of any vertex and all edges incident with that vertex produces a planar graph?

a) $\boldsymbol{K_5}$ **b)** $\boldsymbol{K_6}$ **C)** $\boldsymbol{K_{3,\ 3}}$ **D)** $\boldsymbol{K_{3,4}}$

Solution:

a) If we remove any vertex from K_5 and all edges incident with that vertex, then it produces K_4 and it is planar.

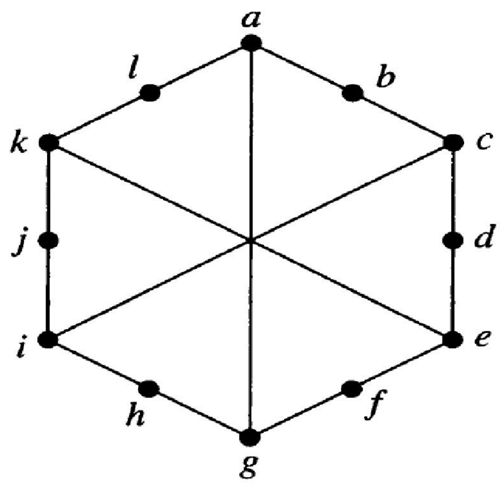
b) If we remove any vertex from K_6 and all edges incident with that vertex, then it produces K_5 and it is nonplanar.

c) If we remove any vertex from $K_{3,3}$ and all edges incident with that vertex, then it produces $K_{2,3}$ or $K_{3,2}$ and both are planar.

d) If we remove any vertex from $K_{3,4}$ and all edges incident with that vertex, then it produces $K_{3,3}$ or $K_{2,4}$ and both are nonplanar.

P6.

Determine whether the graph given below is homeomorphic to $K_{3,3}$



Solution:

We have $V = \{a, b, c, d, \ldots, j, k, l\}$. Let $v_1 = \{a, e, i\}$ and $v_2 = \{c, g, k\}$. Now, we have $K_{3,3}$ with vertex sets v_1 and v_2 ($i.e.$ a bipartition)

We obtain the given graph from $K_{3,3}$ by the following sequence of elementary sub divisions.

i) Remove $\{a, c\}$, add the vertex b and add edges $\{b, a\}$ and $\{b, c\}$

ii) Remove $\{e, c\}$, add the vertex d and add edges $\{d, e\}$ and $\{d, c\}$

iii) Remove $\{e, g\}$, add the vertex f and add edges $\{f, e\}$ and $\{f, g\}$

iv) Remove $\{i, g\}$, add the vertex h and add edges $\{h, i\}$ and $\{h, g\}$

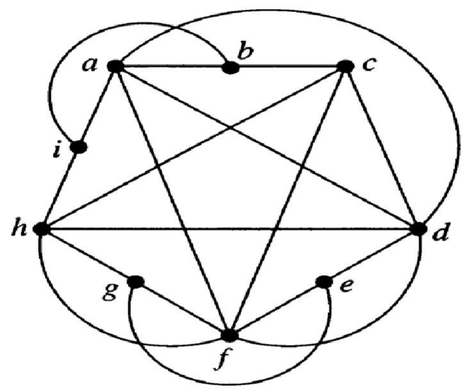
v) Remove $\{i, k\}$, add the vertex j and add edges $\{j, i\}$ and $\{j, k\}$

vi) Remove $\{a, k\}$, add the vertex l and add edges $\{l, a\}$ and $\{l, k\}$

Thus, the given graph is homeomorphic to $K_{3,3}$.

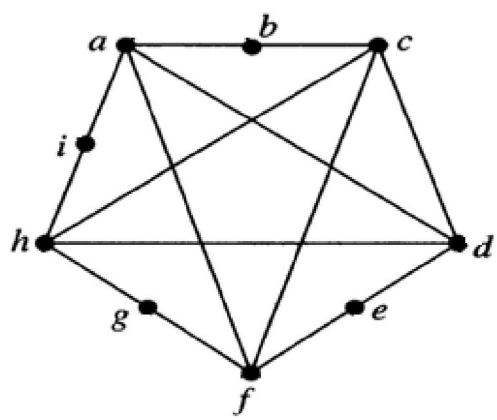
P7.

Use Kuratowski's theorem to determine whether the given graph is planar.



Solution:

Let H be the subgraph of the given graph by deleting one of the two edges between a, d; and delete the edges $\{b, i\}, \{f, d\}, \{e, g\}, \{f, h\}$.



Now consider K_5 with vertices a, c, d, f and h. We obtain H from K_5 by the following sequence of elementary subdivisions:

i) delete $\{a, c\}$, add the vertex b and add edges $\{b, a\}$ and $\{b, c\}$
ii) delete $\{a, h\}$, add the vertex i and add edges $\{i, a\}$ and $\{i, h\}$
iii) delete $\{h, f\}$, add the vertex g and add edges $\{g, h\}$ and $\{g, f\}$
iv) delete $\{f, d\}$, add the vertex e and add edges $\{e, f\}$ and $\{e, d\}$

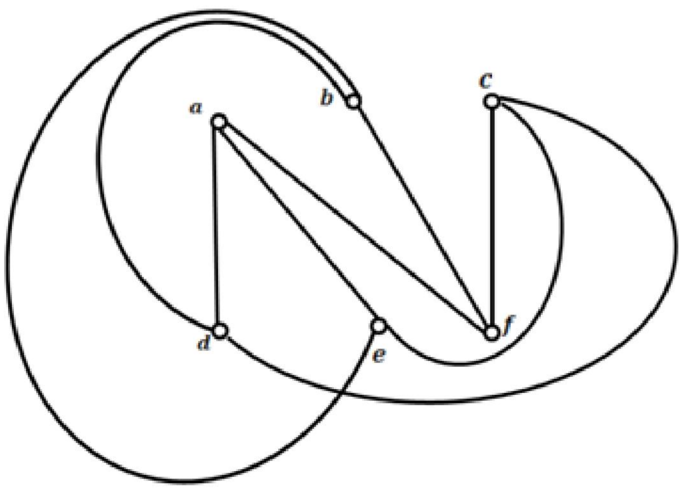
Thus, H is homeomorphic to K_5. This shows that the given graph has a subgraph homeomorphic to K_5. Therefore, by Kuratowski's theorem, the given graph is nonplanar.

P8:

Example: Show that the crossing number of $K_{3,3}$ is 1.

Solution:

First note that $K_{3,3}$ is nonplanar

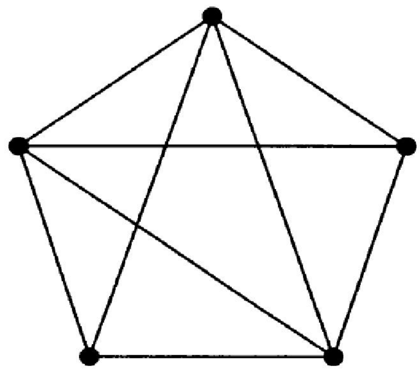


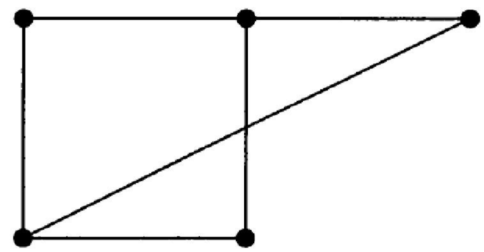
The minimum number of crossings that can occur when the graph is drawn in the plane is 1. Therefore, the crossing number of $K_{3,3}$ is 1.1

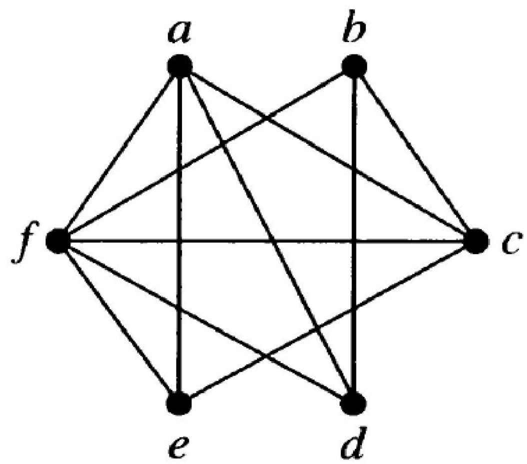
3.5 Planar Graphs

Exercises:

1. Draw the given planar graph without any crossings:





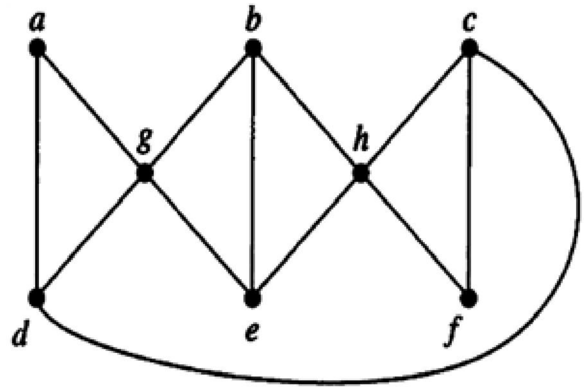


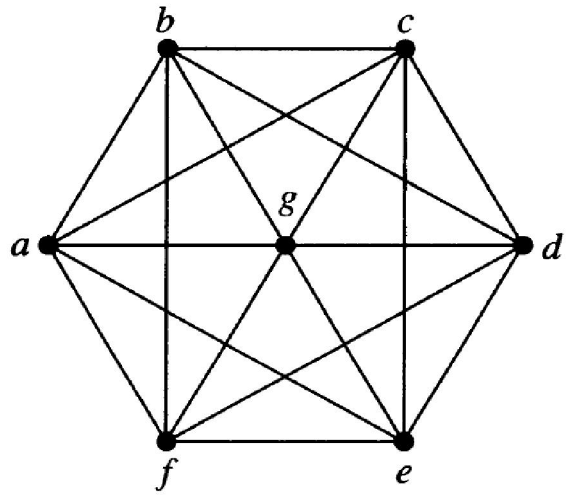
2.

a) Suppose that a connected planar graph has 8 vertices, each of degree 3. Into how many regions is the plane divided by a planar representation of this graph?

b) Suppose that a connected planar graph has 30 edges. If a planar representation of this graph divides the plane into 20 regions, how many vertices does this graph have?

3. Use Kuratowski's theorem to determine whether the given graphs is planar.





4. Find the crossing numbers of each of these nonplanar graphs.

a) K_5 b) K_7 c) $K_{3,\ 4}$ d) $K_{4,4}$

MODULE-3

Graph coloring

3.6

Graph Coloring

Consider the problem of determining the least number of colors that can be used to color a map so that adjacent regions never have the same color.

For example, for the map shown below, four colors are sufficient, but three colors are not enough.

