



WINTER SEMESTER 2022-2023

SCHOOL OF ADVANCED SCIENCES DEPARTMENT OF MATHEMATICS

CONTINUOUS ASSESSMENT TEST – I

Course Code	: BMAT205L	
Course Name	: Discrete Mathematics and Graph Theory	
Slot	: A1+TA1+TAA1	
Duration	: 90 Minutes	
Date	: 22.01.2023	Max. Marks: 50

Answer ALL the following questions.

Q. No.	Question	Marks	CO	BL
1.	Define principal Conjunctive normal form (PCNF) and without constructing the truth table, find the PCNF of the following statement $(p \rightarrow (q \wedge r)) \wedge (\neg p \rightarrow (\neg q \wedge \neg r))$	10	[CO1]	BL1
2.	Construct an argument using rules of inference to show that the hypotheses “Radha works hard”, “If Radha works hard, then she is a dull girl” and “ If Radha is a dull girl, then she will not get the job ”imply the conclusion “ Radha will not get the job ”.	10	[CO1]	BL2
3.	Verify the validity of the following argument: Every living thing is a plant or an animal. Rama’s dog is alive and it is not a plant. All animals have hearts. Therefore Rama’s dog has a heart.	10	[CO1]	BL3
4.	(i) Symbolize the following statement: (a)Every Mathematics student needs a course in Compter science. (b) There is a student in this class who owns a Personal computer. (5 Marks)	10	[CO2]	BL3

	(ii) Prove for any commutative monoid $\langle M, * \rangle$, the set of idempotent elements of M forms a submonoid. (5 Marks)			
5.	Show that the set Q^+ of all positive rational numbers forms an abelian group under the operation * defined by $a * b = \frac{1}{2}ab; a, b \in Q^+$.	10	[CO2]	BL2



VIT®

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Vellore – 632014, Tamil Nadu, India
DEPARTMENT OF MATHEMATICS
SCHOOL OF ADVANCED SCIENCES
FALL SEMESTER 2022-2023

CONTINUOUS ASSESSMENT TEST – II

Programme Name & Branch : B. Tech
Course Code : BMAT205L
Course Name : Discrete Mathematics and Graph Theory
Slot : A2 + TA2 + TAA2
Date of the Examination :
Duration : 90 minutes **Max. Marks : 50**

General instruction(s): Answer All The Questions

Q. No	Question	Marks	Course Outcome (CO)	Bloom's Taxonomy (BL)
1.	<p>The Cayley's table for a group defined on the set $S = \{ e, a, b, c, d, f \}$ with respect to a binary operator * is given below. Determine</p> $\begin{array}{c cccccc} * & e & a & b & c & d & f \\ \hline e & e & a & b & c & d & f \\ a & a & e & d & f & b & c \\ b & b & f & e & d & c & a \\ c & c & d & f & e & a & b \\ d & d & c & a & b & f & e \\ f & f & b & c & a & e & d \end{array}$ <p>a. A set $H_1 \subseteq S$ such that $\langle H_1, * \rangle$ is not a subgroup of $\langle S, * \rangle$. b. A set $H_2 \subseteq S$ such that $\langle H_2, * \rangle$ is a subgroup of $\langle S, * \rangle$. c. The left and right cosets of H_2 in S.</p>	2 10		BL5
2.	<p>Let $H = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ be a parity check matrix. Determine the</p> <p>$(2, 5)$ group code function $e_H : B^2 \rightarrow B^5$. Create the decoding table. What is the original message if the received message is 11101.</p>	2 10		BL5

Vellore – 632014, Tamil Nadu, India
 DEPARTMENT OF MATHEMATICS
 SCHOOL OF ADVANCED SCIENCES
 FALL SEMESTER 2022-2023

3.	How many integers are there between 1 and 1000 both inclusive, that are divisible by atleast one of the integers 2, 3, 5 and 7.	10	3	BL2
4.	Find the generating function of the recurrence relation $S(n) - 2S(n-1) - 3S(n-2) = 0$, $n \geq 2$, with $S(0) = 3$, $S(1) = 1$, and hence find its solution.	10	3	BL1
5.	Let $n = 60$, and let X be the set of all positive integers which are divisors of 60. Let ' \leq ' be the relation ' divisor of ' on X . <ol style="list-style-type: none"> Draw the Hasse diagram of $\langle X, \leq \rangle$. Find the least upper bound and greatest lower bound of $(2, 5)$ and $(12, 30)$. What is the greatest and least element of $\langle X, \leq \rangle$. 	10	4	BL3



Fall Semester 2022-2023

Continuous Assessment Test -II (October 2022)

Slot: A1+TA1+TAA1

Programme: B.Tech(CSE/IT)

Course : BMAT205L – Discrete Mathematics and Graph Theory

Max. Time: 90 minutes

Max. Marks: 50

Answer all the questions (5x10=50)

1. Verify Lagrange's theorem for the subgroup generated by 4 of the group $\langle Z_{17}^*, \times_{17} \rangle$
2. An encoding function $e: B^3 \rightarrow B^6$ is given by the generator matrix $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$.
a) Determine all code words generated by the matrix. b) Find the associated parity check matrix H c) Use H to decode the following received words 100100, 010100
3. a) How many positive integers between 100 and 999 inclusive
(i) are not divisible by either 3 or 4? (ii) are divisible by 3 but not by 4?
b) How many different ways are there to choose 3 donuts from the 5 varieties at a donut shop?
Assume that there are at least 3 donuts of each variety.
4. Solve the recurrence relation
$$a_{n+2} + 3a_{n+1} + 2a_n = 3^n, \quad n \geq 0, a_0 = 0, a_1 = 1$$
5. Draw the Hasse diagram for the poset $\{S_{30}, D\}$, divisors of 30 under the relation divides. Hence or otherwise prove that it is a lattice, also find $3 * (10 \oplus 3)$ and $3 \oplus (10 * 3)$

Question Format & QP Setter Information (Common QP)

Name of Examination		Final Assessment Test, Winter 2022-23 Semester, (APRIL 2023)					
Slot: A1+TA1+TAA1		Course Mode: CBL			Class Number (s): VL2022230500698, 500718, 500730, 500733, 500743, 500748, 500749, 500763, 500769, 500777, 500783, 500792, 500795, 500850, 502171, 502172, 502546, 502547, 504012		
Course Code:		BMAT205L		Course Title:	Discrete Mathematics and Graph Theory		
Emp. No.:		13402		Faculty Name:	Manimaran A		School: SAS
Contact No.:		7402620220		Email:	manimaran.a@vit.ac.in		

General Instructions (if any):

Q. No.	Sub-division	Question Text	Ma rks	Un it / Mo du le No.	Diffi cu lt y Leve l E/A /T	BL	CO
--------	--------------	---------------	-----------	---	--	----	----

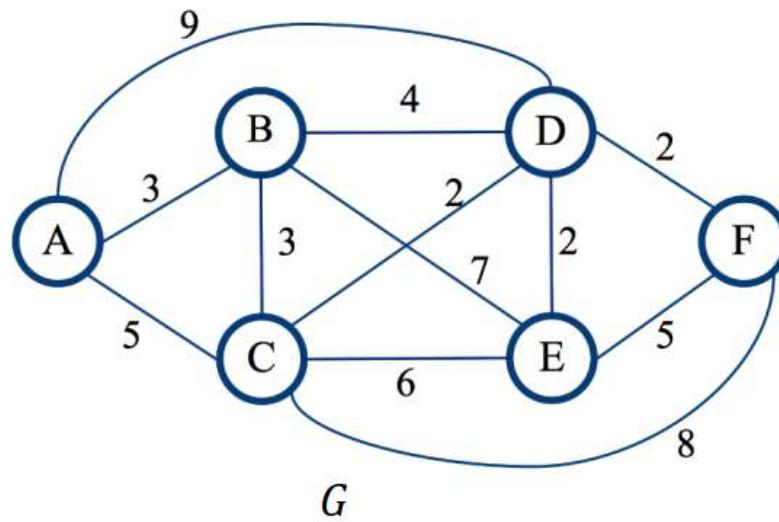
Answer any TEN

Total Marks: 10 X 10 = 100 Marks

1.		Show that the following set of premises is inconsistent: “If Rama gets his degree, he will go for a job.” “If he goes for a job, he will get married soon.” “If he goes for higher study, he will not get married.” “Rama gets his degree and goes for higher study.”	10	1	A	L3	1
2.		Show that $(x)(P(x) \vee Q(x)) \Rightarrow (x)P(x) \vee (\exists x)Q(x)$ by the indirect method.	10	1	A	L6	1
3.		Verify whether $G = \{(a,b) : a, b \text{ are rationals}, a \neq 0\}$ is a group or not under the binary operation * on G defined as $(a,b)*(c,d) = (ac, ad + b)$. Is it an abelian group?	10	2	T	L5	2
4.		State and prove Lagrange's theorem in groups and verify whether the converse is true or not. Justify the answer in detail.	10	2	A	L2	2
5.		ABC is an equilateral triangle whose sides are of 1cm each. If we select 10 points inside the triangle ABC, then prove that at least two of these points are such that whose distance between them is less than 1/3 cm.	10	3	A	L5	3
6.		State and prove distributive inequality in a Lattice.	10	4	A	L2	4
7.		Expand the given Boolean expression $x_1 * x_2$ in an equivalent sum of products canonical form and product of sums canonical form in terms of three variables namely x_1, x_2 & x_3 .	10	4	T	L5	4
8.		Verify whether the complete graph with 5 vertices is planar or non-planar.	10	5	A	L4	5

9.

(i). Apply the Dijkstra's algorithm to find the shortest path between the vertices A and F in the following weighted connected graph G and hence compute the total weight of the obtained shortest path between the mentioned vertices.



10

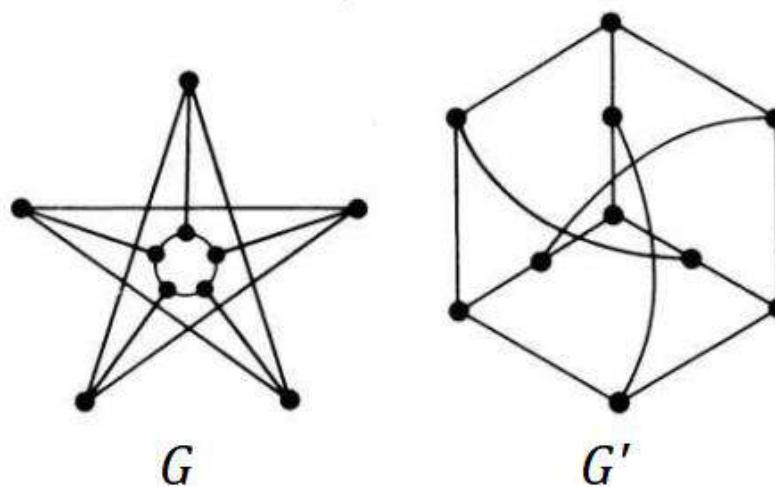
5

5

T

L4

(ii). Explain isomorphism of graphs and verify whether the following two graphs G and G' are isomorphic. If so, exhibit an isomorphism between them.



10.

Prove that every tree has either one or two centers.

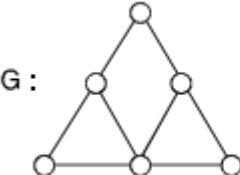
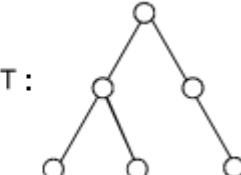
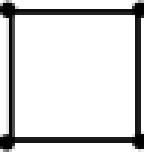
10

6

T

L5

5

11.	<p>Find all the possible fundamental circuits for the given graph G with respect to the given spanning tree T. Also find at least seven possible spanning trees for the given graph G</p>  <p>$G:$</p>  <p>$T:$</p>	10	6	A	L4	5
12.	<p>Find the chromatic polynomial and chromatic number for the following graph G.</p>  <p>G</p>	10	7	T	L4	5

Question Paper Setter Information

QP

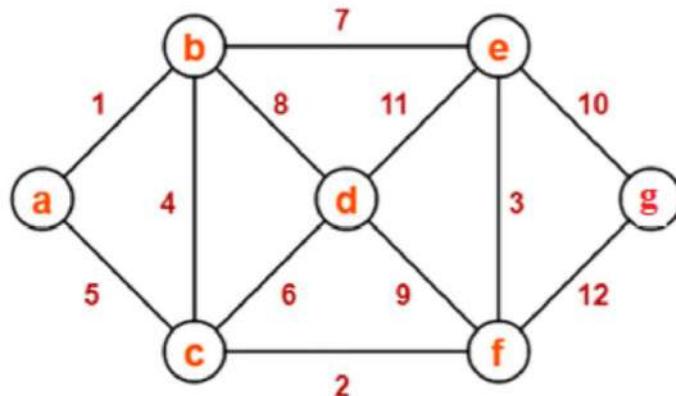
Name of Examination		Final Assessment Test (FAT), Winter Semester – 2022~2023 (April 2023)				
Slot: A2+TA2+TAA2		Class Number(s): VL2022230500728 / Other Common Slots				
Course Code: BMAT205L		Course Title: Discrete Mathematics and Graph Theory				
Emp. No.: 13721		Faculty Name: D. Easwaramoorthy		School: SAS		
Contact No.: 9487255390		E-Mail:	easwar@vit.ac.in			

General Instructions (if any): ---

Part	Q. No.	Sub-Division	Question Text	Marks	Unit / Module No.	Difficulty Level E/A/T	Bloom's Level [1-6]	CO
A	Answer Any 10 Questions						Total Marks: 10 X 10 Marks = 100	
1.	---		Show that $(P \rightarrow]S)$ can be derived from the premises $(P \rightarrow (Q \vee R)), (Q \rightarrow]P), (S \rightarrow]R)$ and P , by the indirect method.	10	1	E	2	1
2.	---		Show that the premises "A student in the Discrete Mathematics class has not read the book," and "Everyone in the Discrete Mathematics class passed the Final Assessment Test" imply the conclusion "Someone who passed the Final Assessment Test has not read the book."	10	1	A	3	1
3.	---		Show that a non-empty subset H of G is a subgroup of a group $\langle G, * \rangle$ if and only if for any pair of elements $a, b \in H; a * b^{-1} \in H$.	10	2	A	4	2
4.	---		Find all the code words generated by the encoding function $e: B^3 \rightarrow B^6$ with respect to the following parity check matrix. $H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$	10	2	A	5	2
5.	---		In how many ways can 20 students out of a class of 30 be selected for an extra-curricular activity, if (i). Mr. X refuses to be selected? (ii). Mr. Y insists on being selected? (iii). Mr. X and Mr. Y insist on being selected? (iv). Either Mr. X or Mr. Y or both get selected?	10	3	E	1	3

6.	---	Let $\langle L, \leq, *, \oplus \rangle$ be a lattice in which $*$ and \oplus denote the operations of meet and join respectively. For any $a, b \in L$, prove that $a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$.	10	4	T	4	4
7.	---	If $P(S)$ is the power set of a non-empty set S , then prove that $\langle P(S), \subseteq, \cap, \cup, , \emptyset, S \rangle$ is a Boolean algebra, where $S A$ is the complement of a set A ($\subseteq S$) . Also draw the Hasse diagram of the POSET $\langle P(S), \subseteq \rangle$, where $S = \{a, b, c\}$.	10	4	A	3	4
8.	---	Show that a simple graph with n vertices and k components can have at most $\frac{(n-k)(n-k+1)}{2}$ edges.	10	5	T	4	5
9.	---	(a). Draw a connected graph with 5 vertices (i). that is Eulerian and also Hamiltonian. (ii). that is Eulerian but not Hamiltonian. (iii). that is Hamiltonian but not Eulerian. (iv). that is not Hamiltonian and also not Eulerian. (v). that has a Hamiltonian path but does not have a Hamiltonian circuit. (b). Draw a graph G with 5 vertices such that the adjacency matrix of G with the trace 0. Also construct the incidence matrix for the graph G .	10	5	E	3	5
10.	----	(a). A tree T with maximum degree 4 and also T has five vertices of degree 2, three vertices of degree 3 and four vertices of degree 4. How many pendant vertices does it have? (b). A tree T has $2k$ vertices of degree 1, $3k$ vertices of degree 2 and k vertices of degree 3. Determine the number of vertices and edges in T .	10	6	A	3	5
11.	---	(a). Draw the complete bipartite graph $K_{2,3}$ and construct at least 5 spanning trees of $K_{2,3}$.	10	6	E	2	5

(b). Find the minimal spanning tree by using the Prim's algorithm for the following weighted connected graph and hence compute the total weight of the obtained minimal spanning tree.



12. --- Let a and b be two non-adjacent vertices in a graph G . Let G' be a graph obtained by adding an edge between a and b ; and G'' be a simple graph obtained from G by fusing the vertices a and b together and replacing sets of parallel edges with single edges. Then prove that $P_n(\lambda)$ of $G = P_n(\lambda)$ of $G' + P_{n-1}(\lambda)$ of G'' . Illustrate the same result with a suitable graph with 5 vertices.

10 7 T 4 5

Course Assessment Rubrics

Fall Semester 2023 – 24

Course Code	Course Title	Course Type	Slot
BMAT205L	Discrete Mathematics and Graph Theory	TH	A1+TA1+TAA1

Sl. No.	Assessment Title	Due Date	Max. Marks	Weightage	Remarks
1.	QUIZ-I	August 19, 2023	10	10	Class Test
2.	CAT-I	Will be informed later	50	15	Will be informed later
3.	QUIZ-II	November 4, 2023	10	10	Class Test
4.	CAT-II	Will be informed later	50	15	Will be informed later
5.	Digital Assignment	Submit before October 13, 2023	10	10	VTOP Submission
6.	FAT	Will be informed later	100	40	Will be informed later

Module 1: Mathematical logics

- ▶ Introduction-Statements and Notation
- ▶ Connectives
- ▶ Tautologies
- ▶ Two State Devices and Statement logic
- ▶ Equivalence - Implications-Normal forms
- ▶ The Theory of Inference for the Statement Calculus

Basics

Logic: Logic is the discipline that considers the methods of reasoning. It provides the rules and techniques for determining whether an argument is valid or not.

In everyday life, we use reasoning to prove different points. For example: to prove our parents that we passed an exam, we might show the test and the score.

Similarly, in mathematics and computer science, mathematical logic or logic is used to prove results. To be specific, in mathematics we use logic and logical reasoning to prove the correctness of programs and also to prove the theorems.

Statement or proposition:

A statement, or a proposition is the declarative sentence that is either true or false but not both and one of the values ‘truth’ or ‘falsity’ that is assigned to a statement is called its truth values.

We abbreviate ‘truth’ to T or 1 and ‘false’ to F or 0.

Examples:

1. Canada is a country.
2. 5 is less than 3.
3. This statement is false.
4. $1+101=110$
5. Close the door.

Connectives:

In our everyday language, we use connectives such as ‘and’ , ‘but’, ‘or’ etc. to combine two or more statements to form other statements.

We will discuss some of the connectives:

1. Negation (Not or \sim):

The negation of a statement ‘P’ is written as $\sim P$ and read as ‘not P’.

The truth table for the negation is

P	$\sim P$
T	F
F	T

Remark: Also we can read as ‘it is not the case that P’. And it is a unary operation.

Examples:

1. **P**: London is a city.

~P: London is not a city.

Or

~P: It is not the case that London is a city.

2. **P**: John is a rich man

~P: John is not a rich man

Or

~P: It is not the case that John is a rich man

2. Conjunction (And, \wedge):

The conjunction of two statements ‘P’ and ‘Q’ is written as $P \wedge Q$ and is read as ‘P and Q’.

It has the truth value ‘true’ only when both P and Q are true otherwise ‘false’.

Truth table:

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

Remark: Conjunction is a binary operation and it is symmetric.

Examples:

1. **P**: It is cold.

Q: It is rainy.

So

P \wedge Q : It is cold and it is rainy.

2. **P**: John is a rich man

Q: John is intelligent

So

P \wedge Q : John is a rich man and John is intelligent.

3. Disjunction (Or, ‘ \vee ’):

The disjunction of two statements ‘P’ and ‘Q’ is written as $P \vee Q$ and is read as ‘P or Q’.

It has the truth value ‘false F’ only when both P and Q have the truth value false otherwise True.

Truth table:

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

Remark: Disjunction is also a binary operation and it is symmetric.

Examples:

1. **P**: It is cold.

Q: It is rainy.

So

P v Q : It is cold or it is rainy.

2. **P**: John is a rich man

Q: John is intelligent

So

P v Q : John is a rich man or John is intelligent.

4. Conditional statements (\rightarrow):

Let '**P**' and '**Q**' be any two statements. Then the statement ' $P \rightarrow Q$ ' is read as ' If **P** then **Q**' and has the truth value false only when **P** is true and **Q** is false.

Truth table:

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

Example:

P: There is a flood.

Q: The crop will be destroyed.

So

$P \rightarrow Q$: If there is a flood then crop will be destroyed.

Remark: $P \rightarrow Q$ can be represented by anyone of the following expression:

- a) Q is necessary for P.
- b) P is sufficient for Q
- c) P only if Q.

The statement P is called as the antecedent and Q the consequent in $P \rightarrow Q$.

Again, according to the definition, it is not necessary that there be any kind of relation between P and Q in order to form $P \rightarrow Q$.

Example:

P: The Sun is shining today.

Q: $2+7 > 4$.

So

$P \rightarrow Q$: If the Sun is shining today then $2+7 > 4$.

5. Bi-conditional statements (\leftrightarrow):

Let 'P' and 'Q' be any two statements. Then the statement ' $P \leftrightarrow Q$ ' is read as '**P if and only if Q**' or '**P iff Q**' and has the truth value true if both P and Q are identical.

Truth table:

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

Example:

P: x is an even number.

Q: x is divisible by 2.

So

$P \rightarrow Q$: x is an even number if and only if x is divisible by 2.

Atomic Statements:

Declarative sentences which cannot be further split into simple sentences are called as atomic statements (or primary statements or primitive statements).

Example: p is a prime number.

Compound statements:

New statements can be formed from atomic statements by using connectives ‘and’ , ‘but’ , ‘or’ etc., the resulting statements are called as molecular or compound statements.

Statement formula:

If we represent the definite statements by means of the statement variables like P, Q, R,..., then the compound statement is called statement formula.

Example:

If P : Martin is poor

Q : Martin is happy

Write the following statements in symbolic form

- (a) Martin is rich and happy
- (b) Martin is neither poor nor happy
- (c) Martin is rich or he is both poor and unhappy.

Solution:

- (a) $\sim P \wedge Q$
- (b) $\sim P \wedge \sim Q$
- (c) $\sim P \vee (P \wedge \sim Q)$

Converse:

The statement $Q \rightarrow P$ is called the converse of the implication $P \rightarrow Q$.

Example:

P: Today is Sunday.

Q: I will go for a walk.

So,

$Q \rightarrow P$: If I will go for a walk then today is Sunday.

Inverse:

The statement $\sim P \rightarrow \sim Q$ is called the converse of the implication $P \rightarrow Q$.

$\sim P \rightarrow \sim Q$: If today is not Sunday then I will not go for a walk.

Contrapositive:

The statement $\sim Q \rightarrow \sim P$ is called the contrapositive of the implication $P \rightarrow Q$.

Example:

P: Today is Sunday.

Q: I will go for a walk.

So,

$\sim Q \rightarrow \sim P$: If I will not go for a walk then today is not Sunday.

Truth table for statement formula

$$S = (P \rightarrow Q) \vee (\sim P \wedge Q)$$

P	Q	$\sim P$	$P \rightarrow Q$	$\sim P \wedge Q$	S
T	T	F	T	F	T
T	F	F	F	F	F
F	T	T	T	T	T
F	F	T	T	F	T

Construct the truth table for the following statement formulae

(i) $(p \rightarrow q) \longleftrightarrow (\neg p \vee q)$

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

(iii) $(p \rightarrow q) \rightarrow p$

(iv) $\neg(p \wedge q) \longleftrightarrow (\neg p \vee \neg q)$

(v) $(p \vee \neg q) \rightarrow q$

$$1. S = (Q \wedge (P \rightarrow Q)) \rightarrow P$$

$$2. S = (P \vee Q) \wedge (\neg R \leftrightarrow Q)$$

Tautology: A statement formula which is true regardless of the truth values of the statements which replace the variables in it is called a universally valid formula or a Tautology. It is denoted by T.

Example: $P \vee \neg P$

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

Contradiction: A statement formula which is false regardless of the truth values of the statements which replace the variables in it is called a contradiction. It is denoted by F.

Example: $P \wedge \sim P$

P	$\sim P$	$P \wedge \sim P$
T	F	F
F	T	F

Contingency: A statement formula which is neither a tautology nor a contradiction is called a contingency.

Example: $P \vee Q$

Examples: Using truth table prove that the following statement formula is a Tautology

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

P	Q	R	$P \wedge Q$ (1)	$P \rightarrow R$ (2)	(1) \vee (2) (3)	$\neg Q$	$\neg R$	$\neg Q \rightarrow \neg R$ (4)	(3) \vee (4)
T	T	T	T	T	T	F	F	T	T
T	T	F	T	F	T	F	T	T	T
T	F	T	F	T	T	T	F	F	T
T	F	F	F	F	F	T	T	T	T
F	T	T	F	T	T	F	F	T	T
F	T	F	F	T	T	F	T	T	T
F	F	T	F	T	T	T	F	F	T
F	F	F	F	T	T	T	T	T	T

Equivalence of formulas: Let A and B be two statement formulas and let $P_1, P_2, P_3, \dots, P_n$ denote all the variables occurring in both A and B. If the truth value of A is equal to the truth value of B for every 2^n possible combination of truth values, then A and B are said to be equivalent and it is denoted by $A \Leftrightarrow B$

Example: $\sim\sim P \Leftrightarrow P$, $P \vee P$, etc.

Remarks:

1. \Leftrightarrow is not a connective.
2. Two statement formulas A and B are equivalent iff $A \Leftrightarrow B$ is a tautology.

Example : Prove that

- (a) $P \rightarrow Q \Leftrightarrow \neg P \vee Q,$
- (b) $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$
- (c) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
- (d) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

v

Equivalent formulae:

1. $P \vee P \Leftrightarrow P$ and $P \wedge P \Leftrightarrow P$ (Idempotent law)
2. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ and $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ (Associative law)
3. $P \vee Q \Leftrightarrow Q \vee P$ and $P \wedge Q \Leftrightarrow Q \wedge P$ (Commutative law)
4. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ and $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ (Distributive law)

Equivalence of formulas: Let A and B be two statement formulas and let $P_1, P_2, P_3, \dots, P_n$ denote all the variables occurring in both A and B. If the truth value of A is equal to the truth value of B for every 2^n possible combination of truth values, then A and B are said to be equivalent and it is denoted by $A \Leftrightarrow B$

Example: $\sim\sim P \Leftrightarrow P$, $P \vee P$, etc.

Remarks:

1. \Leftrightarrow is not a connective.
2. Two statement formulas A and B are equivalent iff $A \Leftrightarrow B$ is a tautology.

Example : Prove that

- (a) $P \rightarrow Q \Leftrightarrow \neg P \vee Q,$
- (b) $P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$
- (c) $\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$
- (d) $\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$

Equivalent formulae:

1. $P \vee P \Leftrightarrow P$ and $P \wedge P \Leftrightarrow P$ (Idempotent law)
2. $(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ and $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ (Associative law)
3. $P \vee Q \Leftrightarrow Q \vee P$ and $P \wedge Q \Leftrightarrow Q \wedge P$ (Commutative law)
4. $P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$ and $P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$ (Distributive law)
5. $P \vee F \Leftrightarrow P$ and $P \wedge T \Leftrightarrow P$ (Identity law)
6. $P \vee T \Leftrightarrow T$ and $P \wedge F \Leftrightarrow F$

7. $P \vee \sim P \Leftrightarrow T$ and $P \wedge \sim P \Leftrightarrow F$ (Negation law)

8. $P \vee (P \wedge Q) \Leftrightarrow P$ and $P \wedge (P \vee Q) \Leftrightarrow P$ (Absorption law)

9. $\sim(P \vee Q) \Leftrightarrow \sim P \wedge \sim Q$ and $\sim(P \wedge Q) \Leftrightarrow \sim P \vee \sim Q$ (Demorgan's law)

Logic equivalence involving implications

Implications
$p \rightarrow q \Leftrightarrow \neg p \vee q$
$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$
$\neg(p \rightarrow q) \Leftrightarrow p \wedge \neg q$
$p \vee q \Leftrightarrow \neg p \rightarrow q$
$p \wedge q \Leftrightarrow \neg(p \rightarrow \neg q)$
$(p \rightarrow q) \wedge (p \rightarrow r) \Leftrightarrow p \rightarrow (q \wedge r)$
$(p \rightarrow q) \vee (p \rightarrow r) \Leftrightarrow p \rightarrow (q \vee r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \Leftrightarrow (p \vee q) \rightarrow r$
$(p \rightarrow r) \vee (q \rightarrow r) \Leftrightarrow (p \wedge q) \rightarrow r$

Logic equivalence involving Bi conditional

Biconditions
$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q \Leftrightarrow \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \Leftrightarrow p \leftrightarrow \neg q$

Without using Truth tables, prove the following

- (i) Show that $(p \vee q) \wedge \neg p \Leftrightarrow (\neg p \wedge q)$
- (ii) Show that $(p \vee q) \wedge \neg(\neg p \wedge q) \Leftrightarrow p$
- (iii) Show that $\neg(p \vee (\neg p \wedge q)) \Leftrightarrow \neg p \wedge \neg q$
- (iv) Show that $\neg(\neg((p \vee q) \wedge r) \vee \neg q) \Leftrightarrow q \wedge r$
- (v) Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.
- (vi) Show that $p \rightarrow (q \rightarrow r) \Leftrightarrow (p \wedge q) \rightarrow r$.

(i)

$S \Leftrightarrow (p \vee q) \wedge \neg p$	Reasons
$\Leftrightarrow (p \vee q) \wedge \neg p$	Given
$\Leftrightarrow (p \wedge \neg p) \vee (q \wedge \neg p)$	Distributive law
$\Leftrightarrow F \vee (\neg p \wedge q)$	Negation law, Commutative law
$\Leftrightarrow \neg p \wedge q$	Identity law

(ii)

$S \Leftrightarrow (p \vee q) \wedge \neg(\neg p \wedge q)$	Reasons
$\Leftrightarrow (p \vee q) \wedge \neg(\neg p \wedge q)$	Given
$\Leftrightarrow (p \vee q) \wedge (\neg \neg p \vee \neg q)$	De Morgan's law
$\Leftrightarrow (p \vee q) \wedge (p \vee \neg q)$	Negation law
$\Leftrightarrow p \vee (q \wedge \neg q)$	Distributive law
$\Leftrightarrow p \vee F$	Negation law
$\Leftrightarrow p$	Identity law

(iii)

$S \Leftrightarrow \neg(p \vee (\neg p \wedge q))$	Reasons
$\Leftrightarrow \neg(p \vee (\neg p \wedge q))$	Given
$\Leftrightarrow \neg p \wedge \neg(\neg p \wedge q)$	De Morgan's law
$\Leftrightarrow \neg p \wedge (p \vee \neg q)$	De Morgan's law
$\Leftrightarrow (\neg p \wedge p) \vee (\neg p \wedge \neg q)$	Distributive law
$\Leftrightarrow F \vee (\neg p \wedge \neg q)$	Negation law
$\Leftrightarrow \neg p \wedge \neg q$	Identity law

(iv)

$\begin{aligned} S &\Leftrightarrow \neg(\neg((p \vee q) \wedge r) \vee \neg q) \Leftrightarrow q \wedge r \\ &\Leftrightarrow \neg(\neg((p \vee q) \wedge r) \vee \neg q) \\ &\Leftrightarrow ((p \vee q) \wedge r) \wedge q \\ &\Leftrightarrow (p \vee q) \wedge (r \wedge q) \\ &\Leftrightarrow (p \wedge (r \wedge q)) \vee (q \wedge (r \wedge q)) \\ &\Leftrightarrow (p \wedge (r \wedge q)) \vee (r \wedge q) \\ &\Leftrightarrow r \wedge q \end{aligned}$	Reasons
	Given
	De Morgan's law
	Associative law
	Distributive law
	Idempotent law
	Absorption law

Tautological Implications:

A statement A is said to be tautologically imply a statement B iff $A \rightarrow B$ is a tautology and it is denoted by $A \Rightarrow B$, which is read as A implies B.

Remark:

1. ' \Rightarrow ' is not a connective.
2. $A \Rightarrow B$ is not a statement formula.
3. ' \Rightarrow ' is transitive.
4. If $H_1, H_2, \dots, H_n \Rightarrow Q$, then $(H_1 \wedge H_2 \wedge \dots \wedge H_n \Rightarrow Q)$

Example:

1. Prove that $P \wedge (P \rightarrow Q) \Rightarrow Q$ using truth table and without using truth table.
2. $(P \wedge Q) \Rightarrow (P \rightarrow Q)$
3. $\sim(P \leftrightarrow Q) \Leftrightarrow (P \vee Q) \wedge \sim(P \wedge Q)$

Normal Forms:

Let $A (P_1, P_2, P_3, \dots, P_n)$ be a statement formula, where $P_1, P_2, P_3, \dots, P_n$ are the atomic variables. If we consider all possible assignments of the truth values to $P_1, P_2, P_3, \dots, P_n$ and obtain the resulting truth values of the formula A , then we get the truth table for A .

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

Satisfiable: If A has truth values T for atleast one combination of truth values assigned to $P_1, P_2, P_3, \dots, P_n$ then A is said to be satisfiable.

Construction of truth tables may not be practical , we consider other procedure known as reduction to normal forms.

Elementary Product:

A product of the variables and their negations in a formula is called an elementary product.

Example: If P and Q are two atomic variables then P , $\sim P \wedge Q$, $\sim Q \wedge P \wedge \sim P$, $Q \wedge \sim P$ etc. are sum examples of elementary products.

Elementary Sum:

A sum of the variables and their negations in a formula is called an elementary sum.

Example: If P and Q are two atomic variables then P , $\sim P \vee Q$, $\sim Q \vee P \vee \sim P$, $Q \vee \sim P$ etc. are sum examples of elementary products

Remark:

1. A necessary and sufficient condition for an elementary product to be identically false is that it contains atleast one pair of factors in which one is the negation of the other.
2. A necessary and sufficient condition for an elementary sum to be identically true is that it contains atleast one pair of factors in which one is the negation of the other.

Disjunctive Normal form:

A formula which is equivalent to a given formula and which consist of a sum of elementary product is called as disjunctive normal form.

Example: Obtain the disjunctive normal form of $P \wedge (P \rightarrow Q)$

$$\begin{aligned}\text{Solution: } P \wedge (P \rightarrow Q) &\Leftrightarrow P \wedge (\neg P \vee Q) \\ &\Leftrightarrow (P \wedge \neg P) \vee (P \wedge Q) \quad \text{Distributive law}\end{aligned}$$

Example: Obtain the disjunctive normal form (DNF) of the following

(a) $\neg(P \vee Q) \leftrightarrow (P \wedge Q)$

Solution:

$$\sim(P \vee Q) \leftrightarrow (P \wedge Q) \Leftrightarrow [\sim(P \vee Q) \rightarrow (P \wedge Q)] \wedge [(P \wedge Q) \rightarrow \sim(P \vee Q)] \quad [P \leftrightarrow Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)]$$

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

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

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

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

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

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

Example 2. Obtain the disjunctive normal form (DNF) of the following

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

Solution:

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

$$[P \rightarrow Q \Leftrightarrow \sim P \vee Q]$$

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

$$[P \rightarrow Q \Leftrightarrow \sim P \vee Q]$$

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

$$[\text{Distributive law}]$$

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

$$[\text{Commutative law}]$$

is the required disjunctive normal form.

Solution:

$$\sim(P \vee Q) \leftrightarrow (P \wedge Q) \Leftrightarrow [\sim(P \vee Q) \rightarrow (P \wedge Q)] \wedge [(P \wedge Q) \rightarrow \sim(P \vee Q)]$$

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

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

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

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

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

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

Conjunctive Normal form:

A formula which is equivalent to a given formula and which consist of a product of a elementary sum is called as conjunctive normal form.

Example 1. Obtain the conjunctive normal form of $P \leftrightarrow Q$

Solution:

$$\begin{aligned} P \leftrightarrow Q &\Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P) \\ &\Leftrightarrow (\sim P \vee Q) \wedge (\sim Q \vee P) \end{aligned}$$

Example 2. $P \rightarrow ((P \rightarrow Q) \wedge \sim(\sim Q \vee \sim P))$.

Solution:

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

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

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

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

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

Example 3. $(Q \vee (P \wedge R)) \wedge \sim((P \vee R) \wedge Q)$

Solution:

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

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

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

Minterms:

For two variables P and Q, there are $2^2 = 4$ possible formulas which consists of conjunctions of P or its negation and conjunctions of Q or its negation, given by $P \wedge Q$, $P \wedge \sim Q$, $\sim P \wedge Q$ and $\sim P \wedge \sim Q$.

These formulas are called minterms.

1. Minterms for the two variables P and Q

$$P \wedge Q,$$

$$P \wedge \sim Q,$$

$$\sim P \wedge Q$$

$$\sim P \wedge \sim Q.$$

2. Minterms for the three variables P, Q and R

$$P \wedge Q \wedge R$$

$$P \wedge Q \wedge \sim R$$

$$P \wedge \sim Q \wedge R$$

$$\sim P \wedge Q \wedge R$$

$$\sim P \wedge Q \wedge \sim R$$

$$\sim P \wedge \sim Q \wedge R$$

$$P \wedge \sim Q \wedge \sim R$$

$$\sim P \wedge \sim Q \wedge \sim R$$

Remark: 1. No minterms are equivalent.

2. Either $P \wedge Q$ or $Q \wedge P$ is included not both.

Principal disjunctive Normal form (PDNF):

For a given formula, an equivalent formula consisting of disjunctions of minterms only is known as its principal disjunctive normal form. Such a normal form is also called as the **sum of products canonical form**

Example 1. $P \rightarrow Q \Leftrightarrow (P \wedge Q) \vee (\sim P \wedge Q) \vee (\sim P \wedge \sim Q)$

Remark: The number of minterms appearing in the PDNF is same as the number of entries with the truth value T in the truth table of $P \rightarrow Q$

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

Example 1. Obtain the principle disjunctive normal form of

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

Solution:

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

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

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

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

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

Alternate Method: (Using truth table)

P	Q	$P \rightarrow Q$	$Q \rightarrow P$	$(P \rightarrow Q) \wedge (Q \rightarrow P)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Example 2. Obtain the principle disjunctive normal form of

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

Solution:

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

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

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

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

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

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

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

Example 3. Obtain the principle disjunctive normal form of

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

Solution:

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

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

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

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

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

Duality Law:

The two formulas A and A^* are said to be duals of each other if either one can be obtained by replacing ' \wedge ' by ' \vee ' (and ' \vee ' by ' \wedge ') and **T** by **F** (and **F** by **T**).

Maxterms:

For two variables P and Q, there are $2^2 = 4$ possible formulas which consists of disjunction of P or its negation and disjunctions of Q or its negation, given by $P \vee Q$, $P \vee \sim Q$, $\sim P \vee Q$ and $\sim P \vee \sim Q$.

These formulas are called maxterms.

1. Maxterms for the two variables P and Q

$$P \vee Q,$$

$$P \vee \sim Q,$$

$$\sim P \vee Q$$

$$\sim P \vee \sim Q.$$

2. Maxterms for three variables P, Q and R

$$P \vee Q \vee R$$

$$P \vee Q \vee \sim R$$

$$P \vee \sim Q \vee R$$

$$\sim P \vee Q \vee R$$

$$\sim P \vee Q \vee \sim R$$

$$\sim P \vee \sim Q \vee R$$

$$P \vee \sim Q \vee \sim R$$

$$\sim P \vee \sim Q \vee \sim R$$

Remark: 1. No maxterms are equivalent.

2. Either $P \vee Q$ or $Q \vee P$ is included not both.

3. Maxterms are the dual of minterms.

Principal conjunctive Normal form (PCNF):

For a given formula, an equivalent formula consisting of conjunctions of maxterms only is known as its principal conjunctive normal form. Such a normal form is also called as the **product of sums** canonical form.

Example 1. $P \rightarrow Q \Leftrightarrow \sim P \vee Q$

Remark: The number of maxterms appearing in the PCNF is same as the number of entries with the truth value F in the truth table of $P \rightarrow Q$

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

Principal conjunctive Normal form (PCNF):

For a given formula, an equivalent formula consisting of conjunctions of maxterms only is known as its principal conjunctive normal form. Such a normal form is also called as the **product of sums** canonical form.

Example 1. $P \rightarrow Q \Leftrightarrow \sim P \vee Q$

Remark: The number of maxterms appearing in the PCNF is same as the number of entries with the truth value F in the truth table of $P \rightarrow Q$

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

Example 2. Obtain the principle conjunctive normal form of

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

Solution:

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

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

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

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

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

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

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

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

Example 3. Obtain the principle conjunctive normal form of

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

Solution:

$$A = (P \wedge Q) \vee (\sim P \wedge Q \wedge R)$$

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

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

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

This is PDNF of the given formula.

$$A = (P \wedge Q \wedge R) \vee (P \wedge Q \wedge \sim R) \vee (\sim P \wedge Q \wedge R)$$

$\sim A$ contains the remaining terms

$$\sim A = (\sim P \wedge \sim Q \wedge \sim R) \vee (\sim P \wedge \sim Q \wedge R) \vee (\sim P \wedge Q \wedge \sim R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R)$$

We know that $\sim \sim A = A$. Taking negation of $\sim A$, we get PCNF

$$\begin{aligned}\sim \sim A &\Leftrightarrow \sim(\sim P \wedge \sim Q \wedge \sim R) \wedge \sim(\sim P \wedge \sim Q \wedge R) \wedge \sim(\sim P \wedge Q \wedge \sim R) \wedge \sim(P \wedge \sim Q \wedge R) \wedge \sim(P \wedge \sim Q \wedge \sim R) \\ &\Leftrightarrow (P \vee Q \vee R) \wedge (P \vee Q \vee \sim R) \wedge (P \vee \sim Q \vee R) \wedge (\sim P \vee Q \vee \sim R) \wedge (\sim P \vee Q \vee R)\end{aligned}$$

is the PCNF of A.

What are Rules of Inference for?

Mathematical logic is often used for logical proofs. Proofs are valid arguments that determine the truth values of mathematical statements.

An argument is a sequence of statements. The last statement is the conclusion and all its preceding statements are called **premises** (or hypothesis).

A valid argument is one where the conclusion follows from the truth values of the premises.

Rules of Inference provide the templates or guidelines for constructing valid arguments from the statements that we already have.

Theory of Inference:

Let A and B be two statement formulas. Then “B logically follows from A” or “ B is a valid conclusion (consequence) of the premise A” if and only if $A \rightarrow B$ is a tautology and is denoted by $A \Rightarrow B$.

A set of premises $\{H_1, H_2, \dots, H_n\}$ derives a conclusion C iff,

$$H_1 \wedge H_2 \dots \wedge H_n \Rightarrow C$$

Given a set of premises and a conclusion, it is possible to determine whether the conclusion logically follows from the given premises by constructing truth table.

Example:

Determine whether the conclusion C follows logically from the premises H_1 and H_2 .

(a) $H_1 : P \rightarrow Q$ $H_2 : P$ $C : Q$

(b) $H_1 : P \rightarrow Q$ $H_2 : \neg P$ $C : Q$

(c) $H_1 : P \rightarrow Q$ $H_2 : \neg(P \wedge Q)$ $C : \neg P$

Solution.

P	Q	$\neg P$	$P \rightarrow Q$	$P \wedge Q$	$\neg(P \wedge Q)$
T	T	F	T	T	F
T	F	F	F	F	T
F	T	T	T	F	T
F	F	T	T	F	T

- (a) We observe that in the first row, we have the truth value ‘true’ for both premises H_1, H_2 and the conclusion C . Hence it is a valid conclusion from the premises H_1 and H_2 .
- (b) We observe from 3rd and 4th rows, $P \rightarrow Q$ and $\neg P$ are true but the conclusion Q is true only in the third row but not in the fourth row and hence the conclusion Q is not valid.

(c) We observe that in the 3rd and 4th row, $P \rightarrow Q$ and $\neg(P \wedge Q)$ are true and the conclusion $\neg P$ is also true in these rows. Hence the conclusion $\neg P$ is valid.

(i.e.) $P \rightarrow Q, \neg(P \wedge Q) \Rightarrow \neg P$.

VALID ARGUMENT:

Any conclusion which is arrived at by following the given set of premises H_1, H_2, \dots, H_m and a set of inference rules is called a valid conclusion, and the argument is called a valid argument.

RULES OF INFERENCE

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

Rule T: A formula S may be introduced in a derivation if S is tautologically implied by any one or more of the preceding formulae in the derivation.

Implifications:

Simplification

$$I_1 : P \wedge Q \Rightarrow P$$

$$I_2 : P \wedge Q \Rightarrow Q$$

Addition

$$I_3 : P \Rightarrow P \vee Q$$

$$I_4 : Q \Rightarrow P \vee Q$$

Modes Ponens

$$I_5 : P, P \rightarrow Q \Rightarrow Q$$

Modes Tollens

$$I_6 : \neg Q, P \rightarrow Q \Rightarrow \neg P$$

Disjunctive syllogism

$$I_7 : \sim P, P \vee Q \Rightarrow Q$$

Hypothetical syllogism

$$I_8 : P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$$

Example:

Demonstrate that R is a valid inference from the premises

$$P \rightarrow Q, Q \rightarrow R \text{ and } P.$$

Line of derivation number	Statement formula	Rule of inference and implications/equivalences
(1)	$P \rightarrow Q$	Rule P
(2)	P	Rule P
(3)	Q	Rule T, (1), (2) and Implication 11 (modus ponens)
(4)	$Q \rightarrow R$	Rule P
(5)	R	Rule T (3), (4) and Implication 11.

Example: Show that $\neg P$ follows logically from $\neg(P \wedge \neg Q)$, $\neg Q \vee R$, $\neg R$.

(1) $\neg(P \wedge \neg Q)$	Rule <i>P</i>
(2) $\neg P \vee Q$	$\therefore \neg P \vee Q \Leftrightarrow \neg P \vee \neg \neg Q$
(3) $P \rightarrow Q$	$\therefore P \rightarrow Q \Leftrightarrow \neg P \vee Q$
(4) $\neg Q \vee R$	Rule <i>P</i>
(5) $Q \rightarrow R$	
(6) $P \rightarrow R$	From (3), (5)
(7) $\neg R$	Rule <i>P</i>
(8) $\neg P$	$\therefore \neg Q, P \rightarrow Q \Rightarrow \neg P$

Example: Show that $R \wedge (P \wedge Q)$ is a valid conclusion from the premises

$P \vee Q, Q \rightarrow R, P \rightarrow M, \sim M.$

Solution:

- | | | |
|----|-----------------------|------------------|
| 1. | $P \rightarrow M$ | Rule P |
| 2. | $\sim M$ | Rule P |
| 3. | $\sim P$ | Rule T, (1), (2) |
| 4. | $P \vee Q$ | Rule P |
| 5. | Q | Rule T, (3), (4) |
| 6. | $Q \rightarrow R$ | Rule P |
| 7. | R | Rule T, (5),(6) |
| 8. | $R \wedge (P \vee Q)$ | Rule T, (4), (7) |

Example:

Show that the premises “It is not sunny this afternoon and it is colder than yesterday,” “We will go swimming only if it is sunny,” “If we do not go swimming, then we will take a canoe trip,” and “If we take a canoe trip, then we will be home by sunset” lead to the conclusion “We will be home **by** sunset.”

Solution:

p: It is sunny this afternoon

q: It is colder than yesterday

r : we go swimming

s: We will take a canoe trip

t: We will be home by sunset (the conclusion)

$$1. \quad \neg p \wedge q$$

$$2. \quad r \rightarrow p$$

$$3. \quad \neg r \rightarrow s$$

$$4. \quad s \rightarrow t$$

$$5. \quad t$$

We construct an argument to show that our premises lead to the desired conclusion as follows.

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

Let us introduce the third rule of inference known as rule CP or Conditional proof:

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

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

Instead of deriving $R \rightarrow S$, we shall include R as an additional premise and arrive at S . That is, to prove ' S ' as a conclusion.

1. $\neg R \vee P$ Rule P
2. $R \rightarrow P$ Rule T , (1); $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
3. R Rule P (Assumed Premise)
4. P Rule T , (2), (3); $P, P \rightarrow Q \Rightarrow Q$
5. $P \rightarrow (Q \rightarrow S)$ Rule P
6. $Q \rightarrow S$ Rule T , (4), (5), $P, P \rightarrow Q \Rightarrow Q$
7. Q Rule P
8. S Rule T , (6), (7), $P, P \rightarrow Q \Rightarrow Q$
9. $R \rightarrow S$ Rule CP

Example: Show that $\sim P \vee Q, \sim Q \vee R, R \rightarrow S \Rightarrow P \rightarrow S$

Solution:

1. $\neg P \vee Q$ Rule *P*
2. $P \rightarrow Q$ Rule *T*, (1), $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
3. $\neg Q \vee R$ Rule *P*
4. $Q \rightarrow R$ Rule *T*, (3), $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
5. $P \rightarrow R$ Rule *T*, (2), (4), $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$
6. $R \rightarrow S$ Rule *P*
7. $P \rightarrow S$ Rule *T*, (5), (6), $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$

Thus $\neg P \vee Q, \neg Q \vee R, R \rightarrow S \Rightarrow P \rightarrow S$.

Alternate Method [Using Rule CP]:

Solution:

Include P as an additional premise and arrive at S .

1. $\neg P \vee Q$ Rule P
2. $P \rightarrow Q$ Rule T , (1), $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
3. P Rule P (Assumed Premise)
4. Q Rule T , (2), (3), $P, P \rightarrow Q \Rightarrow Q$
5. $\neg Q \vee R$ Rule P
6. $Q \rightarrow R$ Rule T , (5), $P \rightarrow Q \Rightarrow \neg P \vee Q$
7. R Rule T , (4), (6), $P, P \rightarrow Q \Rightarrow Q$
8. $R \rightarrow S$ Rule P
9. S Rule T , (7), (8), $P, P \rightarrow Q \Rightarrow Q$
10. $P \rightarrow S$ Rule CP.

Consistent and inconsistent:

A set of formulas H_1, H_2, \dots, H_n is said to be **consistent** if their conjunction has the truth value T for some assignment of the truth values to the atomic variables in H_1, H_2, \dots, H_n .

If for every assignment of the truth values to the atomic variables, atleast one of the formula H_1, H_2, \dots, H_n is false, so that their conjunction is identically false, then the formulae H_1, H_2, \dots, H_n are called **inconsistent**.

Example: Check whether the following premises are consistent:

$$P \rightarrow Q, Q \rightarrow R, (P \vee R), \sim R.$$

Solution:

1. $Q \rightarrow R$ Rule P
2. $\sim R$ Rule P
3. $\sim Q$ Rule $T, (1), (2), \sim Q, P \rightarrow Q \Rightarrow \sim P$
4. $P \rightarrow Q$ Rule P
5. $\sim P$ Rule $T, (3), (4), \sim Q, P \rightarrow Q \Rightarrow \sim P$
6. $P \vee R$ Rule P
7. R Rule $T, (5), (6); \sim P, P \vee R \Rightarrow R$
8. $R \wedge \sim R \Leftrightarrow F$ Rule $T, (2), (7); P, Q \Rightarrow P \wedge Q$

Hence the given premises are inconsistent.

Example: Show that $P \rightarrow Q, P \rightarrow R, Q \rightarrow \sim R, P$ are inconsistent.

Solution:

- | | |
|--|------------------|
| 1. $P \rightarrow Q$ | Rule P |
| 2. $Q \rightarrow \sim R$ | Rule P |
| 3. $P \rightarrow \sim R$ | Rule T, (1), (2) |
| 4. P | Rule P |
| 5. $\sim R$ | Rule T, (3), (4) |
| 6. $P \rightarrow R$ | Rule P |
| 7. $\sim P$ | Rule T, (5),(6) |
| 8. $P \wedge \sim P \Leftrightarrow F$ | Rule T, (4), (7) |

Indirect method

The technique of indirect method of proof run as follows:

1. Introduced the negation of the desired conclusion as a new premise.
2. Derive a contradiction from the set of premises including the new premise.
3. Assert the desired conclusion as a logical inference from the premises.

Example: Show by indirect method

$$R \rightarrow \sim Q, R \vee S, S \rightarrow \sim Q, P \rightarrow Q \implies \sim P$$

1. P Rule P , Additional premise
2. $P \rightarrow Q$ Rule P
3. Q Rule $T, (1), (2), P, P \rightarrow Q \Rightarrow Q$
4. $S \rightarrow \neg Q$ Rule P
5. $\neg Q \rightarrow \neg S$ Rule $T, (4), P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
6. $\neg S$ Rule $T, (3), (5), P, P \rightarrow Q \Rightarrow Q$
7. $R \vee S$ Rule P
8. $\neg R \rightarrow S$ Rule $T, (7), P \rightarrow Q \Leftrightarrow \neg P \vee Q$
9. $\neg S \rightarrow R$ Rule $T, (8), P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
10. R Rule $T, (6), (9), P, P \rightarrow Q \Rightarrow Q$
11. $R \rightarrow \neg Q$ Rule P
12. $\neg Q$ Rule $T, (10), (11), P, P \rightarrow Q \Rightarrow Q$
13. $Q \wedge \neg Q \Leftrightarrow F$ Rule $T, (3), (12), P, Q \Rightarrow P \wedge Q$

Example: Show by indirect method

$$P \rightarrow (Q \vee R), Q \rightarrow \sim P, S \rightarrow \sim R, P \implies P \rightarrow \sim S$$

Including $\sim(\sim P \vee \sim S)$ (i.e $P \wedge S$) as an additional premise

Solution:

- | | | |
|-----|-------------------------------------|---|
| 1. | $P \rightarrow (Q \vee R)$ | Rule P |
| 2. | P | Rule P |
| 3. | $Q \vee R$ | Rule T, (1), (2) |
| 4. | $S \rightarrow \sim R$ | Rule P |
| 5. | $P \wedge S$ | Rule P, Additional premise |
| 6. | S | Simplification $P \wedge S \Rightarrow S$ |
| 7. | $\sim R$ | Modus ponens , (4),(6) |
| 8. | Q | Modus Tollens (3), (7) |
| 9. | $Q \rightarrow \sim P$ | Rule P |
| 10. | $\sim P$ | Modus ponens (8), (10) |
| 11. | $P \wedge \sim P \Leftrightarrow F$ | Rule T, (6), (10) |

VALIDITY OF ARGUMENTS:

In day-to-day life, we come across arguments expressed as sentences. We can represent these sentences in English as symbols and thereby verify the validity of these arguments.

Example:

Show that the following set of premises are inconsistent:

If the contract is valid, then John is liable for penalty. If John is liable for penalty, he will go bankrupt. If the bank will loan him money, he will not go bankrupt. As a matter of fact, the contract is valid and the bank will loan him money.

Solution:

P: The contract is valid

Q: John is liable for penalty

R: Bank will loan him money

S: He will go bankrupt

The given premises are

$$P \rightarrow Q, Q \rightarrow R, S \rightarrow \sim R, P \wedge S$$

To prove ,

$$P \rightarrow Q, Q \rightarrow R, S \rightarrow \sim R, P \wedge S \Rightarrow F$$

- | | |
|---|---|
| 1. $P \rightarrow Q$ | Rule P |
| 2. $Q \rightarrow R$ | Rule P |
| 3. $P \rightarrow R$ | Rule T, (1), (2) |
| 4. $P \wedge S$ | Rule P |
| 5. P | Simplification $P \wedge S \Rightarrow P$ |
| 6. S | Simplification $P \wedge S \Rightarrow S$ |
| 7. R | Rule T, (3),(5) |
| 8. $S \rightarrow \neg R$ | Rule P |
| 9. $R \rightarrow \neg S$ | Rule T |
| 10. $\neg S$ | Modus ponens (7) (8) |
| 11. $S \wedge \neg S \Leftrightarrow F$ | Rule T, (6), (10) |

Example:

"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.

Let P : There was a ball game

Q : Travelling was difficult

R : They arrived on time.

The premises are:

$P \rightarrow Q, R \rightarrow \neg Q, R$ and the conclusion is $\neg P$

1. $P \rightarrow Q$ Rule P
2. $R \rightarrow \neg Q$ Rule P
3. $Q \rightarrow \neg R$ Rule T , (2), $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
4. $P \rightarrow \neg R$ Rule T , (1), (3), $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$
5. $R \rightarrow \neg P$ Rule T , (4), $P \rightarrow Q \Leftrightarrow \neg Q \rightarrow \neg P$
6. R Rule P
7. $\neg P$ Rule T , (5), (6), $P, P \rightarrow Q \Rightarrow Q$

Hence the given statements constitute a valid argument.

Introduction of Predicate calculus

The discussion of symbolic logic has been limited to the consideration of statements and statement formulae. It was not possible to express the fact that any two atomic statements have some features in common. In order to investigate questions of this nature, **we introduce the concept of a predicate in an atomic statement.** The logic based upon the analysis of predicates in any statement is called predicate logic.

Predicate calculus:

Let us consider two statements

- ▶ Ramu is clever
- ▶ Sita is clever

If we express these statements by symbols, we require two different symbols to denote them and it does not reveal the common features of these two statements i.e., both statements are about two different individuals who are clever.

We can introduce some symbol to denote “ **is clever**” and a method to join it with symbols denoting the name of individuals. The part “ **is clever**” is called a **predicate**.

We symbolize a predicate by a capital letter and the name of individuals or objects in general by small letters.

Let us denote:

Ramu by 'r'

Sita by 's'

And a predicate “**is clever**” by a letter C

Now, the given statements can be written as C(r) and C(s).

Note: A statement which is expressed by using a predicate letter must have at least one name of object associated with the predicate.

Type of Predicates:

- One place predicate:

This painting is red.
Can be symbolized as $R(p)$.

- Two place predicate:

Ex: Mani is taller than Ravi.
We can denote this as $T(m,r)$.

T is two place predicate as two subjects needed to complete the statement.

3-place predicate:

Ex: Mohan stands between Raj and Nitin.

$B(m,r,n)$

4-place predicate:

David & Tendulkar played cricket against Ganguly and Kambli.

$P(d,t,g,k)$

EXAMPLE 1

Let $P(x)$ denote the statement “ $x > 3$.” What are the truth values of $P(4)$ and $P(2)$?

Solution: We obtain the statement $P(4)$ by setting $x = 4$ in the statement “ $x > 3$.” Hence, $P(4)$, which is the statement “ $4 > 3$,” is true. However, $P(2)$, which is the statement “ $2 > 3$,” is false.

Statement function and variables

A simple statement function of one variable is defined to be an expression consisting of a predicate symbol and an individual variable.

Example: $M(x)$: x is a man.

We can also combine one or more statement functions using logical connectives which form **compound statement function**.

Example: $M(x)$: x is a man and $H(x)$: x is mortal, then $M(x) \wedge H(x)$, $M(x) \rightarrow H(x)$, $\sim M(x)$, etc

Same way we can define a statement function of two variables and more:

Ex: Let $G(x, y)$: x is taller than y .

If x is replaced by Pooja and y by Megha.

Then $G(x, y)$ becomes

Pooja is taller than Megha.

It is possible to form statement function of two variable from statement function of one variable:

Ex: $M(x)$: x is a man.

$H(y)$: y is mortal.

Then $M(x) \wedge H(y)$: x is a man and y is mortal.

Quantifiers

By which we can indicate the quantity by means of words like ‘all’, ‘some’, ‘none’, etc.

Example: *Some* man are mortal.

Types of quantifiers

1. Universal Quantifiers
2. Existential Quantifiers

Universal Quantifiers

The quantifiers ‘all’ is called the universal quantifier. It is denoted by the symbol $\forall x$ or (x) for the variable x .

Phrases for Universal Quantifiers:

1. For all x ,
2. For every x ,
3. For each x ,
4. Everything x is such that
5. Each thing x is such that

Examples: “All men are mortal”

Let $M(x)$: x is a man

$H(x)$: x is Mortal.

The symbolic form of the given statement is $(\forall x)(M(x) \rightarrow H(x))$.

Existential Quantifiers

The quantifiers ‘some’ is called the existential quantifier. It is denoted by the symbol $(\exists x)$ for some variable x .

Phrases for Existential Quantifiers:

1. For some x ,
2. For some x such that,
3. There exist an x such that,
4. There is an x such that,
5. There is atleast one x such that.

Example 1: The proposition:

There is a dog without a tail can be written as

$$(\exists \text{ a dog}) (\text{the dog without tail})$$

Example 2: The proposition:

There is an integer between 2 and 8 inclusive may be written as

$$(\exists \text{ an integer}) (\text{the integer is between 2 and 8})$$

The propositions which include quantifiers may be negated as follows:

Example 3: Negate the proposition

All integers are greater than 8.

Solution: We can write the given proposition as

$$(\forall \text{ integers } x) (x > 8)$$

The negation is

$$(\exists \text{ an integer } x) (x \leq 8)$$

i.e., the negated proposition is: There is an integer less than or equal to 8.

In the negation a proposition ‘for all’ becomes ‘there is’ and ‘there is’ becomes ‘for all’ i.e., the symbol \forall becomes \exists and \exists becomes \forall .

Example

Symbolize the following statements

- a) Some men are honest.
- b) Few cars have AC facility.
- c) No cats has a tail.
- d) All babies are innocent.

Universe of discourse

We can restrict our discussion to a particular set of objects or persons, (i.e.) the variables which are quantified stand for only those objects which are members of a particular set of class. Such a restricted class is called the **universe of discourse** or **domain of discourse** or **universe**.

Example: Let us take the statement

$P(x)$: x is a cricket player

then the domain of discourse for this statement can be taken as the set of all human beings

All cats are animals.

Which is true for any universe of discourse.

Let Universe of discourse is $E = \{cuddle, lilly, 0,1\}$, where cuddle and lilly are the names of the cat.

Then statement is true over E.

If we denote

$C(x)$: x is a cat.

$A(x)$: x is a animal.

Then the statement $(\forall x) (C(x) \rightarrow A(x))$ is true over E.

And the statement $(\forall x) (C(x) \wedge A(x))$ is false.

i.e. in symbolic expressions of the type “All A are B” the correct connective that should be used is conditional.

Some cats are black.

Let Universe of discourse is $E = \{cuddle, lilly, kitty, 0, 1\}$, where cuddle and lilly are black cats.

If we denote

$C(x)$: x is a cat.

$B(x)$: x is a black.

Then the statement

$(\exists x) (C(x) \rightarrow B(x))$ is false over E.

And the statement $(\exists x) (C(x) \wedge B(x))$ is true over E.

i.e. in symbolic expressions of the type “Some A are B” the correct connective that should be used as conjunction.

Free and Bound Variable

A part of the formula containing $(\forall x)P(x)$ or $(\exists x) P(x)$ is called x -bound part of the formula.

An occurrence of x in x bound part of a formula is called bound occurrence.

Any occurrence of x that is not bound occurrence is free occurrence.

Scope of the quantifier

The formula $P(x)$ in $(\forall x)P(x)$ or in $(\exists x) P(x)$ called scope of the quantifier i.e. scope of the quantifier is the formula immediately following the quantifier.

Example: $(\forall x)P(x, y)$

Here $P(x, y)$ is the scope of the quantifier.

Both occurrences of x is bound occurrences while occurrence of y is free occurrence.

Example: $(\forall x)(P(x) \rightarrow Q(x))$

Scope of the quantifier is $P(x) \rightarrow Q(x)$ and all occurrences of are bound occurrences.

Example 1. Find the truth value of $(\forall x)P(x)$, where $P(x):x^2 < 10$ and universe of discourse consist of a positive integer not exceeding 4.

Solution: The statement $(\forall x)P(x)$ for the given universe of discourse, is same as

$$\begin{aligned} P(1) \wedge P(2) \wedge P(3) \wedge P(4) &\Leftrightarrow T \wedge T \wedge T \wedge F \\ &\Leftrightarrow F \end{aligned}$$

i.e. $(\forall x)P(x)$ is false.

- Determine the truth value of following, consider set of real numbers as universe of discourse:

(a) $\exists x, x^2 = x.$

Ans: true

(b) $\exists x, x + 2 = x.$

Ans: False

- Determine the truth value if $A = \{1, 2, 3, \dots, 9, 10\}$

(a) $(x)(\exists y)(x + y < 14)$ Ans: True

(b) $(x)(y)(x + y < 14)$ Ans: False

Equivalence Formula of Predicate Calculus:

1. $(\exists x)(A(x) \vee B(x)) \Leftrightarrow (\exists x)A(x) \vee (\exists x)B(x)$
2. $(\forall x)(A(x) \wedge B(x)) \Leftrightarrow (\forall x)A(x) \wedge (\forall x)B(x)$
3. $(\forall x)(A \vee B(x)) \Leftrightarrow A \vee (\forall x)B(x)$
4. $(\exists x)(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)B(x)$
5. $(\forall x)A(x) \rightarrow B \Leftrightarrow (\exists x)(A(x) \rightarrow B)$
6. $(\exists x)A(x) \rightarrow B \Leftrightarrow (\forall x)(A(x) \rightarrow B)$
7. $A \rightarrow (\forall x)B(x) \Leftrightarrow (\forall x)(A \rightarrow B(x))$
8. $A \rightarrow (\exists x)B(x) \Leftrightarrow (\exists x)(A \rightarrow B(x))$

Implications of Predicate Calculus

1. $(\forall x)A(x) \vee (\forall x)B(x) \Rightarrow (\forall x)(A(x) \vee B(x))$
2. $(\exists x)(A(x) \wedge B(x)) \Rightarrow (\exists x)A(x) \wedge (\exists x)B(x)$

Demorgan's Laws for Predicate Calculus:

1. $\neg(\forall x)P(x) \Leftrightarrow (\exists x)\neg P(x)$
2. $\neg(\exists x)P(x) \Leftrightarrow (\forall x)\neg P(x)$

Proof : Let domain is the set $S=\{x_1, x_2, \dots, x_n\}$

Then $(\forall x)P(x)=P(x_1)\wedge P(x_2)\wedge \dots \wedge P(x_n)$

And $(\exists x)P(x)=P(x_1)\vee P(x_2)\vee \dots \vee P(x_n)$

$$\begin{aligned} \text{Now, } \neg(\forall x)P(x) &\Leftrightarrow \neg [P(x_1)\wedge P(x_2)\wedge \dots \wedge P(x_n)] \\ &\Leftrightarrow \neg P(x_1)\vee \neg P(x_2)\vee \dots \vee \neg P(x_n) \\ &\Leftrightarrow (\exists x)\neg P(x) \end{aligned}$$

i.e. $\neg(\forall x)P(x) \Leftrightarrow (\exists x)\neg P(x)$

Example : Symbolize the following statements and also negate them.

1. All cities in India are clean.
2. Some cities in India are polluted.
3. Some birds cannot fly.
4. No dog is Intelligent.
5. No cat has a tail.
6. All babies are innocent.
7. Few cars have AC facility.

Inference Theory for Predicate Calculus:

Let $A(x)$ be any predicate formula, where x is particular object.

1. Universal Specification (Rule U.S) or Universal Instantiation: It is the rule of inference which states that $A(y)$ is true, if $(\forall x) A(x)$ is true, where y is any arbitrary member of the universe of discourse.

i.e.

$$(\forall x) A(x) \Rightarrow A(y)$$

2. Universal Generalization (Rule U.G): It is the rule which states that $(\forall x) A(x)$ is true, if $A(y)$ is true,

where y is the arbitrary member of the universe of discourse.

i.e.

$$A(y) \Rightarrow (\forall x) A(x)$$

3. Existential Specification (Rule E.S) : Existential Specification is the rule of inference which allows us to conclude that $A(y)$ is true, if $(\exists x) A(x)$ is true where y is not an arbitrary member of the universe, but one for which $A(y)$ is true.

i.e.

$$(\exists x) A(x) \Rightarrow A(y)$$

4. Existential Generalization (Rule E.G): Existential Generalization is the rule that is used to conclude that $(\exists x) A(x)$ is true, when $A(y)$ is true, where y is a particular member of the universe of discourse.

$$A(y) \Rightarrow (\exists x) A(x)$$

Example 1.: Show that

$$(x)(H(x) \rightarrow M(x)) \wedge H(a) \Rightarrow M(a).$$

Solution:

- | | |
|--|------------------------|
| 1. $(x)(H(x) \rightarrow M(x))$ | Rule P |
| 2. $H(a) \rightarrow M(a)$ | Rule US, (1) |
| 3. $H(a)$ | Rule P |
| 4. $M(a)$ | Modus Ponens, (2), (3) |

Example 2.: Show that

$$(x)(P(x) \rightarrow Q(x)) \wedge (x)(Q(x) \rightarrow R(x)) \Rightarrow (x)(P(x) \rightarrow R(x))$$

Solution:

- | | | |
|----|------------------------------|--------------|
| 1. | $(x)(P(x) \rightarrow Q(x))$ | Rule P |
| 2. | $P(y) \rightarrow Q(y)$ | Rule US, (1) |
| 3. | $(x)(Q(x) \rightarrow R(x))$ | Rule P |
| 4. | $Q(y) \rightarrow R(y)$ | Rule US, (3) |
| 5. | $P(y) \rightarrow R(y)$ | Rule T |
| 6. | $(x)(P(x) \rightarrow R(x))$ | Rule UG, (5) |

Example 3: Show that

$$(\exists x)(H(x) \rightarrow M(x)), (\exists x)H(x) \Rightarrow (\exists x)M(x)$$

Solution:

- | | | |
|----|--------------------------------------|------------------------|
| 1. | $(\exists x)H(x)$ | Rule P |
| 2. | $H(y)$ | Rule ES, (1) |
| 3. | $(\exists x)(H(x) \rightarrow M(x))$ | Rule P |
| 4. | $H(y) \rightarrow M(y)$ | Rule US, (3) |
| 5. | $M(y)$ | Modus ponens, (2), (5) |
| 6. | $(\exists x)M(x)$ | Rule EG, (5) |

Example 4: Show that

$$(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x)P(x) \wedge (\exists x)Q(x)$$

Solution:

- | | | |
|----|--|------------------|
| 1. | $(\exists x)(P(x) \wedge Q(x))$ | Rule P |
| 2. | $P(y) \wedge Q(y)$ | Rule ES, (1) |
| 3. | $P(y)$ | Rule T |
| 4. | $(\exists x)P(x)$ | Rule EG, (3) |
| 5. | $Q(y)$ | Rule T |
| 6. | $(\exists x)Q(x)$ | Rule EG, (5) |
| 7. | $(\exists x)P(x) \wedge (\exists x)Q(x)$ | Rule T, (4), (6) |

Example: Show that from

(a) $(\exists x)(F(x) \wedge S(x)) \rightarrow (\forall y)(M(y) \rightarrow W(y))$ and

(b) $(\exists y)(M(y) \wedge \neg W(y))$

the conclusion $(\forall x)(F(x) \rightarrow \neg S(x))$ follows.

