SURESH
GYAN VIHAR
UNIVERSITY
Accredited by NAAC with 'A+' Grade

Bachelor of Computer Application

(B.C.A.)

Discrete Mathematiss

Semester-III

Author- Lakshmi Jasti

SURESH GYAN VIHAR UNIVERSITY
Centre for Distance and Online Education
Mahal, Jagatpura, Jaipur-302025

Published by:

S. B. Prakashan Pvt. Ltd.

WZ-6, Lajwanti Garden, New Delhi: 110046

Tel.: (011) 28520627 | Ph.: 9205476295

Email: info@sbprakashan.com | Web.: www.sbprakashan.com

Every effort has been made to avoid errors or omissions in the publication. In spite of this, some errors might have crept in. Any mistake, error or discrepancy noted may be brought to our notice and it shall be taken care of in the next edition. It is notified that neither the publishers nor the author or seller will be responsible for any damage or loss of any kind, in any manner, therefrom.

For binding mistakes, misprints or for missing pages, etc., the publishers' liability is limited to replacement within one month of purchase by similar edition. All expenses in this connection are to be borne by the purchaser.

Designed & Graphic by : S. B. Prakashan Pvt. Ltd.

Printed at :

Syllabus

Discrete Mathematics

Learning Objectives

- The primary objective of the course is that students should learn a particular set of mathematical facts and how to apply them.
- In particular it teaches students how to think logically and mathematically through five important themes: mathematical reasoning, combinatorial analysis, discrete structures, algorithmic thinking, and applications and modeling.
- A successful discrete mathematics course should carefully blend and balance all five themes.

Unit I

Logic: Propositional equivalence, predicates and quantifiers, Methods of proofs, proof strategy, sequences and summation, mathematical induction, recursive definitions and structural induction, program correctness. Counting: The basics of counting, the pigeonhole principle, permutations and combinations, recurrence relations, solving recurrence relations, generating functions, inclusion-exclusion principle, application of inclusion-exclusion.

Unit II

Relations: Relations and their properties, n-array relations and their applications, representing relations, closure of relations, equivalence of relations, partial orderings. Graph theory: Introduction to graphs, graph terminology, representing graphs and graph isomorphism, connectivity, Euler and Hamilton paths, planar graphs, graph coloring, introduction to trees, application of trees.

Unit III

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

Unit IV

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

References

- K.H. Rosen: Discrete Mathematics and its application, 5th edition, Tata McGraw Hill.Chapter
- C. L. Liu: Elements of Discrete Mathematics, 2nd edition, TMH 2000.
- B.Kalman: Discrete Mathematical Structure, 3rd edition,

- “Discrete Mathematical Structures”: Tremblay and Manohar, Tata McGraw Hill
- “Discrete Mathematics”: 1 st edition by Maggard Thomson
- “Discrete Mathematics ”: Semyour Lipschutz, Varsha Patil IInd Edition Schaum’s Series, TMH
- “Discrete Mathematical Structures”: Kolman, Busby and Ross, Prentice Hall India, Edition 3

Contents

* * *

1 Mathematical Logic

I. Introduction

The rules of LOGIC give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments. LOGIC has numerous applications in Computer Science. These rules are used in the design of computer circuits, the construction of computer programs, the verification of the correctness of programs and in many other ways.

Propositions

A proposition is a declarative sentence that is either True or False, but not both.

Example

All the following declarative sentences are propositions:

1. Delhi, is the capital of India.
2. $5 + 3 = 7$
3. The earth is round.

Proposition 1 and 3 are True, where as 2 is False.

Example

Consider the following sentence:

1. Do you speak English?
2. Read this carefully.
3. $x + 1 = 2$
4. $3 - x = 1$

Sentences 1 and 2 are not propositions because they are not declarative sentences.

1 is a question, 2 is a command, 3 and 4 are declarative sentences, since it is True or False depending on the value of x.

The area of logic that deals with propositions is called the **Propositional Calculus** or **Propositional Logic**. Letters are used to denote variables and propositions. In logic, the letters p, q, r, s, … denote propositional variables. Many mathematical statements are constructed by combining one or more propositions. New propositions, called **Compound Propositions**, are formed from existing propositions using Logical Operators.

2. Connectives

Negations

Let p be a proposition. The statement "It is not the case that p" is another proposition, called the **Negation** of p. The negation of p is denoted by $\neg p$ or ~p. The proposition $\neg p$ is read "not p".

Example

1. **Find the negation of the proposition "Today is Sunday" and express this in simple English.**

Solution

The negation is "It is not the case that today is Sunday" or "Today is not Sunday" or "It is not Sunday today".

The truth value of a proposition is True, denoted by T, if it is a True proposition and False, denoted by F, if it is a False proposition. Giving the truth values of a compound statement in terms of its component parts, is called a **Truth Table**.

Truth table for the negation of a proposition

P	$\neg$P
T	F
F	T

The logical operators that are used to form new propositions from two or more existing propositions. These logical operators are also called **connectives**.

Conjunction

Let P and Q be propositions. The propositions "P and Q" denoted by $P \wedge Q$, is the proposition that is True when P and Q are both True and is False otherwise. The proposition $P \wedge Q$ is called the Conjunction of P and Q.

Truth table for the conjuction of two proposition

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

Disjunction

Let P and Q be propositions. The proposition "P or Q" denoted by $P \vee Q$, is the proposition that is False when P and Q are both False and is True otherwise. The proposition $P \vee Q$ is called the **Disjunction** of P and Q.

Truth table for the disjunction of two propositions

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

Exclusive Or

Let P and Q be propositions. The Exclusive Or of P and Q, denoted by $P \oplus Q$, is the proposition that is True when exactly one of P and Q is True and is False otherwise.

Truth table for the Exclusive Or of two proposition

P	Q	$P \oplus Q$ or $P \bar{\vee} Q$
T	T	F
T	F	T
F	T	T
F	F	F

Examples

1. Using the following statements:

p: Ayush is rich
q: Ayush is happy
Write the following statements in symbolic form:

i. Ayush is rich but unhappy
ii. Ayush is poor but happy
iii. Ayush is neither rich nor happy
iv. Ayush is poor or he is both rich and unhappy.

1
PU
Oct. 2009 – *6M*

Solution

i. Ayush is rich but unhappy: $p \wedge \sim q$

ii. Ayush is poor but happy: $\sim p \wedge q$

iii. Ayush is neither rich nor happy: $\sim p \wedge \sim q$

iv. Ayush is poor or he is both rich and unhappy: $\sim p \vee (p \wedge \sim q)$.

2. Construct the truth table for the following formulas:

i. $\neg(\neg P \vee \neg Q)$

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

iii. $P \wedge (P \vee Q)$

iv. $P \wedge (Q \wedge P)$

v. $(P \wedge Q) \vee (\neg P \wedge Q) \ \vee \ (P \wedge \neg Q) \vee (\neg P \wedge \neg Q)$

vi. $(\neg P \wedge (\neg Q \wedge R)) \ \vee \ (Q \wedge R) \vee (P \wedge R)$

Solution

i. $\neg(\neg P \vee \neg Q)$

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$\neg(\neg P \vee \neg Q)$
T	T	F	F	F	T
T	F	F	T	T	F
F	T	T	F	T	F
F	F	T	T	T	F

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

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

iii. $P \wedge (P \vee Q)$

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

iv. $P \wedge (Q \wedge P)$

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

v. $\overbrace{(P \wedge Q) \vee (\neg P \wedge Q)}^{A} \vee \overbrace{(P \wedge \neg Q) \vee (\neg P \wedge \neg Q)}^{B}$

P	Q	$P \wedge Q$	$\neg P$	$\neg P \wedge Q$	A	$\neg Q$	$P \wedge \neg Q$	$\neg P \wedge \neg Q$	B	$A \vee B$
T	T	T	F	F	T	F	F	F	F	T
T	F	F	F	F	F	T	T	F	T	T
F	T	F	T	T	T	F	F	F	F	T
F	F	F	T	F	F	T	F	T	T	T

vi. $\overbrace{(\neg P \wedge (\neg Q \wedge R))}^{A} \vee \overbrace{(Q \wedge R) \vee (P \wedge R)}^{B}$

P	Q	R	$\neg P$	$\neg Q$	$\neg Q \wedge R$	$\neg P \wedge (\neg Q \wedge R)$ or A	$Q \wedge R$	$P \wedge R$	B	$A \vee B$
T	T	T	F	F	F	F	T	T	T	T
T	T	F	F	F	F	F	F	F	F	F
T	F	T	F	T	T	F	F	T	T	T
T	F	F	F	T	F	F	F	F	F	F
F	T	T	T	F	F	F	T	F	T	T
F	T	F	T	F	F	F	F	F	F	F
F	F	T	T	T	T	T	F	F	F	T
F	F	F	T	T	F	F	F	F	F	F

Note: We have 3 variables and the values can be computed as:
Base [K] = 2^{n-k}; k = 1, 2, 3; n = 3
Base [1] = $2^{3-1} = 2^2 = 4$ (4 times True)
Base [2] = $2^{3-2} = 2^1 = 2$ (2 times True)
Base [3] = $2^{3-3} = 2^0 = 1$ (1 time True)

3. Given the truth values of P and Q as T and those of R and S as F, find the truth values of the following:

a. $P \vee (Q \wedge R)$

b. $(P \wedge (Q \wedge R)) \vee \neg((P \vee Q) \wedge (R \vee S))$

c. $(\neg(P \wedge Q) \vee \neg R) \vee (((\neg P \wedge Q) \vee \neg R) \wedge S)$

Solution

a. $P \vee (Q \wedge R)$

$T \vee (T \wedge F)$

$T \vee F$

T

b. $(P \wedge (Q \wedge R)) \vee \neg((P \vee Q) \wedge (R \vee S))$

$(T \wedge (T \wedge F)) \vee \neg((T \vee T) \wedge (F \vee F))$

$(T \wedge F) \vee \neg(T \wedge F)$

$F \vee \neg F$

$F \vee T$

T

c. $(\neg(P \wedge Q) \vee \neg R) \vee (((\neg P \wedge Q) \vee \neg R) \wedge S)$

$(\neg(T \wedge T) \vee \neg F) \vee (((\neg T \wedge T) \vee \neg F) \wedge F)$

$(\neg(T) \vee T) \vee ((F \wedge T) \vee T) \wedge F)$

$(F \vee T) \vee ((F \vee T) \wedge F)$

$T \vee (T \wedge F)$

$T \vee F$

T

3. Implications

Conditional

If P and Q are any two statements, then the statement P → Q which is read as "If P, then Q" is called a **Conditional Statement**. The statement P → Q has a truth value F when Q has the truth value F and P the truth value T; otherwise it has the truth value T.

The statement P is called the antecedent and Q the consequent in P → Q.

Truth table for conditional

P	Q	P → Q
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional

Let P and Q be propositions. The biconditional $P \rightleftarrows Q$ is the proposition that is True when P and Q have the same truth values and is False otherwise.

Truth table for biconditional

P	Q	$P \rightleftarrows Q$
T	T	T
T	F	F
F	T	F
F	F	T

Examples

1. Construct the truth tables for the following:

$\neg(P \leftrightarrow (Q \to (R \vee P)))$

1

PU
Oct. 2008 – *8M*

Solution

P	Q	R	$R \vee P$	$Q \to (R \vee P)$	$P \leftrightarrow (Q \to (R \vee P))$(A)	$\neg A$
T	T	T	T	T	T	F
T	T	F	T	T	T	F
T	F	T	T	T	T	F
T	F	F	T	T	T	F
F	T	T	T	T	F	T
F	T	F	F	F	F	T
F	F	T	T	T	F	T
F	F	F	F	T	F	T

2. Show that the truth values of the following formulas are independent of their components.

i. $(P \wedge (P \to Q)) \to Q$

ii. $P \to Q$ is equivalent to $\neg P \vee Q$

iii. $(P \rightleftarrows Q) \rightleftarrows (P \wedge Q) \vee (\neg P \wedge \neg Q)$

iv. $((P \to Q) \wedge (Q \to R)) \to (P \to R)$

Solution

i. $(P \wedge (P \to Q)) \to Q$

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

ii. $P \to Q$ is equivalent to $\neg P \vee Q$

$(P \to Q) \rightleftarrows (\neg P \vee Q)$

P	Q	$\neg P$	$P \to Q$	$\neg P \vee Q$	$(P \to Q) \rightleftarrows (\neg P \vee Q)$
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

iii. $(P \rightleftarrows Q) \rightleftarrows \overbrace{(P \wedge Q) \vee (\rceil P \wedge \rceil Q)}^{A})$

P	Q	$P \rightleftarrows Q$	$P \wedge Q$	$\rceil P \wedge \rceil Q$	A	$(P \rightleftarrows Q) \rightleftarrows A$
T	T	T	T	F	T	T
T	F	F	F	F	F	T
F	T	F	F	F	F	T
F	F	T	F	T	T	T

iv. $(\underbrace{(P \rightarrow Q) \wedge (Q \rightarrow R)}_{A}) \rightarrow \underbrace{(P \rightarrow R)}_{B}$

P	Q	R	$P \rightarrow Q$	$Q \rightarrow R$	$P \rightarrow R$	A	$A \rightarrow B$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	T	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

3. **Construct the truth tables of the following formulas:**

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

ii. $\rceil(P \vee (Q \wedge R)) \rightleftarrows ((P \vee Q) \wedge (P \vee R))$

iii. $\rceil(P \wedge Q) \rightleftarrows (\rceil P \vee \rceil Q)$

Solution

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

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

ii. $\overbrace{\neg(P \vee (Q \wedge R))}^{A} \rightleftarrows \overbrace{((P \vee Q) \wedge (P \vee R))}^{B}$

P	Q	R	$Q \wedge R$	$\overbrace{\neg(P \vee (Q \wedge R))}$	$P \vee Q$	$P \vee R$	B	$A \rightleftarrows B$
T	T	T	T	F	T	T	T	F
T	T	F	F	F	T	T	T	F
T	F	T	F	F	T	T	T	F
T	F	F	F	F	T	T	T	F
F	T	T	T	F	T	T	T	F
F	T	F	F	T	T	F	F	F
F	F	T	F	T	F	T	F	F
F	F	F	F	T	F	F	F	F

$P \leftrightarrows Q$ is equivalent to $(P \to Q) \wedge (Q \to P)$

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

iii. $\overbrace{\neg(P \wedge Q)}^{A} \rightleftarrows \overbrace{(\neg P \vee \neg Q)}^{B}$

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$A \rightleftarrows B$
T	T	T	F	F	F	F	T
T	F	F	T	F	T	T	T
F	T	F	T	T	F	T	T
F	F	F	T	T	T	T	T

4. Propositional equivalences

Tautology

A compound proposition that is always True, no matter what the truth values of the proposition that occur in it, is called a **Tautology**.

Contradiction

A compound proposition that is always False is called a **Contradiction**.

Contingency

A proposition that is neither a tautology nor a contradiction is called a **Contingency**.

Examples

1. Indicate which ones are tautology or contradictions.

i. $(P \to (P \vee Q)$ ii. $((P \to (\neg P)) \to \neg P)$

iii. $((\neg Q \wedge P) \wedge Q)$ iv. $(\neg P \to Q) \to (Q \to P)$

v. $((P \wedge Q) \rightleftarrows P)$ vi. $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$

Solution

i. $(P \to (P \vee Q)$

P	Q	P ∨ Q	P → (P ∨ Q)
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Tautology

ii. $((P \to (\neg P)) \to \neg P)$

P	¬P	P → ¬P	((P → (¬P) → ¬P)
T	F	F	T
F	T	T	T

Tautology

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

P	Q	¬Q ∧ P	((¬Q ∧ P) ∧ Q)
T	T	F	F
T	F	T	F
F	T	F	F
F	F	F	F

Contradiction

iv. $\overbrace{(\neg P \to Q)}^{A} \to \overbrace{(Q \to P)}^{B}$

P	Q	¬P → Q	Q → P	A → B
T	T	T	T	T
T	F	T	T	T
F	T	T	F	F
F	F	F	T	T

Contingency

v. $((P \wedge Q) \rightleftarrows P)$

P	Q	P ∧ Q	(P ∧ Q) ⇄ P
T	T	T	T
T	F	F	F
F	T	F	T
F	F	F	T

Contingency

vi. $\overbrace{(P \rightarrow (Q \rightarrow R))}^{A} \rightarrow \overbrace{((P \rightarrow Q) \rightarrow (P \rightarrow R))}^{B}$

P	Q	R	Q → R	(P → (Q → R))	P → Q	P → R	B	A → B
T	T	T	T	T	T	T	T	T
T	T	F	F	F	T	F	F	T
T	F	T	T	T	F	T	T	T
T	F	F	T	T	F	F	T	T
F	T	T	T	T	T	T	T	T
F	T	F	F	T	T	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	T	T	T	T

2. Determine which is tautology or a fallacy:

i. $p \Rightarrow q \wedge q \Rightarrow p$ **ii.** $(p \wedge q) \wedge (p \vee q)$

PU
Oct. 2010 – 5M
1

Solution

i. $p \Rightarrow q \wedge q \Rightarrow p$

p	q	p ⇒ q	q ⇒ p	p ⇒ q ∧ q ⇒ p
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

∴ $p \Rightarrow q \wedge q \Rightarrow p$ is neither tautology nor a fallacy, it is contingent.