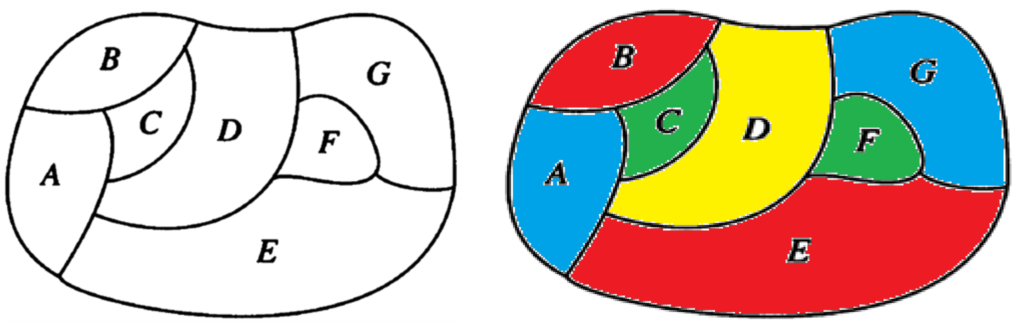


Figure-1

For the map shown below three colors are sufficient but two are not enough.

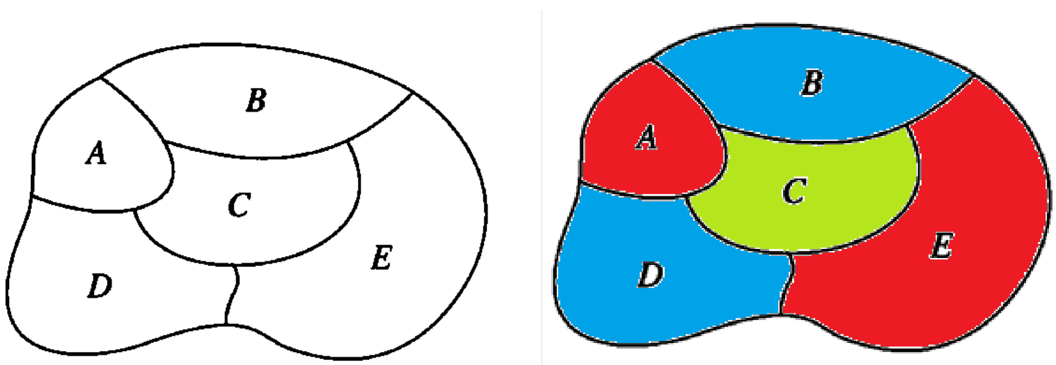
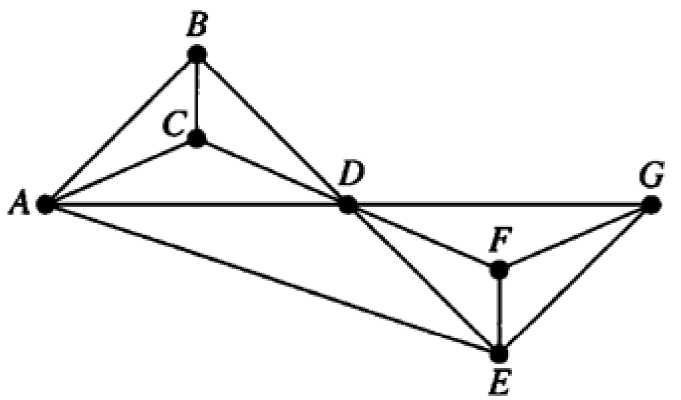
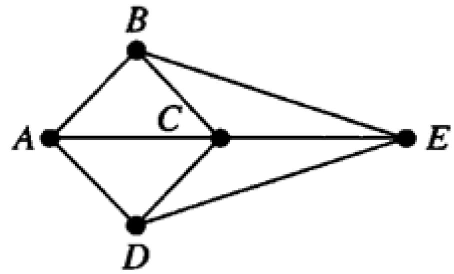


Figure-2

Representation of maps: Each map in the plane can be represented by a graph. Each region of the map is represented by a vertex and edges connect two vertices if the regions represented by these vertices have a common border. Two regions that touch at only one point are not considered adjacent. The graph so obtained corresponding to the map is called the ***dual graph*** of the map. It is clear that the dual graph of maps, so constructed are planar (That is, the dual graph in the plane corresponding to a map is a planar graph).

The following are the dual graphs corresponding to maps in fig.1 and fig.2 respectively.





The problem of coloring the regions of a map is equivalent to the problem of coloring the vertices of the dual graph so that no two adjacent vertices in this graph have the same color.

Graph coloring: A ***coloring*** of a simple graph is the assignment of a color to each vertex of the graph so that no two adjacent vertices are assigned the same color.

For most graphs a coloring can be found that uses fewer colors than the number of vertices in the graph. What is the least number of colors necessary?

Chromatic number: The ***chromatic number*** of a graph is the least number of colors needed for a coloring of this graph.

The chromatic number of a graph G is denoted by $\chi(G)$. (where χ is the Greek letter ***chi***).

Note that the chromatic number of a planar graph is same as the minimum number of colors required to color a planar map so that no two adjacent regions are assigned the same color. This question has been studied for more than a 100 years. The answer is provided by one of the most famous theorems in mathematics.

Theorem 1: ***The Four Color Theorem: The chromatic number of a planar graph is no greater than four.***

The Four Color Theorem was originally posed as a conjecture in the 1850's. It was finally proved by the American mathematicians ***Kenneth Appel*** and ***Wolfgang Haken*** in 1976. Prior to 1976, many incorrect proofs were published, often with hard to find errors. In addition, many futile attempts were made to construct counter examples by drawing maps that require more than four colors.

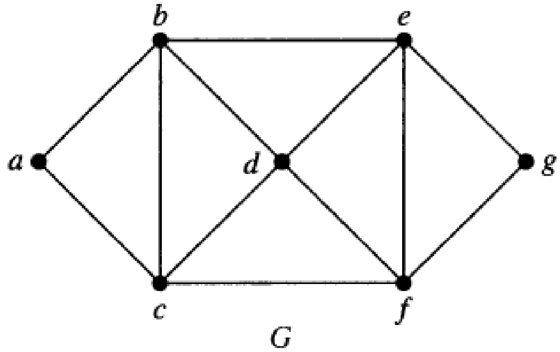
Perhaps the most notorious fallacious proof in all of mathematics is the incorrect proof of Four Color Theorem published in 1879 by a London barrister and a mateur mathematician, Alfred Kempe. Mathematicians accepted his proof as correct until 1890, when Percy Heawood found an error that made Kempe's argument incomplete. However, Kempe's line of reasoning turned out to be the basis of the successful proof given by Appel and Haken. Their proof relies on a careful case-by-case analysis carried out by computer. They showed that if the Four Color Theorem was false, there would have to be a counterexample of one of approximately 2000 different types, and they then showed that none of these types exists. They used over 1000 hours of computer time in their proof. This proof generated a large amount of controversy, because computers played such an important role in it. For example, could there be an error in a computer program that led to incorrect results? Was their argument really a proof it is depended on what could be unreliable computer output?

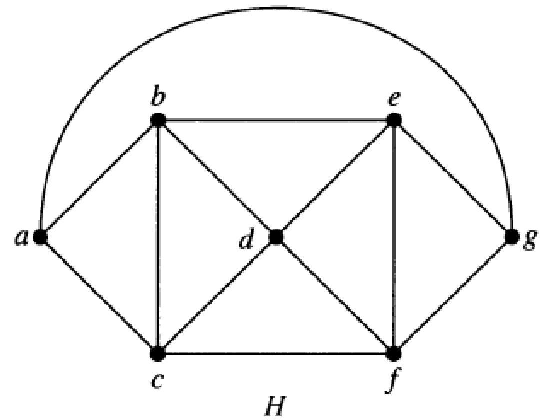
Note:

(i) The Four Color Theorem applies only to planar graphs
(ii) Nonplanar graphs can have arbitrarily large chromatic numbers.

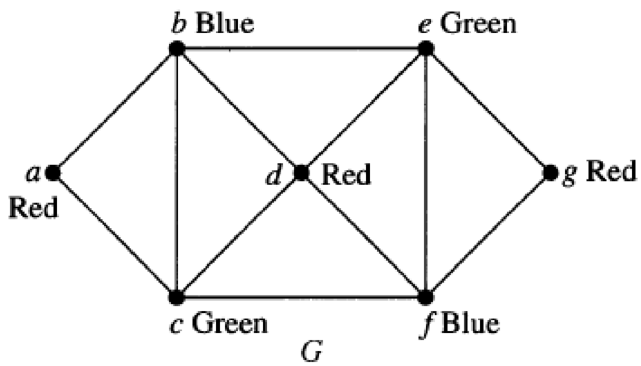
To show that the chromatic number of a graph is k, first, we must show that the graph can be colored with k colors (and this can be done by constructing such a coloring) and then show that the graph cannot be colored using fewer than k colors.

Example: What are the chromatic numbers of the graphs G and H shown below.



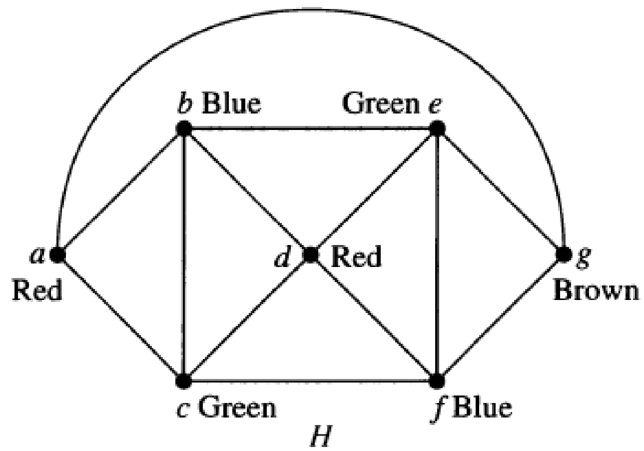


Solution: Notice that the vertices a, b and c in G are pairwise adjacent. Therefore, we need at least three colors. Thus, the chromatic number of G is at least three.



Now, assign colors red, blue and green to the vertices a, b and c respectively. Since d is adjacent to b(blue) and c(green), d must be colored red. Further, e must be colored green because it is adjacent to b(blue) and e(red) and f must be colored blue because it is adjacent to d(red) and e(green). Finally, g must be colored red because it is adjacent to f(blue) and e(green). Thus, G can be colored using exactly three colors. Therefore $\chi(G) = 3$.

Notice that the graph H is made up of the graph G with an edge $\{a, g\}$. Any attempt to color H using three colors must follow the same steps as that used to color G, except at the last stage, i.e., coloring the vertex g.

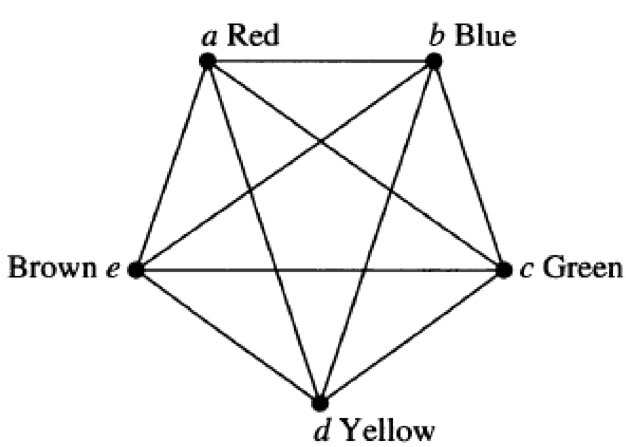


Now observe that g is adjacent to vertices a(red), e(green) and f(blue). This shows that a fourth color, say brown, needs to be used. Thus, H can be colored using exactly 4 colors. Therefore, $\chi(H) = 4$.