Solution:

1. $(\exists y)(M(y) \wedge \neg W(y))$

Rule P

2. $M(a) \wedge \neg W(a)$

Rule ES, (1)

3. $\neg(M(a) \rightarrow W(a))$

Rule T, (2) $P \wedge \neg Q \Leftrightarrow \neg(P \rightarrow Q)$

4. $(\exists y)\neg(M(y) \rightarrow W(y))$

Rule EG, (3)

5. $\neg(\forall y)(M(y) \rightarrow W(y))$

Rule T, Demorgan's law

6. $(\exists x)(F(x) \wedge S(x)) \rightarrow (\forall y)(M(y) \rightarrow W(y))$

Rule P

7. $\neg(\exists x)(F(x) \wedge S(x))$

Modus Tollens, (5), (6)

- 8. $(x)\sim(F(x) \wedge S(x))$
- 9. $\sim(F(a) \wedge S(a))$
- 10. $\sim F(a) \vee \sim S(a)$
- 11. $F(a) \rightarrow \sim S(a)$
- 12. $(x)(F(x) \rightarrow \sim S(x))$

Rule T

Rule US, (8)

Rule T, (2) $P \wedge \sim Q \Leftrightarrow \sim(P \rightarrow Q)$

Rule T, (10)

Rule UG,

Example: Use indirect method of proof to show that

$$(x)(P(x) \rightarrow Q(x)) \wedge (\exists y)P(y) \Rightarrow (\exists z)Q(z)$$

Solution: Assuming $\sim(\exists z)Q(z)$ as an additional premise

- | | | |
|-----|--|-------------------------|
| 1. | $\sim(\exists z)Q(z)$ | Rule P, Assumed premise |
| 2. | $(\forall z)\sim Q(z)$ | Rule T, DeMorgan's law |
| 3. | $(\exists y)P(y)$ | Rule P |
| 4. | $P(a)$ | Rule ES, (3) |
| 5. | $\sim Q(a)$ | Rule US, (2) |
| 6. | $P(a) \wedge \sim Q(a)$ | Rule T, (4), (5) |
| 7. | $\sim(P(a) \rightarrow Q(a))$ | Rule T, (6) |
| 8. | $(x)(P(x) \rightarrow Q(x))$ | Rule P |
| 9. | $P(a) \rightarrow Q(a)$ | US, (8) |
| 10. | $(P(a) \rightarrow Q(a)) \wedge \sim(P(a) \rightarrow Q(a)) \Leftrightarrow F$ | Rule T |

Example: Use Conditional proof to prove that

$$(x)(P(x) \rightarrow Q(x)) \Rightarrow (x)P(x) \rightarrow (x)Q(x)$$

Solution: Take $(x)P(x)$ as an assumed premise

1. $(x)(P(x) \rightarrow Q(x))$ *Rule P*
2. $P(y) \rightarrow Q(y)$ *Rule US, (1)*
3. $(x)P(x)$ *Rule P(Assumed premise)*
4. $P(y)$ *Rule US, (3)*
5. $Q(y)$ *Rule T, (2), (4), P, P → Q ⇒ Q*
6. $(x)Q(x)$ *Rule UG, (5)*
7. $(x)P(x) \rightarrow (x)Q(x)$ *Rule CP*

Validity of Arguments:

Example 1. Verify the validity of the following arguments:

- (a) All humming birds are richly coloured
- (b) No large birds live on honey
- (c) Birds that do not live on honey are dull in colour.
- (d) Therefore humming birds are small.

Solution: $H(x)$: x is a humming bird

$C(x)$: x is richly coloured

$S(x)$: x lives on honey

$L(x)$: x is a large bird

Given Premises are

$$\begin{aligned}(x)(H(x) \rightarrow C(x)), \\ (x)(L(x) \rightarrow \sim S(x)) \\ (x)(\sim S(x) \rightarrow \sim C(x))\end{aligned}$$

And the conclusion is

$$(x)(H(x) \rightarrow \sim L(x)),$$

Solution:

- | | |
|---|------------------|
| 1. $(x)(L(x) \rightarrow \sim S(x))$ | Rule P |
| 2. $L(y) \rightarrow \sim S(y)$ | Rule US, (1) |
| 3. $(x)(\sim S(x) \rightarrow \sim C(x))$ | Rule P |
| 4. $\sim S(y) \rightarrow \sim C(y)$ | Rule US, (3) |
| 5. $L(y) \rightarrow \sim C(y)$ | Rule T, (2), (4) |
| 6. $C(y) \rightarrow \sim L(y)$ | Rule T, (5) |
| 7. $(x)(H(x) \rightarrow C(x))$ | Rule P |
| 8. $H(y) \rightarrow C(y)$ | Rule US, (7) |
| 9. $H(y) \rightarrow \sim L(y)$ | Rule T, (6), (8) |
| 10. $(x)(H(x) \rightarrow \sim L(x))$ | Rule UG, (9) |

Example 2. Verify the validity of the following arguments:

- (a) All men are mortal
- (b) Socrates is a man.

Therefore Socrates is a mortal.

Solution: $H(x)$: x is a man

$M(x)$: x is a mortal

s : Socrates

The given premises are:

$(x)(H(x) \rightarrow M(x)), H(s)$ and the conclusion is $M(s)$

- | | | |
|----|------------------------------|------------------|
| 1. | $(x)(H(x) \rightarrow M(x))$ | Rule P |
| 2. | $H(s) \rightarrow M(s)$ | Rule US |
| 3. | $H(s)$ | Rule |
| 4. | $M(s)$ | Rule T, (2), (3) |

Example 3. Verify the validity of the following arguments:

Lions are dangerous animals. There are lions. Therefore there are dangerous animals.

Solution: $L(x)$: x is a Lion

$D(x)$: x is a dangerous animal

The given premises are:

$(x)(L(x) \rightarrow D(x))$, and $(\exists x)L(x)$ and the conclusion is $(\exists x)D(x)$.

Proof:

1. $(\exists x)L(x)$ Rule P

2. $L(y)$ Rule ES

3. $(x)(L(x) \rightarrow D(x))$ Rule P

4. $L(y) \rightarrow D(y)$ Rule US, (3)

5. $D(y)$ Rule T, (2), (4)

6. $(\exists x)D(x)$ Rule EG

Worksheet-I

Discrete Mathematics and Graph Theory

(BMAT205L)

Ankush Chanda

August 14, 2023

Problems

1 Propositional Calculus

1. Prove the following without using truth table:

$$(p \vee q) \wedge (p \rightarrow r) \wedge (q \rightarrow r) \implies r.$$

2. Find the disjunctive normal form of the following statement:

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

3. Find the conjunction normal form of the following statement:

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

4. Without constructing the truth table, find the principal conjunctive normal form of the following statement:

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

5. Show that

$$(p \rightarrow q) \wedge (r \rightarrow s), (q \rightarrow t) \wedge (s \rightarrow u), \sim (t \wedge u) \text{ and } (p \rightarrow r) \implies p.$$

6. Derive $p \rightarrow (q \rightarrow s)$ using the CP-rule from the premises $p \rightarrow (q \rightarrow r)$ and $q \rightarrow (r \rightarrow s)$.

7. Using indirect method of proof, derive $p \rightarrow \sim s$ from the premises $p \rightarrow (q \vee r), q \rightarrow \sim p, s \rightarrow \sim r, p.$
8. Prove that the premises $a \rightarrow (b \rightarrow c), d \rightarrow (b \wedge \sim c)$ and $(a \wedge d)$ are inconsistent.
9. Construct an argument to show that the following premises imply the conclusion “it rained”. “If it does not rain or if there is no traffic dislocation, then the sports day will be held and the cultural programme will go on”, “If the sports day is held, the trophy will be awarded” and “the trophy was not awarded”.
10. Show that the following set of premises is inconsistent:

If Neel gets his degree, he will go for a job.
 If he goes for a job, he will get married soon.
 If he goes for higher study, he will not get married.
 Neel gets his degree and goes for higher study.
11. Show that the premises “If you send me an e-mail, then I will finish writing the program,” “If you do not send me an e-mail, then I will go to sleep early,” and “If I go to sleep early, then I will wake up feeling refreshed” lead to the conclusion “If I do not finish writing the program, then I will wake up feeling refreshed.”

2 Predicate Calculus

1. Express each of the following statements using mathematical and logical operations, predicates and quantifiers, where the universe of discourse consists of all computer science students/mathematics courses.
 - (a) Every computer science student needs a course in mathematics.
 - (b) There is a student in this class who owns a personal computer.
 - (c) Every student in this class has taken at least one mathematics course.
 - (d) There is a student in this class who has taken at least one mathematics course.
2. Show, by indirect method of proof, that $\forall x : (P(x) \vee Q(x)) \implies (\forall x : P(x)) \vee (\exists x : Q(x)).$
3. Show that $\forall x : (P(x) \vee Q(x)) \implies \forall x : P(x) \vee \exists x : Q(x)$, using the indirect method.
4. Show that the premises “A student in this class has not read the book,” and “Everyone in this class passed the first exam” imply the conclusion “Someone who passed the first exam has not read the book.”

ALGEBRAIC STRUCTURES

Introduction

Let A be any set. A Mapping $f : A \times A \times \dots \times A \rightarrow A$ (or) $f : A^n \rightarrow A$ is called an n-ary operation and ‘n’ called the order of the operation.

Unary operation:

$n=1, f : A \rightarrow A$

Binary operation:

$n=2, f : A \times A \rightarrow A$

Algebraic system (or) algebra:

A set together with a number of operations (binary) on the set is called an **Algebraic system**

Example

- Semi groups
- Monoids
- Groups are algebraic systems with one binary operation.
- Rings, Integral domains ,Fields are algebraic systems with two binary operation.

Properties of Binary operations

- **Closure property:** A binary operation $*: G \times G \rightarrow G$ is said to be closed if for all $a, b \in G$ an element an element $a*b = x \in G$.
- **Associative:** $a*(b*c) = (a*b)*c$, for all $a, b, c \in G$
- **Existence of Identity:** There exists an element $e \in G$ such that $e*a = a*e = a$, $a \in G$ for all. The elements e called the identity element.
- **Existence of inverse:** For $a \in G$, there exists an element $b \in G$ such that $a*b = b*a = e$. The element b is called the inverse of ' a ' and it is denoted by $b = a^{-1}$
- **Commutative:** For all $a, b \in G$, if $a*b = b*a$, then $*$ is commutative(abelian)
- **Distributive properties:**

$$a*(b . c) = (a*b) . (a*c)$$

(left distributive law)

$$(b . c)*a = (b*a) . (c*a)$$

(right distributive law)

for all $a, b, c \in G$

- **Cancellation properties:**

$$a*b = a*c \Rightarrow b = c$$

[left cancellation Law]

$$b*a = c*a \Rightarrow b = c, \text{ for all } a, b, c \in G$$

[right cancellation Law]

Semi groups:

- **Definition:**

A non-empty set S together with the binary operation $*: S \times S \rightarrow S$ is said to be a **Semi group** if $*$ satisfies the following conditions, namely the closure property and associative property. We denote the semi group by $(S, *)$.

- **Example.1**

Let $N = \{1, 2, 3, \dots\}$ be the set of natural numbers. Then $(N, +)$ and (N, \times) are semi group under the binary operations addition and multiplication respectively.

- **Example.2**

Let $E = \{2, 4, 6, \dots\}$ be the set of all even numbers. Then $(E, +)$ and (E, \times) are semi groups.

- **Morphism of semi groups:**

Let $(S, *)$ and (T, Δ) be any two semi groups. A mapping $f : S \rightarrow T$ is said to be a **semi group homomorphism** if $f(f(a * b)) = f(a) \Delta f(b)$, for all $a, b \in S$.

$f : (S, *)$	$\xrightarrow[1-1]{\text{homomorphism}} (T, \Delta)$	\rightarrow monomorphism
$f : (S, *)$	$\xrightarrow{\text{Onto}} (T, \Delta)$	\rightarrow epimorphism
$f : (S, *)$	$\xrightarrow{\text{homomorphism}} (T, \Delta)$	\rightarrow isomorphism
$f : (S, *)$	$\xrightarrow[1-1 \text{ and onto}]{\text{isomorphism}} (T, \Delta)$	\rightarrow endomorphism
$f : (S, *)$	$\xrightarrow[1-1]{\text{isomorphism}} (T, \Delta)$	\rightarrow automorphism

Example:

Let $(N, +)$ and $(Z_e, +_m)$ be any two semi groups.

Define a map $f : N \rightarrow Z_m$ by $f(a) = [a]_m$, for all $a \in N$.

Then $f(a + b) = [a + b]_m = [a]_m +_m [b]_m = f(a) +_m f(b)$

Therefore f is a semi group homomorphism.

Monoids:

- **Definition:**

A semi group (M , *) with an identity element with respect to the operation * is called a **Monoid (or)** a non empty set M together with the binary operation *: $M \times M \rightarrow M$ is said to be a **Monoid if** * satisfies the closure property, associative property and identity property.

- **Example.1**

Let $N = \{1, 2, 3, \dots\}$ be the set of natural numbers. Then (N, X) is a monoid with the identity element **1**, but $(N, +)$ is not a monoid since the additive identity **0** is not a natural number.

- **Example.2**

Let $Z_+ = \{0, 1, 2, 3, \dots\}$ be the set of all non-negative integers. Then $(Z_+, +)$ and (Z_+, X) are semi groups as well as monoids.

- **Example.3**

Let S be a nonempty set and $P(s)$ be its power set. Then $(P(s), U)$ and $(P(s), \cap)$ are monoids with identities φ and S respectively.

- **Morphism of monoids:**

Let $(M, *, e_M)$ and (T, Δ, e_T) be any two monoids with the identity elements e_M and e_T respectively. A mapping

$f : M \rightarrow T$ is said to be a **monoid morphism** if for any two elements $a, b \in M$, $f(a * b) = f(a) \Delta f(b)$ and $f(e_M) = e_T$

¹

$f : (M, *, e_M) \xrightarrow{1-1} (T, \Delta, e_T) \rightarrow \text{monomorphism}$

$f : (M, *, e_M) \xrightarrow{\text{onto}} (T, \Delta, e_T) \rightarrow \text{epimorphism}$

$f : (M, *, e_M) \xrightarrow{\text{1-1 and onto}} (T, \Delta, e_T) \rightarrow \text{isomorphism}$

- **Theorem 1:**

For any commutative monoid $(M, *)$, the set of idempotent element of M forms a submonoid.

Proof:

Let $(M, *)$ be a commutative monoid.

Let $S = \{a \in M / a * a = a\}$, the set of idempotent elements of M .

Clearly $e \in S$, as $e * e = e$.

Let $a, b \in S$ with $a * a = a$ $b * b = b$.

$$\text{Now } (a * b) * (a * b) = (a * b) * (b * a)$$

$$= a * (b * b) * a$$

$$= a * (b) * a$$

$$= a * (b * a)$$

$$= a * (a * b)$$

$$= (a * a) * b$$

$$= a * b$$

Hence $a * b \in S$

Therefore $(S, *)$ is a sub monoid of $(M, *)$

GROUPS

Definition (1):

A non-empty set G together with the binary operation $*$, $(G, *)$ is called a **group** if $*$ satisfies the following conditions

- Associative:** For every $a, b, c \in G$, $a*(b*c)=(a*b)*c$.
- Identity:** There exists an element $e \in G$ called the identity element such that $a*e=e*a=a$, for all $a \in G$.
- Inverse:** There exists an element $a^{-1} \in G$ called the inverse of 'a' such that $a * a^{-1} = a^{-1} * a = e$, for each $a \in G$

Definition (2):

A group $(G, *)$ is said to be abelian group if $a*b=b*a$, for all $a, b \in G$. otherwise it is non-abelian group.

Definition (3):

The order of a group $(G, *)$, denote by $O(G)$ or $|G|$, is the number of elements of G , is finite.

Example (1):

The set of all integers Z with the operation of ordinary addition is an infinite abelian group.

Example (2):

The set of all integers Z is not a group under multiplication. (Z, \cdot) is not a group. Because there is no multiplicative inverse in Z . But (Z, \cdot) is a monoid and hence a semi group.

Example (3):

The set of all non-zero real numbers R from an infinite abelian group under the binary operation $*$ defined by $a*b=ab/2$, for all $a, b \in R$

Example (4):

The set of all non-zero real numbers R , under the operation of ordinary multiplication is a group. An inverse of $a \neq 0$ is $1/a$ i.e. $a^{-1} = 1/a$

Example (5):

Prove that the set $A = \{1, \omega, \omega^2\}$ is an abelian group of order 3 under multiplication. Where $1, \omega, \omega^2$ are cube roots of unity and $\omega^3 = 1$.

Properties of groups

Properties of groups

Property 1:

The identity of a group is unique (or) If $(G, *)$ is a group and e is an identity of G , then no other element of G is an identity of G .

Proof:

Suppose that e_1 and e_2 are two identities of the group $(G, *)$.

Now e_1 is the identity, then $e_1 * e_2 = e_2 * e_1 = e_2 \rightarrow (1)$

Again e_2 is the identity, then $e_2 * e_1 = e_1 * e_2 = e_1 \rightarrow (2)$

From (1) and (2) we see that $e_1 = e_2$

The identity is unique

Property 2:

In a group , the left and right cancellation laws are true. That $a*b=a*c \Rightarrow b=c$ and $b*a=c*a \Rightarrow b=c$.

Proof:

Let $G=(G, *)$ be a group For $a \in G$, there exists an $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

(i)Left cancellation law:

Let $a*b=a*c$.

$$\begin{aligned} a^{-1}*(a*b) &= a^{-1}*(a*c) \Rightarrow (a^{-1}*a)*b = (a^{-1}*a)*c \\ &\Rightarrow e*b = e*c \Rightarrow b = c. \end{aligned}$$

(ii)Right cancellation law :

$$\Rightarrow \text{Let } b*a = c*a \Rightarrow (b*a)*a^{-1} = (c*a)*a^{-1}$$

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

$$\Rightarrow b*e = c*e \Rightarrow b = c.$$

Property 3:

The inverse of any element of group is unique.

Proof:

Let G be a group, $a \in G$ and e be the identity element of G .

Suppose that b and c be two inverses of an element $a \in G$.

$$b^* a = e = a^* b \quad \text{and} \quad c^* a = e = a^* c.$$

$$\text{Now } (b^* a)^* c = c \Rightarrow b^*(a^* c) = c$$

$$\Rightarrow b^* e = c \Rightarrow b = c$$

There is one and only one inverse for each element in a group.

Property 4:

A group can not have any element which is idempotent expect the identity element

Proof:

Let G be a group. Let us assume that $a \in G$ is idempotent. Then

$$a * a = a.$$

$$\begin{aligned} \text{Now } e &= a^{-1} * a = a^{-1} * (a * a) = (a^{-1} * a) * a \\ &= e * a = a \\ \Rightarrow e &= a \end{aligned}$$

Property 5: If a is an element of group G , then $(a^{-1})^{-1} = a$ (or) If the inverse of a is a^{-1} , then the inverse of a^{-1} is a .

Proof:

If e is the identity of the group G , then

$$a^{-1}*a = e = a*a^{-1}, \text{ for every } a \in G.$$

$$(a^{-1})^{-1} * (a^{-1}*a) = (a^{-1})^{-1} * e = (a^{-1})^{-1}$$

$$\Rightarrow (a^{-1})^{-1} * (a^{-1}*a) = (a^{-1})^{-1}$$

$$\Rightarrow ((a^{-1})^{-1} * a^{-1})*a = (a^{-1})^{-1}$$

$$\Rightarrow e*a = (a^{-1})^{-1}$$

$$\Rightarrow a = (a^{-1})^{-1}$$

Property 6:

If a has inverse b and b has inverse c , then $a=c$.

Proof:

$$\text{Given } a * b = e = b * a \rightarrow (1)$$

$$\text{and } b * c = e = c * b \rightarrow (2)$$

$$a = a * e = a * (b * c)$$

$$= e * c$$

$$= c$$

$$a = c$$

Property 7:

The inverse of the product of two element of a group is the product of their inverse order. That is $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof:

Let $a, b \in G$ and a^{-1}, b^{-1} be their inverse respectively.

$$a * a^{-1} = e = a^{-1} * a \text{ and } b * b^{-1} = e = b^{-1} * b$$

$$\begin{aligned} \text{Now } (a * b) * (b^{-1} * a^{-1}) &= a * [b * (b^{-1} * a^{-1})] \\ &= a * [(b * b^{-1}) * a^{-1}] \\ &= a * [e * a^{-1}] = a * a^{-1} \\ &= e \end{aligned}$$

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

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

We see that $(b^{-1} * a^{-1})$ is the inverse of $(a * b)$

That is $(a * b)^{-1}$ is the inverse of $(a * b)$

$$\text{That is } (a * b)^{-1} = b^{-1} * a^{-1}$$

Property 8:

The existence of a unique inverse of every element of G guarantees the unique solvability of any equation of the type $a^*x = b$ has a unique solution $x = a^{-1}*b$. in addition, the equation $x^*a=b$ has a unique solution $x = b^* a^{-1}$.

Proof:

Let G be a group. Then for any $a, b \in G$,
we have $a^* a^{-1} = e = a^{-1}*a$ and $b^*b^{-1} = e = b^{-1}*b$.

Now

$$\begin{aligned} a^* x &= b = e * b \\ &= (a^* a^{-1})*b \\ &= a^* (a^{-1}*b) \\ \Rightarrow x &= a^{-1}*b \end{aligned}$$

To prove this solution is unique, let us suppose x_1 and x_2 are two solutions of $a^* x = b$.
Then

$$a^* x_1 = b \text{ and } a^* x_2 = b$$

$$a^* x_1 = a^* x_2$$

$$\Rightarrow x_1 = x_2$$

$x = a^{-1}*b$ is the unique solution for $a^* x = b$. similarly we can prove the second part.

Property 9:

A group G is abelian iff $(a * b)^2 = a^2 * b^2$

Proof:

Let us assume that G is abelian. Hence, for $a, b \in G$.

We have $a * b = b * a$

Now

$$\begin{aligned} a^2 * b^2 &= (a * a) * (b * b) \\ &= a * [a * (b * b)] \\ &= a * [(a * b) * b] \\ &= a * [(b * a) * b] \\ &= (a * b) * (a * b) \\ &= (a * b)^2 \end{aligned}$$

$$(a * b)^2 = a^2 * b^2$$

Conversely, assume that $(a * b)^2 = a^2 * b^2$

$$\Rightarrow (a * b) * (a * b) = (a * a) * (b * b)$$

$$\Rightarrow a * [b * (a * b)] = a * [a * (b * b)]$$

$$\Rightarrow b * (a * b) = a * (b * b)$$

$$\Rightarrow (b * a) * b = (a * b) * b$$

$$\Rightarrow b * a = a * b$$

$\Rightarrow G$ is abelian

Property 10:

For any group G, if $a^2 = e$ with $a \neq e$, then G is abelian
(0r)

If every element of group G is its own inverse, then G is abelian. Is the converse also true.

Proof:

Let G be a group and $a, b \in G$, then $a * b \in G$.

Given $a = a^{-1}$ and $b = b^{-1}$

$$\begin{aligned} (a * b) &= (a * b)^{-1} \\ &= b^{-1} * a^{-1} \\ &= b * a \\ \Rightarrow G \text{ is abelian} \end{aligned}$$

Modular Arithmetic

Modular Arithmetic:

- The addition modulo n is defined by $a +_n b = r$, where a, b are integers, n is a +ve integer and r is the least +ve remainder when $(a+b)$ is divided by n .
 $a +_n b$ =the least +ve remainder when $(a+b)$ is divided by n .

Eg: $8 +_5 3 = 11 = 2(5) + 1 = 1$ (Addition mod 5)

$-23 +_7 3 = -20 = -3(7) + 1 = 1$ (Addition mod 7)

The multiplication modulo n is defined by $a \cdot b$ = the least +ve remainder when $(a \cdot b)$ is divided by n .

$$3 \cdot 5 = 15 = 3(4) + 3 = 3$$

$$-5 \cdot 6 = -30 = -8(4) + 2 = 2$$

Properties of Modular Arithmetic on Z_n

Addition modulo n is always commutative and associative. 0 is the identity for $+_n$ and every element of Z_n has an additive inverse .

Multiplication modulo n is always commutative and associative and 1 is identity for \cdot_n . multiplication modulo n is distributive over addition modulo n . also every element of Z_n has the multiplicative inverse.

Example 1:

Prove that $(Z_3, +_3)$ is an abelian group.

Let $Z_3 = \{0, 1, 2\}$, Let us defined the addition table as

$+3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

For $x, y \in Z_3$, define,

$x +_3 y$ = the least +ve remainder , when $(x+y)$ divided by 3,

since all the entries in the addition table are the element of Z_3 , it is closed under $+_3$. Associative, commutative, with identity element 0 and every element of Z_n has an additive inverse , we see that $(Z_3, +_3)$ is an additive abelian group.

Example 2:

Prove that (Z_5, \times_5) is an abelian group.

Solution:

Let $Z_5 = \{1, 2, 3, 4\}$. Let us define the multiplication mod 5 table as

\times_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Since all the entries in the multiplication table are the element of Z_5 , It is closed under \times_5 . Here 1 is the identity. Also from fact that multiplication mod n is always associative, commutative and every element of Z_n has a multiplicative inverse, we see that (Z_5, \times_5) is an abelian group.

Worksheet for BMAT205L

Discrete Mathematics and Graph Theory

Ankush Chanda

August 22, 2023

Problems

1. Show that $\{\mathbb{Z}^+, *\}$ where $*$ is defined by

$$a * b = \max(a, b)$$

for all $a, b \in \mathbb{Z}^+$, is a monoid. What is the identity element? \mathbb{Z}^+ denotes the set of positive integers.

2. Check whether the set \mathbb{Z}_{10} with respect to addition is a group or not.
3. Check whether the set U_{10} with respect to multiplication is a group or not.
4. Check whether the set of matrices $M_2(\mathbb{R})$ with respect to matrix multiplication is a group or not.
5. Show that $\{\mathbb{Z}^+, *\}$, where $*$ is defined by $a * b = a$, for all $a, b \in \mathbb{Z}^+$, is a semigroup. Is it a monoid? \mathbb{Z}^+ denotes the set of positive integers.

6. Show that $\{\mathbb{Z}^+, *\}$ where $*$ is defined by $a * b = \max(a, b)$ for all $a, b \in \mathbb{Z}^+$, is a monoid. What is the identity element? \mathbb{Z}^+ denotes the set of positive integers.
7. Prove that the set $A = \{1, \omega, \omega^2\}$ is an Abelian group of order 3 under multiplication, where $1, \omega, \omega^2$ are cube roots of unity, $1 + \omega + \omega^2 = 0$ and $\omega^3 = 1$.
8. Verify whether $G = \{(a, b) : a, b \text{ are rationals, } a \neq 0\}$ is a group or not under the binary operation $*$ on G defined as $(a, b) * (c, d) = \{(ac, ad + b)\}$. Is it an Abelian group?
9. Show that the set $S = \{1, i, -1, -i\}$, where $i^4 = 1$, is an Abelian group with respect to multiplication or not.



Sub Groups

Definition:

A non-empty subset H of a group G is said to be a subgroup of G if H itself is a group under the same operation defined on G and with the same identity element.

Let $(G, *)$ be a group and $H \subseteq G$ ($H \neq \varnothing$) is said to be subgroup $(H, *)$ of $(G, *)$ if

1. $e \in H$, where e is the identity of G
2. For any $a \in H$, $a^{-1} \in H$
3. For $a, b \in H$, $a * b \in H$.

Example :

1. The set of all integers is a subgroup of the set of all real numbers under addition. That is $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$
2. The set of even integer $2\mathbb{Z} = \{2k | k \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$
3. The set of non-negative integers is not a subgroup of $(\mathbb{Z}, +)$, because, except 0, no element have the additive inverse.

Theorem 1

The necessary and sufficient condition that a non-empty subset H of a group G be a subgroup is $a \in H, b \in H \Rightarrow a * b^{-1} \in H$

Proof

Necessary Conditions:

Assume that H is a subgroup of G. since H itself is a group ; we have $a, b \in H$.
Also $b \in H \Rightarrow b^{-1} \in H$.
 $a, b \in H \Rightarrow a * b^{-1} \in H$

Sufficient Conditions : Let $a * b^{-1} \in H \rightarrow (1)$ for all $a, b \in H$ and $H \subseteq G$. we have to prove that H is a subgroup of G.

For,

Identity : Let $a \in H, a \in H \Rightarrow a * a^{-1} \in H$
 $\Rightarrow e \in H$

Hence the identity e is the element of H

Existence of inverse :

Let $e \in H, a \in H \Rightarrow e * a^{-1} \in H \Rightarrow a^{-1} \in H$
Every element of H has an inverse which is in H.

•Closure :

Let $b \in H \Rightarrow b^{-1} \in H$

For $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} \in H$

$\Rightarrow a * b \in H$

H is closed under the composition.

Associative :

Since $H \subseteq G$, the elements of H are also the elements of G. since the composition in G is associative, it must also be associative in H.

H itself is a group for the composition in G.

H is a subgroup of G.

Theorem 2:

The intersection of two subgroup of a group is also a subgroup of the group (OR) If H_1, H_2 are two subgroup of a group G , then $H_1 \cap H_2$ is also a subgroup of G .

Proof:

Let H_1 and H_2 be any two subgroups of G then $H_1 \cap H_2 \neq \varnothing$, because at least the identity element is common to both H_1 and H_2 .

To prove $H_1 \cap H_2$ is a subgroup , it is enough if we show that, for $a, b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$.

For let $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ and $a, b \in H_2$

$\Rightarrow a * b^{-1} \in H_1$ and $a * b^{-1} \in H_2$

$\Rightarrow a * b^{-1} \in H_1 \cap H_2$

$a, b \in H_1 \cap H_2 \Rightarrow a * b^{-1} \in H_1 \cap H_2$

$\Rightarrow H_1 \cap H_2$ is a subgroup of G

Theorem 3:

The union of two subgroup of G need not be a subgroup of G.

Proof:

To prove these consider the following example. Let G be a group of integers under addition

$(\mathbb{Z}, +) = (G, +)$ is group

Now define $H_1 = \{x \mid x = 2n, n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \dots\}$

$H_2 = \{x \mid x = 3n, n \in \mathbb{Z}\} = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \dots\}$

We see that H_1 and H_2 are subgroup of G.

Define $H_1 \cup H_2 = \{x \mid x \in H_1 \text{ or } x \in H_2\}$
 $= \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \dots\}$

For $2, 9 \in H_1 \cup H_2 \Rightarrow 2+9 = 11 \notin H_1 \cup H_2$

$H_1 \cup H_2$ is not closed under addition

$H_1 \cup H_2$ is not a group

$H_1 \cup H_2$ is not a subgroup of G

Cyclic Groups

Definition:

A group $(G, *)$ is said to be cyclic if there exists $a \in G$ such that any $x \in G$ can be written as either $x = a^n$ or $x = na$, where n is some integer. Here the element ‘ a ’ is called the ‘generator’ of the cyclic group G . That is the cyclic group generated by ‘ a ’ and we denote it by $G = (a)$

Theorem 1:

Every cyclic group is abelian.

Proof:

Let $(G, *)$ be a cyclic group generated by an element $a \in G$. i.e $G = (a)$. Then for any two elements $x, y \in G$, we have $x = a^n, y = a^m$, where m, n are integers.

$$\begin{aligned}x * y &= a^n * a^m = a^{n+m} = a^{m+n} \\&= a^m * a^n \\&= y * x\end{aligned}$$

$(G, *)$ is abelian.

Theorem 2:

If ‘a’ is a generator of a cyclic group G, then a^{-1} is also a generator of G (or). If a is an element of group G, then $(a) = (a^{-1})$.

Proof

Let $G = (a)$ be a cyclic group generated by ‘a’. Then $a^r \in G$, where r is some integer we can write $a^r = (a^{-1})^{-r}$, since $-r$ is also some integer

Each element of G is generated by a^{-1}

a^{-1} is also a generator of G.

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

Theorem 3:

Prove that the group $G = \{1, -1, i, -i\}$ is cyclic and find its generators.

Solution

We can write $1 = (i)^4$, $-1 = (i)^2$, $i = (i)^1$, $-i = (i)^3$

i.e., All the elements of G can be expressed as integral powers of the element i.
G is a cyclic group generated by i.

Since ‘i’ is the generator of G, $(i)^{-1}$ is also a generator of G. Hence G is a cyclic group and its generators are I and $(i)^{-1} = 1/i = -i$

Theorem 4:

Every subgroup of a cyclic group is cyclic

Theorem 5:

Let $(G, *)$ be a finite group generated by an element $a \in G$. If G is of order n , that is $O(G) = n$, then $a^n = e$ so that $G = \{a, a^2, \dots, a^n = e\}$. Further, n is the least positive integer for which $a^n = e$.

Theorem 6:

The direct product of two or more groups is again a group.

Morphism of Group

Definition:

Let $(G, *)$ and (H, Δ) be any two groups. A mapping $f: G \rightarrow H$ is said to be a **homomorphism** if $f(a * b) = f(a) \Delta f(b)$, for any $a, b \in G$.

Theorem 1:

If f is a homomorphism of a group G into a group G' , then

(i) Group homomorphism preserves identities

i.e., $f(e) = e'$, where e is the identity of G and e' is the identity of G'

(ii) (Group homomorphism preserves inverses

i.e., $f(a^{-1}) = [f(a)]^{-1}$, for all $a \in G$.

Proof:

Let $a \in G$ and f is a homomorphism from G into G' , then $f(a) \in G'$

$$\begin{aligned} f(a) * e' &= f(a) = f(a * e) \\ &= f(a) * f(e) \\ \Rightarrow e' &= f(e) \end{aligned}$$

Let $a \in G$, then $a^{-1} \in G$ and $a * a^{-1} = e = a^{-1} * a$

$$\begin{aligned} e' &= f(e) = f(a * a^{-1}) \\ &= f(a) * f(a^{-1}) \\ \Rightarrow f(a) * f(a^{-1}) &= e' \end{aligned}$$

We see that $f(a^{-1})$ is the inverse of $f(a)$ in G'

$$\text{i.e., } [f(a)]^{-1} = f(a^{-1})$$

Theorem 2:

Let f be a homomorphism from G to G' . Let $f(G)$ be the homomorphic image of G into G' is a subgroup of G' .

Proof:

$$\text{Let } f(G) = \{f(x) / x \in G\}$$

Clearly $f(G)$ is a non-empty subset of G' .

Now for any $a' , b' \in f(G)$, we have $f(a) = a'$, $f(b) = b'$, for $a , b \in G$.

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

But $a * b^{-1} \in G \Rightarrow f(a * b^{-1}) \in f(G) \Rightarrow a' * (b')^{-1} \in f(G)$

i.e., For $a' , b' \in f(G) \Rightarrow a' * (b')^{-1} \in f(G)$

$\Rightarrow f(G)$ is a subgroup of G' .

Theorem 3:

Let $f: G \rightarrow G'$ be a group homomorphism and H is a subgroup of G' , then $f^{-1}(H)$ is a subgroup of G .

Proof:

$$\text{Let } f^{-1}(H) = \{ x = f^{-1}(y) \in G \mid f(x) = y \in H \}$$

Since H is a subgroup of G' , the set $f^{-1}(H)$ will be a non-empty subset of G .

Now consider $x_1 = f^{-1}(y_1), x_2 = f^{-1}(y_2) \in f^{-1}(H)$ for any $y_1, y_2 \in H$

With $f(x_1) = y_1$ and $f(x_2) = y_2$.

$$\begin{aligned} \text{Let } x_1, x_2 \in f^{-1}(H) &\Rightarrow f(x_1), f(x_2) \in H \\ &\Rightarrow f(x_1) * [f(x_2)]^{-1} \in H \\ &\Rightarrow f(x_1) * f(x_2^{-1}) \in H \\ &\Rightarrow f(x_1 * x_2^{-1}) \in H \\ &\Rightarrow x_1 * x_2^{-1} \in f^{-1}(H) \end{aligned}$$

$$x_1, x_2 \in f^{-1}(H) \Rightarrow x_1 * x_2^{-1} \in f^{-1}(H)$$

$f^{-1}(H)$ is a subgroup of G .

Kernel of a homomorphism:

Definition:

Let $f: G \rightarrow G'$ be a group homomorphism

The set of elements of G which are mapped into e' , the identity of G' is called the kernel of f and is denoted by $\text{Ker}(f)$

$$\text{i.e., } \text{Ker}(f) = \{ x \in G / f(x) = e' , \text{the identity of } G' \}$$

Theorem:

Proof:

$$\text{Ker } (f) = \{ x \in G / f(x) = e' , \text{the identity of } G' \}$$

Since $f(e) = e'$ is true always, at least $e \in \text{Ker } (f)$

i.e., $\text{Ker}(f)$ is a non-empty subset of G .

Let $a, b \in \text{Ker } (f)$, with $f(a) = e'$ and $f(b) = e'$

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

$$\Rightarrow a * b^{-1} \in \text{Ker } (f)$$

i.e., $a, b \in \text{Ker } (f) \Rightarrow a * b^{-1} \in \text{Ker } (f)$

$\text{Ker } (f)$ is a subgroup of G .

Definition:

A mapping f from a Group G to a group G' is said to be an **Isomorphism** if

- f is a homomorphism i.e. $f(a \cdot b) = f(a) \cdot f(b)$, for any $a, b \in G$
- f is one-one. (injective) i.e. distinct elements of G have different f -image in G' .
- f is onto (surjective) i.e. every element of G' should be the f -image of some elements in G .

Cosets

Definition:

- For any $a \in G$, the set $a * H$ defined by $a * H = \{a * h / h \in H\}$ is called the **Left coset** of H in G determined by the element $a \in G$.
- For any $a \in G$, the set $H * a$ defined by $H * a = \{h * a / h \in H\}$ is called the **Right coset** of H in G determined by the element $a \in G$.

The element $a \in G$ is called the representative element of the left coset $a * H$ and right coset $H * a$

Note

The right or left coset of H in G is not empty.

Since $e \in H$, $e * H = H = H * e$, H itself is right as well as left coset .

$H * a$, $a * H$ are also subsets of G

If G is abelian, then $a * H = H * a$

In all the subsequent discussion in this chapter, aH means $a * H$ and Ha means $H * a$

Example.1

Let $G = \{ 1, a, a^2, a^3 \}$ be a group and $H = \{ 1, a^2 \}$ is a subgroup of G under multiplication. Find all the cosets of H .

Solution:

Let us find the right cosets of H in G .

$$H1 = \{ 1, a^2 \} = H$$

$$Ha = \{ a, a^2 \},$$

$$Ha^2 = \{ a^2, a^4 \} = \{ a^2, 1 \} = H$$

$$Ha^3 = \{ a^3, a^5 \} = \{ a^3, a \} = Ha$$

$$H.1 = H = Ha^2 = \{ 1, a^2 \} \text{ and } Ha = Ha^3 = \{ a, a^3 \}$$

are two distinct right cosets of H in G . Similarly we can find the left cosets of H in G .

Example.2

Find the right cosets of $\{[0],[2]\}$ in the group $(Z_4, +_4)$.

Solution

Let $Z_4 = \{[0],[1],[2],[3]\}$ be a group and $H = \{[0],[2]\}$ be a subgroup of Z_4 under $+_4$ (addition mode 4).

The left cosets of H are

$$[0] + H = \{[0],[2]\} = H ;$$

$$[1] + H = \{[1],[3]\} ;$$

$$[2] + H = \{[2],[4]\} = \{[2],[0]\} = \{[0],[2]\} = H$$

$$[3] + H = \{[3],[5]\} = \{[3],[1]\} = \{[1],[3]\} = [1] + H.$$

$[0]+H = [2]+H = H$ and $[1]+H = [3]+H$ are the two distinct left cosets of H in Z_4 .

Note:

The union of all distinct left cosets of H in G is equal to G .

If H any subgroup of G and $a \in H$, then $Ha = H = aH$.

Theorem1:

If $a \in Hb$ then $Ha = Hb$ and if $a \in Hb$, then $aH = bH$.

Theorem2:

Any two right cosets of H in G are either disjoint or identical.

Definition:

A subgroup $(H, *)$ of group $(G, *)$ is said to be a **normal subgroup** of G , if for every $x \in G$ and for every $h \in H$, $xhx^{-1} \in H$ $xHx^{-1} = H$.

Theorem1:

A subgroup H of a group G is normal iff $xHx^{-1} = H$

Proof:

Let $xHx^{-1} = H \Rightarrow xHx^{-1} \subseteq H$, for all $x \in G$

$\Rightarrow H$ is a normal subgroup of G

Conversely,

assume that H is a normal subgroup of G , then $xHx^{-1} = H$, for all $x \in G \rightarrow (1)$

Now $x \in G \Rightarrow x^{-1} \in G$, then

$x^{-1}H(x^{-1})^{-1} = H$, for all $x \in G$

$\Rightarrow x^{-1}Hx \subseteq H \Rightarrow x(x^{-1}Hx) x^{-1} \subseteq xHx^{-1}$

$\Rightarrow x^{-1}xHx x^{-1} \subseteq xHx^{-1} \Rightarrow e \in H \text{ and } xHx^{-1}$

$\Rightarrow H = xHx^{-1}$, for all $x \in G \rightarrow (2)$

From (1) and (2)

$xHx^{-1} = H$, for all $x \in G$.

Definition:

Let $(H, *)$ be a subgroup of the group $(G, *)$. We define the congruency relation on G called a left cosets relation with respect to the subgroup H or a left cosets relation mod H denoted by $+$ such that for $a, b \in G$, **a is congruent to b mod H** written $a+b \pmod{H}$ iff $b^{-1} * a \in H$.

Theorem1:

The left cosets relation mode H on $(G, *)$ defined by, for $a, b \in G$, $a+b \pmod{H}$ iff $b^{-1} * a \in H$ is an equivalence relation.

Theorem2:

Let $(H, *)$ be a subgroup of $(G, *)$. The set of left cosets of H in G forms a partition of G .

Theorem3:

If $(H, *)$ is a subgroup of a group $(G, *)$ and right cosets of H in G , then there exists a one-to-one correspondence between the elements of H and Ha (or)

$$O(H) = O(Ha).$$

Note:

There is a one-to-one correspondence between H and aH .

$$O(H) = O(aH)$$

Lagrange's therom

Theorem1:

The order of each subgroup of a finite group is a divisor of the order of the group.

Proof:

Let $(G, *)$ be finite group and $O(G) = n$. Let $(H, *)$ be a subgroup of $(G, *)$ and $O(H) = m$

Suppose that $h_1, h_2, h_3, \dots, h_m$ are the m members of H . For $a \in G$, the right coset Ha of H in G is defined by

$$Ha = \{h_1 * a, h_2 * a, h_3 * a, \dots, h_m * a\}$$

Since there should be a one-to-one correspondence between H and Ha , the members of Ha are distinct.

Hence each right coset of H in G has m distinct members.

We know that any right cosets of H in G are either disjoint or identical. Since G is a finite group, the number of distinct right cosets of H in G will be finite, The union of these k distinct right cosets of H in G is equal to G .

Hence, if $Ha_1, Ha_2, Ha_3, \dots, Ha_k$ are the k distinct right cosets of H in G , then

$$G = Ha_1 \cup Ha_2 \cup H(a_3 \cup \dots \cup Ha_k)$$

$$O(G) = O(Ha_1) + O(Ha_2) + O(Ha_3) + \dots + O(Ha_k)$$

$$n = m + m + m + \dots + m \\ \text{(k times)}$$

$n = km \Rightarrow n/m = k \Rightarrow m$ is a divisor of n
 $\Rightarrow O(H)$ is divisor of $O(G)$
 $\Rightarrow O(H)$ divides $O(G)$.

Hence proof.

Note

- The converse of the Lagrange thermo is not true. That is, if m is a divisor of n , then it is not necessary that G must have a subgroup of order m . For example, the alternating group A_4 of degree 4 is of order 12. But there is no subgroup of A_4 of order 6, though 6 is a divisor of 12
- It is evident from Lagrange's theorem that if G is a finite group of order n and if m is not a divisor of n , then can be no subgroup of G of order m .

Worksheet-III for BMAT205L

Discrete Mathematics and Graph Theory

Ankush Chanda

September 1, 2023

1. Examine φ is a homomorphism or not, where $\varphi : G \rightarrow G$ such that $G = (\mathbb{Z}, +)$ and φ is defined by

$$\varphi(x) = x + 1, \quad x \in G.$$

2. Let $G = (\mathbb{Z}, +)$ and $G' = (\mathbb{Z}_n, +)$ and $\varphi : G \rightarrow G'$ be defined by $\varphi(m) = \overline{m}$, $m \in \mathbb{Z}$, where \overline{m} is the remainder of m ($\text{mod } n$). Examine φ is a homomorphism.
3. Check whether the set $S = \{1, i, -1, -i\}$ with respect to multiplication is a group or not. Explain if the group is a cyclic group. If yes, find a generator of the group.
4. Consider the set H of all real matrices

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \right\}.$$

Prove that H is a subgroup of the group $GL_2(\mathbb{R})$.

5. Consider $G = (\mathbb{Z}_{15}, +)$ and $H = \langle 5 \rangle$. Find all the right cosets of H in G .

INTRODUCTION TO CODING THEORY

- The process of communication involves transmitting some information carrying signal(message) that is conveyed by a sender to a receiver.
- Even though the sender may like to have his message received by the receiver without any distortion ,it is not possible due to a variety of disturbances(noise) to which the communication channel is subjected.
- Coding theory deals with minimizing the distortions of the conveyed message due to noise and to retrieve the original message to the optimal extent possible from the corrupted message.

The communication model: A communication process may take place in a variety of ways, e.g., by making a telephone call, sending a message by a telegram or a letter, using a sign language, etc.,

An ideal communication system can be represented by atleast three essential parts:

1. Transmitter, sender or source
2. Channel or storage medium
3. Receiver

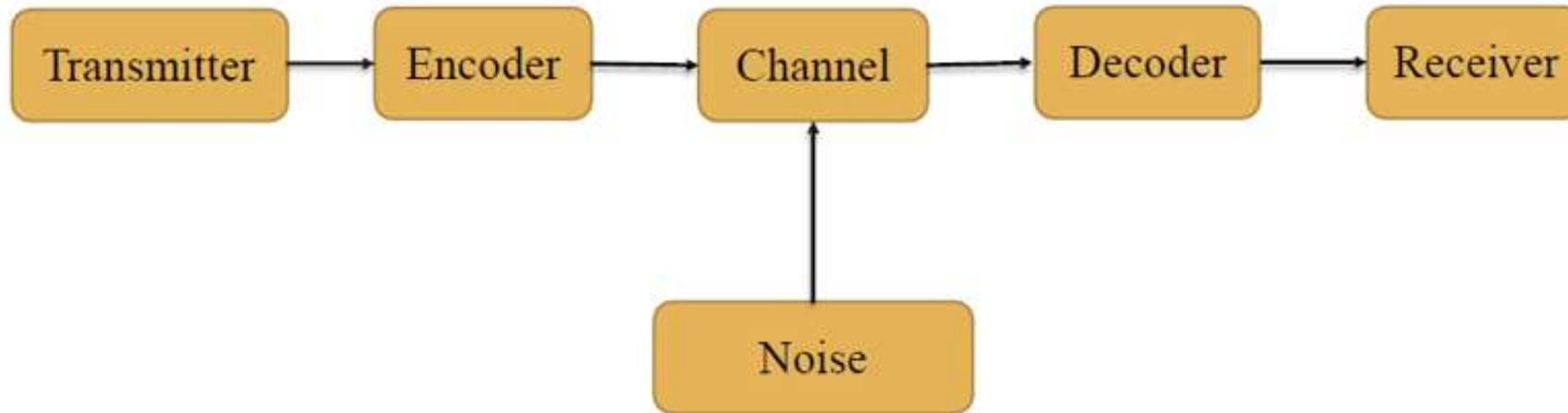
The communication channel is subjected to variety of disturbances which results in a distortion of the commodity being transmitted. Any such disturbance is called noise.

The form in which noise may appear depends on the channel. For ex. In a conversation between two individuals, the channel can be subjected to noises, such as wind, a passing car, other voices, etc., On the other hand these noises may not affect a radio transmission.

Encoder: A device that can be used to improve the efficiency of the communication channel is called an encoder. It transform the incoming message in such a way that the presence of noise on the transformed message is detectable.

Decoder: A decoder is used to transform the encoded message into their original form that is acceptable to the receiver

The following diagram provides a rough idea of a general information transmission system.



The encoding or enciphering process is a procedure for associating words from one language with given words of another language in one-to-one fashion. Similarly, the decoding or deciphering process is either the inverse operation or some other one-to-one mapping.

Binary Channel:

In most applications the communication channel is restricted to binary valued alphabet, whose signals may be designated by 0 and 1, such a channel is called a binary channel.

Here, we are interested in the transmission of binary string (binary string over $\{0,1\}$).

Let us choose the alphabet in the set $B = \{0, 1\}$. Now every character which we want to transmit is represented by m elements (say) from B .

Let $B^n = B \times B \times B \times \dots \times B$ (n factors), then $B^n = \{x_1, x_2, x_3, \dots, x_n : x_i \in B\}$ will form a group under the binary operation addition modulo 2 (denoted by \oplus).

Theorem: Prove that (B^n, \oplus) is an abelian group.

Hamming Codes:

The codes obtained by introducing additional digits called parity digits to the digits in the original message are called hamming codes.

- If the original message is a binary string of length m then hamming encoded message is a binary string of length n . ($n > m$)
- Out of n digits, m digits are used to represent information part of message and rest $(n - m)$ digits are used to detection and correction of errors in received message.
- In Hamming's single-error detection code of length n , the first $(n - 1)$ digits contains information part of the message and last digit is made either 0 or 1.

Even and Odd Parity Check:

If the digit introduced in the last position gives an even number of 1's in the encoded word, the extra digit is called **even parity check**.

If the digit introduced in the last position gives an odd number of 1's in the encoded word, the extra digit is called **odd parity check**.

EXAMPLE OF PARITY CHECK

Code before parity check	Code after even parity check	Code after odd parity check
000	0000	0001
001	0011	0010
010	0101	0100
011	0110	0111
100	1001	1000
101	1010	1011
110	1100	1101
111	1111	1110

Weight of binary string:

The number of 1's in binary string $x \in B^n$, is called the weight of x and denoted by $|x|$.

Example: Find the weight of (i) 10010, (ii) 1111, (iii) 10110

$$|10010|=2$$

$$|1111|=4$$

$$|10110|=3$$

Hamming distance:

Suppose if x and y represents binary strings $x_1x_2x_3 \dots x_n$ and $y_1y_2y_3 \dots y_n$ then the number of positions in the strings for which $x_i \neq y_i$ is called **Hamming Distance** between x and y .

Denoted by $H(x,y)$

$$H(x,y) = \text{weight of } x \oplus y = |x \oplus y|$$

Example: Let $x = 1011, y = 0101$, then

$$H(x,y) = |1011 \oplus 0101| = |1110| = 3$$

Minimum Distance of a code:

The minimum distance of a code, whose words are n tuples, is the minimum of the Hamming distances between all pairs of code.

Ex: Find the minimum distance of a code $x = 10110$, $y = 11110$, $z = 10011$

$$H(x, y) = 1,$$

$$H(y, z) = 3,$$

$$H(z, x) = 2$$

Minimum distance 1.

Encoding Function: The one-one function $e: B^m \rightarrow B^n$ is called (m, n) encoding function, where $n > m$.

If $x = (x_1 x_2 x_3 \dots \dots x_n) \in B^m$ is the original word, then $e(x)$ is called the code word representing x .

Group Code:

An (m, n) encoding function $e: B^m \rightarrow B^n$ is called a group code if the range of e is $e(B^m) = \{e(x): x \in B^m\}$ is a subgroup of B^n .

Parity check code

A function $e : B^m \rightarrow B^{m+1}$ defined by

$$e(b_1, b_2, \dots, b_m) = b_1 b_2 \dots b_m b_{m+1}$$

where $b_{m+1} = \begin{cases} 0, & \text{if } |b| \text{ is even} \\ 1, & \text{if } |b| \text{ is odd} \end{cases}$

is an encoding function. (e has to be one-to-one) This function is called parity $(m, m + 1)$ check code.

Note that $|e(b)|$ is always even.

Ex: Consider (3,6) encoding function $e: B^3 \rightarrow B^6$ defined by

$x \in B^3$	Code word $e(x) \in B^6$
000	000000
001	001100
010	010011
011	011111
100	100101
101	101001
110	110110
111	111010

Show that this encoding function is group code.

Example. Show that the $(2, 5)$ encoding function defined by

$$e(00) = 00000 \quad e(01) = 01110$$

$$e(10) = 10101 \quad e(11) = 11011$$
 is a group code.

Solution : Denote $e(00), e(01), e(10), e(11)$ by x^0, x^1, x^2, x^3 . The set of these code words is closed under \oplus as can be seen from the table

	x^0	x^1	x^2	x^3
x^0	x^0	x^1	x^2	x^3
x^1	x^1	x^0	x^3	x^2
x^2	x^2	x^3	x^0	x^1
x^3	x^3	x^2	x^1	x^0

As the code x^0 is the identity element and the inverse of any element is itself, the code words form a subgroup of B^5 . Hence e is a group code.

Theorem 1:

A code [**(m, n) encoding function**] can detect at most k errors iff the minimum distance between any two code word is at least $(k + 1)$.

Theorem 2:

A code [**(m, n) encoding function**] can correct at most k errors iff the minimum distance between any two code word is at least $(2k + 1)$.

Example: Let $e: B^2 \rightarrow B^6$ defined by $e(00) = 000000, e(01) = 011110,$
 $e(10) = 101010, e(11) = 111000$. How many errors e can detect?

Solution:

Let $x_1 = 000000, x_2 = 011110, x_3 = 101010, x_4 = 111000$

Now $|x_1 \oplus x_2| = 4, |x_1 \oplus x_3| = 3$

$|x_1 \oplus x_n| = 3 |x_2 \oplus x_3| = 3 |x_2 \oplus x_4| = 3 |x_3 \oplus x_4| = 2$

The minimum distance is 2.

By the previous theorem, a code can detect k or fewer errors if and only if the minimum distance between any two code word is at least $(k + 1)$.

Here the minimum distance is 2, therefore

$$2 \geq k + 1 \text{ i.e., } k \leq 1.$$

Hence the code can detect only one error.

Parity check and Generator matrix:

Generator Matrix:

- For the (m, n) encoding function $e: B^m \rightarrow B^n$, the corresponding matrix is defined by $G_{m \times n}$, called generator matrix for the code.

$G_{m \times n}$ is of the form $[I_m | A]$, where I_m is the identity matrix of order $m \times m$ and A is $m \times (n - m)$ matrix to be chosen suitably.

If w be a message $\in B^m$, then $e(w) = w G$ and the code $C = e(B^m) \subseteq B^n$ where w is a $(1 \times m)$ vector.

Parity check matrix:

- $H = [A^T | I_{n-m}]$ is the parity check matrix of order $(n \times n - m)$.

Example : Find the code word generated by a parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ when the encoding function is } e: B^3 \rightarrow B^6.$$

Solution: $H = [A^T | I_{n-m}]$ is the parity check matrix.

$G = [I_m | A]$ is the generator matrix.

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [A^T | I_3]$$

i.e. $A^T = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

Generator matrix $G = [I_3 | A]$

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

Now $B^3 = \{000, 100, 010, 001, 110, 011, 101, 111\}$, and $e(w) = w G$

$$e(000) = [000]G = [000] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 0\ 0\ 0\ 0\ 0]$$

$$e(001) = [001] \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [0\ 0\ 1\ 0\ 1\ 1]$$

$$e(0\ 1\ 0) = [0\ 1\ 0]G = [0\ 1\ 0\ 1\ 0\ 1]$$

$$e(1\ 0\ 0) = [1\ 0\ 0]G = [1\ 0\ 0\ 1\ 1\ 1]$$

$$e(0\ 1\ 1) = [0\ 1\ 1]G = [0\ 1\ 1\ 1\ 1\ 0]$$

$$e(1\ 0\ 1) = [1\ 0\ 1]G = [1\ 0\ 1\ 1\ 0\ 0]$$

$$e(1\ 1\ 0) = [1\ 1\ 0]G = [1\ 1\ 0\ 0\ 1\ 0]$$

$$e(1\ 1\ 1) = [1\ 1\ 1]G = [1\ 1\ 1\ 0\ 0\ 1]$$

The generated code words are

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{matrix},$$

$$\begin{matrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{matrix},$$

$$\begin{matrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{matrix},$$

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 & 0 \end{matrix},$$

Example: Find the code word generated by a parity check matrix

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ when the encoding function is } e: B^2 \rightarrow B^5.$$

Solution: $B^2 = \{00, 10, 01, 11\}$

Here $H = [A^T \mid I_3]$ is the parity check matrix.

$G = [I_2 \mid A]$ is the generator matrix.

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

$$A^T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ i.e. } A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

Now, Generator matrix $G = [I_2 \mid A]$

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

Using G code can be generated as:

$$e(w) = w G \text{ where } w \in B^2$$

$$e(0\ 0) = (0\ 0)G = (0\ 0) \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = (0\ 0\ 0\ 0\ 0)$$

$$e(0\ 1) = (0\ 1)G = (1\ 0\ 1\ 1\ 0)$$

$$e(1\ 0) = (1\ 0)G = (0\ 1\ 0\ 1\ 1)$$

$$e(1\ 1) = (1\ 1)G = (1\ 1\ 1\ 0\ 1)$$

Example: Decode each of the following received words corresponding to the encoding function $e: B^3 \rightarrow B^6$, given by

$e(0\ 0\ 0) = 0\ 0\ 0\ 0\ 0\ 0$, $e(0\ 0\ 1) = 0\ 0\ 1\ 0\ 1\ 1$, $e(1\ 0\ 0) = 1\ 0\ 0\ 1\ 1\ 1$,
 $e(0\ 1\ 0) = 0\ 1\ 0\ 1\ 0\ 1$, $e(0\ 1\ 1) = 0\ 1\ 1\ 1\ 1\ 0$, $e(1\ 0\ 1) = 1\ 0\ 1\ 1\ 0\ 0$,
 $e(1\ 1\ 0) = 1\ 1\ 0\ 0\ 1\ 0$, $e(1\ 1\ 1) = 1\ 1\ 1\ 0\ 1\ 1$, assuming that no or single
error has been occurred.

0 1 1 1 1 0, 1 1 0 1 1 1, 1 1 0 0 0 0, 1 1 1 0 0 0, 0 1 1 1 1 1

Solution: The minimum distance between the code words is 3 and hence at most 1 error can be corrected that might have occurred in received words.

- The word 0 1 1 1 1 0 is identical with $e(0\ 1\ 1)$. Hence no error occurred in this word. i.e original message is 0 1 1.

The word 1 1 0 1 1 1 differs from $e(1\ 0\ 0)=1\ 0\ 0\ 1\ 1\ 1$ in the second position only. Correcting this error the transmitted word is 1 0 0 1 1 1 and original message is 1 0 0.

- The word 1 1 0 0 0 0 differs from $e(1\ 1\ 0)=1\ 1\ 0\ 0\ 1\ 0$ at the fifth position only. Correcting this error the transmitted word is 1 1 0 0 1 0 and original message is 1 1 0.
- The word 1 1 1 0 0 0 differs from $e(1\ 1\ 1)=1\ 1\ 1\ 0\ 0\ 1$ at the sixth position only. Correcting this error the transmitted word is 1 1 1 0 0 1 and original message is 1 1 1

The word 0 1 1 1 1 1 differs from $e(0\ 1\ 1)=0\ 1\ 1\ 1\ 1\ 0$ at the sixth position only. Correcting this error the transmitted word is 0 1 1 1 1 0 and original message is 0 1 1

Example Given the generator matrix $G \equiv \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$

corresponding to the encoding function $e: B^3 \rightarrow B^6$, find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message. Are all the words decoded uniquely?

- (i) 1 1 0 1 0 1, (ii) 0 0 1 1 1 1, (iii) 1 1 0 0 0 1, (iv) 1 1 1 1 1 1

If we assume that $G = [I_3 | A]$, then

$$H = [A^T | I_3] = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We compute the *syndrome* of each of the received word by using $H \cdot [r]^T$.

$$(i) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Since, $H \cdot [e(w)]^T = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, the received word in this case is the transmitted

(encoded) word itself. Hence, the original message is 1 1 0.

$$(ii) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Since, the syndrome $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is the same as the fifth column of H , the element in the fifth position of r is changed.
 \therefore The decoded word is $0 \ 0 \ 1 \ 1 \ 0 \ 1$ and the original message is $0 \ 0 \ 1$.

$$(iii) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Since, the syndrome $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ is the same as the fourth column of H , the

fourth component of r is changed to get the decoded word. It is
 $1 \ 1 \ 0 \ 1 \ 0 \ 1$ and the original message is $1 \ 1 \ 0$.

$$(iv) H \cdot [r]^T = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Since, the syndrome is not identical with any column of H , the received word cannot be decoded uniquely.

Example Construct the decoding table for the group code given by the generator matrix.

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

Decode the following received words using the decoding table obtained. Which of the words could not be decoded uniquely?

1 0 1 1 1 1, 0 1 1 0 1 0, 1 0 1 1 1 0, 1 1 1 1 1 1.

Now, $B^3 = \{000, 001, 010, 100, 011, 101, 110, 111\}$
 $e(000) = [000]G = [00000];$

Similarly $e(001) = [001011]; e(010) = [010101]$
 $e(100) = [100111]; e(011) = [011110];$
 $e(101) = [101100]; e(110) = [110010]$
and $e(111) = [111001].$

We form the decoding table by making these encoded words as the elements of the first row and the coset leaders as the elements of the first column. The coset leaders with only one 1 have been taken in a certain order and then those with two 1's have been taken. The decoding table is given in Table

Table

Code words →

000000	001011	010101	100111	011110	101100	110010	111001
100000	101011	110101	000111	111110	001100	010010	011001
010000	011011	000101	110111	001110	111100	100010	101001
001000	000011	011101	101111	010110	100100	111010	110001
000100	001111	010001	100011	011010	101000	110110	111101
000010	001001	010111	100101	011100	101110	110000	111011
000001	001010	010100	100110	011111	101101	110011	111000
011000	010011	001101	111111	000110	110100	101010	100001



Coset leaders

The decoding table is not unique as the coset leader of the last row could have been taken as 1 0 0 0 0 1 or 0 0 0 1 1 0.

Decoding of the received words

- (i) 101 111 appears in the 4th row and 4th column. The coset leader of the 4th row is 001 000, which contains only one 1,

Since the minimum weight of the code words is 3, atmost one error can be corrected in the received word.

The corrected (received) word, viz., the code word transmitted is the top element of the 4th column. It is 100 111 and hence the original message is 100.

- (ii) 0 1 1 0 1 0 appears in the 5th row and 5th column. Hence the corresponding code word transmitted is 0 1 1 1 1 0 and hence the original message is 0 1 1.

- (iii) 1 0 1 1 1 0 appears in the 6th row and 6th column. Hence the corresponding code word transmitted is 1 0 1 1 0 0 and hence the original message is 1 0 1.
- (iv) 1 1 1 1 1 1 appears in the 8th row, the coset leader of which contains two 1's viz., the received word contains 2 errors. Hence, they cannot be corrected and the code word transmitted cannot be uniquely determined.

INTRODUCTION TO CODING THEORY

- The process of communication involves transmitting some information carrying signal(message) that is conveyed by a sender to a receiver.
- Even though the sender may like to have his message received by the receiver without any distortion, it is not possible due to a variety of disturbances(noise) to which the communication channel is subjected.
- Coding theory deals with minimizing the distortions of the conveyed message due to noise and to retrieve the original message to the optimal extent possible from the corrupted message.

ENCODERS AND DECODERS

Encoder:

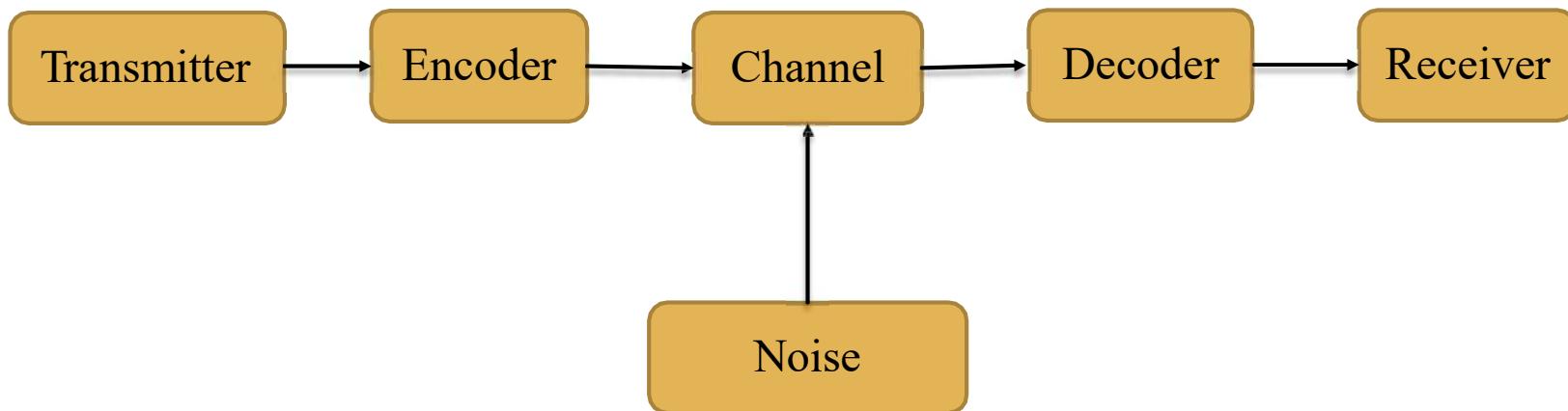
An encoder is a device which transforms the incoming messages in such a way that the presence of noise in the transformed messages is detectable.

Decoder:

A decoder is a device which transforms the encoded message into their original form that can be understood by the receiver.

- So, by using a suitable encoder and decoder, it may be possible to detect the distortions in the messages due to noise in the channel and to correct them.

TYPICAL DATA COMMUNICATION MODEL WITH NOISE



EXPLANATION

- The input message can consist of a sequence of letters, characters or symbol set called alphabet.
- The input message will be transformed by the encoder into a string of characters or symbols of another alphabet in a one-to-one fashion.
- We will discuss a binary channel in which the encoder will transform an input message into a binary string consisting of the symbols 0 and 1.
- Decoding can be seen as the inverse operation of encoding.

GROUP CODE

Definition:

If $B = \{0,1\}$ then $B^n = \{x_1, x_2, x_3, \dots, x_n \mid x_i \in B, i=1,2,3, \dots n\}$ is a group under the binary operation of addition modulo 2 (denoted by \oplus), then (B^n, \oplus) is called a **group code**.

HAMMING CODES

Definition:

- The codes obtained by introducing additional digits called *parity digits* to the digits in the original message are called **hamming codes**.

In Hamming's single-error detecting code, the last digit is made either 0 or 1 and the remaining digits contain the information part of the message.

If the digit introduced in the last position gives an even number/odd number of 1's in the encoded word, the extra digit is called an even/ odd **parity check**.

EXAMPLE OF PARITY CHECK

Code before parity check	Code after even parity check	Code after odd parity check
000	0000	0001
001	0011	0010
010	0101	0100
011	0110	0111
100	1001	1000
101	1010	1011
110	1100	1101
111	1111	1110

HAMMING DISTANCE

Definition:

- Suppose if x and y represents binary strings $x_1x_2x_3 \dots x_n$ and $y_1y_2y_3 \dots y_n$ then the number of positions in the strings for which $x_i \neq y_i$ is called **Hamming Distance** between x and y .
- Denoted by $H(x,y)$

$$H(x,y) = \text{weight of } x \oplus y = |x \oplus y|$$



The number of 1's in the binary string

BASIC NOTATIONS OF ERRORS CORRECTION USING MATRICES

- Where $m, n \in \mathbb{Z}^+$, ($m < n$) { m should be strictly less than n }, the coding function $e: B^m \rightarrow B^n$ [Where $B = \{0,1\}$] is given by a mxn matrix G over B .
- The matrix G is called as generator matrix for the code and is of the form $[I_m | A]$ where I_m is the mxn unit matrix and A is an $m*(n-m)$ matrix chosen suitably.

$$H = [A^T | I_{n-m}]$$

- If w is a message $\in B^m$ then $e(w) = wG$ and the code (the set of code words) $c = e(B^m) \subseteq B^n$, where w is a $(1xm)$ vector.

EXAMPLE

- Let $w \in B^2$ and G is $\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$
- The words belonging to B^2 are $00, 01, 10, 11$. Then we have the code words as:

$$e(00) = [0 \ 0] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [00 \ 000]$$

$$e(10) = [1 \ 0] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [10 \ 110]$$

$$e(01) = [0 \ 1] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [01 \ 011]$$

$$e(11) = [1 \ 1] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} = [111 \ 01]$$

- Question. Find the code words generated by the encoding function $e: B^m \rightarrow B^n$ with respect to the parity check matrix given by

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

Note: In our discussion, if the encoding function is $e: B^m \rightarrow B^n$, the generator matrix was assumed as an $m \times n$ matrix $G = [I_m | A]$ and the parity check matrix was assumed as an $(n - m) \times m$ matrix $H = [A^T | I_{n-m}]$ and as such there was less number of rows and more number of columns in H. We shall stick to our notation. As per our notation, what is given in this problem is not H, but H^T . However some authors use this notation to denote the parity check matrix.