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

p	q	p ∧ q	p ∨ q	(p ∧ q) ∧ (p ∨ q)
T	T	T	T	T
T	F	F	T	F
F	T	F	T	F
F	F	F	F	F

Equivalence of Formulas

$P \rightleftarrows Q$ is True whenever both P and Q have the same truth values. Therefore the statement formulas A and B are equivalent provided $A \rightleftarrows B$ is a tautology and conversely, if $A \rightleftarrows B$ is a tautology then A and B are equivalent. We shall represent the equivalence of two formulas $A \Leftrightarrow B$.

▶ Prove $(P \to Q) \Leftrightarrow (\neg P \vee Q)$

P	Q	$P \to Q$	$\neg P \vee Q$	$(P \to Q) \rightleftarrows (\neg P \vee Q)$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

Equivalences

E_1	$\neg\neg P \Leftrightarrow P$	(Double negation)
E_2	$P \wedge Q \Leftrightarrow Q \wedge P$	Commutative laws
E_3	$P \vee Q \Leftrightarrow Q \vee P$	
E_4	$(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$	Associative laws
E_5	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$	
E_6	$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$	Distributive laws
E_7	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	
E_8	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$	De Morgan's law
E_9	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	
E_{10}	$P \vee P \Leftrightarrow P$	Idempotent laws
E_{11}	$P \wedge P \Leftrightarrow P$	
E_{12}	$R \vee (P \wedge \neg P) \Leftrightarrow R$	
E_{13}	$R \wedge (P \vee \neg P) \Leftrightarrow R$	
E_{14}	$R \vee (P \vee \neg P) \Leftrightarrow T$	
E_{15}	$R \wedge (P \wedge \neg P) \Leftrightarrow F$	
E_{16}	$P \to Q \Leftrightarrow \neg P \vee Q$	
E_{17}	$\neg(P \to Q) \Leftrightarrow P \wedge \neg Q$	
E_{18}	$P \to Q \Leftrightarrow \neg Q \to \neg P$	
E_{19}	$P \to (Q \to R) \Leftrightarrow (P \wedge Q) \to \neg R$	
E_{20}	$\neg(P \rightleftarrows Q) \Leftrightarrow P \rightleftarrows \neg Q$	
E_{21}	$P \rightleftarrows Q \Leftrightarrow (P \to Q) \wedge (Q \to P)$	
E_{22}	$(P \rightleftarrows Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$	

Special valid formulas involving quantifiers

E_{23} $(\exists x)\,(A(x) \vee B(x)) \Leftrightarrow (\exists x)\,A(x) \vee (\exists x)\,(B(x)$

E_{24} $(x)\,(A(x) \wedge B(x)) \Leftrightarrow (x)\,A(x) \wedge (x)\,B(x)$

E_{25} $\neg(\exists x)\,A(x) \Leftrightarrow (x)\,\neg A(x)$

E_{26} $\neg(x)\,A(x) \Leftrightarrow (\exists x)\,\neg A(x)$

E_{27} $(x)\,(A \vee B(x)) \Leftrightarrow A \vee (x)\,B(x)$

E_{28} $(\exists x)\,(A \wedge B(x)) \Leftrightarrow A \wedge (\exists x)\,B(x)$

E_{29} $(x)\,A(x) \rightarrow B \Leftrightarrow (\exists x)\,(A(x) \rightarrow B)$

E_{30} $(\exists x)\,A(x) \rightarrow B \Leftrightarrow (x)\,(A(x) \rightarrow B)$

E_{31} $A \rightarrow (x)\,B(x) \Leftrightarrow (x)\,(A \rightarrow B(x))$

E_{32} $A \rightarrow (\exists x)\,B(x) \Leftrightarrow (\exists x)\,(A \rightarrow B(x))$

Using E_{23}, we can prove

E_{33} $(\exists x)\,(A(x) \rightarrow B(x)) \Leftrightarrow (x)\,A(x) \rightarrow (\exists x)\,B(x)$

From I_{15} and I_{16} we can prove

E_{34} $(\exists x)\,A(x) \rightarrow (x)\,B(x) \Leftrightarrow (x)\,(A(x) \rightarrow B(x))$

Examples

1. Show that $P \rightarrow (Q \rightarrow R) \Leftrightarrow P \rightarrow (\neg Q \vee R) \Leftrightarrow (P \wedge Q) \rightarrow R$

Solution

L.H.S: $\neg P \vee (\neg Q \vee R) \Leftrightarrow (\neg P \vee \neg Q) \vee R$ (∵ Associative law)

$\Leftrightarrow \neg(P \wedge Q) \vee R$ (∵ De Morgan's law)

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

2. Show that $(\neg P \wedge (\neg Q \wedge R)) \vee (Q \wedge R) \vee (P \wedge R) \Leftrightarrow R$

Solution

L.H.S.: $(\neg P \wedge (\neg Q \wedge R)) \vee ((Q \vee P) \wedge R)$ (∵ Distributive law)

$((\neg P \wedge \neg Q) \wedge R) \vee ((Q \vee P) \wedge R)$ (∵ Associative law)

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

$(\underbrace{\neg(P \vee Q) \vee (P \vee Q)}_{T})\ \wedge\ R$ (∵ De Morgan's of commutative)

$T\ \wedge\ R$ (∵ $P \vee \neg P \Leftrightarrow T$)

R (∵ $P \wedge T \Leftrightarrow P$)

3. Show that $((P \vee Q) \wedge \neg(\neg P \wedge (\neg Q \vee \neg R))) \vee (\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)$ is a tautology.

Solution

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

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

$((P \vee Q) \wedge (P \vee R)) \vee \neg((P \vee Q) \wedge (P \vee R))$ $(\because P \wedge P \Leftrightarrow P)$

$\underbrace{(P \vee Q) \vee \neg(P \vee Q)}_{T} \wedge \underbrace{(P \vee R) \vee \neg(P \vee R)}_{T}$

$T \wedge T$ $\because P \vee \neg P \Leftrightarrow T$

T

4. $\neg(P \wedge Q) \rightarrow (\neg P \vee (\neg P \vee Q)) \Leftrightarrow (\neg P \vee Q)$

Solution

L.H.S.: $(P \wedge Q) \vee ((\neg P \vee \neg P) \vee Q)$ $(\because$ Commutative law)

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

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

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

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

$Q \vee Q \vee \neg P$

$\neg P \vee Q$

5. $(P \vee Q) \wedge (\neg P \wedge (\neg P \wedge Q)) \Leftrightarrow (\neg P \wedge Q)$

Solution

L.H.S.: $(P \vee Q) \wedge (\neg P \wedge \neg P) \wedge Q$

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

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

$F \vee Q \wedge \neg P$

$\neg P \wedge Q$

Show the following equivalence:

$P \to (Q \vee R) \Leftrightarrow (P \to Q) \vee (P \to R)$.

1

PU
Oct. 2008 – *5M*

olution

P	Q	R	P → Q	P → R	Q ∨ R	P → (Q∨R)	(P → (P →R)
T	T	T	T	T	T	T	T
T	T	F	T	F	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	F	F	F	F
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	F	T	T

lence $P \to (Q \vee R) \Leftrightarrow (P \to Q) \vee (P \to R)$.

Prove that $p \to (q \to r)$ and $(p \wedge \overline{r}) \to \overline{q}$ are logically equivalent.

1

PU
Oct. 2009 – *5M*

olution

LHS $= p \to (q \to r)$

$\Leftrightarrow \sim p \vee (q \to r)$

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

$\Leftrightarrow \sim p \vee \sim q \vee r$ ....(1)

RHS $= (p \wedge \overline{r}) \to \overline{q}$

$\Leftrightarrow (p \wedge \sim r) \to \sim q$

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

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

$\Leftrightarrow \sim p \vee r \vee \sim q$ **(Double negation)**

$\Leftrightarrow \sim p \vee \sim q \vee r$ **Associativity** ....(2)

rom (1) and (2),

$$p \to (q \to r) \equiv (p \wedge \overline{r}) \to \overline{q}$$

Show that the following statements are equivalent.

$A \to (B \vee C) \Leftrightarrow (A \wedge \sim B) \to C$

1

PU
Oct. 2010 – *5M*

olution

Consider LHS $= A \to (B \vee C)$

$\equiv \sim A \vee (B \vee C)$ (E_{16})

$\equiv \sim A \vee B \vee C$ (E_5 Associative law) ....(1)

Now RHS $= (A \wedge \sim B) \rightarrow C$

$\equiv \sim (A \wedge \sim B) \vee C$ (E_{16})

$\equiv (\sim A \vee \sim(\sim B)) \vee C$ (De Morgan's Law)

$\equiv (\sim A \vee B) \vee C$ (Double negation)

$\equiv \sim A \vee B \vee C$ (E_5 Associative law) ....(2)

From (1) and (2), it follows that

$$A \rightarrow (B \vee C) \Leftrightarrow (A \wedge \sim B) \rightarrow C$$

5. Tautological Implications

A statement A is said to be tautologically imply a statement B if and only if $A \rightarrow B$ is a tautology. $A \Rightarrow B$ states that $A \rightarrow B$ is a tautology or A tautologically implies B.

Implications

I_1 $P \wedge Q \Rightarrow P$ } Simplification

I_2 $P \wedge Q \Rightarrow Q$

I_3 $P \Rightarrow P \vee Q$ } Addition

I_4 $Q \Rightarrow P \vee Q$

I_5 $\neg P \Rightarrow P \rightarrow Q$

I_6 $Q \Rightarrow P \rightarrow Q$

I_7 $\neg(P \rightarrow Q) \Rightarrow P$

I_8 $\neg(P \rightarrow Q) \Rightarrow \neg Q$

I_9 $P, Q \Rightarrow P \wedge Q$

I_{10} $\neg P, P \vee Q \Rightarrow Q$ Disjunctive Syllogism

I_{11} $P, P \rightarrow Q \Rightarrow Q$ Modus Ponens

I_{12} $\neg Q, P \rightarrow Q \Rightarrow \neg P$ Modus Tollens

I_{13} $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$ Hypothetical Syllogism

I_{14} $P \vee Q, P \rightarrow R, Q \rightarrow R \Rightarrow R$ Dilemma

Special valid formulas involving quantifiers

I_{15} $(x)\, A(x) \vee (x)\, B(x) \Rightarrow (x)\, (A(x) \vee B(x))$

I_{16} $(\exists x)\, (A(x) \wedge B(x)) \Rightarrow (\exists x)\, A(x) \wedge (\exists x)\, B(x)$

Examples

1. **Show the following implications**

i. **$(P \wedge Q) \Rightarrow (P \rightarrow Q)$** ii. **$P \Rightarrow (Q \rightarrow P)$**

iii. **$(P \rightarrow (Q \rightarrow R)) \Rightarrow (P \rightarrow Q) \rightarrow (P \rightarrow R)$**

Solution

i. **$(P \wedge Q) \Rightarrow (P \rightarrow Q)$**

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

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

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

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

$\neg P \vee T$

T

ii. **$P \Rightarrow (Q \rightarrow P)$**

$P \rightarrow (\neg Q \vee P)$

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

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

$T \vee \neg Q$

T

iii. **$(P \rightarrow (Q \rightarrow R)) \Rightarrow (P \rightarrow Q) \rightarrow (P \rightarrow R)$**

$(\neg P \vee (\neg Q \vee R)) \rightarrow (\neg P \vee Q) \rightarrow (\neg P \vee R)$

$(\neg P \vee (\neg Q \vee R)) \rightarrow (\neg(\neg P \vee Q)) \vee (\neg P \vee R)$

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

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

$(P \wedge Q \wedge \neg R) \vee ((T \vee R) \wedge (\neg P \vee \neg Q \vee R))$

$(P \wedge Q \wedge \neg R) \vee (T \wedge(\neg P \vee \neg Q \vee R))$

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

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

$(T \vee \neg Q \vee R) \wedge (T \vee \neg P \vee R) \wedge (T \vee \neg P \vee \neg Q)$

$T \wedge T \wedge T$

T

2. Show the following equivalences:

i. $\mathbf{P \rightarrow (Q \rightarrow P) \Leftrightarrow \neg P \rightarrow (P \rightarrow Q)}$ ii. $\mathbf{P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)}$

iii. $\mathbf{(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q}$ iv. $\mathbf{\neg(P \rightleftarrows Q) \Leftrightarrow (P \vee Q) \wedge \neg(P \wedge Q)}$

Solution

i. $\mathbf{P \rightarrow (Q \rightarrow P) \Leftrightarrow \neg P \rightarrow (P \rightarrow Q)}$

L.H.S. $\neg P \vee (\neg Q \vee P) \Leftrightarrow \neg P \vee (P \vee \neg Q) \Leftrightarrow (\neg P \vee P) \vee \neg Q$

$\Leftrightarrow T \vee \neg Q \Leftrightarrow T$

R.H.S. $\neg\neg P \vee (\neg P \vee Q)$

$\Leftrightarrow P \vee (\neg P \vee Q)$

$\Leftrightarrow (P \vee \neg P) \vee Q$

$\Leftrightarrow T \vee Q$

$\Leftrightarrow T$

ii. $\mathbf{P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)}$

L.H.S $\neg P \vee (Q \vee R) \Leftrightarrow \neg P \vee Q \vee R$

R.H.S. $(\neg P \vee Q) \vee (\neg P \vee R) \Leftrightarrow (\neg P \vee Q \vee \neg P \vee R)$

$(\neg P \vee \neg P \vee Q \vee R) \Leftrightarrow \neg P \vee Q \vee R$

iii. $\mathbf{(P \rightarrow Q) \wedge (R \rightarrow Q) \Leftrightarrow (P \vee R) \rightarrow Q}$

L.H.S. $(\neg P \vee Q) \wedge (\neg R \vee Q) \Leftrightarrow (\neg P \wedge \neg R) \vee Q$

R.H.S. $\neg(P \vee R) \vee Q \Leftrightarrow (\neg P \wedge \neg R) \vee Q$

iv. $\mathbf{\neg(P \rightleftarrows Q) \Leftrightarrow (P \vee Q) \wedge \neg(P \wedge Q)}$

L.H.S. $\neg((P \rightarrow Q) \wedge (Q \rightarrow P))$

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

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

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

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

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

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

$\Leftrightarrow$ R.H.S.

3. Show the following implications without constructing the truth tables:

a. $P \rightarrow Q \Rightarrow P \rightarrow (P \wedge Q)$

b. $(P \rightarrow Q) \rightarrow Q \Rightarrow P \vee Q$

c. $((P \vee \neg P) \rightarrow Q) \rightarrow ((P \vee \neg P) \rightarrow R) \Rightarrow (Q \rightarrow R)$

Solution

a. $P \rightarrow Q \Rightarrow P \rightarrow (P \wedge Q)$

L.H.S. $\neg P \vee Q$

R.H.S. $\neg P \vee (P \wedge Q) \Rightarrow (\neg P \vee P) \wedge (\neg P \vee Q)$

$\Rightarrow T \wedge (\neg P \vee Q) \Rightarrow \neg P \vee Q$

b. $(P \rightarrow Q) \rightarrow Q \Rightarrow P \vee Q$

$(\neg P \vee Q) \rightarrow Q \Rightarrow \neg(\neg P \vee Q) \vee Q$

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

$\Rightarrow (P \vee Q) \wedge T \Rightarrow P \vee Q$

c. $((P \vee \neg P) \rightarrow Q) \rightarrow ((P \vee \neg P) \rightarrow R) \Rightarrow (Q \rightarrow R)$

$(T \rightarrow Q) \rightarrow (T \rightarrow R)$

$(\neg T \vee Q) \rightarrow (\neg T \vee R)$

$(F \vee Q) \rightarrow (F \vee R)$

$Q \rightarrow R$

4. Verify the following implication is a tautology by using truth table.
$[(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)] \rightarrow R$.