Example: What is the chromatic number of K_n?

Solution: A coloring of K_n can be constructed using n colors by assigning a different color to each vertex. Since every two vertices are adjacent in K_n , no two vertices can be assigned the same color. This shows that K_n cannot be colored using fewer than n colors.Thus, K_n colored using exactly n colors. Therefore, $\chi(K_n) = n$.

A coloring of K_5 using five colors is shown below:

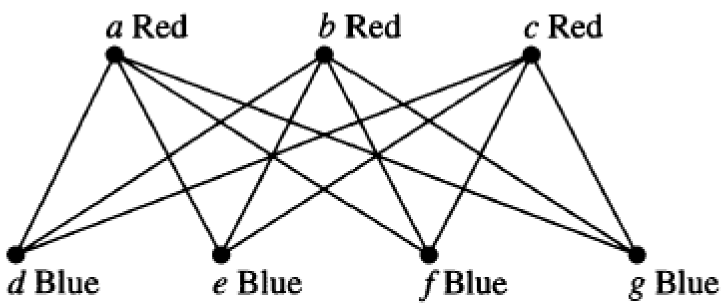


A coloring of K_5

Note: Recall that K_n is nonplanar when $n \geq 5$ and this result $\chi(K_n) = n$ does not contradict the Four Color Theorem.

Example: Show that $\chi(K_{m,n}) = 2$.

Solution: Since $K_{m,n}$ is a bipartite graph, its $m + n$ vertices are partitioned into V_1 and V_2 with $|V_1| = m$ and $|V_2| = n$. We color the vertices of V_1 with one color and the vertices of V_2 with a second color. Because edges connect only a vertex of V_1 and a vertex of V_2 , no two adjacent vertices have the same color. This shows that $K_{m,n}$ can be colored using exactly two colors. Therefore, $\chi(K_{m,n}) = 2$.



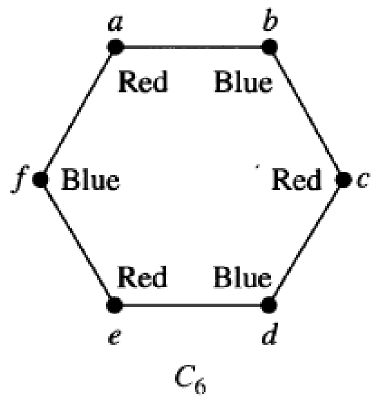
A coloring of $K_{3,4}$

Note: The chromatic number of a bipartite graph is **two.**

Example: Determine the chromatic number of C_n(the cycle graph with n vertices) $n \geq 3$.

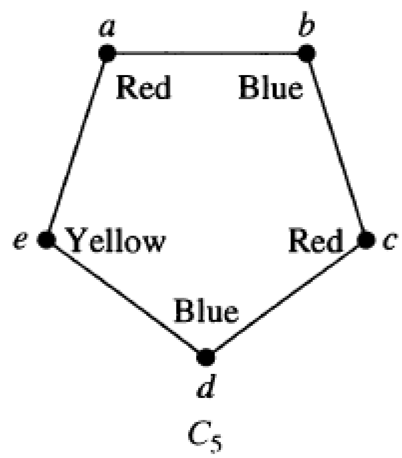
Solution: We consider two cases.

(i) Let n be even. Choose a vertex and color it red. Proceed around the graph in a clockwise direction (because C_n is planar) coloring the second vertex blue, the third vertex red and so on. Finally, the n^{th} vertex can be colored blue, because the two vertices adjacent to it, namely, $(n-1)^{\text{th}}$ and the first vertices, are both colored red. Thus, $\chi(C_n) = 2$, when n is an even positive integer with $n \geq 4$.



Coloring of C_6

(ii) Let n be odd. Choose a vertex and color it red. Proceed as in the above case in the clockwise direction. Finally we note that the n^{th} vertex is adjacent to two vertices of different colours, namely, the first vertex (red) and $(n-1)^{\text{th}}$ vertex(blue). Hence, a third color must be used. Thus $\chi(C_n) = 3$, when n is an odd positive integer with $n \geq 3$.



Coloring of C_5

Summarising, when n is a positive integer, $n \geq 3$.

$$\chi(C_n) = \begin{cases} 2, & \text{if } n \text{ is even} \\ 3, & \text{if } n \text{ is odd} \end{cases}$$

Note: The best algorithm known for finding the chromatic number of a graph have exponential worst-case time complexity (in the number of vertices of the graph).

Applications of Graph Colorings

Graph coloring has a variety of applications to problems involving scheduling and assignments.

Scheduling Final Examinations:

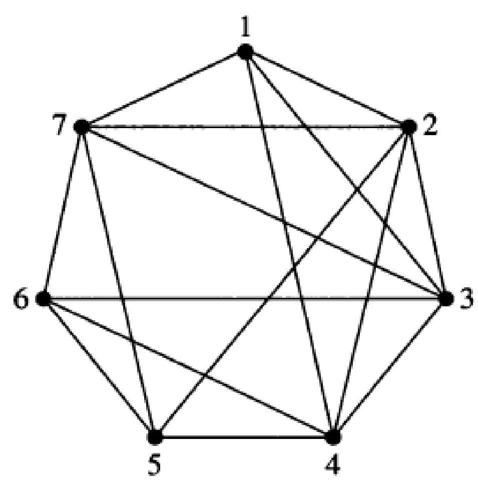
How can the final exams at a university be scheduled so that no student has two exams at the same time.

Solution: This scheduling problem can be solved using a graph model, with vertices representing courses and with an edge between two vertices if there is a common student in the courses they represent. Each time slot for a final exam is represented by a different color. A scheduling of the exams corresponds to a coloring of the associated graph.

For example, suppose that there are seven finals to be scheduled. Suppose that the courses are numbered as 1,2,3,…,7. Suppose that the following pairs of courses have common students:

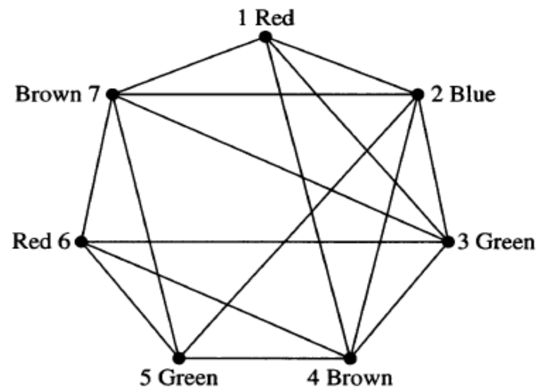
$$1,2\ ;\ \ 1,3\ \ ;\ 1,4\ \ ;\ \ 1,7\ ;\ 2,3\ \ ;2,4\ \ ;2,5\ ;\ 2,7\ ;$$
$$3,4\ ;\ \ 3,6\ ;\ \ 3,7\ \ ;\ \ 4,5\ ;\ 4,6\ \ ;5,6\ \ ;5,7\ ;\ 6,7\ .$$

The graph associated with this set of classes is shown below:



The graph representing the scheduling of final exams

A scheduling consists of a coloring of this graph. A coloring of the graph is shown below:

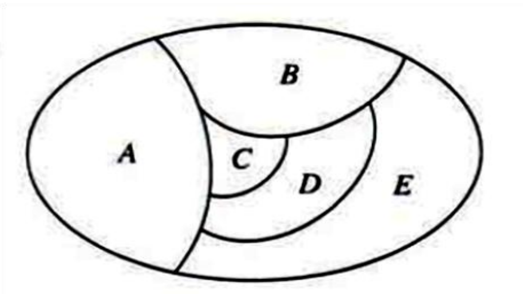


Notice that the chromatic number of this graph 4. Therefore, four time slots are needed and the associated schedule is given below:

Time period	Courses
I	1,6
II	2
III	3,4
IV	4,7

P1:

Construct the dual graph for the map given below:

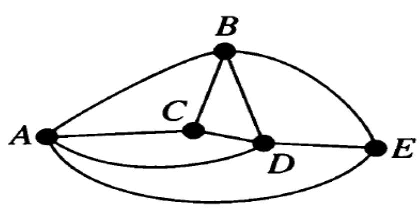


Find the number of colors needed to color the map so that no two adjacent regions have the same color.

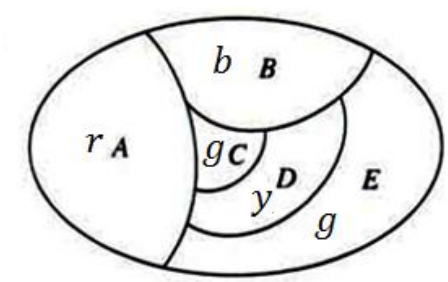
Solution:

Each map in the plane can be represented by a graph. Each region of the map is represented by a vertex. Edges connect two vertices if the regions represented by these vertices have a common border. The resulting graph is called the ***dual graph*** of the map.

The dual graph of the given map is



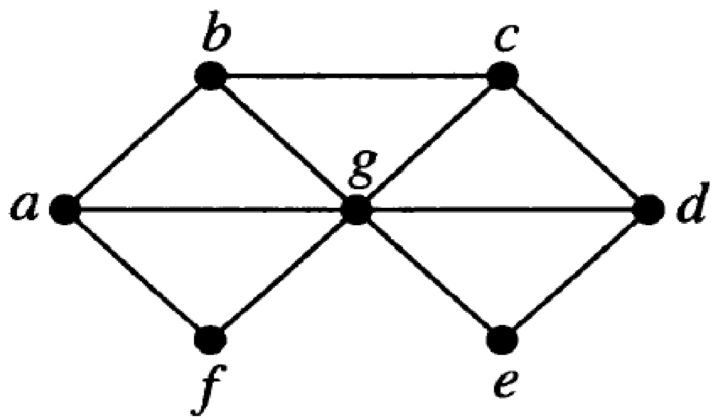
The number of colors required to color the graph is 4



r-red, b-blue , g-green, y-yellow

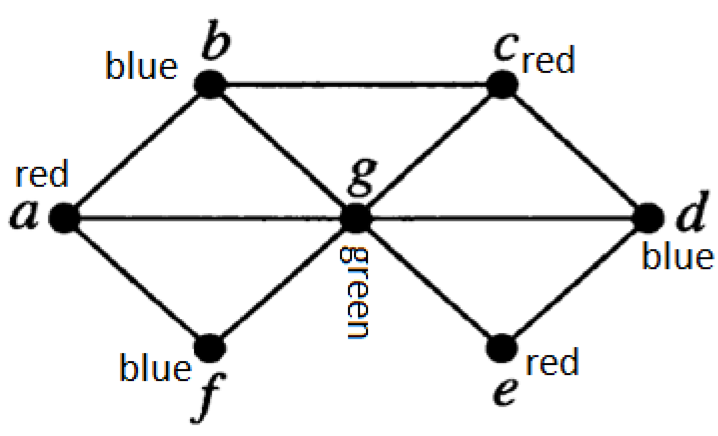
P2:

Find the chromatic number of the graph



Solution:

Assign the color green to g notice that g is adjacent to every vertex. Therefore, no vertex receives the colour green. Assign color red to the vertex a. Observe that the vertices c and e are not adjacent to the vertex a and so we assign color red to the vertices c and e. Now assign color blue to the vertex b and observe that the vertices d and f are not adjacent to b. So, assign the color blue to the vertices d and f.