Solution: Let $e = B^m \rightarrow B^n$ where $m < n$ be the encoding function.

Here $n = 5$ and $m = 2$.

Hence, the generator matrix G is given by

$$G = [I_m | A] = \left[\begin{array}{cc|cc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right]$$

Now $B^2 \equiv \{0\ 0, 0\ 1, 1\ 0, 1\ 1\}$ and $e(w) = w \ G$

$$\therefore e(0\ 0) = [0\ 0] \left[\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [0\ 0\ 0\ 0\ 0]$$

$$\therefore e(0\ 1) = [0\ 1] \left[\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [0\ 1\ 0\ 1\ 1]$$

$$\therefore e(1\ 0) = [1\ 0] \left[\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [1\ 0\ 0\ 1\ 1]$$

$$\therefore e(1\ 1) = [1\ 1] \left[\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{array} \right] = [1\ 1\ 0\ 0\ 0]$$

Hence, the code words generated by H are $0\ 0\ 0\ 0\ 0, 0\ 1\ 0\ 1\ 1, 1\ 0\ 0\ 1\ 1$ and $1\ 1\ 0\ 0\ 0$.

- Question. Find the code words generated by the parity check matrix given by

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

when the encoding function is $e: B^3 \rightarrow B^6$.

Solution:

Let $e : B^m \rightarrow B^n$ where $m < n$ be the encoding function. Here, $m=3$ and $n = 6$

$G = [I_m | A]$ be the generated matrix, So, we have

$$G = [I_m | A] = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{array} \right]$$

Now, $B^3 = \{000, 001, 010, 100, 101, 110, 111\}$

From $e(w) = wG$ we have :

∴

$$e(0 \ 0 \ 0) = [0 \ 0 \ 0] \cdot G = [0 \ 0 \ 0 \ 0 \ 0 \ 0]$$

$$e(0 \ 0 \ 1) = [0 \ 0 \ 1] \cdot G = [0 \ 0 \ 1 \ 0 \ 1 \ 1]$$

$$e(0 \ 1 \ 0) = [0 \ 1 \ 0] \cdot G = [0 \ 1 \ 0 \ 1 \ 0 \ 1]$$

$$e(1 \ 0 \ 0) = [1 \ 0 \ 0] \cdot G = [1 \ 0 \ 0 \ 1 \ 1 \ 1]$$

$$e(0 \ 1 \ 1) = [0 \ 1 \ 1] \cdot G = [0 \ 1 \ 1 \ 1 \ 1 \ 0]$$

$$e(1 \ 0 \ 1) = [1 \ 0 \ 1] \cdot G = [1 \ 0 \ 1 \ 1 \ 0 \ 0]$$

$$e(1 \ 1 \ 0) = [1 \ 1 \ 0] \cdot G = [1 \ 1 \ 0 \ 0 \ 1 \ 0]$$

$$e(1 \ 1 \ 1) = [1 \ 1 \ 1] \cdot G = [1 \ 1 \ 1 \ 0 \ 0 \ 1]$$

Thus, the code words generated are 0 0 0 0 0, 0 0 1 0 1 1,
0 1 0 1 0 1, 1 0 0 1 1 1, 0 1 1 1 1 0, 1 0 1 1 0 0, 1 1 0 0 1 0
and 1 1 1 0 0 1.

PARITY CHECK MATRIX

- Parity check matrix is used for decoding at receiver.
- Parity check matrix is denoted by H
- $H = [A^T \mid I_{n-k}]$
- Where A is same parity bits matrix that is used to construct G (generator matrix) for encode and I is identity matrix.

ERROR DETECTION USING PARITY CHECK MATRIX

Given, r : which is received word

H : unique parity check matrix which corrects the single error in transmission.

Three cases:

$$1. H \cdot r^t = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

There is no error in transition and r is the code word transmitted.

ERROR DETECTION USING PARITY CHECK MATRIX

2. If $H \cdot r^t =$ ith column of H, then we conclude that there is a single error in r during transmission and it has occurred in the ith component of r. Changing the ith component of r, we get the code word c.

$$H \cdot r^t = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

ERROR DETECTION USING PARITY CHECK MATRIX

3. If neither case (i) nor case (ii) occurs we conclude that more than one transmission error have occurred. Detection is possible in this case but correction is not possible.

$H \cdot r^t$ is not equal to any column of H

$$H \cdot r^t = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

PRACTICE QUESTIONS

Q1. Given the generator matrix, G=

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

Corresponding to the encoding function, $e: B^3 \rightarrow B^6$, find the corresponding parity check matrix and use it to decode the following received words and hence, to find the original message. Are all words decoded uniquely?

- (i) 110101 (ii) 001111 (iii) 111111

PRACTICE QUESTIONS

solution : we assume $G = [I_3 | A]$

$$\text{Then, } H = [A^T | I_3] \quad H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$(i) H \cdot r^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Since it is 0, the received word in this case is
the transmitted word itself. Original message is
110.

PRACTICE QUESTIONS

(ii)

$$H \cdot r^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

Since $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is the fifth column of H, the element in the fifth position of r is changed.

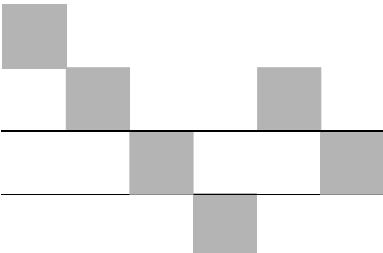
The decoded word is 001101 and original message is 001.

PRACTICE QUESTIONS

(iii)

$$H \cdot r^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Since, the syndrome is not identical with any column of H , the received word cannot be decoded uniquely.



Chapter 2

Combinatorics

INTRODUCTION

Combinatorics is an important part of discrete mathematics that solves counting problems without actually enumerating all possible cases. More specifically, combinatorics deals with counting the number of ways of arranging or choosing objects from a finite set according to certain specified rules. In other words, combinatorics is concerned with problems of permutations and combinations, which the students have studied in some detail in lower classes.

As combinatorics has wide applications in Computer Science, especially in such areas as coding theory, analysis of algorithms and probability theory, we shall briefly first review the notions of permutations and combinations and then deal with other related concepts.

PERMUTATIONS AND COMBINATIONS

Definitions

An ordered arrangement of r elements of a set containing n distinct elements is called an *r -permutation of n elements* and is denoted by $P(n, r)$ or ${}^n P_r$, where $r \leq n$. An unordered selection of r elements of a set containing n distinct elements is called an *r -Combination of n elements* and is denoted by $C(n, r)$ or ${}^n C_r$ or $\binom{n}{r}$.

Note A permutation of objects involves ordering whereas a combination does not take ordering into account.

Values of $P(n, r)$ and $C(n, r)$

The first element of the permutation can be selected from a set having n elements in n ways. Having selected the first element for the first position of

the permutation, the second element can be selected in $(n - 1)$ ways, as there are $(n - 1)$ elements left in the set.

Similarly, there are $(n - 2)$ ways of selecting the third element and so on. Finally there are $n - (r - 1) = n - r + 1$ ways of selecting the r^{th} element. Consequently, by the product rule (stated as follows), there are

$$n(n - 1)(n - 2) \dots (n - r + 1)$$

ways of ordered arrangement of r elements of the given set.

Thus,

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

In particular, $P(n, n) = n!$

Product Rule

If an activity can be performed in r successive steps and step 1 can be done in n_1 ways, step 2 can be done in n_2 ways, ..., step r can be done in n_r ways, then the activity can be done in $(n_1 \cdot n_2 \dots n_r)$ ways.

The r -permutations of the set can be obtained by first forming the $C(n, r)$ r -combinations of the set and then arranging (ordering) the elements in each r -combination, which can be done in $P(r, r)$ ways. Thus

$$\begin{aligned} P(n, r) &= C(n, r) \cdot P(r, r) \\ \therefore C(n, r) &= \frac{P(n, r)}{P(r, r)} = \frac{n!/(n-r)!}{r!/(r-r)!} \\ &= \frac{n!}{r!(n-r)!} \end{aligned}$$

In particular, $C(n, n) = 1$.

Note

Since the number of ways of selecting out r elements from a set of n elements is the same as the number of ways of leaving $(n - r)$ elements in the set, it follows that

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

This is obvious otherwise, as

$$\begin{aligned} C(n, n - r) &= \frac{n!}{(n - r)! \{n - (n - r)\}!} \\ &= \frac{n!}{(n - r)! r!} = C(n, r) \end{aligned}$$

PASCAL'S IDENTITY

If n and r are positive integers, where $n \geq r$, then $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$.

Proof

Let S be a set containing $(n + 1)$ elements, one of which is ' a '. Let $S' \equiv S - \{a\}$.

The number of subsets of S containing r elements is $\binom{n+1}{r}$.

Now a subset of S with r elements either contains ‘ a ’ together with $(r - 1)$ elements of S' or contains r elements of S' which do not include ‘ a ’.

The number of subsets of $(r - 1)$ elements of $S' = \binom{n}{r-1}$.

\therefore The number of subsets of r elements of S that contain ‘ a ’ = $\binom{n}{r}$.

Also the number of subsets of r elements of S that do not contain ‘ a ’ = that of $S' = \binom{n}{r}$. Consequently, $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$

Note This result can also be proved by using the values of $\binom{n}{r-1}, \binom{n}{r}$ and $\binom{n+1}{r}$.

Corollary

$$C(n+1, r+1) = \sum_{i=r}^n C(i, r)$$

Proof

Changing n to i and r to $r+1$ in Pascal’s identity, we get

$$\begin{aligned} C(i, r) + C(i, r+1) &= C(i+1, r+1) \\ \text{i.e.,} \quad C(i, r) &= C(i+1, r+1) - C(i, r+1) \end{aligned} \quad (1)$$

Putting $i = r, r+1, \dots, n$ in (1) and adding, we get

$$\begin{aligned} \sum_{i=r}^n C(i, r) &= C(n+1, r+1) - C(r, r+1) \\ &= C(n+1, r+1) [\because C(r, r+1) = 0] \end{aligned}$$

VANDERMONDE’S IDENTITY

If m, n, r are non-negative integers where $r \leq m$ or n , then

$$C(m+n, r) = \sum_{i=0}^r C(m, r-i) \cdot C(n, i)$$

Proof

Let m and n be the number of elements in sets 1 and 2 respectively.

Then the total number of ways of selecting r elements from the union of sets 1 and 2

$$= C(m+n, r)$$

The r elements can also be selected by selecting i elements from set 2 and $(n-i)$ elements from set 1, where $i = 0, 1, 2, \dots, r$. This selection can be done in $C(m, r-i) \cdot C(n, i)$ ways, by the product rule.

The $(r+1)$ selections corresponding to $i = 0, 1, 2, \dots, r$ are disjoint. Hence, by the sum rule (stated as follows), we get

$$C(m+n, r) = \sum_{i=0}^r C(m, r-i) \cdot C(n, i) \quad \text{or} \quad \sum_{i=0}^r C(m, i) \cdot C(n, r-i)$$

Sum rule

If r activities can be performed in n_1, n_2, \dots, n_r ways and if they are disjoint, viz., cannot be performed simultaneously, then any one of the r activities can be performed in $(n_1 + n_2 + \dots + n_r)$ ways.

PERMUTATIONS WITH REPETITION**Theorem**

When repetition of n elements contained in a set is permitted in r -permutations, then the number of r -permutations is n^r .

Proof

The number of r -permutations of n elements can be considered as the same as the number of ways in which the n elements can be placed in r positions.

The first position can be occupied in n ways, as any one of the n elements can be used.

Similarly, the second position can also be occupied in n ways, as any one of the n elements can be used, since repetition of elements is allowed.

Hence, the first two positions can be occupied in $n \times n = n^2$ ways, by the product rule. Proceeding like this, we see that the ' r ' positions can be occupied by ' n ' elements (with repetition) in n^r ways.

i.e., the number of r -permutations of n elements with repetition = n^r .

Theorem

The number of different permutations of n objects which include n_1 identical objects of type I, n_2 identical objects of type II, ... and n_k identical objects of type k is equal to $\frac{n!}{n_1! n_2! \cdots n_k!}$, where $n_1 + n_2 + \dots + n_k = n$.

Proof

The number of n -permutations of n objects is equal to the number of ways in which the n objects can be placed in n positions.

n_1 positions to be occupied by n_1 objects of the I type can be selected from n positions in $C(n, n_1)$ ways.

n_2 positions to be occupied by the n_2 objects of the II type can be selected from the remaining $(n - n_1)$ positions in $C(n - n_1, n_2)$ ways and so on. Finally n_k positions to be occupied by the n_k objects of type k can be selected from the remaining $(n - n_1 - n_2 - \dots - n_{k-1})$ positions in $C(n - n_1 - n_2 - \dots - n_{k-1}, n_k)$ ways.

Hence, the required number of different permutations

$$\begin{aligned}
 &= C(n, n_1) \times C(n - n_1, n_2) \times \dots \times C(n - n_1 - n_2 - \dots - n_{k-1}, n_k) \\
 &\quad (\text{by the product rule}) \\
 &= \frac{n!}{n_1!(n - n_1)!} \times \frac{(n - n_1)!}{n_2!(n - n_1 - n_2)!} \times \dots \times \frac{(n - n_1 - n_2 - \dots - n_{k-1})!}{n_k! 0!} \\
 &\quad (\because n_1 + n_2 + \dots + n_k = n) \\
 &= \frac{n!}{n_1! n_2! \cdots n_k!}.
 \end{aligned}$$

Example

Let us consider the 3-permutations of the 3 letters A, B_1, B_2 , the number of which is $3!$ They are: $AB_1B_2, AB_2B_1, B_1AB_2, B_1B_2A, B_2AB_1$ and B_2B_1A . If we replace B_1 and B_2 by B , the above permutations become

$$ABB, ABB, BAB, BBA, BAB \text{ and } BBA.$$

These permutations are not different. The different 3-permutations of the 3 letters A, B, B are ABB, BAB and BBA . Thus the number of different 3-permutations of 3 letters, of which 2 are identical of one type and 1 is of another type is equal to

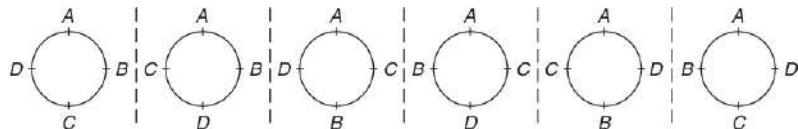
$$3 = \frac{3!}{2!1!}$$

This example illustrates the above theorem.

CIRCULAR PERMUTATION

The permutations discussed so far can be termed as linear permutations, as the objects were assumed to be arranged in a line. If the objects are arranged in a circle (or any closed curve), we get circular permutation and the number of circular permutations will be different from the number of linear permutations as seen from the following example:

We can arrange 4 elements A, B, C, D in a circle as follows: We fix one of the elements, say A , at the top point of the circle. The other 3 elements B, C, D are permuted in all possible ways, resulting in $6 = 3!$ different circular permutations are as follows:

**Note**

Circular arrangements are considered the same when one can be obtained from the other by rotation, viz., The relative positions (and not the actual positions) of the objects alone count for different circular permutations.

From the example given above, we see that the number of different circular arrangements of 4 elements $= (4 - 1)! = 6$.

Similarly, the number of different circular arrangements of n objects $= (n - 1)!$ If no distinction is made between clockwise and counterclockwise circular arrangements [For example, if the circular arrangements in the first and the last figures are assumed as the same], then the number of different circular arrangements $= \frac{1}{2}(n - 1)!$

PIGEONHOLE PRINCIPLE

Though this principle stated as follows is deceptively simple, it is sometimes useful in counting methods. The deception often lies in recognising the problems where this principle can be applied.

Statement

If n pigeons are accommodated in m pigeon-holes and $n > m$ then at least one pigeonhole will contain two or more pigeons. Equivalently, if n objects are put in m boxes and $n > m$, then at least one box will contain two or more objects.

Proof

Let the n pigeons be labelled P_1, P_2, \dots, P_n and the m pigeonholes be labelled H_1, H_2, \dots, H_m . If P_1, P_2, \dots, P_m are assigned to H_1, H_2, \dots, H_m respectively, we are left with the $(n - m)$ pigeons $P_{m+1}, P_{m+2}, \dots, P_n$. If these left over pigeons are assigned to the m pigeonholes again in any random manner, at least one pigeonhole will contain two or more pigeons.

GENERALISATION OF THE PIGEONHOLE PRINCIPLE

If n pigeons are accommodated in m pigeonholes and $n > m$, then one of the pigeonholes must contain at least $\left\lfloor \frac{(n-1)}{m} \right\rfloor + 1$ pigeons, where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x , which is a real number.

Proof

If possible, let each pigeonhole contain at the most $\left\lfloor \frac{(n-1)}{m} \right\rfloor$ pigeons.

Then the maximum number of pigeons in all the pigeonholes

$$= m \left\lfloor \frac{(n-1)}{m} \right\rfloor \leq m \cdot \frac{(n-1)}{m} \quad \left\{ \because \left\lfloor \frac{(n-1)}{m} \right\rfloor \leq \frac{(n-1)}{m} \right\}$$

i.e., the maximum number of pigeons in all the pigeonholes $\leq (n-1)$

This is against the assumption that there are n pigeons.

Hence, one of the pigeonholes must contain at least $\left\lfloor \frac{(n-1)}{m} \right\rfloor + 1$ pigeons.

PRINCIPLE OF INCLUSION-EXCLUSION**Statement**

If A and B are finite subsets of a finite universal set U , then $|A \cup B| = |A| + |B| - |A \cap B|$, where $|A|$ denotes the cardinality of (the number of elements in) the set A .

This principle can be extended to a finite number of finite sets A_1, A_2, \dots, A_n as follows:

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_i |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots \\ &\quad + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n| \end{aligned}$$

where the first sum is over all i , the second sum is over all pairs i, j with $i < j$, the third sum is over all triples i, j, k with $i < j < k$ and so on.

Proof

$$\begin{aligned} \text{Let } A \setminus B &= \{a_1, a_2, \dots, a_r\} \\ B \setminus A &= \{b_1, b_2, \dots, b_s\} \\ A \cap B &= \{x_1, x_2, \dots, x_t\}, \end{aligned}$$

where $A \setminus B$ is the set of those elements A which are not in B .

$$\text{Then } A = \{a_1, a_2, \dots, a_r, x_1, x_2, \dots, x_t\}$$

$$\text{and } B = \{b_1, b_2, \dots, b_s, x_1, x_2, \dots, x_t\}$$

$$\text{Hence, } A \cup B = \{a_1, a_2, \dots, a_r, x_1, x_2, \dots, x_t, b_1, b_2, \dots, b_s\}$$

$$\text{Now } |A| + |B| - |A \cap B| = (r + t) + (s + t) - t$$

$$= r + s + t = |A \cup B| \quad (1)$$

Let us now extend the result to 3 finite sets A, B, C .

$$\begin{aligned} |A \cup B \cup C| &= |A \cup (B \cup C)| \\ &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| - \{|(A \cap B) \cup (A \cap C)| \text{ by (1)}\} \\ &= |A| + |B| + |C| - |B \cap C| - \{|A \cap B| + |A \cap C| \\ &\quad - |(A \cap B) \cap (A \cap C)|\}, \text{ by (1)} \\ &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| \\ &\quad + |A \cap B \cap C| \end{aligned}$$

Generalising, we get the required result.

**WORKED EXAMPLES 2(A)****Example 2.1**

- Assuming that repetitions are not permitted, how many four-digit numbers can be formed from the six digits 1, 2, 3, 5, 7, 8?
- How many of these numbers are less than 4000?
- How many of the numbers in part (a) are even?
- How many of the numbers in part (a) are odd?
- How many of the numbers in part (a) are multiples of 5?
- How many of the numbers in part (a) contain both the digits 3 and 5?
- The 4-digit number can be considered to be formed by filling up 4 blank spaces with the available 6 digits. Hence, the number of 4-digits numbers

$$\begin{aligned}
 &= \text{the number of 4-permutations of 6 numbers} \\
 &= P(6, 4) = 6 \times 5 \times 4 \times 3 = 360
 \end{aligned}$$
- If a 4-digit number is to be less than 4000, the first digit must be 1, 2, or 3. Hence the first space can be filled up in 3 ways. Corresponding to any one of these 3 ways, the remaining 3 spaces can be filled up with the remaining 5 digits in $P(5, 3)$ ways. Hence, the required number $= 3 \times P(5, 3)$

$$= 3 \times 5 \times 4 \times 3 = 180.$$
- If the 4-digit number is to be even, the last digit must be 2 or 8. Hence, the last space can be filled up in 2 ways. Corresponding to any one of

these 2 ways, the remaining 3 spaces can be filled up with the remaining 5 digits in $P(5, 3)$ ways. Hence the required number of even numbers
 $= 2 \times P(5, 3) = 120.$

- (d) Similarly the required number of odd numbers $= 4 \times P(5, 3) = 240.$
- (e) If the 4-digit number is to be a multiple of 5, the last digit must be 5. Hence, the last space can be filled up in only one way. The remaining 3 spaces can be filled up in $P(5, 3)$ ways.
Hence, the required number $= 1 \times P(5, 3) = 60.$
- (f) The digits 3 and 5 can occupy any 2 of the 4 places in $P(4, 2) = 12$ ways. The remaining 2 places can be filled up with the remaining 4 digits in $P(4, 2) = 12$ ways. Hence, the required number $= 12 \times 12 = 144.$

Example 2.2

- (a) In how many ways can 6 boys and 4 girls sit in a row?
- (b) In how many ways can they sit in a row if the boys are to sit together and the girls are to sit together?
Corresponding to any one of these 2 ways, the boys can be arranged in a row in $6!$ ways and the girls in $4!$ ways.
 \therefore Required number of ways $= 2 \times 6! \times 4! = 34,560.$
- (c) The girls are considered as one unit (object) and there are 7 objects consisting of one object of 4 girls and 6 objects of 6 boys.
These 7 objects can be arranged in a row in $7!$ ways.
Corresponding to any one of these ways, the 4 girls (considered as one object) can be arranged among themselves in $4!$ ways. Hence, the required number of ways $= 7! 4! = 1,20,960.$
- (d) No. of ways in which girls only sit together
 $= (\text{No. of ways in which girls sit together})$
 $- (\text{No of ways in which boys sit together and girls sit together})$
 $= 1,20,960 - 34,560 = 86,400.$

Example 2.3 How many different paths in the xy -plane are there from $(1, 3)$ to $(5, 6)$, if a path proceeds one step at a time by going either one step to the right (R) or one step upward (U)?

To reach the point $(5, 6)$ from $(1, 3)$, one has to traverse $5 - 1 = 4$ steps to the right and $6 - 3 = 3$ steps to the up.

Hence, the total number of 7 steps consists of 4 R's and 3 U's.

To traverse the paths, one can take R's and U's in any order.

Hence, the required number of different paths is equal to the number of permutations of 7 steps, of which 4 are of the same type (namely R) and 3 are of the same type (namely U).

$$\therefore \text{Required number of paths} = \frac{7!}{4!3!} = 35.$$

Example 2.4 How many positive integers n can be formed using the digits 3, 4, 4, 5, 5, 6, 7, if n has to exceed 50,00,000?

In order that n may be greater than 50,00,000, the first place must be occupied by 5, 6 or 7.

When 5 occupies the first place, the remaining 6 places are to be occupied by the digits 3, 4, 4, 5, 6, 7.

The number of such numbers

$$\begin{aligned} &= \frac{6!}{2!} \quad (\because \text{the digit 4 occurs twice}) \\ &= 360. \end{aligned}$$

When 6 (or 7) occupies the first place, the remaining 6 places are to be occupied by the digits 3, 4, 4, 5, 5, 7 (or 3, 4, 4, 5, 5, 6).

The number of such numbers

$$\begin{aligned} &= \frac{6!}{2!2!} \quad [\because 4 \text{ and } 5 \text{ each occurs twice}] \\ &= 180 \end{aligned}$$

$$\therefore \text{No. of numbers exceeding } 50,00,000 = 360 + 180 + 180 = 720.$$

Example 2.5 How many bit strings of length 10 contain (a) exactly four 1's, (b) atmost four 1's, (c) at least four 1's (d) an equal number of 0's and 1's?

(a) A bit string of length 10 can be considered to have 10 positions. These 10 positions should be filled with four 1's and six 0's.

$$\therefore \text{No. of required bit strings} = \frac{10!}{4!6!} = 210.$$

(b) The 10 positions should be filled up with no 1 and ten 0's or one 1 and nine 0's or two 1's and eight 0's or three 1's and seven 0's or four 1's and six 0's.

$$\therefore \text{Required no. of bit strings}$$

$$= \frac{10!}{0!10!} + \frac{10!}{1!9!} + \frac{10!}{2!8!} + \frac{10!}{3!7!} + \frac{10!}{4!6!} = 386.$$

(c) The ten positions are to be filled up with four 1's and six 0's or five 1's and five 0's etc. or ten 1's and no 0's.

$$\therefore \text{Required no. of bit strings}$$

$$= \frac{10!}{4!6!} + \frac{10!}{5!5!} + \frac{10!}{6!4!} + \frac{10!}{7!3!} + \frac{10!}{8!2!} + \frac{10!}{9!1!} + \frac{10!}{10!0!} = 848.$$

(d) The ten positions are to be filled up with five 1's and five 0's.

$$\therefore \text{Required no. of bit strings}$$

$$= \frac{10!}{5!5!} = 252.$$

Example 2.6 How many permutations of the letters $A\ B\ C\ D\ E\ F\ G$ contain (a) the string BCD , (b) the string CFG , (c) the strings BA and GF , (d) the strings ABC and DE , (e) the strings ABC and CDE , (f) the strings CBA and BED ?

- (a) Treating BCD as one object, we have the following 5 objects:

$$A, (BCD), E, F, G.$$

These 5 objects can be permuted in

$$P(5, 5) = 5! = 120 \text{ ways}$$

Note B, C, D should not be permuted in the string BCD .

- (b) Treating CFG as one object, we have the following 4 objects: $B, D, E, (CFG)$.

The no. of ways of permuting these 4 objects $= 4! = 24$.

- (c) The objects $(BA), C, D, E$ and (GF) can be permuted in $5! = 120$ ways.

- (d) The objects $(ABC), (DE), F, G$ can be permuted in $4! = 24$ ways.

- (e) Even though (ABC) and (CDE) are two strings, they contain the common letter C . If we include the strings $(ABCDE)$ in the permutations, it includes both the strings (ABC) and (CDE) . Moreover we cannot use the letter C twice.

Hence, we have to permute the 3 objects $(ABCDE), F$ and G . This can be done in $3! = 6$ ways.

- (f) To include the 2 strings (CBA) and (BED) in the permutations, we require the letter B twice, which is not allowed. Hence, the required no. of permutations $= 0$.

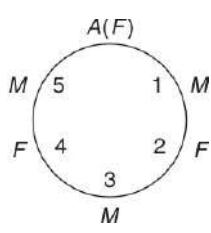
Example 2.7 If 6 people A, B, C, D, E, F are seated about a round table, how many different circular arrangements are possible, if arrangements are considered the same when one can be obtained from the other by rotation?

If A, B, C are females and the others are males, in how many arrangements do the sexes alternate?

The no. of different circular arrangements of n objects is $(n - 1)!$

\therefore The required no. of circular arrangements $= 5! = 120$.

Since rotation does not alter the circular arrangement, we can assume that A occupies the top position as shown in the figure.



Of the remaining places, positions 1, 3, 5 must be occupied by the 3 males. This can be achieved in $P(3, 3) = 3! = 6$ ways.

The remaining two places 2 and 4 should be occupied by the remaining two females. This can be achieved in $P(2, 2) = 2$ ways.

\therefore Total no. of required circular arrangements $= 6 \times 2 = 12$.

Example 2.8 From a club consisting of 6 men and 7 women, in how many ways can we select a committee of

- (a) 3 men and 4 women?
 (b) 4 persons which has at least one woman?
 (c) 4 persons that has at most one man?
 (d) 4 persons that has persons of both sexes?
 (e) 4 persons so that two specific members are not included?
- (a) 3 men can be selected from 6 men in $C(6, 3)$ ways.
 4 women can be selected from 7 women in $C(7, 4)$ ways.
 \therefore The committee of 3 men and 4 women can be selected in $C(6, 3) \times C(7, 4)$ ways. (by the product rule)
 i.e., in $\frac{6!}{3!3!} \times \frac{7!}{4!3!} = 700$ ways.

- (b) For the committee to have at least one woman, we have to select 3 men and 1 woman or 2 men and 2 women or 1 man and 3 women or no man and 4 women.

This selection can be done in

$$\begin{aligned} & C(6, 3) \cdot C(7, 1) + C(6, 2) \cdot C(7, 2) + C(6, 1) \cdot C(7, 3) \\ & \quad + C(6, 0) \cdot C(7, 4) \\ & = 20 \times 7 + 15 \times 21 + 6 \times 35 + 1 \times 35 \\ & = 140 + 315 + 210 + 35 = 700 \text{ ways.} \end{aligned}$$

- (c) For the committee to have at most one man, we have to select no man and 4 women or 1 man and 3 women.

This selection can be done in

$$C(6, 0) \cdot C(7, 4) + C(6, 1) \cdot C(7, 3) = 1 \times 35 + 6 \times 35 = 245 \text{ ways.}$$

- (d) For the committee to have persons of both sexes, the selection must include 1 man and 3 women or 2 men and 2 women or 3 men and 1 woman.

This selection can be done in

$$\begin{aligned} & C(6, 1) \times C(7, 3) + C(6, 2) \times C(7, 2) + C(6, 3) \times C(7, 1) \\ & = 6 \times 35 + 15 \times 21 + 20 \times 7 \\ & = 210 + 315 + 140 = 665 \text{ ways.} \end{aligned}$$

- (e) First let us find the number of selections that contain the two specific members. After removing these two members, 2 members can be selected from the remaining 11 members in $C(11, 2)$ ways. In each of these selections, if we include those 2 specific members removed, we get $C(11, 2)$ selections containing the 2 members.

The no. of selections not including these 2 members

$$\begin{aligned} & = C(13, 4) - C(11, 2) \\ & = 715 - 55 = 660. \end{aligned}$$

Example 2.9 In how many ways can 20 students out of a class of 30 be selected for an extra-curricular activity, if

- (a) Rama refuses to be selected?
 (b) Raja insists on being selected?

- (c) Gopal and Govind insist on being selected?
 (d) either Gopal or Govind or both get selected?
 (e) just one of Gopal and Govind gets selected?
 (f) Rama and Raja refuse to be selected together?
- (a) We first exclude Rama and then select 20 students from the remaining 29 students.
 \therefore Number of ways = $C(29, 20) = 1, 00, 15, 005.$
- (b) We separate Raja from the class, select 19 students from 29 and then include Raja in the selections.
 \therefore Number of ways = $C(29, 19) = 2, 00, 30, 010.$
- (c) We separate Gopal and Govind, select 18 students from 28 and then include both of them in the selections.
 \therefore Number of ways = $C(28, 18) = 1, 31, 23, 110$
- (d) Number of selections which include Gopal = $C(29, 19)$
 Number of selections which include Govind = $C(29, 19)$
 Number of selections which include both = $C(28, 18)$
 \therefore By the principle of inclusion – exclusion, the required number of selections
 $= C(29, 19) + C(29, 19) - C(28, 18)$
 $= 2, 69, 36, 910.$
- (e) Number of selections including either Gopal or Govind
 $= (\text{Number of selections including either Gopal or Govind or both})$
 $\quad - (\text{Number of selections including both})$
 $= [C(29, 19) + C(29, 19) - C(28, 18)] - C(28, 18)$
 $= 2, 69, 36, 910 - 1, 31, 23, 110 = 1, 38, 13, 800.$
- (f) Number of ways of selecting 20 excluding Rama and Raja together
 $= (\text{Total number of selections}) - (\text{Number of selections including both Rama and Raja})$
 $= C(30, 20) - C(28, 18) [\text{as in part (c)}]$
 $= 3, 00, 45, 015 - 1, 31, 23, 110 = 1, 69, 21, 905.$

Example 2.10 In how many ways can 2 letters be selected from the set $\{a, b, c, d\}$ when repetition of the letters is allowed, if (i) the order of the letters matters (ii) the order does not matter?

- (i) When the order of the selected letters matters, the number of possible selections = $4^2 = 16$, which are listed below:

$$\begin{aligned} &aa, ab, ac, ad \\ &ba, bb, bc, bd \\ &ca, cb, cc, cd \\ &da, db, dc, dd \end{aligned}$$

In general, the number of r -permutations of n objects, if repetition of the objects is allowed, is equal to n^r , since there are n ways to select an object from the set for each of the r -positions.

- (ii) When the order of the selected letter does not matter, the number of possible selections $C(4 + 2 - 1, 2) = C(5, 2) = 10$, which are listed below:

$$\begin{array}{c}
 aa, ab, ac, ad \\
 bb, bc, bd \\
 cc, cd \\
 dd
 \end{array}$$

In general, the number of r -combinations of n kinds of objects, if repetitions of the objects is allowed = $C(n + r - 1, r)$.

[The reader may try to prove this result.]

Example 2.11 There are 3 piles of identical red, blue and green balls, where each pile contains at least 10 balls. In how many ways can 10 balls be selected:

- (a) if there is no restriction?
 - (b) if at least one red ball must be selected?
 - (c) if at least one red ball, at least 2 blue balls and at least 3 green balls must be selected?
 - (d) if exactly one red ball must be selected?
 - (e) if exactly one red ball and at least one blue ball must be selected?
 - (f) if at most one red ball is selected?
 - (g) if twice as many red balls as green balls must be selected?
- (a) There are $n = 3$ kinds of balls and we have to select $r = 10$ balls, when repetitions are allowed.
- \therefore No. of ways of selecting = $C(n + r - 1, r) = C(12, 10) = 66$.
- (b) We take one red ball and keep it aside. Then we have to select 9 balls from the 3 kinds of balls and include the first red ball in the selections.
 \therefore No. of ways of selecting = $C(11, 9) = 55$.
- (c) We take away 1 red, 2 blue and 3 green balls and keep them aside.
 Then we select 4 balls from the 3 kinds of balls and include the 6 already chosen balls in each selection.
 \therefore No. of ways of selecting = $C(3 + 4 - 1, 4) = 15$.
- (d) We select 9 balls from the piles containing blue and green balls and include 1 red ball in each selection.
 \therefore No. of ways of selecting = $C(2 + 9 - 1, 9) = 10$.
- (e) We take away one red ball and one blue ball and keep them aside. Then we select 8 balls from the blue and green piles and include the already reserved red and blue balls to each selection.
 \therefore No. of ways of selecting = $C(2 + 8 - 1, 8) = 9$.
- (f) The selections must contain no red ball or 1 red ball.
 \therefore No. of ways of selecting = $C(2 + 10 - 1, 10) + C(2 + 9 - 1, 9)$
 $= 11 + 10 = 21$
- (g) The selections must contain 0 red and 0 green balls or 2 red and 1 green balls or 4 red and 2 green balls or 6 red and 3 green balls.
 \therefore No. of ways of selecting = $C(1 + 10 - 1, 10) + C(1 + 7 - 1, 7)$
 $+ C(1 + 4 - 1, 4) + C(1 + 1 - 1, 1)$
 $= 1 + 1 = 1 + 1 = 4$.

Example 2.12 5 balls are to be placed in 3 boxes. Each can hold all the 5 balls. In how many different ways can we place the balls so that no box is left empty, if

- (a) balls and boxes are different?
 - (b) balls are identical and boxes are different?
 - (c) balls are different and boxes are identical?
 - (d) balls as well as boxes are identical?
 - (a) 5 balls can be distributed such that the first, second and third boxes contain 1, 1 and 3 balls respectively.
- ∴ No. of ways of distributing in this manner

$$= \frac{5!}{1!1!3!} = 20.$$

Similarly the boxes I, II, III may contain 1, 3 and 1 balls respectively or 3, 1 and 1 balls respectively. (\because the boxes are different). No. of ways of distributing in each of these manners = 20.

Again the boxes I, II, III may contain 1, 2, 2 balls respectively or 2, 1, 2 balls respectively or 2, 2, 1 balls respectively. No. of ways of distributing

$$\text{in each of these manners} = \frac{5!}{1!2!2!} = 30.$$

∴ Total no. of required ways

$$= 20 + 20 + 20 + 30 + 30 + 30 = 150$$

- (b) Total no. of ways of distributing r identical balls in n different boxes is the same as the no. of r -combinations of n items, repetitions allowed.

It is $= C(n + r - 1, r) = C(3 + 2 - 1, 2) = 6$ since 3 balls must be first put, one in each of 3 boxes and the remaining 2 balls must be distributed in 3 boxes.

- (c) When the boxes are identical, the distributions of 1, 1, 3 balls, 1, 3, 1 balls and 3, 1, 1 balls considered in (a) will be treated as identical distributions. Thus there are 20 ways of distributing 1 ball in each of any two boxes and 3 balls in the third box.

Similarly, there are 30 ways of distributing 2 balls in each of any 2 boxes and 1 ball in the third box.

$$\therefore \text{No. of required ways} = 20 + 30 = 50.$$

- (d) By an argument similar to that given in (c), we get from the answer in (b)

$$\text{that the required no. of ways} = \frac{6}{3} = 2.$$

Example 2.13 Determine the number of integer solutions of the equation

$$x_1 + x_2 + x_3 + x_4 = 32, \text{ where}$$

- (a) $x_i \geq 0, 1 \leq i \leq 4;$
- (b) $x_i > 0, 1 \leq i \leq 4;$
- (c) $x_1, x_2 \geq 5$ and $x_3, x_4 \geq 7;$
- (d) $x_1, x_2, x_3 > 0$ and $0 < x_4 \leq 25.$
- (a) One solution of the equation is $x_1 = 15, x_2 = 10, x_3 = 7$ and $x_4 = 0.$
Another solution is $x_1 = 7, x_2 = 15, x_3 = 0$ and $x_4 = 10.$ These two

solutions are considered different, even though the same 4 integers 15, 10, 7, 0 are used. The first solution can be interpreted as follows:

We have 32 identical chocolates and are distributing them among 4 distinct children. We have given 15, 10, 7 and 0 chocolates to the first, second, third and fourth child respectively.

Thus, each non-negative solution of the equation corresponds to a selection of 32 identical items from 4 distinct sets, repetitions allowed.

$$\begin{aligned}\text{Hence, } \text{the no. of solutions} &= C(4 + 32 - 1, 32) \\ &= C(35, 32) = 6545\end{aligned}$$

- (b) Now $x_i > 0; 1 \leq i \leq 4$

$$\text{i.e., } x_i \geq 1; 1 \leq i \leq 4$$

Let us put $u_i = x_i - 1$, so that $u_i \geq 0; 1 \leq i \leq 4$

Then the given equation becomes

$$u_1 + u_2 + u_3 + u_4 = 28,$$

for which the no. of non-negative integer solutions is required.

$$\begin{aligned}\text{The required number} &= C(4 + 28 - 1, 28) \\ &= C(31, 28) = 4495.\end{aligned}$$

- (c) Putting $x_1 - 5 = u_1, x_2 - 5 = u_2, x_3 - 7 = u_3$ and $x_4 - 7 = u_4$, the equation becomes $u_1 + u_2 + u_3 + u_4 = 8$, where $u_1, u_2, u_3, u_4 \geq 0$.

$$\begin{aligned}\text{The required no. of solutions} &= C(4 + 8 - 1, 8) \\ &= C(11, 8) = 165.\end{aligned}$$

No. of solutions such that $x_1, x_2, x_3 > 0$ and $0 < x_4 \leq 25$ = (No. of solutions such that $x_i > 0; i = 1, 2, 3, 4$) – (No. of solutions such that $x_i > 0; i = 1, 2, 3$ and $x_4 > 25$) = $a - b$, say.

From part (b); $a = C(31, 28) = 4495$

To find b , we put $u_1 = x_1 - 1, u_2 = x_2 - 1, u_3 = x_3 - 1$ and $u_4 = x_4 - 26$.

The equation becomes $u_1 + u_2 + u_3 + u_4 = 3$.

We have to get the solution satisfying $u_i \geq 0; i = 1, 2, 3, 4$.

$$\begin{aligned}\text{No. of solutions} &= b = C(4 + 3 - 1, 3) \\ &= C(6, 3) = 20.\end{aligned}$$

$$\therefore \text{Required no. of solutions} = 4495 - 20 \\ = 4475.$$

Example 2.14 Find the number of non-negative integer solutions of the inequality $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 < 10$?

We convert the inequality into an equality by introducing an auxiliary variable $x_7 > 0$.

Thus, we get $x_1 + x_2 + \dots + x_6 + x_7 = 10$, where

$$x_i \geq 0, i = 1, 2, \dots, 6 \text{ and } x_7 > 0 \text{ or } x_7 \geq 1.$$

Putting $x_i = y_i, i = 1, 2, \dots, 6$ and $x_7 - 1 = y_7$, the equation becomes

$$y_1 + y_2 + \dots + y_7 = 10 - 1 = 9, \text{ where } y_i \geq 0, \text{ for } 1 \leq i \leq 7$$

The number of required solutions

$$= C(7 + 9 - 1, 9) = C(15, 9) = 5005.$$

Example 2.15 How many positive integers less than 10,00,000 have the sum of their digits equal to 19?

Any positive integer less than 10,00,000 will have a maximum of 6 digits. If we denote them by x_i ; $1 \leq i \leq 6$, the problem reduces to one of finding the number of solutions of the equation

$$x_1 + x_2 + \dots + x_6 = 19, \text{ where } 0 \leq x_i \leq 9 \quad (1)$$

There are $C(6 + 19 - 1, 19) = C(24, 5)$ solutions if $x_i \geq 0$.

We note that one of the six x_i 's can be ≥ 10 , but not more than one, as the sum of the x_i 's = 19.

Let $x_1 \geq 10$ and let $u_1 = x_1 - 10$, $u_i = x_i$, $2 \leq i \leq 6$

Then the equation becomes

$$u_1 + u_2 + \dots + u_6 = 9, \text{ where } u_i \geq 0$$

There are $C(6 + 9 - 1, 9) = C(14, 5)$ solutions for this equations.

The digit which is ≥ 10 can be chosen in 6 ways (viz., it may be x_1, x_2, \dots, x_6).

Hence, the number of solutions of the equation $x_1 + x_2 + \dots + x_6 = 19$, where any one $x_i \geq 10$ is $6 \times C(14, 5)$.

Hence, the required number of solutions of (1)

$$\begin{aligned} &= C(24, 5) - 6 \times C(14, 5) \\ &= 42,504 - 6 \times 2002 = 30,492. \end{aligned}$$

Example 2.16 A man hiked for 10 hours and covered a total distance of 45 km. It is known that he hiked 6 km in the first hour and only 3 km in the last hour. Show that he must have hiked at least 9 km within a certain period of 2 consecutive hours.

Since, the man hiked $6 + 3 = 9$ km in the first and last hours, he must have hiked $45 - 9 = 36$ km during the period from second to ninth hours.

If we combine the second and third hours together, the fourth and fifth hours together, etc. and the eighth and ninth hours together, we have 4 time periods.

Let us now treat 4 time periods as pigeonholes and 36 km as 36 pigeons.

Using the generalised pigeonhole principle,

the least no. of pigeons accommodated in one pigeonhole

$$\begin{aligned} &= \left\lceil \frac{36-1}{4} \right\rceil + 1 \\ &= \lfloor 8.75 \rfloor + 1 = 9 \end{aligned}$$

viz., the man must have hiked at least 9 km in one time period of 2 consecutive hours.

Example 2.17 If we select 10 points in the interior of an equilateral triangle of side 1, show that there must be at least two points whose distance apart is less than $\frac{1}{3}$.

Let ADG be the given equilateral triangle. The pairs of points B, C ; E, F and H, I are the points of trisection of the sides AD , DG and GA respectively. We have divided the triangle ADG into 9 equilateral triangles each of side $\frac{1}{3}$.

The 9 sub-triangles may be regarded as 9 pigeonholes and 10 interior points may be regarded as 10 pigeons.

Then by the pigeonhole principle, at least one sub triangle must contain 2 interior points.

The distance between any two interior points of any sub triangle cannot exceed the length of the side, namely, $\frac{1}{3}$.

Hence the result.

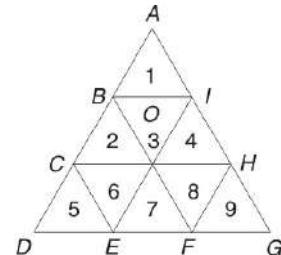
Example 2.18

- If n pigeonholes are occupied by $(kn + 1)$ pigeons, where k is a positive integer, prove that at least one pigeonhole is occupied by $(k + 1)$ or more pigeons.
- Hence, find the minimum number m of integers to be selected from $S = \{1, 2, \dots, 9\}$ so that (a) the sum of two of the m integers is even; (b) the difference of two of the m integers is 5. But there are $(kn + 1)$ pigeons. This results in a contradiction. Hence the result.
- If at least one pigeonhole is not occupied by $(k + 1)$ or more pigeons, each pigeonhole contains at most k pigeons. Hence, the total number of pigeons occupying the n pigeonholes is at most kn .
But there are $(kn + 1)$ pigeons. This results in a contradiction. Hence, the result
- (a) Sum of 2 even integers or of 2 odd integers is even.
Let us divide the set S into 2 subsets $\{1, 3, 5, 7, 9\}$ and $\{2, 4, 6, 8\}$, which may be treated as pigeonholes. Thus $n = 2$.
At least 2 numbers must be chosen either from the first subset or from the second.
i.e., at least one pigeonhole must contain 2 pigeons
i.e., $k + 1 = 2$ or $k = 1$
 \therefore The minimum no. of pigeons required or the minimum number of integers to be selected is equal to
$$kn + 1 = 3.$$

- Let us divide the set S into the 5 subsets $\{1, 6\}$, $\{2, 7\}$, $\{3, 8\}$, $\{4, 9\}$, $\{5\}$, which may be treated as pigeonholes. Thus $n = 5$.

If $m = 6$, then 2 of integers of S will belong to one of the subsets and their difference is 5.

Example 2.19 If $(n + 1)$ integers not exceeding $2n$ are selected, show that there must be an integer that divides one of the other integers. Deduce that if 151 integers are selected from $\{1, 2, 3, \dots, 300\}$ then the selection must include two integers x, y either of which divides the other.



Let the $(n + 1)$ integers be a_1, a_2, \dots, a_{n+1} . Each of these numbers can be expressed as an odd multiple of a power of 2.
i.e., $a_i = 2^{ki} \times m_i$, where k_i is a non-negative integer and m_i is odd ($i = 1, 2, \dots, n + 1$)

[For example, let $n = 5$ so that $2n = 10$. Let us consider $n + 1 = 6$ nos. that are less than or equal to 10, viz., 7, 5, 4, 6, 3, 10. Clearly $7 = 2^0 \cdot 7$; $5 = 2^0 \cdot 5$; $4 = 2^2 \cdot 1$; $6 = 2^1 \cdot 3$; $3 = 2^0 \cdot 3$ and $10 = 2^1 \cdot 5$].

The integers m_1, m_2, \dots, m_{n+1} are odd positive integers less than $2n$ (pigeons).

But there are only n odd positive integers less than $2n$ (pigeonholes).

Hence, by the pigeonhole principle, 2 of the integers must be equal. Let them be $m_i = m_j$.

$$\therefore a_i = 2^{ki}m_i \text{ and } a_j = 2^{kj}m_j$$

$$\therefore \frac{a_i}{a_j} = \frac{2^{ki}}{2^{kj}} \quad (\because m_i = m_j)$$

If $k_i < k_j$, then 2^{ki} divides 2^{kj} and hence a_i divides a_j .

If $k_i > k_j$, then a_j divides a_i .

Putting $n = 150$ (and hence, $2n = 300$ and $n + 1 = 151$) the deduction follows.

Example 2.20 If m is an odd positive integer, prove that there exists a positive integer n such that m divides $(2^n - 1)$.

Let us consider the $(m + 1)$ positive integers $2^1 - 1, 2^2 - 1, 2^3 - 1, \dots, 2^m - 1$ and $2^{m+1} - 1$.

When these are divided by m , two of the numbers will give the same remainder, by the pigeonhole principle [$(m + 1)$ numbers are $(m + 1)$ pigeons and the m remainders, namely, 0, 1, 2, ..., $(m - 1)$ are the pigeonholes].

Let the two numbers be $2^r - 1$ and $2^s - 1$ which give the same remainder r' , upon division by m .

viz., let $2^r - 1 = q_1m + r'$ and $2^s - 1 = q_2m + r'$

$$\therefore 2^r - 2^s = (q_1 - q_2)m$$

$$\text{But } 2^r - 2^s = 2^s(2^{r-s} - 1)$$

$$\therefore (q_1 - q_2)m = 2^s(2^{r-s} - 1)$$

But m is odd and hence cannot be a factor of 2^s .

$$\therefore m \text{ divides } 2^{r-s} - 1.$$

Taking $n = r - s$, we get the required results.

Example 2.21 Prove that in any group of six people, at least three must be mutual friends or at least three must be mutual strangers.

Let A be one of the six people. Let the remaining 5 people be accommodated in 2 rooms labeled “ A ’s friends” and “strangers to A ”.

Treating 5 people as 5 pigeons and 2 rooms as pigeonholes, by the generalised

pigeonhole principle, one of the rooms must contain $\left\lfloor \frac{5-1}{2} \right\rfloor + 1 = 3$ people.

Let the room labeled “ A ’s friends” contain 3 people. If any two of these 3 people are friends, then together with A , we have a set of 3 mutual friends. If no two of these 3 people are friends, then these 3 people are mutual strangers. In either case, we get the required conclusion.

If the room labeled “strangers to A ” contain 3 people, we get the required conclusion by similar argument.

Example 2.22 During a four-week vacation, a school student will attend at least one computer class each day, but he won’t attend more than 40 classes in all during the vacation. Prove that, no matter how he distributes his classes during the four weeks, there is a consecutive span of days during which he will attend exactly 15 classes.

Let the student attend a_1 classes on day 1, a_2 classes on day 2 and so on a_{28} classes on day 28.

Then $b_i = a_1 + a_2 + \dots + a_i$ will be the total no. of classes he will attend from day 1 to day i , both inclusive ($i = 1, 2, \dots, 28$).

$$\text{Clearly} \quad 1 \leq b_1 < b_2 < \dots < b_{28} \leq 40$$

$$\text{and} \quad b_1 + 15 < b_2 + 15 < \dots < b_{28} + 15 \leq 55$$

Now there are 56 distinct numbers (pigeons) b_1, b_2, \dots, b_{28} and $b_1 + 15, b_2 + 15, \dots, b_{28} + 15$.

These can take only 55 different values (1 through 55) (pigeonholes).

Hence, by the pigeonhole principle, at least two of the 56 numbers are equal.

Since $b_j > b_i$ if $j > i$, the only way for two numbers to be equal is $b_j = b_i + 15$, for some i and j where $j > i$.

$$\therefore \quad b_j - b_i = 15$$

$$\text{i.e.,} \quad a_{i+1} + a_{i+2} + \dots + a_j = 15$$

i.e., from the start of day $(i+1)$ to the end of day j , the student will attend exactly 15 classes.

Example 2.23 If S is a set of 5 positive integers, the maximum of which is at most 9, prove that the sums of the elements in all the nonempty subsets of S cannot all be distinct.

Let the subsets of S be such that $1 \leq n_A \leq 3$ (i.e., A consists of only one or two or three elements of S).

The number of such subsets $C(5, 1) + C(5, 2) + C(5, 3)$

$$\begin{aligned} &= 5 + 10 + 10 \quad (\because \text{there are 5 elements in } S) \\ &= 25 \end{aligned}$$

Let s_A be the sum of the elements of A .

Then $1 \leq s_A \leq 7 + 8 + 9$ (\because the maximum of any element of $S = 9$)

$$\text{i.e.,} \quad 1 \leq s_A \leq 24$$

Treating the 24 values of s_A as pigeonholes and 25 subsets A as pigeons, we get, by the pigeonhole principle, that there are 2 subsets A of S whose elements give the same sum.

Example 2.24 Find the number of integers between 1 and 250 both inclusive that are not divisible by any of the integers 2, 3, 5 and 7.

Let A, B, C, D be the sets of integers that lie between 1 and 250 and that are divisible by 2, 3, 5, and 7 respectively.

The elements of A are 2, 4, 6, ..., 250

$$\therefore |A| = 125, \text{ which is the same as } \left\lfloor \frac{250}{2} \right\rfloor$$

$$\text{Similarly, } |B| = \left\lfloor \frac{250}{3} \right\rfloor = 83; |C| = \left\lfloor \frac{250}{5} \right\rfloor = 50, |D| = \left\lfloor \frac{250}{7} \right\rfloor = 35.$$

The set of integers between 1 and 250 which are divisible by 2 and 3, viz., $A \cap B$ is the same as that which is divisible by 6, since 2 and 3 are relatively prime numbers.

$$\therefore |A \cap B| = \left\lfloor \frac{250}{6} \right\rfloor = 41$$

$$\text{Similarly, } |A \cap C| = \left\lfloor \frac{250}{10} \right\rfloor = 25; |A \cap D| = \left\lfloor \frac{250}{14} \right\rfloor = 17$$

$$|B \cap C| = \left\lfloor \frac{250}{15} \right\rfloor = 16; |B \cap D| = \left\lfloor \frac{250}{21} \right\rfloor = 11;$$

$$|C \cap D| = \left\lfloor \frac{250}{35} \right\rfloor = 7; |A \cap B \cap C| = \left\lfloor \frac{250}{30} \right\rfloor = 8;$$

$$|A \cap B \cap D| = \left\lfloor \frac{250}{42} \right\rfloor = 5; |A \cap C \cap D| = \left\lfloor \frac{250}{70} \right\rfloor = 3;$$

$$|B \cap C \cap D| = \left\lfloor \frac{250}{105} \right\rfloor = 2; |A \cap B \cap C \cap D| = \left\lfloor \frac{250}{210} \right\rfloor = 1$$

By the Principle of Inclusion-Exclusion, the number of integers between 1 and 250 that are divisible by at least one of 2, 3, 5 and 7 is given by

$$\begin{aligned} |A \cup B \cup C \cup D| &= \{|A| + |B| + |C| + |D|\} - \{|A \cap B| + \dots \\ &\quad + |C \cap D| + \{|A \cap B \cap C| + \dots \\ &\quad + |B \cap C \cap D|\} - \{|A \cap B \cap C \cap D|\} \\ &= (125 + 83 + 50 + 35) - (41 + 25 + 17 \\ &\quad + 16 + 11 + 7) + (8 + 5 + 3 + 2) - 1 \\ &= 293 - 117 + 18 - 1 = 193 \end{aligned}$$

$$\begin{aligned} \therefore \text{Number of integers between 1 and 250 that are not divisible by any of the integers 2, 3, 5 and 7} \\ &= \text{Total no. of integers} - |A \cup B \cup C \cup D| \\ &= 250 - 193 = 57. \end{aligned}$$

Example 2.25 How many solutions does the equation $x_1 + x_2 + x_3 = 11$ have, where x_1, x_2, x_3 are non-negative such that $x_1 \leq 3, x_2 \leq 4$ and $x_3 \leq 6$? Use the principle of inclusion-exclusion.

Let the total no. of solutions with no restrictions be N .

Let P_1, P_2, P_3 denote respectively the properties $x_1 > 3, x_2 > 4$ and $x_3 > 6$.

Then the required no. of solutions is given by

$$N = \{ |P_1| + |P_2| + |P_3| - |P_1 \cap P_2| - |P_2 \cap P_3| - |P_3 \cap P_1| \\ + |P_1 \cap P_2 \cap P_3| \} \quad (1)$$

Now $N = C(3 + 11 - 1, 11) = 78$ (Refer to Example 2.13)

$$|P_1| = \text{no. of solutions subject to } P_1 \text{ (viz. } x_1 \geq 4 \text{ or } x_1 = 4, 5, 6, \dots, 11) = C(3 + 7 - 1, 7) = C(9, 7) = 36 \quad (\because x_2 \leq 7 \text{ and } x_3 \leq 7)$$

$$\text{Similarly, } |P_2| = C(3 + 6 - 1, 6) = C(8, 6) = 28$$

$$|P_3| = C(3 + 4 - 1, 4) = C(6, 4) = 15$$

$$|P_1 \cap P_2| = \text{no. of solutions subject to } x_1 \geq 4 \text{ and } x_2 \geq 5 \\ = C(3 + 2 - 1, 2) = C(4, 2) = 6 \quad [\because x_3 \leq 2]$$

$$\text{Similarly, } |P_2 \cap P_3| = 0 \quad (\because x_1 \leq -1) \text{ and } |P_3 \cap P_1| = C(3 + 0 - 1, 0) = 1$$

$$|P_1 \cap P_2 \cap P_3| = \text{no. of solutions subject to } x_1 \geq 4, x_2 \geq 5 \text{ and } x_3 \geq 7 \\ = 0$$

\therefore Required number of solutions

$$= 78 - \{(36 + 28 + 15) - (6 + 0 + 1) + 0\} \\ = 6.$$

Example 2.26 There are 250 students in an engineering college. Of these 188 have taken a course in Fortran, 100 have taken a course in C and 35 have taken a course in Java. Further 88 have taken courses in both Fortran and C. 23 have taken courses in both C and Java and 29 have taken courses in both Fortran and Java. If 19 of these students have taken all the three courses, how many of these 250 students have not taken a course in any of these three programming languages?

Let F, C and J denote the students who have taken the languages Fortran, C and Java respectively.

$$\text{Then } |F| = 188; |C| = 100; |J| = 35$$

$$|F \cap C| = 88; |C \cap J| = 23; |F \cap J| = 29 \text{ and } |F \cap C \cap J| = 19.$$

Then the number of students who have taken at least one of the three languages is given by

$$|F \cup C \cup J| = |F| + |C| + |J| - |F \cap C| - |C \cap J| - |F \cap J| + |F \cap C \cap J| \\ = (188 + 100 + 35) - (88 + 23 + 29) + 19 \\ = 323 - 140 + 19 = 202.$$

No. of students who have not taken a course in any of these languages

$$= 250 - 202 = 48.$$

Example 2.27 A_1, A_2, A_3 and A_4 are subsets of a set U containing 75 elements with the following properties. Each subset contains 28 elements; the intersection of any two of the subsets contains 12 elements; the intersection of any three of the subsets contains 5 elements; the intersection of all four subsets contains 1 element.

- (a) How many elements belong to none of the four subsets?

- (b) How many elements belong to exactly one of the four subsets?
(c) How many elements belong to exactly two of the four subsets?

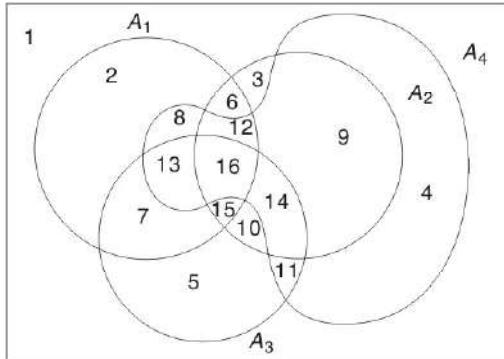


Fig. 2.1

- (a) No. of elements that belong to at least one of the four subsets
 $= |A_1 \cup A_2 \cup A_3 \cup A_4|$
 $= [|\{A_1\}| + |\{A_2\}| + |\{A_3\}| + |\{A_4\}|] - |\{A_1 \cap A_2\}| - |\{A_1 \cap A_3\}| - |\{A_1 \cap A_4\}|$
 $\quad + |\{A_2 \cap A_3\}| + |\{A_2 \cap A_4\}| + |\{A_3 \cap A_4\}| + |\{A_1 \cap A_2 \cap A_3\}|$
 $\quad + |\{A_1 \cap A_2 \cap A_4\}| + |\{A_1 \cap A_3 \cap A_4\}| + |\{A_2 \cap A_3 \cap A_4\}|$
 $\quad - |\{A_1 \cap A_2 \cap A_3 \cap A_4\}|$
 $= [4 \times 28 - 6 \times 12 + 4 \times 5 - 1] = 59$
- \therefore No. of elements that belong to none of the four subset = $75 - 59 = 16$.
- (b) With reference to the Venn diagram given above Fig. 2.1, $n(A_1 \text{ alone})$
 $= n[(2)]$
 $= n(A_1) - [n(6) + n(7) + n(8) + n(12) + n(13) + n(15) + n(16)]$
 $= n(A_1) - [\{n(6) + n(12) + n(15) + n(16)\} + \{n(7) + n(13) + n(15)$
 $\quad + n(16)\} + \{n(8) + n(12) + n(13) + n(16)\} - n(12) - n(13) - n(15)$
 $\quad - 2n(16)]$
 $= n(A_1) - [n(A_1 \cap A_2) + n(A_1 \cap A_3) + n(A_1 \cap A_4)] + [n(A_1 \cap A_2 \cap A_4)$
 $\quad + n(A_1 \cap A_3 \cap A_4) + n(A_1 \cap A_2 \cap A_3)] - 2n[(A_1 \cap A_2 \cap A_3 \cap A_4)]$
 $= 28 - 3 \times 12 + 3 \times 5 + 2 \times 1$
 $= 9$
- Similarly $n(A_2 \text{ alone}) = n(A_3 \text{ alone}) = n(A_4 \text{ alone}) = 9$
 \therefore No. of elements that belong to exactly one of the subsets = 36.
- (c) With reference to the Venn diagram of Fig. 2.1 given above,
 $n(A_1 \text{ and } A_2 \text{ only}) = n(6)$
 $= n(A_1 \cap A_2) - \{n(15) + n(16)\} - \{n(12) + n(16)\} + n(16)$
 $= n(A_1 \cap A_2) - n(A_1 \cap A_2 \cap A_3) - n(A_1 \cap A_2 \cap A_4)$
 $\quad + n(A_1 \cap A_2 \cap A_3 \cap A_4)$
 $= 12 - 5 - 5 + 1 = 3$
- Similarly $n(A_1 \text{ and } A_3 \text{ only}) = n(A_1 \text{ and } A_4 \text{ only})$
 $= n(A_2 \text{ and } A_3 \text{ only}) = n(A_2 \text{ and } A_4 \text{ only}) = n(A_3 \text{ and } A_4 \text{ only}) = 3$
 \therefore No. of elements that belong to exactly two of the subsets = 18.

Example 2.28 Show that the number of derangements of a set of n elements is given by

$$D_n = n! \left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right].$$

Note A *derangement* is a permutation of objects in which no object occupies its original position. For example, the derangements of 1 2 3 are 2 3 1 and 3 1 2. viz., $D_3 = 2$. 2 1 4 5 3 is a derangement of 1 2 3 4 5, but 2 1 5 4 3 is not a derangement of 1 2 3 4 5, since 4 occupies its original position.

Proof

Let a permutation have the property A_r , if it contains the r^{th} element in the r^{th} position.

Then D_n = the no. of the permutations having none of the properties

$$\begin{aligned} & A_r(r = 1, 2, \dots, n) \\ &= |A'_1 \cap A'_2 \cap \cdots \cap A'_n| \\ &= N - \sum_i |A_i| + \sum_{i < j} |A_i \cap A_j| - \sum_{i < j < k} |A_i \cap A_j \cap A_k| + \cdots \\ &\quad + (-1)^n |A_1 \cap A_2 \dots A_n| \end{aligned} \tag{1}$$

by the principle of inclusion-exclusion, where N is no. of permutations of n elements and so equals $n!$

Now $|A_i| = (n - 1)!$, since $|A_i|$ is the number of permutations in which the i^{th} position is occupied by the i^{th} element, but each of the remaining positions can be filled arbitrarily.

Similarly, $|A_i \cap A_j| = (n - 2)!$, $|A_i \cap A_j \cap A_k| = (n - 3)!$ and so on.

Since there are $C(n, 1)$ ways of choosing one element from n , we get

$$\sum_i |A_i| = C(n, 1) \cdot (n - 1)!$$

Similarly, $\sum_{i < j} |A_i \cap A_j| = C(n, 2) \cdot (n - 2)!$,

$$\sum_{i < j < k} |A_i \cap A_j \cap A_k| = C(n, 3) \cdot (n - 3)! \text{ and so on.}$$

Using these values in (1), we have

$$\begin{aligned} D_n &= n! - C(n, 1) \cdot (n - 1)! + C(n, 2) \cdot (n - 2)! - \dots \\ &\quad + (-1)^n \cdot C(n, n) \cdot (n - n)! \end{aligned} \tag{2}$$

$$\text{i.e., } D_n = n! - \frac{n!}{1!(n-1)!}(n-1)! + \frac{n!}{2!(n-2)!}(n-2)! - \cdots + (-1)^n \frac{n!}{n!0!}0!$$

$$= n! \left\{ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right\}$$

Example 2.29 Five gentlemen A, B, C, D and E attend a party, where before joining the party, they leave their overcoats in a cloak room. After the party, the overcoats get mixed up and are returned to the gentlemen in a

random manner. Using the principle of inclusion-exclusive, find the probability that none receives his own overcoat.

$$\text{Required probability} = \frac{\text{No. of permutations in which none gets his overcoat}}{\text{No. of all possible permutations of the coats}}$$

$$\begin{aligned} &= \frac{D_5}{5!} = \frac{5! \left\{ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} \right\}}{5!} \\ &= 1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120} = \frac{11}{30}. \end{aligned}$$

Example 2.30 In how many ways can the integers 1 through 9 be permuted such that

- (a) no odd integer will be in its natural position?
- (b) no even integer will be in its natural position?
- (c) there are 5 odd integers between 1 and 9 inclusive.

Proceeding as in example (2.28) and from step (2) of that example,

$$\begin{aligned} \text{The required no. of ways} &= 9! - [C(5, 1) \cdot 8! - C(5, 2) \cdot 7! \\ &\quad + C(5, 3) \cdot 6! - C(5, 4) \cdot 5! + C(5, 5) \cdot 4!] \\ &= 2, 05, 056. \end{aligned}$$

- (b) There are 4 even integers between 1 and 9.

$$\begin{aligned} \therefore \text{The required no. of ways} &= 9! - [C(4, 1) \cdot 8! - C(4, 2) \cdot 7! \\ &\quad + C(4, 3) \cdot 6! - C(4, 4) \cdot 5!] \\ &= 2, 29, 080. \end{aligned}$$

EXERCISE 2(A)



Part A: (Short answer questions)

1. Define r -permutation and r -combination of n elements and express their values in terms of factorials.
2. Establish Pascal's identity in the theory of combinations.
3. How many permutations are there for the 8 letters a, b, c, d, e, f, g, h ? How many of them (i) start with a , (ii) end with h , (iii) start with a and end with h ?
4. In how many ways can the symbols a, b, c, d, e, e, e, e be arranged so that no e is adjacent to another e ?
5. What is the number of arrangements of all the six letters in the word PEPPER?
6. How many distinct four-digit integers can one make form the digits 1, 3, 3, 7, 7 and 8?
7. In how many ways can 7 people be arranged about a circular table? If 2 of them insist on sitting next to each other, how many arrangements are possible?

Permutations and Combinations

Type	Formulas	Explanation of Variables	Example
Permutation with repetition (Use permutation formulas <i>when order matters</i> in the problem.)	n^r	Where n is the number of things to choose from, and you choose r of them.	A lock has a 5 digit code. Each digit is chosen from 0-9, and a digit can be repeated. How many different codes can you have? $n = 10, r = 5$ $10^5 = 100,000 \text{ codes}$
Permutation without repetition (Use permutation formulas <i>when order matters</i> in the problem.)	$\frac{n!}{(n - r)!}$	Where n is the number of things to choose from, and you choose r of them. Sometimes you can see the following notation for the same concept: $P(n, r) = {}^n P_r = {}_nP_r = \frac{n!}{(n - r)!}$	How many ways can you order 3 out of 16 different pool balls? $n = 16, r = 3$ $\frac{16!}{(16 - 3)!} = 3,360 \text{ ways}$
Combination with repetition (Use combination formulas <i>when order doesn't matter</i> in the problem.)	$\frac{(n + r - 1)!}{r!(n - 1)!}$	Where n is the number of things to choose from, and you choose r of them.	If there are 5 flavors of ice cream and you can have 3 scoops of ice cream, how many combinations can you have? You can repeat flavors. $n = 5, r = 3$ $\frac{(5 + 3 - 1)!}{3!(5 - 1)!} = 35 \text{ combinations}$
Combination without repetition (Use combination formulas <i>when order doesn't matter</i> in the problem.)	$\frac{n!}{r!(n - r)!}$	Where n is the number of things to choose from, and you choose r of them. Sometimes you can see the following notation for the same concept: $C(n, r) = {}^n C_r = {}_n C_r = \binom{n}{r} = \frac{n!}{r!(n - r)!}$	The state lottery chooses 6 different numbers between 1 and 50 to determine the winning numbers. How many combinations are possible? $n = 50, r = 6$ $\frac{50!}{6!(50 - 6)!} = 15,890,700 \text{ combinations}$

Examples

- 1) Mr. Smith is the chair of a committee. How many ways can a committee of 4 be chosen from 9 people given that Mr. Smith must be one of the people selected?**

Mr. Smith is already chosen, so we need to choose another 3 from 8 people. In choosing a committee, order doesn't matter, so we need the combination without repetition formula.

$$\frac{n!}{r!(n-r)!} = \frac{8!}{3!(8-3)!} = 56 \text{ ways}$$

- 2) A certain password consists of 3 different letters of the alphabet where each letter is used only once. How many different possible passwords are there?**

Order does matter in a password, and the problem specifies that you cannot repeat letters. So, you need a permutations without repetitions formula. The number of permutations of 3 letters chosen from 26 is

$$\frac{n!}{(n-r)!} = \frac{26!}{(26-3)!} = 15,600 \text{ passwords}$$

- 3) A password consists of 3 letters of the alphabet followed by 3 digits chosen from 0 to 9. Repeats are allowed. How many different possible passwords are there?**

Order does matter in a password, and the problem specifies that you can repeat letters. So, you need a permutations with repetitions formula.