1

PU
Apr. 2010 – *5M*

Solution

P	Q	R	$P \vee Q$	$P \rightarrow R$	$Q \rightarrow R$	$(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)$	$(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)] \rightarrow R$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	T	T	T	T	T
T	F	F	T	F	T	F	T
F	T	T	T	T	T	T	T
F	T	F	F	T	F	F	T
F	F	T	T	T	T	T	T
F	F	F	F	T	T	F	T

Functionally Complete Sets of Connectives

Any set of connectives in which every formula can be expressed interms of an equivalent formula containing the connectives from this set is called a functionally complete set of connectives. It is assumed that such a functionally complete set does not contain any redundant connectives i.e., a connective which can be expressed interms of other connectives.

Write an equivalent formula for $P \wedge (Q \rightleftarrows R) \vee (R \rightleftarrows P)$ which does not contain conditional and biconditional.

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

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

6. Normal forms

The problem of determining, in a finite number of steps, whether a given statement formula is a tautology or a contradiction or atleast satisfiable is known as a decision problem. Constructing truth tables for this purpose may not always be practical, even with the aid of computer. We therefore consider other procedures known as reduction to **Normal Forms**.

A "Product" (in place of "conjunction") of the variables and their negations in a formula is called an elementary product. Let P and Q be any two atomic variables. Then P, $\urcorner P \wedge Q$, $\urcorner Q \wedge P \wedge \urcorner P$, $P \wedge \urcorner P$ are some examples of elementary products.

A "Sum" of the variables and their negations is called an elementary sum. P, $\urcorner P \vee Q$, $\urcorner Q \vee P \vee \urcorner P$, $P \vee \urcorner P$ are some examples of elementary sum.

6.1 Disjunctive Normal Form (DNF)

A formula which is equivalent to a given formula and which consists of a sum of elementary products is called a disjunctive normal form of the given formula.

Example

1. **Obtain disjunctive normal forms of:**

   i. $\mathbf{P \wedge (P \to Q)}$ ii. $\mathbf{\urcorner(P \vee Q) \rightleftarrows (P \wedge Q)}$ iii. $\mathbf{\urcorner(P \to (Q \wedge R))}$

Solution

i. $\mathbf{P \wedge (P \to Q)}$

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

ii. $\underbrace{\neg(\mathbf{P} \vee \mathbf{Q})}_{\mathbf{P}} \rightleftarrows \underbrace{(\mathbf{P} \wedge \mathbf{Q})}_{\mathbf{Q}}$

$\because P \rightleftarrows Q \rightleftarrows (P \wedge Q) \vee (\neg P \wedge \neg Q)$

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

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

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

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

$\Leftrightarrow$ Sum of elementary products

iii. $\neg(\mathbf{P} \rightarrow (\mathbf{Q} \wedge \mathbf{R}))$

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

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

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

6.2 Principal Disjunctive Normal Forms (PDNF)

For two variables P and Q, there are 2^2 such formulas given by $P \wedge Q$, $P \wedge \neg Q$,$P \wedge Q$ and $\neg P \wedge \neg Q$.

These formulas are called *minterms*.

From the truth tables of these minterms, it is clear that no two minterms are equivalent. Each minterm has the truth value T for exactly one combination of the truth values of the variables P and Q. For a given formula, an equivalent formula consisting of disjunctions of minterms only known as its PDNF. Such a normal form is also called the sum-of-products canonical form.

Example

1. Obtain the principal disjunctive normal forms of these formulas:

a. $\mathbf{P} \rightarrow \mathbf{Q}$ **b.** $\mathbf{P} \vee \mathbf{Q}$ **c.** $\neg(\mathbf{P} \wedge \mathbf{Q})$

Solution

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

The rows of P, Q in which T appears in the last column.

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

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

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

Note: To find out PDNF you can use laws as well as Truth tables.

2. Find the disjunctive normal form of $(q \rightarrow p) \wedge (\neg p \wedge q)$.

1

PU
Oct. 2009 – 5M

Solution

p	q	~p	~q	$q \rightarrow p$	$\sim p \wedge q$	$(q \rightarrow p) \wedge (\sim p \wedge q)$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	F	T	F
F	F	T	T	T	F	F

Since the last column uniformly contains F, disjunctive normal form of

$(q \rightarrow p) \wedge (\neg p \wedge q)$ does not exits.

2. Obtain PDNF $(\sim p \wedge q) \vee (p \wedge q) \vee q$.

1

PU
Oct. 2010 – 5M

Solution

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

$\therefore$ PDNF of $(\sim p \wedge q) \vee (p \wedge q) \vee q$ is,

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

6.3 Conjunctive Normal Forms (CNF)

A formula which is equivalent to a given formula and which consists of a product of elementary sums is called a conjunctive normal form of the given formula.

Example

1. **Obtain a conjunctive normal form of:**

   i. $\mathbf{P \wedge (P \rightarrow Q)}$ ii. $\mathbf{\neg(P \vee Q) \rightleftarrows (P \wedge Q)}$

Solution

i. $\mathbf{P \wedge (P \rightarrow Q)}$

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

ii. $\mathbf{\neg\underbrace{(P \vee Q)}_{P} \rightleftarrows \underbrace{(P \wedge Q)}_{Q}}$

$\because P \rightleftarrows Q \Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P)$

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

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

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

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

$\Leftrightarrow$ Product of elementary sums

6.4 Principal Conjunctive Normal Forms (PCNF)

For two variables P and Q, there are 2^2 such formulas given by:

$$P \vee Q,\ P \vee \neg Q,\ \neg P \vee Q \text{ and } \neg P \vee \neg Q$$

These formulas are called *maxterms*. It can be ascertained that each of the maxterms has the truth value F for exactly one combination of the truth values of the variables. Different maxterms have the truth value F for different combinations of the truth values of the variables.

A given formula, an equivalent formula consisting of conjunction of the maxterms is known as its PCNF. This normal form is also called the product-of-sums canonical form.

Examples

1. **Obtain the principal conjunctive normal form the formula S is given by:**

   $\mathbf{(\neg P \rightarrow R) \wedge (Q \rightleftarrows P)}$

Solution

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

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

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

$\Leftrightarrow (P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R)$ (Or)

P	Q	R	$\neg P \to R$	$Q \rightleftarrows P$	$(\neg P \to R) \wedge (Q \rightleftarrows P)$
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	T	F	F
T	F	F	T	F	F
F	T	T	T	F	F
F	T	F	F	F	F
F	F	T	T	T	T
F	F	F	F	T	F

The rows of P, Q, R in which F appears in the last column.

2. Obtain the principal disjunctive and conjunctive normal forms of the following formulas:

i. $(\neg P \vee \neg Q) \to (P \rightleftarrows \neg Q)$ **ii.** $Q \wedge (P \vee \neg Q)$

iii. $P \vee (\neg P \to (Q \vee (\neg Q \to R)))$ **iv.** $(P \to (Q \wedge R)) \wedge (\neg P \to (\neg Q \wedge \neg R))$

v. $P \to (P \wedge (Q \to P))$

Solution

i. $(\neg P \vee \neg Q) \to (P \rightleftarrows \neg Q)$

P	Q	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$	$P \rightleftarrows \neg Q$	$(\neg P \vee \neg Q) \to (P \rightleftarrows \neg Q)$
T	T	F	F	F	F	T
T	F	F	T	T	T	T
F	T	T	F	T	T	T
F	F	T	T	T	F	F

PDNF: $(P \wedge Q) \vee (P \wedge \neg Q) \vee (\neg P \wedge Q)$

PCNF: $\neg P \vee \neg Q$

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

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

PDNF: $P \wedge Q$

PCNF: $(P \vee \neg Q) \wedge (\neg P \vee Q) \wedge (\neg P \vee \neg Q)$

iii. $P \vee (\overbrace{\neg P \to (Q \vee (\neg Q \to R))}^{A})$

P	Q	R	$\neg P$	$\neg Q$	$\neg Q \to R$	$Q \vee (\neg Q \to R)$	A	$P \vee A$
T	T	T	F	F	T	T	T	T
T	T	F	F	F	T	T	T	T
T	F	T	F	T	T	T	T	T
T	F	F	F	T	F	F	T	T
F	T	T	T	F	T	T	T	T
F	T	F	T	F	T	T	T	T
F	F	T	T	T	T	T	T	T
F	F	F	T	T	F	F	F	F

PDNF: $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R)$
$\vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R)$

PCNF: $(\neg P \vee \neg Q \vee R)$

iv. $\underbrace{(P \to (Q \wedge R))}_{A} \wedge (\neg P \to \underbrace{(\neg Q \wedge \neg R))}_{B}$

P	Q	R	$Q \wedge R$	$P \to Q \wedge R$	$\neg P$	$\neg Q$	$\neg R$	$\neg Q \wedge \neg R$	$\neg P \to (\neg Q \wedge \neg R)$	$A \wedge B$
T	T	T	T	T	F	F	F	F	T	T
T	T	F	F	F	F	F	T	F	T	F
T	F	T	F	F	F	T	F	F	T	F
T	F	F	F	F	F	T	T	T	T	F
F	T	T	T	T	T	F	F	F	F	F
F	T	F	F	T	T	F	T	F	F	F
F	F	T	F	T	T	T	F	F	F	F
F	F	F	F	T	T	T	T	T	T	T

PDNF: $(P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$

PCNF: $(P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (\neg P \vee Q \vee \neg R)$
$\wedge (\neg P \vee \neg Q \vee R)$

v. $P \to (P \wedge (Q \to P))$

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

The given one is a Tautology.

3. Obtain the Principal Conjunctive Normal Form(PCNF) for the following:

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

1

PU
Oct. 2008 – *5M*

Solution

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

Principal conjunctive normal form is $\neg P \vee \neg Q$

1

PU
Apr. 2010 – *5M*

4. Obtain PCNF of $(\neg P \rightarrow R) \wedge (P \rightleftarrows Q)$.

Solution

$(\neg P \rightarrow R) \wedge (P \rightleftarrows Q)$

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

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

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

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

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

6.5 Logical Implication (Definition)

A Compound proposition S_1 is said to logically imply another compound proposition S_2 if and only if $S_1 \rightarrow S_2$ is a tautology. We denote logical implication by the symbol "$\Rightarrow$".

Examples

1. **Prove that $(p \to q) \wedge p$ logically imply q.**

Solution

p	q	$p \to q$	$(p \to q) \wedge p$	$(p \to q) \wedge p \to q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

Thus $(p \to q) \wedge p \Rightarrow q$.

2. **Prove the following chain rule $(p \to q) \wedge (q \to r) \Rightarrow (p \to r)$**

Solution

p	q	r	$p \to q$	$q \to r$	$(p \to q) \wedge (q \to r)$	$(p \to r)$	$(p \to q) \wedge (q \to r) \to (p \to r)$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

Hence the result.

▶Laws related to Logical Implication

1. $p \wedge (p \to q) \Rightarrow q$ (Detachment) Modus Ponens
2. $[(p \to q) \wedge (q \to r)] \Rightarrow (p \to r)$ Law of the Syllogism.
3. $[(p \to q) \wedge {\sim} q] \Rightarrow {\sim} p$ Modus tollens (Contrapositive)
4. $p \Rightarrow p \vee q$ Disjunctive addition
5. $p \wedge q \Rightarrow p$ and
   $p \wedge q \Rightarrow q$ Conjunctive simplification
6. $(p \vee q) \wedge {\sim} p \Rightarrow q$ and
   $(p \vee q) \wedge {\sim} q \Rightarrow p$ Disjunctive Simplification
7. $({\sim} p \to F) \Rightarrow p$ Rule of Contradiction.

⏭ Remark

Modus ponens and Modus tollens are Latin words. Modus ponens means ' the method of affirming'. Modus tollens means " method of denying". This is appropriate because we deny the conclusion q to prove ~ p

Example

1. **Test the validity of the following arguments: If there was a game, then swimming was impossible.**

   If they started on right time, then swimming was possible.

   They started on right time.

   Therefore, there was no game.

PU
Apr. 2010 – *5M*

Solution

Let p: There is a game

q: Swimming is impossible

r: They start on right time.

Given argument in symbolic form is,

$p \rightarrow q, r \rightarrow \sim q, \quad r \lceil \sim p$

Proof:

i.	$r \rightarrow \sim q,\ r$	Premises
ii.	$\therefore \sim q$	(1) and Modus Ponens.
iii.	$p \rightarrow q, \sim q$	Premise and (2)
iv.	$\therefore \sim p$	(3) and Modus Tollens.

Hence given argument is valid.

7. Theory of inference for Statement calculus

7.1 Rules of Inference

To prove the theorems, proof is needed. Proof consists of a sequence of statements. Some of these statements may be axioms (Universal truths), some may be previously proved theorems and other statements may be hypothesis (assumed to be True). To construct a proof, we need to derive new assertions from existing ones. This is done using Rules of Inference.

In the rules of inference the conclusion are derived from premises. Any conclusion which is arrived at by following these rules is called a valid conclusion and the argument is called a valid argument.

7.2 Validity using Truth Tables

A set of premises $\{H_1, H_2, \ldots, H_m\}$ a conclusion C follows logically iff.

$$H_1 \wedge H_2 \wedge \ldots \wedge H_m \Rightarrow C \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

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

The rows in which all $H_1, H_2, \ldots, H_m$ have the value T if for every such row, C also has the value T, hen (1) holds. The rows in which C has the value F if in every such row, at least one of the values of H_1, $H_2, \ldots, H_m$ is F then (1) also holds. We call such a method a "Truth Table Technique" for the determination of the validity of a conclusion.

Examples

1. **Show that the conclusion C follows from the premises $H_1, H_2, \ldots$ in the following cases:**

a.	**H_1: $\neg P$**	**H_2: $P \vee Q$**	**C : Q**
b.	**H_1: $P \rightarrow Q$**	**H_2: $Q \rightarrow R$**	**C : $P \rightarrow R$**
c.	**H_1: R**	**H_2: $P \vee \neg P$**	**C : R**
d.	**H_1: $\neg Q$**	**H_2: $P \rightarrow Q$**	**C : $\neg P$**

Solution

a. **H_1: $\neg P$** **H_2: $P \vee Q$** **C : Q**

P	Q	$H_1 : \neg P$	H_2: $P \vee Q$	C : Q
T	T	F	T	T
T	F	F	T	F
F	T	T	T	T
F	F	T	F	F

Valid

b. **H_1: $P \rightarrow Q$** **H_2: $Q \rightarrow R$** **C : $P \rightarrow R$**

P	Q	R	H_1: $P \rightarrow Q$	H_2: $Q \rightarrow R$	C: $P \rightarrow R$
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	T
T	F	F	F	T	F
F	T	T	T	T	T
F	T	F	T	F	T
F	F	T	T	T	T
F	F	F	T	T	T

Valid

c. $H_1: R$ $H_2: P \vee \neg P$ $C : R$

P	R	$\neg P$	$H_1: R$	$H_2: P \vee \neg P$	$C : R$
T	T	F	T	T	T
T	F	F	F	T	F
F	T	T	T	T	T
F	F	T	F	T	F
Valid					

d. $H_1: \neg Q$ $H_2: P \to Q$ $C : \neg P$

P	Q	$H_1 : \neg Q$	$H_2: P \to Q$	$C : \neg P$
T	T	F	T	F
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T
Valid				

2. **Determine whether the conclusion C is valid in the following, when H_1, H_2, ... are the premises.**

a. $H_1: P \vee Q$ $H_2: P \to R$ $H_3: Q \to R$ $C : R$

b $H_1: P \to (Q \to R)$ $H_2: R$ $C : P$

c. $H_1: \neg P$ $H_2: P \vee Q$ $C : P \wedge Q$

Solution

a. $H_1: P \vee Q$ $H_2: P \to R$ $H_3: Q \to R$ $C : R$

P	Q	R	$H_1: P \vee Q$	$H_2: P \to R$	$H_3: Q \to R$	$C : R$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	T	T	T	T
T	F	F	T	F	T	F
F	T	T	T	T	T	T
F	T	F	T	T	F	F
F	F	T	F	T	T	T
F	F	F	F	T	T	F
Valid						

b. **$H_1: P \rightarrow (Q \rightarrow R)$ $H_2: R$ $C : P$**

P	Q	R	$Q \rightarrow R$	$H_1: P \rightarrow (Q \rightarrow R)$	$H_2: R$	$C : P$
T	T	T	T	T	T	T
T	T	F	F	F	F	T
T	F	T	T	T	T	T
T	F	F	T	T	F	T
F	T	T	T	T	T	F
F	T	F	F	T	F	F
F	F	T	T	T	T	F
F	F	F	T	T	F	F
Invalid						

c. **$H_1: \neg P$ $H_2: P \vee Q$ $C : P \wedge Q$**

P	Q	$H_1: \neg P$	$H_2: P \vee Q$	$C : P \wedge Q$
T	T	F	T	T
T	F	F	T	F
F	T	T	T	F
F	F	T	F	F
Invalid				

7.3 Rules of Inference

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

Rule T: A formula S may be introduced in a derivation if S is tautologically implied by any one or more of the preceding formulas in the derivation. Determine whether the following is a valid argument.