It is a coloring of the graph and $\chi(G) = 3$.

P3:

Which graphs have a chromatic number 1.

Solution:

Graphs with no edges will have a chromatic number 1.

P4:

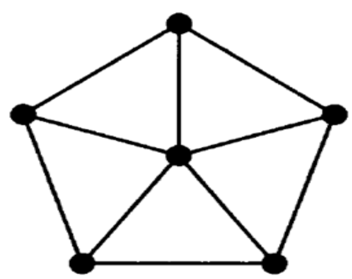
What is the chromatic number of W_n.

Solution:

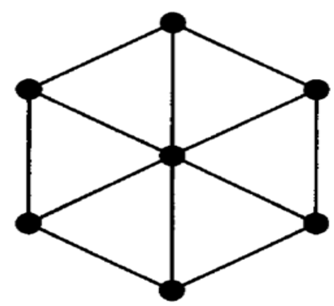
Note that we obtain the wheel graph W_n by adding an additional vertex to the cycle graph C_n , $n \geq 3$ and connecting this additional vertex to each of the n vertices of C_n. Assign a colour 1 to this additional vertex.

Now, no other vertex receives colour 1 because the additional vertex is adjacent to all other vertices. We have to colour C_n. It is known that $\chi(C_n)$ is 2 if n is even and is 3 if n is odd. Thus

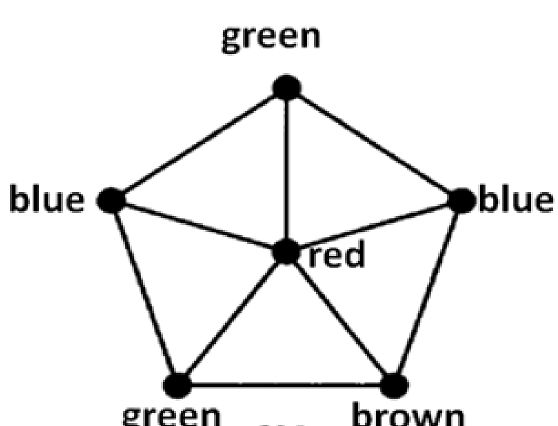
$$\chi(W_n) = \begin{cases} 3 & if\ n\ is\ even\ , n \geq 4 \\ 4 & if\ n\ is\ odd\ , n \geq 3 \end{cases}$$



W_5

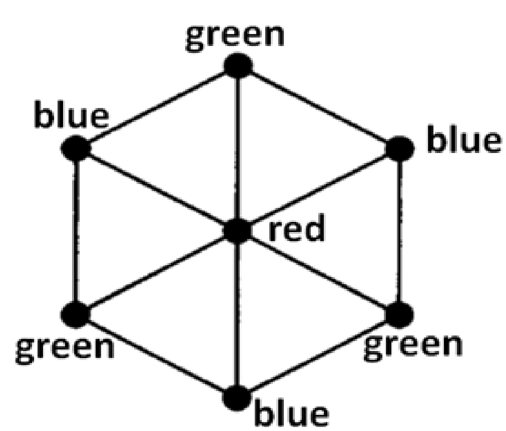


W_6



W_5

$\chi(W_5) = 4$



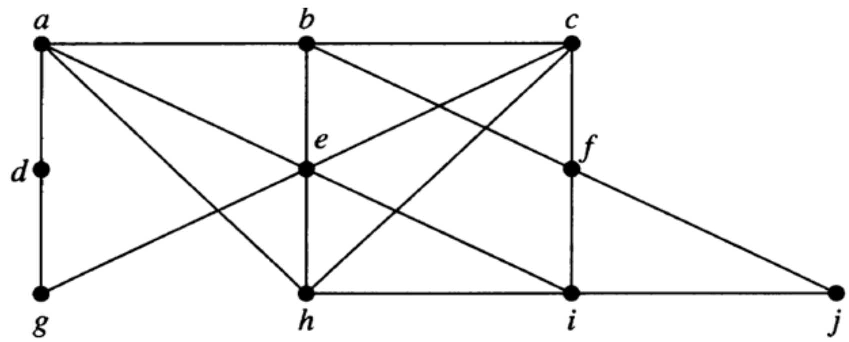
W_6

$\chi(W_6) = 3$

P5:

a) Construct a coloring of the graph G using the algorithm

b) Find the chromatic number of G



Solution:

The given graph is a simple graph. We find a coloring by Welsh-Powell algorithm

List the vertices of in order of non increasing degrees as shown below.

Vertex :	e	a	b	c	f	h	i	d	g	j
Degree :	6	4	4	4	4	4	4	2	2	2

Assign color 1 to the vertex e and to the vertex in the list not adjacent to e, namely the vertex f. The vertex next to f in the list not adjacent to a, e (the vertices colored color 1) is d. Assign color 1 to d. Thus

Vertex :	e	a	b	c	f	h	i	d	g	j
Degree :	6	4	4	4	4	4	4	2	2	2
Color :	1				1			1		

Now, assign color 2 to the vertex a (the first vertex in the list not already colored). Successively assign color 2 to vertices in the list,that have not already been colored, and are not adjacent to vertices assigned color 2.

The vertex not adjacent to a in the list is c, assign color 2 to c. The vertex not adjacent to a and c in the list is i, assign color 2 to i. The vertex not adjacent to a, c, i is g, assign color 2 to g. Thus

Vertex :	e	a	b	c	f	h	i	d	g	j
Degree :	6	4	4	4	4	4	4	2	2	2
Color :	1	2		2	1		2	1	2	

Now assign color 3 to b and proceeding as above we get

Vertex :	e	a	b	c	f	h	i	d	g	j
Degree :	6	4	4	4	4	4	4	2	2	2
Color :	1	2	3	2	1	3	2	1	2	3

The following is a coloring of the graph

Color 1 : e, f, d

Color 2 : a, c, i, g

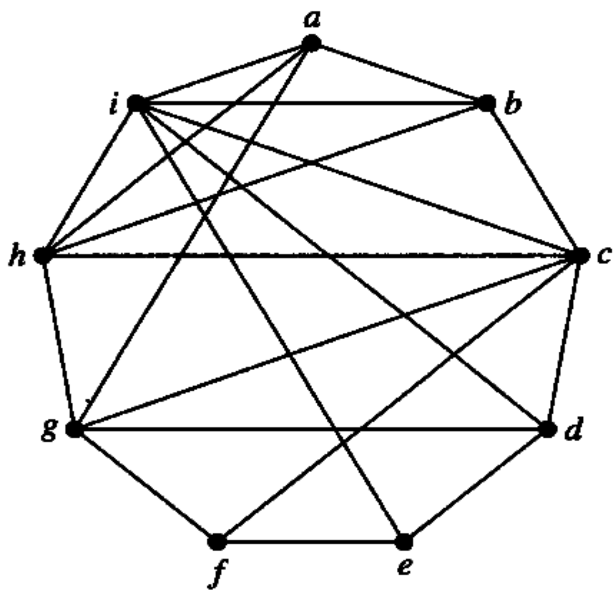
Color 3 : b, h, j

The vertices e, a and b are connected to each other, so at least three colors are need to color G.

Thus, $\chi(G) = 3$.

P6:

Find the chromatic number of the graph



Solution:

Following the steps of the Welsh-Powell algorithm yields the following data.

Vertex :	c	i	g	h	a	b	d	e	f
Degree :	6	6	5	5	4	4	4	3	3
Color :	1	2	2	3	1	4	3	1	3

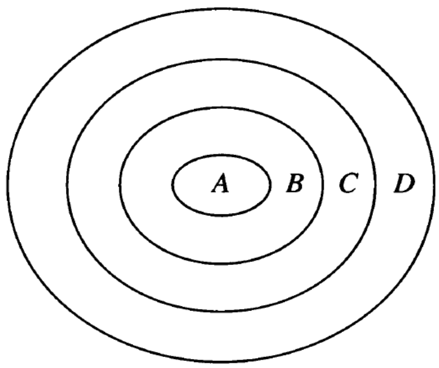
The vertices c, i, h and b are connected to each other, so at least four colors are needed to color the given graph G. Thus

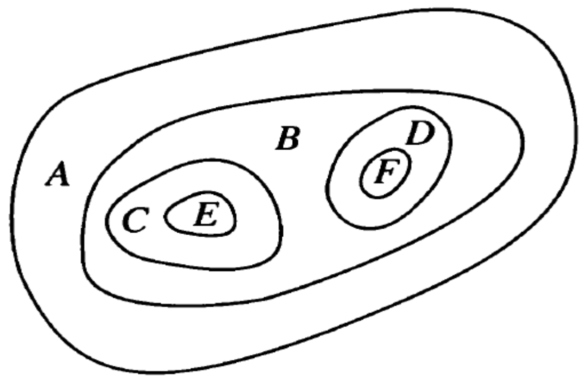
$$\chi(G) = 4$$

3.6. Graph Coloring

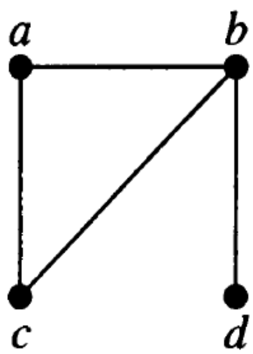
Exercise:

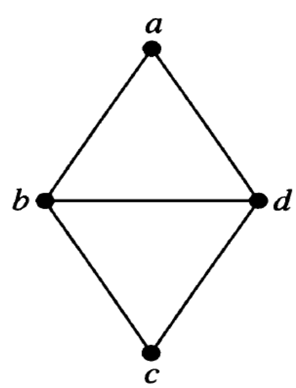
1. Construct the dual graph for the map shown below. Then find the number of colors needed to color the map so that no two adjacent regions have the same color:

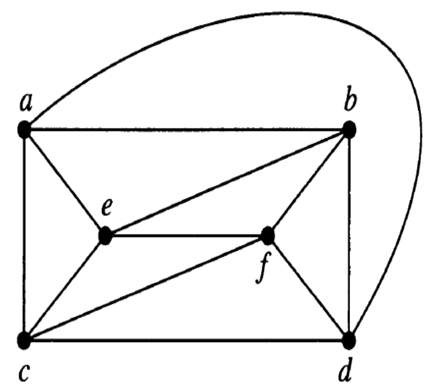


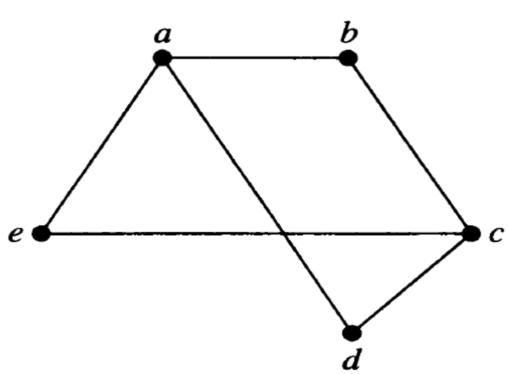


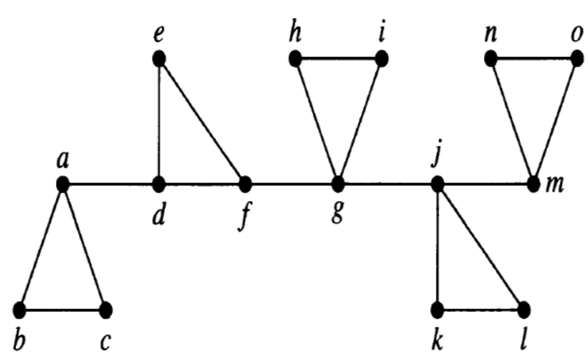
2. Find the chromatic number of the graphs given below:











3. What is the chromatic number of W_n ?

4. Schedule the final exams for Math 115, Math 116, Math 185, Math 195, CS 101, CS 102, CS 273 and CS 473, using the fewest number of different time slots, if there are no students taking both Math 115 and CS 473, both Math 116 and CS 473, both Math 195 and CS 101, both Math 195 and CS 102, both Math 115 and Math 116, both Math 115 and Math 185, and both Math 185 and Math 195, but there are students in every other combination of courses.