The different ways you can arrange the letters = $n^r = 26^3 = 17,576$

The different ways you can arrange the digits = $n^r = 10^3 = 1,000$

So the number of possible passwords = $17,576 \times 1,000 = 17,576,000$ passwords

- 4) An encyclopedia has 6 volumes. In how many ways can the 6 volumes be placed on the shelf?**

This problem doesn't require a formula from the chart. Imagine that there are 6 spots on the shelf. Place the volumes one by one.

The first volume to be placed could go in any 1 of the 6 spots. The second volume to be placed could then go in any 1 of the 5 remaining spots, and so on. So the total number of ways the 6 volumes could be placed is

$$6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720 \text{ ways}$$

8. What are the number of r -permutations and r -combinations of n objects if the repetition of objects is allowed?
9. How many different outcomes are possible when 5 dice are rolled?
10. A book publisher has 3000 copies of a Discrete Mathematics book. How many ways are there to store these books in their 3 warehouses if the copies of the book are identical?
11. State pigeonhole principle and its generalisation.
12. Show that in any group of eight people, at least two have birthdays which fall on the same day of the week in any given year.
13. In a group of 100 people, several will have birth days in the same month. At least how many must have birth days in the same month?
14. If 20 processors are interconnected and every processor is connected to at least one other, show that at least two processors are directly connected to the same number of processors.
15. State the principle of inclusion-exclusion as applied to two finite subsets. Extend it for three finite subsets.
16. Among 30 Computer Science students, 15 know JAVA, 12 know C++ and 5 know both. How many students know (i) at least one of the two languages (ii) exactly one of the languages.
17. How many positive integers not exceeding 1000 are divisible by 7 or 11?
18. What is a derangement? Given an example.
19. Seven books are arranged in alphabetical order by author's name. In how many ways can a little boy rearrange these books so that no book is in its original position?
20. How many permutations of 1, 2, 3, 4, 5, 6, 7 are not derangements?

Part B

21. (i) In how many numbers with 7 distinct digits do only the digits 1 – 9 appear?
 (ii) How many of the numbers in (i) contain a 3 and a 6?
 (iii) In how many of the numbers in (i), do 3 and 6 occur consecutively in any order?
 (iv) How many of the numbers in (i) contain neither a 3 nor a 6?
 (v) How many of the numbers in (i) contain a 3 not a 6?
 (vi) In how many of the numbers in (i) do exactly one of the numbers 3, 6 appear?
 (vii) In how many of the numbers in (i) do neither of the consecutive pairs 36 and 63 appear?
22. In how many ways can two couples Mrs. and Mr. A and Mrs. and Mr. B form a line so that (i) the A's are beside each other? (ii) the A's are not beside each other? (iii) each couple is together? (iv) the A's are beside each other but the B's are not? (v) at least one couple is together? (vi) exactly one couple is together?
23. Three couples, A's, B's and C's are going to form a line (i) In how many such lines will Mr. and Mrs. B be next to each other? (ii) In how many

- such lines will Mr. and Mrs. B be next to each other and Mr. and Mrs. C be next to each other? (iii) In how many such lines will at least one couple be next to each other?
24. A Computer Science professor has 7 different programming books on a shelf, 3 of them deal with C++ and the other 4 with Java. In how many ways can the professor arrange these books on the shelf (i) if there are no restrictions? (ii) if the languages should alternate? (iii) if all the C++ books must be next to each other and all the Java books must be next to each other? (iv) if all the C++ books must be next to each other?
 25. (i) In how many possible ways could a student answer a 10-question true or false test? (ii) In how many ways can the student answer the test in (i) if it is possible to leave a question unanswered in order to avoid an extra penalty for a wrong answer?
 26. How many bit strings of length 12 contain (i) exactly three 1s? (ii) at most three 1s? (iii) at least three 1s? (iv) an equal number of 0s and 1s?
 27. A coin is flipped 10 times where each flip comes up either head or tail. How many possible outcomes (i) are there in total? (ii) contain exactly 2 heads? (iii) contain at most 3 tails? (iv) contain the same number of heads and tails?
 28. How many bit strings of length 10 have (i) exactly three 0s? (ii) at least three 1s? (iii) more 0s than 1s? (iv) an odd number of 0s?
 29. How many permutations of the letters $ABCDEFGH$ contain (i) the string ED ? (ii) the string CDE ? (iii) the strings BA and FGH ? (iv) the strings AB , DE and GH ? (v) the strings CAB and BED ? (vi) the strings BCA and ABF ?
 30. Determine how many strings can be formed by arranging the letters $ABCDE$ such that (i) A appears before D , (ii) A and D are side by side, (iii) neither the pattern AB nor the pattern CD appears, (iv) neither the pattern AB nor the pattern BE appears.
 31. In how many ways can the letters A, B, C, D, E, F be arranged so that (i) B is always to the immediate left of the letter E (ii) B is always to the left of the letter E (iii) B is never to the left of the letter E ?
 32. In how different ways can the letters in the word MISSISSIPPI be arranged (i) if there is no restriction? (ii) if the two P s must be separated?
 33. In how many ways can the letters $A, A, A, A, A, B, C, D, E$ be permuted such that (i) no two A s are adjacent? (ii) if no two of the letters B, C, D, E are adjacent?
 34. A computer password consists of a letter of the English alphabet followed by 3 or 4 digits. Find the number of passwords (i) that can be formed and (ii) in which no digit repeats.
 35. (i) In how many ways can 7 people be arranged about a circular table? (ii) If two of the people insist on sitting next to each other, how many arrangements are possible?

36. There are 6 gentlemen and 4 ladies to dine at a round table. In how many ways can they be seated so that no two ladies are together?
 37. A committee of 12 is to be selected from 10 men and 10 women. In how many ways can the selection be carried out if (i) there are no restrictions? (ii) there must be equal number of men and women? (iii) there must be an even number of women? (iv) there must be more women than men? (v) there must be at least 8 men?
 38. 7 women and 9 men are on the faculty in the mathematics department of a college. (i) How many ways are there to select a committee of 5 members of the department if at least one woman must be on the committee? (ii) How many ways are there to select a committee of 5 members of the department if at least one woman and at least one man must be on the committee?
 39. How many licence plates consisting of 3 English letters followed by 3 digits contain no letter or digit twice?
 40. How many strings of 6 distinct letters from the English alphabet contain (i) the letter A ? (ii) the letters A and B ? (iii) the letters A and B in consecutive positions with A preceding B ? (iv) the letters A and B where A is somewhere to the left of B in the string?
 41. A student has to answer 10 out of 13 questions in an exam. How many choices has he (i) if there is no restriction? (ii) if he must answer the first two questions? (iii) if he must answer the first or second question but not both? (iv) if he must answer exactly three out of the first 5 questions? (v) if he must answer at least 3 of the first 5 questions?
 42. In how many ways can we distribute 8 identical white balls into 4 distinct containers so that (i) no container is left empty? (ii) the fourth container has an odd number of balls in it?
 43. Find the number of unordered samples of size 5 (repetition allowed) from the set of letters (A, B, C, D, E, F) , if (i) there is no restriction, (ii) the letter A occurs exactly twice, (iii) the letter A occurs at least twice.
 44. Find the number of integer solutions of the equation $x_1 + x_2 + x_3 + x_4 = 21$, where $x_1 \geq 8$ and x_2, x_3, x_4 are non-negative.
 45. There are 10 questions on a discrete mathematics test. How many ways are there to assign marks to the problems, if the maximum of the test paper is 100 and each question is worth at least 5 marks?
 46. How many integers between 1 and 10,00,000 have the sum of the digits equal to 15?
 47. Show that among $(n + 1)$ arbitrarily chosen integers, there must exist two whose difference is divisible by n .
- [*Hints:* n of $(n + 1)$ integers, when divided by n will leave any of the remainders $0, 1, 2, \dots, (n - 1)$ and $(n + 1)^{\text{th}}$ integer also will leave one of the remainders $0, 1, 2, \dots, (n - 1)$.]
48. If there are 5 points inside a square of side length 2, prove that two of the points are within a distance of $\sqrt{2}$ of each other.

49. Of any 5 points chosen within an equilateral triangle whose sides are of length 1, show that two are within a distance of $\frac{1}{2}$ of each other.
50. Of any 26 points within a rectangle measuring 20 cm by 15 cm, show that at least two are within 5 cm of each other.
- [Hint: Divide the rectangle into subrectangles of dimension 4×3 cm.]
51. Prove that, in any list of 10 natural numbers a_1, a_2, \dots, a_{10} , there is a string of consecutive items of the list whose sum is divisible by 10.
52. How many integers between 1 and 300 (both inclusive) are divisible by (i) at least one of 3, 5, 7? (ii) 3 and by 5, but not by 7? (iii) 5 but by neither 3 nor 7?
53. How many prime numbers are less than 200? Use the principle of inclusion-exclusion.
- [Hint To check if a natural number n is prime, we have to check whether the prime numbers less than or equal to \sqrt{n} are divisors of n .]
54. How many solutions does the equation $x_1 + x_2 + x_3 = 13$ have, where x_1, x_2, x_3 are non-negative integers less than 6? Use the principle of inclusion-exclusion.
55. A total of 1232 students have taken a course in Tamil, 879 have taken a course in English and 114 have taken a course in Hindi. Further, 103 have taken courses in both Tamil and English, 23 have taken courses in both Tamil and Hindi and 14 have taken courses in both English and Hindi. If 2092 students have taken at least one of Tamil, English and Hindi, how many students have taken a course in all the three languages?
56. How many derangements of $\{1, 2, 3, 4, 5, 6\}$ (i) begin with the integers 1, 2 and 3 in some order? (ii) end with the integers 1, 2 and 3 in some order?
57. In how many ways can a teacher distribute 10 distinct books to his 10 students (one book to each student) and then collect and redistribute the books so that each student has the opportunity to peruse two different books?
58. There are 7 letters to be delivered to 7 houses in a block, one addressed to each house. If the letters are delivered completely at random, at the rate of one letter to each house, in how many ways can this be done if (i) no letter arrives at the right house? (ii) at least one letter arrives at the right house? (iii) all letters arrive at the right house?
59. Twenty people check their hats at a theatre. In how many ways can their hats be returned, so that (i) no one receives his or her own hat? (ii) at least one person receives his or her own hat? (iii) exactly one person receives his or her own hat?
60. A child inserts letters randomly into envelopes. What is the probability that in a group of 10 letters

- (i) no letter is put into the correct envelope?
- (ii) exactly one letter is put into the correct envelope?
- (iii) exactly 8 letters are put into the correct envelopes?
- (iv) exactly 9 letters are put into the correct envelopes?
- (v) all letters are put into the correct envelope?

MATHEMATICAL INDUCTION

One of the most basic methods of proof is mathematical induction, which is a method to establish the truth of a statement about all the natural numbers. It will often help us to prove a general mathematical statement involving positive integers when certain instances of that statement suggest a general pattern.

Statement of the Principle of Mathematical Induction

Let $S(n)$ denote a mathematical statement (or a set of such statements) that involves one or more occurrences of the variable n , which represents a positive integer (a) If $S(1)$ is true and (b) If, whenever $S(k)$ is true for some particular, but arbitrarily chosen $k \in \mathbb{Z}^+$, $S(k + 1)$ is also true, then $S(n)$ is true for all $n \in \mathbb{Z}^+$.

- Note**
- (1) The condition (a) is known as the *basis step* and the condition (b) is known as the *inductive step*.
 - (2) In condition (a), the choice of 1 is not mandatory, viz., $S(n)$ may be true for some first element $n_0 \in \mathbb{Z}$, so that the induction process has a starting place.

Strong Form of the Principle

Given a mathematical statement $S(n)$ that involves one or more occurrences of the positive integer n and if

- (a) $S(1)$ is true and
- (b) whenever $S(1), S(2), \dots, S(k)$ are true, $S(k + 1)$ is also true, then $S(n)$ is true for all $n \in \mathbb{Z}^+$.

Well-ordering Principle

As an application of the principle of mathematical induction, we shall now establish the *well-ordering principle* which states that every non-empty set of non-negative integers has a smallest element.

A set containing just one element has a smallest member, namely the element itself. Hence, the well-ordering principle is true for sets of size 1.

Now let us assume that the principle is true for sets of size k , viz., any set of k non-negative integers has a smallest member.

Let us not consider a set S of $(k + 1)$ numbers from which one element ' a ' is removed. The remaining k numbers have a smallest element, say b . [by the induction hypothesis]. The smaller of a and b is the smallest element of S .

Hence, by the principle of mathematical induction, it follows that any finite set of non-negative integers has a smallest element.

RECURRENCE RELATIONS

Definition

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

If the terms of a sequence satisfy a recurrence relation, then the sequence is called a *solution* of the recurrence relation.

For example, let us consider the geometric progression 4, 12, 36, 108, ..., the common ratio of which is 3. If $\{a_n\}$ represents this infinite sequence, we see

that $\frac{a_{n+1}}{a_n} = 3$ viz., $a_{n+1} = 3a_n, n \geq 0$ is the recurrence relation corresponding

to the geometric sequence $\{a_n\}$. However, the above recurrence relation does not represent a unique geometric sequence. The sequence 5, 15, 45, 135, ... also satisfies the above recurrence relation. In order that the recurrence relation $a_{n+1} = 3a_n, n \geq 0$ may represent a unique sequence, we should know one of the terms of the sequence, say, $a_0 = 4$. If $a_0 = 4$, then the recurrence relation represents the sequence 4, 12, 36, 108, ... The value $a_0 = 4$ is called the *initial condition*. If $a_0 = 4$, then from the recurrence relation, we get $a_1 = 3(4)$, $a_2 = 3^2(4)$ and so on. In general when $n \geq 0$, $a_n = 4 \cdot 3^n$. This is called the *general solution* of the recurrence relation.

As another example, we consider the famous Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, \dots,$$

which can be represented by the recurrence relation

$$F_{n+2} = F_{n+1} + F_n, \text{ where } n \geq 0 \text{ and } F_0 = 0, F_1 = 1$$

Definitions

A recurrence relation of the form

$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} = f(n)$ is called a *linear recurrence relation of degree k with constant coefficients*, where c_0, c_1, \dots, c_k are real numbers and $c_k \neq 0$. The recurrence relation is called *linear*, because each a_r is raised to the power 1 and there are no products such as $a_r \cdot a_s$. Since a_n is expressed in terms of the previous k terms of the sequence, the *degree or order* of the recurrence relation is said to be k . In other words the degree is the difference between the greatest and least subscripts of the members of the sequence occurring in the recurrence relation.

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

Note

The recurrence relations given in the above examples are linear homogeneous recurrence relations with constant coefficients and of degrees 1 and 2 respectively.

Solving Recurrence Relations

Systematic procedures have been developed for solving linear recurrence relations with constant coefficients. Let us first consider the solution of a homogeneous relation of order 2, viz., the recurrence relation of the form

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0, \quad n \geq 2 \quad (1)$$

Let $a_n = r^n$ ($r \neq 0$) be a solution of (1).

Then

$$c_0 r^n + c_1 r^{n-1} + c_2 r^{n-2} = 0$$

i.e.,

$$c_0 r^2 + c_1 r + c_2 = 0, \text{ since } r \neq 0 \quad (2)$$

(2) is a quadratic equation in r , which is called *the characteristic equation*, whose roots r_1 and r_2 are called *the characteristic roots* of the recurrence relation.

Depending on the nature of the roots r_1 and r_2 , we get 3 different forms of the solution of the recurrence relation. We state them as follows without proof:

Case (i) r_1 and r_2 are real and distinct.

The solution of the recurrence relation is $a_n = k_1 r_1^n + k_2 r_2^n$, where k_1 and k_2 , are arbitrary constants determined by initial conditions.

Case (ii) r_1 and r_2 are real and equal.

The solution is $a_n = (k_1 + k_2 n)r^n$, where $r_1 = r_2 = r$.

Case (iii) r_1 and r_2 are complex conjugate.

Let the modulus-amplitude form of $r_1 = r(\cos \theta + i \sin \theta)$

Then $r_2 = r(\cos \theta - i \sin \theta)$

The solution in this case is, $a_n = r^n(k_1 \cos n\theta + k_2 \sin n\theta)$

Theorem

The solution of a linear non-homogeneous recurrence relation with constant coefficients, viz., a recurrence relation of the form

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_{n-k} a_{n-k} = f(n) \quad (1)$$

where $f(n) \neq 0$ is of the form $a_n = a_n^{(h)} + a_n^{(p)}$, where $a_n^{(h)}$ is the solution of the associated homogeneous recurrence relation, namely,

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0 \quad (2)$$

and $a_n^{(p)}$ is a particular solution of (1).

Proof

Since $a_n = a_n^{(p)}$ is a particular solution of (1),

we have $c_0 a_n^{(p)} + c_1 a_{n-1}^{(p)} + \cdots + c_k a_{n-k}^{(p)} = f(n)$ (3)

Let $a_n = b_n$ be a second solution of (1).

Then $c_0 b_n + c_1 b_{n-1} + \cdots + c_k b_{n-k} = f(n)$ (4)

(4)–(3) gives

$$c_0 \{b_n - a_n^{(p)}\} + c_1 \{b_{n-1} - a_{n-1}^{(p)}\} + \cdots + c_{n-k} \{b_{n-k} - a_{n-k}^{(p)}\} = 0 \quad (5)$$

Step (5) means that $b_n - a_n^{(p)}$ is a solution of recurrence relation (2), viz., $a_n^{(h)}$

$$\therefore b_n = a_n^{(h)} + a_n^{(p)} \text{ for all } n.$$

i.e., the general solution of relation (1) is of the form $a_n = a_n^{(h)} + a_n^{(p)}$.

PARTICULAR SOLUTIONS

There is no general procedure for finding the particular solution of a recurrence relation. However for certain functions $f(n)$ such as polynomials in n and powers of constants, the forms of particular solutions are known and they are exactly found out by the method of undetermined coefficients.

The following table gives certain forms of $f(n)$ and the forms of the corresponding particular solution, on the assumption that $f(n)$ is not a solution of the associated homogeneous relation:

Form of $f(n)$	Form of $a_n^{(p)}$ to be assumed
c, a constant	A , a constant
n	$A_0 n + A_1$
n^2	$A_0 n^2 + A_1 n + A_2$
$n^t, t \in \mathbb{Z}^+$	$A_0 n^t + A_1 n^{t-1} + \dots + A_n$
$r^n, r \in R$	$A r^n$
$n^t r^n$	$r^n (A_0 n^t + A_1 n^{t-1} + \dots + A_n)$
$\sin \alpha n$	$A \sin \alpha n + B \cos \alpha n$
$\cos \alpha n$	$A \sin \alpha n + B \cos \alpha n$
$r^n \sin \alpha n$	$r^n (A \sin \alpha n + B \cos \alpha n)$
$r^n \cos \alpha n$	$r^n (A \sin \alpha n + B \cos \alpha n)$

When $f(n)$ is a linear combination of the terms in the first column, then $a_n^{(p)}$ is assumed as a linear combination of the corresponding terms in the second column of the table. When $f(n) = r^n$ or $(A + Bn)r^n$ where r is a non-repeated characteristic root of the recurrence relation, then $a_n^{(p)}$ is assumed as $An r^n$ or $cn(A + Bn)r^n$ as the case may be. When $f(n) = r^n$, where r is a twice repeated characteristic root, then $a_n^{(p)}$ is assumed as $An^2 r^n$ and so on.

Note For a different treatment of difference equation (recurrence relations) using the finite difference operators such as Δ and E , the students are advised to refer to the chapter on ‘Difference Equations’ in the author’s book “Numerical Methods with Programs in C”.

SOLUTION OF RECURRENCE RELATIONS BY USING GENERATING FUNCTIONS

Definition

The generating function of a sequence a_0, a_1, a_2, \dots is the expression

$$G(x) = a_0 + a_1 x + a_2 x^2 + \dots \infty = \sum_{n=0}^{\infty} a_n x^n$$

For example,

(i) the generating function for the sequence 1, 1, 1, 1, ... is given by

$$G(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

(ii) the generating function for the sequence 1, 2, 3, 4, ... is given by

$$G(x) = \sum_{n=0}^{\infty} (n+1)x^n = 1 + 2x + 3x^2 + \dots = \frac{1}{(1-x)^2}$$

(iii) the generating function for the sequence 1, a , a^2 , a^3 , ... is given by

$$G(x) = 1 + ax + a^2x^2 + \dots = \frac{1}{1-ax}, \text{ for } |ax| < 1.$$

To solve a recurrence relation (both homogeneous and non-homogeneous) with given initial conditions, we shall multiply the relation by an appropriate power of x and sum up suitably so as to get an explicit formula for the associated generating function. The solution of the recurrence relation a_n is then obtained as the coefficient of x^n in the expansion of the generating function. The procedure is explained clearly in the worked examples that follow.



WORKED EXAMPLES 2(B)

Example 2.1 Prove, by mathematical induction, that

$$1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{1}{3}n(2n-1)(2n+1).$$

Let $S(n)$: $1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{1}{3}n(2n-1)(2n+1)$.

When $n = 1$,

$$S(1): 1^2 = \frac{1}{3} \cdot 1 \cdot 1 \cdot 3$$

So $S(1)$ is true, viz., the basic step is valid.

Let $S(n)$ be true for $n = k$

$$\text{i.e., } 1^2 + 3^2 + 5^2 + \dots + (2k-1)^2 = \frac{1}{3}k(2k-1)(2k+1)$$

$$\begin{aligned} \text{Now } 1^2 + 3^2 + 5^2 + \dots + (2k-1)^2 + (2k+1)^2 \\ &= \frac{1}{3}k(2k-1)(2k+1) + (2k+1)^2, \text{ using the truth of } S(k) \\ &= \frac{1}{3}(2k+1) \{k(2k-1) + 3(2k+1)\} \\ &= \frac{1}{3}(2k+1)(2k^2+5k+3) \\ &= \frac{1}{3}(2k+1)(2k+3)(k+1) \text{ or } \frac{1}{3}(k+1)(2k+1)(2k+3) \end{aligned}$$

i.e., $S(k+1)$ is valid.

Thus the inductive step is also true.

Hence, $S(n)$ is true for all $n \in \mathbb{Z}^+$.

Example 2.2 Prove, by mathematical induction, that

$$\begin{aligned} & 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \cdots + n(n+1)(n+2) \\ &= \frac{1}{4}n(n+1)(n+2)(n+3). \end{aligned}$$

Let S_n : $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = \frac{1}{4}n(n+1)(n+2)(n+3)$.

Now S_1 : $1 \cdot 2 \cdot 3 = \frac{1}{4} \cdot 1 \cdot 2 \cdot 3 \cdot 4$

Thus, the basic step S_1 is true.

Let S_k be true

$$\text{i.e., } 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + k(k+1)(k+2) = \frac{1}{4}k(k+1)(k+2)(k+3) \quad (1)$$

$$\begin{aligned} \text{Now } [1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + k(k+1)(k+2)] + (k+1)(k+2)(k+3) \\ &= \frac{1}{4}k(k+1)(k+2)(k+3) + (k+1)(k+2)(k+3), \text{ by (1)} \\ &= \frac{1}{4}(k+1)(k+2)(k+3)\{k+4\} \end{aligned}$$

Thus S_{k+1} is true, if S_k is true.

i.e., the inductive step is true.

Hence, S_n is true for all $n \in \mathbb{Z}^+$.

Example 2.3 Prove, by mathematical induction, that

$$\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

$$\text{Let } S_n: \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

$$\text{Then } S_1: \frac{1}{1.2} = \frac{1}{1+1} \text{ which is true.}$$

i.e., the basic step S_1 is true.

Let S_k be true.

$$\text{i.e., } \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1} \quad (1)$$

$$\text{Now } \frac{1}{1.2} + \frac{1}{2.3} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)}$$

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

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

$$= \frac{1}{k+1} \left\{ \frac{(k+1)^2}{k+2} \right\} = \frac{k+1}{k+2} \quad (2)$$

(2) means that S_{k+1} is also true.

i.e., the inductive step is true.

Hence, S_n is true for all $n \in \mathbb{Z}^+$.

Example 2.4 Use mathematical induction to show that

$$n! \geq 2^{n-1}, \text{ for } n = 1, 2, 3, \dots$$

Let

$$S_n: n! \geq 2^{n-1}$$

$$\therefore S_1: 1! \geq 2^0, \text{ which is true.}$$

i.e., the basic step is true

Let S_k be true

$$\text{i.e., } k! \geq 2^{k-1}$$

$$\text{Now } (k+1)! = (k+1) \cdot k!$$

$$\geq (k+1) \cdot 2^{k-1}, \text{ by (1)}$$

$$\geq 2 \cdot 2^{k-1}, \text{ since } k+1 \geq 2$$

$$= 2^k \quad (2)$$

Step (2) means that S_{k+1} is also true.

i.e., the inductive step is true.

Hence, S_n is true for $n = 1, 2, 3, \dots$

Example 2.5 Use mathematical induction to show that

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}, \text{ for } n \geq 2$$

$$\text{Let } S_n: \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > \sqrt{n}$$

$$\therefore S_2: \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} > \sqrt{2}, \text{ since L.S = 1.707 and R.S = 1.414}$$

i.e., the basic step is true for $n = 2$.

Let S_k be true.

$$\text{i.e., } \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} > \sqrt{k} \quad (1)$$

$$\text{Now } \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} > \sqrt{k} + \frac{1}{\sqrt{k+1}}, \text{ by (1)}$$

$$\text{Now } \sqrt{k} + \frac{1}{\sqrt{k+1}} = \frac{\sqrt{k(k+1)} + 1}{\sqrt{k+1}} > \frac{\sqrt{k \cdot k} + 1}{\sqrt{k+1}}$$

$$\text{i.e., } > \frac{k+1}{\sqrt{k+1}}$$

i.e.,

$$> \sqrt{k+1}$$

$$\therefore \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} > \sqrt{k+1} \quad (2)$$

Step (2) means that S_{k+1} is also true.

Hence, S_n is true for $n = 2, 3, 4, \dots$.

Example 2.6 Use mathematical induction to show that

$$\frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} \leq \frac{1}{\sqrt{n+1}}, \text{ for } n = 1, 2, 3, \dots$$

Let $S_n: \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} \leq \frac{1}{\sqrt{n+1}}$

$$\therefore S_1: \frac{1}{2} \leq \frac{1}{2}, \text{ which is true.}$$

i.e., the basic step is true.

Let S_k be true.

$$\text{i.e., } \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)}{2 \cdot 4 \cdot 6 \cdots (2k)} \leq \frac{1}{\sqrt{k+1}} \quad (1)$$

$$\text{Now } \frac{1 \cdot 3 \cdot 5 \cdots (2k-1) \cdot (2k+1)}{2 \cdot 4 \cdot 6 \cdots (2k) \cdot (2k+2)} \leq \frac{1}{\sqrt{k+1}} \cdot \frac{2k+1}{2k+2}, \text{ by (1)} \quad (2)$$

$$\text{Now } \frac{2k+1}{2k+2} \leq \frac{\sqrt{k+1}}{\sqrt{k+2}},$$

$$\text{if } \frac{(2k+1)^2}{(2k+2)^2} \leq \frac{k+1}{k+2}$$

$$\text{i.e., if } \frac{4k^2 + 4k + 1}{4k^2 + 8k + 4} \leq \frac{k+1}{k+2}$$

$$\text{i.e., if } 4k^3 + 12k^2 + 9k + 2 \leq 4k^3 + 12k^2 + 12k + 4$$

$$\text{i.e., if } 9k + 2 \leq 12k + 4$$

$$\text{i.e., if } 3k + 2 \geq 0, \text{ which is true.}$$

Using this in step (2), we get

$$\begin{aligned} \frac{1 \cdot 3 \cdot 5 \cdots (2k-1)(2k+1)}{2 \cdot 4 \cdot 6 \cdots (2k)(2k+2)} &\leq \frac{1}{\sqrt{k+1}} \cdot \frac{\sqrt{k+1}}{\sqrt{k+2}} \\ \text{i.e.,} &\leq \frac{1}{\sqrt{k+2}} \end{aligned} \quad (3)$$

Step (3) means that S_{k+1} also true.

i.e., the induction step is true.

Hence, S_n is true for $n = 1, 2, 3, \dots$

Example 2.7 Use mathematical induction to prove that $H_{2^n} \geq 1 + \frac{n}{2}$, where

$$H_j = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{j}.$$

$$\text{Let } S_n: H_{2^n} \geq 1 + \frac{n}{2}$$

$$\therefore S_1: H_2 = 1 + \frac{1}{2} \geq 1 + \frac{1}{2}, \text{ which is true.}$$

i.e., the basic step is true.

Let S_k be true.

$$\text{i.e., } 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k} \geq 1 + \frac{k}{2} \quad (1)$$

$$\text{Now } 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k} + \frac{1}{2^{k+1}}$$

$$= \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{2^k} \right) + \left(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^{k+1}} \right)$$

$$\geq \left(1 + \frac{k}{2} \right) + \left(\frac{1}{2^k+1} + \frac{1}{2^k+2} + \dots + \frac{1}{2^k+2^k} \right)$$

$$\geq \left(1 + \frac{k}{2} \right) + 2k \cdot \frac{1}{2^{k+1}} \quad (\because \text{each of the } 2^k \text{ terms in the second group } \geq \frac{1}{2^{k+1}}, \text{ the last term})$$

$$\text{i.e., } \geq \left(1 + \frac{k}{2} \right) + \frac{1}{2}$$

$$\text{i.e., } \geq 1 + \left(\frac{k+1}{2} \right) \quad (2)$$

Step (2) means that S_{k+1} is true.

i.e., the inductive step is true.

$\therefore S_n$ is true for $n \in \mathbb{Z}^+$.

Example 2.8 Use mathematical induction to prove that $n^3 + 2n$ is divisible by 3, for $n \geq 1$.

Let $S_n: (n^3 + 2n)$ is divisible by 3.

$\therefore S_1: (1^3 + 2)$ is divisible by 3, which is true.

i.e., the basic step is true.

Let S_k be true.

$$\text{i.e., } k^3 + 2k \text{ is divisible by 3} \quad (1)$$

Now
$$(k+1)^3 + 2(k+1) \\ = (k^3 + 2k) + (3k^2 + 3k + 3)$$

$(k^2 + 2k)$ is divisible by 3, by (1)

Also $3k^3 + 3k + 3 = 3(k^2 + k + 1)$ is divisible by 3.

∴ The sum, namely, $(k+1)^3 + 2(k+1)$ is divisible by 3 (2)

i.e., S_{k+1} is also true

i.e., the inductive step is true.

∴ S_n is true for $n \geq 1$.

Example 2.9 Use mathematical induction to prove that

$n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9, for $n \geq 1$.

Let $S_n: n^3 + (n+1)^3 + (n+2)^3$ is divisible by 9.

∴ $S_1: 1^3 + 2^3 + 3^3 = 36$ is divisible by 9, which is true.

i.e., the basic step is true.

Let S_k be true.

i.e., $k^3 + (k+1)^3 + (k+2)^3$ is divisible by 9 (1)

Now
$$(k+1)^3 + (k+2)^3 + (k+3)^3 \\ = [k^3 + (k+1)^3 + (k+2)^3] + [9k^2 + 27k + 27] \\ = [k^3 + (k+1)^3 + (k+2)^3] + 9(k^2 + 3k + 3)$$

The first expression is divisible by 9 [by (1)] and the second expression is a multiple of 9.

∴ Their sum is divisible by 9

i.e., S_{k+1} is true.

i.e., the inductive step is true.

∴ S_n is true for $n \geq 1$.

Example 2.10 Use mathematical induction to prove that $(3^n + 7^n - 2)$ is divisible by 8, for $n \geq 1$.

Let $S_n: (3^n + 7^n - 2)$ is divisible by 8

∴ $S_1: (3+7-2)$ is divisible by 8, which is true.

i.e., the basic step is true.

Let S_k be true.

i.e., $(3^k + 7^k - 2)$ is divisible by 8 (1)

Now
$$3^{k+1} + 7^{k+1} - 2 = 3(3^k) + 7(7^k) - 2 \\ = 3\{3^k + 7^k - 2\} + 4(7^k + 1) \quad (2)$$

$3(3^k + 7^k - 2)$ is divisible by 8, by step (1)

$7^k + 1$ is an even number, for $k \geq 1$

∴ $4(7^k + 1)$ is divisible by 8

∴ R.S. of (2) is divisible by 8

i.e., $3^{k+1} + 7^{k+1} - 2$ is divisible by 8

i.e., S_{k+1} is also true.

i.e., the inductive step is true

∴ S_n is true for $n \geq 1$.

Example 2.11 Solve the recurrence relation $a_n - 2a_{n-1} = 3^n$; $a_1 = 5$

The characteristic equation of the recurrence relation is $r - 2 = 0 \therefore r = 2$.

$$\therefore a_n^{(h)} = c \cdot 2^n$$

Since the R.S. of the relation is 3^n , let a particular solution of the relation be $a_n = A \cdot 3^n$. Using this in the relation, we get

$$A \cdot 3^n - 2 \cdot A \cdot 3^{n-1} = 3^n$$

$$\text{i.e., } 3A - 2A = 3 \text{ or } A = 3$$

$$\therefore a_n^{(p)} = 3^{n+1}$$

$$\therefore \text{General solution is } a_n = a_n^{(h)} + a_n^{(p)} = c \cdot 2^n + 3^{n+1}$$

$$\text{Using the condition } a_1 = 5, \text{ we get } 2c + 9 = 5$$

$$\therefore c = -2$$

$$\text{Hence, the required solution is } a_n = 3^{n+1} - 2^{n+1}.$$

Example 2.12 Solve the recurrence relation

$$a_n = 2a_{n-1} + 2^n; a_0 = 2$$

The characteristic equation of the R.R. is $r - 2 = 0 \therefore r = 2$

$$\therefore a_n^{(h)} = c \cdot 2^n$$

Since the R.S. of the R.R. is 2^n and 2 is the characteristic root of the R.R., let

$$a_n = An \cdot 2^n \text{ be a particular solution of the R.R.}$$

Using this in the R.R., we get

$$An \cdot 2^n - 2(n-1)2^{n-1} = 2^n$$

$$\text{i.e., } An - (n-1) = 1 \therefore A = 1$$

$$\therefore a_n^{(p)} = n2^n$$

\therefore General solution of the R.R. is

$$\begin{aligned} a_n &= a_n^{(h)} + a_n^{(p)} \\ &= c \cdot 2^n + n \cdot 2^n \end{aligned}$$

$$\text{Given: } a_0 = 2 \therefore c = 2$$

$$\text{Hence, the required solution is } a_n = (n+2) \cdot 2^n.$$

Example 2.13 n circular disks with different diameters and with holes in their centres can be stacked on any of the three pegs mounted on a board. To start with, the pegs are stacked on peg 1 with no disk resting upon a smaller one. The objective is to transfer the disks one at a time so that we end up with the original stack on peg 2. Each of the three pegs may be used as temporary location for any disk, but at no time a larger disk should lie on a smaller one on any peg. What is the minimum number of moves required to do this for n disks?

Note This problem is popularly known as the *Tower of Hanoi problem*.

Let H_n denote the number of moves required to solve the Tower of Hanoi problem with n disks. Let us form a recurrence relation for H_n and then solve it.

To start with, the n disks are on peg 1 in the decreasing order from bottom to top. We can transfer the top $(n - 1)$ disks to peg 3, as per the rules specified, in H_{n-1} moves (by the meaning assigned to H_n). We keep the largest disk fixed in peg 1 during these moves. Then we use one move to transfer the largest disk to peg 2. We can transfer the $(n - 1)$ disks now on peg 3 to peg 2 using H_{n-1} additional moves, placing them on top of the largest disk which remains fixed in peg 2 during the second set of H_{n-1} moves.

Since the problem cannot be solved using fewer moves, we get

$H_n = 2H_{n-1} + 1$, which is the required R.R. Obviously $H_1 = 1$, since one disk can be transferred from peg 1 to peg 2 in one move.

The characteristic equation of the R.R. is $r - 2 = 0 \Rightarrow r = 2$

$$\therefore H_n^{(h)} = c \cdot 2^n.$$

Since the R.S. of the R.R. $H_n - 2H_{n-1} = 1$ is 1, let

$H_n = A$ be a particular solution of the R.R. Using this in the R.R., we have

$$A = 2A + 1$$

$$\text{i.e., } A = -1 \text{ or } H_n^{(p)} = -1$$

\therefore The general solution of the R.R. is

$$H_n = c \cdot 2^n - 1$$

Using the initial condition $H_1 = 1$, we get $2c - 1 = 1 \Rightarrow c = 1$

\therefore The required solution of the Tower of Hanoi problem is $H_n = 2^n - 1$.

Example 2.14 Solve the recurrence relation $a_{n+1} - a_n = 3n^2 - n$; $n \geq 0$, $a_0 = 3$.

The characteristic equation of the R.R. is

$$r - 1 = 0 \text{ i.e., } r = 1$$

$$\therefore a_n^{(h)} = c \cdot 1^n = c$$

Since the R.S. of the R.R. is $3n^2 - n \equiv (3n^2 - n) \cdot 1^n$, let the particular solution of the R.R. be assumed as $a_n = (A_0n^2 + A_1n + A_2)n$, since 1 is a characteristic root of the R.R. Using this in the R.R., we have

$$\{A_0(n+1)^3 + A_1(n+1)^2 + A_2(n+1)\} - \{A_0n^3 + A_1n^2 + A_2n\} = 3n^2 - n$$

$$\text{i.e., } A_0(3n^2 + 3n + 1) + A_1(2n + 1) + A_2 = 3n^2 - n$$

Comparing like terms, we have

$$A_0 = 1, \quad 3A_0 + 2A_1 = -1 \quad \text{and} \quad A_0 + A_1 + A_2 = 0.$$

Solving these equations, we get

$$A_0 = 1, \quad A_1 = -2 \quad \text{and} \quad A_2 = 1$$

$$\begin{aligned} \therefore a_n^{(p)} &= n^3 - 2n^2 + n \\ &= n(n-1)^2 \end{aligned}$$

\therefore The general solutions of the R.R. is

$$\begin{aligned} a_n &= a_n^{(h)} + a_n^{(p)} \\ &= c + n(n-1)^2 \end{aligned}$$

Given that $a_0 = 3$. $\therefore c = 3$

\therefore The required solution of the R.R. is

$$a_n = 3 + n(n - 1)^2.$$

Example 2.15 Find a formula for the general term F_n of the Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, 13,

The recurrence relation corresponding to the Fibonacci sequence $\{F_n\}$; $n \geq 0$ is $F_{n+2} = F_{n+1} + F_n$; $n \geq 0$ with the initial conditions $F_0 = 0$, $F_1 = 1$.

The characteristic equation of the R.R. is

$$r^2 - r - 1 = 0.$$

Solving it, we have $r = \frac{1 \pm \sqrt{5}}{2}$.

Since the R.S. of $F_{n+2} - F_{n+1} - F_n = 0$ is zero, the solution of the R.R. is

$$F_n = c_1 \left(\frac{1+\sqrt{5}}{2} \right)^n + c_2 \left(\frac{1-\sqrt{5}}{2} \right)^n.$$

$$F_0 = 0 \text{ gives } c_1 + c_2 = 0 \quad (1)$$

$$F_1 = 1 \text{ gives } c_1 \left(\frac{1+\sqrt{5}}{2} \right) + c_2 \left(\frac{1-\sqrt{5}}{2} \right) = 1 \quad (2)$$

$$\text{Using (1) in (2), we get } c_1 - c_2 = \frac{2}{\sqrt{5}} \quad (3)$$

$$\text{Using (1) in (3), we have } c_1 = \frac{1}{\sqrt{5}} \text{ and } c_2 = -\frac{1}{\sqrt{5}}.$$

\therefore The general term F_n of the Fibonacci sequence is given by

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n; n \geq 0.$$

Example 2.16 A particle is moving in the horizontal direction. The distance it travels in each second is equal to two times the distance it travelled in the previous second. If a_r denotes the position of the particle in the r^{th} second, determine a_r , given that $a_0 = 3$ and $a_3 = 10$.

Let a_r , a_{r+1} , a_{r+2} be the positions of the particle in the r^{th} , $(r+1)^{\text{st}}$ and $(r+2)^{\text{nd}}$ seconds.

Then $a_{r+2} - a_{r+1} = 2(a_{r+1} - a_r)$

$$\text{i.e., } a_{r+2} - 3a_{r+1} + 2a_r = 0 \quad (1)$$

The characteristic equation of the R.R. (1) is $m^2 - 3m + 2 = 0$

$$\text{i.e., } (m - 1)(m - 2) = 0 \text{ or } m = 1, 2$$

Since the R.S. of (1) is zero, the solution of the R.R. is

$$a_r = c_1 \cdot 1^r + c_2 \cdot 2^r \\ \text{i.e.,} \quad a_r = c_1 + c_2 \cdot 2^r \quad (2)$$

$$\text{Using } a_0 = 3, \text{ we have} \quad c_1 + c_2 = 3 \quad (3)$$

$$\text{Using } a_3 = 10, \text{ we have} \quad c_1 + 8c_2 = 10 \quad (4)$$

Solving (3) and (4), we get $c_1 = 2; c_2 = 1$.

\therefore The required solutions is

$$a = 2^r + 2.$$

Example 2.17 Solve the recurrence relation

$$a_{n+2} - 6a_{n+1} + 9a_n = 3(2^n) + 7(3^n), n \geq 0, \\ \text{given that } a_0 = 1 \text{ and } a_1 = 4.$$

The characteristic equation of the R.R. is

$$r^2 - 6r + 9 = 0 \quad \text{or} \quad (r - 3)^2 = 0$$

$$\therefore r = 3, 3$$

$$\therefore a_n^{(h)} = (c_1 + c_2 n) 3^n$$

Noting that 3 is a double root of the characteristic equation, we assume the particular solution of the R.R. as

$$a_n = A_0 \cdot 2^n + A_1 n^2 \cdot 3^n$$

Using this in the R.R., we have

$$A_0 \cdot 2^{n+2} + A_1(n+2)^2 \cdot 3^{n+2} - 6\{A_0 \cdot 2^{n+1} + A_1 \cdot (n+1)^2 \cdot 3^{n+1}\} \\ + 9\{A_0 \cdot 2^n + A_1 n^2 \cdot 3^n\} = 3(2^n) + 7(3^n)$$

$$\text{i.e.,} \quad A_0 2^n (4 - 12 + 9) + A_1 \cdot 3^n \{9(n+2)^2 - 18(n+1)^2 + 9n^2\} \\ = 3 \cdot (2^n) + 7 \cdot (3^n)$$

$$\text{i.e.,} \quad A_0 \cdot 2^n + A_1 \cdot 3^n \times 18 = 3 \cdot (2^n) + 7 \cdot (3^n)$$

Comparing like terms, we get

$$A_0 = 1 \text{ and } A_1 = \frac{7}{18}$$

$$\therefore a_n^{(p)} = 2^n + \frac{7}{18} n^2 \cdot 3^n$$

Hence, the general solution of the R.R. is

$$a_n = a_n^{(h)} + a_n^{(p)}$$

$$\text{i.e.,} \quad a_n = (c_1 + c_2 \cdot n) \cdot 3^n + 2^n + \frac{7}{18} n^2 \cdot 3^n$$

$$\text{Given } a_0 = 1 \quad \therefore c_1 + 1 = 1$$

$$\text{i.e.,} \quad c_1 = 0$$

$$\text{Given } a_1 = 4 \quad \therefore 3c_2 + 2 + \frac{7}{6} = 4 \quad \text{i.e., } c_2 = \frac{5}{18}$$

\therefore The required solution is

$$a_n = \frac{5}{18} n \cdot 3^n + 2^n + \frac{7}{18} n^2 \cdot 3^n.$$

Example 2.18 Solve the recurrence relation

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

The given R.R. is $a_n - 4a_{n-1} + 4a_{n-2} = (n+1)2^n$.

The characteristic equation of the R.R. is

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

i.e., $(r-2)^2 = 0$, i.e., $r = 2, 2$.

$$\therefore a_n^{(h)} = (c_1 + c_2 n) \cdot 2^n$$

Since the R.S. of the R.R. is $(n+1)2^n$, where 2 is a double root of the characteristic equation, we assume the particular solution of the R.R. as

$$a_n = n^2(A_0 + A_1 n) \cdot 2^n$$

Using this in the R.R., we have

$$n^2(A_0 + A_1 n) \cdot 2^n - 4(n-1)^2 \{A_0 + A_1(n-1)\} 2^{n-1} + 4(n-2)^2 \{A_0 + A_1(n-2)\} 2^{n-2} = (n+1)2^n$$

$$\text{i.e., } 4n^2(A_0 + A_1 n) - 8(n-1)^2 \{A_0 + A_1(n-1)\} + 4(n-2)^2 \{A_0 + A_1(n-2)\} = 4(n+1)$$

Equating coefficients of n on both sides,

$$A_1 = \frac{1}{6}$$

Equating constant terms on both sides,

$$2A_0 - 6A_1 = 1$$

$$\text{i.e., } A_0 = 1$$

$$\therefore a_n^{(p)} = \left(n^2 + \frac{n^3}{6} \right) 2^n$$

Hence, the general solution of the R.R. is

$$a_n = a_n^{(h)} + a_n^{(p)}$$

$$\text{i.e., } a_n = \left(c_1 + c_2 n + n^2 + \frac{n^3}{6} \right) 2^n.$$

Example 2.19 Solve the recurrence relation

$$a_n = 2(a_{n-1} - a_{n-2}); n \geq 2 \text{ and } a_0 = 1, a_1 = 2.$$

The given recurrence relation is

$$a_n - 2a_{n-1} + 2a_{n-2} = 0$$

The characteristic equation of the R.R. is

$$r^2 - 2r + 2 = 0$$

Solving, we have $r = 1 \pm i$

The modulus-amplitude form of

$$1 \pm i = \sqrt{2} \left(\cos \frac{\pi}{4} \pm i \sin \frac{\pi}{4} \right)$$

Hence, the general solution of the R.R. is

$$a_n = (\sqrt{2})^n \left\{ c_1 \cos \frac{n\pi}{4} \pm c_2 \sin \frac{n\pi}{4} \right\} \quad (1)$$

Using the condition $a_0 = 1$ in (1), we get $c_1 = 1$

Using $a_1 = 2$ in (1), we get

$$\sqrt{2} \left\{ \frac{1}{\sqrt{2}} + c_2 \cdot \frac{1}{\sqrt{2}} \right\} = 2$$

i.e., $c_2 = 1$

\therefore The required solution is

$$a_n = (\sqrt{2})^n \left(\cos \frac{n\pi}{4} + \sin \frac{n\pi}{4} \right).$$

Example 2.20 Form a recurrence relation satisfied by $a_n = \sum_{k=1}^n k^2$ and

find the value of $\sum_{k=1}^n k^2$, by solving it

$$a_n = \sum_{k=1}^n k^2 \quad \text{and} \quad a_{n-1} = \sum_{k=1}^{n-1} k^2$$

Hence, $a_n - a_{n-1} = n^2$. Clearly $a_1 = 1$

The characteristic equation of the R.R. is

$$r - 1 = 0 \quad \text{or} \quad r = 1$$

$$\therefore a_n^{(h)} = c \cdot 1^n = c$$

Since the R.S. of the R.R. is $n^2 = n^2 \cdot 1^n$, let the particular solution be assumed as $a_n = (A_0 n^2 + A_1 n + A_2) n$.

Using this in the R.R., we have

$$(A_0 n^2 + A_1 n + A_2) n - \{A_0(n-1)^2 + A_1(n-1) + A_2\}(n-1) = n^2$$

Equating like terms and solving, we get

$$A_0 = \frac{1}{3}, A_1 = \frac{1}{2} \text{ and } A_2 = \frac{1}{6}$$

$$\text{Hence, } a_n^{(p)} = \frac{n}{6} (2n^2 + 3n + 1)$$

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

Hence, the general solution of the R.R. is

$$a_n = c + \frac{n}{6}(n+1)(2n+1)$$

Using $a_1 = 1$, we get $c = 0$

$$\therefore a_n = \sum n^2 = \frac{1}{6}n(n+1)(2n+1).$$

Example 2.21 Use the method of generating function to solve the recurrence relation

$$a_n = 3a_{n-1} + 1; n \geq 1, \text{ given that } a_0 = 1.$$

Let the generating function of $\{a_n\}$ be $G(x) = \sum_{n=0}^{\infty} a_n x^n$.

The given R.R. is $a_n = 3a_{n-1} + 1$ (1)

$$\therefore \sum_{n=1}^{\infty} a_n x^n = 3 \sum_{n=1}^{\infty} a_{n-1} x^n + \sum_{n=1}^{\infty} x^n,$$

on multiplying both sides of (1) by x^n and summing up.

$$\text{i.e., } G(x) - a_0 = 3x G(x) + \frac{x}{1-x}$$

$$\text{i.e., } (1 - 3x) G(x) = 1 + \frac{x}{1-x} \quad (\because a_0 = 1)$$

$$\therefore G(x) = \frac{1}{(1-x)(1-3x)} = \frac{-\frac{1}{2}}{1-x} + \frac{\frac{3}{2}}{1-3x}$$

$$\text{i.e., } G(x) = -\frac{1}{2}(1-x)^{-1} + \frac{3}{2}(1-3x)^{-1}$$

$$\text{i.e., } \sum_{n=0}^{\infty} a_n x^n = -\frac{1}{2} \sum_{n=0}^{\infty} x^n + \frac{3}{2} \sum_{n=0}^{\infty} 3^n x^n$$

$\therefore a_n = \text{coefficient of } x^n \text{ in } G(x)$

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

Example 2.22 Use the method of generating function to solve the recurrence relation

$$a_n = 4a_{n-1} - 4a_{n-2} + 4^n; n \geq 2, \text{ given that } a_0 = 2 \text{ and } a_1 = 8.$$

Let the generating function of $\{a_n\}$ be $G(x) = \sum_{n=0}^{\infty} a_n x^n$.

Multiplying both sides of the given R.R. by x^n and summing up, we have

$$\sum_{n=2}^{\infty} a_n x^n = 4 \sum_{n=2}^{\infty} a_{n-1} x^n - 4 \sum_{n=2}^{\infty} a_{n-2} x^n + \sum_{n=2}^{\infty} 4^n x^n$$

i.e., $\{G(x) - a_0 - a_1 x\} = 4x \{G(x) - a_0\} - 4x^2 G(x) + \frac{1}{1-4x} - 1 - 4x.$

i.e., $(1 - 4x + 4x^2) G(x) = \frac{1}{1-4x} - 1 - 4x + 2 \quad (\because a_0 = 2 \text{ and } a_1 = 8)$

$$\begin{aligned} \therefore G(x) &= \frac{1 + (1 - 4x)^2}{(1 - 2x)^2 \cdot (1 - 4x)} \\ &= \frac{4}{1 - 4x} - \frac{2}{(1 - 2x)^2}, \text{ on splitting into partial fractions} \end{aligned}$$

i.e., $G(x) = \sum_{n=0}^{\infty} a_n x^n = 4[1 + 4x + (4x)^2 + \dots + (4x)^n + \dots \infty]$
 $- 2[1 + 2 \cdot (2x) + 3 \cdot (2x)^2 + \dots + (n+1)(2x)^n + \dots \infty]$
 $\therefore a_n = 4^{n+1} - (n+2)2^{n+1}.$

Example 2.23 Use the method of generating function to solve the recurrence relation

$$a_{n+1} - 8a_n + 16a_{n-1} = 4^n; n \geq 1; a_0 = 1, a_1 = 8.$$

Let the generating functions of $\{a_n\}$ be

$$G(x) = \sum_{n=0}^{\infty} a_n x^n$$

Multiplying both sides of the given R.R. by x^n and summing up, we have

$$\sum_{n=1}^{\infty} a_{n+1} x^n - 8 \sum_{n=1}^{\infty} a_n x^n + 16 \sum_{n=1}^{\infty} a_{n-1} x^n = \sum_{n=1}^{\infty} (4x)^n$$

i.e., $\frac{1}{x} \{G(x) - a_0 - a_1 x\} - 8 \{G(x) - a_0\} + 16x G(x) = \frac{1}{1-4x} - 1$

i.e., $(1 - 8x + 16x^2) G(x) - a_0 - a_1 x + 8a_0 x = \frac{4x^2}{1-4x}$

i.e., $G(x) = \frac{a_0 + (a_1 - 8a_0)x}{(1-4x)^2} + \frac{4x^2}{(1-4x)^3}$
 $= \frac{1}{(1-4x)^2} + \frac{4x^2}{(1-4x)^3}, \text{ on using the values of } a_0 \text{ and } a_1.$
 $= (1 - 4x + 4x^2) (1 - 4x)^{-3}$

$$\begin{aligned} \text{i.e., } \sum_{n=0}^{\infty} a_n x^n &= (1 - 4x + 4x^2) \cdot \frac{1}{2} \{1 \cdot 2 + 2 \cdot 3 (4x) + 3 \cdot 4(4x)^2 + \dots \\ &\quad + (n+1)(n+2)(4x)^n \dots\} \\ \therefore a_n &= \frac{1}{2} [(n+1)(n+2)4^n - n(n+1)4^n + (n-1)n4^{n-1}] \\ &= \frac{1}{2} 4^{n-1} \{4(n^2 + 3n + 2) - 4(n^2 + n) + (n^2 - n)\} \\ &= \frac{1}{2} (n^2 + 7n + 8) \cdot 4^{n-1}. \end{aligned}$$

Example 2.24 Use the method of generating function to solve the recurrence relation $a_{n+2} - 4a_n = 9n^2$; $n \geq 0$.

Let the generating function of $\{a_n\}$ be

$$G(x) = \sum_{n=0}^{\infty} a_n x^n$$

Multiplying both sides of the given R.R. by x^n and summing up, we have

$$\begin{aligned} \sum_{n=0}^{\infty} a_{n+2} x^n - 4 \sum_{n=0}^{\infty} a_n x^n &= 9 \sum_{n=0}^{\infty} n^2 x^n \\ \text{i.e., } \frac{1}{x^2} \{G(x) - a_0 - a_1 x\} - 4G(x) &= 9 \sum_{n=0}^{\infty} n(n+1) - n x^n \\ &= 9[1 \cdot 2x + 2 \cdot 3x^2 + \dots] - 9[x + 2x^2 + 3x^3 + \dots] \\ &= 9x \times 2(1-x)^{-3} - 9x(1-x)^{-2} \end{aligned}$$

$$\begin{aligned} \text{i.e., } \left(\frac{1}{x^2} - 4\right) G(x) &= \frac{a_0}{x^2} + \frac{a_1}{x} + \frac{18x}{(1-x)^3} - \frac{9x}{(1-x)^2} \\ \therefore G(x) &= \frac{a_0 + a_1 x}{1 - 4x^2} + \frac{18x^3}{(1-x)^3(1-4x^2)} - \frac{9x^3}{(1-x)^2(1-4x^2)} \\ &= \frac{a_0 + a_1 x}{(1-2x)(1+2x)} + \frac{9x^3 + 9x^4}{(1-x)^3(1-2x)(1+2x)} \\ &= \frac{A}{1-2x} + \frac{B}{1+2x} - \frac{3}{1-x} + \frac{5}{(1-x)^2} - \frac{6}{(1-x)^3} - \frac{1}{1+2x} + \frac{27}{1-2x} \end{aligned}$$

(On splitting into partial fractions)

$$= c_1(1 - 2x)^{-1} + c_2(1 + 2x)^{-1} - \frac{17}{3}(1 - x)^{-1} + 5(1 - x)^{-2} - 6(1 - x)^{-3},$$

where $c_1 = A + \frac{27}{4}$ and $c_2 = B - \frac{1}{12}$

$$\text{i.e., } \sum_{n=0}^{\infty} a_n x^n = c_1 \sum_{n=0}^{\infty} 2^n x^n + c_2 \sum_{n=0}^{\infty} (-1)^n 2^n x^n - \frac{17}{3} \sum_{n=0}^{\infty} x^n + 5 \sum_{n=0}^{\infty} (n+1) x^n - 3 \sum_{n=0}^{\infty} (n+1)(n+2)x^n$$

Equating coefficients of x^n , we get the general solution of the given R.R. as

$$a_n = c_1 \cdot 2^n + c_2 \cdot (-1)^n 2^n - \frac{17}{3} + 5(n+1) - 3(n+1)(n+2)$$

$$\text{i.e., } a_n = c_1 \cdot 2^n + c_2 \cdot (-1)^n \cdot 2^n - 3\left(n^2 + \frac{4}{3}n + \frac{20}{9}\right).$$

Example 2.25 Use the method of generating function to solve the recurrence relation

$$a_n = 4a_{n-1} + 3n \cdot 2^n; n \geq 1, \text{ given that } a_0 = 4.$$

Let the generating function of $\{a_n\}$ be

$$G(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Multiplying both sides of the given R.R. by x^n and summing up, we have

$$\sum_{n=1}^{\infty} a_n x^n - 4 \sum_{n=1}^{\infty} a_{n-1} x^n = 3 \sum_{n=1}^{\infty} n(2x)^n$$

$$\text{i.e., } \{G(x) - a_0\} - 4x G(x) = 6x \cdot \sum_{n=1}^{\infty} n(2x)^{n-1}$$

$$\text{i.e., } (1 - 4x) G(x) = \frac{6x}{(1-2x)^2} + 4 [\because a_0 = 4]$$

$$\therefore G(x) = \frac{6x}{(1-4x)(1-2x)^2}$$

$$= \frac{10}{1-4x} - \frac{3}{1-2x} - \frac{3}{(1-2x)^2}, \text{ on splitting into partial fractions}$$

$$\text{i.e., } \sum_{n=0}^{\infty} a_n x^n = 10 \sum_{n=0}^{\infty} (4x)^n - 3 \sum_{n=0}^{\infty} (2x)^n - 3 \sum_{n=0}^{\infty} (n+1)(2x)^n$$

Equating coefficients of x^n , we get

$$a_n = 10 \times 4^n - 3 \times 2^n - 3(n+1) \times 2^n$$

$$= 10 \times 4^n - (3n+6) \times 2^n$$



EXERCISE 2(B)

Part A: (Short answer questions)

1. What is mathematical induction? In what way is it useful?
2. State the principle of mathematical induction.
3. What are basic and inductive steps in mathematical induction?
4. State the strong form of the principle of mathematical induction.
5. What is well-ordering principle. Establish it using mathematical induction.
6. Use mathematical induction to show that $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$.
7. Use mathematical induction to show that $1 + 2 + 3 + \dots + n = \frac{1}{2}n(n + 1)$.
8. Use mathematical induction to prove that $n < 2^n$, for all positive integers n .
9. Find a formula for the sum of the first n even positive integers and prove it by induction.
10. Define a recurrence relation. What do you mean by its solution?
11. Define a linear recurrence relation. What is meant by the degree of such a relation?
12. When is a recurrence relation said to be homogeneous? Non-homogeneous?
13. Define the characteristic equation and characteristic polynomial of a recurrence relation.
14. What do you mean by particular solution of a recurrence relation?
15. Define generating function of a sequence and give an example.
16. How will you use the notion of generating function to solve a recurrence relation?

Part B

Prove, by mathematical induction, the following results:

$$17. 1 + 3 + 5 + \dots + (2n - 1) = n^2.$$

$$18. 1^2 - 2^2 + 3^2 - \dots + (-1)^{n-1}n^2 = \frac{(-1)^{n-1} \cdot n(n+1)}{2}.$$

$$19. 1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4} n^2(n+1)^2.$$

$$20. 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}.$$

$$21. 1 \cdot 2 + 3 \cdot 4 + 5 \cdot 6 + \dots + (2n - 1) \cdot 2n = \frac{1}{3} n(n+1)(4n-1).$$

$$22. \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \dots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}.$$

$$\begin{aligned}
 23. \quad & \frac{1}{2 \cdot 4} + \frac{1 \cdot 3}{2 \cdot 4 \cdot 6} + \frac{1 \cdot 3 \cdot 5}{2 \cdot 4 \cdot 6 \cdot 8} + \cdots + \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n+2)} \\
 & = \frac{1}{2} - \frac{1 \cdot 3 \cdot 5 \cdots (2n+1)}{2 \cdot 4 \cdot 6 \cdots (2n+2)}.
 \end{aligned}$$

$$24. \quad \sum_{r=1}^n \frac{r^2}{(2r-1)(2r+1)} = \frac{n(n+1)}{2(2n+1)}.$$

Prove, by mathematical induction, the following inequalities, when $n \in \mathbb{Z}^+$.

- 25. $n < 2^n$, for $n \geq 1$.
- 26. $n^2 < 2^n$, for $n > 4$.
- 27. $2^n < n^3$, for $n \geq 10$.
- 28. $2^n < n!$ for $n > 3$.
- 29. $2^n \geq (2n+1)$, for $n \geq 3$.

$$30. \quad \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots 2n} \geq \frac{1}{2n}, \text{ for } n \geq 1.$$

Prove, by mathematical induction, the following results, when $n \in \mathbb{Z}^+$.

- 31. $n^3 - n$ is divisible by 6.
- 32. $n^5 - n$ is divisible by 5.
- 33. $5^n - 1$ is divisible by 4.
- 34. $8^n - 3^n$ is divisible by 5.
- 35. $5^{2n} - 2^{5n}$ is divisible by 7.
- 36. $10^{n+1} + 10^n + 1$ is divisible by 3.
- 37. $6 \times 7^n - 2 \times 3^n$ is divisible by 4.

Solve the following recurrence relations:

- 38. $a_{n+1} - 2a_n = 5$; $n \geq 0$; $a_0 = 1$.
- 39. $a_n - 2a_{n-1} = n + 5$; $n \geq 1$; $a_0 = 4$.
- 40. $a_{n+1} - a_n = 2n + 3$; $n \geq 0$; $a_0 = 1$.
- 41. $a_n - 2a_{n-1} = 2n^2$; $n \geq 1$; $a_1 = 4$.
- 42. $a_n - 3a_{n-1} = 2^n$; $n \geq 1$; $a_0 = 1$.
- 43. $a_n = 2a_{n-1} + 3 \cdot 2^n$; $n \geq 1$; $a_0 = 5$.
- 44. $a_n - a_{n-1} = 3(b_n - a_{n-1})$, where

$$b_n = \begin{cases} 1000 \cdot (3/2)^n, & \text{for } 0 \leq n \leq 10 \\ 1000 \cdot (3/2)^{10}, & \text{for } n \geq 10 \end{cases} \text{ given that } a_0 = 0.$$

- 45. $a_{n+1} = 2a_n + 3a_{n-1}$; $n \geq 1$; given $a_0 = 0$, $a_1 = 8$.
- 46. $9a_n = 6a_{n-1} - a_{n-2}$; $n \geq 2$, given $a_0 = 3$, $a_1 = -1$.
- 47. $a_{n+2} - a_{n+1} - 2a_n = 4$; $n \geq 0$, given $a_0 = -1$, $a_1 = 3$.
- 48. $a_{n+2} + 4a_{n+1} + 4a_n = 7$; $n \geq 0$; given $a_0 = 1$, $a_1 = 2$.
- 49. $a_{n+2} + 3a_{n+1} + 2a_n = 3^n$; $n \geq 0$; given $a_0 = 0$, $a_1 = 1$.
- 50. $a_{n+2} - 3a_{n+1} + 2a_n = 2^n$; $n \geq 0$; given $a_0 = 3$, $a_1 = 6$.
- 51. $a_n = 5a_{n-1} - 6a_{n-2} + 2^n + 3n$.

52. $a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3$; $n \geq 2$, given $a_0 = 1$; and $a_1 = 4$.

53. $a_{n+2} - 4a_{n+1} + 3a_n = 2^n \cdot n^2$; $n \geq 0$; given $a_0 = a_1 = 0$.

54. $a_{n+2} - 7a_{n+1} - 8a_n = n(n-1)2^n$.

Use the method of generating functions to solve the following recurrence relations:

55. $a_n + 3a_{n-1} - 4a_{n-2} = 0$; $n \geq 2$, given $a_0 = 3$, $a_1 = -2$.

56. $a_{n+2} - 5a_{n+1} + 6a_n = 36$; $n \geq 0$; given $a_0 = a_1 = 0$.

57. $a_{n+2} - a_n = 2^n$; $n \geq 0$; given $a_0 = 0$; $a_1 = 1$.

58. $a_{n+2} - 6a_{n+1} + 9y_n = 3^n$; $n \geq 0$; given $a_0 = 2$ and $a_1 = 9$.

59. $a_{n+1} + 4a_n + 4a_{n-1} = n - 1$; $n \geq 1$, given $a_0 = 0$ and $a_1 = 1$.

60. $a_{n+2} + a_n = n \cdot 2^n$; $n \geq 0$.



ANSWERS

Exercise 2(A)

- | | | | |
|------------------------------|---------------|-------------------------------------|-------------|
| 3. (i) 8! | (ii) 7! | (iii) 7! | (iv) 6! |
| 4. 24 | 5. 60 | 6. 90 | 7. 720, 240 |
| 9. 252 | 10. 45,04,501 | 13. 9 | 16. 22; 17 |
| 17. 220 | 19. 1854 | 20. 3186 | |
| 21. (i) 1,81,440 | (ii) 1,05,840 | (iii) 30,240 | (iv) 5040 |
| (v) 35,280 | (vi) 70,560 | (vii) 75,600 | |
| 22. 12; 12; 8; 4; 16; 8 | | 23. 240; 96; 708 | |
| 24. (i) 5040 | (ii) 144 | (iii) 288 | (iv) 720 |
| 25. (i) 2^{10} | (ii) 3^{10} | | |
| 26. (i) 220 | (ii) 299 | (iii) 4017 | (iv) 924 |
| 27. (i) 1024 | (ii) 45 | (iii) 176 | (iv) 252 |
| 28. (i) 120 | (ii) 968 | (iii) 386 | (iv) 512 |
| 29. (i) 5040 | (ii) 720 | (iii) 120 | (iv) 120 |
| (v) 24 | (vi) 0 | | |
| 30. (i) 60 | (ii) 48 | (iii) 78 | (iv) 78 |
| 31. (i) 120 | (ii) 360 | (iii) 360 | |
| 32. (i) 34650 | (ii) 28350 | | |
| 33. (i) 24 | (ii) 24 | | |
| 34. (i) 720 | (ii) 240 | | |
| 35. (i) 2,86,000 | (ii) 1,49,760 | | |
| 36. 43,200 | | | |
| 37. (i) 1,25,970 | (ii) 44,100 | (iii) 63,900 | (iv) 40,935 |
| (iv) 10,695 | | | |
| 38. (i) 4242 | (ii) 4221 | | |
| 39. (i) 1,12,32,000 | | | |
| 40. (i) $C(25, 5) \times 6!$ | | (ii) $C(24, 4) \times 6!$ | |
| (iii) $C(24, 4) \times 5!$ | | (iv) $15 \times C(24, 4) \times 4!$ | |
| 41. (i) 286 | (ii) 165 | (iii) 110 | (iv) 80 |
| (v) 276 | | | |

- | | |
|-------------------------------------|-----------------------------|
| 42. (i) 35 | (ii) 70 |
| 43. (i) 252 | (ii) 35 |
| 44. 560 | 45. $C(59, 9)$ |
| 52. (i) 162 | (ii) 18 |
| 53. 46 | 54. 6 |
| 56. (i) 4 | (ii) 36 |
| 58. (i) D_7 | (ii) $7! - D_7$ |
| 59. (i) D_{20} | (ii) $20! - D_{20}$ |
| 60. (i) $D_{10}/10!$ | (ii) $10 \times D_9/10!$ |
| | (iii) $C(10, 2)/10!$ (iv) 0 |
| | (v) $1/10!$ |
| 46. $C(20, 15) - 6 \times C(10, 5)$ | |
| 53. 7 | |
| 57. $10! \times D_{10}$ | |
| 59. 1 | |
| 60. 20 $\times D_{19}$ | |

Exercise 2(B)

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

39. $a_n = 11(2^n) - (n + 7)$

40. $a_n = (n + 1)^2$

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

42. $a_n = 2(3^n - 2^n)$

43. $a_n = (3n + 5)2^n$

44.
$$a_n = \frac{9000}{7} \left\{ \left(\frac{3}{2}\right)^n - (-2)^n \right\}, \text{ for } 0 \leq n \leq 10$$

$$= 1000 \left(\frac{3}{2}\right)^{10} \{1 - (-2)^{10}\}, \text{ for } n > 10.$$

45. $a_n = 2(3^n) - 2(-1)^n$

46. $a_n = (1 - 2n)/3^{n-1}$

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

48. $a_n = \left(\frac{2}{9} - \frac{5n}{6}\right)(-2)^n + \frac{7}{9}$

49. $a_n = \frac{3}{4}(-1)^n - \frac{4}{5}(-2)^n + \frac{1}{20}(3)^n. \quad 50. \quad a_n = 1 + 2^{n+1} + n \cdot 2^{n-1}$

51. $a_n = A \cdot 2^n + B \cdot 3^n - n \cdot 2^{n+1} + \frac{3}{4}(2n + 7)$

52. $a_n = \frac{1}{8} + \frac{39}{8}(3^n) - 2^{n+2} - \frac{1}{4}n^2 - \frac{5}{2}n.$

53. $a_n = 3 + 5(3^n) - (n^2 + 8) \cdot 2^n.$

54. $a_n = A \cdot 8^n + B \cdot (-1)^n - \frac{1}{54}(3n^2 - 5n + 2) \cdot 2^n \quad 55. \quad a_n = 2 + (-4)^n$

56. $a_n = 18[3^n - 2^{n+1} + 1] \quad 57. \quad a_n = \frac{1}{3}[2^n - (-1)^n]$

58. $a_n = \frac{1}{18}(n^2 + 17n + 36) \cdot 3^n$

59. $a_n = \frac{2}{27}(-2)^n - \frac{5}{9}n(-2)^n - \frac{2}{27} + \frac{1}{9}n.$

60. $a_n = A \cos \frac{n\pi}{2} + B \sin \frac{n\pi}{2} + \frac{(5n-8)}{25} \cdot 2^n.$

Worksheet-IV for BMAT205L

Discrete Mathematics and Graph Theory

Ankush Chanda

October 11, 2023

1. Use method of generating functions to solve the recurrence relation:

$$a_n = 4a_{n-1} - 4a_{n-2} + 4^n, \quad n \geq 2$$

given that $a_0 = 2, a_1 = 8$.