Examples

1. **Test the validity of following arguments:**

If Sita goes to class, she is on time
But Sita is late.
She will therefore miss class.

Solution

Let P: Sita goes to class
Q: Sita is on time

$P \rightarrow Q$	Rule P
$\neg Q$	Rule P
$\neg p$	Rule T, I_{12}

The argument is valid.

2. Determine the validity of the arguments:

If I study, then I will pass.

If I do not go to a movie, then I will study.

I failed.

Therefore, I went to a movie.

1

PU
Oct. 2008 – *5M*

Solution

Let p: I study

q : I will pass

r : I go to movies

The argument may be written as symbolically.

$p \rightarrow q, \sim r \rightarrow p, \sim q \vdash r.$

i.	$p \rightarrow q$	Premise
ii.	$\sim q$	Premise
iii.	$\sim p$	Rule of Modus Tollen for (1) and (2).
iv.	$\sim r \rightarrow p$	Premise
v.	$\sim(\sim r)$	Rule of Modus Tollen for (3) and (4)
vi.	r	Double Negation law for (5).

Hence the given agreement is valid.

3. Test the validity of following argument:

If today is Tuesday, then there is a test in Computer Science (C.S) or Discrete Mathematics (D.M). If the D.M professor is sick, there will be no test in D.M. Today is Tuesday and the professor of D.M is sick. Hence there will be a test in C.S.

Solution

Let p: Today is Tuesday

Q: There is a test in C.S

r: There is test in D.M

s: D.M professor is sick

	(1) $p \wedge s$	Rule P
{1}	(2) p	Rule T, I_1
	(3) $p \rightarrow Q \vee r$	Rule P
{2, 3}	(4) $Q \vee r$	Rule T, I_{11}
{1}	(5) s	Rule T, I_2

	(6) $s \rightarrow \neg r$	Rule P
$\{5, 6\}$	(7) $\neg r$	Rule T, I_{11}
$\{4\}$	(8) $r \vee Q$	Rule T
$\{7, 8\}$	(9) Q	Rule T, I_{10}

The argument is valid.

4. Demonstrate that R is valid inference from the premises $P \rightarrow Q$, $Q \rightarrow R$ and P.

Solution

	(1) $P \rightarrow Q$	Rule P
	(2) $Q \rightarrow R$	Rule P
$\{1, 2\}$	(3) $P \rightarrow R$	Rule T, I_{13}
	(4) P	Rule P
$\{3, 4\}$	(5) R	Rule T, I_{11}

5. Show the validity of the following arguments, for which the premises are given on the left and the conclusion on the Right.

i.	$\neg(P \wedge \neg Q), \neg Q \vee R, \neg R$	$\neg P$
ii.	$\neg J \rightarrow (M \vee N), (H \vee G) \rightarrow \neg J, H \vee G$	$M \vee N$
iii.	$P \rightarrow Q, Q \rightarrow \neg R, R, P \vee (J \wedge S)$	$J \wedge S$
iv.	$(P \wedge Q) \rightarrow R, \neg R \vee S, \neg S$	$\neg P \vee \neg Q$
v.	$(A \rightarrow B) \wedge (A \rightarrow C), \neg(B \wedge C), D \vee A$	D
vi.	$P \vee Q, Q \rightarrow R, P \rightarrow M$ and $\neg M$	$R \wedge (P \vee Q)$

Solution

i. $\neg(P \wedge \neg Q), \neg Q \vee R, \neg R$ $\neg P$

	(1) $\neg(P \wedge \neg Q)$	Rule P
	(2) $\neg P \vee Q$	Rule T, E8
	(3) $P \rightarrow Q$	Rule T, $P \rightarrow Q \Leftrightarrow \neg P \vee Q$
	(4) $\neg Q \vee R$	Rule P
	(5) $Q \rightarrow R$	Rule T
$\{3, 5\}$	(6) $P \rightarrow R$	Rule T
	(7) $\neg R$	Rule P
$\{6, 7\}$	(8) $\neg P$	Rule T, I_{12}

ii. $\mathbf{\neg J \rightarrow (M \vee N), (H \vee G) \rightarrow \neg J, H \vee G}$ $\mathbf{M \vee N}$

(1) $(H \vee G) \rightarrow \neg J$	Rule P
(2) $\neg J \rightarrow (M \vee N)$	Rule P
(3) $(H \vee G) \rightarrow (M \vee N)$	Rule T, I_{13}
(4) $(H \vee G)$	Rule P
(5) $M \vee N)$	Rule T, I_{11}

iii. $\mathbf{P \rightarrow Q, Q \rightarrow \neg R, R, P \vee (J \wedge S)}$ $\mathbf{J \wedge S}$

(1) $P \rightarrow Q$	Rule P
(2) $Q \rightarrow \neg R$	Rule P
{1, 2} (3) $P \rightarrow \neg R$	Rule T, I_{13}
(4) R	Rule P
{3, 4} (5) $\neg P$	Rule T, I_{12}
(6) $P \vee (J \wedge S)$	Rule P
{5, 6} (7) $J \wedge S$	Rule T, I_{10}

iv. $\mathbf{(P \wedge Q) \rightarrow R, \neg R \vee S, \neg S}$ $\mathbf{\neg P \vee \neg Q}$

(1) $\neg R \vee S$	Rule P
(2) $R \rightarrow S$	Rule T, E_{16}
(3) $\neg S$	Rule P
{2, 3} (4) $\neg R$	Rule T, I_{12}
(5) $(P \wedge Q) \rightarrow R$	Rule P
{4, 5} (6) $\neg(P \wedge Q)$	Rule T, I_{12}
(7) $\neg P \vee \neg Q$	Rule T

v. $\mathbf{(A \rightarrow B) \wedge (A \rightarrow C), \neg(B \wedge C), D \vee A}$ $\mathbf{D}$

(1) $(A \rightarrow B) \wedge (A \rightarrow C)$	Rule P
(2) $\neg A \vee (B \wedge C)$	Rule T
(3) $\neg(B \wedge C)$	Rule P
(4) $\neg A$	Rule T, I_{10}
(5) $D \vee A$	Rule P
(6) D	Rule T, I_{10}

vi. $\mathbf{P \vee Q, Q \rightarrow R, P \rightarrow M}$ **and** $\mathbf{\neg M}$ $\mathbf{R \wedge (P \vee Q)}$

	(1) $P \vee Q$	Rule P
	(2) $\neg P \rightarrow Q$	Rule T
	(3) $Q \rightarrow R$	Rule P
$\{2, 3\}$	(4) $\neg P \rightarrow R$	Rule T
	(5) $P \rightarrow M$	Rule P
	(6) $\neg M$	Rule P
$\{5, 6\}$	(7) $\neg P$	Rule T, I_{12}
$\{4, 7\}$	(8) R	Rule T, I_{11}
$\{1, 8\}$	(9) $R \wedge (P \vee Q)$	Rule T, I_9

Rule CP

If we can derive S from R and a set of premises, that we can derive R → S from the set of premises alone.

Rule CP is also called the deduction theorem and is generally used if the conclusion is of the form R → S. In such cases, R is taken as an additional premised and S is derived from the given premises and R.

Example

1. Derive the following, using rule CP if necessary:

i. $\mathbf{\neg P \vee Q, \neg Q \vee R, R \rightarrow S \Rightarrow P \rightarrow S}$

ii. $\mathbf{P, P \rightarrow (Q \rightarrow (R \wedge S)) \Rightarrow Q \rightarrow S}$

iii. $\mathbf{P \rightarrow (Q \rightarrow S), \neg R \vee P}$ **and** $\mathbf{Q \Rightarrow R \rightarrow S}$

iv. $\mathbf{P \rightarrow (Q \rightarrow R), Q \rightarrow (R \rightarrow S) \Rightarrow P \rightarrow (Q \rightarrow S)}$

Solution

i. $\mathbf{\neg P \vee Q, \neg Q \vee R, R \rightarrow S \Rightarrow P \rightarrow S}$

	(1) $\neg P \vee Q$	Rule P
$\{1\}$	(2) $P \rightarrow Q$	Rule T
	(3) $\neg Q \vee R$	Rule P
$\{3\}$	(4) $Q \rightarrow R$	Rule T
$\{2, 4\}$	(5) $P \rightarrow R$	Rule T
	(6) $R \rightarrow S$	Rule P
$\{5, 6\}$	(7) $P \rightarrow S$	Rule T

ii. $\mathbf{P, P \to (Q \to (R \land S)) \Rightarrow Q \to S}$

$(1)\ P$	Rule P
$(2)\ P \to (Q \to R \land S)$	Rule P
$\{1, 2\}\ (3)\ Q \to R \land S$	Rule T, I_{11}
$\{3\}\ \ (4)\ R \land S$	Rule T, I_6
$(5)\ S$	Rule T, I_2
$(6)\ Q$	Rule P (assumed premise)
$\{5, 6\}\ (7)\ Q \to S$	Rule CP

iii. $\mathbf{P \to (Q \to S), \neg R \lor P}$ **and** $\mathbf{Q \Rightarrow R \to S}$

$(1)\ \neg R \lor P$	Rule P
$(2)\ R$	Rule P (assumed premises)
$\{1, 2\}\ (3)\ P$	Rule T, I_{10}
$(4)\ P \to (Q \to S)$	Rule P
$\{3, 4\}\ (5)\ Q \to S$	Rule T, I11
$(6)\ Q$	Rule P
$(7)\ S$	Rule T, I_{11}
$\{2, 7\}\ (8)\ R \to S$	CP

iv. $\mathbf{P \to (Q \to R), Q \to (R \to S) \Rightarrow P \to (Q \to S)}$

$(1)\ P$	Rule P (AP)
$(2)\ P \to (Q \to R)$	Rule P
$\{1, 2\}\ (3)\ Q \to R$	Rule T, I_{11}
$(4)\ Q \to (R \to S)$	Rule P
$\{4\}\ \ (5)\ R \to S$	Rule T, I_6
$\{3, 5\}\ (6)\ Q \to S$	Rule T, I13
$\{1, 6\}\ (7)\ P \to (Q \to S)$	CP

7.4 Consistency of Premises and Indirect Method of Proof

A set of formulas $H_1, H_2, \ldots, H_m$ is inconsistent if their conjunction implies a contradiction, that is

$$H_1 \land H_2 \land \ldots \land H_m \Rightarrow R \land \neg R$$

where R is any formula.

Example

1. Show that the following sets of premises are inconsistent:

i. $P \rightarrow Q, P \rightarrow R, Q \rightarrow \neg R, P$

ii. $A \rightarrow (B \rightarrow C), D \rightarrow (B \wedge \neg C), A \wedge D$

iii. $(R \rightarrow \neg Q), R \vee S, S \rightarrow \neg Q, P \rightarrow Q \Rightarrow \neg P$

Solution

i. $P \rightarrow Q, P \rightarrow R, Q \rightarrow \neg R, P$

	(1) $P \rightarrow Q$	Rule P
	(2) $Q \rightarrow \neg R$	Rule P
{1, 2}	(3) $P \rightarrow \neg R$	Rule T, I_{13}
	(4) $P \rightarrow R$	Rule P
{4}	(5) $\neg R \rightarrow \neg P$	Rule T, E_{18}
{4, 5}	(6) $P \rightarrow \neg P$	Rule T, I_{13}
	(7) P	Rule P
{6, 7}	(8) $\neg P$	Rule T, I_{11}
	(9) $P \wedge \neg P$	Rule T, I_9

ii. $A \rightarrow (B \rightarrow C), D \rightarrow (B \wedge \neg C), A \wedge D$

	(1) $A \wedge D$	Rule P
{1}	(2) A	Rule T, I_1
	(3) $A \rightarrow (B \rightarrow C)$	Rule P
{2, 3}	(4) $B \rightarrow C$	Rule T, I_{11}
{4}	(5) $\neg B \vee C$	Rule T, E_{16}
	(6) $D \rightarrow (B \wedge \neg C)$	Rule P
{6}	(7) $\neg(B \wedge \neg C) \rightarrow \neg D$	Rule T, E_{18}
	(8) $\neg B \vee C \rightarrow \neg D$	Rule T
{5, 8}	(9) $\neg D$	Rule T
{1}	(10) D	Rule T, I_2
{9, 10}	(11) $D \wedge \neg D$	Rule T

iii. $(R \to \neg Q), R \vee S, S \to \neg Q, P \to Q \Rightarrow \neg P$

	(1) $P \to Q$	Rule P
	(2) $R \to \neg Q$	Rule P
{2}	(3) $Q \to \neg R$	Rule T, E_{18}
{1, 3}	(4) $P \to \neg R$	Rule T, I_{13}
	(5) $R \vee S$	Rule P
{5}	(6) $\neg R \to S$	Rule T
{4, 6}	(7) $P \to S$	Rule T, I_{13}
	(8) $S \to \neg Q$	Rule P
{7, 8}	(9) $P \to \neg Q$	Rule T, I_{13}
{9}	(10) $Q \to \neg P$	Rule T, E_{18}
{10}	(11) $\neg P$	Rule T, I_6

8. Predicate Calculus

The logic based upon the analysis of predicates in any statement is called predicate logic. Every predicate describes something about one or more objects.

The part “is a bachelor” is called a predicate. Denote the predicate “is a bachelor” symbolically by the predicate letter B, “Ravi” by r. The statement can be written as B(r).

The symbols (x) or (∀x) are called **Universal Quantifiers**. Quantification symbol is “( )” or “(∀)”, and it contains the variable which is to be quantified.

A(x): x is an apple

R(x): x is Red

$(x)\ (A(x) \to R(x))$

The universal quantifier was used to translate expression such as “for all”, “every” and “for any”.

Another quantifier is “for some”, “there is atleast one” or “there exists some”. “(∃x)”, called the existential quantifier.

M(x): x is a man

C(x): x is clever

$(\exists x)$: $(M(x) \wedge C(x))$

Example

1. Let P(x), Q(x) and R(x) be the statements “x is clear explanation”, “x is satisfactory”, and ‘x is an excuse” respectively. Suppose that the universe of discourse for x is the set of all English text. Express each of the following statements using quantifiers.

i. All clear explanations are satisfactory.

ii. Some excuses are not clear explanations.

1

PU
Apr. 2010 – *5M*

Solution

V = {x | x is set of all English text}

i. $(x)\,[P(x) \rightarrow Q(x)]$

ii. $(\exists\, x)\,[R(x) \rightarrow \neg P(x)]$

8.1 Free and Bound Variables

A formula containing a part of the form $(x)\,P(x)$ or $(\exists x)\,P(x)$, such a part is called an x-bound part of the formula. Any occurrence of x in an x-bound part of a formula is called **Bound Occurrence** of x, while any occurrence of x or of any variable that is not a bound occurrence is called a **Free Occurrence**. The formula P(x) either in $(x)\,P(x)$ or in $(\exists x)\,P(x)$ is described as the scope of the quantifier.

$(x)\,P(x, y)$

P(x, y) is the scope of the quantifier and both occurrence of x are bound occurrences, while the occurrence of y is a free occurrence.

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

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

$(x)\,(P(x) \rightarrow (\exists y)\,R(x, y)$

The scope of (x) is $P(x) \rightarrow (\exists y)\,R(x, y)$

while the scope of $(\exists y)$ is R(x, y).

All occurrences of both x and y are bound occurrences.

$(x)\,(P(x) \rightarrow R(x)) \vee (x)\,(P(x) \rightarrow Q(x))$

The scope of the first quantifier is $P(x) \rightarrow R(x)$ and the scope of the second is $P(x) \rightarrow Q(x)$. All occurrences of x are bound occurrences.

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

The scope of $(\exists x)$ is $P(x) \wedge Q(x)$. The occurrence of x are bound.

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

The scope of $(\exists x)$ is P(x) and the last occurrence of x in Q(x) is free.