5. How many different channels are needed for six stations located at the distances shown in the table, if two stations cannot use the same channel when they are within 150 miles of each other?

	1	*2*	*3*	*4*	*5*	*6*
1	—	85	175	200	50	100
2	85	—	125	175	100	160
3	175	125	—	100	200	250
4	200	175	100	—	210	220
5	50	100	200	210	—	100
6	100	160	250	220	100	—

MODULE-4

Trees

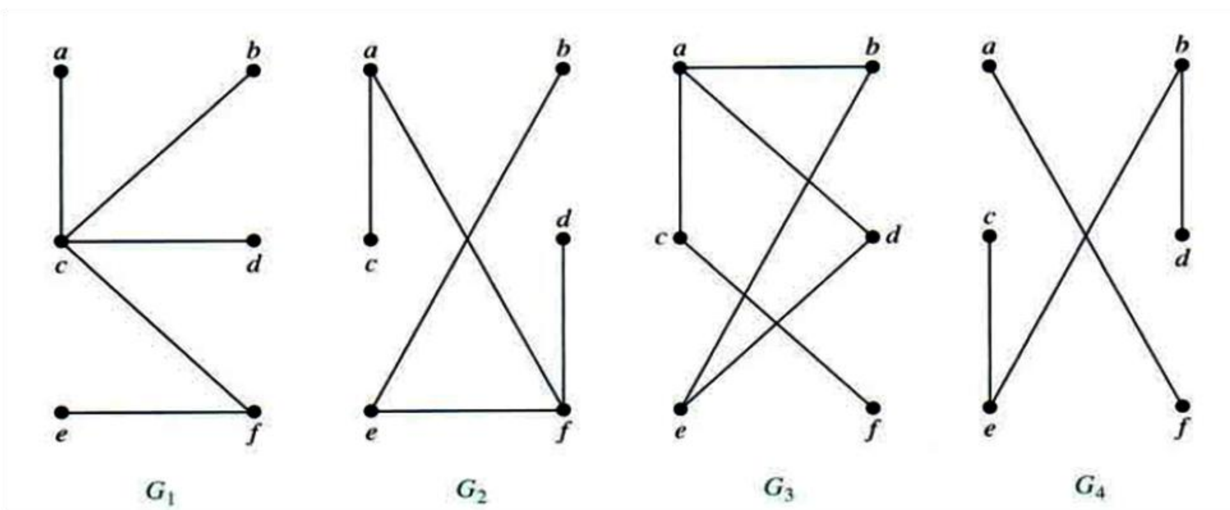
3.7

Trees

We have seen how graphs can be used to model and solve many problems. In this module we will focus on a particular type of graph called a **tree.** It is so named because such a graph resembles a tree. For example, family trees use vertices to represent the members of a family and edges to represent parent-child relationships.

Tree: A **tree** is a connected undirected graph with no simple circuits.
A tree does not contain multiple edges or loops, because it does not contain simple circuits. Therefore, a tree must be a simple graph.

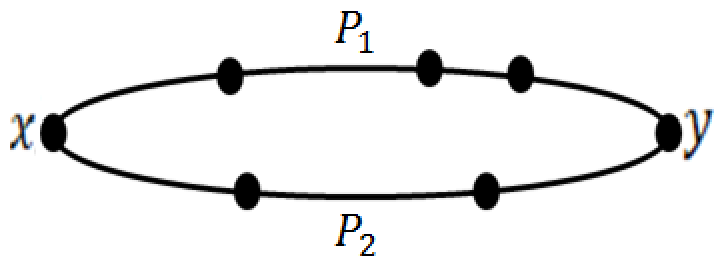
Example 1: Which of the following graphs shown below are tree?



Solution: The graphs G_1 and G_2 are trees, because both are connected graphs with no simple circuits. The graph G_3 is not a tree, because it contains a simple circuit a, b, e, d, a . The graph G_4 is not a tree, because it is not connected.

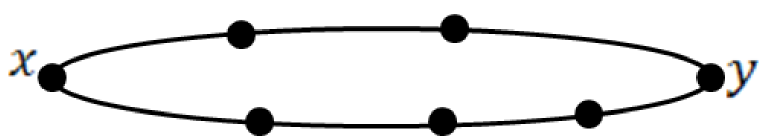
Theorem 1: An undirected graph is a tree if and only if there is a unique simple path between any two of its vertices.

Proof: Let T be an undirected graph.
Suppose that T is a tree. Let x and y be any two vertices. Because T is connected, there is a simple path between x and y.



To show that this path is unique, assume that there is another simple path between x and y. Then the path formed by combining the first path from x to y followed by the path from y to x(obtained by reversing the order of the second path from x to y) would form a simple circuit. This is a contradiction. Hence, there is a unique simple path between any two vertices of a tree.

Conversely, suppose that there is a unique simple path between any two vertices in the graph T. Therefore, T is connected. Assume that T has a simple circuit containing two vertices x and y. Then there would be two simple paths

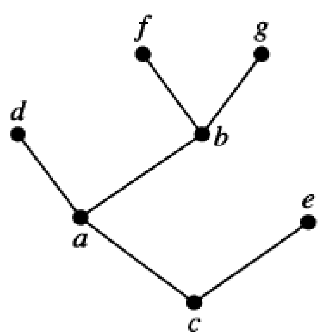


between x and y- a contradiction. This shows that T has no simple circuits. Thus, T is connected and has no simple circuits. Therefore, T is a tree.
Hence the theorem.

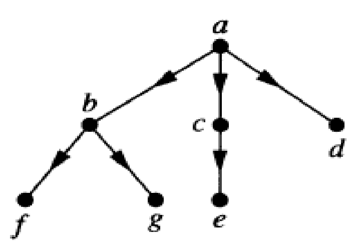
In many applications of trees, a particular vertex of a tree is designated as the *root***.** Because there is a unique path from the root to each vertex of the graph, we direct each edge away from the root. Once, we specify a root, we can assign a direction to each edge. Thus, a tree together with its root produces a directed graph called a *rooted tree.*

Rooted tree: A **rooted tree** is a tree in which one vertex is designated as the root and every edge is directed away from the root.
We can change any undirected tree into a rooted tree by choosing any vertex as the root.

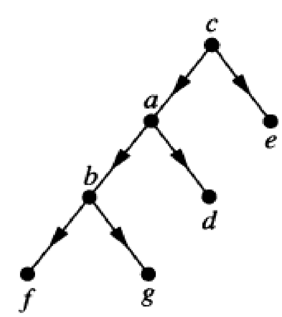
We usually draw a rooted tree with its root at the top of the graph. The rooted treed formed by designating a as the root and c as the root respectively in the tree T are given below:



T



Rooted tree with a as a root



Rooted tree with c as a root

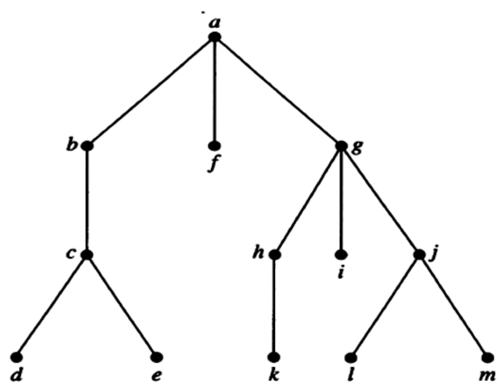
Note:

i. Different choices of the root produces different rooted trees.
ii. The arrows indicating the directions of the edges in a rooted tree can be omitted, because the choice of the root determines the direction of the edges.

Terminology: The terminology for trees has botanical and genealogical origins. Suppose, that T is a rooted tree. If v is a vertex in a tree T other than the root, then the **parent** of v is the unique vertex u such that there is a directed edge from u to v. When u is the parent of v, v is called a **child** of u. Vertices with the same parent are called **siblings**. The **ancesestors** of a vertex v other than the root are the vertices in the path from the root to v, excluding v itself and including the root, $i.e$, its parent, its parent's parent, and so on, until the root is reached. The **descendents** of a vertex v are those vertices that have v as an ancestor. A vertex of a tree is called a **leaf** if it has no **children**. Vertices that have children are called **internal vertices.** The root is an internal vertex unless it is the only vertex in the graph, in which case it is a leaf.

If a is a vertex in a tree, the **subtree** with a as its root is the subgraph of the tree consisting of a, its descendents and all edges incident with these descendents

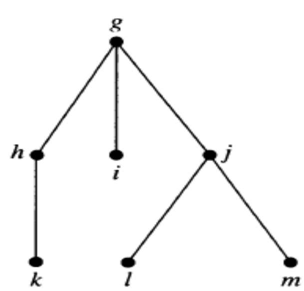
For the rooted tree T given below:



A Rooted Tree *T*.

i. The root of the rooted tree T is a vertex a.
ii. The parent of c is b
iii. The children of g are h, i and j
iv. The siblings of h are i and j
v. The ancestors of e are c, b and a
vi. The descendents of b are c, d and e
vii. The internal vertices of T are a, b, g, c, h and j.
viii. The leaves of T are d, e, f, i, k, l and m

The subtree rooted at g is shown below

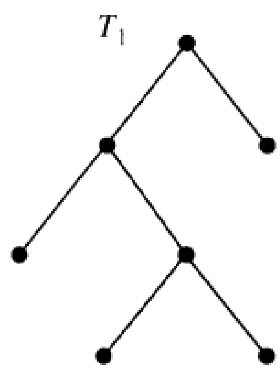


Rooted trees with the property that all the internal vertices have the same number of children are used in many applications. Such trees are used to study the problems related to searching, sorting and coding.