2. Identify the sequence having the expression

$$\frac{5 + 2x}{1 - 4x^2}$$

as a generating function.

3. Find the generating function of the recurrence relation

$$a_n = 2a_{n-1} + 3a_{n-2}, \quad n \geq 2$$

with $a_0 = 3, a_1 = 1$, and hence find its solution.

4. Solve the recurrence relation

$$a_{n+2} + 3a_{n+1} + 2a_n = 3n, \quad n \geq 0,$$

given that $a_0 = 0, a_1 = 1$.

5. Using generating functions solve the recurrence relation:

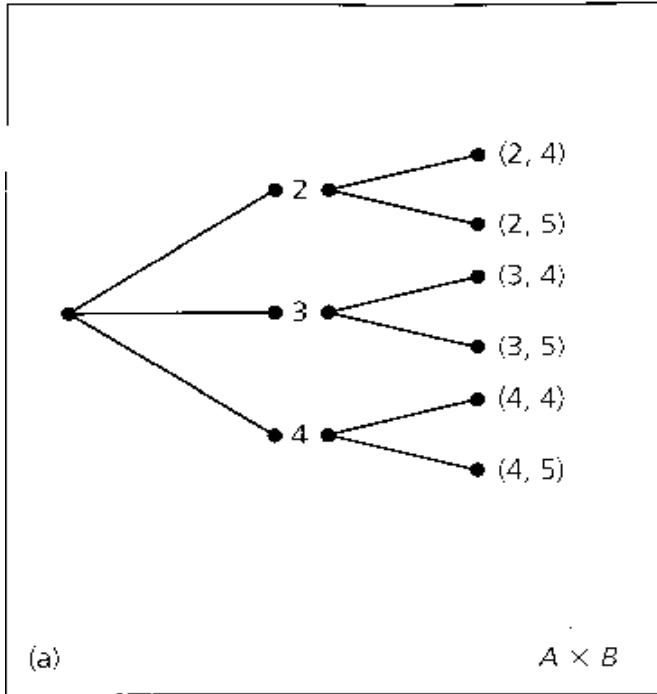
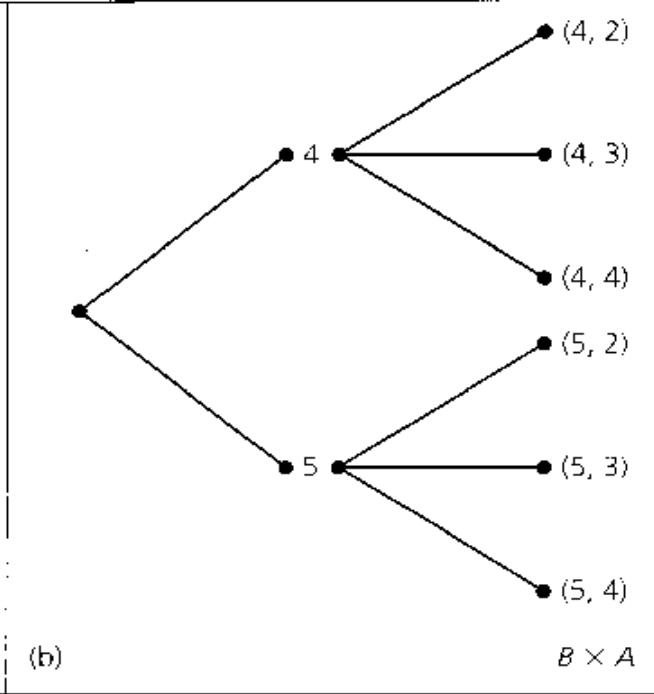
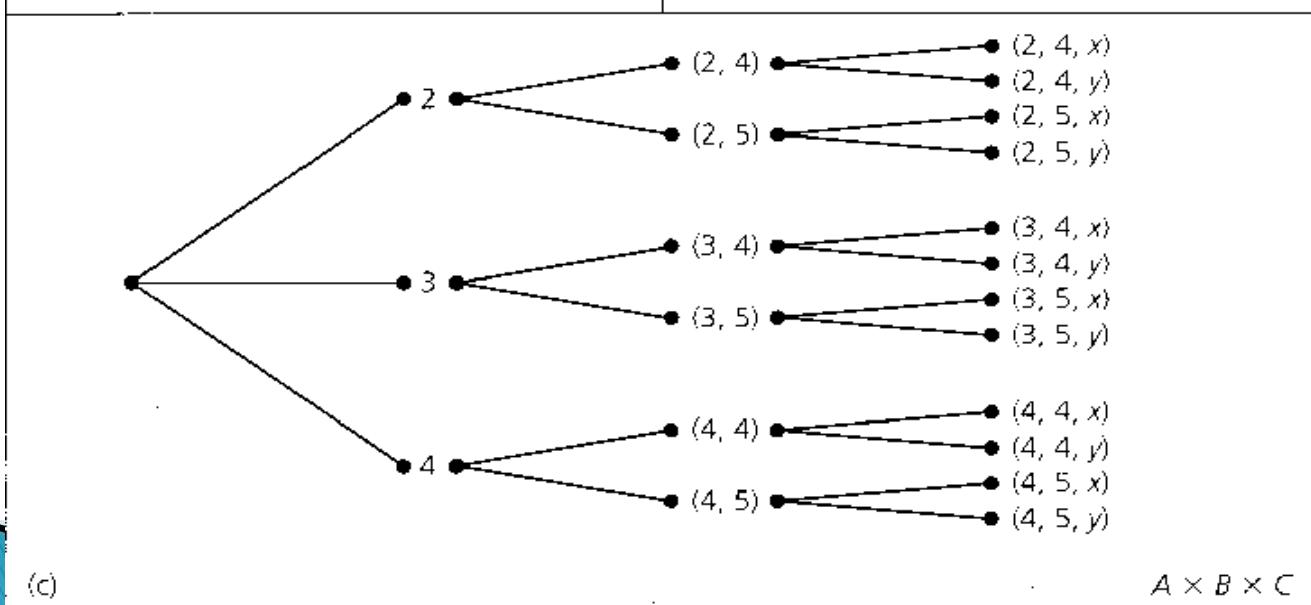
$$a_n = a_{n-1} + 6a_{n-2}, \quad n \geq 2$$

given that $a_0 = 2, a_1 = 1$.

Partially Ordered Relations with Posets-Hasse Diagram

Cartesian products and relations

- ▶ The Cartesian product of A and B is denoted by $A \times B$ and equals $\{(a, b) \mid a \in A \text{ and } b \in B\}$. The elements of $A \times B$ are ordered pairs. The elements of $A_1 \times A_2 \times \dots \times A_n$ are ordered n-tuples.
- ▶ Let $A = \{2, 3, 4\}$, $B = \{4, 5\}$, $C = \{x, y\}$. Then its Cartesian product $A \times B$, $B \times A$ and $A \times B \times C$ is given by fig a, b and c respectively.


 $A \times B$

 $B \times A$

 $A \times B \times C$

Relations

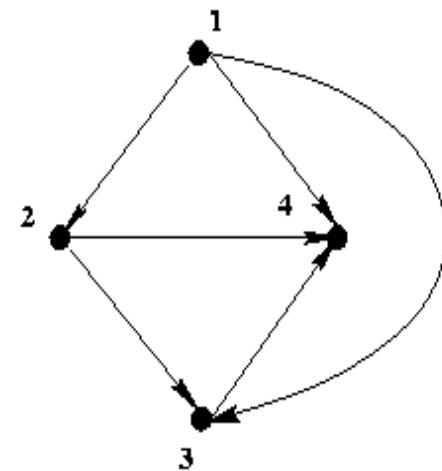
- ▶ Any subsets of the Cartesian product $A \times B$ is called a relation from A to B. Any subset of the Cartesian product $A \times A$ is called a binary relation on A.
- ▶ The following are some of relations from $A = \{2, 3, 4\}$ to $B = \{4, 5\}$:
 - (a) \emptyset
 - (b) $\{(2, 4)\}$
 - (c) $\{(2, 4), (2, 5)\}$
 - (d) $\{(2, 4), (3, 4), (4, 4)\}$
 - (e) $A \times B$
- ▶ For finite sets A and B with $|A|=m$ and $|B|=n$, there are 2^{mn} relations from A to B. There are also 2^{mn} relations from B to A.

Digraph representing a relation

A binary relation on a set can be represented by a digraph. Let R be a binary relation on a set A , that is R is a subset of A . Then a digraph representing R can be constructed as follows:

Let the elements of A be the vertices of the digraph G , and let (x, y) be an arc of G from vertex x to vertex y if and only if (x, y) is in R .

Example: The less than relation R on the set of integers $A = \{1, 2, 3, 4\}$ is the set $\{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$ and it can be represented by the following digraph.



Relation properties

- ▶ Six properties of relations we will study:
 - Reflexive
 - Irreflexive
 - Symmetric
 - Asymmetric
 - Antisymmetric
 - Transitive

Reflexivity

- ▶ A relation is reflexive if every element is related to itself
 - Or, $(a,a) \in R$
- ▶ Examples of reflexive relations:
 - $=, \leq, \geq$

Irreflexivity

- ▶ A relation is irreflexive if every element is *not* related to itself
 - Or, $(a,a) \notin R$
 - Irreflexivity is the opposite of reflexivity
- ▶ Examples of irreflexive relations:
 - $<$, $>$

Symmetry

- ▶ A relation is symmetric if, for every $(a,b) \in R$, then $(b,a) \in R$
- ▶ Examples of symmetric relations:
 - $=$, `isTwinOf()`

Asymmetry

- ▶ A relation is asymmetric if, for every $(a, b) \in R$, then $(b, a) \notin R$
 - Asymmetry is the opposite of symmetry
- ▶ Examples of asymmetric relations:
 - $<$, $>$

Antisymmetry

- ▶ A relation is antisymmetric if, for every $(a,b) \in R$, then $(b,a) \in R$ is true only when $a=b$
 - Antisymmetry is *not* the opposite of symmetry
- ▶ Examples of antisymmetric relations:
 - $=, \leq, \geq$
- ▶ Examples of relations that are not antisymmetric:
 - $<, >, \text{isTwinOf}()$

Transitive

- ▶ A relation is transitive if, for every $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$
- ▶ If $a < b$ and $b < c$, then $a < c$
 - Thus, $<$ is transitive
- ▶ If $a = b$ and $b = c$, then $a = c$
 - Thus, $=$ is transitive

Equivalence Relation

Definition:

A relation R is an **equivalence relation** if and only if it is reflexive, symmetric and transitive.

Example:

The relation of similarity of triangles is transitive.

Proof:-

Consider the set T of all triangles and relation $R = \{(x,y) | x \text{ and } y \text{ have equal angles}\}$

R is an equivalence relation. It has the three properties:

Reflexivity xRx

Symmetry: If xRy then yRx

Transitivity: If xRy and yRz , then xRz

Partially ordered sets or Posets

Definition:

Let R be a binary relation defined on a set A.

R is a partial order relation iff R is transitive and anti-symmetric.

Weak partial order: R is reflexive.

Strict partial order: R is not reflexive (irreflexive or neither reflexive nor irreflexive).

A set A together with a partial order relation R is called a partially ordered set or poset.

Examples:

Let $A=\{0, 1, 2, 3\}$ and $R=\{(0,0), (0,1), (0,2), (1,1), (1,2), (2,2), (0,3), (3,3)\}$

R is a partial order relation

Total orders

Definition:

A partial order is a **total or linear order** iff for all x and y in the set either xRy or yRx is true.

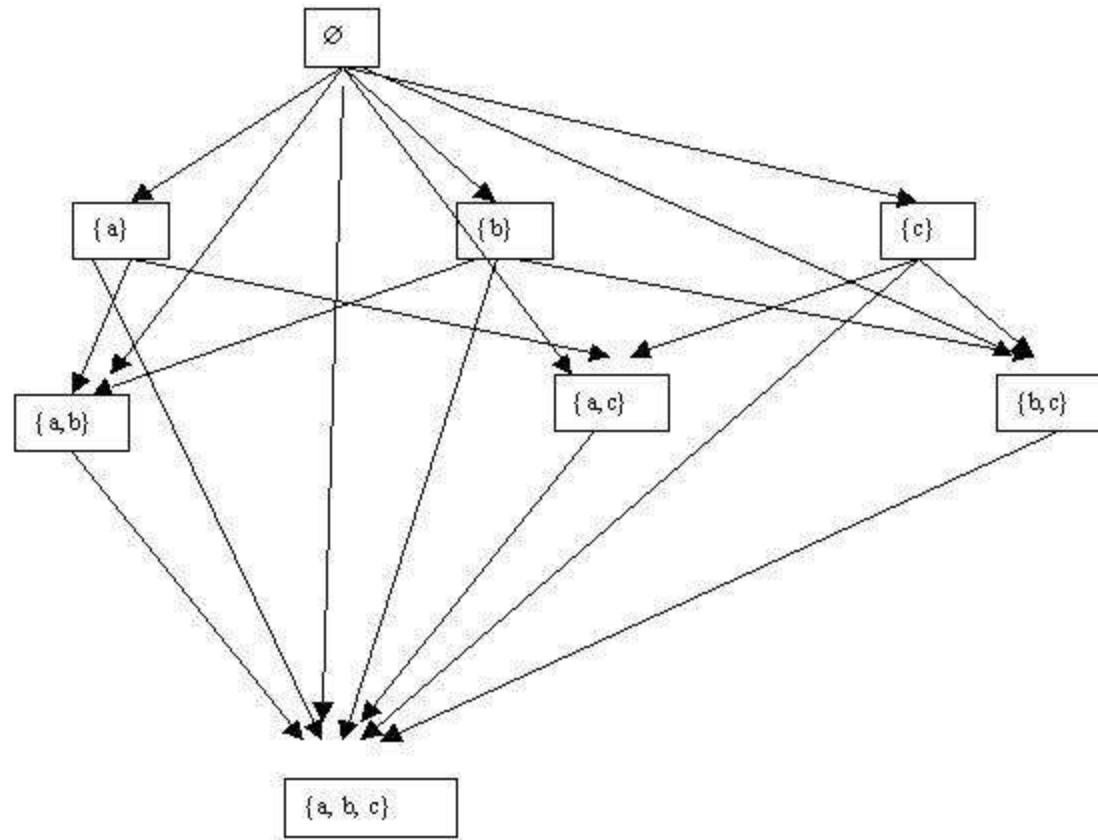
In a totally ordered set all elements are comparable.

Example:

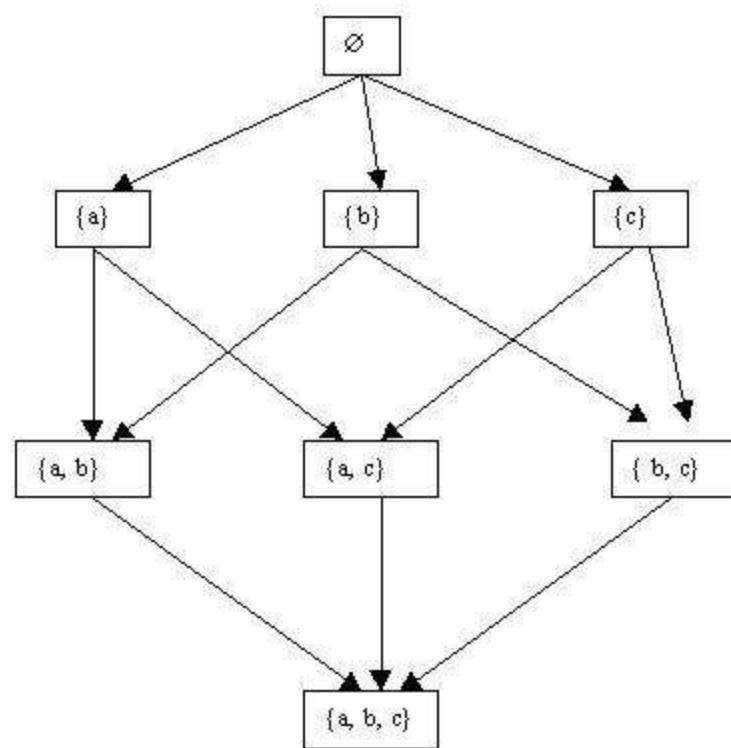
The relation "less than or equal to" is a total order relation.

Consider the power set of a set $A = \{a, b, c\}$ and the relation R defined on the power set of A .

$R = \{(A_i, A_j) \mid A_i \text{ is a subset of } A_j\}$. R is a partial order. It is not a total order.



If we eliminate the links implied by the transitivity, we get a simpler diagram, called **Hasse diagram**:



Hasse Diagram

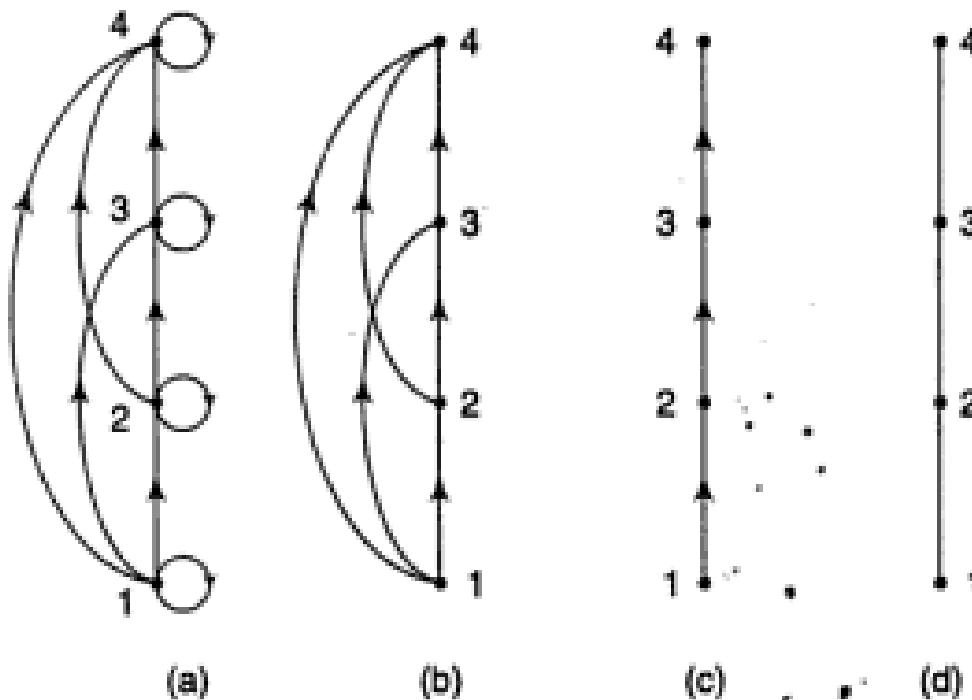
The simplified form of the digraph of a partial ordering on a finite set that contains sufficient information about the partial ordering is called a *Hasse diagram*, named after the twentieth-century mathematician Helmut Hasse.

The simplification of the digraph as a Hasse diagram is achieved in three ways:

- (i) Since the partial ordering is a reflexive relation, its digraph has loops at all vertices. We need not show these loops since they must be present.
- (ii) Since the partial ordering is transitive, we need not show those edges that must be present due to transitivity. For example, if $(1, 2)$ and $(2, 3)$ are edges in the digraph of a partial ordering, $(1, 3)$ will also be an edge due to transitivity. This edge $(1, 3)$ need not be shown in the corresponding Hasse diagram.
- (iii) If we assume that all edges are directed upward, we need not show the directions of the edges.

Thus the Hasse diagram representing a partial ordering can be obtained from its digraph, by removing all the loops, by removing all edges that are present due to transitivity and by drawing each edge without arrow so that its initial vertex is below its terminal vertex.

For example, let us construct the Hasse diagram for the partial ordering $\{(a, b) | a \leq b\}$ on the set $\{1, 2, 3, 4\}$ starting from its digraph. (Fig. 2.15)

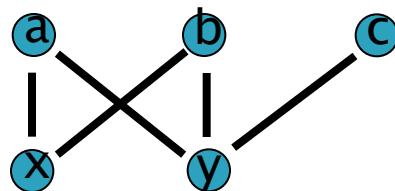


Upper and Lower Bounds

- ▶ If a poset is built from relation R on set A , then any $x \in A$ satisfying xRy is an upper bound of y , and any $x \in A$ satisfying yRx is a lower bound of y .
- ▶ Examples: If $A = \{a, b, c\}$ and R is \supseteq , then $\{a, c\}$
 - is an upper bound of $\{a\}$, $\{c\}$, and \emptyset .
 - is also an upper bound of $\{a, c\}$ (weak poset).
 - is a lower bound of $\{a, b, c\}$.
 - is also a lower bound of $\{a, c\}$ (weak poset).

Least Upper Bound and Greatest Lower Bound

- ▶ A least upper bound of two elements x and y is a minimal element in the intersection of the upper bounds of x and y .
- ▶ A greatest lower bound is a maximal element in the intersection of the lower bounds of x and y .
- ▶ Examples:
 - For \supseteq , $\{a, c\}$ is a least upper bound of $\{a\}$ and $\{c\}$, \emptyset is a greatest lower bound of $\{a\}$ and $\{b, c\}$, and $\{a\}$ is a least upper bound of \emptyset .
 - For the following strict poset, $\text{lub}(x,y) = \{a,b\}$, $\text{lub}(y,y) = \{a,b,c\}$, $\text{lub}(a,y) = \emptyset$, $\text{glb}(a,b) = \{x,y\}$, $\text{glb}(a,c) = \{y\}$



Module 4

Lattices

Lattices

- Partially Ordered Relations
- Lattices as Posets
- Hasse Diagram
- Properties of Lattices.

Relation: If A and B are two sets, then relation R from A to B is the subset of the cartesian product $A \times B$.

If a is related to b under the relation R , then we write $a R b$.

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

The set of first entries of the ordered pairs in a relation is called the **domain of the relation**. The set of second entries of the ordered pairs in a relation is called the **range of the relation**.

Example: If $A = \{2, 3, 4, 5, 6\}$, $B = \{2, 4, 6, 8\}$ and $xRy : x \text{ divides } y$, then

$$R = \{(2, 2), (2, 4), (2, 6), (2, 8), (3, 6), (4, 4), (4, 8), (6, 6)\}$$

Domain of $R=\{2,3,4,6\}$,

Range of $R=\{2,4,6,8\}$

Note:

For finite sets A and B with $|A| = m$ and $|B| = n$, there are 2^{mn} relations from A to B .
There are also 2^{mn} relations from B to A .

PROPERTIES OF RELATIONS

Reflexive Relation

Let R be a relation defined in a set A ; then R is reflexive if $a R a$ holds for all $a \in A$, i.e., if $(a, a) \in R$ for all $a \in A$.

Example 1: Let $A = \{a, b, c\}$ and $R = \{(a, a), (b, b), (c, c)\}$ then R is a reflexive relation in A .

Example 2: 'Equality' is a reflexive relation, since an element equals itself.

Symmetric Relation

A relation R defined in set A is said to be 'symmetric' if $b R a$ holds whenever $a R b$ holds for $b \in A$, i.e., R is symmetric in A if

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

Example: Let R be relation 'is perpendicular to' in the set of all straight lines, then R is a symmetric relation.

Transitive Relation

A relation R in set A is said to be transitive if

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

i.e., if $a R b$ and $b R c \Rightarrow a R c$, where $a, b, c \in A$.

Example 1: Let A denote the set of straight lines in a plane and R be a relation in A defined by 'is parallel to' then R is a transitive relation in A .

Example 2: Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$ then R is transitive.

Anti-symmetric Relation

Let R be a relation in a set A , then R is called anti-symmetric.

$$(a, b) \in R, (b, a) \in R \Rightarrow a = b \quad \forall a, b \in R$$

$$i.e. \quad a R b \text{ and } b R a \Rightarrow a = b$$

Example : Let N denote the set of Natural Numbers R be a relation in N , defined by 'a is a divisor' of b , i.e., $a R b$ if a divides b then R is anti-symmetric since a divides b and b divides $a \Rightarrow a = b$.

Equivalence Relation

A relation R in a set A is said to be an equivalence relation in A , if R is reflexive, symmetric and transitive.

Example :

- (i) Let A be the set of all triangle in a plane and let R be a relation in A defined by 'is congruent to', then R is reflexive, symmetric and transitive.
 $\therefore R$ is an Equivalence relation in A .
- (ii) Let $A = \{a, b, c\}$, and $R = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}$ then R is an equivalence relation in A .

Example: Consider the following relations on $\{1,2,3,4\}$:

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

$$R_2 = \{(1,1), (1,2), (2,1)\},$$

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

$$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\},$$

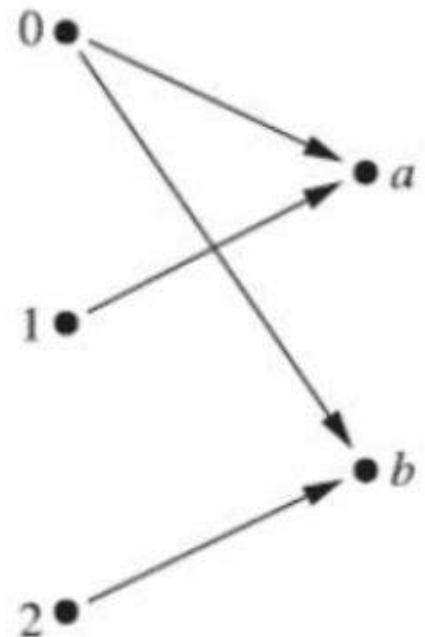
$$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\},$$

$$R_6 = \{(3,4)\}.$$

Which of these relations are reflexive?

Solution: The relations R_3 and R_5 are reflexive because they both contain all pairs of the form (a, a) , namely, $(1,1), (2,2), (3,3)$, and $(4,4)$. The other relations are not reflexive because they do not contain all of these ordered pairs. In particular, R_1, R_2, R_4 , and R_6 are not reflexive because $(3,3)$ is not in any of these relations.

Let $A = \{0,1,2\}$ and $B = \{a,b\}$. Then $\{(0,a), (0,b), (1,a), (2,b)\}$ is a relation from A to B . This means, for instance, that $0 R a$, but that $1 R b$. Relations can be represented graphically,



RELATIONS AND DIGRAPHS

A relation can be represented pictorially by drawing its graph. Let R be a relation on the set $A = \{a_1, a_2, \dots, a_n\}$. The elements a_i of A are represented by points (or circles) called nodes (or vertices). If $(a_i, a_j) \in R_j$ then we connect the vertices a_i and a_j by means of an arc and put an arrow in the direction from a_i to a_j . If $(a_i, a_j) \in R$ and $(a_j, a_i) \in R$ then we draw two arcs between a_i and a_j (sometimes by one arc which starts from node a_i and relatives to node x_i (such an arc is called a loop). When all the nodes corresponding to the ordered pairs in R are connected by arcs with proper arrows, we get a graph of the relation R . If R is reflexive, then there must be a loop at each node in the graph of R . If R is symmetric, then $(a_i, a_j) \in R$ implies $(a_j, a_i) \in R$ and the nodes a_i and a_j will be connected by two arcs (edges) one from a_i to a_j and the other from a_j to a_i .

Example 1: Let $A = \{a, b, d\}$ and R be a relation on A given by

$$R = \{(a, b), (a, d), (b, d), (d, a), (d, d)\}$$

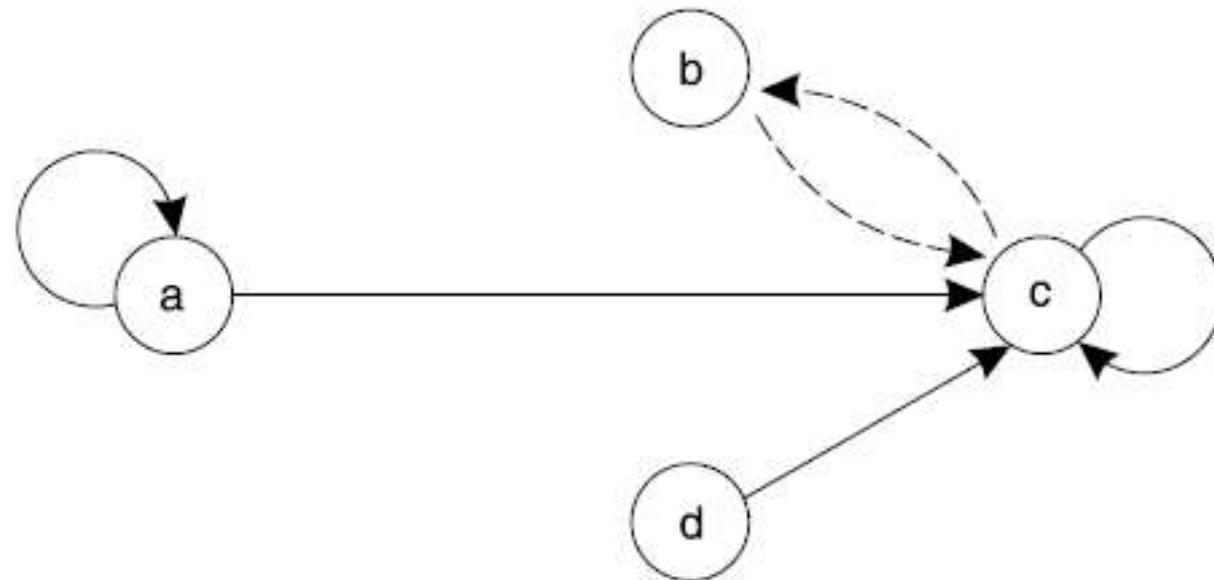
Construct the digraph of R .

Example 2: Let $A = \{1, 2, 3, 4\}$

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

Construct the digraph of R .

Example 3: Find the relation determined by Fig. 3.9.



Solution: The relation R of the digraph is

$$R = \{(a, a), (a, c), (b, c), (c, b), (c, c), (d, c)\}$$

PARTIAL ORDERING

A relation R on a set S is called a *partial ordering* or *partial order* if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a *partially ordered set*, or *poset*, and is denoted by (S, R) . Members of S are called *elements* of the poset.

Example:

Let $A=\{0,1,2,3\}$ and $R=\{(0,0),(0,1),(0,2),(1,1), (1,2), (2,2),(0,3),(3,3)\}$

R is a partial order relation

Comparability

Let R be a partial order on A and $a, b \in A$ whenever $aR b$ or $bR a$, we say that a and b are comparable otherwise a and b are non-comparable.

TOTALLY ORDERED SET

Definition: A partial order is a total or linear order iff for all x and y in the set either xRy or yRx is true. In a totally ordered set all elements are comparable.

Example 1: Let N be the set of positive integers ordered by divisibility. The elements 5 and 15 are comparable. Since $5/15$ on similarly the elements 7 and 21 are comparable since $7/21$. The positive integers 3 and 5 are non-comparable since neither $3/5$ nor $5/3$. Similarly the integers 5 and 7 are non-comparable.

Example 2: The set N of positive integers with the usual order \leq (less than equal) is a linear order on N . The set (N, \leq) is a totally ordered set.

Hasse Diagrams

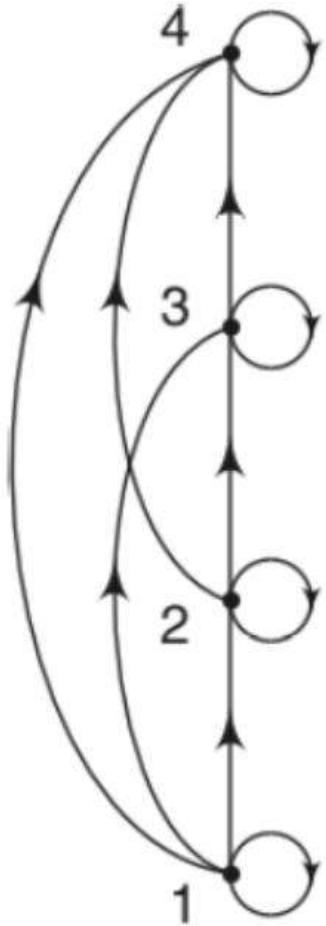
The simplified form of the digraph of a partial ordering on a finite set that contains sufficient information about the partial ordering is called a Hasse diagram, named after the twentieth-century mathematician Helmut Hasse.

The simplification of the digraph as a Hasse diagram is achieved in three ways:

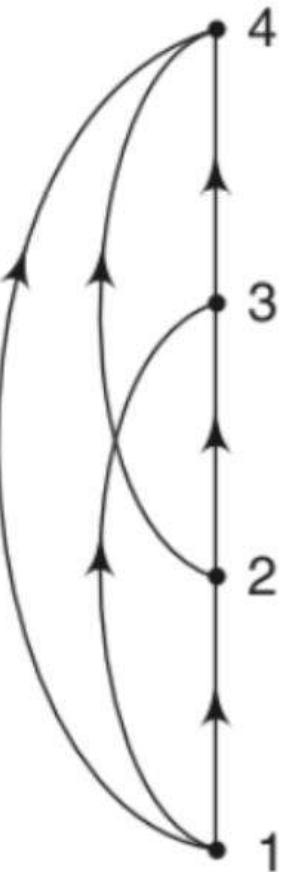
- Since the partial ordering is a reflexive relation, its digraph has loops at all vertices. We need not show these loops since they must be present.
- Since the partial ordering is transitive, we need not show those edges that must be present due to transitivity. For example, if $(1,2)$ and $(2,3)$ are edges in the digraph of a partial ordering, $(1,3)$ will also be an edge due to transitivity. This edge $(1,3)$ need not be shown in the corresponding Hasse diagram.
- If we assume that all edges are directed upward, we need not show the directions of the edges.

Thus the Hasse diagram representing a partial ordering can be obtained from its digraph, by removing all the loops, by removing all edges that are present due to transitivity and by drawing each edge without arrow so that its initial vertex is below its terminal vertex.

Example: let us construct the Hasse diagram for the partial ordering $\{(a, b) \mid a \leq b\}$ on the set $\{1, 2, 3, 4\}$ starting from its digraph.



(a)



(b)



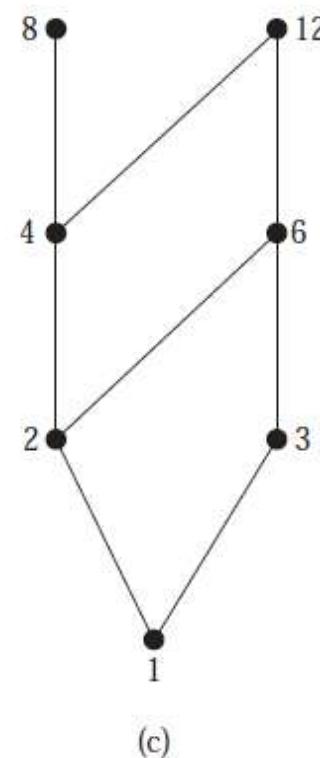
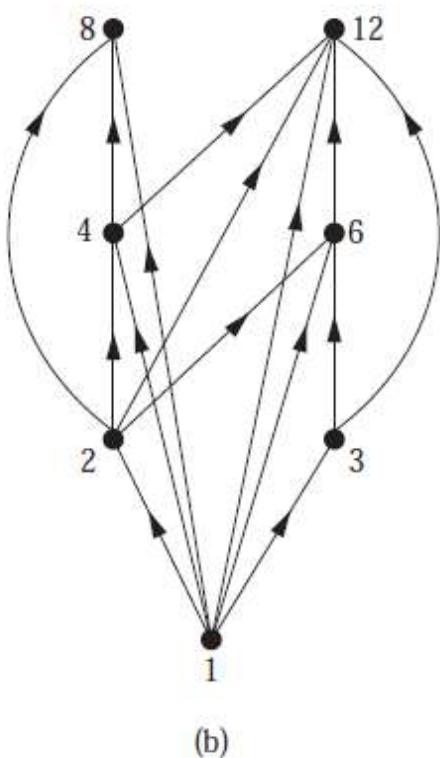
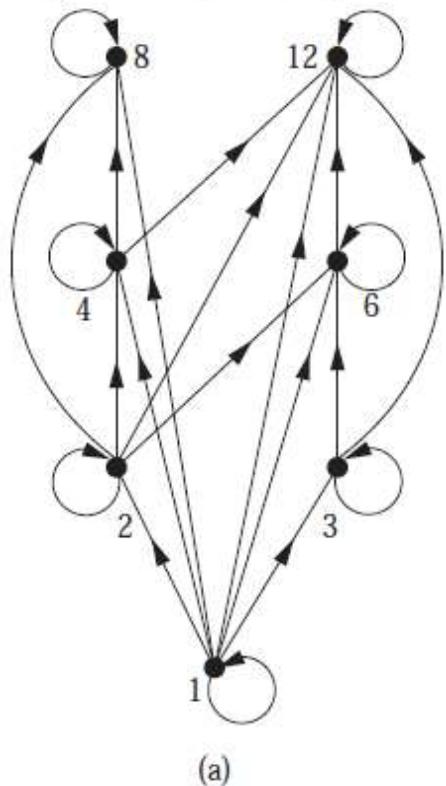
(c)



(d)

Draw the Hasse diagram representing the partial ordering $\{(a, b) | a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$.

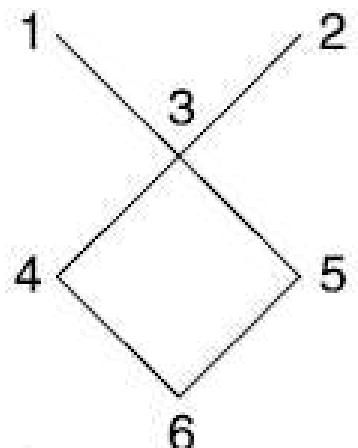
Solution: Begin with the digraph for this partial order, as shown in Figure 3(a). Remove all loops, as shown in Figure 3(b). Then delete all the edges implied by the transitive property. These are $(1, 4)$, $(1, 6)$, $(1, 8)$, $(1, 12)$, $(2, 8)$, $(2, 12)$, and $(3, 12)$. Arrange all edges to point upward, and delete all arrows to obtain the Hasse diagram. The resulting Hasse diagram is shown



UPPER AND LOWER BOUNDS

Sometimes it is possible to find an element that is greater than or equal to all the elements in a subset A of a poset (S, \preceq) . If u is an element of S such that $a \preceq u$ for all elements $a \in A$, then u is called an **upper bound** of A . Likewise, there may be an element less than or equal to all the elements in A . If l is an element of S such that $l \preceq a$ for all elements $a \in A$, then l is called a **lower bound** of A .

Example 1: $A = \{1, 2, 3, \dots, 6\}$ be ordered as pictured in



Solution: If $B = \{4, 5\}$ then

The upper bounds of B are 1, 2, 3

The lower bound of B is 6.

The element x is called the **least upper bound (LUB)** or supremum of the subset A of a poset $\{P, \leq\}$, if x is an upper bound that is less than every other upper bound of A .

Similarly the element y is called the **greatest lower bound (GLB)** or infimum of the subset A of a poset $\{P, \leq\}$, if y is a lower bound that is greater than every other lower bound of A .

Example: let us consider the poset with the Hasse diagram given in Fig

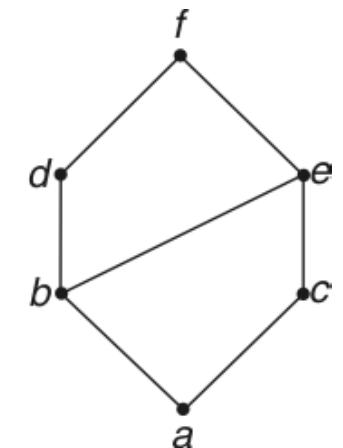
Solution: The upper bounds of the subset $\{a, b, c\}$ are e and f .

[Note: d is not an upper bound, since c is not related to d]

and LUB of $\{a, b, c\}$ is e .

The lower bounds of the subset $\{d, e\}$ are a and b and GLB of $\{d, e\}$ is b .

c is not a lower bound, since c is not related to d .



LATTICES

Definition:

A lattice is a partially ordered set $\{L, \leq\}$ in which every pair of elements $a, b \in L$ has a greatest lower bound and least upper bound.

The greatest lower bound of a subset $\{a, b\} \subseteq L$ will be denoted by $a * b$ and the least upper bound by $a \oplus b$.

Join or sum: The LUB of a subset $\{a, b\} \subseteq L$ is denoted by $a \oplus b$ (or $a \vee b$ or $a + b$) and is called the join or sum of a and b .

Meet or product: The GLB of a subset $\{a, b\} \subseteq L$ is denoted by $a * b$ (or $a \cdot b$ or $a \wedge b$) is called the meet or product of a and b .

A totally ordered set is trivially a lattice, but not all partially ordered sets are lattices

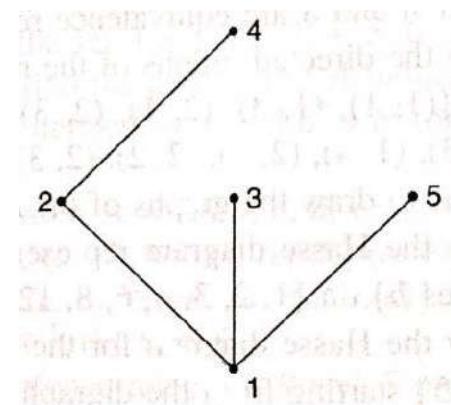
Example: $(\{1,2,4,8\}, |)$, where $|$ means ‘divisor of’. The hasse diagram

LUB = 8, GLB = 1

So, it is a lattice.

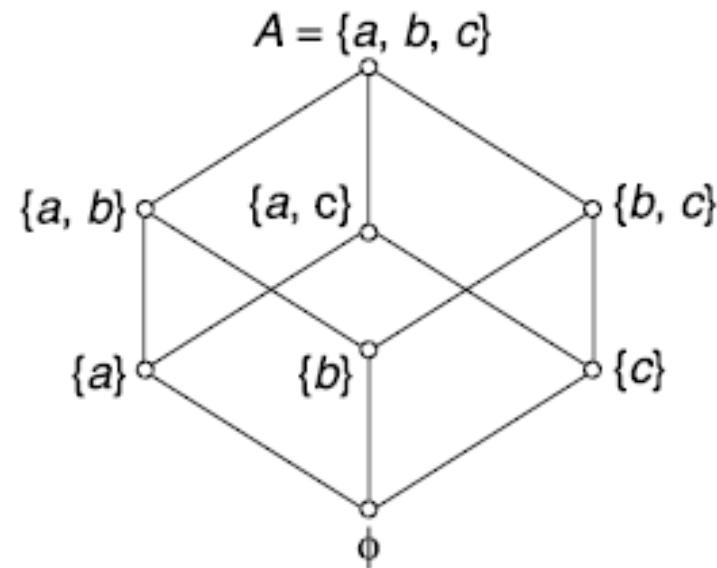


Example: $(\{1,2,3,4,5\}, |)$ It is not a lattice, since LUB of the pair $(2, 3)$ and $(3, 5)$ do not exist.



Example: In the case of power set $P(S)$ of any set S , $(P(S), \subseteq)$ is a lattice

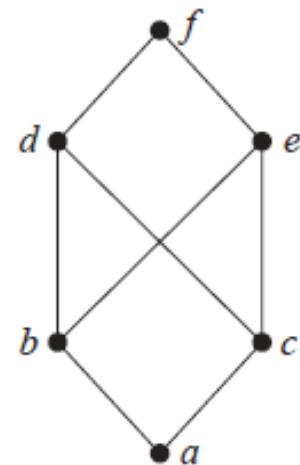
Here $LUB = A \cup B$ and $GLB = A \cap B$, where A and B are any subsets of $P(S)$.



Example: Is the poset $(Z^+, |)$ a lattice?

Solution: Let $a, b \in Z^+$, now, LUB of these two integers is the LCM (Least Common multiple) and GLB is the GCD (Greatest Common Divisor).

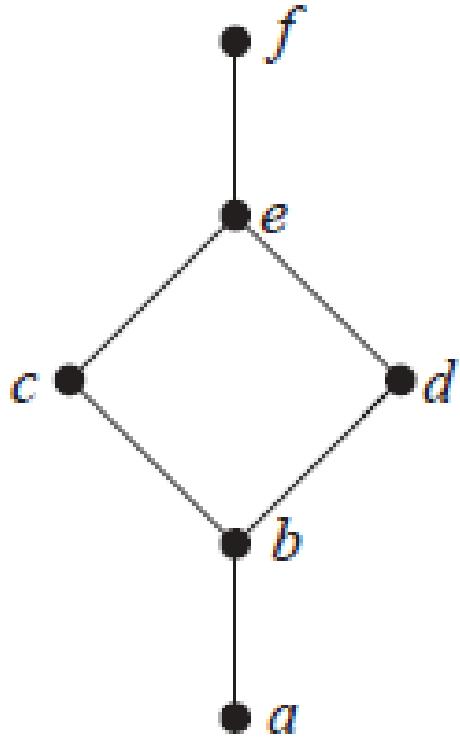
Example:



(b)

It is not a lattice since the pair (b, c) have no least upper bound.

Example:



It is a lattice since every pair of elements has LUB and GLB.

Properties of Lattice:

We shall first list some of the properties of the two binary operations of meet and join denoted by $*$ and \oplus on a lattice (L, \leq) .

For any $a, b, c \in L$, we have

Idempotent law

$$(L - 1) \quad a * a = a, \quad (L - 1)' \quad a \oplus a = a$$

Commutative Law

$$(L - 2) \quad a * b = b * a, \quad (L - 2)' \quad a \oplus b = b \oplus a$$

Associativity

$$(L - 3) \quad (a * b) * c = a * (b * c), \quad (L - 3)' \quad (a \oplus b) \oplus c = a \oplus (b \oplus c),$$

Absorption Law

$$(L - 4) \quad a * (a \oplus b) = a \quad (L - 4)' \quad a \oplus (a * b) = a$$

Lattices an Algebraic systems:

Definition:

A lattice is an algebraic system $\langle L, *, \oplus \rangle$ with two binary operation * and \oplus on L which are both (1) commutative and (2) associative and (3) satisfy the absorption laws. In other words the operation * and \oplus satisfy the identities (L-2) to (L-4) and (L-2)' to (L-4)'.

Sub lattices

Definition:

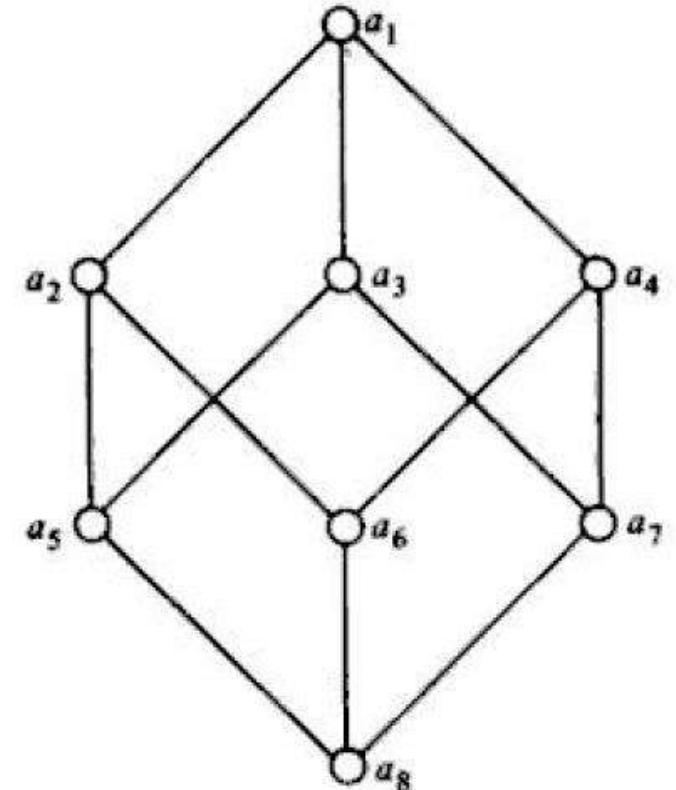
Let $\langle L, *, \oplus \rangle$ be lattices and let S is a subset of L . The algebra $\langle S, *, \oplus \rangle$ is a sub-lattices of $\langle L, *, \oplus \rangle$ iff S is closed under both operations * and \oplus .

Example 1:

Let $\langle L, \leq \rangle$ be a lattices in which $L = \{a_1, a_2, \dots, a_8\}$ and S_1, S_2 and S_3 be the subsets of L given by $S_1 = \{a_1, a_2, a_4, a_6\}$, $S_2 = \{a_3, a_5, a_7, a_8\}$ and $S_3 = \{a_1, a_2, a_4, a_8\}$.

Observe that $\langle S_1, \leq \rangle$ and $\langle S_2, \leq \rangle$ are sub lattices of $\langle L, \leq \rangle$

But $\langle S_3, \leq \rangle$ is not a sub lattices , because $a_2, a_4 \in S_3$ but $a_2 * a_4 = a_6 \notin S_3$ note that $\langle S_3, \leq \rangle$ is a lattices.



Example 2:

The lattices of divisor of any positive integer n denoted by $\langle S_n, | \rangle$ is a sub lattices of $\langle \mathbb{Z}^+, | \rangle$.

Some special lattices:

Definition:

A lattices is called **complete** if each of its non-empty subsets has a least upper bound and a greatest lower bound.

Definition:

A lattice $(L, *, \oplus)$ is said to be **bounded** if it has a greatest element and a least element. The greatest and least elements are denoted by 1 and 0 respectively.

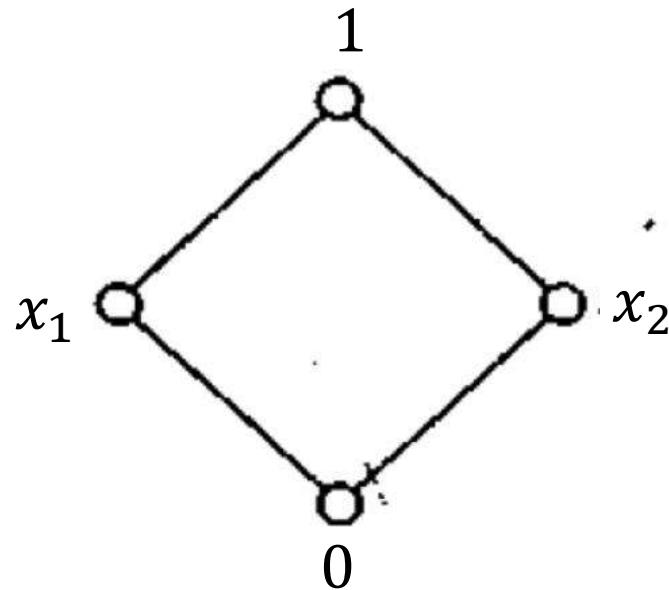
Definition:

In a bounded lattice $< L, *, \oplus, 0, 1 >$ an element $b \in L$ is called a **complement of an element** $a \in L$ if $a * b = 0$ & $a \oplus b = 1$.

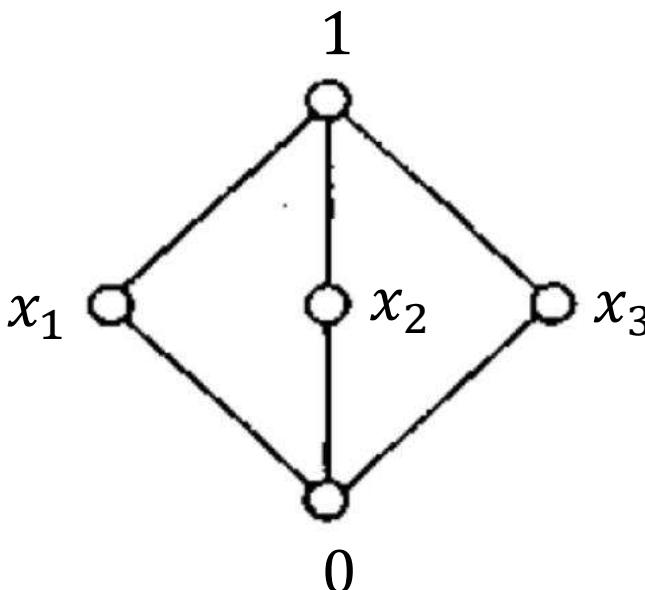
Definition:

A lattice $\langle L, *, \oplus, 0, 1 \rangle$ is said to be **complemented lattices** if every element of L has at least one complement.

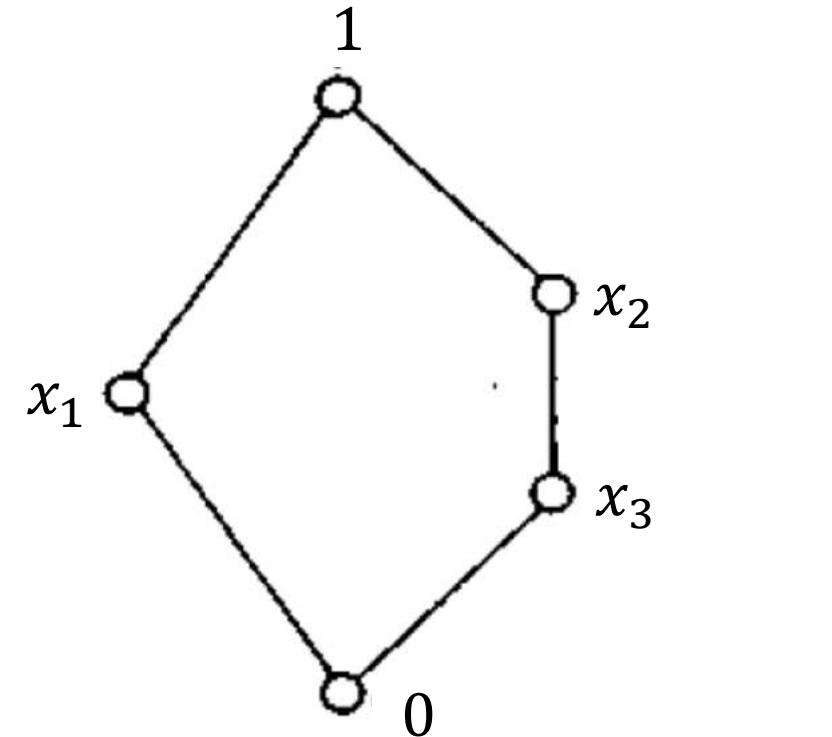
In fig some lattices are shown and the complement of some of the elements are noted below the diagram.



Complement of
 x_1 is x_2

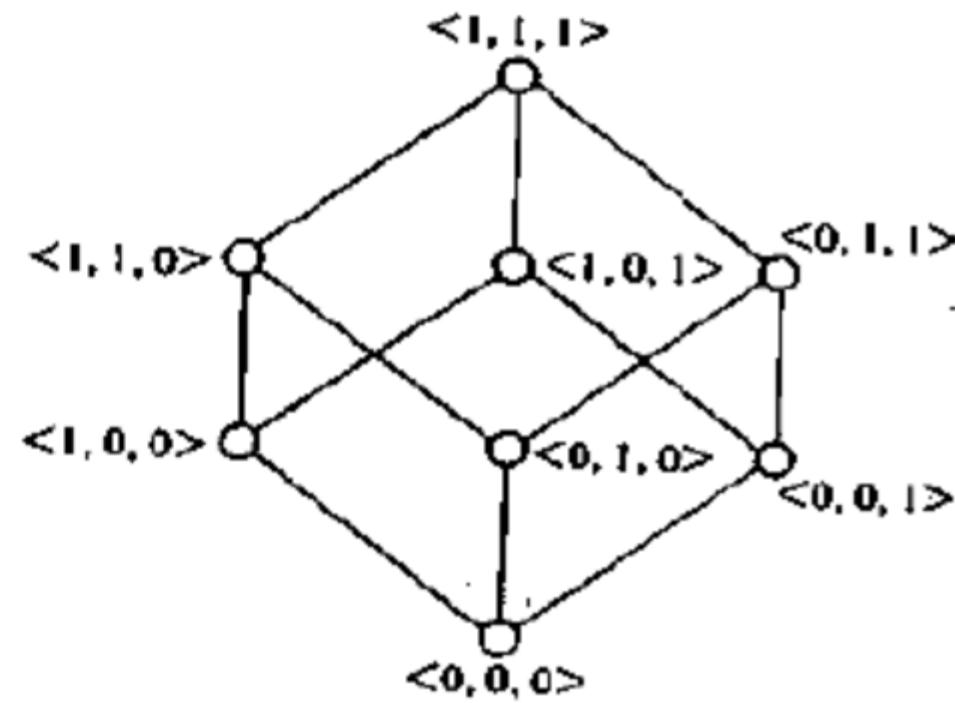
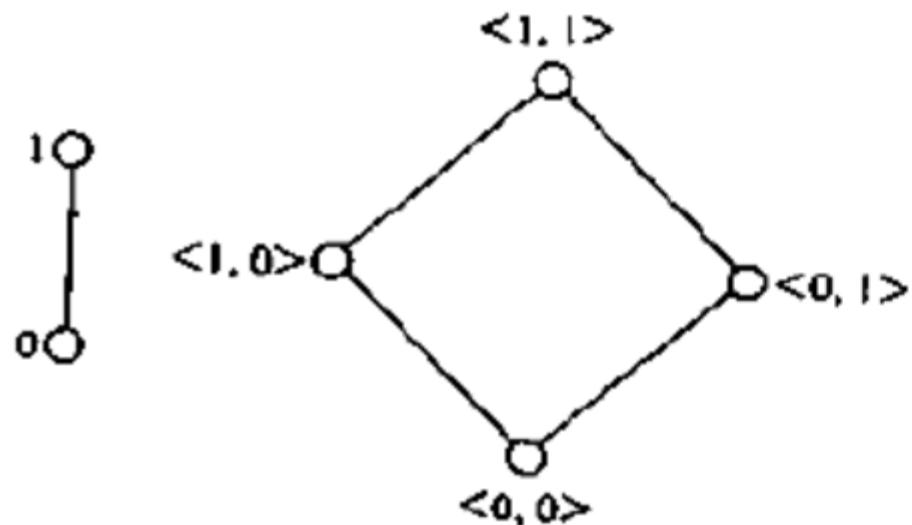


Complements of x_1 are
 x_2, x_3
Complements of x_2 are
 x_1, x_3



Complements of x_1 are x_2, x_3

let $L = \{0,1\}$ and the lattices $\langle L, \leq \rangle$ be as shown in fig.



The lattices $\langle L^2, \leq_2 \rangle$, $\langle L^3, \leq_3 \rangle$, are shown in fig .
In general of $\langle L^n, \leq_n \rangle$, is an n cube.

Example:

Let $\langle L^n, \leq_n \rangle$ be the lattice of n- tuples of 0 and 1 . This is a complemented lattice in which every element has a unique complement.

The complement of an element of L^n can obtained by interchanging 1 by 0 and 0 by 1 in the n- tuples representing the element. As a special case let n=3 . The bounds of $\langle L^n, \leq_n \rangle$, $\langle 0,0,0 \rangle$ and $\langle 1,1,1 \rangle$ the complement of $\langle 1,0,1 \rangle$ is $\langle 0,1,0 \rangle$

Definition:

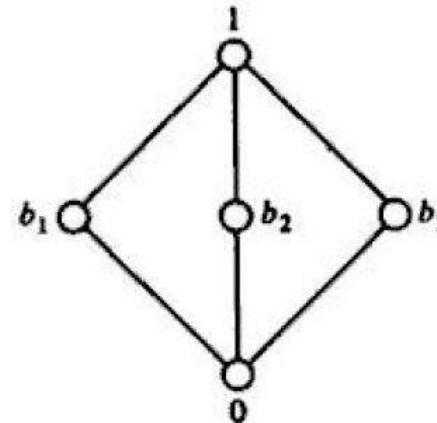
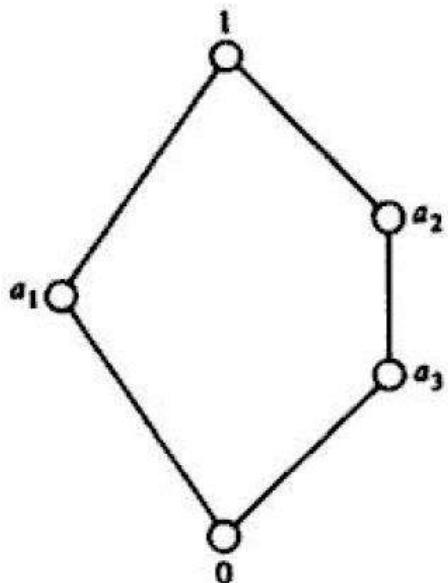
A lattices $\langle L, *, \oplus \rangle$ is called a distributive lattice if for any $a, b, c \in L$

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

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

Example :

show that the lattices given by the diagram are not distributive.



Solution:

$$a_3 * (a_1 \oplus a_2) = a_3 * 1 = a_3 = (a_3 * a_1) \oplus (a_3 * a_2)$$

$$a_1 * (a_2 \oplus a_3) = 0 = (a_1 * a_2) \oplus (a_1 * a_3)$$

But

$$a_2 * (a_1 \oplus a_3) = a_2 * 1 = a_2$$

$$(a_2 * a_1) \oplus (a_2 * a_3) = 0 * a_3 = a_3$$

hence the lattices is not distributive . In the other case,

$$b_1 * (b_2 \oplus b_3) = b_1 \text{ while } (b_1 * b_2) \oplus (b_1 * b_3) = 0$$

which shows that the lattices is not distributive.

4

LATTICES AND BOOLEAN ALGEBRA

INTRODUCTION

The statement algebra of Chap. 1 and the algebra of sets given in Chap. 2 provide a motivation for the study of an abstract algebraic system possessing all the essential properties of these algebras. Such an algebraic system was introduced by George Boole in 1854 and is known as Boolean algebra. Before we study Boolean algebra in this chapter, we consider a more general algebraic system called a lattice. A Boolean algebra is then introduced as a special lattice.

A basic difference between the algebraic systems studied in this chapter and those given in Chap. 3 is the fact that the ordering relation plays a significant role in the algebraic systems studied here. In order to emphasize the role of an ordering relation, a lattice is first introduced as a partially ordered set, followed by the definition of a lattice as an algebraic system.

Both lattices and Boolean algebra have important applications in the theory and design of computers. There are many other areas such as engineering and science to which Boolean algebra is applied.

4-1 LATTICES AS PARTIALLY ORDERED SETS

In this section we introduce a lattice as a partially ordered set satisfying certain properties. Partially ordered sets, their properties, and associated terminology given in Sec. 2-3.9 will be used throughout our discussion here. In particular, the notion of the least upper bound (LUB) and the greatest lower bound (GLB) of a subset of a partially ordered set will be used repeatedly.

4-1.1 Definition and Examples

Definition 4-1.1 A *lattice* is a partially ordered set (L, \leq) in which every pair of elements $a, b \in L$ has a greatest lower bound and a least upper bound.

The greatest lower bound of a subset $\{a, b\} \subseteq L$ will be denoted by $a * b$ and the least upper bound by $a \oplus b$. It is customary to call the GLB $\{a, b\} = a * b$ the *meet* or *product* of a and b , and the LUB $\{a, b\} = a \oplus b$ the *join* or *sum* of a and b . Other symbols such as \wedge and \vee or \cdot and $+$ are also used to denote the meet and join of two elements respectively. When using the symbols \cdot and $+$ it is not uncommon to suppress the dot and write $a \cdot b$ simply as ab . In certain cases, the symbols \cap and \cup are also used to denote the meet and join respectively. It follows from the definition of a lattice that both $*$ and \oplus are binary operations on L because of the uniqueness of the least upper bound and greatest lower bound of any subset of a partially ordered set.

A totally ordered set is trivially a lattice, but not all partially ordered sets are lattices, as can be seen from the Hasse diagrams of some of the partially ordered sets given in Figs. 4-1.1 and 4-1.2. For the sake of brevity, throughout this chapter we shall refer to the Hasse diagrams simply as the diagrams of partially ordered sets. Naturally, the diagram of a totally ordered set is a chain.

The following are some examples of lattices. These examples will be referred to frequently throughout this chapter.

EXAMPLE 1 Let S be any set and $\rho(S)$ be its power set. The partially ordered set $(\rho(S), \subseteq)$ is a lattice in which the meet and join are the same as the operations \cap and \cup respectively. In particular, when S has a single element, the corresponding lattice is a chain containing two elements. When S has two and three elements, the diagrams of the corresponding lattices are as shown in Fig. 4-1.1b and f respectively.

EXAMPLE 2 Let \mathbb{L}_+ be the set of all positive integers, and let D denote the relation of "division" in \mathbb{L}_+ such that for any $a, b \in \mathbb{L}_+$, $a D b$ iff a divides b . Then (\mathbb{L}_+, D) is a lattice in which the join of a and b is given by the least common multiple (LCM) of a and b , that is, $a \oplus b = \text{LCM of } a \text{ and } b$, and the meet of a and b , that is, $a * b$ is the greatest common divisor (GCD) of a and b .

EXAMPLE 3 Let n be a positive integer and S_n be the set of all divisors of n ; for example, $n = 6$, $S_6 = \{1, 2, 3, 6\}$ and for $n = 24$, $S_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$. Let D denote the relation of "division" as defined in Example 2. The

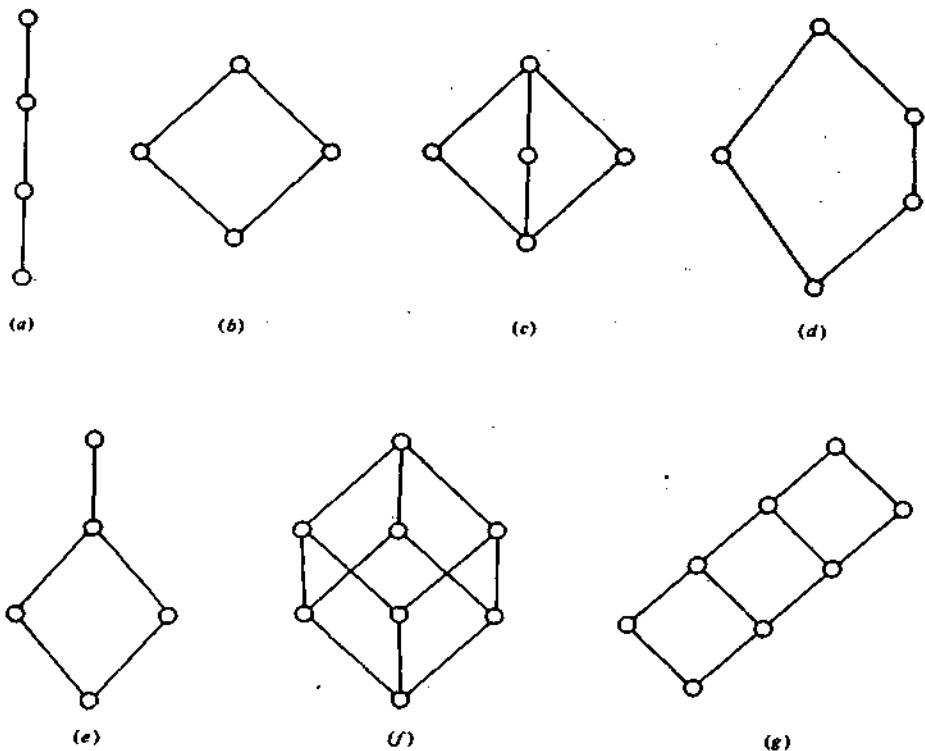


FIGURE 4-1.1 Lattices.

lattices $\langle S_8, D \rangle$, $\langle S_{24}, D \rangle$, $\langle S_8, D \rangle$, and $\langle S_{20}, D \rangle$ are given in Fig. 4-1.1b, g, a, and f respectively.

EXAMPLE 4 Let S be a nonempty set and $\Pi(S)$ be the set of all partitions of S . Two binary operations $*$ and \oplus on $\Pi(S)$ were introduced in Sec. 3-2-1. We can also define a corresponding partial ordering relation \leq on $\Pi(S)$ such that for $\Pi_1, \Pi_2 \in \Pi(S)$, $\Pi_1 \leq \Pi_2$ iff every block of Π_1 is a subset of some block of Π_2 . It is easy to see that $(\Pi(S), \leq)$ is a lattice in which the operations $*$ and \oplus are the required meet and join respectively.

In particular, let $S = \{a, b, c\}$; then

$$\Pi(S) = \{\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Pi_5\}$$

$$\text{where } \Pi_1 = \{\overline{a, b, c}\} \quad \Pi_2 = \{\overline{a, b, \bar{c}}\} \quad \Pi_3 = \{\overline{a, \bar{c}, \bar{b}}\}$$

$$\Pi_4 = \{\bar{a}, \overline{b, c}\} \quad \text{and} \quad \Pi_5 = \{\bar{a}, \bar{b}, \bar{c}\}$$

The diagram of $\langle \Pi(S), \leq \rangle$ is given in Fig. 4-1-1c.

One can show that there are 15 partitions of a set of four elements, 52 partitions of a set of five elements, and so on.

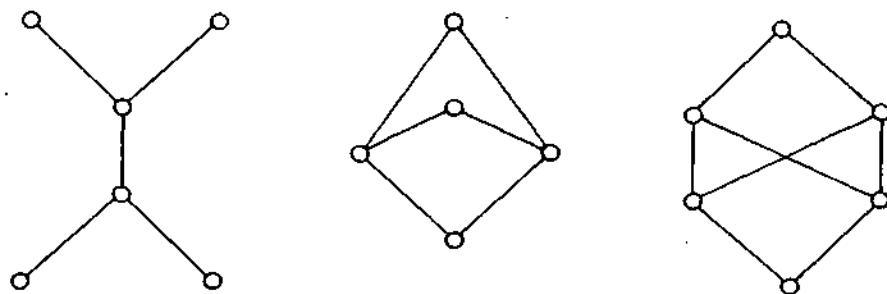


FIGURE 4-1.2 Partially ordered sets which are not lattices.

The previous examples show that different lattices can be represented by the same diagram except that the nodes have different labels. We show in Sec. 4-1-4 that different partially ordered sets may be represented by the same diagram if they are order-isomorphic.