Examples

1. **Indicate the variables that are free and bound. Also show the scope of the quantifiers.**

   i. $(x)\,(P(x) \wedge R(x)) \rightarrow (x)\,P(x) \wedge Q(x)$ **ii.** $(x)\,(P(x) \wedge (\exists x)\,Q(x)) \vee ((x)\,P(x) \rightarrow Q(x))$

   iii. $(x)\,(P(x) \rightleftarrows Q(x) \wedge (\exists x)\,R(x)) \wedge S(x)$

Solution

i. $(x)\,(P(x) \wedge R(x)) \rightarrow (x)\,P(x) \wedge Q(x)$

The scope of the 1^{st} quantifier s $P(x) \wedge R(x)$, all occurrences of x are bound. The scope of the 2^{nd} quantifier is P(x) and the last occurrence of x in Q(x) is free.

ii. $(x)\,(P(x) \wedge (\exists x)\,Q(x)) \vee ((x)\,P(x) \rightarrow Q(x))$

The scope of (x) is $P(x) \wedge (\exists x)\,Q(x)$ while the scope of $(\exists x)$ is Q(x). The scope of (x) is $P(x) \rightarrow Q(x)$.

All occurrences of x are bound.

iii. $(x)\,(P(x) \rightleftarrows Q(x) \wedge (\exists x)\,R(x)) \wedge S(x)$

The scope of (x) is $P(x) \rightleftarrows Q(x) \wedge (\exists x)\,R(x)$ while the scope of $(\exists x)$ is R(x) all the occurrences of x are bound and the last occurrences of x in S(x) is free.

2. **Indicate the variables that are free and bound and scope of quantifiers.**

   i. $(P(x) \wedge (\exists x)\,Q(x)) \vee ((\forall x)\,P(x) \rightarrow Q(x))$

   ii. $(\forall x)\,R(x) \wedge (\forall x)\,S(x)$

1
PU
Oct. 2008 – 5M

Solution

i. $(P(x) \wedge (\exists x)\,Q(x) \vee ((\forall x)\,P(x) \rightarrow Q(x))$

Here Q(x) and $P(x) \rightarrow Q(x)$ are scope of quantifiers and all occurrence of x are bound variables.

Also occurrence of x in P(x) is free variable.

ii. $(\forall x)\,R(x) \wedge (\forall x)\,S(x)$

Here R(x) and S(x) is the scope of quantifier and all occurrence of x are bound variables.

Here there is no free variables.

8.2 Universe of Discourse

The variables which are quantified stand for only those objects which are members of a particular set or class. Such a restricted class is called the Universe of discourse or the domain of individuals or simply the universe.

Examples

1. **Find the truth values of:**

   i. **(x) (P(x) ∨Q(x)), where P(x) : x = 1, Q(x) : x = 2 and the universe of discourse is {1, 2}.**

   ii. **(x) (P → Q(x)) ∨ R(a) where P: 2 > 1, Q(x): x ≤ 3, R(x): x > 5 and a: 5, with the universe being {–2, 3, 6}.**

Solution

i. **(x) (P(x) ∨Q(x)), where P(x) : x = 1, Q(x) : x = 2 and the universe of discourse is {1, 2}.**

$P(1) \vee Q(1)$ when $x = 1$

$x = 1 \Rightarrow 1 = 1 \Rightarrow T$

$x = 2 \Rightarrow 1 = 2 \Rightarrow F$

$P(1) \vee Q(1)$

$T \vee F$

T

$P(2) \vee Q(2)$ when $x = 2$

$x = 1 \Rightarrow 2 = 1 \Rightarrow F$

$x = 2 \Rightarrow 2 = 2 \Rightarrow T$

$P(2) \vee Q(2)$

$F \vee T$

T

ii. **(x) (P → Q(x)) ∨ R(a) where P: 2 > 1, Q(x): x ≤ 3, R(x): x > 5 and a: 5, with the universe being {–2, 3, 6}.**

$(x)\ (P \rightarrow Q(x)) \vee R(a)$

$(2 > 1 \rightarrow Q\ (-2)) \vee R(-2)$

$\therefore\ Q(-2) = -2 \leq 3 \Rightarrow T$

$R(-2) = -2 > 5 \Rightarrow F$

$T \vee F$

T

$(2 > 1 \rightarrow Q(3)) \vee R(3)$

$Q(3): 3 \leq 3 \Rightarrow T$

$R(3): 3 > 5 \Rightarrow F$

$(T \rightarrow T) \vee F$

$T \vee F$

T

$(2 > 1 \rightarrow Q(6)) \vee R(6)$

$Q(6): 6 \le 3 \Rightarrow F$

$R(6): 6 > 5 \Rightarrow T$

$(T \to F) \vee T$

$F \vee T$

T

2. **$(\exists x)\ (P(x) \to Q(x)) \wedge T$, where $P(x)$: $x > 2$, $Q(x)$: $x = 0$ and T is any tautology, with the universe of the discourse as {1}.**

Solution

$(P(x) \to Q(x)) \wedge T$

$P(x): x > 2 \Rightarrow 1 > 2 \Rightarrow F$

$Q(x): x = 0 \Rightarrow 1 = 0 \Rightarrow F$

$(F \to F) \wedge T$

$T \wedge T$

T

▶ Theorem

$\urcorner((x)\ A(x)) \Leftrightarrow (\exists x)\ \urcorner A(x)$

Proof

Let the universe of discourse be denoted by a finite set S given by
$S = \{a_1, a_2, \ldots, a_n\}$
$(x)\ A(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \ldots \wedge A(a_n)$
L.H.S: $\urcorner((x)\ A(x)) \Leftrightarrow \urcorner(A(a_1) \wedge A(a_2) \wedge \ldots \wedge A(a_n))$

$\Leftrightarrow \urcorner A(a_1) \vee \urcorner A(a_2) \vee \ldots \vee \urcorner A(a_n)$

$\Leftrightarrow (\exists x)\ \urcorner A(x)$

$\Leftrightarrow$ R.H.S

8.3 Theory of Inference for the Predicate Calculus

In order to use the equivalences and implications, we need some rules on how to eliminate quantifiers during the course of derivations. This elimination is done by rules of specification called rules US and ES. Once the quantifiers are eliminated, the derivation proceeds as in the case of statement calculus and the conclusion is reached. It may happen that the desired conclusion is quantified. In this case we need rules of generalization called rules UG and EG.

The rules of generalization and specification follow. Here A(x) is used to denote a formula with a free occurrences of x. A(y) denotes a formula obtained by the substitution of y for x in A(x).

▶Rule US (Universal Specification)

From (x) A(x) one can conclude A(y).

▶Rule ES (Existential Specification)

From (∃x) A(x) one can conclude A(y) provided that y is not free in any given premise and also not free in any prior step of the derivation. These requirements can easily be met by choosing a new variable each time ES is used.

▶Rule EG (Existential Generalization)

From A(x) one can conclude (∃y) A(y).

▶Rule UG (Universal Generalization)

From A(x) one can conclude (y) A(y) provided that x is not free in any of the given premises and provided that if x is free in a prior step which resulted from use of ES, then no variables introduced by that use of ES appear free in A(x).

Examples

1. **All men are mortal**
Socrates is a man
Therefore Socrates is a mortal
If we denote
H(x): x is a man
M(x): x is a mortal
and S: Socrates
Show that (x) (H(x) → M(x)) ∧ H(S) ⇒ M(S).

Solution

	(1) (x) (H(x) → M(x))	P
{1}	(2) H(S) → M(S)	US
	(3) H(S)	P
{2, 3}	(4) M(S)	T, I_{11}

2. **Show that (x) (P(x) → Q(x)) ∧ (x) (Q(x) → R(x)) ⇒ (x) (P(x) → R(x)).**

Solution

	(1)(x) (P(x) → Q(x))	P
{1}	(2) P(y) → Q(y)	US
	(3) (x) (Q(x) → R(x)	P
{3}	(4) Q(y) → R(y)	US
{2, 4}	(5) P(y) → R(y)	T, I_{13}
	(6) (x) (P(x) → R(x))	UG

3. Show that $(\exists x)\ M(x)$ follows logically from the premises $(x)\ (H(x) \rightarrow M(x))$ and $(\exists x)\ H(x)$.

Solution

	(1) $(\exists x)\ H(x)$	P
{1}	(2) $H(y)$	ES
	(3) $(x)\ (H(x) \rightarrow M(x))$	P
{3}	(4) $H(y) \rightarrow M(y)$	US
{2, 4}	(5) $M(y)$	T, I_{11}
	(6) $(\exists x)\ M(x)$	EG

4. Show that $(\exists x)\ M(x)$ follows logically from the premises $(x)\ (H(x) \rightarrow M(x))$, $(\exists x)\ H(x)$

1

PU
Apr. 2010 – *5M*

Solution

	(1) $(\exists x)\quad H(x)$	Premise
{1}	(2) $H(y)$	Existential specification
	(3) $(x)\ (H(x) \rightarrow M(x))$	Premise
{3}	(4) $H(y) \rightarrow M(y)$	Universal specification
{2, 4}	(5) $M(y)$	Modus pones
	(6) $(\exists x)\ M(x)$	Existential Generalization

5. Prove that $(\exists x)\ (P(x) \wedge Q(x)) \Rightarrow (\exists x)\ P(x) \wedge (\exists x)\ Q(x)$.

Solution

	(1) $(\exists x)\ (P(x) \wedge Q(x))$	P
{1}	(2) $P(y) \wedge Q(y)$	ES, y fixed
{2}	(3) $P(y)$	T, I_1
{2}	(4) $Q(y)$	T, I_2
{3}	(5) $(\exists x)\ P(x)$	EG
{4}	(6) $(\exists x)\ Q(x)$	EG
{3, 4}	(7) $(\exists x)\ P(x) \wedge (\exists x)\ Q(x)$	T, I_9

6. Show that from

i. $(\exists x)\ (F(x) \wedge S(x)) \rightarrow (y)\ (M(y) \rightarrow W(y)$ **ii.** $(\exists y)\ (M(y) \wedge \neg W(y)$

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

Solution

	(1) $(\exists y)\ (M(y) \wedge \neg W(y))$	P
{1}	(2) $M(z) \wedge \neg W(z)$	ES

{2} (3) $\urcorner((M(z) \rightarrow W(z))$ T, E_{17}

(4) $(\exists y)\ \urcorner(M(y) \rightarrow W(y))$ EG

{4} (5) $\urcorner(y)\ (M(y) \rightarrow W(y))$ T, E_{26}

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

{5, 6} (7) $\urcorner(\exists x)\ (F(x) \wedge S(x))$ T, I_{12}

{7} (8) $(x)\ \urcorner(F(x) \wedge S(x))$ T, E_{25}

(9) $\urcorner(F(x) \wedge S(x))$ US

(10) $F(x) \rightarrow \urcorner S(x)$ T, E_9, E_{16}, E_{17}

(11) $(x)\ (F(x) \rightarrow \urcorner S(x))$ UG

7. **Show that $(\forall x)\ (P(x)) \rightarrow Q\ (x)) \wedge (\forall x)\ (Q\ (x) \rightarrow R\ (x)) \rightarrow (\forall x)\ (P(x) \rightarrow R\ (x))$.**

PU
Oct. 2009 – *5M*
1

Solution

i. $(\forall\ x)\ (P(x) \longrightarrow Q\ (x))$ P- Premise

1} ii. $P\ (y) \longrightarrow Q\ (y)$ US- Universal Specification

iii. $(\forall\ x)\ (Q\ (x) \longrightarrow R\ (x))$ P- Premise

3} iv. $Q\ (y) \longrightarrow R\ (y)$ US

2,4} v. $P\ (y) \longrightarrow R\ (y)$ T, I_{13} (Hypothetical Syllogism)

vi. $(\forall\ x)\ (P\ (x) \longrightarrow R\ (x))$ UG- Universal Generation.

8. **Show that: $(x)\ (P(x) \vee Q(x)) \Rightarrow (x)\ P(x) \vee (\exists x)\ Q(x)$.**

Solution

We shall use the indirect method of proof by assuming $\urcorner((x)\ P(x) \vee (\exists x)\ Q(x))$ as an additional premise.

(1) $\urcorner((x)\ P(x) \vee (\exists x)\ Q(x))$ P(assumed)

{1} (2) $\urcorner(x)\ P(x) \wedge \urcorner(\exists x)\ Q(x)$ T, E_9

{2} (3) $\urcorner(x)\ P(x)$ T, I_1

{3} (4) $(\exists x)\ \urcorner P(x)$ T, E_{26}

{2} (5) $\urcorner(\exists x)\ Q(x)$ T, I_2

{5} (6) $(x)\ \urcorner Q(x)$ T, E_{25}

{4}	(7) $\neg P(y)$	ES
{6}	(8) $\neg Q(y)$	US
{7, 8}	(9) $\neg P(y) \wedge \neg Q(y)$	T, I_9
{9}	(10) $\neg(P(y) \vee Q(y))$	T, E_9
	(11) $(x)\,(P(x) \vee Q(x))$	P
{11}	(12) $P(y) \vee Q(y)$	US
{10, 12}	(13) $\neg(P(y) \vee Q(y)) \wedge (P(y) \vee Q(y))$	T, I_9

Contradiction

Formulas involving more than one quantifier

$(x)\,(y)\,P(x, y) \Leftrightarrow (y)\,(x)\,P(x, y)$

$(x)\,(y)\,P(x, y) \Rightarrow (\exists y)\,(x)\,P(x, y)$

$(y)\,(x)\,P(x, y) \Rightarrow (\exists x)\,(y)\,P(x, y)$

$(\exists y)\,(x)\,P(x, y) \Rightarrow (x)\,(\exists y)\,P(x, y)$

$(\exists x)\,(y)\,P(x, y) \Rightarrow (y)\,(\exists x)\,P(x, y)$

$(x)\,(\exists y)\,P(x, y) \Rightarrow (\exists y)\,(\exists x)\,P(x, y)$

$(y)\,(\exists x)\,P(x, y) \Rightarrow (\exists x)\,(\exists y)\,P(x, y)$

$(\exists x)\,(\exists y)\,P(x, y) \Rightarrow (\exists y)\,(\exists x)\,P(x, y)$

The negation of any of the above formulas can be obtained by repeated applications of the equivalences E_{25} and E_{26}.

$\neg(\exists y)\,(x)\,P(x, y) \Leftrightarrow (y)\,(\neg(x)\,P(x, y)) \Leftrightarrow (y)\,(\exists x)\,\neg P(x, y)$

Example

1. Show that $\neg P(a, b)$ follows logically from $(x)\,(y)\,(P(x, y) \rightarrow W(x, y))$ and $\neg W(a, b)$:

Solution

	(1) $(x)\,(y)\,(P(x, y) \rightarrow W(x, y))$	P
{1}	(2) $(y)\,(P(a, y) \rightarrow W(a, y))$	US
{2}	(3) $P(a, b) \rightarrow W(a, b)$	US
	(4) $\neg W(a, b)$	P
{3, 4}	(5) $\neg P(a, b)$	T, I_{12}

Solved Examples

1. Use statement calculus to derive the following arguments.

$$P, P \rightarrow (Q \rightarrow \{R \wedge S\} = Q \rightarrow S$$

1 PU Oct.2008 – 5M

Solution

i.	$R \wedge S$	Premise
ii.	S	Conjuctive Simplification for (1)
iii.	$Q \rightarrow S$	(1) and (2)
iv.	$P \rightarrow (Q \rightarrow S)$	Premise and (3)
v.	P	Premise
vi.	$Q \rightarrow S$	Modus Ponens rule for (4) and (5)

2. Show that the premises P_1: $\rceil(A \wedge \rceil B)$, P_2: $\rceil B \vee D$, P_3: $\rceil D$ leads to a conclusion $\rceil A$.

1 PU Apr. 2010 – 5M

Solution

P_1: $\rceil(A \wedge \rceil B)$

P_2: $\rceil B \vee D$

P_3: $\rceil D$

C: $\rceil A$

Proof

i.	$\rceil B \vee D, \rceil D$	Premises P_2, P_3.
ii.	$\rceil B$	Disjunctive syllogism.
iii.	$\rceil(A \wedge \rceil B)$	Premise P1.
iv.	$\rceil A \vee \rceil(\rceil B)$	De Morgan's law
v.	$\rceil A \vee B$	Double negation.
vi.	$\rceil A \vee B, \rceil B$	(5) and (2)
vii.	$\rceil A$	Disjunctive syllogism.

∴ Conclusion $\rceil A$ follows from the given premises.