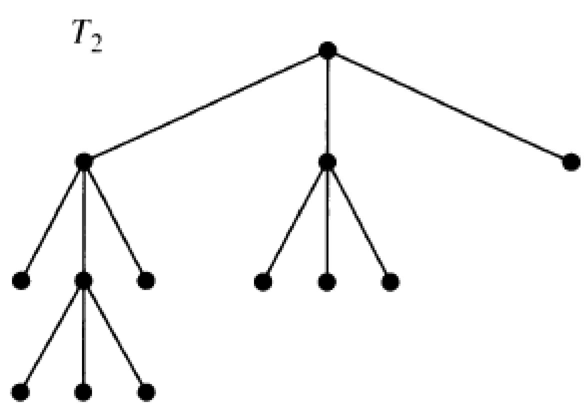
m −ary, full m −ary and binary trees: A rooted tree is called an **m −ary tree ,** if every internal vertex has no more than m children . A rooted tree is called a **full m −ary tree**, if every internal vertex has exactly m children. An **m −ary tree** with $m = 2$ is called a **binary tree.**

A **complete $m - ary$ tree** is a full $m - ary$ tree **,** where every leaf is at the same level**.**

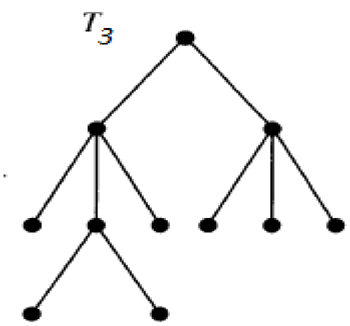
For example:



T_1 is a full binary tree, because each of its internal vertices has exactly two children.



T_2 is a full 3 −ary tree, because each of its internal vertices has exactly three children.

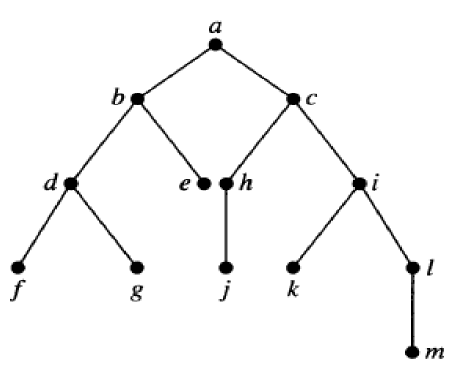


T_3 is not a full m −ary tree for any m, because some of its internal vertices have two children and others have three children. It is a 3 −ary tree, because each internal vertex has no more than three children.

Ordered root tree: An **Ordered tree** is a rooted where the children of each internal vertex are ordered.
Ordered root trees are drawn such that the children of each internal vertex are shown in the order from left to right.

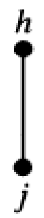
In an ordered binary tree(usually called just a binary tree), if an internal vertex has two children, the first child is called the **left child** and the second child is called the **right child**. The tree rooted at the left child of a vertex v is called the **left subtree** of v and the tree rooted at the right child of a vertex v is called the **right subtree** of v

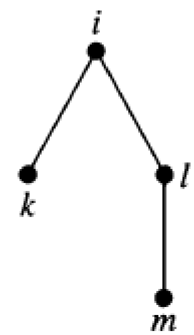
For example in the tree T shown below, the left child of d is f and right child is g



A binary tree T

The following are the left subtree of the vertex c and the right subtree of the vertex c respectively:





Left subtree of the vertex c Right subtree of the vertex c

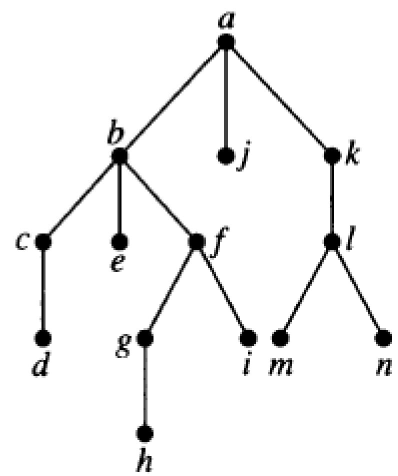
The following are the concepts related to the *balanced tree*.

Level of a vertex: The level of a vertex v in a rooted tree is the length of the unique path from the root to the vertex v. The level of the root is defined to be zero.

The height of the rooted tree: The height of a rooted tree is the maximum of the levels of the vertices. That is, the height of a rooted tree is the length of the longest path from the root to any vertex.

A rooted m −ary tree of height h **is balanced** if all its leaves are at levels h or $h - 1$

Example 2: Find the level of each vertex in the rooted tree given below. Find the height of the tree

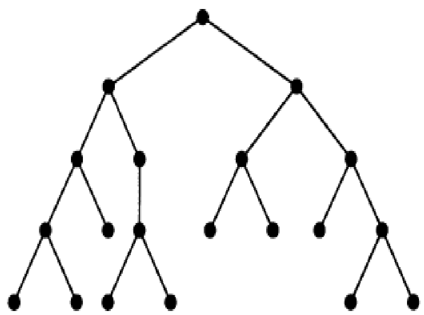


Solution:

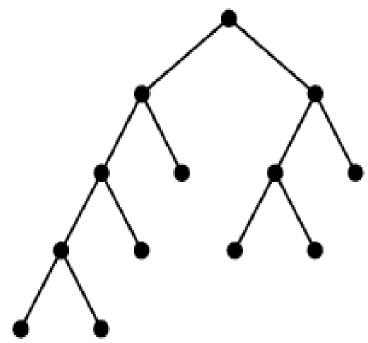
Vertex	Level
a (root)	0
b, j, k	1
c, e, f, l	2
d, g, i, m, n	3
h	4

The height of the tree is 4, because the largest level of any vertex is 4.

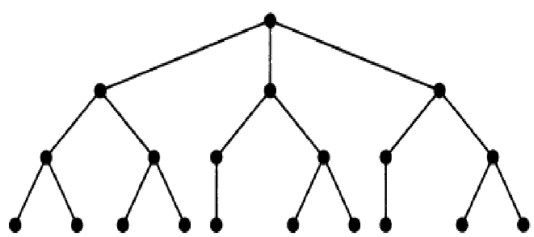
Example 3: which of the following rooted trees shown below are balanced



T_1



T_2



T_3

Solution: The height of T_1 is 4. Notice that all its leaves are at levels 3 and 4. Therefore, T_1 is a balanced tree.

The height of T_2 is 4. Notice, that all its leaves are at levels 2,3 and 4. Therfore, T_2 is not a balanced tree.

The height of T_3 is 3 . Notice that all its leaves are at level 3.Therefore, T_3 is a balanced tree

Properties of Trees: We often need results related to the number of edges and vertices in various types of trees.

Theorem 2: A tree with $\boldsymbol{n}$ vertices has $\boldsymbol{n-1}$ edges.

Proof: We furnish proof by mathematical induction. Note that for any tree, we can choose a root and consider the rooted tree.

Basis Step: When $n = 1$, a tree with one vertex has no edges. Thus, The result is true for $n = 1$.

Inductive Step: The induction hypothesis is: Every tree with k vertices has $k - 1$ edges, where k is a positive integer. Let T be a tree with $k + 1$ vertices. Let v be a leaf of T(this is possible since the tree is finite). Let w be the parent of v.We remove the vertex v and the edge connecting w. The resulting graph is a tree T' with k vertices. By induction hypothesis T' has $k - 1$ edges. It follows that T has k edges because it has one more edge than T' ($i.e$ the edge connecting v and). By mathematical induction the result follows.

The following theorem gives the number of vertices in a full m –ary tree with a specified number of internal vertices. Throughout, the discussion n denotes the number of vertices in a tree.

Theorem 3: A full m –ary tree with i internal vertices contains $n = mi + 1$ vertices.

Proof: Notice that every vertex, except the root, is the child of all internal vertices. Since each of the i internal vertices has exactly m children, there are mi vertices in the tree other than the root. Therefore, the tree has $n = mi + 1$ vertices. Hence the theorem

Let T be a full m –ary tree with n vertices.Let i be the number of internal vertices and l be the number of leaves in T. The following theorem gives the relationships among m, n, i and l.

Theorem 4: A full m –ary tree with n vertices has $i = \frac{n-1}{m}$ internal vertices and $l = \frac{(m-1)n+1}{m}$ vertices.

Proof: Let n, i and l respectively denote the number of vertices, the number of internal vertices and the number of leaves of an m –ary tree T. By Theorem 1 , $n = mi + 1$. Note that each vertex is either a leaf or an internal vertex. Therefore, $n = l + i$.Solving for i in $n = mi + 1$, we get $i = \frac{n-1}{m}$. Substituting the expression for i in the equation $n = l + i$ we obtain

$$l = n - i = n - \frac{(n-1)}{m} = \frac{(m-1)n+1}{m}$$

Corollary 1: A full m −ary tree with

(i) i Internal vertices have $n = mi + 1$ vertices and $l = (m-1)i + 1$ leaves.

(ii) l leaves have $n = \frac{ml-1}{m-1}$ vertices and $i = \frac{l-1}{m-1}$ internal vertices.

Example 4: Suppose that someone starts a chain letter. Each person who receives the letter is asked to send it on to four other people. Some people do this, but others do not send any letters. How many people have seen the letter, including the first person, if no one receives more than one letter and if the chain letter ends after there have been 100 people who read it but did not send it out? How many people sent out the letter?

Solution: The chain letter can be represented by a full 4 −ary tree, $i.e.\ m = 4$. The internal vertices (i) correspond to people who sent out the letter and the leaves (l) correspond to people who did not send it out.

Given that 100 people did not send out the letter, therefore $l = 100$ .The number of people who have seen the letter n and

$$n = \frac{ml-1}{m-1} = \frac{4.100-1}{4-1} = 133$$

The number of internal vertices $i = n - l = 133 - 100 = 33$ .Thus 33 people sent out the letter.

The following result estimates the number of leaves in an m −ary tree.

Theorem 5: There are atmost m^h leaves in an m −ary tree of height h

Corollary 2: if an m −ary tree of height h has l leaves, then $h \geq \lceil log_m l \rceil$.
If the m −ary tree is full and balanced, then $h = \lceil log_m l \rceil$
(Here $\lceil x \rceil$ is the least integer grater than or equal to x)

Note: A complete m −ary tree of height h has m^h leaves

Trees as Models: Trees are used as models in such diverse areas as Computer Science, Chemistry, Geology, Botany and Psychology.

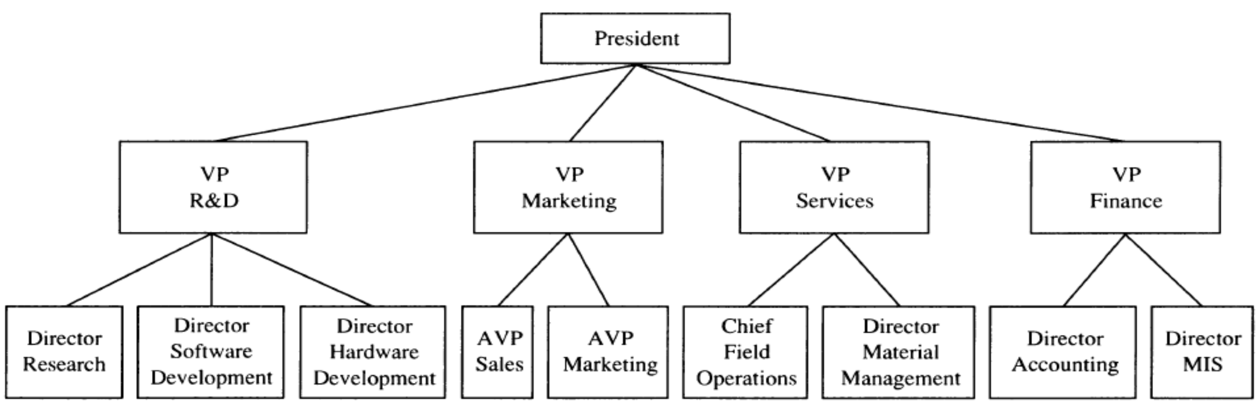
1. **Saturated Hydrocarbons and Trees**

Graphs can be used to represent molecules, where atoms are represented by vertices and bonds between them by edges.