Recall that for any partial ordering relation \leq on a set S , the converse relation \geq is also a partial ordering relation on S . The diagram of $\langle S, \geq \rangle$ can be obtained from that of $\langle S, \leq \rangle$ by simply turning it upside down. The partially ordered sets $\langle S, \leq \rangle$ and $\langle S, \geq \rangle$ are called duals of each other. If $A \subseteq S$, then LUB A with respect to the relation \leq is the same as GLB A with respect to the relation \geq , and vice versa. In other words, the GLB and LUB are interchanged if we interchange the relations \leq and \geq . In terms of lattices, we can say that the operations of meet and join on $\langle L, \leq \rangle$ become the operations of join and meet on $\langle L, \geq \rangle$. In any case, $\langle L, \geq \rangle$ is a lattice if $\langle L, \leq \rangle$ is a lattice. We may now formulate the *principle of duality* of lattices as follows.

Any statement about lattices involving the operations $*$ and \oplus and the

relations \leq and \geq remains true if $*$ is replaced by \oplus , \oplus by $*$, \leq by \geq , and \geq by \leq .

The operations $*$ and \oplus are called *duals* of each other as are the relations \leq and \geq . Similarly, the lattices $\langle L, \leq \rangle$ and $\langle L, \geq \rangle$ are called duals of each other.

EXERCISES 4-1.1

- 1 Explain why the partially ordered sets given in Fig. 4-1.2 are not lattices.
- 2 Draw the diagrams of lattices $\langle S_n, D \rangle$ given in Example 3 for $n = 4, 6, 10, 12, 15, 45, 60, 75$, and 210. For what values of n do you expect $\langle S_n, D \rangle$ to be a chain?
- 3 Show that there are 15 partitions of a set of four elements. Draw the diagram of the corresponding lattice.
- 4 Show that the operations of meet and join on a lattice are commutative, associative, and idempotent.
- 5 Let $S = \{a, b, c\}$. Draw the diagram of $\langle \wp(S), \subseteq \rangle$.
- 6 Let R be the set of real numbers in $[0, 1]$ and \leq be the usual operation of "less than or equal to" on R . Show that $\langle R, \leq \rangle$ is a lattice. What are the operations of meet and join on this lattice?
- 7 Let the sets S_0, S_1, \dots, S_7 be given by

$$S_0 = \{a, b, c, d, e, f\} \quad S_1 = \{a, b, c, d, e\} \quad S_2 = \{a, b, c, e, f\}$$

$$S_3 = \{a, b, c, e\} \quad S_4 = \{a, b, c\} \quad S_5 = \{a, b\} \quad S_6 = \{a, c\} \quad S_7 = \{a\}$$

Draw the diagram of $\langle L, \subseteq \rangle$ where $L = \{S_0, S_1, \dots, S_7\}$.

4-1.2 Some Properties of Lattices

We shall first list some of the properties of the two binary operations of meet and join denoted by $*$ and \oplus on a lattice $\langle L, \leq \rangle$. For any $a, b, c \in L$, we have:

- | | |
|---|--|
| $(L-1) \quad a * a = a$
$(L-2) \quad a * b = b * a$
$(L-3) \quad (a * b) * c = a * (b * c)$
$(L-4) \quad a * (a \oplus b) = a$ | $(L-1)' \quad a \oplus a = a$
$(L-2)' \quad a \oplus b = b \oplus a$
$(L-3)' \quad (a \oplus b) \oplus c = a \oplus (b \oplus c)$
$(L-4)' \quad a \oplus (a * b) = a$ |
| | <i>(Idempotent)</i>
<i>(Commutative)</i>
<i>(Associative)</i>
<i>(Absorption)</i> |

The identities (L-1) to (L-4) can be proved using the definitions of the operators $*$ and \oplus . The identities (L-1)' to (L-4)' then follow from the principle of duality. The latter identities can also be proved directly. We shall prove the identity (L-4).

For any $a \in L$, $a \leq a$ and $a \leq a \oplus b$ by definition of \oplus ; hence $a \leq a * (a \oplus b)$. On the other hand, $a * (a \oplus b) \leq a$ by the definition of $*$. Therefore, $a * (a \oplus b) = a$.

These identities along with the following theorem will be used in defining a lattice as an algebraic system in the next section.

Theorem 4-1.1 Let $\langle L, \leq \rangle$ be a lattice in which $*$ and \oplus denote the operations of meet and join respectively. For any $a, b \in L$,

$$a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$$

PROOF We shall first prove that $a \leq b \Leftrightarrow a * b = a$. In order to do this, let us assume that $a \leq b$. We also know that $a \leq a$. Therefore $a \leq a * b$. But from the definition of $a * b$, we have $a * b \leq a$. Hence $a \leq b \Rightarrow a * b = a$. Next, assume that $a * b = a$; but it is only possible if $a \leq b$, that is, $a * b = a \Rightarrow a \leq b$. Combining these two results, we get the required equivalence.

It is possible to show that $a \leq b \Leftrightarrow a \oplus b = b$ in a similar manner. Alternatively, from $a * b = a$, we have

$$b \oplus (a * b) = b \oplus a = a \oplus b$$

but

$$b \oplus (a * b) = b$$

Hence $a \oplus b = b$ follows from $a * b = a$. By repeating similar steps, we can show that $a * b = a$ follows from $a \oplus b = b$, and hence these are equivalent. ////

Theorem 4-1.1 establishes a connection between the partial ordering relation \leq and the two binary operations $*$ and \oplus on the meet and join in a lattice $\langle L, \leq \rangle$. We shall use this result in Sec. 4-1.3 to show that a lattice can be defined as an algebraic system. We now prove some basic inequalities that hold between the elements of a lattice.

Theorem 4-1.2 Let $\langle L, \leq \rangle$ be a lattice. For any $a, b, c \in L$, the following properties called *isotonicity* hold.

$$b \leq c \Rightarrow \begin{cases} a * b \leq a * c \\ a \oplus b \leq a \oplus c \end{cases}$$

PROOF From Theorem 4-1.1,

$$b \leq c \Leftrightarrow b * c = b$$

To show that $a * b \leq a * c$, we shall show that

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

Note that

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

The second result can be proved in a similar manner. ////

We shall now list some implications which hold for any $a, b, c \in L$ where $\langle L, \leq \rangle$ is a lattice. These implications follow from the definitions of the opera-

tions $*$ and \oplus on L . They can also be proved by using the properties of isotonicity.

$$a \leq b \wedge a \leq c \Rightarrow a \leq b \oplus c \quad (1)$$

$$a \leq b \wedge a \leq c \Rightarrow a \leq b * c \quad (2)$$

Of course (1) is obvious from the definition of \oplus . Implication (2) can also be proved from the definition of $*$ and from the fact that both b and c are comparable to a . It can also be proved by using Theorem 4-1.2. In a similar manner, we can write the duals of (1) and (2) as

$$a \geq b \wedge a \geq c \Rightarrow a \geq b * c \quad (3)$$

$$a \geq b \wedge a \geq c \Rightarrow a \geq b \oplus c \quad (4)$$

We shall frequently employ these implications in our proofs.

Theorem 4-1.3 Let $\langle L, \leq \rangle$ be a lattice. For any $a, b, c \in L$, the following inequalities, called the *distributive inequalities*, hold:

$$a \oplus (b * c) \leq (a \oplus b) * (a \oplus c)$$

$$a * (b \oplus c) \geq (a * b) \oplus (a * c)$$

PROOF From $a \leq a \oplus b$ and $a \leq a \oplus c$ we have, using (2),

$$a \leq (a \oplus b) * (a \oplus c) \quad (5)$$

$$b * c \leq b \leq a \oplus b$$

and

$$b * c \leq c \leq a \oplus c$$

Hence, by using (2) again we get

$$b * c \leq (a \oplus b) * (a \oplus c) \quad (6)$$

From (5) and (6) and by using (4), we get the required inequality

$$a \oplus (b * c) \leq (a \oplus b) * (a \oplus c)$$

The second distributive inequality can be proved in a similar manner or by using the principle of duality. ////

Theorem 4-1.4 Let $\langle L, \leq \rangle$ be a lattice. For any $a, b, c \in L$ the following holds:

$$a \leq c \Leftrightarrow a \oplus (b * c) \leq (a \oplus b) * c \quad (7)$$

PROOF Since $a \leq c \Leftrightarrow a \oplus c = c$ from Theorem 4-1.1, we get the required result by substituting c for $a \oplus c$ in the first distributive inequality. One could prove the above equivalence directly using an argument similar to the one given in the proof of Theorem 4-1.3. ////

The inequality given in Theorem 4-1.4 is called the *modular inequality*. There are other ways in which the modular inequalities are expressed:

$$(a * b) \oplus (a * c) \leq a * [b \oplus (a * c)] \quad (8)$$

$$(a \oplus b) * (a \oplus c) \geq a \oplus [b * (a \oplus c)] \quad (9)$$

The method of proof is similar to the one used in proving Theorem 4-1.3. We shall leave it as an exercise.

EXERCISES 4-1.2

1 Show that the identities (L-1) and (L-1)' follow from the identities (L-2) to (L-4) and their duals.

2 Complete the proof of Theorem 4-1.1 by showing that in a lattice

$$a \leq b \Leftrightarrow a \oplus b = b$$

3 Show that in a lattice if $a \leq b \leq c$, then

$$a \oplus b = b * c$$

and

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

4 Show that in a lattice if $a \leq b$ and $c \leq d$, then $a * c \leq b * d$.

5 In a lattice, show that

$$(a * b) \oplus (c * d) \leq (a \oplus c) * (b \oplus d)$$

$$(a * b) \oplus (b * c) \oplus (c * a) \leq (a \oplus b) * (b \oplus c) * (c \oplus a)$$

6 Show that a lattice with three or fewer elements is a chain.

7 Prove that every finite subset of a lattice has an LUB and a GLB. (*Hint:* Use the principle of mathematical induction.) What can you say about a finite lattice?

8 Prove inequalities (8) and (9).

9 Show that Theorem 4-1.4 is a self-dual.

4-1.3 Lattices as Algebraic Systems

In this section we define a lattice as an algebraic system on which it is possible to define a partial ordering relation. The advantage of considering a lattice as an algebraic system is that many concepts which are associated with algebraic systems can be applied to lattices as well. Thus it is possible to define sublattices, direct product of lattices, and also lattice homomorphisms.

Definition 4-1.2 A lattice is an algebraic system $\langle L, *, \oplus \rangle$ with two binary operations $*$ and \oplus on L which are both (1) commutative and (2) associative and (3) satisfy the absorption laws. In other words, the operations $*$ and \oplus satisfy the identities (L-2) to (L-4) and (L-2)' to (L-4)' given in Sec. 4-1.2.

The absence of the identities (L-1) and (L-1)' in the definition here is due to the fact that (L-4) and its dual imply the identities (L-1) and (L-1)' as follows. For any $a \in L$,

$$a * a = a * [a \oplus (a * a)] = a$$

where we have replaced the second a in $a * a$ by $a \oplus (a * a)$ and then from (L-4)' obtained a in the second step. The identity $a \oplus a = a$ can be proved in a similar manner or by the principle of duality.

Note that Definition 4-1.2 does not assume the existence of any partial

ordering on L . We shall now show that a partial ordering relation on L follows as a consequence of the properties of the operations $*$ and \oplus .

Let us define a relation R on L such that for $a, b \in L$

$$a R b \Leftrightarrow a * b = a$$

Obviously, for any $a \in L$, $a * a = a$, so that $a R a$, or the relation R is reflexive. Now for some $a, b \in L$ let us assume that $a R b$ and $b R a$, so that $a * b = a$ and $b * a = b$. But $a * b = b * a$, and so $a = b$. The assumptions $a R b$ and $b R a$ imply $a = b$, or that the relation R is antisymmetric. Finally, let us assume that for some $a, b, c \in L$, $a R b$ and $b R c$. This requires that $a * b = a$ and $b * c = b$. Thus, $a * c = (a * b) * c = a * (b * c) = a * b = a$, or $a R c$. The last step shows that the relation R is transitive. From this we can conclude that R is a partial ordering relation.

It is easy to show that $a * b = a \Leftrightarrow a \oplus b = b$. Hence we could have defined the same partial ordering relation R on L as

$$a R b \Leftrightarrow a \oplus b = b \quad \text{for any } a, b \in L$$

Our next step is to show that for any two elements $a, b \in L$, the greatest lower bound and the least upper bound of $\{a, b\} \subseteq L$ with respect to the partial ordering R are $a * b$ and $a \oplus b$, respectively.

From the absorption laws $a * (a \oplus b) = a$ and $b * (a \oplus b) = b$, we have $a R (a \oplus b)$ and $b R (a \oplus b)$. Let us now assume that there exists an element $c \in L$ such that $a R c$ and $b R c$. This means that

$$a \oplus c = c \quad \text{and} \quad b \oplus c = c$$

$$\text{or} \quad (a \oplus c) \oplus (b \oplus c) = (a \oplus b) \oplus c = c \oplus c = c$$

implying that $(a \oplus b) R c$. The last step shows that $a \oplus b$ is the least upper bound of a and b . In a similar manner, we can show that $a * b$ is the greatest lower bound of $\{a, b\}$ with respect to the partial ordering relation R . We can summarize the discussion by saying that on a lattice $\langle L, *, \oplus \rangle$ it is possible to define a partial ordering relation R such that for any $a, b \in L$

$$a R b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$$

and that $\text{LUB } \{a, b\} = a \oplus b$ and $\text{GLB } \{a, b\} = a * b$ with respect to the relation R on L .

On the other hand, it was shown earlier in Sec. 4-1.1 that in a lattice $\langle L, \leq \rangle$ defined as a partially ordered set, it is possible to define two binary operations $*$ and \oplus such that for any $a, b \in L$

$$a * b = \text{GLB } \{a, b\} \quad \text{and} \quad a \oplus b = \text{LUB } \{a, b\}$$

and

$$a \leq b \Leftrightarrow a * b = a \Leftrightarrow a \oplus b = b$$

where the operations $*$ and \oplus are both commutative and associative and satisfy the absorption laws. This establishes the equivalence of the two definitions where the relation R is the same as the relation \leq on L .

4-1.4 Sublattices, Direct Product, and Homomorphism

The advantage of defining a lattice as an algebraic system is that we can introduce the concept of sublattices in a natural way.

Definition 4-1.3 Let $\langle L, *, \oplus \rangle$ be a lattice and let $S \subseteq L$ be a subset of L . The algebra $\langle S, *, \oplus \rangle$ is a sublattice of $\langle L, *, \oplus \rangle$ iff S is closed under both operations $*$ and \oplus .

From the definition it follows that a sublattice itself is a lattice. However, any subset of L which is a lattice need not be a sublattice, as will be shown by an example. Note that for a partially ordered set the situation is simpler in the sense that every subset of a partially ordered set is also a partially ordered set under the same partial ordering relationship. Thus, if $\langle P, \leq \rangle$ is a partially ordered set and $Q \subseteq P$, then $\langle Q, \leq \rangle$ is also a partially ordered set.

For a lattice $\langle L, *, \oplus \rangle$ and for any two elements $a, b \in L$ such that $a \leq b$, the closed interval $[a, b]$ consisting of all the elements $x \in L$ such that $a \leq x \leq b$ is a sublattice of L .

EXAMPLE 1 Let $\langle L, \leq \rangle$ be a lattice in which $L = \{a_1, a_2, \dots, a_6\}$ and S_1 , S_2 , and S_3 be the subsets of L given by $S_1 = \{a_1, a_2, a_4, a_6\}$, $S_2 = \{a_3, a_4, a_5, a_6\}$, and $S_3 = \{a_1, a_2, a_4, a_5\}$. The diagram of $\langle L, \leq \rangle$ is given in Fig. 4-1.3. Observe that $\langle S_1, \leq \rangle$ and $\langle S_2, \leq \rangle$ are sublattices of $\langle L, \leq \rangle$, but $\langle S_3, \leq \rangle$ is not a sublattice, because $a_2, a_4 \in S_3$ but $a_2 * a_4 = a_6 \notin S_3$. Note that $\langle S_3, \leq \rangle$ is a lattice.

EXAMPLE 2 The lattice of divisors of any positive integer n given in Example 3, Sec. 4-1.1, and denoted by $\langle S_n, D \rangle$ is a sublattice of $\langle I_+, D \rangle$ given in Example 2 of the same section.

EXAMPLE 3 Let S be any set and $\rho(S)$ be its power set. It was shown in Example 1, Sec. 4-1.1, that $\langle \rho(S), \subseteq \rangle$ is a lattice in which the meet and join are the usual operations of intersection and union respectively. A family of subsets of S such that for any two subsets A and B in this family both $A \cap B$ and $A \cup B$ are in the family, is obviously a sublattice of $\langle \rho(S), \subseteq \rangle$. Such a family is called a *ring of subsets* of S and is denoted by $\langle R(S), \cap, \cup \rangle$. The lattice $\langle R(S), \cap, \cup \rangle$ is not a ring in the sense of the definition of a ring given in Sec. 3-5.5; that is why some authors prefer to call it a *lattice of subsets*.

As a particular case of Example 3, let $S = \{p, q, r\}$. The diagram of the lattice $\langle \rho(S), \cap, \cup \rangle$ is the same as given in Fig. 4-1.3 in which $a_1 = S = \{p, q, r\}$, $a_2 = \{p, q\}$, $a_3 = \{p, r\}$, $a_4 = \{q, r\}$, $a_5 = \{p\}$, $a_6 = \{q\}$, $a_7 = \{r\}$, and $a_8 = \emptyset$. The sets S_1 and S_2 given in Example 1 are both examples of a ring of subsets of S and are sublattices of $\langle \rho(S), \cap, \cup \rangle$.

Definition 4-1.4 Let $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$ be two lattices. The algebraic system $\langle L \times S, \cdot, + \rangle$ in which the binary operations \cdot and $+$ on $L \times S$

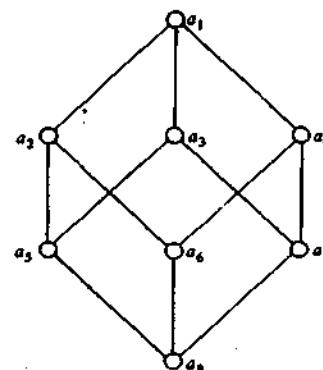


FIGURE 4-1.3

are such that for any $\langle a_1, b_1 \rangle$ and $\langle a_2, b_2 \rangle$ in $L \times S$

$$\langle a_1, b_1 \rangle \cdot \langle a_2, b_2 \rangle = \langle a_1 * a_2, b_1 \wedge b_2 \rangle$$

$$\langle a_1, b_1 \rangle + \langle a_2, b_2 \rangle = \langle a_1 \oplus a_2, b_1 \vee b_2 \rangle$$

is called the *direct product* of the lattices $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$.

The operations $+$ and \cdot on $L \times S$ are commutative and associative and satisfy the absorption laws because they are defined in terms of the operations $*$, \oplus and \wedge , \vee . Therefore, the direct product is itself a lattice. Since $\langle L \times S, \cdot, + \rangle$ is a lattice, we can form a direct product of this lattice with another lattice, and so on. As before, we shall write $L \times L$ as L^2 and $L \times L \times L$ as L^3 . The order of the lattice formed by the direct product of two lattices is equal to the product of the orders of the lattices appearing in the direct product. It should be noted that not all lattices can be written as a direct product of other lattices. The direct product of lattices can be used to construct large lattices from smaller ones.

EXAMPLE 4 Let $L = \{0, 1\}$ and the lattice $\langle L, \leq \rangle$ be as shown in Fig. 4-1.4. The lattices $\langle L^2, \leq_2 \rangle$, $\langle L^3, \leq_3 \rangle$ are shown in Fig. 4-1.4. In general, the diagram of $\langle L^n, \leq_n \rangle$ is an n cube.

Note that in the lattice $\langle L^n, \leq_n \rangle$ any element can be written as $\langle a_1, a_2, \dots, a_n \rangle$ in which a_i is either 0 or 1 for $i = 1, 2, \dots, n$. The partial ordering relation \leq_n on L^n can be defined for any $a, b \in L^n$, where $a = \langle a_1, a_2, \dots, a_n \rangle$ and $b = \langle b_1, b_2, \dots, b_n \rangle$, as

$$a \leq_n b \Leftrightarrow a_i \leq b_i \quad \text{for all } i = 1, 2, \dots, n$$

where \leq means the relation of "less than or equal to" on $\{0, 1\}$. The operations $*$ and \oplus on L^n can also be defined easily. The lattice $\langle L^n, \leq_n \rangle$ will be called the *lattice of n-tuples of 0 and 1*.

EXAMPLE 5 Consider the chains of divisors of 4 and 9, that is, $L_1 = \{1, 2, 4\}$ and $L_2 = \{1, 3, 9\}$, and the partial ordering relation of "division" on L_1 and L_2 . The lattice $L_1 \times L_2$ is shown in Fig. 4-1.5. Notice that the diagram of the lattice

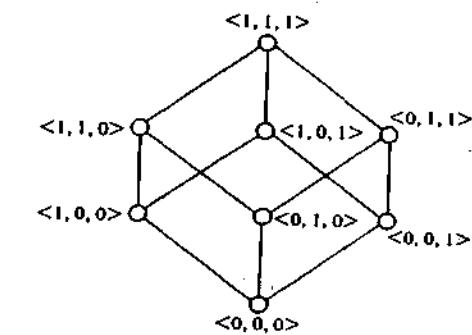
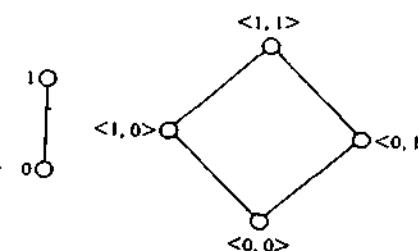


FIGURE 4-1.4

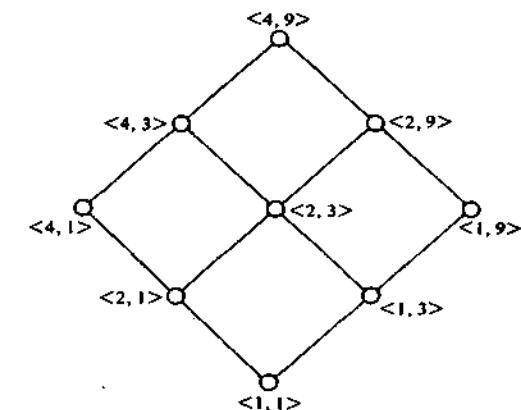


FIGURE 4-1.5

of divisors of 36 is the same as the one given in Fig. 4-1.5 except that the node $\langle a, b \rangle$ is replaced by the product ab .

Definition 4-1.5 Let $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$ be two lattices. A mapping $g: L \rightarrow S$ is called a *lattice homomorphism* from the lattice $\langle L, *, \oplus \rangle$ to $\langle S, \wedge, \vee \rangle$ if for any $a, b \in L$,

$$g(a * b) = g(a) \wedge g(b) \quad \text{and} \quad g(a \oplus b) = g(a) \vee g(b)$$

Observe that both the operations of meet and join are preserved. There may be mappings which preserve only one of the two operations. Such mappings are not lattice homomorphisms.

Let $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$ be two lattices and the partial ordering relations on L and S corresponding to the operations of meet and join be \leq and

\leq' respectively. If $g: L \rightarrow S$ is a homomorphism, then we show that g preserves the ordering relations also; i.e., for any $a, b \in L$ such that $a \leq b$, we must have $g(a) \leq' g(b)$.

From $a \leq b \Leftrightarrow a * b = a$, we have

$$g(a * b) = g(a) \wedge g(b) = g(a) \Leftrightarrow g(a) \leq' g(b)$$

This means $a \leq b \Rightarrow g(a) \leq' g(b)$ if g is a homomorphism.

If a homomorphism $g: L \rightarrow S$ of two lattices $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$ is bijective, i.e., one-to-one onto, then g is called an *isomorphism*. If there exists an isomorphism between two lattices, then the lattices are called *isomorphic*.

If the lattices $\langle L, *, \oplus \rangle$ and $\langle S, \wedge, \vee \rangle$ are isomorphic and g denotes an isomorphism, then g preserves the ordering relation; i.e., for any $a, b \in L$, $a \leq b \Rightarrow g(a) \leq' g(b)$. In addition to this, we also have $g(a) \leq' g(b) \Rightarrow a \leq b$. This result also shows that the two lattices which are isomorphic can be represented by the same diagram in which the nodes are replaced by the images. This fact explains why we found that several different lattices could be represented by the same diagram.

EXAMPLE 6 Let S be any set containing n elements and $\rho(S)$ be its power set. The lattice $\langle \rho(S), \cap, \cup \rangle$ or $\langle \rho(S), \subseteq \rangle$ is isomorphic to the lattice $\langle L^n, \leq_n \rangle$ given in Example 4.

It is interesting to observe that the lattices with one, two, or three elements are isomorphic to the chains containing one, two, or three elements, respectively. On the other hand, any lattice of order 4 must be isomorphic to one of the two lattices given in Figs. 4-1.1 a and b. Similarly, any lattice of order 5 is isomorphic to one of the lattices whose diagrams are given in Fig. 4-1.6.

A homomorphism $g: L \rightarrow L$ where $\langle L, *, \oplus \rangle$ is a lattice is called an *endomorphism*. If $g: L \rightarrow L$ is an isomorphism, then g is called an *automorphism*.

It is interesting to observe that if $g: L \rightarrow L$ is an endomorphism, then the image set of g is a sublattice of L .

Although the concepts of homomorphism and isomorphism are associated with any algebraic system, we shall now show how these concepts can be applied to partially ordered sets also.

Definition 4-1.6 Let $\langle P, \leq \rangle$ and $\langle Q, \leq' \rangle$ be two partially ordered sets. A mapping $f: P \rightarrow Q$ is said to be *order-preserving* relative to the ordering \leq in P and \leq' in Q iff for any $a, b \in P$ such that $a \leq b$, $f(a) \leq' f(b)$ in Q .

If $\langle P, \leq \rangle$ and $\langle Q, \leq' \rangle$ are lattices and $g: P \rightarrow Q$ is a lattice homomorphism, then g is order-preserving.

Definition 4-1.7 Two partially ordered sets $\langle P, \leq \rangle$ and $\langle Q, \leq' \rangle$ are called *order-isomorphic* if there exists a mapping $f: P \rightarrow Q$ which is bijective and if both f and f^{-1} are order-preserving.

It may happen that a mapping $f: P \rightarrow Q$ is bijective and order-preserving, but that f^{-1} is not order-preserving (see Example 7). In such a case, P and Q are not order-isomorphic. For lattices $\langle L, \leq \rangle$ and $\langle S, \leq' \rangle$, an order isomorphism

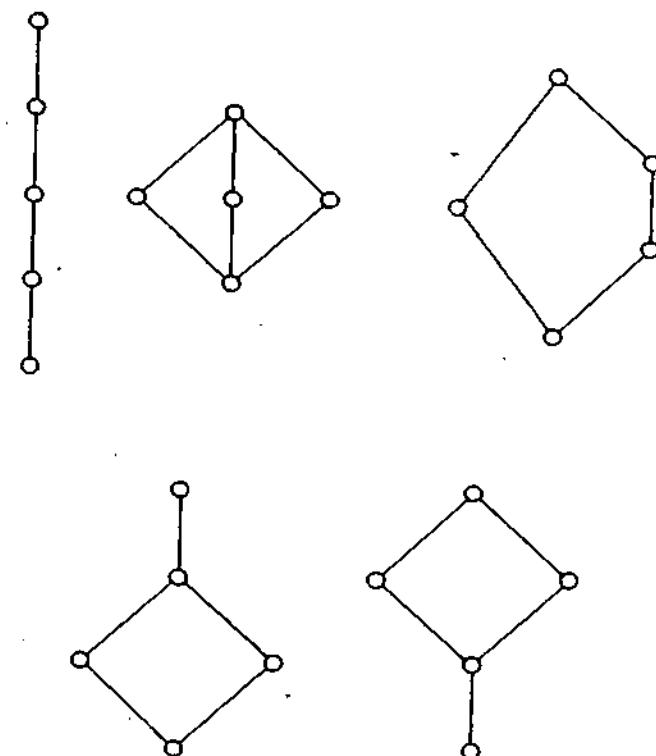


FIGURE 4-1.6 Lattices of order 5.

is equivalent to lattice isomorphism. Hence lattices which are order-isomorphic as partially ordered sets are isomorphic. The importance of order isomorphism lies in the fact that two partially ordered sets which are order-isomorphic can be represented by the same diagram.

EXAMPLE 7 Consider the lattice $\langle S_n, D \rangle$ for $n = 12$, that is, the lattice of divisors of 12 in which the partial ordering relation D means "division" as given in Example 3, Sec. 4-1.1. Consider another lattice $\langle S_n, \leq \rangle$ in which \leq denotes the ordering relation "less than or equal to." A mapping $f: S_n \rightarrow S_n$ given by $f(x) = x$ is order-preserving and bijective, but f^{-1} is not order-preserving. Hence $\langle S_n, D \rangle$ and $\langle S_n, \leq \rangle$ are neither order-isomorphic nor isomorphic.

EXERCISES 4-1.4

- For the lattice $\langle L, \subseteq \rangle$ given in Prob. 7 of Exercises 4-1.1, what are the operations of meet and join?

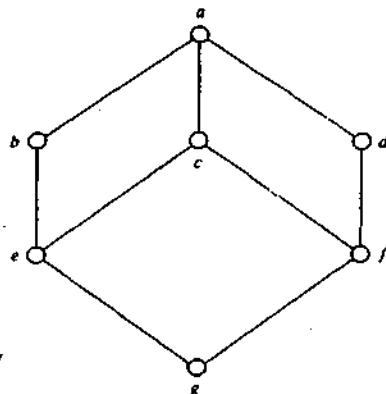


FIGURE 4-1.7

- 2 Show that the diagram given in Fig. 4-1.7 is a lattice, and it is not a sublattice of the lattice given in Fig. 4-1.1f.
- 3 Show that every interval of a lattice is a sublattice.
- 4 Find all the sublattices of the lattice $\langle S_n, D \rangle$ for $n = 12$.
- 5 Draw the diagram of a lattice which is the direct product of the five-element lattice shown in Fig. 4-1.1c and a two-element chain.
- 6 Show that the lattice $\langle S_n, D \rangle$ for $n = 216$ is isomorphic to the direct product of lattices for $n = 8$ and $n = 27$.
- 7 Show that there exists a mapping from the five-element lattice given in Fig. 4-1.1c to a three-element chain and that this mapping is order-preserving. Is it a homomorphism?

4-1.5 Some Special Lattices

In a lattice every pair of elements has a least upper bound and a greatest lower bound. As a consequence of this fact, one can show by using the principle of mathematical induction that every finite subset of a lattice has a least upper bound and a greatest lower bound. This, however, may not be the case for an infinite subset of a lattice. Consider, for example, the lattice $\langle I_+, \leq \rangle$ in which I_+ is the set of positive integers. The subset consisting of even positive integers has no least upper bound.

Let $\langle L, *, \oplus \rangle$ be a lattice and $S \subseteq L$ be a finite subset of L where $S = \{a_1, a_2, \dots, a_n\}$. The greatest lower bound and the least upper bound of S can be expressed as

$$\text{GLB } S = \underset{i=1}{\overset{n}{*}} a_i \quad \text{and} \quad \text{LUB } S = \underset{i=1}{\overset{n}{\oplus}} a_i \quad (1)$$

where

$$\underset{i=1}{\overset{2}{*}} a_i = a_1 * a_2 \quad \text{and} \quad \underset{i=1}{\overset{k}{*}} a_i = \underset{i=1}{\overset{k-1}{*}} a_i * a_k \quad k = 3, 4, \dots$$

A similar representation can be given for $\underset{i=1}{\overset{n}{\oplus}} a_i$. Because of the associativity of

the operations $*$ and \oplus , we can write

$$\underset{i=1}{\overset{n}{*}} a_i = a_1 * a_2 * \dots * a_n \quad \text{and} \quad \underset{i=1}{\overset{n}{\oplus}} a_i = a_1 \oplus a_2 \oplus \dots \oplus a_n$$

Definition 4-1.8 A lattice is called *complete* if each of its nonempty subsets has a least upper bound and a greatest lower bound.

Obviously, every finite lattice must be complete. Also every complete lattice must have a least element and a greatest element. The least and the greatest elements of a lattice, if they exist, are called the *bounds (units, universal bounds)* of the lattice and are denoted by 0 and 1 respectively. A lattice which has both elements 0 and 1 is called a bounded lattice. For the lattice $\langle L, *, \oplus \rangle$ with $L = \{a_1, \dots, a_n\}$,

$$\underset{i=1}{\overset{n}{*}} a_i = 0 \quad \text{and} \quad \underset{i=1}{\overset{n}{\oplus}} a_i = 1 \quad (2)$$

The bounds 0 and 1 of a lattice $\langle L, *, \oplus, 0, 1 \rangle$ satisfy the following identities. For any $a \in L$,

$$a \oplus 0 = a \quad a * 1 = a \quad (3)$$

$$a \oplus 1 = 1 \quad a * 0 = 0 \quad (4)$$

Obviously, 0 is the identity of the operation \oplus , and 1 is the identity of the operation $*$. Similarly, 0 and 1 are zeros with respect to the operations $*$ and \oplus respectively. In a bounded lattice, 1 and 0 are duals of each other, and the principle of duality can now be extended to include the interchanges of 0 and 1. The identities in (3) are duals of each other, and so also are the identities in (4).

For bounded lattices it is possible to introduce the notion of a complement of an element in the following manner.

Definition 4-1.9 In a bounded lattice $\langle L, *, \oplus, 0, 1 \rangle$, an element $b \in L$ is called a *complement* of an element $a \in L$ if

$$a * b = 0 \quad \text{and} \quad a \oplus b = 1$$

Note that the definition of a complement is symmetric in a and b , so that b is a complement of a if a is a complement of b . Any element $a \in L$ may or may not have a complement. Furthermore, an element of L may have more than one complement in L .

From the identities (3) and (4) we have

$$0 * 1 = 0 \quad \text{and} \quad 0 \oplus 1 = 1 \quad (5)$$

which show that 0 and 1 are complements of each other. It is easy to show that 1 is the only complement of 0. Let us assume that $c \neq 1$ is a complement of 0 and $c \in L$; then

$$0 * c = 0 \quad \text{and} \quad 0 \oplus c = 1$$

However, $0 \oplus c = c$ from (3), and $c \neq 1$ leads to a contradiction. In a similar manner we can show that 0 is the only complement of 1.

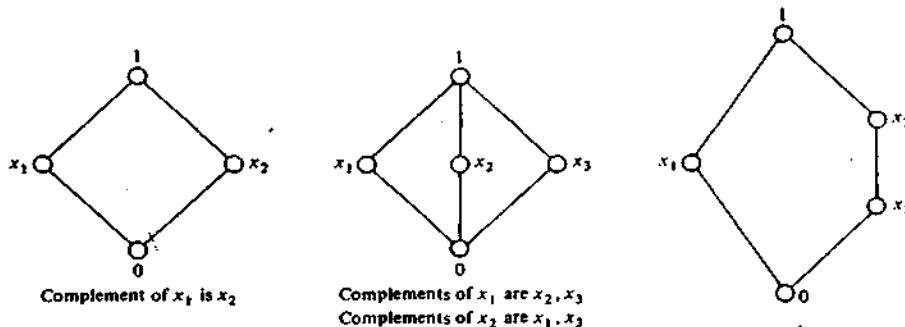


FIGURE 4-1.8 Complements in lattices.

Definition 4-1.10 A lattice $\langle L, *, \oplus, 0, 1 \rangle$ is said to be a *complemented lattice* if every element of L has at least one complement.

In Fig. 4-1.8 some lattices are shown, and the complements of some of the elements are noted below the diagrams.

EXAMPLE 1 Let $\langle L^n, \leq_n \rangle$ be the lattice of n -tuples of 0 and 1 given in Example 4, Sec. 4-1.4. This is a complemented lattice in which every element has a unique complement. The complement of an element of L^n can be obtained by interchanging 1 by 0 and 0 by 1 in the n -tuple representing the element. As a special case, let $n = 3$. The bounds of $\langle L^3, \leq_3 \rangle$ are $\langle 0, 0, 0 \rangle$ and $\langle 1, 1, 1 \rangle$. The complement of $\langle 1, 0, 1 \rangle$ is $\langle 0, 1, 0 \rangle$.

EXAMPLE 2 The lattice $\langle \rho(S), \subseteq \rangle$ of the power set of any set S is isomorphic to the lattice $\langle L^n, \leq_n \rangle$ provided S has n elements. The meet and join operations on $\rho(S)$ are \cap and \cup respectively, while the bounds are \emptyset and S . The lattice $\langle \rho(S), \subseteq \rangle$ is a complemented lattice in which the complement of any subset A of S is the set $S - A$.

It was shown in Theorem 4-1.3 that the elements of any lattice satisfy the distributive inequalities. We shall now define a special class of lattices as follows.

Definition 4-1.11 A lattice $\langle L, *, \oplus \rangle$ is called a *distributive lattice* if for any $a, b, c \in L$,

$$a * (b \oplus c) = (a * b) \oplus (a * c) \quad (6)$$

and

$$a \oplus (b * c) = (a \oplus b) * (a \oplus c) \quad (7)$$

In other words, in a distributive lattice the operations $*$ and \oplus distribute over each other.

It may be mentioned here that the equalities (6) and (7) are equivalent to one another (see Prob. 7, Exercises 4-1.5), and it is sufficient to verify any

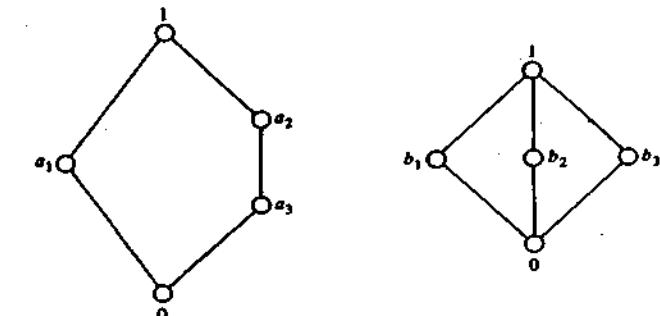


FIGURE 4-1.9 Lattices which are not distributive.

one of these two equalities for all possible combinations of the elements of a lattice. Note that the distributive equalities may be satisfied by some elements of a lattice, but this does not guarantee that the lattice is distributive (see Example 3).

The lattices given in Examples 1 and 2 are distributive lattices.

EXAMPLE 3 Show that the lattices given by the diagrams in Fig. 4-1.9 are not distributive.

SOLUTION

$$a_1 * (a_2 \oplus a_3) = a_1 * 1 = a_1 = (a_1 * a_2) \oplus (a_1 * a_3)$$

$$a_1 * (a_2 \oplus a_3) = 0 = (a_1 * a_2) \oplus (a_1 * a_3)$$

but

$$a_2 * (a_1 \oplus a_3) = a_2 * 1 = a_2$$

$$(a_2 * a_1) \oplus (a_2 * a_3) = 0 \oplus a_2 = a_2$$

Hence the lattice is not distributive. In the other case, $b_1 * (b_2 \oplus b_3) = b_1$ while $(b_1 * b_2) \oplus (b_1 * b_3) = 0$, which shows that the lattice is not distributive. ////

The two five-element lattices given in Fig. 4-1.9 are important because of a theorem which states that a lattice is distributive iff no sublattice is isomorphic to either of the two five-element lattices given there. We shall not prove this theorem.

The following theorems show that certain lattices are always distributive.

Theorem 4-1.5 Every chain is a distributive lattice.

PROOF Let $\langle L, \leq \rangle$ be a chain and $a, b, c \in L$. Consider the following possible cases: (1) $a \leq b$ or $a \leq c$, and (2) $a \geq b$ and $a \geq c$. We shall now show that the distributive law (6) is satisfied by a, b, c .

For (1),

$$a * (b \oplus c) = a \quad \text{and} \quad (a * b) \oplus (a * c) = a$$

For (2),

$$a * (b \oplus c) = b \oplus c \quad \text{and} \quad (a * b) \oplus (a * c) = b \oplus c \quad ////$$

Theorem 4-1.6 The direct product of any two distributive lattices is a distributive lattice.

PROOF The proof of the theorem follows from the definition of direct product. ////

In addition to these distributive lattices, we also have that any sublattice of a distributive lattice is distributive.

Observe that the distributive laws as stated in Eqs. (6) and (7) are duals of each other; therefore, the principle of duality holds for all distributive lattices.

The following are some examples of distributive lattices.

EXAMPLE 4 The ring of subsets of a given set S defined in Example 3, Sec. 4-1.4, and denoted by $\langle R(S), \cap, \cup \rangle$ is a distributive lattice, because of the fact that both set union and set intersection satisfy the distributive laws.

EXAMPLE 5 The lattice $\langle L_+, D \rangle$ given in Example 2, Sec. 4-1.1, is a distributive lattice, and so also are the sublattices $\langle S_n, D \rangle$ for any positive integer n .

The following interesting theorem holds for a distributive lattice.

Theorem 4-1.7 Let $\langle L, *, \oplus \rangle$ be a distributive lattice. For any $a, b, c \in L$,

$$(a * b = a * c) \wedge (a \oplus b = a \oplus c) \Rightarrow b = c$$

PROOF

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

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

$$= b \oplus (a * c) = b \oplus (a * b) = b \quad ////$$

An important consequence of this theorem is that in a distributive lattice, if an element $a \in L$ has a complement, then it must be unique. Suppose that b and c are complements of a ; then

$$a * b = a * c = 0 \quad \text{and} \quad a \oplus b = a \oplus c = 1$$

But from Theorem 4-1.7 this means $b = c$.

Recall that a lattice is called complemented if every element of the lattice has at least one complement. If we now consider those lattices which are complemented as well as distributive, then we are assured that every element of such a lattice has a unique complement, and we denote the complement of an element $a \in L$ by a' . Lattices which are complemented and distributive are called Boolean algebras. We shall study such lattices in detail in the next section.

It may be mentioned here that the converse of Theorem 4-1.7 also holds. We shall, however, omit the proof.

EXERCISES 4-1.5

- 1 Find the complements of every element of the lattice $\langle S_n, D \rangle$ for $n = 75$.
- 2 Show that in a lattice with two or more elements, no element is its own complement.
- 3 Show that a chain of three or more elements is not complemented.
- 4 Which of the two lattices $\langle S_n, D \rangle$ for $n = 30$ and $n = 45$ are complemented? Are these lattices distributive?
- 5 Show that De Morgan's laws, given by

$$(a * b)' = a' \oplus b' \quad \text{and} \quad (a \oplus b)' = a' * b'$$

hold in a complemented, distributive lattice.

- 6 Show that in a complemented, distributive lattice

$$a \leq b \Leftrightarrow a * b' = 0 \Leftrightarrow a' \oplus b = 1 \Leftrightarrow b' \leq a'$$

- 7 Show that Eqs. (6) and (7) are equivalent.

- 8 Show that a lattice is distributive iff

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

- 9 Show that in a distributive lattice, the distributive laws can be generalized as

$$a * (\bigoplus_{i=1}^n b_i) = \bigoplus_{i=1}^n (a * b_i) \quad \text{and} \quad a \oplus (\bigast_{i=1}^n b_i) = \bigast_{i=1}^n (a \oplus b_i)$$

- 10 Show that in a bounded distributive lattice, the elements which have complements form a sublattice.

- 11 A lattice is said to be *modular* if

$$a \leq c \Rightarrow a \oplus (b * c) = (a \oplus b) * c$$

Show that every distributive lattice is modular, but not conversely.

4-2 BOOLEAN ALGEBRA

The example of the power set $P(S)$ of a nonempty set S appeared throughout our discussion of lattices. It is not accidental. In fact, we first started with a general algebraic system called a lattice and gradually imposed those conditions on lattices which are satisfied by the lattice of the power set. Our aim was to arrive at an algebraic system which has all the essential characteristics of the lattice of the power set. Once this is done, we arrive at an abstract algebraic system which will be shown to be isomorphic to the lattice of the power set of a set. Many other algebraic systems such as the statement algebra and switching algebra are also special cases of such an algebraic system called Boolean algebra. We shall be concerned with only finite Boolean algebras in this chapter.

Th: 4.1.5: Every chain is a distributive lattice.

Defn: A poset is called chain if "every two elements are comparable", means, for any two elements a, b either $a \leq b$ (aRb)
 $b \leq a$ (bRa)

Every chain is a lattice. If $a \leq b$, then

$$\text{lub}\{a, b\} = b \text{ and}$$

$$\text{glb}\{a, b\} = a.$$

□ To prove that it is distributive, consider the
for any three distinct elements $a, b, c \in L$, we have

~~such that~~ $a \leq b \leq c$. Hence

$$a * b = a \text{ and } a * c = a,$$

$$b \oplus c = c$$

Now,

$$\begin{aligned} & a * (b \oplus c), (a * b) \oplus (a * c) \\ = & a * c \\ = & a \end{aligned} \quad \begin{aligned} & = a \oplus a \\ & = a \end{aligned}$$

Therefore a chain is distributive.

BOOLEAN ALGEBRA

Definition: A lattice which is complemented and distributive is called a Boolean algebra. or

If B is a non empty set with two binary operations $+$ and \cdot , two distinct elements 0 and 1 and a unary operation $'$, then B is called a Boolean algebra if the following properties hold for all a, b, c in B :

B1: Identity laws: $a + 0 = a, \quad a \cdot 1 = a.$

B2: Commutative laws: $a + b = b + a, \quad a \cdot b = b \cdot a$

B3: Associative law: $(a + b) + c = a + (b + c), \quad (a \cdot b) \cdot c = a \cdot (b \cdot c).$

B4: Distributive law:

$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

B5: Complement law: $a + a' = 1$, $a \cdot a' = 0$

Example Let $B = \{0, 1\}$ and let $+$, \cdot be two operations in B defined by the following operation tables (a) and (b):

$+$	1	0
1	1	1
0	1	0

(a)

\cdot	1	0
1	1	0
0	0	0

(b)

Suppose that the complements are defined by $1^1 = 0$ and $0^1 = 1^1$, then B is a Boolean algebra.

Properties of Boolean Algebra:

1. **Idempotent laws:** $a + a = a$ and $a \cdot a = a$ for all $a \in B$.

Proof: $a + a = (a + a) \cdot 1$

$$= (a + a) \cdot (a + a')$$

$$= a + a \cdot a'$$

$$= a + 0$$

$$= a$$

$$a \cdot a = a \cdot a + 0$$

$$= a \cdot a + a \cdot a'$$

$$= a \cdot (a + a')$$

$$= a \cdot 1$$

$$= a$$

2. Dominance laws: $a + 1 = 1$ and $a \cdot 0 = 0$, for all $a \in B$

Proof:
$$\begin{aligned} a + 1 &= (a + 1) \cdot 1 \\ &= (a + 1) \cdot (a + a') \\ &= a + 1 \cdot a' \\ &= a + a' \\ &= 1 \end{aligned}$$

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + 0 \\ &= a \cdot 0 + a \cdot a' \\ &= a \cdot (0 + a') \\ &= a \cdot (a' + 0) \\ &= a \cdot a' = 0 \end{aligned}$$

3. Absorption laws: $a + (a \cdot b) = a$, and $a \cdot (a + b) = a$, for all $a, b \in B$

Proof:

$$\begin{aligned} a + (a \cdot b) &= a \cdot 1 + (a \cdot b) \\ &= a \cdot (1 + b) \\ &= a \cdot 1 \\ &= a \end{aligned}$$

$$\begin{aligned} a \cdot (a + b) &= (a + 0) (a + b) \\ &= a + 0 \cdot b \\ &= a + 0 \\ &= a \end{aligned}$$

4. De Morgan's laws: $(a + b)' = a' \cdot b'$ and $(a \cdot b)' = a' + b'$, for all $a, b \in B$.

Proof: The theorem is proved if we show that

$$(a + b) + (a' \cdot b') = 1 \text{ and } (a + b) \cdot (a' \cdot b') = 0$$

$$\begin{aligned}(a + b) + (a' \cdot b') &= b + a + (a' \cdot b') \\&= b + (a + a') \cdot (a + b') \\&= b + 1 \cdot (a + b') \\&= b + a + b' \\&= b + b' + a \\&= 1 + a \\&= 1\end{aligned}$$

$$\begin{aligned}(a + b) \cdot (a' \cdot b') \\&= ((a + b) \cdot a') \cdot b' \\&= ((a \cdot a') + (b \cdot a')) \cdot b' \\&= (0 + (b \cdot a')) \cdot b' \\&= (b \cdot a') \cdot b' \\&= (b \cdot b') \cdot a' \\&= 0 \cdot a' \\&= 0\end{aligned}$$

$$(a + b') = a' \cdot b'$$

In the similar manner, we can prove the other part.

5. Involution law or Double complement law:

$$(a')' = a \text{ for all } a \in B.$$

Proof:

$$a + a' = 1 \text{ and } a \cdot a' = 0$$

$$\text{i.e., } a' + a = 1 \text{ and } a' \cdot a = 0$$

Hence, a is the complement of a'

Dual and Principle of duality

The dual of any statement in a Boolean algebra B is the statement obtained by interchanging the operations $+$ and \cdot , and interchanging the elements 0 and 1 in the original statement.

Example: The dual of $a + a \cdot (b + 1) = a$ is $a \cdot a + (b \cdot 0) = a$.

Subalgebra: If C is a non-empty subset of a Boolean algebra such that C itself is a Boolean algebra with respect to the operations in B , then C is called a subalgebra of B .

Boolean Homomorphism:

If $\{B, +, \cdot, ', 0, 1\}$ and $\{C, \cup, \cap, -, \alpha, \beta\}$ are two Boolean algebras, then a mapping $f: B \rightarrow C$ is called a Boolean homomorphism, if for any $a, b \in B$,

$$f(a + b) = f(a) \cup f(b), f(a \cdot b) = f(a) \cap f(b),$$

$$f(a') = \overline{f(a)}, f(0) = \alpha \text{ and } f(1) = \beta,$$

where α and β are the zero and unit elements of C .

Isomorphic Boolean Algebras: Two Boolean algebra B and B' are said to be isomorphic if there is one-to-one correspondence between B and B' with respect to three operations.

Boolean Expressions and Boolean Functions:

A Boolean expression in n Boolean variables x_1, x_2, \dots, x_n is a finite string of symbols formed recursively as follows:

1. $0, 1, x_1, x_2, \dots, x_n$ are Boolean expressions.
2. If E_1 and E_2 are Boolean expressions, then $E_1 + E_2$ and $E_1 \cdot E_2$ are also Boolean expressions.
3. If E is a Boolean Expression, E' is also a Boolean expression.

Boolean Function: If x_1, x_2, \dots, x_n are Boolean variables, then function from $f: B^n \rightarrow B\{0,1\}$ is called a Boolean function of degree n .

- ▶ Each Boolean expression represents a Boolean function, which is evaluated by substituting the value 0 or 1 for each variable.

Example: The values of the Boolean function $f(a, b, c) = ab + c'$ are displayed in the following truth table:

a	b	c	ab	c'	$ab + c'$
1	1	1	1	0	1
1	1	0	1	1	1
1	0	1	0	0	0
1	0	0	0	1	1
0	1	1	0	0	0
0	1	0	0	1	1
0	0	1	0	0	0
0	0	0	0	1	1

Literals: A Boolean variables or its complement is called literal.

Minterm: A minterm in n Boolean variables is a Boolean product of the n literals in which each literal appears exactly once.

Example: $ab, a'b, ab', a'b'$ forms a complete set of minterms for two variables a and b .

Maxterm: A maxterm in n Boolean variables is a Boolean sum of the n literals in which each literal appears exactly once.

Example: $a + b, a' + b, a + b', a' + b'$ forms a complete set of maxterms for two variables a and b .

Disjunctive Normal form (DNF): When a Boolean function is expressed as a sum of minterms then it is said to be in disjunctive normal form.

Conjunctive Normal form (CNF): When a Boolean function is expressed as a product of maxterms then it is said to be in conjunctive normal form.

Complete DNF (CNF): When a Boolean function in n variables is expressed as a sum of (product of) all the 2^n minterms (maxterms), it is said to be in complete DNF (CNF) .

Canonical Form: Boolean functions expressed in the DNF or CNF are said to be in canonical form.

Expression of Boolean function in Canonical form

1. **Truth table method:** If the Boolean function $f(x, y, z)$ is represented by a truth table, we express $f(x, y, z)$ in DNF as follows

x	y	z	f
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

the required DNF is : $xyz' + xy'z + xy'z'$

CNF: The CNF of f is the Boolean product of these maxterms.

$$f = (x' + y' + z')(x + y' + z')(x + y' + z)(x + y + z')(x + y + z)$$

2. **Algebraic method:** To get the DNF of a given Boolean functions, we express it as a sum of products.

Example:

$$\begin{aligned} f &= xy' + xz' = xy' \cdot 1 + xz' \cdot 1 \\ &= xy' \cdot (z + z') + xz' \cdot (y + y') \\ &= xy'z + xy'z' + xyz' + xy'z' \\ &= xy'z + xy'z' + xyz' \end{aligned}$$

This is the required DNF

Now, let us express the same function in the product of sums

$$\begin{aligned}f &= xy' + xz' \\&= x \cdot (y' + z') = (x + 0) \cdot (y' + z' + 0) \\&= (x + yy') \cdot (y' + z' + xx') \\&= (x + y) \cdot (x + y') \cdot (y' + z' + x) \cdot (y' + z' + x') \\&= (x + y + zz') \cdot (x + y' + zz') \cdot (y' + z' + x) \cdot (y' + z' + x') \\&= (x + y + z) \cdot (x + y + z') \cdot (x + y' + z) \cdot (x + y' + z') \\&\quad \cdot (y' + z' + x) \cdot (y' + z' + x') \\&= (x + y + z) \cdot (x + y + z') \cdot (x + y' + z) \cdot (x + y' + z') \\&\quad \cdot (y' + z' + x')\end{aligned}$$

This is the CNF

DEFINITION

- A lattice which is a complemented and distributive is called Boolean algebra.
- If B is a non-empty set with two binary operations $+$ and \cdot , two distinct element 0 and 1 and unary operation $'$, then B is called a Boolean algebra if the following basic properties hold for a, b, c in B .
- B_1 : Identity law

$$a+0=a$$

$$a \cdot 1=a$$

- B_2 : Commutative laws

$$a+b=b+a$$

$$a \cdot b=b \cdot a$$

- B_3 : Associative laws

$$(a+b)+c = a+(b+c)$$

$$(a \cdot b) \cdot c = a \cdot (b+c)$$

- B_4 : Distributive laws

$$a+(b \cdot c) = (a+b) \cdot (a+c)$$

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$

- B_5 : Complemented laws

$$a+a'=1$$

$$a \cdot a'=0$$

• ADDITIONAL PROPERTIES OF BOOLEAN ALGEBRA:

if $\{B, +, ., ', 0, 1\}$ is a boolean algebra, the following properties hold good.

they can be proved by using the basic properties of boolean algebra listed in the definition

Idempotent laws

$$a+a=a \text{ and } a.a=a \text{ for all } a \text{ in } B$$

Dominance laws

$$a+1=1 \text{ and } a.0=0 \text{ for all } a \text{ in } B$$

Absorption laws

$$a.(a+b)=a \text{ and } a+(a.b)=a \text{ for all } a,b \text{ in } B$$

De morgan's laws

$$(a+b)' = a'. b'$$

$$(a,b)'=a'+b' \text{ for all } a,b \text{ in } B$$

Double complemented laws (or) involution laws

$$(a')'=a \text{ for all } a,b \text{ in } B$$

Zero and one laws

$$0'=1 \text{ and } 1'=0$$

Dual and principal of duality:

Definition:

the dual of any statement in a boolean algebra B is the statement obtained by interchanging the operation + and . And interchanging the elements 0 and 1 in the original statement.

For example the dual of $a+a(b+1)=a$ is $a.(a+b.0)=a$.

Principal of duality:

The dual of a theorem in a boolean algebra is also theorem.

For example $(a.b)'=a'+b'$ is a valid result.

Since it is the dual of the valid statement $(a+b)'=a'+b'$

If a theorem in boolean algebra a is proved by using the axioms of boolean algebra, the dual theorem can be proved by using the dual of each step of the proof of the original theorem. This is obvious from the proof of additional properties of boolean algebra.

Sub algebra:

if C is a non-empty subset of a boolean algebra such that C itself is a boolean algebra with respect to the operations of B, the C is called the sub algebra of B.

It is obvious that C is a sub algebra of B iff C is closed under the three operations of B, namely +, . ,and ' and the contains the elements 0 and 1.

Boolean homomorphism:

If $\{B, +, ., ', 0, 1\}$ and $\{C, \cup, \cap, -, \alpha, \beta\}$ are two boolean algebras then a mapping $f : B \rightarrow C$ is called a boolean homomorphism, if all the operations of boolean algebra are preserved. Viz., $a, b \in B$.

$$f(a+b) = f(a) \cup f(b), f(a.b) = f(a) \cap f(b)$$

$$f(a') = \overline{f(a)}, f(0) = \alpha \text{ and } f(1) = \beta$$

where α and β are the zero and unit element of C.
3/13/2017 MAT1014-Module-5-Boolean Algebra - Dr. D. Ezhilmaran

Isomorphic boolean algebras:

the two boolean algebras B and B' are said to be isomorphic if there is one-to-one correspondence between B and B' with respect to the three operations, viz.

there exists a mapping $f : B \rightarrow B'$ such that

$$f(a+b) = f(a) + f(b)$$

$$f(a.b) = f(a).f(b) \text{ and } f(a') = \{f(a)\}'$$

Boolean expressions and boolean functions:

Definition:

A boolean expressions in n boolean variables x_1, x_2, \dots, x_n

Is finite string of symbols formed recursively as follows

1. $0, 1, x_1, x_2, \dots, x_n$ are boolean expressions.

2. If E_1 and E_2 are boolean expressions, then $E_1 \cdot E_2$ and $E_1 + E_2$ are also boolean expressions.
3. If E is a boolean expressions, E' is also a boolean expressions.

Definitions:

1. A **min term** if n boolean variables is boolean product of the n literals in which each literal appears exactly once.

For example: $ab, a'b, ab'$ and $a'b'$ form the complete of min terms of two variables a and b , $abc, abc', ab'c, a'bc, ab'c', a'bc'$, $a'b'c$ and $a'b'c'$ form the complete set of min terms of three variables a, b, c .

2. A **max term** if n boolean variables is boolean sum of the n literals in which each literal appears exactly once.

For example: $a+b, a'+b, a+b'$ and $a'+b'$ form the complete of max terms of two variables a and b

3. When a boolean function is expressed as a sum of min terms, it is called its **sum of products expansions** or it is said to be in the disjunctive normal forms (DNF)
4. When a boolean function is expressed as a products of max terms, it is called its **products of sum expansions** or it is said to be in the conjunctive normal forms (CNF)
5. Boolean functions expressed in the DNF or CNF are said to be in canonical forms.
6. If a boolean functions in n variables is expressed as the sum(product) of all the 2^n min terms(max terms) is said to be in complete DNF (complete CNF)
7. Boolean functions expressed in complete DNF or complete CNF are said to **complete canonical forms**.

EXAMPLE:1

In Boolean algebra, if $a+b=1$ and $a.b=0$, show that $b=a'$, viz, the complement of every element a is unique.

SOLUTION :

$$b=b.1$$

$$=b.(a+a') \quad \text{by B5 (complement laws)}$$

$$=b.a + b.a' \quad \text{by B4 (distributive laws)}$$

$$=a.b + b.a' \quad \text{by B2 (commutative laws)}$$

$$=0 + b.a' \quad \text{given } a.b = 0$$

$$=a.a' + b.a' \quad \text{by B5 (complement laws)}$$

$$=a'.a + a'.b \quad \text{by B2 (commutative laws)}$$

$$=a'.(a+b) \quad \text{by B4 (distributive laws)}$$

$$=a'.1 \quad \text{given } a+b=1$$

$$=a' \quad \text{by B1 (identity laws)}$$

EXAMPLE:2

In a Boolean algebra, prove that the following statements are equivalent :

- (1) $a + b = b$
- (2) $a \cdot b = a$
- (3) $a' + b = 1$
- (4) $a \cdot b' = 0$

SOLUTION :

Let (1) be true.

Then

$$\begin{aligned} a \cdot b &= a \cdot (a + b) \quad \text{by (1)} \\ &= a \quad (\text{by absorption law}) \\ \text{i.e. (1)} &\Rightarrow (2) \end{aligned}$$

$$\begin{aligned} \text{Now } a + b &= a \cdot b + b \quad \text{by (2)} \\ &= b + b \cdot a \\ &= b \end{aligned}$$

$$\text{i.e. (2)} \Rightarrow (1)$$

Therefore (1) and (2) are equivalent

$$a' + b = a' + (a' + b) \text{ by (1)}$$

$$= (a + a') + b$$

$$= 1 + b$$

$$= 1 \text{ (by dominance rule)}$$

i.e (1) => (3)

$$a + b = (a + b) \cdot 1$$

$$= (a + b) \cdot (a' + b) \text{ by (3)}$$

$$= a \cdot a' + b$$

$$= 0 + b$$

$$= b, \text{ by dominance law.}$$

i.e (3) => (1) therefore (1) and (3) are equivalent.

GIVEN : $a' + b = 1$

So $(a' + b') = 1'$

$(a')'.b' = 0$ (by demorgan's law)

$$a.b' = 0$$

I.e. (3) \Rightarrow (4)

GIVEN : $a.b' = 0$

$a' + (b')' = 0'$ (by demorgan's law)

$$a' + b = 1$$

I.e. (4) \Rightarrow (3)

Therefore (4) and (3) are equivalent

Hence all four statements are equivalent.

EXAMPLE :3

Simplify the Boolean function

$a'b'c + a'b'c + a'b'c'$ using Boolean algebra identities.

SOLUTION :

$$\text{Given } a'b'c + a'b'c + a'b'c'$$

$$= a'b'c + a.b' (c + c')$$

$$= a'b'c + a.b'.1$$

$$= b'.(a + a'.c)$$

$$= b'.(a+a') . (a+c)$$

$$= b'.1.(a+c)$$

$$= a.b' + b'.c$$

EXAMPLE:4

In any Boolean algebra, show that

$$ab' + a'b = 0 \text{ if and only if } a = b.$$

SOLUTION :

Let $a=b$.

$$\text{Then } ab' + a'b = aa' + a'a$$

$$0 + 0 = 0$$

$$\text{Let } ab' + a'b = 0$$

$$\text{Then } a + a'b + a'b = a$$

$$a + a' + b = a \text{ (by absorption law)}$$

$$(a+a').(a+b) = a$$

$$1 \cdot (a+b) = a$$

$$\text{So, } a + b = a$$

$$\text{similarly, from (1) } ab' + a'b + b = b$$

$$\text{Then, } b + ab' = b \text{ (by absorption law)}$$

$$(b+b').(a+b) = b$$

$$1 \cdot (a+b) = b$$

$$\text{So, } a + b = b$$

From these equations we know that $a=b$.

EXAMPLE :5

In any Boolean algebra, show that

$$(a+b')(b+c')(c+a') = (a'+b)(b'+c)(c'+a)$$

SOLUTION :

$$\begin{aligned} L.S &= (a+b'+o)(b+c'+o)(c+a'+o) \\ &= (a+b'+c.c') (b+c'+aa') (c+a'+bb') \\ &= (a+b'+c) . (a+b'+c') . (b+c'+a) . (b+c'+a') . (c+a'+b') \\ &\quad (c+a'+b') \\ &= \{(a'+b+c) (a'+b+c')\} \ \{(b'+c+a) (b'+c+a')\} \ \{(c'+a+b) \\ &\quad (c'+a+b')\} \\ &= (a'+b+cc'). (b'+c+aa') . (c'+a+bb') \\ &= (a'+b+o)(b'+c+o)(c'+a+o) \\ &= (a'+b).(b'+c).(c'+a) \\ &= R.S \end{aligned}$$

EXAMPLE :6

In any Boolean algebra, prove that

1. $x + wy + uvz = (x+u+w) (x+u+y) (x+v+w) (x+v+y) (x+w+z)$
 $(x+y+z)$
2. $ab + abc + a'b + ab'c = b + ac$

SOLUTION :

1.
$$\begin{aligned} R.S &= (x+u+wy) (x+v+wy) (x+z+wy) \\ &= \{(x+wy)+uv\} . (x+z+wy) \\ &= x+wy+uvz \\ &= L.S \end{aligned}$$
2.
$$\begin{aligned} L.S &= (ab+a'b) + (abc+ab'c) \\ &= (a+a').b + (b+b').ac \\ &= 1.b + 1.ac \\ &= b+ac \\ &= R.S \end{aligned}$$

EXAMPLE :7

Simplify the following Boolean expressions using Boolean algebra.

- I. $(x+y+xy)(x+z)$
- II. $x[y+ z(xy + xz)']$
- III. $xy' + z + (x'+y) z'$

SOLUTION :

$$\begin{aligned} \text{I. } (x+y+xy)(x+z) &= (x+y)(x+z) && [\text{since } y + xy = y] \\ &= x.x + xz + xy + yz \\ &= x + xz + xy + yz && [\text{since } x.x=x] \\ &= x + xy + yz && [x + xz = x] \\ &= x + yz && [x + xy = x] \end{aligned}$$

II.

$$\begin{aligned}
 &= x[y + z(xy')'.xz')] && [\text{demorgan's law}] \\
 &= x[y + z(x'+y')(x'+z')] && [\text{demorgan's law}] \\
 &= x[y + z(x'+x'z' + x'y' + y'z')] && [x'.x' = x'] \\
 &= x[y + z(x' + x'y' + y'z')] && [x' + x'z' = x'] \\
 &= x[y + z(x' + y'z')] && [x' + x'y' = x'] \\
 &= x[y + zx' + y'zz'] \\
 &= x[y + zx'] && [zz' = 0] \\
 &= xy + zx' \\
 &= xy && [xx' = 0]
 \end{aligned}$$

III.

$$\begin{aligned}
 &xy' + z + (x'+y)z' \\
 &= (xy' + z) + (xy' + z)' && [\text{demorgan's law}] \\
 &= 1 && [a+a'=1]
 \end{aligned}$$

EXAMPLE :8

Simplify the following Boolean expressions using Boolean algebra.

- I. $a'b(a'+c) + ab'(b'+c)$
- II. $a + a'bc' + (b + c)'$

SOLUTION :

$$\text{I. } a'b(a'+c) + ab'(b'+c) = a'b + a'bc + ab' + ab'c \quad (a \cdot a' = a' \text{ and } b \cdot b' = b')$$

$$= (a'b + ab') + (a'b + ab')c \\ = a'b + ab' \quad [x+xy=x]$$

$$\text{II. } a + a'bc' + (b + c)' = a + a'bc' + b'c' \quad [\text{demorgan's}]$$

$$= a + (a'b + b')c' \\ = a + [(a'+b')(b+b')c']$$

$$= a + (a' + b')c' \quad [b + b' = 1]$$

$$= (a + a'c') + b'c' \\ = (a + a')(a + c') + b'c'$$

$$= a + (c' + b'c') \quad [a+a'=1] \\ = a + c' \quad [x + xy = x]$$

EXAMPLE:9

In any Boolean algebra, show that

I. $(x + y)(x' + z) = xz + x'y + yz = xz + x'y$

II. $(xy'z' + xy'z + xyz + xyz')(x + y) = x$

SOLUTION :

I.
$$\begin{aligned} (x + y)(x' + z) &= xx' + xz + x'y + yz \\ &= xz + x'y + yz \quad [\text{since } xx' = 0] \end{aligned}$$

Now $xz + x'y + yz$

$$\begin{aligned} &= xz + x'y + yz(x + x') \\ &= xz + x'y + xyz + x'y z \\ &= (xz + xzy) + (x'y + x'y z) \\ &= xz + x'y \end{aligned}$$

II. L.S. = $[xy'(z + z') + xy(z + z')] \cdot (x + y)$

$$= (xy' + xy)(x + y) \quad [\text{since } a + a' = 1]$$
$$= x(y + y')(x + y)$$
$$= x(x + y) \quad [\text{since } y + y' = 1]$$
$$= x + xy$$
$$= x$$
$$= \text{R.S.}$$

Module 6

GRAPH THEORY

(FUNDAMENTALS OF GRAPHS)

GRAPH THEORY :-

WHAT → The theory deals with the graphs (that are mathematical structures) which are used to model mutual relations between the objects.

WHY → It provides a framework to model a large set of real-life problems e.g. traffic organization, job-scheduling and many others. It is quite elegant and extensively used in Combinatorics, Topology, and Algebra.

Graph:

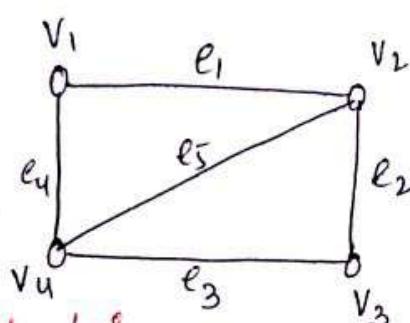
A Graph $G = (V, E)$ consists of a non-empty set V , called the set of vertices (nodes, points) and a set E , of ordered or unordered pairs of elements of V , called the set of edges such that there is a mapping from the set E to the set of ordered or unordered pairs of elements of V .

* $V = \{v_1, v_2, \dots, v_n\}$; set of vertices

$E = \{e_1, e_2, \dots, e_m\}$; set of edges

* The most common representation of a graph is by means of a diagram, in which the vertices are represented as points and each edge as a line segment joining its end vertices.