3. Test the validity of the following argument:
If I study, then I will not fail in mathematics.
If I do not play basketball, then I will study.
But I failed in mathematics.
Therefore I must have played basket ball.

1 PU Oct. 2010 – 5M

Solution

Let p: I study.
q: I will fail in mathematics.
r: I play basketball.

The given statements in symbolic form are

$p \to \sim q, \quad \sim r \to p, \quad q \vdash r$

i.	$p \to \sim q, \quad q$	Premises
ii.	$p \to \sim q, \quad \sim(\sim q)$	Double negation
iii.	$\therefore \sim p$	(2) and modus Tollens
iv.	$\sim r \to p, \sim p$	Premise, (3)
v.	$\sim(\sim r)$	Modus Tollens
vi.	r	Double negation

Hence given argument is valid.

4. Show that the conclusion is valid under the premises for the following without constructing truth table:

$P_1 : \sim(A \wedge \sim B)$, $P_2 : \sim B \vee D$, $P_3 : \sim D$, $C : \sim A$.

1 PU Oct. 2010 – 5M

Solution

$P_1 : \sim(A \wedge \sim B)$, $P_2 : \sim B \vee D$,

$P_3 : \sim D$, $C : \sim A$

i.	$\sim B \vee D, \quad \sim D$	Premises P_2, P_3
ii.	$\sim B$	Disjunctive Syllogism
iii.	$\sim A \vee \sim(\sim B)$	P_1
iv.	$\sim A \vee B$	Double negation
v.	$\sim A \vee B, \quad \sim B$	(4) and (2)
vi.	$\sim A$	Disjunctive syllogism

5. Prove that $(\exists x)(P(x) \wedge Q(x)) \Rightarrow (\exists x)\, P(x) \wedge (\exists x)\, Q(x)$.

1 PU Oct. 2010 – 5M

Solution

	(1) $(\exists x)(P(x) \wedge Q(x))$	P
{1}	(2) $P(y) \wedge Q(y)$	ES, y fixed.
{2}	(3) $P(y)$	T, I_1
{2}	(4) $Q(y)$	T, I_2
{3}	(5) $(\exists x)\ P(x)$	EG
{4}	(6) $(\exists x)\ Q(x)$	EG
{3, 4}	(7) $(\exists x)\ P(x) \wedge (\exists x)\, Q(x)$,	T,I_9

EXERCISE

1. Show the following implication without constructing the truth table:
   $P \rightarrow Q \Rightarrow P \rightarrow (P \wedge Q)$
2. Show the following equivalence:
   $P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)$
3. Show that $P \wedge (P \rightarrow Q) \rightarrow Q$ is a tautology:
4. There are two restaurants next to each other. One has a sign that says "Good food is not cheap" and the other has a sign that says "Cheap food is not good". Are both the signs saying the same thing?
5. Eliminating conditional and biconditional find disjunctive normal form of:

   $P \leftrightarrow (Q \vee R) \rightarrow \neg P$
6. If the universe of discourse is the set {a, b, c}, eliminate the quantifiers in the following formulas:
   i. $(x)(P(x) \rightarrow Q(x))$ ii. $(x)\,R(x) \wedge (x)\,S(x)$
7. Test the validity of the following argument:
   If Tina marries Rahul, she will be in Pune. If Tina marries Ramesh, she will be in Mumbai. If she is either in Pune or Mumbai, she will definitely be settled in life. She is not settled in life. This she did not marry Rahul or Ramesh.
8. Show that R is the conclusion of premised $(P \rightarrow Q) \rightarrow R$; $P \wedge S$ and $Q \wedge T$.
9. Prove that $(\exists x)\,(P(x) \wedge Q(x)) \Rightarrow (\exists x)\,P(x) \wedge (\exists x)\,Q(x)$.
10. Show that the following set of premises are inconsistent:

    $A \rightarrow (B \rightarrow C)$; $D \rightarrow (B \wedge \neg C)$ and $A \wedge D$
11. Let P(x) : x is a man
    F(x, y) : x is a father of y,
    M(x, y) : x is the mother of y.
    Write in symbolic form the predicate "x is the father of the mother of y".

Collection of Questions asked in Previous Exams PU

1. Use statement calculus to derive the following arguments. **[Oct. 2008 – 5*M*]**
   $P, P \rightarrow (Q \rightarrow \{R \wedge S\} = Q \rightarrow S$
2. Indicate the variables that are free and bound and scope of quantifiers. **[Oct. 2008 – 5*M*]**.
   i. $(P(x) \wedge (\exists x)\,Q(x)) \vee ((\forall x)\,P(x) \rightarrow Q(x))$ ii. $(\forall x)\,R(x) \wedge (\forall x)\,S(x)$
3. Show the following equivalence: $P \rightarrow (Q \vee R) \Leftrightarrow (P \rightarrow Q) \vee (P \rightarrow R)$. **[Oct. 2008 – 5*M*]**
4. Obtain the Principal Conjunctive Normal Form(PCNF) for the following: **[Oct. 2008 – 5*M*]**

   $(P \wedge Q) \vee (\neg P \wedge Q) \vee (P \wedge \neg Q)$
5. Determine the validity of the arguments: **[Oct. 2008 – 5*M*]**
   If I study, then I will pass.
   If I do not go to a movie, then I will study.
   I failed.
   Therefore, I went to a movie.

6. Construct the truth tables for the following: **[Oct. 2008 – 5M]**

   i. $\neg(P \leftrightarrow (Q \rightarrow (R \vee P))$ ii. $(P \vee Q) \wedge R) \rightarrow (P \vee R)$

7. Using the following statements: **[Oct. 2009 – 6M]**

   p: Ayush is rich
   q: Ayush is happy
   Write the following statements in symbolic form:

   i. Ayush is rich but unhappy ii. Ayush is poor but happy
   iii. Ayush is neither rich nor happy iv. Ayush is poor or he is both rich and unhappy.

8. Prove that $p \rightarrow (q \rightarrow r)$ and $(p \wedge \overline{r}) \rightarrow \overline{q}$ are logically equivalent. **[Oct. 2009 – 5M]**

9. Find the disjunctive normal form of $(q \rightarrow p) \wedge (\neg p \wedge q)$. **[Oct. 2009 – 5M]**

10. Show that $(\forall x)\,(P(x)) \rightarrow Q\,(x)) \wedge (\forall x)\,(Q\,(x) \rightarrow R\,(x)) \rightarrow (\forall x)\,(P(x) \rightarrow R\,(x))$. **[Oct. 2009 – 5M]**

11. Obtain PCNF of $(\neg P \rightarrow R) \wedge (P \rightleftarrows Q)$. **[Apr. 2010 – 5M]**

12. Test the validity of the following arguments: If there was a game, then swimming was impossible.
    If they started on right time, then swimming was possible.
    They started on right time.
    Therefore, there was no game. **[Apr. 2010 – 5M]**

13. Verify the following implication is a tautology by using truth table:
    $[(P \vee Q) \wedge (P \rightarrow R) \wedge (Q \rightarrow R)\,] \rightarrow R$. **[Apr. 2010 – 5M]**

14. Let P(x), Q(x) and R(x) be the statements "x is clear explanation", "x is satisfactory", and 'x is an excuse" respectively. Suppose that the universe of discourse for x is the set of all English text. Express each of the following statements using quantifiers. **[Apr. 2010 – 5M]**

    i. All clear explanations are satisfactory . ii. Some excuses are not clear explanations.

15. Show that $(\exists x)\, M(x)$ follows logically from the premises $(x)\,(H(x) \rightarrow M(x)),\ (\exists x)\, H(x)$.
    [Apr. 2010 – 5M]

16. Show that the premises P_1: $\neg(A \wedge \neg B)$, P_2: $\neg B \vee D$, P_3: $\neg D$ leads to a conclusion $\neg A$.
    [Apr. 2010 – 5M]

17. Obtain PDNF $(\sim p \wedge q) \vee (p \wedge q) \vee q$. **[Oct. 2010 – 5M]**

18. Test the validity of the following argument: **[Oct. 2010 – 5M]**
    If I study, then I will not fail in mathematics.
    If I do not play basketball, then I will study.
    But I failed in mathematics.
    Therefore I must have played basket ball.

19. Determine which is tautology or a fallacy: **[Oct. 2010 – 5M]**

    i. $p \Rightarrow q \wedge q \Rightarrow p$ ii. $(p \wedge q) \wedge (p \vee q)$

20. Show that the conclusion is valid under the premises for the following without constructing truth table:
    P_1 : $\sim(A \wedge \sim B)$, P_2: $\sim B \vee D$, P_3: $\sim D$, C: $\sim A$. **[Oct. 2010 – 5M]**

21. Prove that $(\exists x)\,(P(x) \wedge Q(x)) \Rightarrow (\exists x)\, P(x) \wedge (\exists x)\, Q(x)$. **[Oct. 2010 – 5M]**

22. Show that the following statements are equivalent. **[Oct. 2010 – 5M]**
    $A \rightarrow (B \vee C) \Leftrightarrow (A \wedge \sim B) \rightarrow C$

2 Relations and Functions

I. Introduction

In our everyday life we use the concept of Relation. Associated with a relation there is an act of comparison of objects which are related to one another.

Meaning of Relation

A relation means bridging two objects in the way that they are defined.

Examples

$$\left.\begin{array}{l}\text{Father to Son}\\ \text{Mother to Son}\\ \text{Brother to sister}\end{array}\right\}\text{General Relation}$$

$$\left.\begin{array}{l}\text{X greater than Y}\\ \text{P lesser than Q}\\ \text{K equal to M}\end{array}\right\}\text{Arithmetic Relation}$$

Any set of ordered pairs (the relation between two objects as an ordered pair.

That is the relationship could be defines as a set of all ordered pairs, in each of which first member is related to second member) defines a **Binary Relation**.

Relation defined as Ordered n-Tuple

Definition

An n-ary operation on a non-empty set A is a function f : $A^n \to A$, A^n being the product set of A. Observe the following properties that a binary operation must satisfy:

i. The n-ary operation must be defined for each n-tuple $(a_1, a_2, \ldots, a_n) \in A$.

ii. Since f is a function, only one element of A should be assigned to each n-tuple of A^n.

If n = 1, f is called unary.

If n = 2, f is called binary.

If n = 3, f is called ternary and so on.

Examples

i. The function f : $Z \to Z$, where $f(x) = -x$, is unary.

ii. f : $Z \times Z \to Z$, defined as $f(x, y) = x + y$, is binary.

iii. f : $Z \times Z \times Z \to Z$, defined as

$$\begin{aligned} f(x, y, z) &= y \quad \text{if } x \neq 0 \\ &= z \quad \text{otherwise} \end{aligned}$$

is ternary.

Notation

$<x, y> \in R$ or xRy or x is related to y by the Relation R.

Let R denote the set of real numbers.

Then $Q = \{<x^2, x> / x \in R\}$ defines the relation of the square of a real number.

Domain

Let B be a binary relation. The domain of B is the set D(B) of all objects x such that for some y, $<x, y> \in B$

$D(B) = \{x / (\exists y) (<x, y> \in B)\}$

Range

The range of a relation B denoted by R(B) is the set of all y such that for some x, $<x, y> \in B$.

$R(B) = \{y / (\exists x) (<x, y> \in B)\}$

Example

1. Consider the relation B, defined as a set of ordered pairs as

$B = \{<a, 2>, <b, 5>, <c, 8>)\}$

Solution

The domain of B is a, b, c.

The range of B is 2, 5, 8.

Relation and Cartesian Product of 2 Sets

Let X, Y be two sets and $X \times Y = \{<x, y>: x \in X \wedge y \in Y\}$ be Cartesian product of X and Y. Then any subset of $X \times Y$ defines a relation E and $D(E) \subseteq X$ and $R(E) \subseteq Y$. If X = Y then E is said to be a relation of X to X and hence $E \subseteq X \times X$.

Any relation in X is a subset of $X \times X$. The set $X \times X$ itself defines a relation in X and is called a Universal Relation in X, while the empty set which is also a subset of $X \times X$ is called a Void Relation in X.

Relation and Set Operations

If P and Q are two relations then $P \cap Q$ is also a relation defined by:

$x\,(P \cap Q)\,y \Leftrightarrow xPy \wedge xQy$

$x\,(P \cup Q)\,y \Leftrightarrow xPy \vee xQy$

$x\,(P - Q)\,y \Leftrightarrow xPy \wedge x\not{Q}y$

$x\,(\urcorner P)\,y \Leftrightarrow x\not{P}y$

Note: If x is not related to y by the relation R then it is denoted by $x\not{R}y$ or $<x, y> \notin R$.

Examples

1. **Let x = {1, 2, 3, 4}. If R = {<x, y> / x ∈ X ∧ y ∈ Y ∧ ((x – y) is an integral non-zero multiples of 3)} and S = {<x, y> / x ∈ X ∧ y ∈ Y ∧ ((x – y) is an integral non-zero multiples of 2)} then find R ∪ S and R ∩ S.**

Solution

$R = \{<1, 4>, <4, 1>\}$

$S = \{<1, 3>, <3, 1>, <2, 4>, <4, 2>\}$

$R \cup S = \{<1, 3>, <1, 4>, <2, 4>, <3, 1>, <4, 1>, <4, 2>\}$

$R \cap S = \phi$

2. **Let P = {<1, 2>, <2, 4>, <3, 3>} and Q = {<1, 3>, <2, 4>, <4, 2>} then find P ∪ Q, P ∩ Q, D(P), R(P), D(P ∪ Q), R(Q) and R(P ∩ Q).**

   Also show that D(P ∪ Q) = D(P) ∪ D(Q)

   R(P ∩ Q) ⊆ R(P) ∩ R(Q).

Solution

$P \cup Q = \{<1, 2>, <1, 3>, <2, 4>, <3, 3>, <4, 2>\}$

$P \cap Q = \{<2, 4>\}$

$D(P) = \{1, 2, 3\}$

$$\begin{aligned}
R(P) &= \{2, 4, 3\}\\
D(P \cup Q) &= \{1, 2, 3, 4\} = \{1, 2, 3\} \cup \{1, 2, 4\} = D(P) \cup D(Q)\\
R(Q) &= \{3, 4, 2\}\\
R(P \cap Q) &= \{4\} \subseteq \{1, 2, 3\} \subseteq R(P) \cap R(Q)
\end{aligned}$$

3. What are the ranges of the relations?

$S = \{<x, x^2> x \in Z_+\}$ and $T = \{<x, 2x> / x \in Z_+\}$ where Z_+ is the set $\{0, 1, 2, \dots\}$. Find $T \cup S$ and $T \cap S$.

Solution

$$\begin{aligned}
\text{Range of } S &= \{0, 1, 4, 9, 16, \dots\}\\
R(S) &= \{x^2 / x \in Z_+\}\\
\text{Range of } T &= \{0, 2, 4, 6, 8, \dots\}\\
R(T) &= \{2x / x \in Z_+\}\\
T \cup S &= \{<x, y> / x \in Z_+ \wedge y \in Z_+ \wedge ((y = 2x) \vee (y = x^2))\}\\
T \cap S &= \{<x, y> / x \in Z_+ \wedge y \in Z_+ \wedge ((y = 2x) \wedge (y = x^2))\}
\end{aligned}$$

4. Let L denote the relation "less than or equal to" and D denote the relation "divides" where x D y means "x divides y". Both L and D are defined on the set {1, 2, 3, 6} write L and D as sets and find L ∩ D.

Solution

$$\begin{aligned}
L &= \{<1,1>, <2, 2>, <3, 3>, <6, 6>, <1, 2>, <1, 3>, <1, 6>, <2, 3>, <2, 6>, <3, 6>\}\\
D &= \{<1, 1>, <2, 2>, <3, 3>, <6, 6>, <1, 2>, <1, 3>, <1, 6>, <2, 6>, <3, 6>\}\\
L \cap D &= \{<1,1>, <2, 2>, <3, 3>, <6, 6>, <1, 2>, <1, 3>, <1, 6, <2, 6>, <3, 6>\}\\
&= D \text{ because } D \subseteq L
\end{aligned}$$

Properties of Binary Relations in a Set

i. **Reflexive:** A binary relation R is reflexive in a set X, if for every $x \in X$, xRx, that is $<x, x> \in R$, which is symbolically represented as:

R is reflexive in X $\Leftrightarrow (x)\ (x \in X \rightarrow xRx)$.