The English mathematician Arthur Cayley discovered trees in 1857 when he was trying to enumente the isomers of compounds of the form C_nH_{2n+2}, which are called *Saturated Hydrocarbons*

2. **Representing Organizations**

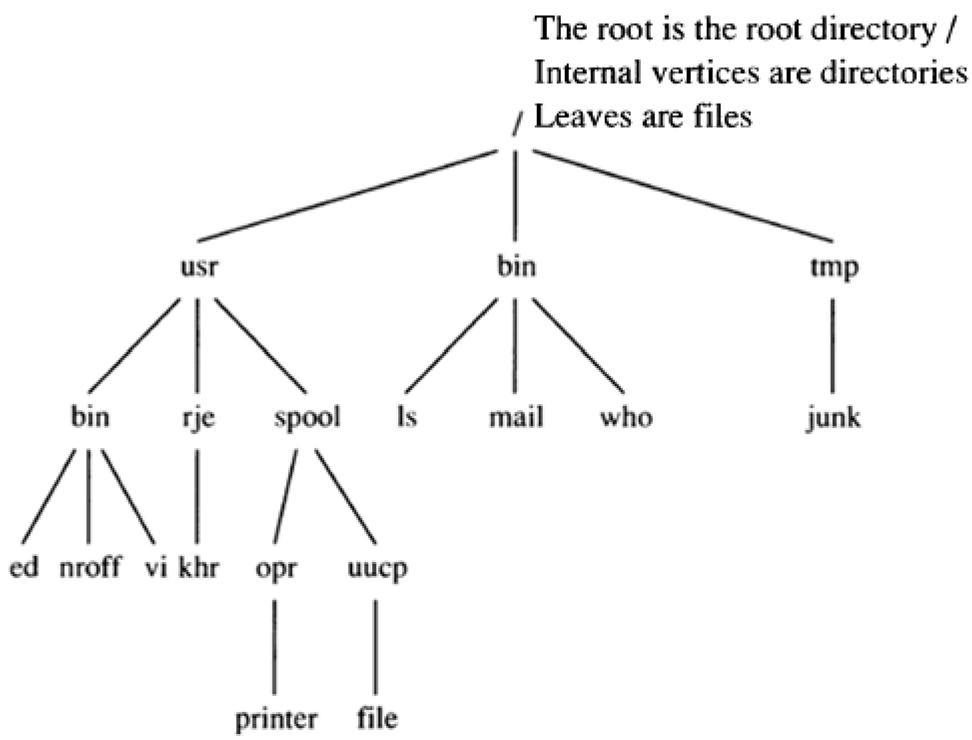
The structure of a large organization can be modeled using a rooted tree. Each vertex in this tree represents a position in the organization. An edge from one vertex to another vertex indicates that the person represented by the initial vertex is the direct boss of the person represented by the terminal vertex.



An organizational tree for a computer company

3. **Complier File System**

Files in computer memory can be organized into directories. A directory can contain both files and subdirectories. The root directory contains the entire file system. Thus, a file system may be represented by a rooted tree, where the root represents the root directory, internal vertices represent the subdirectories, and the leaves represent ordinary files or empty directories. One such file system is given below:

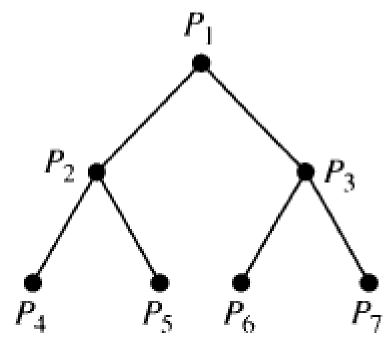


A computer File system

Note: The links to files where the same file may have more than one pathname can lead to circuits in computer file systems

4. Tree –Connected Parallel Processors

A **tree connected network** is an important way to interconnect the processors. The graph representing such a network is a complete binary tree. Such a network interconnects $n = 2^k - 1$ processors, where k is a positive integer. A processor represented by the vertex v that is not a root or a leaf has three two-way connections, one to the processor represented by the parent of v and two to the processor represented by the two children of v. The processor represented by the oot has two-way connections to the processors represented by its two children. A processor represented by a leaf u has a single two-way connections to the parent of u.



A Tree-Connected Network of Seven Processors

Illustration of the use of a tree –connected network for parallel computation

This is an illustration of the use of processors in the above figure to add eight numbers $x_1, x_2, \ldots, x_8$ using three steps.

In the first step, we add x_1 and x_2 using P_4, x_3 and x_4 using P_5, x_5 and x_6 using P_6 and x_7 and x_8 using P_7.

In the second step, we add $x_1 + x_2$ and $x_3 + x_4$ using P_2 and $x_5 + x_6$ and $x_7 + x_8$ using P_3.

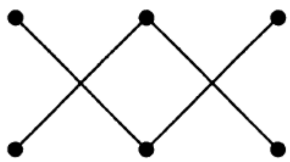
In the third step, we add $x_1 + x_2 + x_3 + x_4$ and $x_5 + x_6 + x_7 + x_8$ using P_1

The three steps used to add eight numbers compares favorably to the seven steps required to add eight numbers serially, where the steps are the addition of one number to the sum of the previous numbers in the list.

P1:

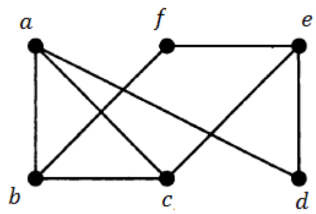
Which of the following graphs shown below are trees?

i



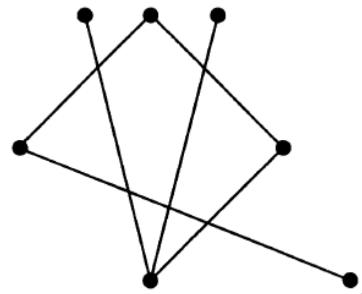
G_1

ii



G_2

iii



G_3

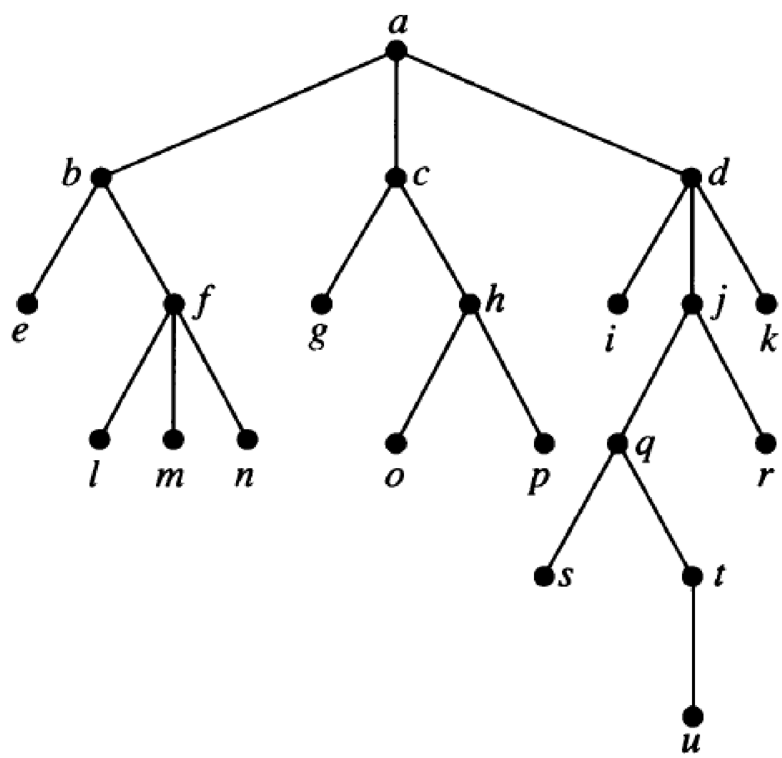
Solution:

Recall that a tree is a connected undirected graph with no simple circuits

i. The graph G_1 is not a tree, because it is not connected.
ii. The graph G_2 is not a tree , because it has a simple circuit a, b, c, a and also b, c, e, f, b
iii. The graph G_3 is a tree, because it is connected and has no simple circuits.

P2:

Answer the following questions for the rooted tree given below.



a. **Which vertex is the root?**
b. **Which vertices are internal?**
c. **Which vertices are leaves?**
d. **Which vertices are children of j?**
e. **Which vertex is the parent of h?**
f. **Which vertices are the siblings of l?**
g. **Which vertices are ancestors of m?**
h. **Which vertices are descendants of b?**

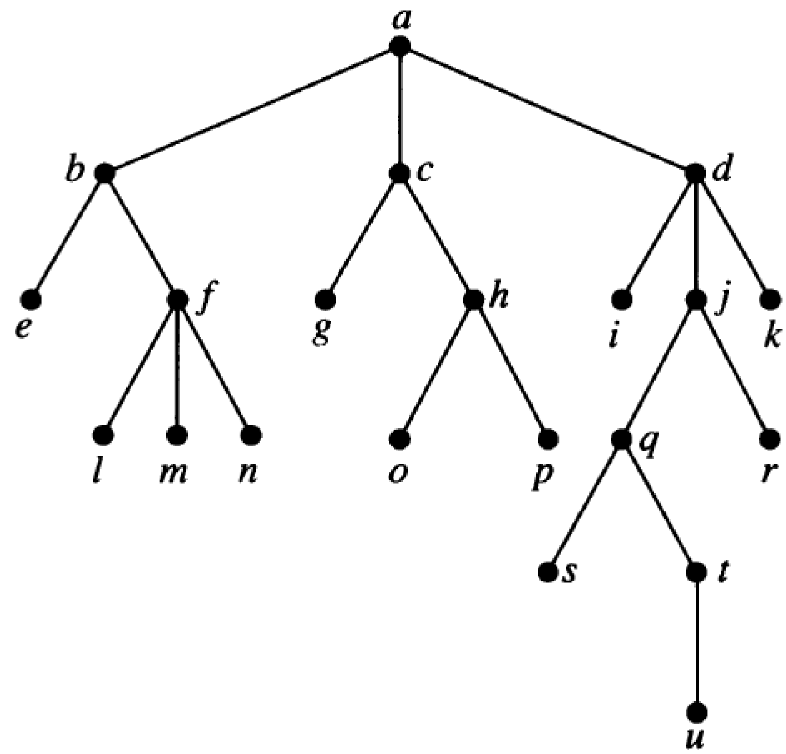
Solution:

a. Vertex a is the root
b. The vertices that have children are internal vertices. The internal vertices of this tree are a, b, c, d, f, h, j, q and t.

c. The vertices that have no children are leaves. The leaves are $e, g, i, k, l, m, n, o, p, r, s$ and u.
d. A vertex x is a child of a vertex y, if there is an edge from y to x.The children of j are q and r.
e. A vertex y is the parent of a vertex x, if there is a edge from y to x.The parent of the vertex h is c.
f. Vertices with the same parent are siblings. The siblings of the vertex l are m and n.
g. The ancestors of a vertex v are the vertices present in the path from the root to v, excluding v. The ancestors of the vertex m are f, b, a.
h. The descendants of a vertex v are those vertices that have v as an ancestor. The descendants of b are e, f, l, m and n.