For example;



$$V = \{v_1, v_2, v_3, v_4\}$$

$$E = \{e_1, e_2, e_3, e_4, e_5\}$$

GRAPH WITH 4 vertices and 5 edges.
Let ϕ be a mapping from the set E to the set of ordered, or unordered pairs of elements of V .

then, $\phi(e_1) = \{v_1, v_2\}$

$$\phi(e_2) = \{v_2, v_3\}$$

$$\phi(e_3) = \{v_3, v_4\}$$

$$\phi(e_4) = \{v_4, v_1\}$$

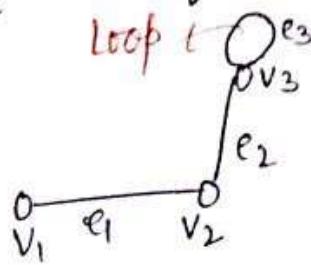
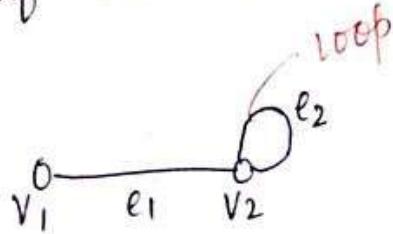
$$\phi(e_5) = \{v_1, v_3\}$$

* If an edge $e \in E$ is associated with an ordered pair (u, v) or an unordered pair (u, v) where $u, v \in V$ then we say that e connects or joins the nodes u and v .

loop or self loop

An edge of a graph that joins a vertex to itself is called a loop (or self-loop)

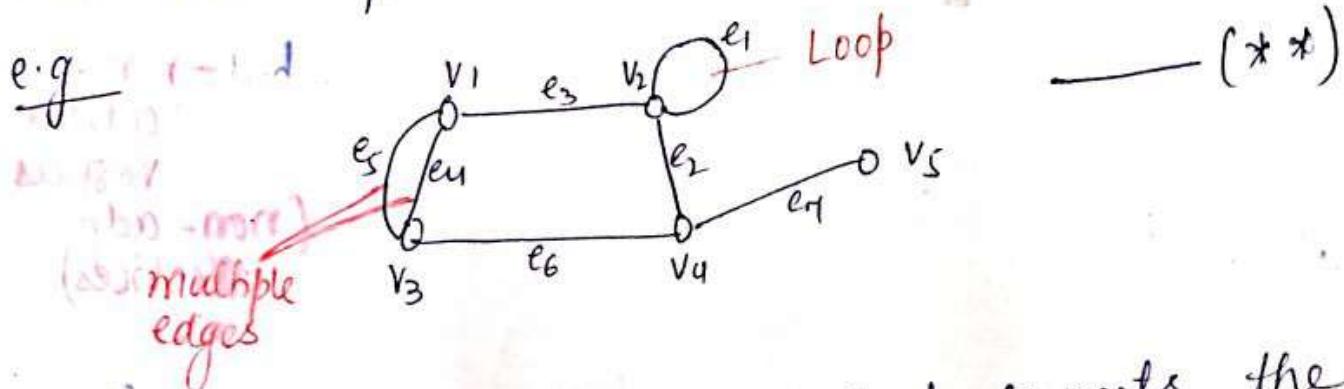
e.g.



Parallel edges (Multiple edges)

When for a given pair of vertices, there are more than two or more edges, the edges are called parallel or multiple edges.

e.g.



Incident edges: The edge e that connects the nodes u and v is said to be incident on each of the nodes.

* In the above graph, e_3 , e_4 and e_5 are incident on the vertex v_1 .

Adjacent edges: Two edges are said to be adjacent if they are incident on same vertex.

* In the above graph, e_2 , e_6 , and e_7 are incident on v_4 . So they are adjacent edges.

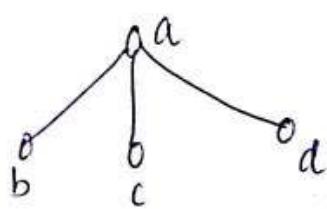
~~degree~~
Adjacent Vertices :- Two vertices are said to be adjacent vertices if they are end vertices of the same edge.

* In the previous graph, v_2 and v_4 are adjacent vertices but v_2 and v_3 are not adjacent vertices.

Examples :-

(1) Let $V = \{a, b, c, d\}$ and $E = \{(a,b), (a,c), (a,d)\}$.
 $G = (V, E)$ is a $(4,3)$ -graph.

The graph can be represented as



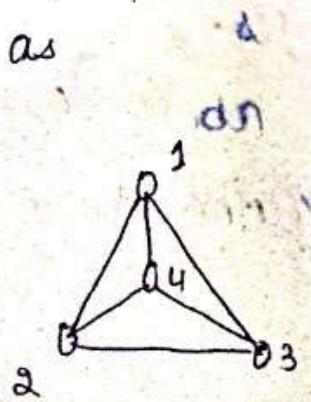
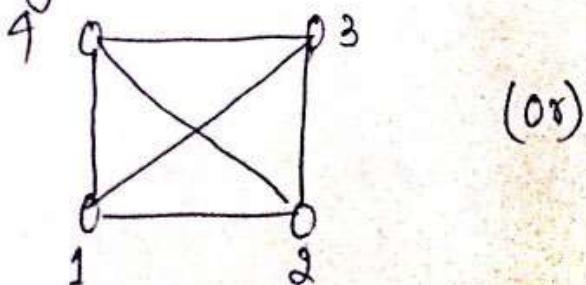
$a, b ; a, c ; a, d \rightarrow$ adjacent vertices

$b, c ; c, d ; b, d \rightarrow$ not adjacent vertices
(non-adjacent vertices)

(2) Let $V = \{1, 2, 3, 4\}$ and $E = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$.

$G = (V, E)$ is a $(4,6)$ graph.

This graph is represented as



* All are adjacent vertices

Degree of a vertex

The degree of a vertex is the number of edges incident on a vertex v_i (self-loop is counted twice).
 Denoted by $d(v_i)$ (**).

For example, in the previous graph, $d(v_1) = 3$, $d(v_3) = 3$, $d(v_2) = 4$.

The handshaking theorem

If $G = (V, E)$ is an undirected graph with 'e' edges then $\sum_i d(v_i) = 2e$.

i.e. the sum of the degrees of all the vertices of an undirected graph is twice the number of edges of the graph and hence even.

Proof: Since every edge is incident with exactly two vertices, every edge contributes '2' to the sum of the degrees of the vertices.

Thus, all the 'e' edges contribute '2e' to the sum of the degrees of the vertices.

$$\text{i.e. } \sum_i d(v_i) = 2e$$

Theorem :- The number of vertices of odd degree in an undirected graph is even.

Proof: Let $G = (V, E)$ be an undirected graph.

Let V_e and V_o be the set of vertices of G of even and odd degrees respectively.

Then, by the handshaking theorem

$$2e = \sum_{v_i \in V_1} d(v_i) + \sum_{v_j \in V_2} d(v_j) \quad \text{--- (1)}$$

Since each $d(v_i)$ is even, $\sum_{v_i \in V_1} d(v_i)$ is even.

Now LHS of (1) is even, so $\sum_{v_j \in V_2} d(v_j)$ should be even.

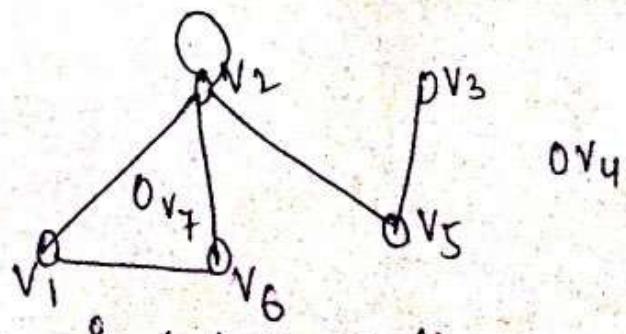
Also, each $d(v_j)$ is odd so the number of terms contained in $\sum_{v_j \in V_2} d(v_j)$ or the number of vertices in V_2 should be even (only then $\sum_{v_j \in V_2} d(v_j)$ will be even)

This means that the number of vertices of odd degree is even.

Hence Proved

Isolated Vertex

A node (or a vertex) of a graph which is not adjacent to any other node is called an isolated node (vertex).



* v_4 and v_7 are isolated vertices.

Edges in series

Two edges are said to be in series if their common vertex is of degree 2.

e.g. In the previous graph, two edges incident on v_1 are in series.

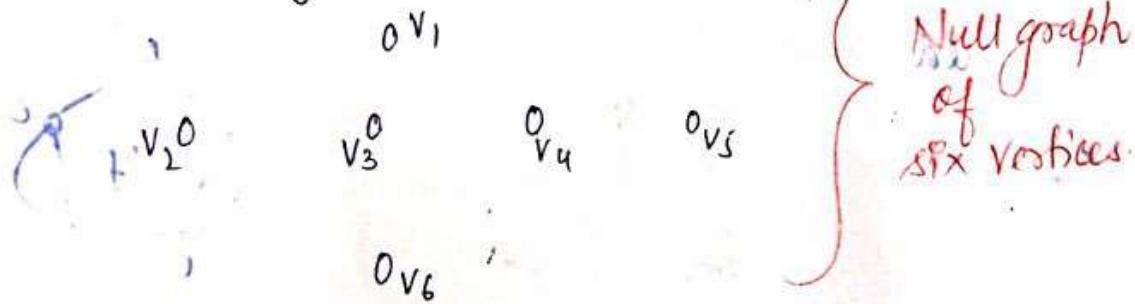
Pendant vertex

A vertex of degree one is called pendant vertex.

e.g. In the previous graph, v_3 is a pendant vertex.

Null graph: Any graph with edge set empty is called Null graph.

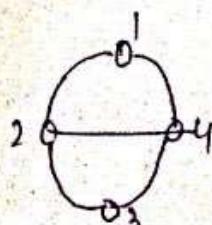
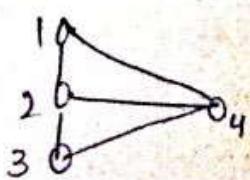
e.g.



Null graph
of
six vertices

* It should be noted that, in drawing a graph, it is immaterial whether the lines are drawn straight or curved, long or short. What is important is the incidence between the edges and vertices.

e.g. The following two graphs are one & the same as the incidence between edges and vertices is the same in both the cases.



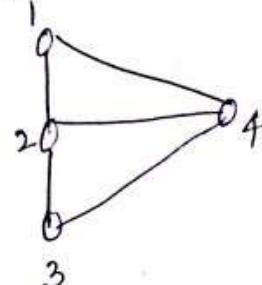
Different diagram
of a same
graph

Finite and Infinite graphs

A graph with a finite number of vertices and edges is called a finite graph. If it has either infinite vertices or infinite edges, it is called an infinite graph.

Simple graph: A graph that has neither self-loops nor parallel edges is called a simple graph.

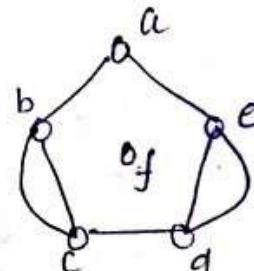
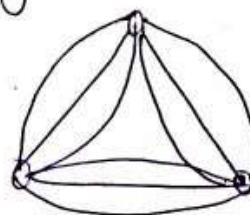
e.g.



Simple graph

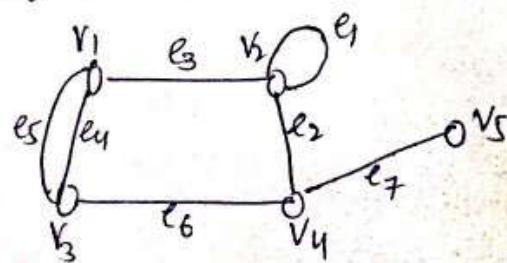
Multigraph: A graph that contains parallel edges is called multigraph.

e.g.



Multigraphs

Pseudograph: A graph in which loops and parallel edges are allowed is called a pseudograph.



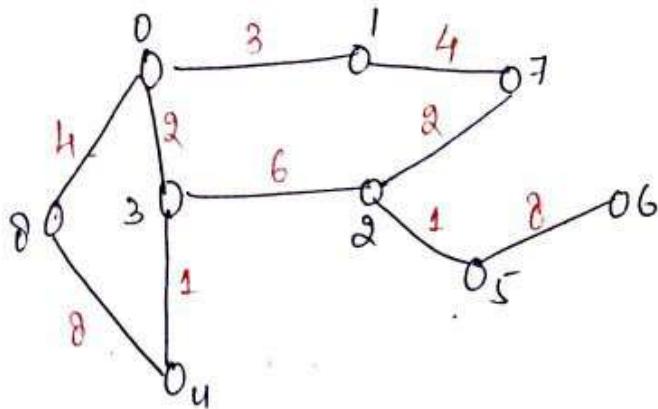
Pseudograph

Regular graph: A graph in which every vertex has the same degree is called a regular graph.



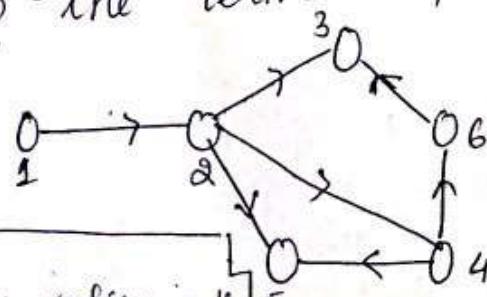
Weighted Graph

Weighted Graph
A graph in which a number (or a weight) is assigned to each edge is called weighted graph.



Digraph or Directed graph :- If in a graph $G = (V, E)$ each edge $e \in E$ is associated with an ordered pair of vertices, then G is called a digraph or directed graph.

- * In such a graph, each edge of the graph has a direction. That is each edge $e = (u, v)$ is represented by means of an arrow from the initial point u to the terminal point v .

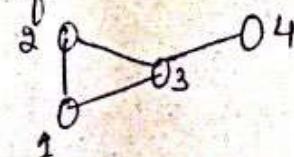


- A directed graph

$$V = \{1, 2, 3, 4, 5, 6\}$$

$$E = \{(1,2), (2,3), (3,4), (4,5), (5,6), (6,1)\}$$

Undirected graph: If each edge is associated with an unordered pair of vertices, then G is called an undirected graph.



An undirected graph can be

graph can be written as
 $V = \{1, 2, 3, 4\}$ $E = \{(1,2), (2,3), (4,3), (1,3)\}$

- * In such a graph, edges do not have a direction.

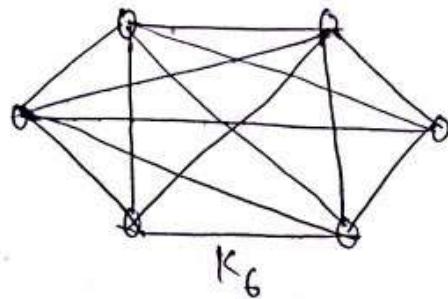
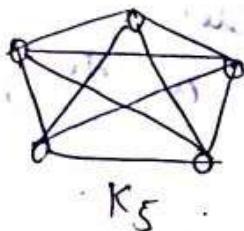
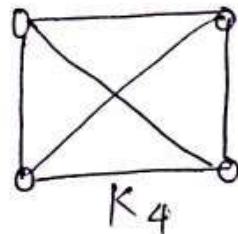
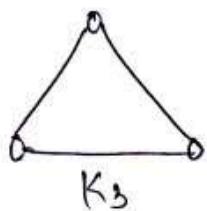
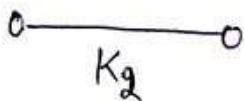
Note:

The direction of a loop in a directed graph is insignificant as the initial and terminal nodes are one and the same.

complete graph:

A simple graph in which every pair of vertices are adjacent. In other words, a graph G with n vertices is said to be complete graph if the degree of every vertex is $n-1$.

- * The complete graph on n vertices is denoted by K_n .



- * The number of edges in K_n are $\frac{n(n-1)}{2}$.
Thus, maximum number of edges in simple graph with n vertices are $\frac{n(n-1)}{2}$.

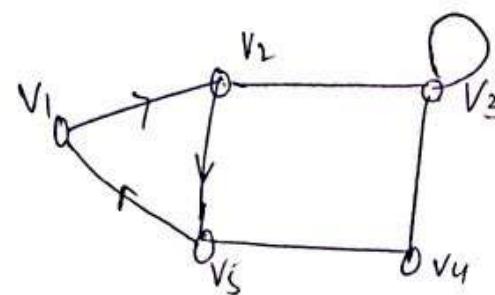
→ Proof: Let G be a simple complete graph with n vertices v_1, v_2, \dots, v_n .

Consider the vertex v_1 , then number of edges drawn from v_1 to all other vertices are $(n-1)$. Similarly, the number of edges drawn from v_2 to other vertices (except v_1) are $n-2$. The number of edges drawn from v_3 (except v_1, v_2) are $n-3$, from v_4 (except v_1, v_2, v_3) are $n-4$, from v_n (except $v_1, v_2, v_3, \dots, v_{n-1}$) to v_n is 1.

Hence, total number of edges are $(n-1) + (n-2) + (n-3) + \dots + 2 + 1 = \sum (n-1) = \frac{n(n-1)}{2}$

Mixed graph: In a graph, if some edges directed and some edges are undirected, then graph is said to be a mixed graph.

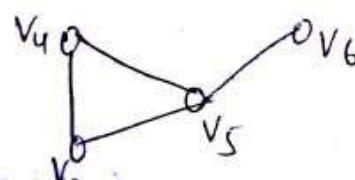
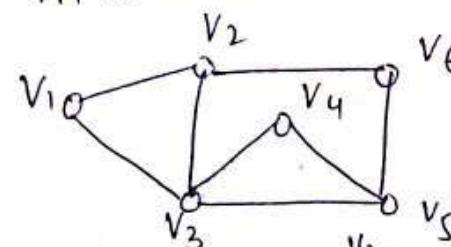
e.g.



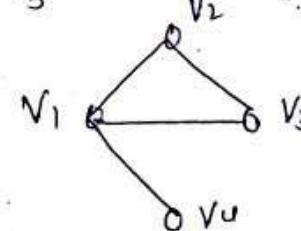
Subgraph: A graph H is said to be a subgraph of G if all the vertices & all the edges of H are in G and if the adjacency is preserved in H . In other words, ** exactly as in G .

e.g.

G



Subgraph of G



Not a subgraph of G

** A graph $H = (V', E')$ is called a subgraph of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$.

Note:

(1) If $V' \subset V$ and $E' \subset E$ then H is called a proper subgraph of G .

(2) If $V' = V$ then H is called a spanning subgraph of G . A spanning subgraph of G need not contain all its edges.

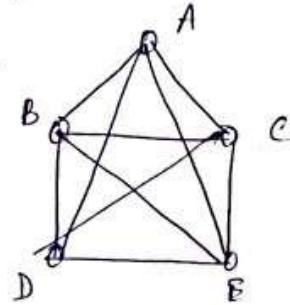
(3) If we delete a subset U of V and all the edges incident on the elements of U from a graph $G = (V, E)$, then the subgraph $(G - U)$ is called a vertex deleted subgraph of G .

* If we delete a subset F of E from a graph $G = (V, E)$, then the subgraph $(G - F)$ is called an edge deleted subgraph of G .

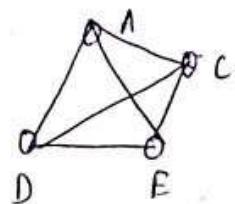
Induced subgraph

A subgraph $H = (V', E')$ of $G = (V, E)$ where $V' \subseteq V$ and E' consists of only those edges that are incident on the elements of V' , is called an induced subgraph of G .

Consider graph G



Now,



- induced subgraph of G

* In directed graphs, the edges are ordered pairs so the definition of the degree of a vertex can be refined to reflect the no. of edges with this vertex as the initial vertex and as the terminal vertex.

In-degree and Out-degree

In a directed graph, the number of edges with v as their terminal vertex is called the in-degree of v and is denoted as $\deg^-(v) \rightarrow (\text{no. of edges ending at } v)$. The number of edges with v as their initial vertex is called the out-degree of v and is denoted as $\deg^+(v) \rightarrow (\text{no. of edges beginning at } v)$.

Note: A vertex with zero in-degree is called a source and a vertex with zero out-degree is called a sink.

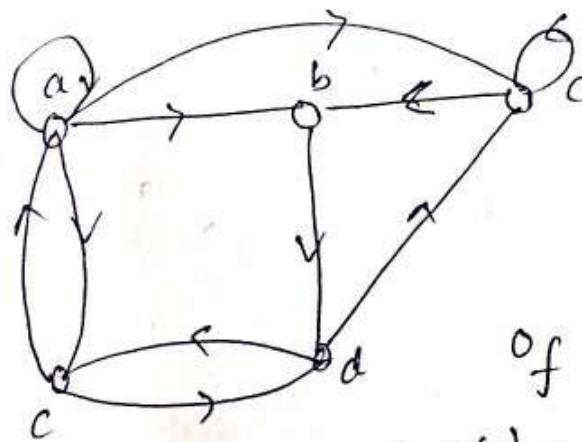
A loop at a vertex contributes '1' to both the in-degree and the out-degree of this vertex.

(2) The sum of the in-degree and out-degree of a vertex is called the total degree of the vertex.

(3) Let $G = (V, E)$ be a graph then

$$(4) |E| = \sum_{v \in V} \deg(v) = \sum_{v \in V} \deg^+(v)$$

no. of elements
in E



$$\text{of } \deg^-(a) = 2, \deg^-(b) = 2, \deg^-(c) = 3, \deg^-(d) = 2, \deg^-(e) = 3$$

$$\text{and } \deg^+(a) = 4, \deg^+(b) = 1, \deg^+(c) = 2, \deg^+(d) = 2,$$

$$\deg^+(e) = 3, \deg^+(f) = 0$$

Matrix representation of graphs

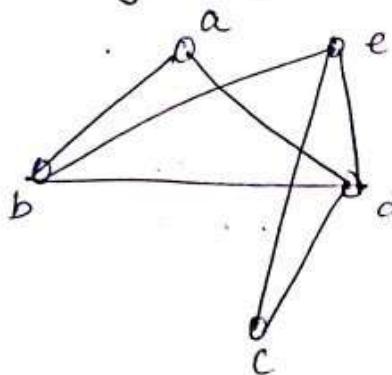
Any graph can be represented by a matrix

Adjacency matrix of an undirected graph with
let G be a simple undirected graph with
n vertices v_1, v_2, \dots, v_n .

The matrix $A = [a_{ij}]$ where $a_{ij} = \begin{cases} 1 & \text{if there is an edge between } v_i \text{ & } v_j \\ 0, & \text{otherwise} \end{cases}$

is called the adjacency matrix of G

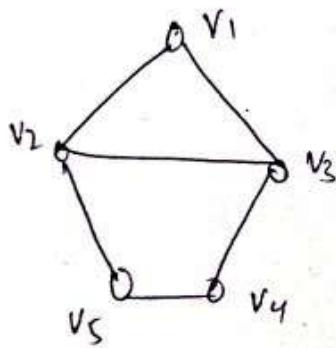
(1)



$$\text{Adjacency matrix; } A(G) = \begin{bmatrix} a & b & c & d & e \\ a & 0 & 1 & 0 & 1 & 0 \\ b & 1 & 0 & 0 & 1 & 1 \\ c & 0 & 0 & 0 & 1 & 1 \\ d & 1 & 1 & 1 & 0 & 1 \\ e & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

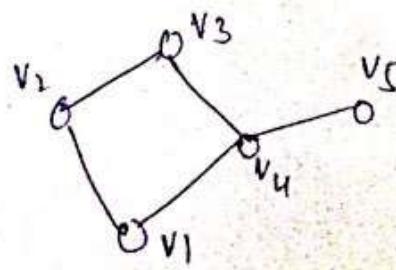
Adjacency matrix; $A(G) =$

(2)



$$A(G) = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 & v_5 \\ v_1 & 0 & 1 & 1 & 0 & 1 \\ v_2 & 1 & 0 & 1 & 0 & 0 \\ v_3 & 1 & 1 & 0 & 1 & 0 \\ v_4 & 0 & 0 & 1 & 0 & 1 \\ v_5 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

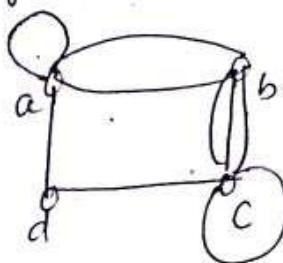
(3)



$$A(G) = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 & v_5 \\ v_1 & 0 & 1 & 1 & 1 & 0 \\ v_2 & 1 & 0 & 1 & 0 & 0 \\ v_3 & 1 & 1 & 0 & 1 & 0 \\ v_4 & 1 & 0 & 1 & 0 & 1 \\ v_5 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

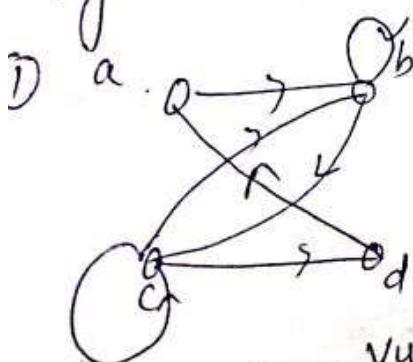
Note:

- (1) All the entries along the leading diagonal are zero iff the graph has no loops.
- (2) sum of all the entries in any row is equal to the degree of the vertices corresponding to that row.
- (3) The adjacency matrix of a simple graph is symmetric.
- (4) A Pseudograph (i.e. an undirected graph with loops and parallel edges) can also be represented by an adjacency matrix. In this case, a loop at the vertex v_i is represented by 1 at (i,i) th position. and the (i,j) th entry equals the no. of edges incident on v_i and v_j . The adjacency matrix for pseudograph is also symmetric.

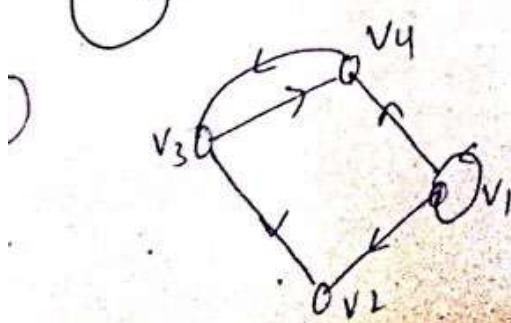


$$A(G) = \begin{bmatrix} a & b & c & d \\ a & 1 & 2 & 0 \\ b & 2 & 0 & 3 \\ c & 0 & 3 & 1 \\ d & 1 & 0 & 0 \end{bmatrix}$$

- (5) Directed simple or multigraphs can also be represented by adjacency matrices that may not be symmetric.



$$A(G) = \begin{bmatrix} a & b & c & d \\ a & 0 & 1 & 0 & 0 \\ b & 0 & 1 & 1 & 0 \\ c & 0 & 1 & 1 & 1 \\ d & 1 & 0 & 0 & 0 \end{bmatrix}$$

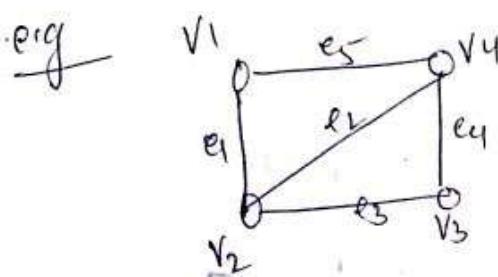


$$A(G) = \begin{bmatrix} v_1 & v_2 & v_3 & v_4 \\ v_1 & 1 & 1 & 0 & 1 \\ v_2 & 0 & 0 & 0 & 0 \\ v_3 & 0 & 1 & 0 & 1 \\ v_4 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Incidence matrix of undirected graph

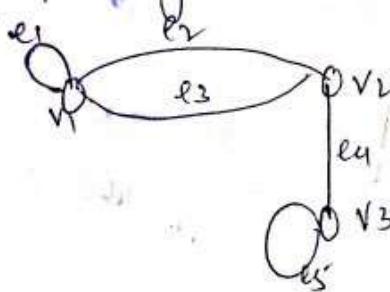
If $G = (V, E)$ is an undirected graph with n vertices v_1, v_2, \dots, v_n and m edges e_1, e_2, \dots, e_m , then the $(n \times m)$ matrix $B = [b_{ij}]$ where $b_{ij} = \begin{cases} 1, & \text{when edge } e_j \text{ is incident on } v_i \\ 0, & \text{otherwise.} \end{cases}$

is called the incidence matrix of G .



$$B = \begin{bmatrix} v_1 & e_1 & e_2 & e_3 & e_4 & e_5 \\ v_2 & 1 & 0 & 0 & 0 & 1 \\ v_3 & 0 & 1 & 1 & 1 & 0 \\ v_4 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

* Incidence matrices can also be used to represent pseudographs

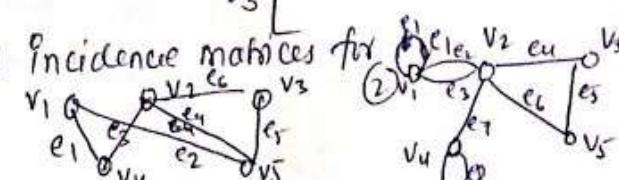


$$B = \begin{bmatrix} v_1 & e_1 & e_2 & e_3 & e_4 & e_5 \\ v_2 & 1 & 1 & 1 & 0 & 0 \\ v_3 & 0 & 1 & 1 & 1 & 0 \\ v_4 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Find Incidence matrices for

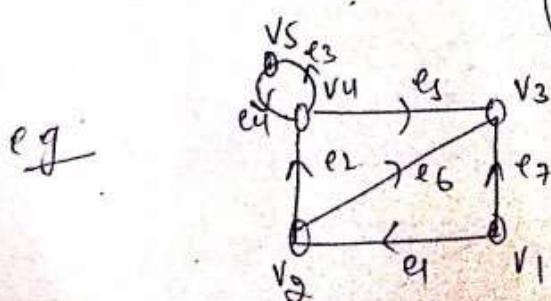
①

②



* For directed graphs The Incidence matrix $B = [b_{ij}]$ can be represented as

$$b_{ij} = \begin{cases} 1 & \text{if } e_j \text{ is incident out of } v_i \\ 0 & \text{" " " not incident on } v_j \\ -1 & \text{" " " incident into } v_i \end{cases}$$



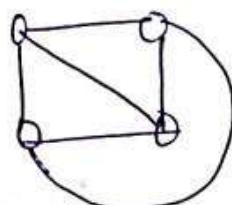
$$B = \begin{bmatrix} v_1 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\ v_2 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ v_3 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ v_4 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ v_5 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Note!

Two graphs are said to be homeomorphic if both can be obtained from the same graph by subdivisions of edges.

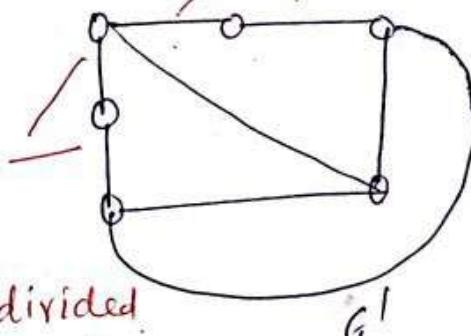
edge is subdivided into two.

e.g.



G

This edge
is subdivided
into two.



G'

The graphs G and G' are homeomorphic.

Planar graphs

A graph G is said to be planar if there exists some geometric representation of G which can be drawn on a plane such that no two of its edges intersect.

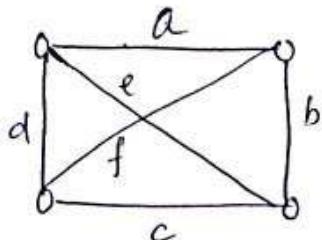
A graph that cannot be drawn on a plane without a crossover between its edges is called non-planar.

* A drawing of a geometric representation of a graph on any surface such that no edges intersect is called embedding. Thus, to declare that a graph G is non-planar, we have to show that of all possible geometric representations of G none can be embedded in a plane.

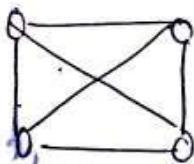
* Equivalently, a graph G is planar if there exists another graph isomorphic to G that is embedded in a plane. Otherwise, G is nonplanar. An embedding

If a planar graph G on a plane is called a plane representation of G .

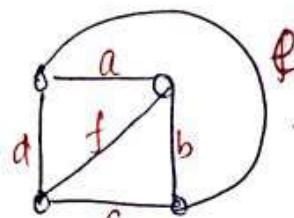
e.g.



This geometric representation is not embedded in a plane because the edges e and f are intersecting.



K_4



Plane representation or embedding of G or Embedding

Redrawing of edge e outside the quadrilateral, leaving the other edges.

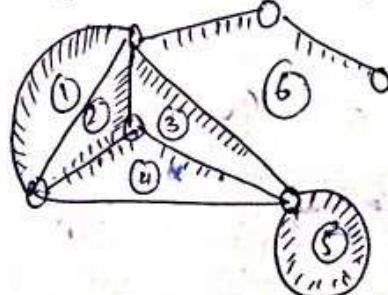
Thus, we see that K_4 is planar.

Conditions of planarity:

Regions or faces or meshes of planar graph.

A plane representation of a graph divides the graph into regions or faces. A region is characterised by the set of edges (or vertices) forming its boundary.

Not e.g.



Note:

- 1) Regions or faces are not defined for non-planar graph.
 - 2) A connected planar graph with n vertices and e edges has $e-n+2$ regions (or faces)
- i.e. $f = e-n+2$.

$$\begin{aligned}f &= \text{no. of faces} \\e &= \text{no. of edges} \\n &= \text{no. of vertices}\end{aligned}$$

Condition of planarity

In any simple, connected planar graph with f regions, n vertices, and e edges ($e \geq 2$), the following inequality must hold:

$$e \leq \frac{3}{2}f$$

$$\text{or, } e \leq 3n - 6$$

Proof: Since each region is bounded by at least three edges and each edge belongs to exactly two regions

$$2e \geq 3f$$

$$e \geq \frac{3}{2}f$$

Substituting $\frac{3}{2}f$ using Euler's formula we have

$$e \geq \frac{3}{2}(e - n + 2)$$

$$\text{or } e \leq 3n - 6.$$

Q. Is K_5 ~~non-planar~~ non-planar?

or Check whether K_5 is planar or non-planar

$$\text{No. of edges in } K_5 = e = \frac{5(5-1)}{2} = 10$$

$$e = 10, n = 5$$

$$3n - 6 = 9 \text{ So, } e \neq 3n - 6.$$

Thus, K_5 is non-planar.

Kuratowski's theorem

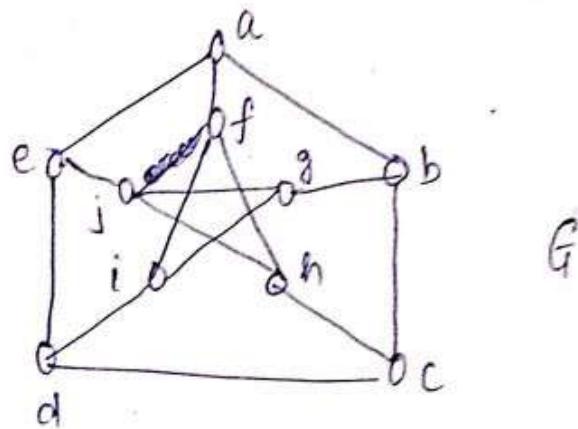
A necessary and sufficient condition for a graph G to be planar is that G does not contain a subgraph that is a subdivision of either $K_{3,3}$ or K_5 (also known as Kuratowski's two graphs)
(or)

A graph G is said to be planar if and only if it has no subgraph homeomorphic to $K_{3,3}$ or K_5 .

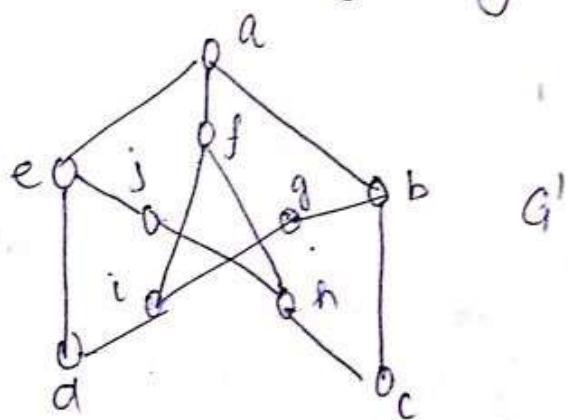
- * The complete graph of five vertices K_5 is the first graph of Kuratowski.
- * The second graph of Kuratowski is a regular connected graph with six vertices and nine edges e.g. $K_{3,3}$.

Show that Petersen graph is non-planar

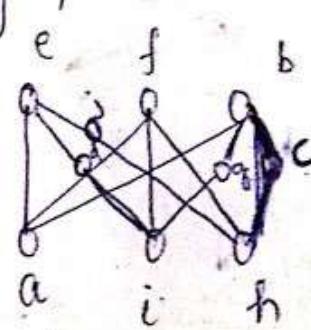
The Petersen graph is an undirected graph with 10 vertices and 15 edges.



Consider the following subgraph of G :



Now, consider the following graph obtained from this subgraph.

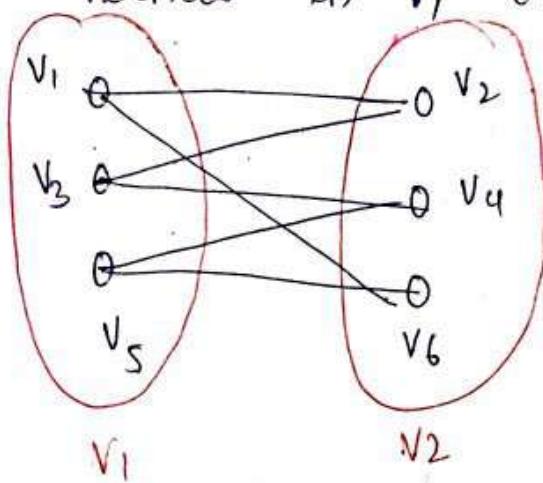


So, the subgraph G' is a subdivision of $K_{3,3}$.
⇒ G is non-planar.

t_i is not directly related to e but there is a path through vertex d (of degree 2) which leads i to e . Similarly, we have from i to b and others

Bipartite graphs

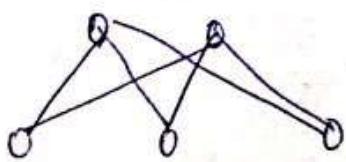
A simple graph G is called bipartite if its vertex set V can be partitioned into two disjoint sets V_1 and V_2 such that every edge in the graph connects a vertex in V_1 and a vertex in V_2 (so that no edge in G connects either two vertices in V_1 or two vertices in V_2)



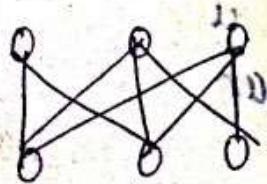
Bipartite graph.

Complete Bipartite graphs

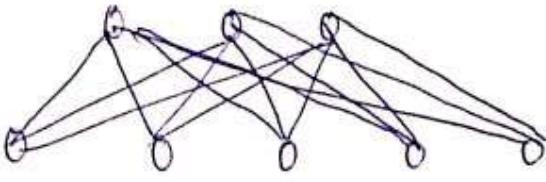
If each vertex of V_1 is connected with every vertex of V_2 by an edge, then graph G is called complete bipartite graph. If V_1 contains m vertices and V_2 contains n vertices, the complete bipartite graph is denoted by $K_{m,n}$.



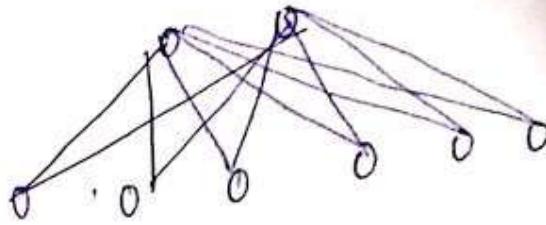
$K_{2,3}$



$K_{3,3}$



$K_{3,5}$



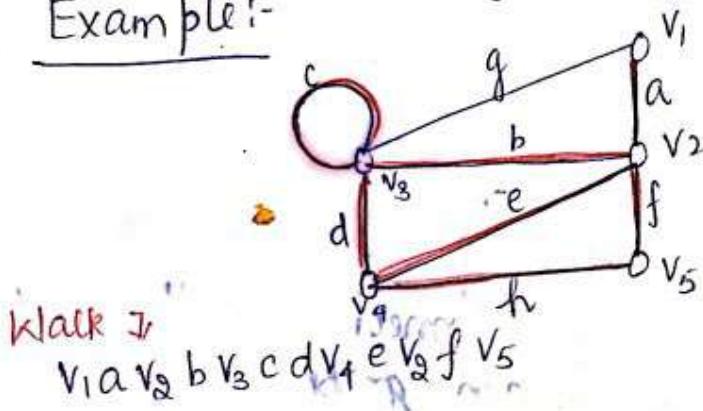
$K_{2,6}$

Complete Bipartite Graphs

Walk: (or edge train) (or chain)

A walk in a graph is a finite alternating sequence of vertices and edges beginning and ending with the vertices, such that each edge is incident on the vertices preceding and following it.

Example:-



Walk I

$v_1 a v_2 b v_3 c d v_4 e v_5 f v_6 g v_7 h v_8$

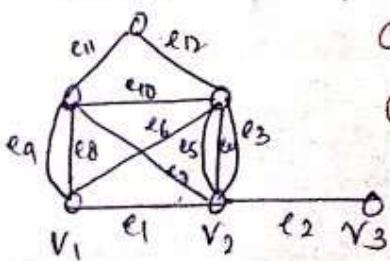
Note!

(1) No edge appears (covered or traversed) more than once in a walk. A vertex may appear more than once.

- (2) Vertices with which a walk begins and ends are called terminal vertices. (v_1 & v_5 are terminal vertices)
- (3) A walk that begins and ends at the same vertex is called a closed walk, otherwise it is called an open walk.

Closed walk:- $v_1 e_1 v_2 e_2 v_4 e_4 v_2 e_7 v_6 e_{10} v_4 e_6 v_1$

Open walk:- $v_1 e_1 v_2 e_3 v_4$



path: if no vertex appears more than once in an open walk then it is called path.

* $v_1 a v_2 b v_3 d v_4$ is a path, whereas $v_1 a v_2 b v_3 c d v_4 e v_2 f v_5$ is not a path.

length of the path:

The number of edges in a path is called the length of the path.

Example: Suppose path is $v_1 e_1 v_2 e_3 v_4$.
length of the path : 2.

Note: ① An edge which is not a self-loop is a path of length one.

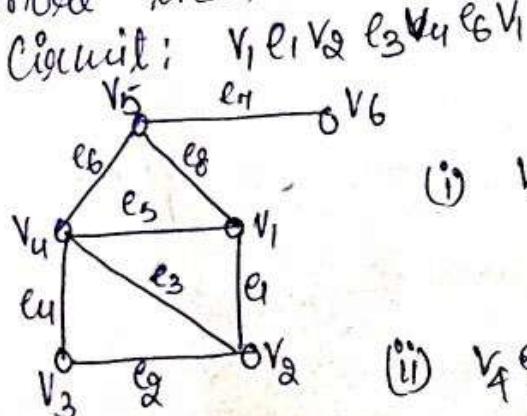
② A self-loop can be included in a walk but not in path.

Circuit: \rightarrow cycle, elementary cycle, circuler path, and polygon. Circuit is defined as a closed walk in which no vertex (except the initial and final vertex) appears more than once.

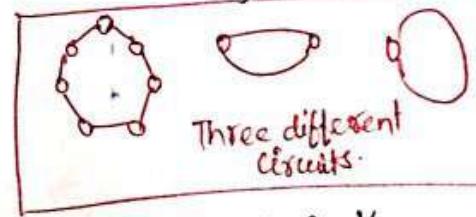
Example:

(i)

Topic:-
CIRCUITS AND
ISOMORPHISM



(i) $v_4 e_5 v_1 e_1 v_2 e_3 v_4 e_4 v_3$



open walk but not a path

(ii) $v_4 e_5 v_1 e_8 v_5 e_7 v_6$
↓
and path, (open walk)

(iv) $v_5 e_3 v_4 e_5 v_1 e_1 v_2$

↓
circuit

(iii) $v_3 e_2 v_2 e_1 v_1 e_5 v_4 e_4 v_3$
↓
circuit or cycle.

Connected graph & disconnected graph

A graph G is said to be connected if there is at least one path between every pair of vertices in G . Otherwise, G is said to be disconnected.

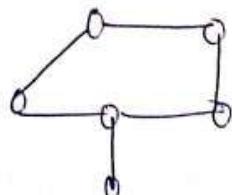
Note:

(1) A disconnected graph consists of two or more connected subgraphs.

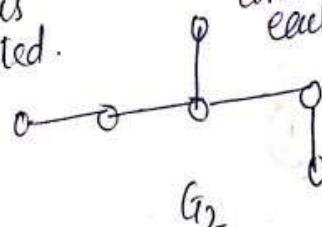
(2) A connected subgraph of a graph G is called a component of the graph G .

(3) A graph of more than one vertex is disconnected.

Example:

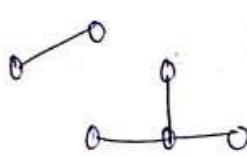


G_1

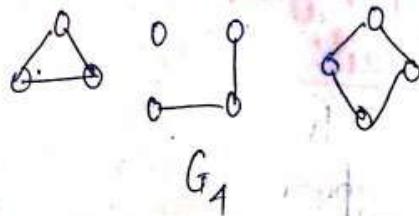


G_2

each connected subgraph called component



G_3



G_1

Connected graphs

(i) G_3 has 2 components.

(ii) G_1 has 3 components.

④ A graph G is disconnected if and only if its vertex set V can be partitioned into two nonempty subsets V_1 and V_2 such that there exists no edge in G whose one vertex is in subset V_1 and other is in V_2 .

conclusion: A simple graph (i.e. a graph without parallel edges or self-loops) with n vertices and k components can have at most $\frac{(n-k)(n-k+1)}{2}$ edges.

or

Let $w(G)$ be the number of components of G , then prove that the number of edges of a simple graph with w components can not exceed $\frac{(n-w)(n-w+1)}{2}$

Let the number of vertices in each of the k components of a graph G be n_1, n_2, \dots, n_k . Thus, we have

$$n_1 + n_2 + \dots + n_k = n, \quad n_i \geq 1$$

$$\Rightarrow \sum_{i=1}^k n_i = n \Rightarrow \sum_{i=1}^k n_i - k = n - k$$

$$\Rightarrow \sum_{i=1}^k (n_i - 1) = n - k \Rightarrow \left[\sum_{i=1}^k (n_i - 1) \right]^2 = n^2 + k^2 - 2nk$$

$$\Rightarrow \sum_{i=1}^k (n_i - 1)^2 + 2 \sum_{i \neq j} (n_i - 1)(n_j - 1) = n^2 + k^2 - 2nk$$

$$\Rightarrow \sum_{i=1}^k (n_i - 1)^2 \leq n^2 + k^2 - 2nk \text{ as } \sum_{i \neq j} (n_i - 1)(n_j - 1) \geq 0 \text{ as each } n_i \geq 1$$

$$\left(\sum_{i=1}^k n_i^2 \right) - k + 2nk \leq n^2 + k^2 - 2nk$$

$$\Rightarrow \left(\sum_{i=1}^k n_i^2 \right) \leq n^2 - (2n - k)(k - 1) \quad \text{--- (1)}$$

We know maximum number of edges in G because
 i^{th} component is $\frac{n_i(n_i-1)}{2}$.

Maximum no. of edges in G are.

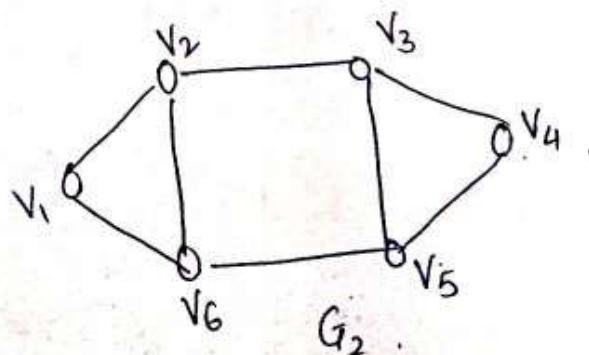
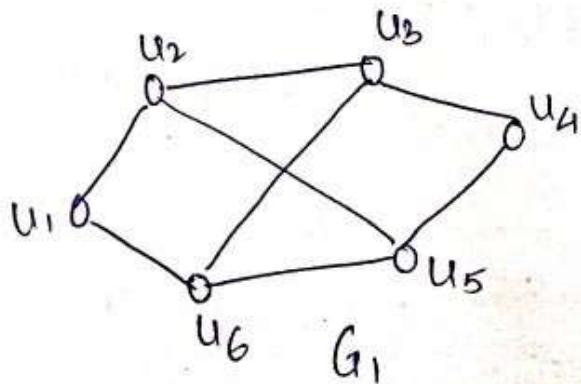
$$\sum_{i=1}^k \frac{n_i(n_i-1)}{2} = \frac{1}{2} \sum_{i=1}^R n_i^2 - \frac{1}{2} \sum_{i=1}^k n_i$$

$$\leq \frac{1}{2} \left(n^2 - (2n-k)(k+1) \right) - \frac{n}{2}$$

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

Circuits and Isomorphism

- * If two graphs are circuits of the same length R , where $R \geq 2$.
 If this condition is not satisfied then the two graphs will not be isomorphic.
- * Consider following two graphs G_1 and G_2 .



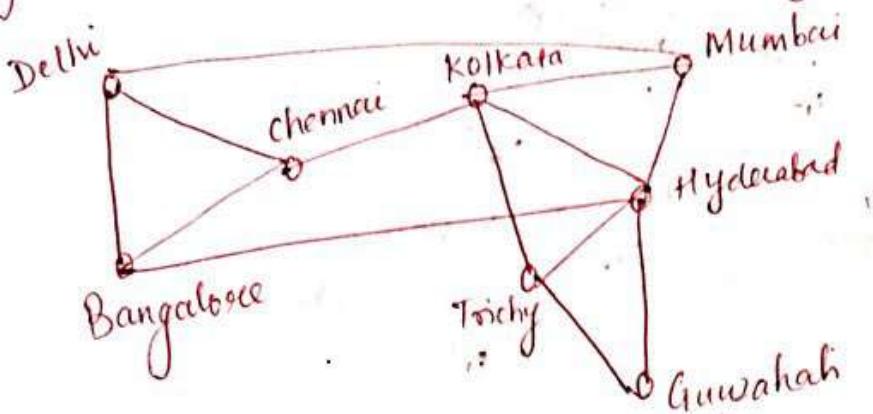
No. of vertices in G_1 and G_2 = 6.

No. of edges in G_1 and G_2 = 8.

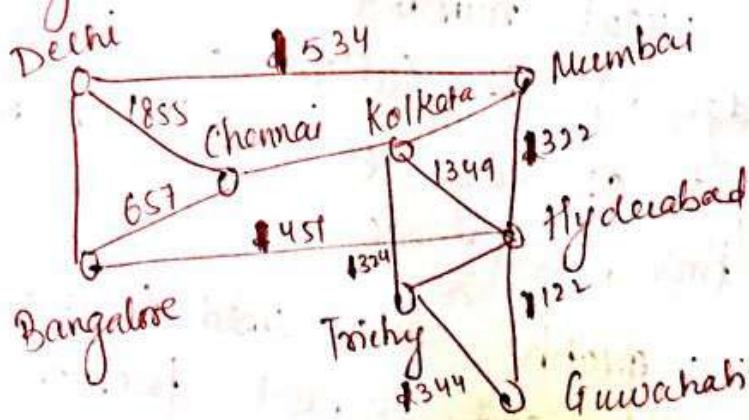
Both of them have 4 vertices of degree 3 and 2 vertices of degree 2.

Shortest Path Problem

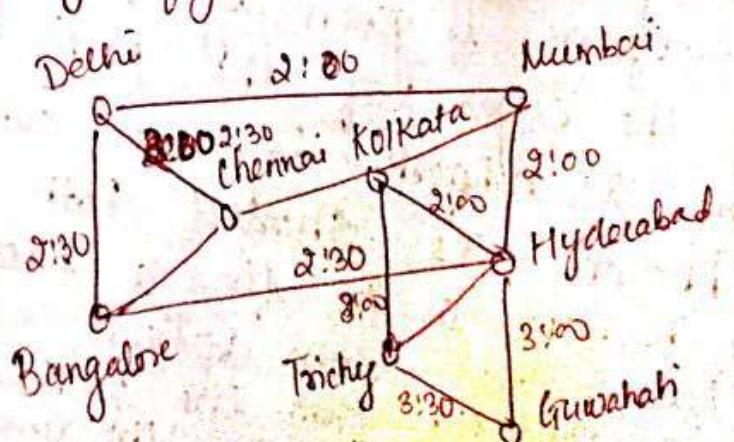
- * Consider the modeling of an airline system
- * Its basic graph model can be represented by ^{describing} cities as vertices and flights by edges



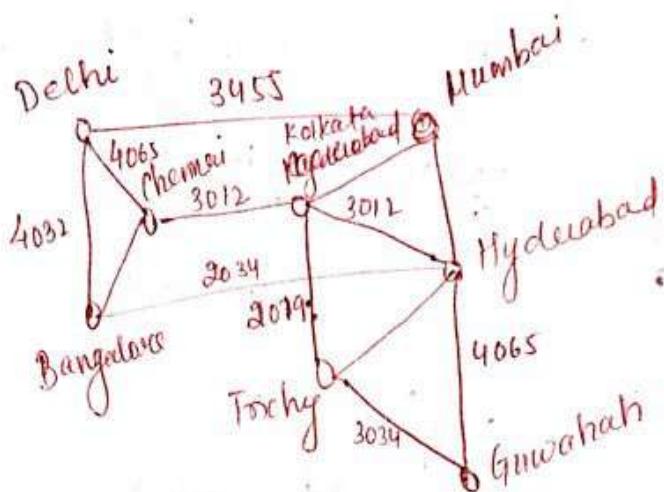
- (1) Problems involving distances can be modeled by assigning distances between cities to the edges.



- (2) Problems involving flight time can be modeled by assigning flight times to edges.



③ Problems involving fares can be modeled by assigning fares to the edges.



Weighted Graph

A graph in which each edge e is assigned a non-negative real number $w(e)$ (also known as weight of edge e) is called weighted graph. This weight of edge e i.e. $w(e)$ may represent distance, time, cost etc.

* Weighted graphs are used to model several networks and several problems involving weighted graphs arise frequently.

* Determining a path of least length (where length of a path is given by the sum of the weights of the edges of the path) between two vertices in a network is one such problem.

It is known as Shortest Path Problem where the problem is to find a path of least length between two given vertices from the previous definition of the length of a path.

For example, in the previous graphs of airline system what is the shortest path in air distance between Delhi and Trichy? what is the cheapest fare between these two cities?

Shortest path Algorithm

- * Several different algorithms that find a shortest path between two vertices in a weighted graph.
- * A greedy algorithm discovered by the Dutch mathematician Edsger Dijkstra in 1959.
- * The version described solves the problem in undirected weighted graphs where all the weights are positive.

Dijkstra's Algorithm

We consider a weighted connected simple graph G with vertices $a = v_0, v_1, v_2, \dots, v_n = z$ and weights $w(v_i, v_j) \geq 0$ where $w(v_i, v_j) = \infty$ if $\{v_i, v_j\}$ is not an edge.

procedure Dijkstra (G : weighted connected simple graph, with all weights positive)

for $i = 1$ to n

$L(v_i) = \infty$

$L(a) = 0$ [The labels are now initialized so that the label of a is 0 and all other labels are ∞ , and S is the empty set]

while $z \notin S$ with $L(u)$ minimal

$u = a$ vertex not in S with $L(u)$ minimal

$S = S \cup \{u\}$

for all vertices v not in S

if $L(u) + \omega(u,v) < L(v)$ then
 $L(v) = L(u) + \omega(u,v)$

This adds
a vector to
with minimal len.
and updates the
labels of vertices
not in S

^{↓ in line with white}
between $L(z)$ [$L(z) = \text{length of shortest path}$
from a to z]

In other words,

This algorithm begins by assigning a label 0 to the starting vertex s and a temporary level ∞ to the remaining $n-1$ vertices. In each iteration, other vertex gets a permanent label, according to the following rule.

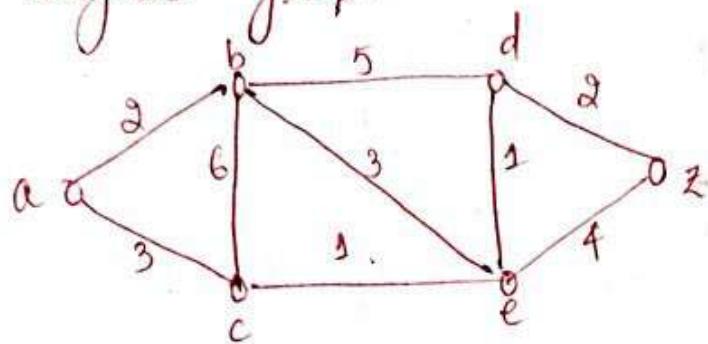
1. Each vertex j that is not yet permanently labeled gets a new temporary label, whose value is given by $\min \{ \text{old label of } j, \text{old label of } i + d_{ij} \}$, where i is the latest vertex permanently labeled in the previous iteration, and d_{ij} is direct distance between vertices i and j.
2. If i and j are not joined by an edge even $d_{ij} = \infty$.
3. The smallest value among all the temporary labels is found, and this becomes the permanent label of corresponding vertex.

In case of tie we can select any one for permanent labeling

Repeat steps 1 and 2 until destination vertex (say d) gets a permanent label.

Ques 2

Question ① Use Dijkstra's algorithm to find the cost of the cheapest path between a and z in the following weighted graph

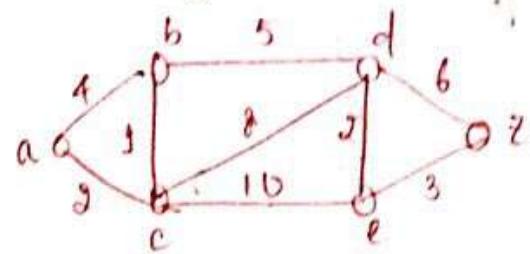


The iterations of Dijkstra's algorithm are described in the following table.

S initially empty	L(a)	L(b)	L(c)	L(d)	L(e)	L(z)
\emptyset	0	∞	∞	∞	∞	∞
$\{a\}$	0	2	∞	∞	∞	∞
$\{a, b\}$	0	2	3	∞	5	∞
$\{a, b, c\}$	0	2	3	7	4	∞
$\{a, b, c, d\}$	0	2	3	7	4	8
$\{a, b, c, d, e\}$	0	2	3	5	4	7
$\{a, b, c, d, e, z\}$	0	2	3	5	4	7

In the last iteration, yes and $L(z) = 7$. Thus, the cheapest path from a to z has a cost of 7.

(2) Find shortest distance between a to z by Dijkstra's algorithm

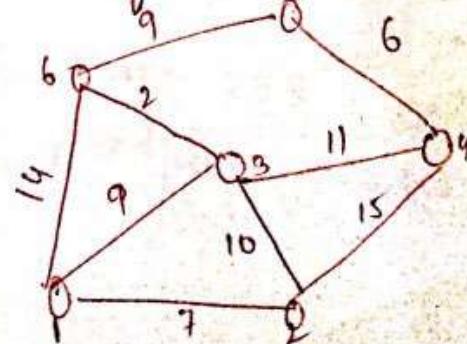


The iterations of Dijkstra's algorithm are described in the following table.

S	L(a)	L(b)	L(c)	L(d)	L(e)	L(z)
\emptyset	0	∞	∞	∞	∞	∞
{a}	0	1	2	∞	∞	∞
{a,c}	0	3	2	10	12	∞
{a,c,b}	0	3	2	8	12	∞
{a,c,b,d}	0	3	2	8	10	14
{a,c,b,d,e}	0	3	2	8	10	13
{a,c,b,d,e,z}	0	3	2	8	10	13

→ a,c,b,d,e
Required cost

(3) Use Dijkstra's algorithm to find the shortest path from node 1 to all the other nodes.



The iterations of Dijkstra's algorithm are described in the following table.

S	L(1)	L(2)	L(3)	L(4)	L(5)	L(6)
\emptyset	10	∞	∞	∞	∞	∞
$\{1\}$	10	7	9	∞	∞	14
$\{1,2\}$	10	4	9	22	∞	14
$\{1,2,3\}$	0	7	9	20	∞	11
$\{1,2,3,6\}$	0	7	9	20	20	11
$\{1,2,3,6,4\}$	0	7	9	20	20	11
$\{1,2,3,6,4,5\}$	0	7	9	20	20	11

Edge covering or Line covering

Let $G = (V, E)$ be a graph. A subset $C(E)$ is called a line covering of G if every vertex of G is incident with atleast one edge in C .

Minimal Line covering

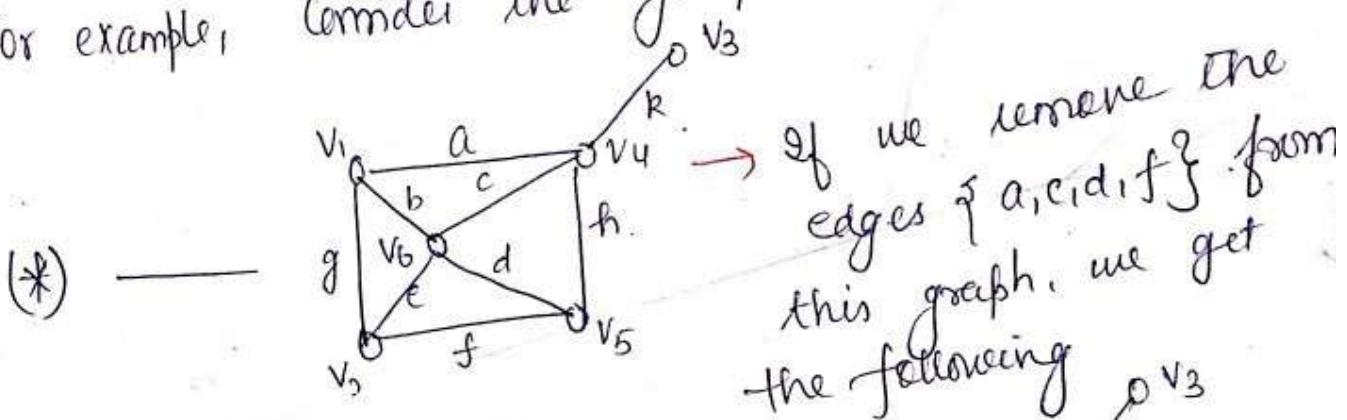
A line covering C of a graph G is said to be minimal if no edge can be deleted from C .

Minimum Line covering

It is also known as smallest minimal line covering. A minimal line covering with minimum number of edges is called a minimum line covering of G .

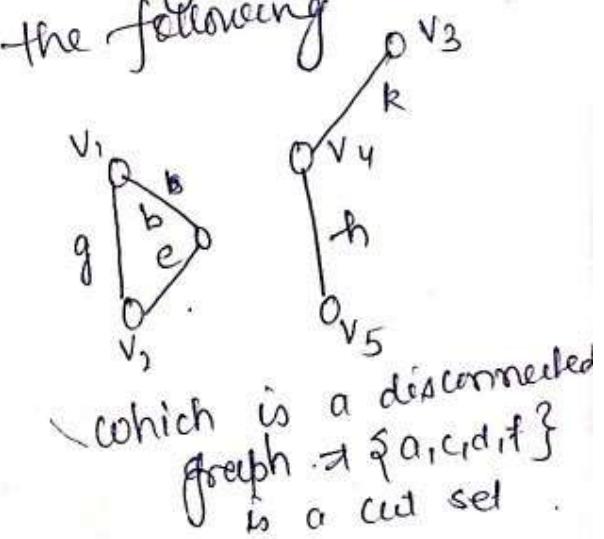
Cut set! In a connected graph G , a cut-set is a set of edges whose removal from G leaves G disconnected, provided removal of no proper subset of these edges disconnects G .

For example, consider the graph



- * Other cut sets of this graph are: $\{a, b, g\}$, $\{a, b, e, f\}$ and $\{d, h, f\}$.

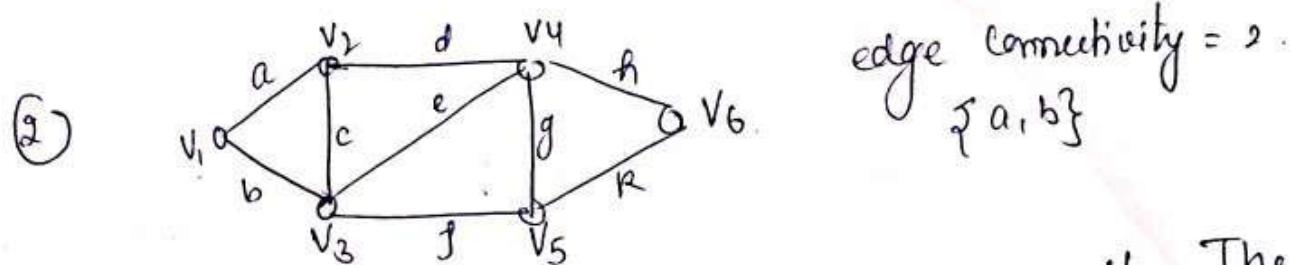
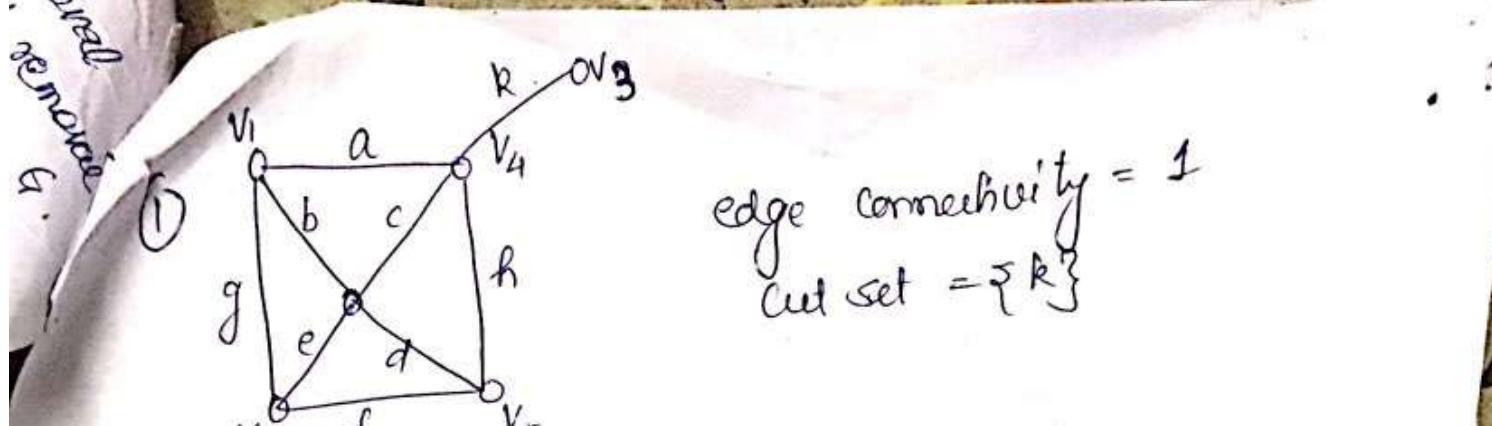
- * Edge set $\{k\}$ is also a cut-set.



Connectivity

Edge Connectivity: Let G be a connected graph. The edge connectivity of G is the minimum number of edges (edges) whose removal results in a disconnected graph. (or) The number of edges in the smallest cut-set (i.e. cut-set with fewest number of edges) is defined as the edge connectivity of G .

- * The edge connectivity of a connected graph G is denoted by $\lambda(G)$. If G is a disconnected graph, $\lambda(G) = 0$.

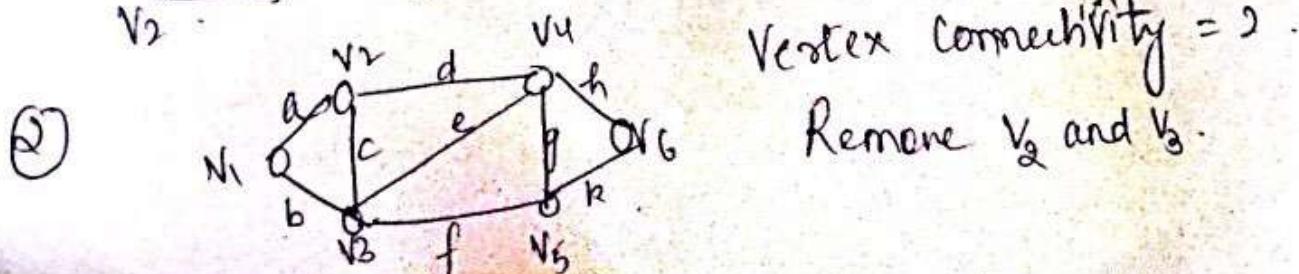
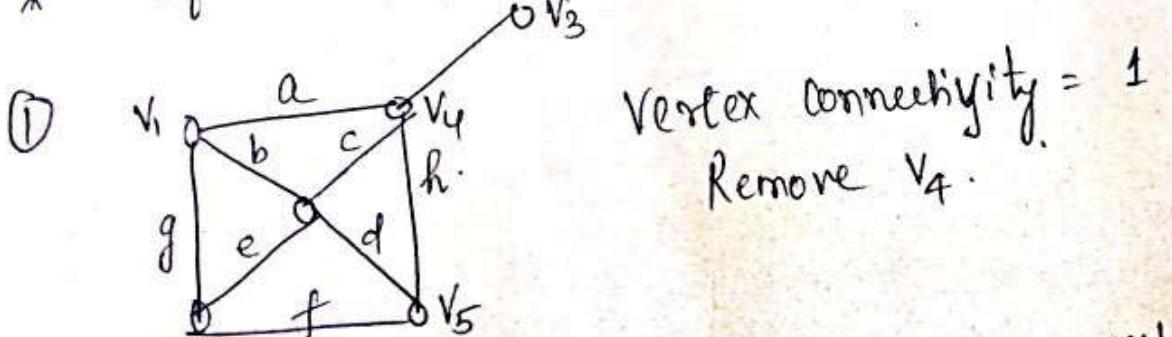


Vertex Connectivity. Let G be a connected graph. The minimum number of vertices whose removal results in a disconnected or trivial graph is called the vertex connectivity of G .

* The vertex connectivity of G is denoted by $k(G)$.
if $k(G) = 1$, then G has a vertex v such that $G - v$ is not connected and the vertex v is called a cut-vertex.

* if $G = K_n$, then $k(G) = n-1$.

* A graph G is separable if its vertex connectivity is 1.



Note:

- (1) The vertex-connectivity of a graph G is always less than or equal to the edge connectivity of G , i.e. $\kappa(G) \leq \lambda(G)$.
- (2) The edge connectivity of a connected graph G : Cannot exceed the minimum degree of G . i.e. $\lambda(G) \leq \delta(G)$
- (3) For any graph G , $\kappa(G) \leq \lambda(G) \leq \delta(G)$.