Note

1. The relation $\leq$ is reflexive in the set of real no's since for any x, we have $x \leq x$.
2. The relation of inclusion is reflexive in the family of all subsets of a **Universal Set**.
3. The relation $<$ is not reflexive in the set of real numbers and the relation of proper inclusion is not reflexive in the family of subsets of a Universal Set.

ii. **Symmetric:** A relation R is symmetric in a set X, if for every x and y whenever xRy then yRx. That is, R is symmetric in X $\Leftrightarrow$

$(x)\,(y)\,(x \in X \wedge y \in X \wedge xRy \rightarrow yRx)$.

Note

1. The relation of similarity of triangles in the set of triangles in a plane is symmetric (also reflexive).
2. The relations $\leq, \geq, <, >$ are not symmetric.
3. The relations of being a brother and sister are not symmetric.
4. However in the set of males being a brother is symmetric and in the set of females being a sister is symmetric.

iii. **Transitive:** A relation R is Transitive in the set X, if for every x, y and z, whenever xRy and yRz then xRz. That is, R is Transitive in X $\Leftrightarrow$

$(x)\,(y)\,(z)\;\;(x \in X \wedge y \in X \wedge z \in X \wedge xRy \wedge yRz \rightarrow xRz)$

Note

1. The relations $\leq, \geq, <, >$ and $=$ are transitive in the set of real numbers.
2. The relations $\subseteq$, $\supseteq$, $\subset$, $\supset$ and equality are also transitive in the set of all subsets of universal set.
3. Relation of similarity of triangles in a plane is transitive.
4. Relation of being a mother is not so.

1.1 Irreflexive

A relation R in a set X is irreflexive if, for every $x \in X$, $< x, x > \notin R$

Note

1. The relation $<$ in the set of real numbers is irreflexive because for number x do we have $x < x$.
2. The relation of proper inclusion in the set of all nonempty subsets of a universal set is irreflexive.

Any relation which is not reflexive is not necessarily irreflexive and vice versa.

1.2 Antisymmetric

A relation R is antisymmetric in X if, for every x and y in X, whenever xRy and yRx, then $x = y$. It could be symbolically written as:

R is antisymmetric in X $\Leftrightarrow$

$(x)\,(y)\,(x \in X \wedge y \in X \wedge xRy \wedge yRx \rightarrow x = y)$

Note

1. It is possible to have a relation which is both symmetric and antisymmetric. This is obviously the case when each element is either related to itself or not related to any element.

2. Let R be the set of real numbers. The relations > and < in R are both irreflexive and transitive. Also the relation = (equality) in R is reflexive, symmetric and transitive.

Examples

1. If relations R and S are both reflexive, show that $R \cup S$ and $R \cap S$ are also reflexive.

Solution

Let R and S be two relations such that R and S are both reflexive. That is xRx and xSx for all $x \in X$.

We know that $x(R \cup S)\,x \Leftrightarrow xRx \vee xSx$ .... (1)

and $x(R \cap S)\,x \Leftrightarrow xRx \wedge xSx$ .... (2)

As $<x, x> \in R$ and $<x, x> \in S$ for $x \in X$ from (1) and (2)

$x(R \cup S)\,x$ and $x(R \cap S)\,x$ for all $x \in X$

$\therefore$ $R \cup S$ and $R \cap S$ are reflexive.

2. Verify whether the following relations are transitive.

$R_1 = \{<1, 1>\}$, $R_2 = \{<1, 2>, <2, 2>\}$

$R_3 = \{<1, 2>, <2, 3>, <1, 3>, <2, 1>\}$

Solution

R_1 is transitive, as it contains exactly one element and R_1 is reflexive.

$1R_22 \wedge 2R_22$, we must have $1R_22$ which is True. Therefore, R_2 is transitive.

$<1, 2> \in R_3 \wedge <2, 3> \in R_3 \rightarrow <1, 3> \in R_3$

which is True.

$<1, 2> \in R_3 \wedge <2, 1> \in R_3 \rightarrow <1, 1> \in R_3$

which is not True.

$\therefore$ R_3 is not transitive.

3. Given S = {1, 2, 3, 4} and a relation R on S defined by

$R = \{<1, 2>, <4, 3>, <2, 2>, <2, 1>, <3, 1>\}$

Show that R is not transitive. Find a relation $R_1 \supseteq R$ such that R_1 is transitive can you find another relation $R_2 \supseteq R$ which is also transitive.

Solution

Consider the elements

$<1, 2>, <2, 1>$ in R. As $1R2 \wedge 2R1$. We must have $1R1$ which is not true.

∴ R is not transitive.

$R_1 \supseteq R$ is defined by

R_1 = {<1, 1>, <1, 2>, <2, 1>, <2, 2>, <3, 1>, <3, 2>, <4, 3>} is transitive.

R_2 = {<1, 1>, <1, 2>, <2, 1>, <2, 2>, <3, 1>, <3, 2>, <4, 3>, <3, 4>, <4, 4>} such that $R_2 \supseteq R_1 \supseteq R$ is also transitive.

4. Given S = {1, 2, ..., 10} and a relation R on S where R = {<x, y> / x + y = 10}. What are the properties of the relation R?

Solution

Relation R is not reflexive because <1, 1>, <2, 2>, <3, 3> ∉ R.

R is irrflexive because <5, 5> ∈ R

R = {<5, 5> / 5 + 5 = 10}

R is symmetric because xRy → yRx but not antisymmetric the relation R is not transitive, because R is both irreflexive and symmetric.

5. Let Z be the set of integers and let aRb; b is a multiple of a. Determine which of the five properties are satisfied by R.

1

PU
Oct. 2009 – 5M

Solution

We have

R = {(a, b) | a is multiple of b, a, b, ∈ Z}

Properties

i. The relation R defined on 2 is reflexive because a = 1.a.

(a, a) ∈ R ∀ a ∈ Z

ii. The relation R defined on Z is not symmetric because if b = k a for some k ∈ Z, then (a, b) ∈ R but

$a = \frac{1}{k} b = k' b$ but $k' \notin Z$ for ∀ a ∈ Z

∴ (b, a) ∉ R

iii. The relation R defined on Z is transitive because if (a, b) ∈ R then b = k a, for some k ∈ Z and (b, c) ∈ R then c = k' b for some k' ∈ Z; ∴ c = k' . k . a = k'' a where k'' = k' . k ∈ Z ∀ k', k ∈ Z.

∴ if (a, b) and (b, c) ∈ R then (a, c) ∈ R, for every a, b, c ∈ Z.

iv. The relation R defined on Z is not irreflexive because ∀ a ∈ Z, (a, a) ∈ R.

v. The relation R defined on Z is anti-symmetric, because for every a, b ∈ Z, whenever aRb and bRa then a = b.

1.3 Relation Matrix and the Graph of a Relation

A relation R from a finite set A to a finite set B can be represented by a matrix which is called Relation Matrix.

Construction of relation matrix for a given two finite sets with relation R

Let A = $\{a_1, a_2, \ldots, a_p\}$ and B = $\{b_1, b_2, \ldots, b_q\}$ be two finite sets. Let R be a relation from A to B. Then the relation matrix of R is obtained by constructing a table whose columns are preceded by a column containing the successive elements of A and whose rows are leaded by a row containing the successive elements of B. If a_iRb_j then enter 1 otherwise enter 0 in the i^{th} and j^{th} column.

Consider the relation R $\{<a_1, b_1>, <a_1, b_3>, <a_2, b_3>, <a_3, b_3>, <a_3, b_4>, <a_2, b_1>\}$. Then the relation matrix R represented as follows:

R	b_1	b_2	b_3	b_4
a_1	1	0	1	0
a_2	0	0	1	0
a_3	0	0	1	1

∴ The relation matrix of R is

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

If we assume A contains m elements and B contains n elements, then the relation matrix M_R of the type m × n, of the relation R from A to B is given by the relation.

$$\begin{aligned} r_{ij} &= 1 \text{ if } a_iRb_j \\ &= 0 \text{ if } a_i \not R b_j \end{aligned}$$

where, r_{ij} is i^{th} row and j^{th} column of the matrix M_R.

i. One can obtain a relation matrix when a relation is given and also obtain the relation if the relation matrix is given.

ii. The relation matrix reflects some of the properties of the relation in a set.

   a. If the relation is reflexive, then all diagonal elements of a relation matrix are 1.

   b. If the relation is symmetric, then relation matrix is symmetric.

   c. If the relation is antisymmetric then the relation matrix is such that if $r_{ij} = 1$ then $r_{ji} = 0$ for $i \neq j$

Representation of Relations using Graphs

A relation can be expressed pictorially by drawing its graph.

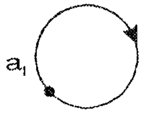
Let R be a relation defined on a set A = $\{a_1, a_2, \ldots, a_m\}$. The elements of A are represented by points or small circles called nodes or vertices.

The nodes or vertices corresponding to the elements a_iRa_j in A then in the graph the corresponding nodes or vertices a_i are connected by a directed arc from a_i to a_j. The graph thus obtained is "relation graph" which could be denoted by G_R.

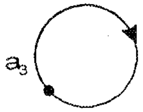
1. Consider the relation R = {<a_1, a_1>, <a_2, b_2>, <b_2, a_2>, <a_3, a_3>}. Find the graph G_R.

Solution

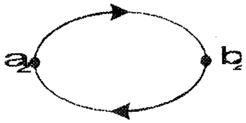
Let R = {<a_1, a_1>, <a_2, b_2>, <b_2, a_2>, <a_3, a_3>}



a_1 is joined to a_1 by a directed arc without passing through any other node, which we call it a loop.



a_3 is joined to a_3 by a directed arc, which is also a loop.



The node a_2 is joined to b_2 be a directed arc from a_2 to b_2 and the node b_2 is joined to a_2 by a directed arc a_2.

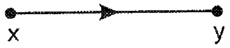
2. Represent the following symbolic expressions as graphical structures.

a.	**xRy**	**b.**	**xRx**
c.	**xRy ∧ yRx**	**d.**	**xRy ∧ yRz ∧ zRx**
e.	**xRy ∧ yRy**	**f.**	**xRx ∧ xRy ∧ yRy**

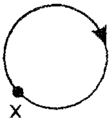
Solution

The corresponding graphs are:

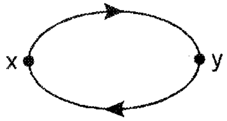
a.



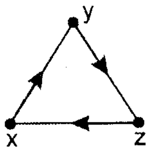
b.



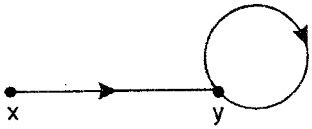
c.



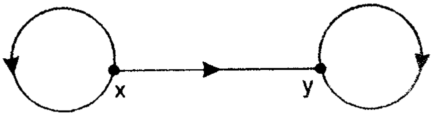
d.



e.



f.



Note

i. If a relation is reflexive then at each node there is a loop.

ii. If a relation is irreflexive then there is no loop at each node.

iii. If the relation is symmetric then if one node joined to another by a directed arc then there is a reverse arc joining those two nodes.

iv. For a relation which is antisymmetric, between any two nodes of the relation graph there exists at most one directed arc between them. That is, for any two nodes a, b either a is joined to b by a directed arc from a to b or b is joined to a by a directed arc from a to b.

v. The properties such as reflexive, symmetric, irreflexive and antisymmetric of a relation could be easily identified from the relation graph.

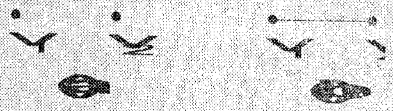
3. Draw all non-isomorphic graphs on 2 and 3 vertices.

1

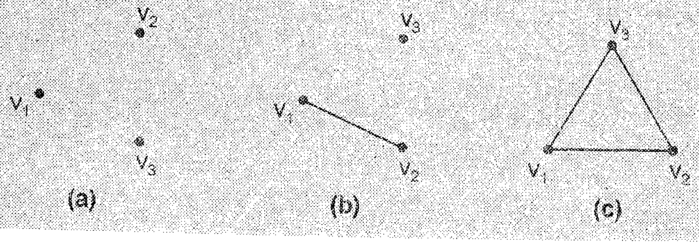
PU
Oct. 2009 – 4M

Solution

Two vertices,



Three vertices,



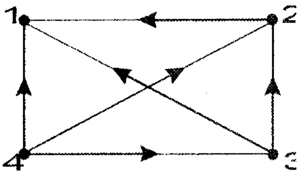
4. Let X = {1, 2, 3, 4} and R = {<x, y> / x > y}. Draw the graph of R and also give its matrix.

Solution

The relation R contains the elements {<2, 1>, <3, 1>, <4, 1>, <3, 2>, <4, 2>, <4, 3>}

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

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



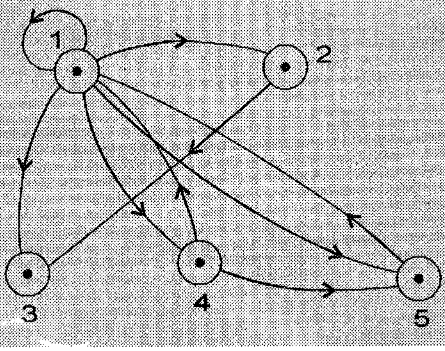
5. **For a set A = {1, 2, 3, 4, 5}, the relation matrix is**

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

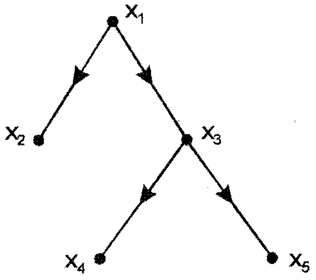
Draw its diagraph.

PU
Oct. 2009 – *5M*
1

Solution



6. **Determine the properties of the relations given by the graphs and also write the corresponding relation matrices.**

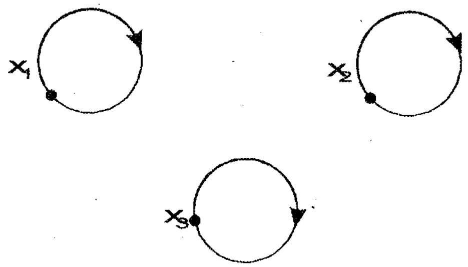


Solution

The relation given by the graph is irreflexive, antisymmetric.

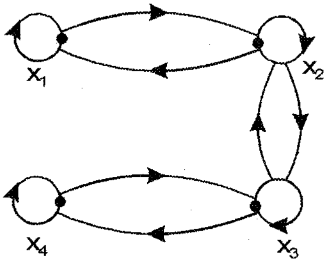
There is no loop at each node – irreflexive. Between any 2 nodes of the relation graph ∃ atmost one directed arc between them – Antisymmetric.

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



The relation given by the graph is reflexive. [At each node there is a loop - reflexive].

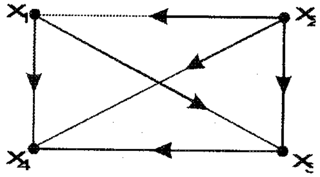
$$M_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$



The relation given by the graph is reflexive and symmetric.

[At each node there is a loop - reflexive. If one node joined to another node by a directed arc then there is a reverse arc joining those two nodes].

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



The relation given by the graph is antisymmetric, irreflexive and transitive.

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

1.4 Partition and Covering of a Set

Let S be a given set and T = $\{T_1, T_2, \ldots, T_n\}$ where each T_i for i = 1, 2, …, n is a subset of S and $\bigcup_{i=1}^{n} T_i = S$. Then T is said to be a covering of S and the sets $T_1, T_2, \ldots, T_n$ are said to cover S.

If each of above T_i for i = 1, 2, …, n is mutually disjoint then T is said to be a partition of S and the sets $T_1, T_2, \ldots, T_n$ are called the blocks of the partition.

Examples

1. **Consider the set S = {1, 2, 3} and the following collection of subsets of S**

$A_1 = \{\{1, 2\}, \{1, 3\}\}$
$A_2 = \{\{1\}, \{1, 3\}\}$
$A_3 = \{\{1\}, \{2, 3\}\}$
$A_4 = \{\{1, 2, 3\}\}$
$A_5 = \{\{1\}, \{2\}, \{3\}\}$
$A_6 = \{\{1\}, \{1, 2\}, \{1, 3\}\}$

Solution

The sets A_1 and A_6 are covering of S while A_3, A_4, A_5 are partitions of S. The set A_2 is neither a covering nor a partition of S.

2. **Consider the set S = {1, 2, 3, 4, 5, 6} and the following collection of subsets of S.**

$A_1 = \{\{1, 3\}, \{2, 5\}, \{4, 6\}, \{5, 6\}\}$
$A_2 = \{\{1, 2, 3\}, \{4, 5, 6\}\}$
$A_3 = \{\{1, 3, 5, 6\}, \{2, 4\}\}$
$A_4 = \{\{1, 2\}, \{2, 4\}, \{3, 5\}, \{6\}\}$

Solution

The sets A_1 and A_4 are covering of S while A_2, A_3 are partitions of S.