P3:

Consider the following rooted tree.



a) Is the above rooted tree a full m-ary tree for some positive integer m
b) What is the level of each vertex of the above rooted tree.
c) What is the height of the above rooted tree.

Solution:

a) A rooted tree is an m-ary tree if every internal vertex has no more than m children. Notice that every internal vertex has no more than 3 children. Therefore, it is 3-ary tree.
 A rooted tree is a full m −ary tree if every internal vertex has exactly m children. It is not a full m-ary tree for any positive integer m because some of its internal vertices have two children, the others have 3 children.

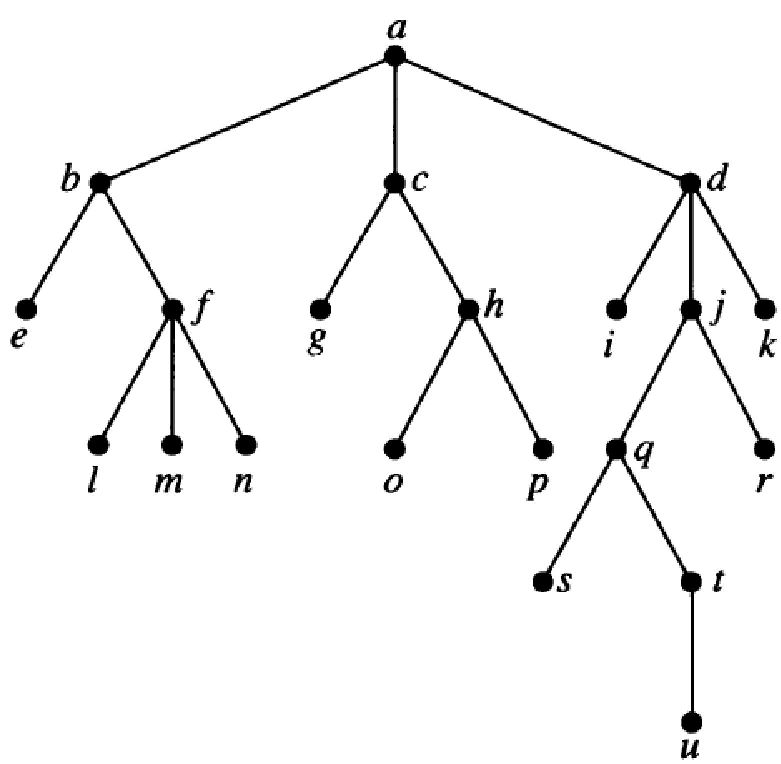
b)

vertices	level
a(root)	0
b, c, d	1
e, f, g, h, i, j, k	2
l, m, n, o, p, q, r	3
s, t	4
u	5

c) The largest level of any vertex is the height of the tree. Therefore, the height of the tree is 5.

P4:

Draw the subtree of the rooted tree given below rooted at (i) a (ii) c (iii) e.

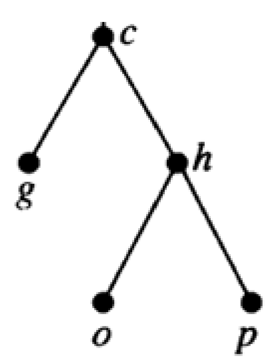


Solution:

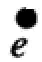
The subtree with v as its root is the subgraph of the tree consisting v and its descendents and all edges incident with these descendents.

(a) The sub tree rooted at a is the entire tree.

(b) The sub tree rooted at c is



(c) The sub tree rooted at e is



$i.e.$, e alone.

P5:

How many edges does a full binary tree with 1000 internal vertices have?

Solution:

We have a full binary tree, i.e., $m = 2$ and 1000 internal vertices, $i.e.$, $i = 1000$.

A full m-ary tree with i internal vertices has $n = mi + 1$ vertices.

Therefore, $n = 2 \times 1000 + 1 = 2001$ vertices.

A tree with n vertices has $e = n - 1$ edges. Therefore, $e = 2001 - 1 = 2000$ edges.

Thus, it has 2000 edges.

Note: If it has l leaves then $n = l + i$

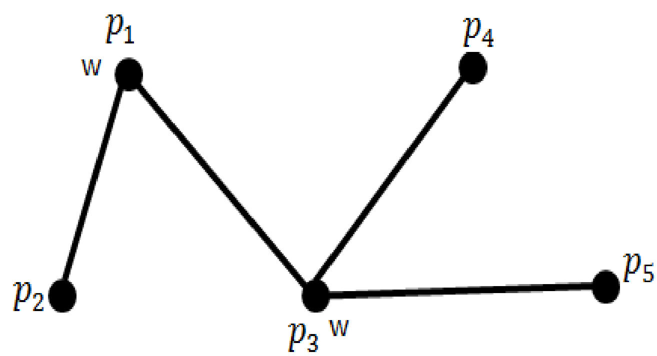
Therefore, $l = n - i = 2001 - 1000 = 1001$.Thus, it has 1001 leaves.

P6:

Suppose 1000 people enter a chess tournament. Use a rooted tree model of the tournament to determine the number of games must be played to determine a champion, if a player is eliminated after one loss and games are played until only one entrant has not lost. Assume that there are no ties.

Solution:

This can be modeled by a rooted tree, where the vertices are players and a game between two players is the edge between the corresponding vertices.



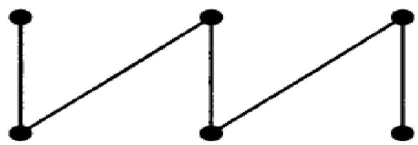
In the above example, there are 5 players $p_1, p_2, \ldots, p_5$. First p_1 and p_2 played and p_1 won. Now p_1 and p_3 played and p_3 won. It is now the turn of p_3 and p_4, and p_3 won. Finally p_3 and p_5 played and p_3 won. Thus the champion is p_3. The number of games played is $e = n - 1$ where n is the number of players.

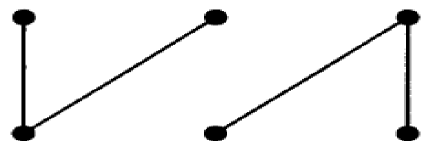
Thus, the number of games played to determine a champion is the number of edges in a rooted with n vertices, $i.e.$, $e = n - 1$. Therefore, the number of games must be played to determine a champion is $1000 - 1 = 999$.

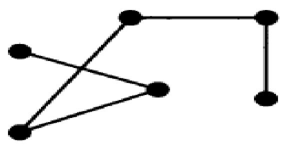
3.7. Trees

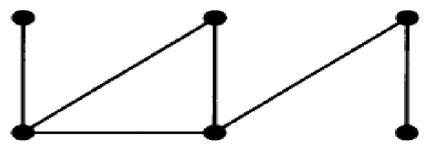
Exercise:

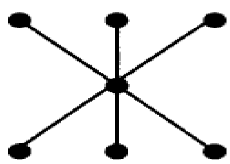
1. Which of the following graphs shown below are trees?

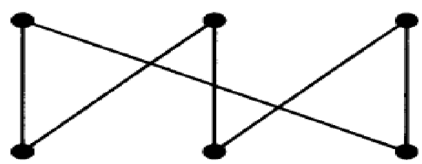
a) 

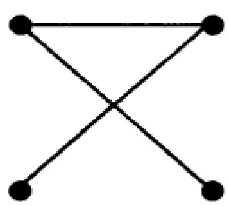
b) 

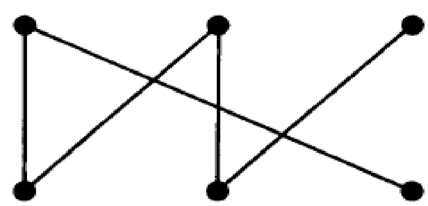
c) 

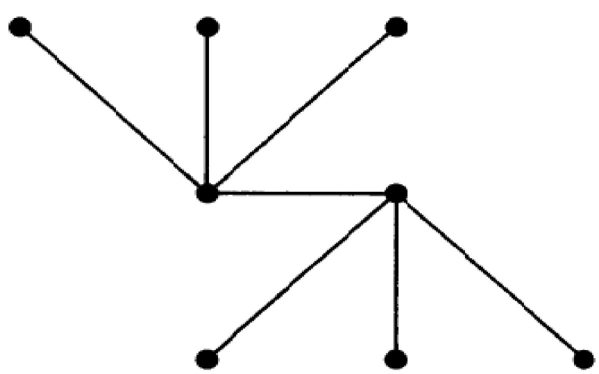
d) 

e) 

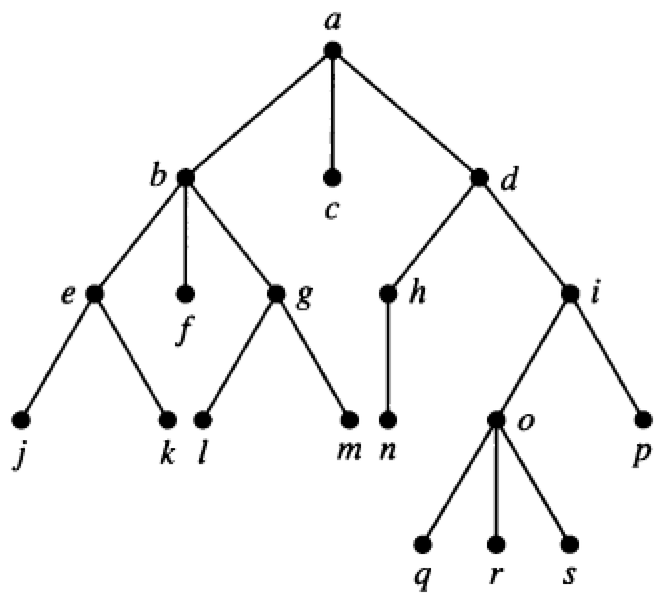
f) 

g) 

h) 

i) 

2. Consider the following rooted tree and answer the following questions?



a. Which vertex is the root?
b. Which vertices are internal?
c. Which vertices are leaves?
d. Which vertices are children of o?
e. Which vertex is the parent of h?
f. Which vertices are the siblings of l?
g. Which vertices are ancestors of m?
h. Which vertices are descendants of b?

3. Is the rooted tree in Exercise 2 a full m −ary tree for some positive integer m?

4. What is the level of each vertex of the rooted tree in Exercise 2?

5. Draw the subtree of the tree in Exercise 2 that is rooted at

a. a b. c c. e d. i

6. How many edges does a tree with 10,000 vertices have?

7. How many vertices does a full 5-ary tree with 100 internal vertices have?

8. How many leaves does a full 3-ary tree with 100 vertices have?

9. A chain letter starts when a person sends a letter to five others. Each person who receives the letter either sends it to five other people who have never received it or does not send it to anyone. Suppose that 10,000 people send out the letter before the chain ends and that no one receives more than one letter. How many people receive the letter, and how many do not send it out?