The degree of the vertex with the least number of edges incident to it.
[max. is denoted by $\Delta(G)$]

Cut-edge (Bridge) Let G be a connected graph where e is one of the edges of G . If $G-e$ is not connected, the edge e is called a cut-edge (or bridge).
For example, in the graph * edge R is cut-edge.

* If edge connectivity of a graph is 1 then the edge of that cut-set is cut-edge.

Cut-Vertex: Let G be a connected graph. If V is a vertex of G such that $G-V$ is not connected, then

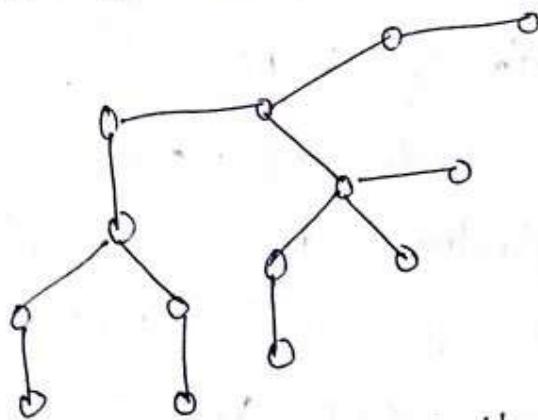
Note: the vertex V is called a cut vertex. If V is a cut vertex of G , then the removal of the vertex V increases the number of components in G .

(2) A cut vertex is also called a cut-point.
For example, in the graph * vertex \bullet is v_4 that is also giving vertex connectivity as 1.

MODULE 7TREES

Tree: A connected graph without any circuits is said to be a tree.

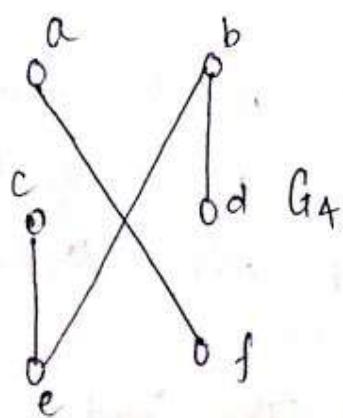
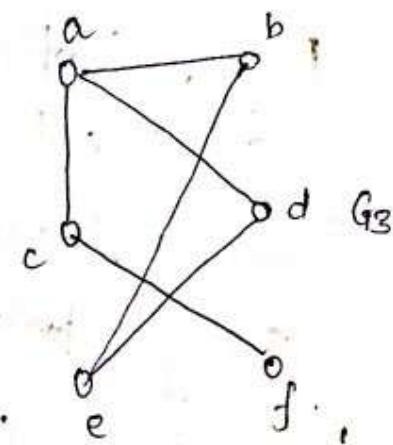
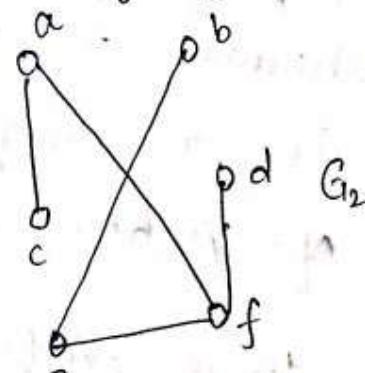
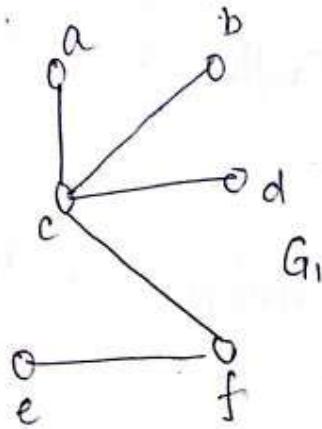
Example:



Note! ① Every tree is a simple graph (\because loops and parallel edges form circuits)
② A subgraph of a tree is also a tree.

(2) A subgraph of a tree is also a tree.

Which of the following graphs are trees?



- * G_1 and G_2 are trees because both are connected graphs with no simple circuits
- * G_3 is not a tree because e, b, a, d, e is a simple circuit in the graph.
- * G_4 is not a tree because it is not connected.

Some Properties

① An undirected graph is a tree if and only if there is a unique simple path between every pair of vertices.

Proof: Let the undirected graph T be a tree.

Then, by definition of a tree, T is connected.

Thus, there is a simple path between any pair of vertices say v_i and v_j .

Now, if possible suppose there are two paths between v_i and v_j - one from v_i to v_j and

the other from v_j to v_i .

But, combination (or union) of these two paths would contain a circuit whereas T cannot have a circuit.

Thus, there is a unique simple path between every pair of vertices in T .

Conversely, let there exists a unique path between every pair of vertices in the graph.

Then, T is connected.

Suppose, T contains a circuit which means there is a pair of vertices v_i and v_j between which two distinct paths exist which leads to a

contradiction.

Hence, T can not have a circuit. This implies that T is a tree.

Q) A tree with n vertices has $n-1$ edges.

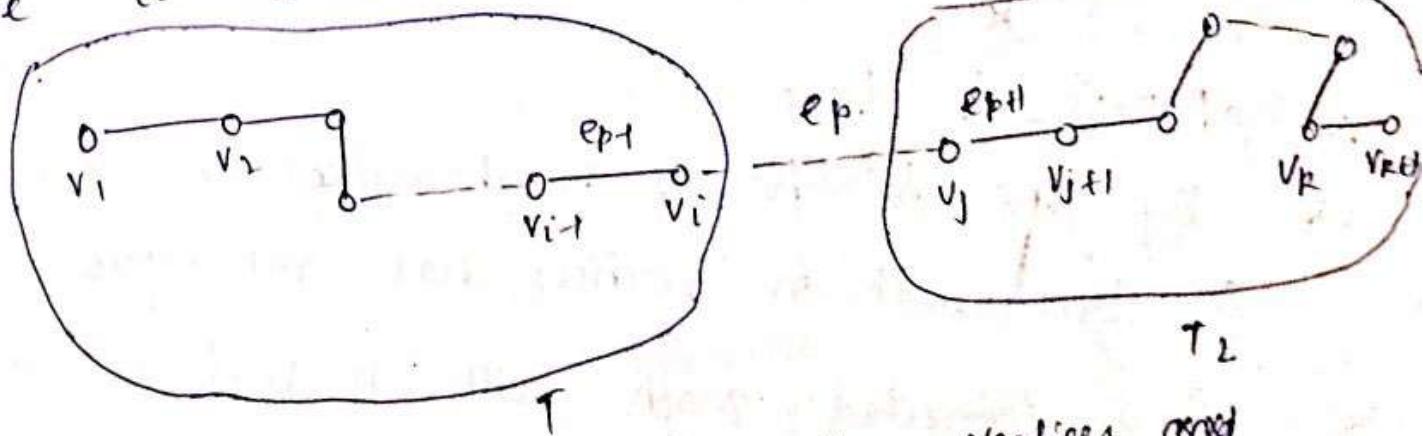
Proof: We shall prove it by principle of mathematical induction.

Let $P(n)$ denotes the statement "A tree with n vertices has $n-1$ edges".
For $n=1$, we have a tree with 1 vertex and 0 edge.

Thus, $P(1)$ is true.

Let us assume that $P(k)$ is true i.e. a tree with k vertices has $k-1$ edges.

Now, we have to prove $P(k+1)$ is true i.e. a tree with $k+1$ vertices has k edges.



Now, let T be a tree with $k+1$ vertices and consider an edge $e_{p+1}(v_i, v_j)$.

Remove $e_{p+1}(v_i, v_j)$ then the graph is disconnected giving us two components namely T_1 & T_2 .

New, number of vertices in $T_1 = k_1$

" " edges in $T_1 = k_1 - 1$ ($\because k_1 < k$)

minimal
meas.

number " of vertices in $T_2 = k_2$ and $(k_2 < k)$
 " edges " " = $k_2 - 1$

Total number of edges in T

= Total number of edges in \tilde{t}_i , \tilde{t}_j

$$= k_1 - 1 + k_2 - 1 + 1$$

$$= k_1 + k_2 - 1$$

$$\therefore k+1-1 \quad (\because k_1+k_2 = k+1)$$

二
一

$\therefore P(k+1)$ is true.

∴ By the principle of mathematical induction.

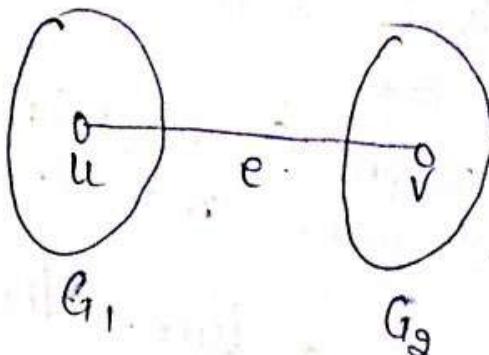
A tree with n vertices has $n-1$ edges.

(3) Any connected graph with n vertices and $(n-1)$ edges is a tree.

④ Any circuitless graph with n vertices and $n-1$ edges is a tree.

Thus, $G \cup \{e\}$ is connected graph (tree) of n vertices, having n edges and no cycles. \Rightarrow
 This contradicts the fact that a tree with n vertices has $n-1$ edges.

Hence, G is connected.

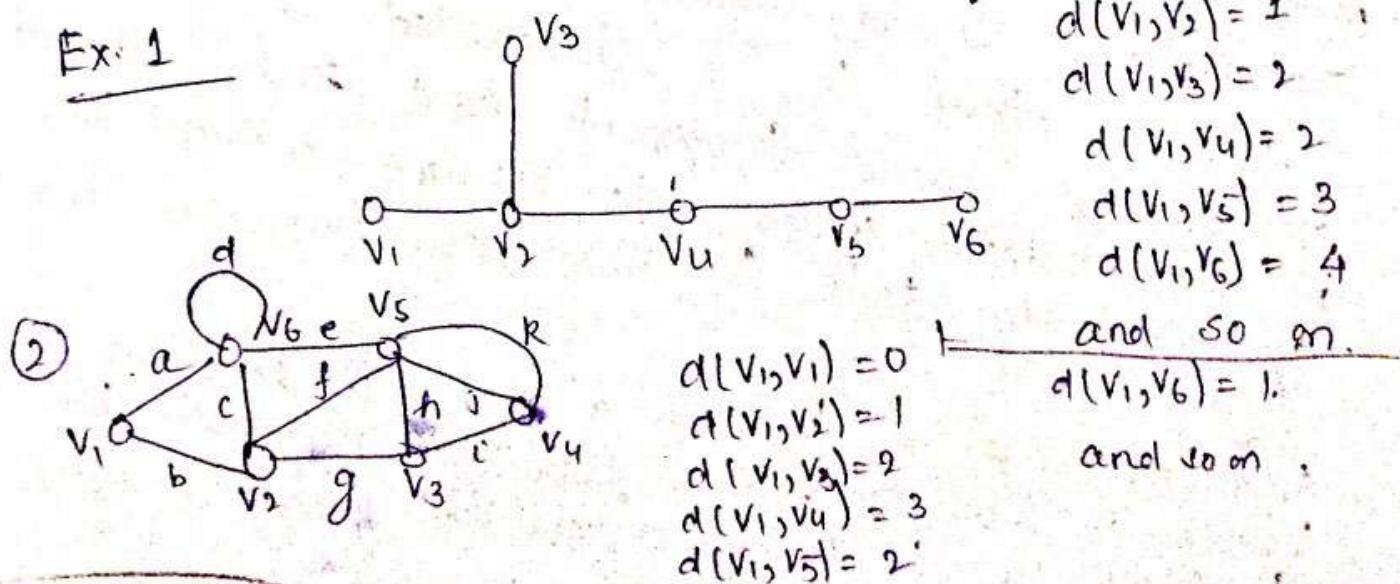


Note: In any tree (with two or more vertices) there are atleast two pendant vertices.

Distance and centre in a tree

Distance: In a connected graph, G , the distance $d(v_i, v_j)$ between two of its vertices v_i & v_j is the length of the shortest path between them.

Ex. 1

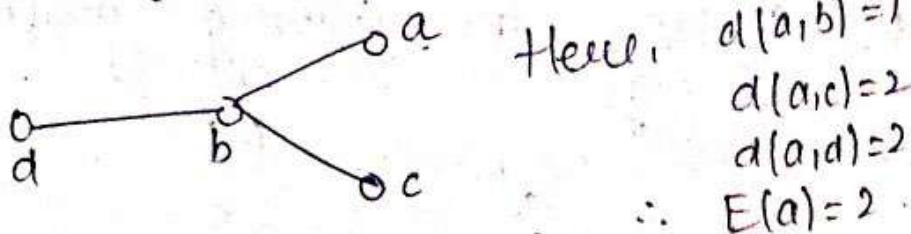


If there is no path connecting u and v then $d(u,v) = \infty$.

Eccentricity of a vertex.

Let G be a graph and v be a vertex of G . The eccentricity of the vertex v is the maximum distance from v to any vertex. i.e. $e(v) = \max \{ d(v,w) : w \in V(G) \}$

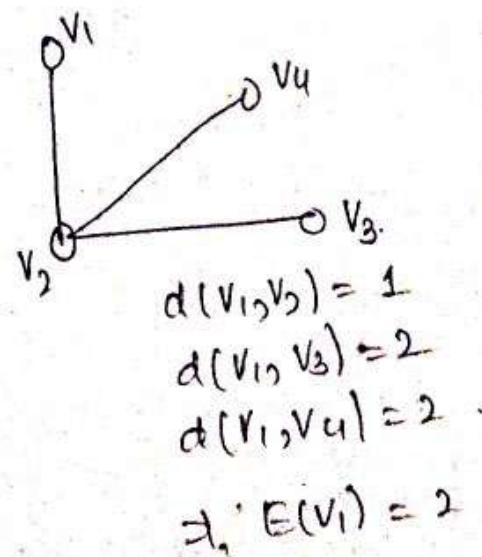
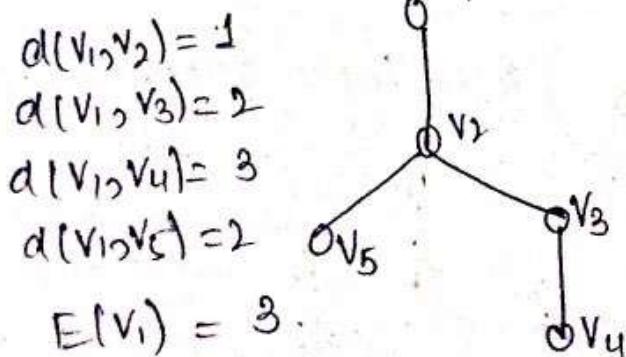
Example:-



What is $E(b)$, $E(c)$, and $E(d)$?

$$E(b) = 1, \quad E(c) = 2, \quad E(d) = 2.$$

Ques. Find the eccentricity of v_1 in the following graphs.

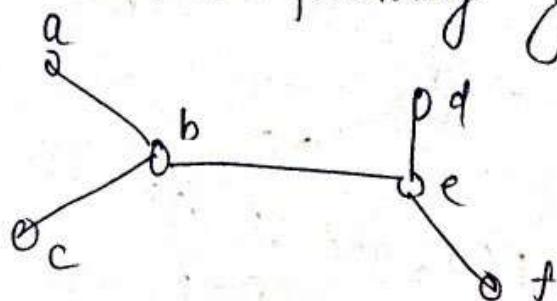


Center of a tree

A vertex with minimum eccentricity in graph G is called a center of G . The eccentricities of the vertices of the previous graphs are $E(a)=2$, $E(b)=1$, $E(c)=2$, $E(d)=2$.

Hence vertex b is the center of that tree.

* Consider the following graph.

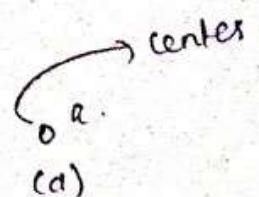
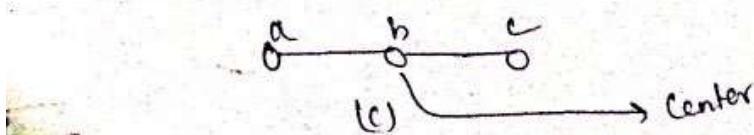
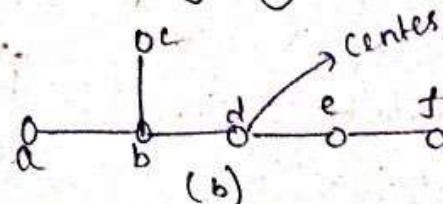
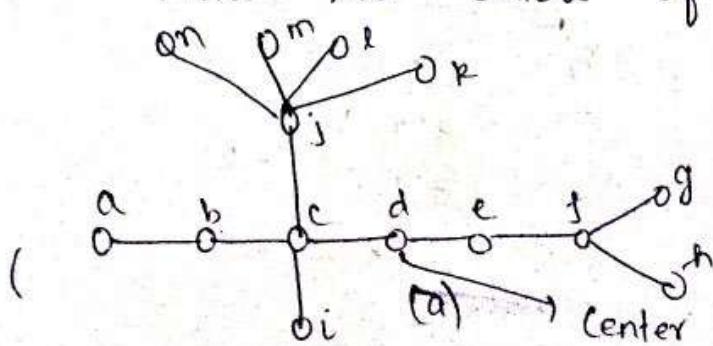


$$\begin{aligned}E(a) &= 3 \\E(b) &= 2 \\E(c) &= 3 \\E(d) &= 3 \\E(e) &= 2 \\E(f) &= 3\end{aligned}$$

Thus, this graph or tree has two centers.

Note: Every tree has either one or two centers.

Find the centers of the following graphs.



Radius of a tree

The radius of G is the minimum eccentricity among the vertices of G (or the eccentricity of the center).
 i.e. $\text{radius}(G) = \min \{e(v) : v \in V(G)\}$

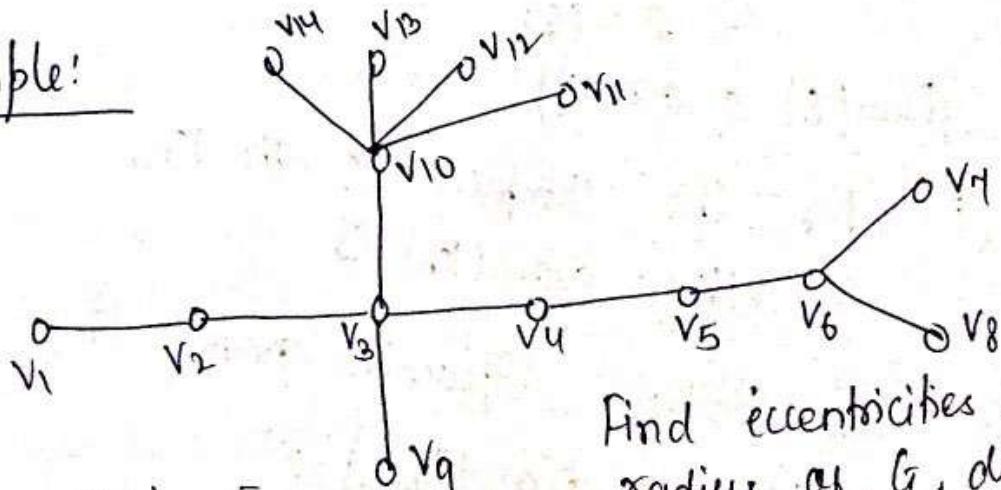
Diameter of a tree

The diameter of a graph G is the maximum eccentricity among the vertices of G .
 Thus, $\text{diameter}(G) = \max \{e(v) : v \in V(G)\}$

Note: The radius of a connected graph may not be half of its diameter.

Example:

G



$$e(v_1) = 6, e(v_2) = 5,$$

$$e(v_3) = 4, e(v_4) = 3$$

$$e(v_5) = 4, e(v_6) = 5$$

$$e(v_7) = 6, e(v_8) = 6$$

$$e(v_9) = 5, e(v_{10}) = 5$$

$$e(v_{11}) = 6, e(v_{12}) = 6$$

$$e(v_{13}) = 6, e(v_{14}) = 6$$

Find eccentricities of every vertex, radius of G , diameter of G , and center of G .

$$\text{Minimum eccentricity} = 3$$

$$\therefore r(G) = 3$$

$$\text{Maximum eccentricity} = 6$$

$$\therefore \text{Diam}(G) = 6$$

Center is $\{v_4\} \because e(v_4) = r(G) = 3$.
 Here, v_4 is called the center of a vertex or a central vertex.

Theorem: In a simple graph G ,

$$\gamma(G) \leq \text{diam}(G) \leq 2\gamma(G)$$

Proof: Obviously, from the definition.

$$\gamma(G) \leq \text{diam}(G)$$

To Prove: $\text{diam}(G) \leq 2\gamma(G)$

Consider two vertices u and v such that
 $d(u, v) = \text{diam}(G)$

$$\begin{aligned}\text{diam}(G) &= d(u, v) \\ &\leq d(u, w) + d(w, v) \\ &\leq e(w) + e(w) \\ &= 2e(w) \\ &= 2\gamma(G)\end{aligned}$$

$$\therefore \text{diam}(G) \leq 2\gamma(G)$$

Note: ① For the complete graph K_n ,
 $\gamma(K_n) = \text{diam}(K_n) = 1$

② For the complete bipartite graph $K_{m,n}$.
 $\gamma(K_{m,n}) = \text{diam}(K_{m,n}) = 2$.

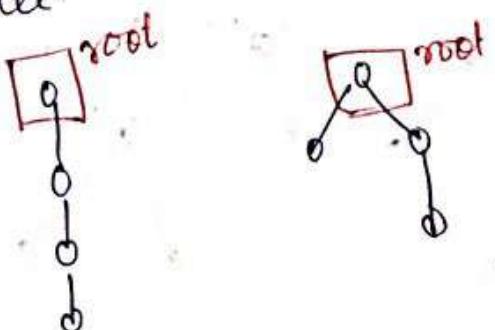
③ For the Petersen graph, $\gamma(P) = \text{diam}(P) = 2$.

Subtree: A connected subgraph of a tree T is a subtree of T .

Rooted tree

A tree in which one vertex (called the root) is distinguished from all the others is called a rooted tree.

Example:



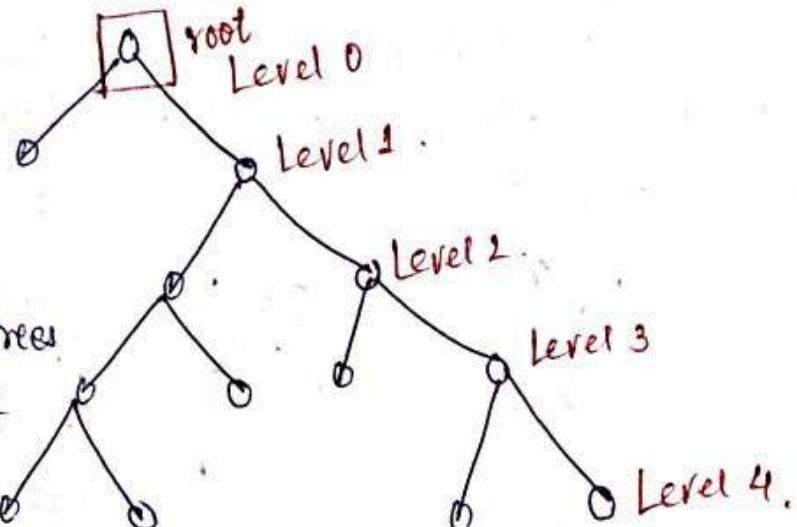
Binary Tree

A Binary tree is defined as a tree in which there is exactly one vertex of degree two & each of the remaining vertices is of degree one (or) three.

* Any tree may be made into a rooted tree by selecting one of the vertices as the root. A rooted is a directed tree if there is a root from which there is a directed path to each vertex of the tree.

- Note!
- ① A node with degree two in a binary tree is said to be a root.
 - ② Every binary tree is a rooted tree.
 - ③ A non-pendant vertex in a tree is called an internal vertex.
 - ④ The number of internal vertices in a binary tree is one less than the number of pendant vertices.
 - ⑤ In a binary tree a vertex v_i is said to be at level i if v_i is at a distance of i from the root. Thus, the root is at level 0.

Example:



Result

13- Vertex, 4-level
binary tree
Pendant Vertices = 7

The number of internal vertices in a binary tree is $7 - 1 = 6$.

The number of vertices at levels 1, 2, 3, and 4 are
2, 2, 4, and 4 respectively.

Theorem: The number of vertices n in a binary tree is always odd.

Proof: Let T be a binary tree with n vertices. By the definition of binary tree, one vertex is of degree two and the remaining $n-1$ vertices are of degree one (or) three. i.e. the remaining $(n-1)$ vertices are of odd degree.

Now, by theorem "The number of odd degree vertices is even number", we get that $n-1$ is even.

∴ n is odd.

Hence Proved

Theorem: The number of Pendant vertices in a binary tree is $\frac{n+1}{2}$.

Proof: Let p be the number of pendant vertices in a binary tree T .

Since p vertices are of degree one; 1 vertex is of degree two; $n-(p+1)$ vertices are of degree three.

We know that, $\sum d(v_i) = 2e$.

A tree with n vertices has $(n-1)$ edges

$$\sum d(v_i) = 2e = 2(n-1)$$

$$n-1 = \frac{1}{2} \sum d(v_i)$$

$$\Rightarrow n-1 = \frac{1}{2} [1 \times p + 2 \times 1 + 3 \times (n-p-1)]$$

$$= \frac{1}{2} [p+2+3n-3p-3]$$

$$\Rightarrow 2n-2 = 3n-2p+1 \Rightarrow 2p = n+1 \Rightarrow p = \frac{n+1}{2}$$

Traversals of Binary Trees

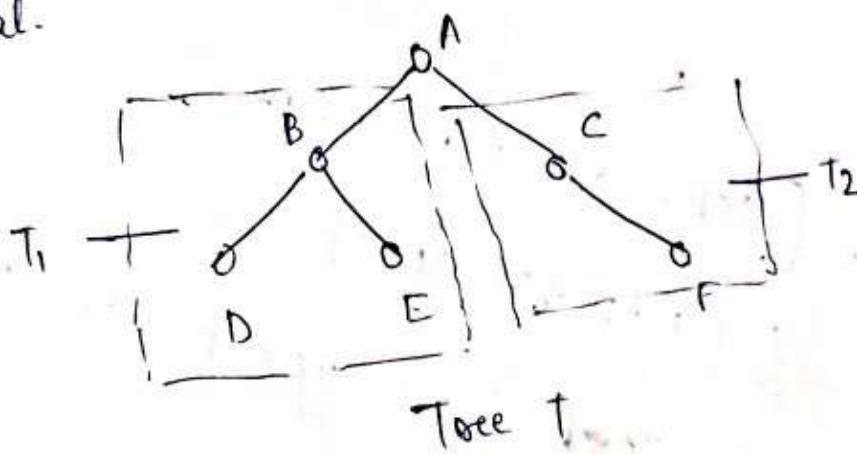
Traversal is nothing but visiting each vertex of the tree in some prescribed order.
i.e. Traversal tree is a process to traverse (walk along) a tree in a systematic manner so that each vertex is visited and processed exactly once.

- There are three methods of Tree Traversal
- (1) Preorder traversal
 - (2) Inorder traversal, and
 - (3) Postorder traversal.

Pre-order traversal

- Visit the root of the tree.
- Pre-order traverse the left subtree.
- Pre-order traverse the right subtree.

Let T_1, T_2, \dots, T_n be the subtrees of the given binary tree T at the root R from left to right. The process of visiting the root R first and traversing T_1 in preorder then T_2 in preorder and so on until T_n is traversed in preorder is called the preorder traversal.



So, the preorder traversal of T visits the root A first and then traverse T_1 and T_2 in preorder. - The preorder traversal of T_1 visits the root B and then D and E in that order. The preorder traversal of T_2 visits the root C and then F . Thus, the preorder traversal of T is ABDEC.

Inorder traversal

- (1) In order traverse the left subtree
- (2) Visit the root of the tree.
- (3) In order traverse the right subtree.

(or)

The process of traversing T_1 first in inorder and then visiting the root R and continuing the traversal of T_2 in inorder, T_3 in inorder etc. until T_n is traversed in inorder is called the inorder traversal.

In the previous tree T;

The inorder traversal of T traverses T_1 in inorder first, then visit the root A and finally traverse T_2 in inorder.

But the inorder traversal of T_1 processes D, B and E in that order and the inorder traversal of T_2 processes C and then F.

Thus, the inorder traversal of T is DBEACF.

Post Order Traversal

- (1) Post order because the left subtree " " right
- (2) " " visit the root of the tree.
- (3) " "

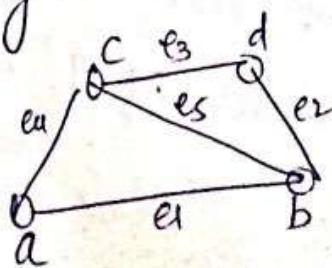
(a) The process of traversing T_1 first in post order and then T_2 in post order, T_3 in post order etc., T_n in post order and finally visiting the root R is called the postorder traversal.

In the previous tree T , the post order traversal of T processes T_1 , then T_2 in post order and finally visits A. But the postorder traversal of T_1 processes D, E, and B in that order and the post order traversal of T_2 processes F and then C. Thus, the post order traversal of T is DEBFCA.

Matching: A matching in a graph is a subset of edges in which no two edges are adjacent.

Note! A single edge in a graph is obviously a matching.

Example:

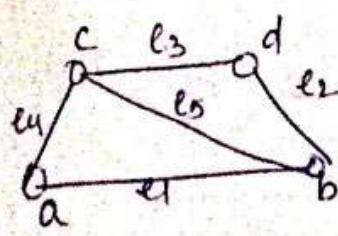


Matchings are $\{e_1\}$, $\{e_2\}$,
 $\{e_3\}$, $\{e_4\}$, $\{e_5\}$, $\{e_1, e_3\}$,
 $\{e_2, e_5\}$.

Maximal Matching:

A matching M of graph G is said to maximal if no other edges of G can be added to M .

Example:



$M_1 = \{e_5\}$,
 $M_2 = \{e_1, e_3\}$,
 $M_3 = \{e_2, e_4\}$
 are the maximal matching of G .

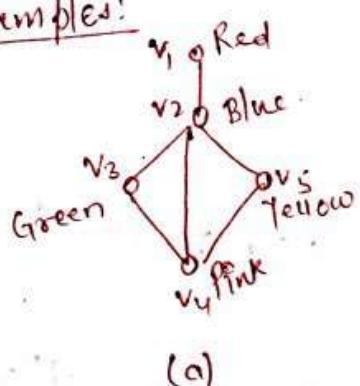
Proper Coloring

Painting all the vertices of a graph with colors such that no two adjacent vertices have the same color is called proper coloring.

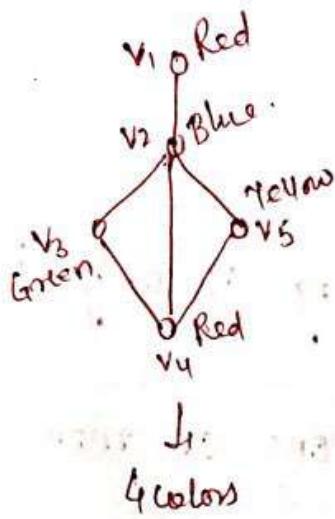
Properly colored graph

A graph in which every vertex has been assigned a color according to a proper coloring is called a properly colored graph.

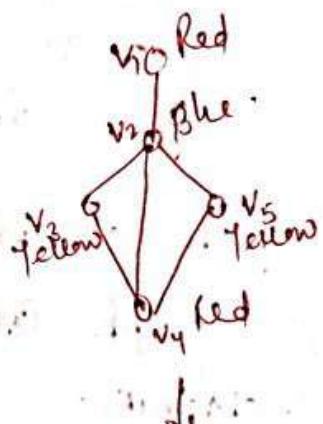
Example:



(a)

Requires
5 colors

4 colors



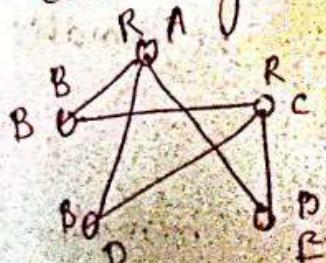
3 colors

Chromatic number

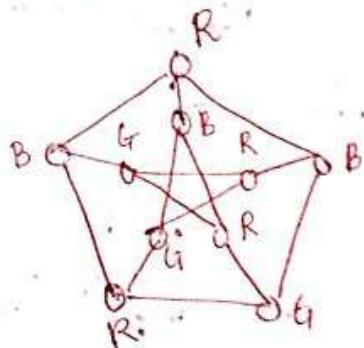
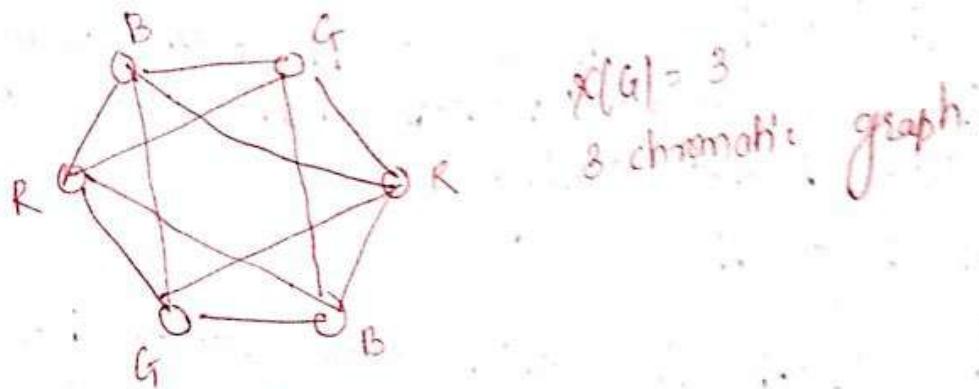
The least number of different colors required for proper coloring of the graph is called Chromatic number of the graph. It is denoted by $\chi(G)$.

Chromatic graph

The graph having chromatic number K is called K -chromatic graph. For example, the above graph is 3-chromatic graph.



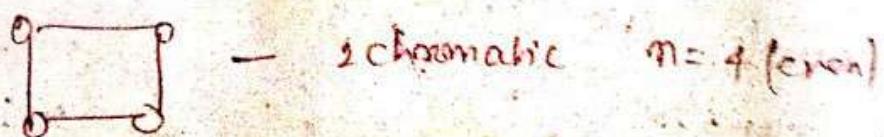
\rightarrow 2-chromatic graph
 $\chi(G) = 2$



Properties / Observations

- (1) A graph consisting of only isolated vertex is 1-chromatic.
- (2) A graph with one or more edges is at least 2-chromatic.
- (3) A complete graph with n -vertices is n -chromatic.
- (4) A graph consisting of simply one circuit with $n \geq 3$ vertices is 2-chromatic if n is even
3-chromatic if n is odd

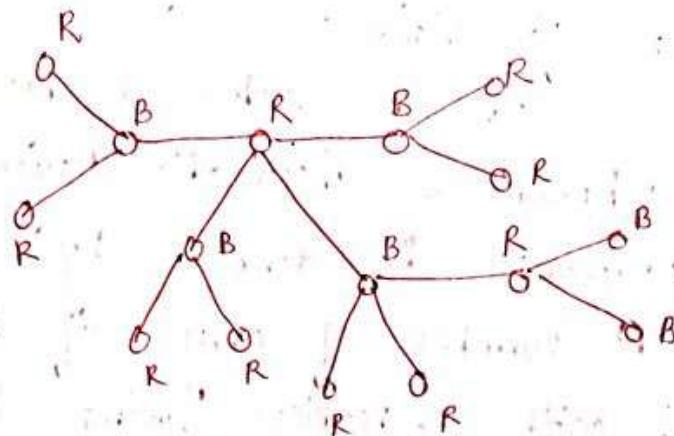
Example:



Theorem:

Every tree with two or more vertices is α -chromatic.
Check whether the converse is true.

Proof:



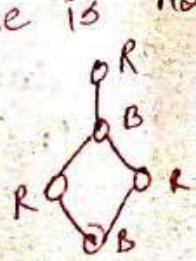
Let T be a tree with root node v . Paint v with color-R. Now, paint all the vertices adjacent to v with color-B. Next, paint the vertices adjacent to these vertices using color-R. Continuing this process till every vertex in T has been painted. Now, in T , we find that all vertices at odd distances from v have color-B, while v and vertices at even distances from v have color-R. Now, along any path in T , the vertices are of alternating colors. Since there is one and only one path between any two vertices in a tree, no two adjacent vertices have same color.

So, T is properly colored with two colors.

Every tree is α -chromatic.

Now, the converse is not true.

For example,



\rightarrow α -chromatic graph
but not a tree.

Thus, every α -chromatic graph may not be a tree.

Chromatic Polynomial

A given graph G of n vertices can be properly colored in many different ways using a sufficient large number of colors.

These ways can be expressed by means of a polynomial known as chromatic polynomial of G . Such a polynomial is denoted by $P_n(\lambda)$ where $P_n(\lambda)$ is the number of ways of proper coloring of a graph with n vertices using λ colors.

Let p_i be the different ways of properly coloring graph G using exactly i colors. Since i colors can be chosen out of λ colors in $\binom{\lambda}{i}$ different ways so, no. of ways of proper coloring of G with exactly i colors out of $\lambda = p_i \binom{\lambda}{i}$ and feasible since $1 \leq i \leq n$ (it is not possible to use more than n colors on n vertices), the chromatic number is the sum of these terms, that is,

$$P_n(\lambda) = \sum_{i=1}^n p_i \binom{\lambda}{i}$$

Chromatic Polynomial of a Complete graph

Number of ways of coloring properly a complete graph with n vertices and λ colors is called a chromatic polynomial of a CG and is given by

$$P_n(\lambda) = \lambda(\lambda-1)(\lambda-2) \dots (\lambda-(n-1))$$

Properties

- (1) Degree of $P_n(\lambda) = n$. i.e. = no. of vertices
- (2) Coefficient of $\lambda^n = 1$ i.e. chromatic polynomial is a monic
- (3) The constant term of $P_n(\lambda)$ is 0.
- (4) The coefficient of $|\lambda^{n-1}|$ is equal to the number of edges in G .
- (5) The coefficient of λ in disconnected graph is always zero.
- (6) If the graph is connected the coefficient of λ is non-zero.

Theorem :- A graph of n vertices is a complete graph if and only if its chromatic polynomial is

$$P_n(\lambda) = \lambda(\lambda-1)(\lambda-2) \dots (\lambda-n+1)$$

Proof: Choose any vertex and paint with colors. The number of ways of different coloring for the selected vertex is λ . Then, choose a second vertex that can be colored properly in exactly $(\lambda-1)$ ways. Similarly, 3rd vertex will have $(\lambda-2)$ ways & n th vertex will have $(\lambda-3)$ ways and so on. n th vertex will be colored in $\lambda-n+1$ ways if and only if every vertex is adjacent to each other i.e. if and only if the graph is complete.

Theorem: An n -vertex graph is a tree if and only if its chromatic polynomial is $P_n(\lambda) = \lambda(\lambda-1)^{n-1} = f(G, \lambda)$

Proof: Let G be a tree.

To Prove: $f(G, \lambda) = P_n(\lambda) = \lambda(\lambda-1)^{n-1}$ by induction on n .

For $n=1$, the result is trivial i.e. $P_1(\lambda) = \lambda$.
Assume the result is true for a tree with almost $(n+1)$ vertices, i.e. $P_{n+1}(\lambda) = \lambda(\lambda-1)^{n-2}$ and e be the

det G be a tree with n vertices
pendant edge of G then
 $P_n(\lambda) = \lambda(\lambda-1)^{n-2} \times (\lambda-1) = P_{n+1}(\lambda) P_1(\lambda)$
 $= \lambda(\lambda-1)^{n-1}$

Conversely, let G be a simple graph with chromatic polynomial $P_n(\lambda) = \lambda(\lambda-1)^{n-1}$

$$= \lambda \left[\lambda^n - (n-1)\lambda^{n-2} + \dots + (-1)^{n-1} \right] \quad \begin{aligned} & \because (\lambda-a)^n \\ & = \lambda^n - n\lambda^{n-1}a + \dots + (-1)^{n-1}na^{n-1} \end{aligned}$$

$$= \lambda^n - (n-1)\lambda^{n-2} + \dots + (-1)^{n-1} \lambda$$

which is a monic polynomial with n vertices (highest degree of one polynomial is one).

Also, the last term $(-1)^{n-1} \lambda$ ensures that G is connected. The next highest degree is $n-1$ & the coefficient of λ^{n-1} is $n-1$ which "gives" the number of edges of the graph $\therefore G$ is a tree.

Theorem:

Let a and b be two non-adjacent vertices in a graph G . Let G' be a graph obtained by adding an edge b/w $a \& b$; let G'' be a graph obtained from G by fusing the vertices a and b together and replacing sets of parallel edges with single edges.

$$\text{Then, } P_n(\lambda) \text{ of } G = P_n(\lambda) \text{ of } G' + P_n(\lambda) \text{ of } G''$$

Proof: The number of ways of properly coloring G .

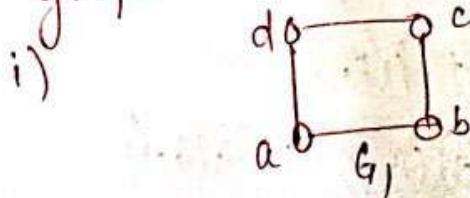
~~can be grouped~~ into two cases.

One, such that vertices a and b are of the same color and the other such that a and b are of different colors.

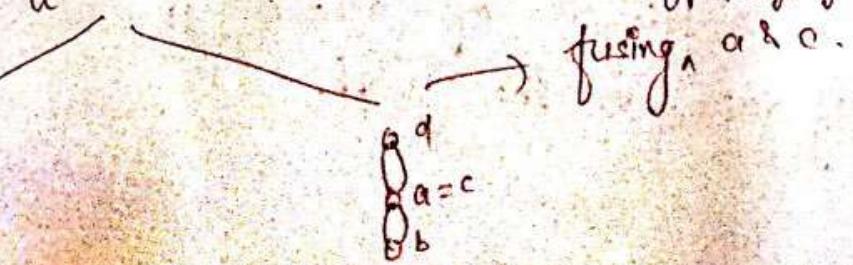
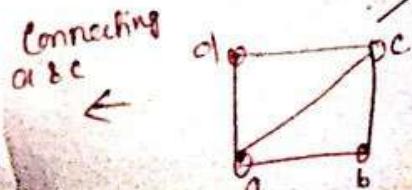
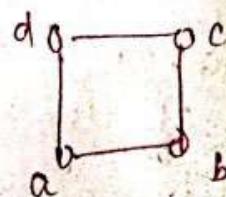
Since the number of ways of properly coloring G such that a and b have different colors = number of ways of properly coloring G' ~~and~~ - the number of ways of properly coloring G such that a and b have same color = no. of ways of properly coloring G''

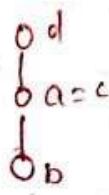
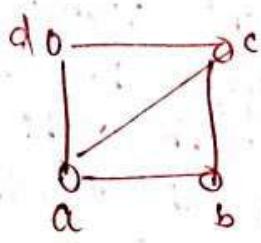
$$P_n(\lambda) \text{ of } G = P_n(\lambda) \text{ of } G' + P_n(\lambda) \text{ of } G''$$

Ques. Find the chromatic polynomial of the given graph.

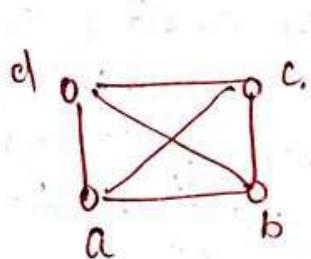
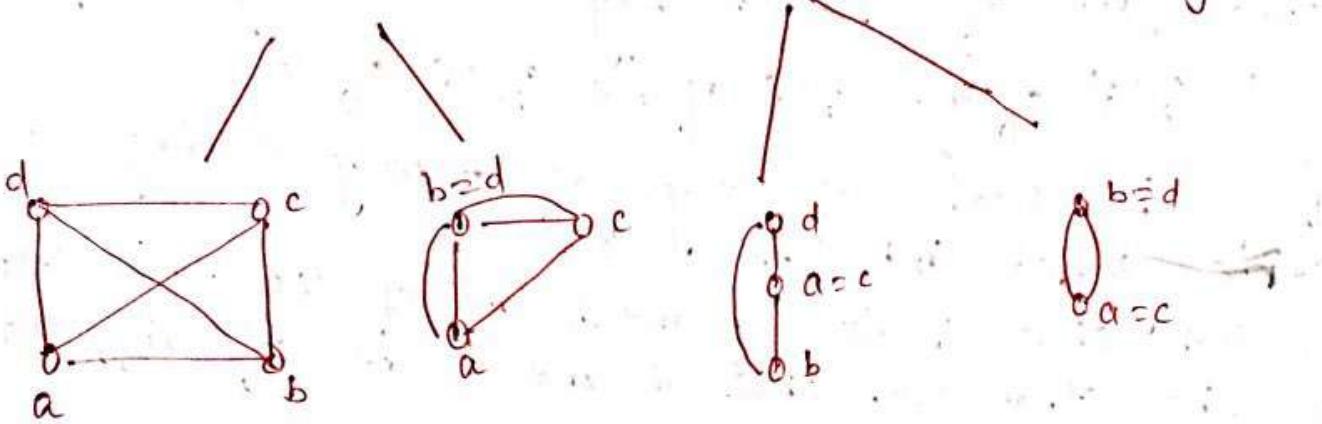


We have,

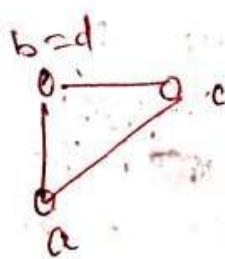




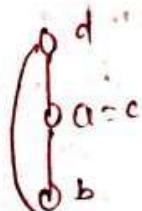
→ deleting multiple edges
and making the previous one a simple graph.



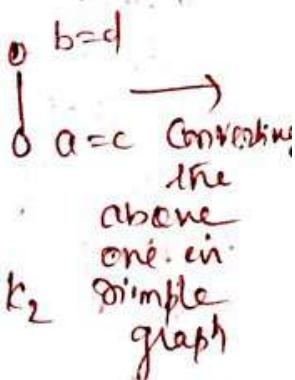
k_4



k_3



k_2



→
Converting
the
above
one. in
simple
graph

Thus, chromatic polynomial

$$= P_4(\lambda) + 2P_3(\lambda) + P_2(\lambda)$$

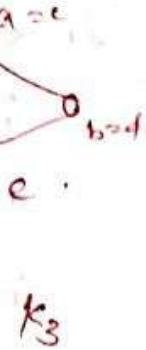
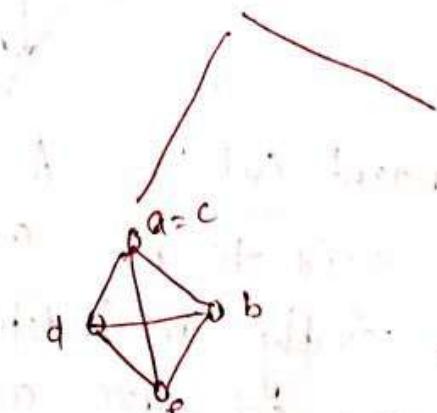
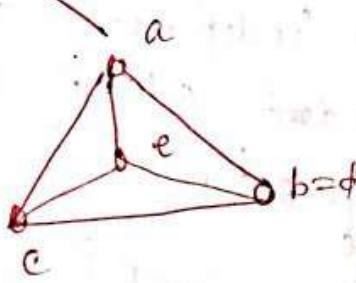
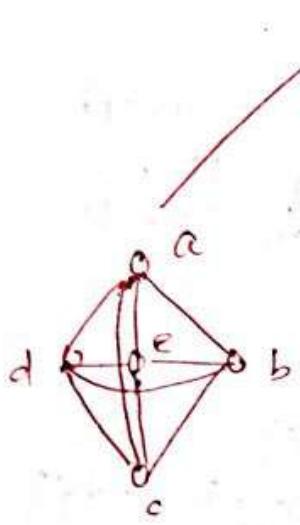
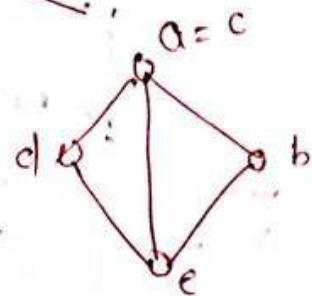
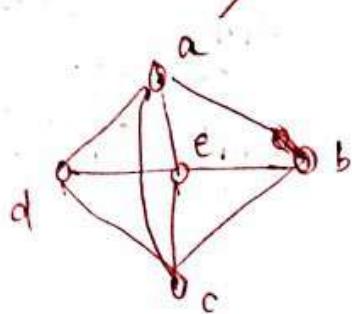
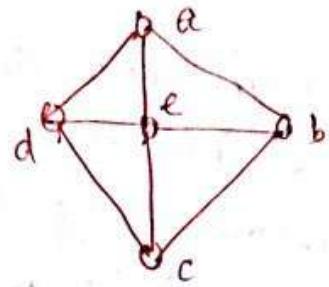
$$= f(k_4, \lambda) + 2f(k_3, \lambda) + f(k_2, \lambda)$$

$$= \lambda(\lambda-1)(\lambda-2)(\lambda-3) + 2\lambda(\lambda-1)(\lambda-2) + \lambda(\lambda-1)$$

$$= \lambda^4 - 4\lambda^3 + 6\lambda^2 - 3\lambda \quad \text{which is a monic polynomial of degree 4.}$$

Also, coefficient of $(\lambda^3) = 4$ that is giving the no. of edges in the graph.

ii)



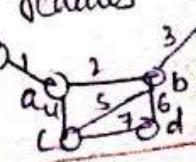
K5

$$\text{Chromatic Polynomial} = P_5(\lambda) + 2P_4(\lambda) + P_3(\lambda)$$

$$= \lambda(\lambda-1)(\lambda-2)(\lambda-3)(\lambda-4) + 2\lambda(\lambda-1)(\lambda-2)(\lambda-3) + \lambda(\lambda-1)(\lambda-2)$$

$$= \lambda(\lambda-1)(\lambda-2)(\lambda^2 - 5\lambda + 7)$$

Fusion: A pair of vertices a, b in a graph are said to be fused (merged or identified) if the two vertices are replaced by a single new vertex such that every edge that was incident on either a or b or on both is incident on the new vertex. Thus, fusion of two vertices does not alter the number of edges; but it reduces the number of vertices by one. For example,

Fusion of vertices
a and b.

Eulerian Path

An open walk of a graph G is called an Eulerian Path, if it includes every edge of G exactly once.

Eulerian Circuit or Cycle

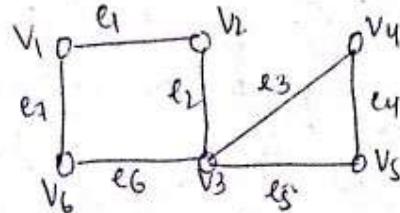
A closed walk of a graph G is called an Eulerian Circuit if it includes every edge of G exactly once.

Eulerian graph

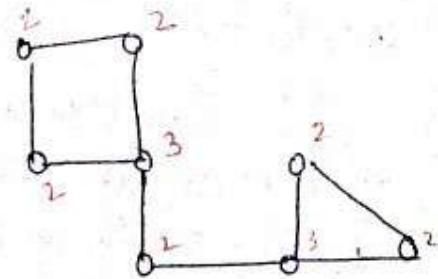
A graph containing an Eulerian circuit is called an Eulerian graph.

Example

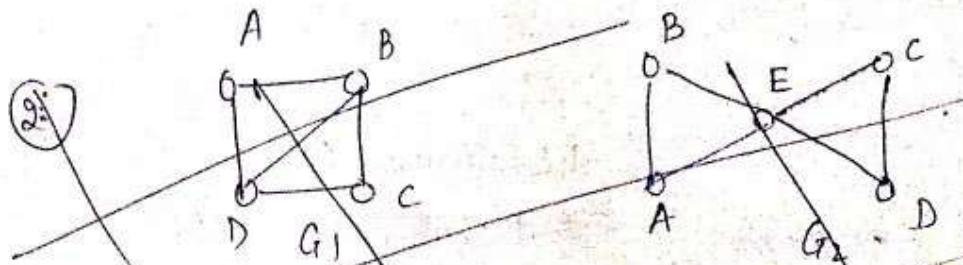
(1)



Eulerian graph



Non-Eulerian graph.



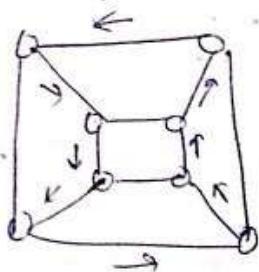
- * Graph G_1 contains an Eulerian path between B and D namely $B-D-C-B-A-D$ since it includes every edge of G exactly once.
- * Graph G_2 contains an Eulerian Circuit namely $A-E-C-D-E-B-A$.

Theorem 1: A connected graph contains Euler circuit or is an Euler graph if and only if all its vertices is of even degree.

Theorem 2: A connected graph contains an Euler path if and only if it has exactly two vertices of odd degree.

Hamiltonian Path and Hamiltonian Circuit

- * An open walk of a graph G is called a Hamiltonian path if it includes every vertex of G exactly once.
- * A Hamiltonian circuit in connected graph G is defined as a closed walk that traverses every vertex of G exactly once, except the starting vertex at which walk terminates.
- * A graph containing a Hamiltonian circuit is called a Hamiltonian graph.

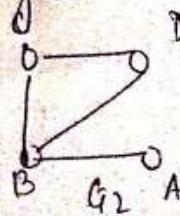
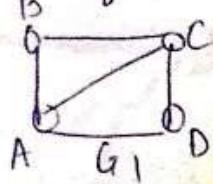


Hamiltonian circuits in
Hamiltonian graphs

Note:

- ① Hamiltonian circuit in a graph of n vertices consists of exactly n edges.

②



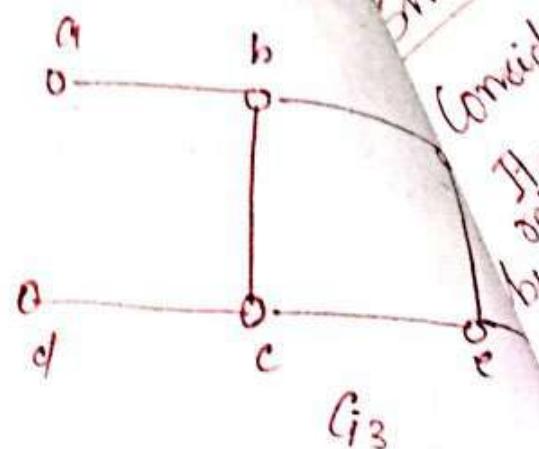
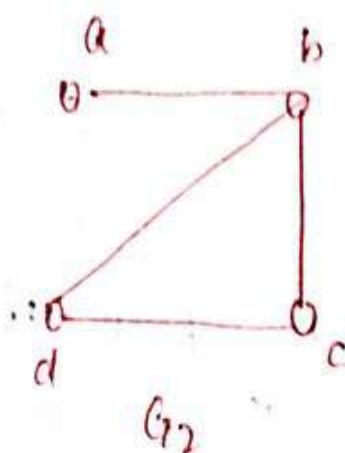
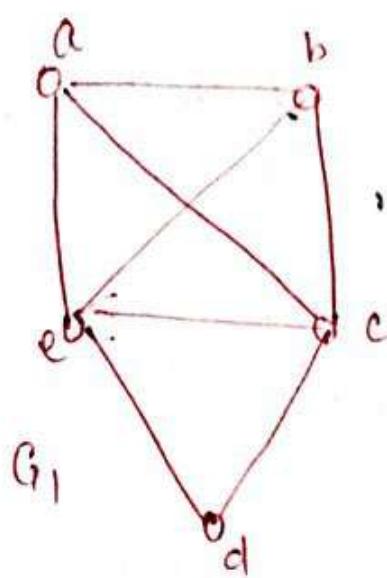
The graph G_1 has a Hamiltonian circuit namely A-B-C-D-A. In this circuit all the vertices appear exactly once.

The graph G_2 has a Hamiltonian path, namely A-B-C-D, but not a Hamiltonian circuit.

Thus, it is clear the path obtained by deleting any one edge from a Hamiltonian circuit is a Hamiltonian path.

- (3) A Hamiltonian circuit contains a Hamiltonian Path but a graph containing a Hamiltonian path need not have a Hamiltonian circuit.
i.e every graph that has a Hamiltonian circuit also has a Hamiltonian Path but there are many graphs with Hamiltonian paths that have no Hamiltonian circuits
- (4) The length of a Hamiltonian path (if it exists) in a connected graph of n vertices is $n-1$.
- (5) A complete graph K_n will always have a Hamiltonian circuit, when $n \geq 3$, due to the fact that an edge exists between any two vertices and a circuit can be formed by beginning at any vertex and by visiting the remaining vertices in any order.
- (6) A given graph may contain more than one Hamiltonian circuit.
- (7) In a complete graph with n vertices there are $\frac{(n-1)!}{2}$ edge-disjoint Hamiltonian circuits if n is an odd number ≥ 3 .

Question: Which of the simple graphs have Hamiltonian circuit or if not, an Hamiltonian



Solution:

(A) G_1 has a Hamiltonian circuit:
 a, b, c, d, e, a ,

(B) There is no Hamiltonian circuit in G_2 (this can be seen by noting that any circuit containing every vertex must contain the edge $\{a,b\}$ twice), but G_2 does have a Hamiltonian path, namely, a, b, c, d .

(C) G_3 has neither a Hamilton circuit nor a Hamiltonian path, because any path containing all vertices must contain one of the edges $\{a,b\}$, $\{e,f\}$, and $\{c,d\}$ more than once.

exactly once? Such a walk is now called an *Euler line*, and a graph that consists of an Euler line is called an *Euler graph*. More formally:

If some closed walk in a graph contains all the edges of the graph, then the walk is called an *Euler line* and the graph an *Euler graph*.

By its very definition a walk is always connected. Since the Euler line (which is a walk) contains all the edges of the graph, an *Euler graph* is always connected, except for any isolated vertices the graph may have. Since isolated vertices do not contribute anything to the understanding of an Euler graph, it is hereafter assumed that Euler graphs do not have any isolated vertices and are therefore connected.

Now we shall state and prove an important theorem, which will enable us to tell immediately whether or not a given graph is an Euler graph.

THEOREM 2-4

A given connected graph G is an Euler graph if and only if all vertices of G are of even degree.

Proof: Suppose that G is an Euler graph. It therefore contains an Euler line (which is a closed walk). In tracing this walk we observe that every time the walk meets a vertex v it goes through two “new” edges incident on v —with one we “entered” v and with the other “exited.” This is true not only of all intermediate vertices of the walk but also of the terminal vertex, because we “exited” and “entered” the same vertex at the beginning and end of the walk, respectively. Thus if G is an Euler graph, the degree of every vertex is even.

To prove the sufficiency of the condition, assume that all vertices of G are of even degree. Now we construct a walk starting at an arbitrary vertex v and going through the edges of G such that no edge is traced more than once. We continue tracing as far as possible. Since every vertex is of even degree, we can exit from every vertex we enter; the tracing cannot stop at any vertex but v . And since v is also of even degree, we shall eventually reach v when the tracing comes to an end. If this closed walk h we just traced includes all the edges of G , G is an Euler graph. If not, we remove from G all the edges in h and obtain a subgraph h' of G formed by the remaining edges. Since both G and h have all their vertices of even degree, the degrees of the vertices of h' are also even. Moreover, h' must touch h at least at one vertex a , because G is connected. Starting from a , we can again construct a new walk in graph h' . Since all the vertices of h' are of even degree, this walk in h' must terminate at vertex a ; but this walk in h' can be combined with h to form a new walk, which starts and ends at vertex v and has

more edges than h . This process can be repeated until we obtain a closed walk that traverses all the edges of G . Thus G is an Euler graph. ■

Königsberg Bridge Problem: Now looking at the graph of the Königsberg bridges (Fig. 1-5), we find that not all its vertices are of even degree. Hence, it is not an Euler graph. Thus it is not possible to walk over each of the seven bridges exactly once and return to the starting point.

One often encounters Euler lines in various puzzles. The problem common to these puzzles is to find how a given picture can be drawn in one continuous line without retracing and without lifting the pencil from the paper. Two such pictures are shown in Fig. 2-12. The drawing in Fig. 2-12(a) is called *Mohammed's scimitars* and is believed to have come from the Arabs. The one in Fig. 2-12(b) is, of course, the *star of David*. (Equal time!)

In defining an Euler line some authors drop the requirement that the walk be closed. For example, the walk $a \rightarrow c \rightarrow 2 \rightarrow d \rightarrow 3 \rightarrow a \rightarrow 4 \rightarrow b \rightarrow 5 \rightarrow d \rightarrow 6 \rightarrow e \rightarrow 7 \rightarrow b$ in Fig. 2-13, which includes all the edges of the graph and does not retrace any edge, is not closed. The initial vertex is a and the final vertex is b . We shall call such an open walk that includes (or traces or covers) all edges of a graph without retracing any edge a *unicursal line* or an *open Euler line*. A (connected) graph that has a unicursal line will be called a *unicursal graph*.

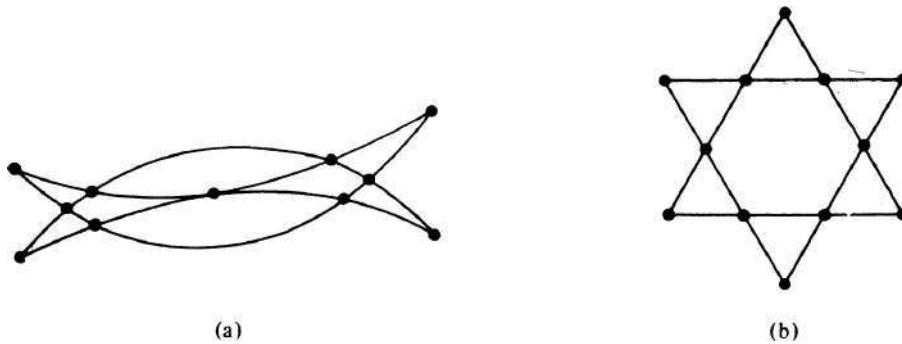


Fig. 2-12 Two Euler graphs.

complete graph G of n vertices. Also the total number of edges in G is $n(n - 1)/2$. See [Problem 1-12](#).

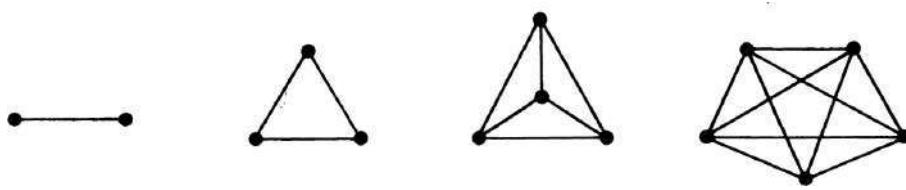


Fig. 2-23 Complete graphs of two, three, four, and five vertices.

It is easy to construct a Hamiltonian circuit in a complete graph of n vertices. Let the vertices be numbered v_1, v_2, \dots, v_n . Since an edge exists between any two vertices, we can start from v_1 and traverse to v_2 , and v_3 , and so on to v_n , and finally from v_n to v_1 . This is a Hamiltonian circuit.

Number of Hamiltonian Circuits in a Graph: A given graph may contain more than one Hamiltonian circuit. Of interest are all the edge-disjoint Hamiltonian circuits in a graph. The determination of the exact number of *edge-disjoint* Hamiltonian circuits (or paths) in a graph in general is also an unsolved problem. However, the number of edge-disjoint Hamiltonian circuits in a complete graph with odd number of vertices is given by [Theorem 2-8](#).

THEOREM 2-8

In a complete graph with n vertices there are $(n - 1)/2$ edge-disjoint Hamiltonian circuits, if n is an odd number ≥ 3 .

Proof: A complete graph G of n vertices has $n(n - 1)/2$ edges, and a Hamiltonian circuit in G consists of n edges. Therefore, the number of edge-disjoint Hamiltonian circuits in G cannot exceed $(n - 1)/2$. That there are $(n - 1)/2$ edge-disjoint Hamiltonian circuits, when n is odd, can be shown as follows:

The subgraph (of a complete graph of n vertices) in [Fig. 2-24](#) is a Hamiltonian circuit. Keeping the vertices fixed on a circle, rotate the polygonal pattern clockwise by $360/(n - 1), 2 \cdot 360/(n - 1), 3 \cdot 360/(n - 1), \dots, (n - 3)/2 \cdot 360/(n - 1)$ degrees. Observe that each rotation produces a Hamiltonian circuit that has no edge in common with any of the previous ones. Thus we have $(n - 3)/2$ new Hamiltonian circuits, all edge disjoint from the one in [Fig. 2-24](#) and also edge disjoint among themselves. Hence the theorem. ■

tree, let us define another term called *eccentricity* (also referred to as *associated number* or *separation*) of a vertex in a graph.

The eccentricity $E(v)$ of a vertex v in a graph G is the distance from v to the vertex farthest from v in G ; that is,

$$E(v) = \max_{v_i \in G} d(v, v_i).$$

A vertex with minimum eccentricity in graph G is called a *center* of G . The eccentricities of the four vertices in Fig. 3-7 are $E(a) = 2$, $E(b) = 1$, $E(c) = 2$, and $E(d) = 2$. Hence vertex b is the center of that tree. On the other hand, consider the tree in Fig. 3-9. The eccentricity of each of its six vertices is shown next to the vertex. This tree has two vertices having the same minimum eccentricity. Hence this tree has two centers. Some authors refer to such centers as *bicenters*; we shall call them just centers, because there will be no occasion for confusion.

The reader can easily verify that a graph, in general, has many centers. For example, in a graph that consists of just a circuit (a polygon), every vertex is a center. In the case of a tree, however, König [1-7] proved the following theorem:

THEOREM 3-9

Every tree has either one or two centers.

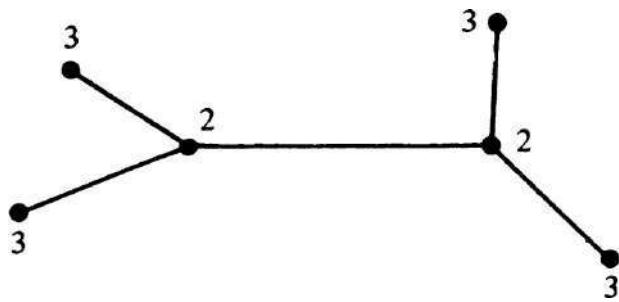
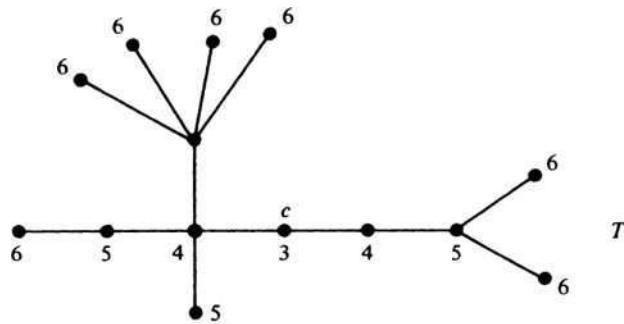
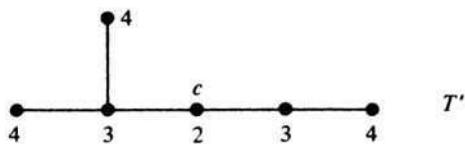


Fig. 3-9 Eccentricities of the vertices of a tree.



(a)



(b)



(c)

\bullet Center
 0

(d)

Fig. 3-10 Finding a center of a tree.

Proof: The maximum distance, $\max d(v, v_i)$, from a given vertex v to any other vertex v_i occurs only when v_i is a pendant vertex. With this observation, let us start with a tree T having more than two vertices. Tree T must have two or more pendant vertices (Theorem 3-7). Delete all the pendant vertices from T . The resulting graph T' is still a tree. What about the eccentricities of the vertices in T' ? A little deliberation will reveal that removal of all pendant vertices from T

uniformly reduced the eccentricities of the remaining vertices (i.e., vertices in T') by one. Therefore, all vertices that T had as centers will still remain centers in T' . From T' we can again remove all pendant vertices and get another tree T'' . We continue this process (which is illustrated in Fig. 3-10) until there is left either a vertex (which is the center of T) or an edge (whose end vertices are the two centers of T). Thus the theorem. ■

COROLLARY

From the argument used in proving Theorem 3-9, we see that if a tree T has two centers, the two centers must be adjacent.

A Sociological Application: Suppose that the communication among a group of 14 persons in a society is represented by the graph in Fig. 3-10(a), where the vertices represent the persons and an edge represents the communication link between its two end vertices. Since the graph is connected, we know that all the members can be reached by any member, either directly or through some other members. But it is also important to note that the graph is a tree—minimally connected. The group cannot afford to lose any of the communication links.

The eccentricity of each vertex, $E(v)$, represents how close v is to the farthest member of the group. In Fig. 3-10(a), vertex c should be the leader of the group, if closeness of communication were the criterion for leadership.

Radius and Diameter: If a tree has a center (or two centers), does it have a radius also? Yes. The eccentricity of a center (which is the distance from the center of the tree to the farthest vertex) in a tree is defined as the *radius* of the tree. For instance, the radius of the tree in Fig. 3-10(a) is three. The *diameter* of a tree T , on the other hand, is defined as the length of the longest path in T . It is left as an exercise for the reader (Problem 3-6) to show that a radius in a tree is not necessarily half its diameter.

3-5. ROOTED AND BINARY TREES

A tree in which one vertex (called the *root*) is distinguished from all the others is called a *rooted tree*. For instance, in Fig. 3-3 vertex N , from where all the mail goes out, is distinguished from the rest of the vertices. Hence N can be considered the root of the tree, and so the tree is rooted. Similarly, in Fig. 3-6 the start vertex may be considered as the root of the tree shown. In a diagram of a rooted tree, the root is generally marked distinctly. We will show the root