Note

i. A partition of a set S is covering but not the converse.

ii. If cardinality of a set S is n, then any partition of S can contain at most n blocks.

Two partitions are said to be equal if they are equal as sets.

Note: If a set S is finite, then every partition is a finite partition. Each partition contains only finite number of blocks.

Partition of Universal Set

Let S be a subset of universal set E. Then $S \cup \sim S = E$ is a partition.

Let S and T be two subsets of E and consider the sets.

$A_0 = \sim S \cap \sim T$, $A_1 = \sim S \cap T$, $A_2 = S \cap \sim T$, $A_3 = S \cap T$

The subsets A_0, A_1, A_2, A_3 are mutually disjoint and

$$E = A_0 \cup A_1 \cup A_2 \cup A_3 = \bigcup_{i=0}^{3} A_i$$

The sets A_0, A_1, A_2, A_3 are called complete intersection or minterms generated by S and T.

The complete intersection or the minterms are blocks of a partition of E generated by S and T.

Let R, S, T be 3. Subset of E and consider the sets.

$A_0 = \sim R \cap \sim S \cap \sim T$ $A_1 = \sim R \cap \sim S \cap T$

$A_2 = \sim R \cap S \cap \sim T$ $A_3 = \sim R \cap S \cap T$

$A_4 = R \cap \sim S \cap \sim T$ $A_5 = R \cap \sim S \cap T$

$A_6 = R \cap S \cap \sim T$ $A_7 = R \cap S \cap T$

Clearly A_i's for $i = 0, 1, 2, \ldots, 7$ are mutually disjoint and $\bigcup_{i=1}^{7} A_i = E$ and hence A_i's; $i = 0, 1, 2, \ldots, 7$ are called minterms of R, S T.

In the case of single subset of E, number of minterms is $2^1 = 2$.

In the case of two subsets of E, number of minterms are $2^2 = 4$.

In the case of n subsets the number of minterms are 2^n which are $A_0, A_1, \ldots, A_{2^n - 1}$.

1.5 Equivalence Relation

A relation R in a set of X is called an equivalence relation if it is reflexive, symmetric and transitive.

Note: If R is an equivalence in X, then the domain of R is X itself. Therefore R will be called a relation on X.

Examples

i. Equality of numbers on a set of real numbers.

ii. Equality of subsets of a universal set.

iii. Similarity of triangles on the set of triangles.

iv. Relation of lines being parallel on a set of lines in a plane.

v. Relation of living in the same town on the set of persons living in Canada.

vi. Relation of statements being equivalence in the set of statements.

Examples

1. **Let A = {a, b, c, d}, R = {<a, a>, <b, a>, <b, b>, <c, c>, <d, d>, <d, c>}. Determine whether R is an equivalence relation.**

Solution

R is reflexive since <a, a>, <b, b>, <c, c> and <d, d> ∈ R.

But R is not symmetric since <b, a> ∈ R but <a, b> ∉ R.

Hence R is not an equivalence relation.

2. A relation R = { <1, 1>, <1, 2>, <1, 4>, <2, 1>, <2, 2>, <3, 3>, <4, 4>} defined over the set A = {1,2,3,4}. Is R an equivalence Relation?

1
PU
Oct. 2008 – *6M*

Solution

To check that R is an equivalence Relation, we check three conditions

i. Reflexivity

Now $\forall$ a $\in$ A,<a, a> $\in$ R i.e. <1,1>, <2, 2>, <3, 3>, and <4, 4> $\in$ R

$\therefore$ R is reflexive (i.e. every element is related to itself).

ii. Symmetric

R is not symmetric because <1, 4>, $\in$R $\not\Rightarrow$ <4, 1> $\in$R

i.e. <a, b> $\in$R $\not\Rightarrow$<b, a> $\in$R

Hence R is not symmetric.

iii. Transitivity

R is not transitive because $\forall$ a, b, c $\in$ A

If <a, b>, $\in$R, <b, c>, $\not\Rightarrow$ <a, c> $\in$ R

i.e. <1, 2>, <2, 1>, $\in$R $\not\Rightarrow$ <1, 1> $\in$R

but <2,1>, <1, 4>, $\in$R $\not\Rightarrow$ <2, 4> $\in$R.

Hence R is not Equivalence Relation.

3. If {(1,3,5), (2,4)} is a partition set of the set A = {(1,2,3,4,5}. Determine the corresponding equivalence relation.

1
PU
Apr. 2010 – *5M*

Solution

Here partition P = {P_1, P_2} where P_1 = <1, 3, 5>, P_2 = <2, 4> then equivalence relation on A is,

R = ($P_1 \times P_1$) $\cup$ ($P_2 \times P_2$)

Now $P_1 \times P_1$ = {1, 3, 5} × {1, 3, 5}

= {<1,1>, <1, 3>, <1, 5>, <3, 1>, <3,3>, <3, 5> <5, 1>, <5, 3>, <5, 5>}

$P_2 \times P_2$ = {2, 4} × {2, 4}

= {<2, 2>, <2, 4>, <4, 2> <4, 4>}.

4. Let A = {1, 2, 3, 4, 5, 6, 7} Determine a relation R on A by aRb iff 3 divides (a – b). Show that R is an equivalence relation. Also determine the partition generated by R.

1
PU
Apr. 2010 – *5M*

Solution

i. $\forall$ a $\in$ A,

3 divides (a – a)

$\therefore$ a R a, i.e., R is reflexive.

ii. If $3|(a-b)$ for any $a, b \in A$ then

$(a-b) = 3k$ for some $k \in Z$

i.e. $b - a = -3k$

i.e. $b - a = 3k'$ where $k' = -k \in Z$

$\therefore 3|(b-a)$

i.e., If 3 divides $(a-b)$ then 3 also divides $(b-a)$

i.e., If aRb then bRa so R is symmetric.

iii. If $3|(a-b)$ and $3|(b-c)$ for any $a, b, c \in A$

then

$(a-b) = 3k_1$, $(b-c) = 3k_2$ for some $k_1, k_2 \in Z$

$(a-b) + (b-c) = 3k_1 + 3k_2$

i.e. $a - c = 3(k_1 + k_2)$

$= 3k_3$ where $k_3 = k_1 + k_2 \in Z$

$\therefore 3|(a-c)$

i.e., if aRb and bRc then aRc so R is transitive and hence R is an equivalence relation.

$R = \{(1, 4)\ (4, 1)\ (2, 5)\ (5, 2)\ (3, 6), (6, 3)\ (4, 7)\ (7, 4)\ (1,7)\ (7, 1)\}$

$\therefore P = \left\{\underset{P_1}{(1, 4, 7)}, \underset{P_2}{(2, 5)}, \underset{P_3}{(3, 6)}\right\}$

5. Let A = {1, 2, 3, 4, 5, 6}, Let R = {(a, b) | a ≡ b mod 2}. Is R an equivalence relation?

1

PU
Oct. 2010 – 5M

Solution

$R = \{(a, b) \mid a \equiv b \bmod 2\}$

i. $a \equiv a \pmod 2$ $\forall a \in R.$

i.e. $(a, a) \in R$ $\forall a \in A$, so R is reflexive.

ii. If $a \equiv b \pmod 2$

then $2|(a-b)$ i.e. $a - b = 2k$ for $k \in Z$

$\therefore b - a = -2k$

$= 2k'$ where, $k' = -k \in Z$

$\therefore 2 | (b-a)$

$\therefore b \equiv a (\bmod 2)$ $\forall b, a \in A$

$\therefore$ R is symmetric.

iii. If $a \equiv b (\bmod 2)$ and $b \equiv c \pmod 2$

for $a, b, c \in A$

then $2|(a-b)$ and $2|(b-c)$

$\therefore a - b = 2k_1$ and $b - c = 2k_2$, where, $k_1, k_2 \in Z$

$\therefore$ a – b + b – c = $2k_1 + 2k_2$

i.e., a – c = $2(k_1 + k_2)$

= $2k_3$ $\quad$ $k_3 = k_1 + k_2 \in Z$

$\therefore 2 \mid (a - c)$

$\therefore a \equiv c \pmod 2$

$\therefore$ R is transitive on A.

Hence R is an equivalence relation on A.

6. Let A = {a, b, c} and let

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

Determine whether R is an equivalence relation.

Solution

R = {<a, a>, <b, b>, <c, b>, <c, c>}

R is reflexive since <a, a>, <b, b>, <c, c> ∈ R

R is symmetric since <b, c> ∈ R → <c, b> ∈ R

R is transitive since

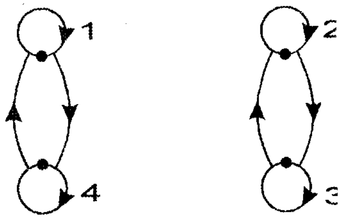
<b, b> and <b, c> ∈ R implies <b, c> ∈ R
<b, c> and <c, b> ∈ R implies <b, b> ∈ R
<c, c> and <c, b> ∈ R implies <c, b> ∈ R
<c, b> and <b, b> ∈ R implies <c, b> ∈ R
<c, b> and <b, c> ∈ R implies <c, c> ∈ R
<b, c> and <c, c> ∈ R implies <b, c> ∈ R

Hence R is an equivalence relation.

7. Let X = {1, 2, 3, 4} and R = {<1, 1>, <1, 4>, <4, 4>, <4, 1>, <2, 2>, <2, 3>, <3, 2>, <3, 3>}. Write the matrix of R and sketch its graph.

Solution

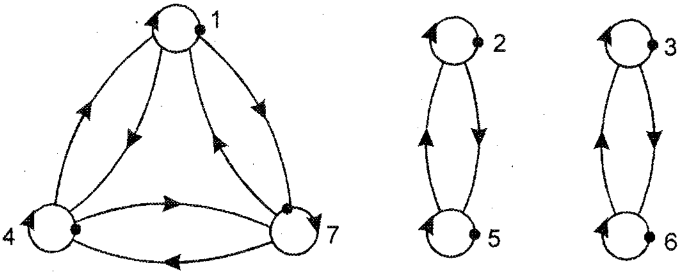
$$M_R = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$



8. Let X = {1, 2, ..., 7} and R = {<x, y> / x – y is divisible by 3}. Show that R is an equivalence relation. Draw the graph of R.

Solution

R = {<1, 1>, <1, 4,>, <1, 7>, <2, 2>, <2, 5>, <3, 3>, <3, 6>, <4, 1>, <4, 4>, <4, 7>, <5, 2>, <5, 5>, <6, 3>, <6, 6>, <7, 1>, <7, 4>, <7, 7>}.



Reflexive: For every x ∊ R, x – x is divisible by 3 and hence xRx.

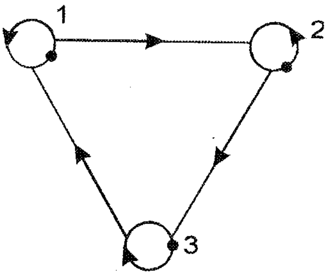
Symmetry: Let xRy then x – y is divisible by 3 and hence y – x is also divisible by 3. Therefore yRx.

xRy ⇒ yRx

Transitive: Let xRy and yRz, then both (x – y) and (y – z) are divisible by 3, so that x – z = (x – y) + (y – z) is divisible by 3 and hence xRz.

∴ R is an equivalence relation.

9. Determine whether the relation r whose diagraph is given below is an equivalence relation.



Solution

R is reflexive since there is a loop at each node.

But R is not symmetric since (1, 2) ∊ R but (2, 1) ∉ R.

Hence R is not an equivalence relation.

10. Let I denote the set of all positive integers and let m be a positive integer. For x ∊ I and y ∊ I, define R as

R = {<x, y> / x – y is divisible by m}

Solution

"x – y is divisible by m" is equivalent to the statement that both x and y have the same remainder when each is divided by m. x ≡ y (mod m) which is read as "x equals y modulo m". The relation ≡ is also called a congruence relation.

1.6 Equivalence Classes

Let R be an equivalence relation on a set X. For any $x \in X$, the set $[x]_R \subseteq X$ given by $[x]_R = \{y / y \in X \wedge xRy\}$ is called an R-equivalence class generated by $x \in X$.

Examples

1. **Let A = {1, 2, 3, 4} and let R = {<1, 1>, <1, 2>, <1, 3>, <2, 1>, <2, 2>, <3, 1>, <2, 3>, <3, 2>, <3, 3>, <4, 4>}. Show that R is an equivalence relation and determine the equivalence classes.**

Solution

R is reflexive since <1, 1>, <2, 2>, <3, 3>, <4, 4> ∈ R

R is symmetric since both <1, 2>, <2, 1> ∈ R

Similarly <2, 3>, <3, 2> ∈ R and <1, 3>, <3, 1> ∈ R

R is transitive since <1, 2> and <2, 1> ∈ R implies <1, 1> ∈ R

<1, 3>, <3, 1> ∈ R → <1, 1> ∈ R

<2, 3>, <3, 2> ∈ R → <2, 2> ∈ R

<3, 1>, <1, 3> ∈ R → <3, 3> ∈ R

<3, 2>, <2, 1> ∈ R → <3, 1> ∈ R

Hence R is an equivalence relation. The equivalence classes of A are:

$$[1]_R = \{1, 2, 3\}$$
$$[2]_R = \{1, 2, 3\}$$
$$[3]_R = \{1, 2, 3\}$$
$$[4]_R = \{4\}$$

Here two distinct equivalence classes.

2. **Let Z be the set of integers and let R be the relation called "congruence modulo 3" defined by $R = \{<x, y> / x \in Z \wedge y \in Z \wedge (x - y)$ is divisible by 3}. Determine the equivalence classes generated by the elements of Z.**

Solution

The equivalence classes are:

$$[0]_R = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1]_R = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2]_R = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$
$$[Z]_R = \{[0]_R, [1]_R, [2]_R\}$$

This way we can find the equivalence classes generated by a relation "congruence modulo m" for any integer m.

1.7 Quotient Set

Let R be an equivalence relation on A. We denote by $\frac{A}{R}$ the partition induced by R. Hence partition of A is called a quotient set of A.

1. Let A = {1, 2, 3} and let R = {<1, 1>, <2, 2>, <1, 3>, <3, 1>, <3, 3>}. Find $\frac{A}{R}$.

Solution

$\frac{A}{R}$ is the partition of A induced by R.

Hence, $\frac{A}{R} = \{\{1, 3\}, \{2\}\}$

2. Let Z be the set of integers. Define a relation R on Z as aRb iff $\frac{6}{(a-b)}$, show that R is an equivalence relation and find $\frac{Z}{R}$.

Solution

Since $\frac{6}{(a-a)}$, a R a. Hence, R is reflexive.

If $\frac{6}{(a-b)}$, then $\frac{6}{(b-a)}$, which shows that R is symmetric.

If $\frac{6}{(a-b)}$ and $\frac{6}{(b-c)}$ then obviously $\frac{6}{((a-b)+(b-c))}$ i.e. $\frac{6}{(a-c)}$. Hence, R is transitive.

∴ R is an equivalence relation.

$\frac{Z}{R} = \{[0]_R, [1]_R, [2]_R, [3]_R, [4]_R, [5]_R\}$

where,
$$[0]_R = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$$
$$[1]_R = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$$
$$[2]_R = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$$
$$[3]_R = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$$
$$[4]_R = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$$
$$[5]_R = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$$

The quotient set $\frac{Z}{R}$ is denoted by Z_6 and is called the set of congruence classes modulo 6. R is also called a congruence relation.

1.8 Compatible Relation

A relation R in X is said to be compatible, if it is reflexive and symmetric.

Note

i. From the definition of compatible relation every equivalence relation is compatible but the converse is not true.

ii. Although an equivalence relation on a set defines a partition of the set into equivalence classes, a compatibility relation does not necessarily define a partition. However, a compatibility relation does define a covering of the set.

1.9 Maximal Compatibility Block

Let X be a set and $\approx$ a compatibility relation on X. A subset $A \subseteq X$ is called a maximal compatibility block if any element of A is compatible to every other element of A and no element of $X - A$ is compatible to all the elements of A.

Note: To find the maximal compatibility blocks corresponding to a compatibility relation on a set X, first we draw a simplified graph of the compatibility relation and pick from this graph the largest complete polygons. A polygon in which any vertex is connected to every other vertex.

Example

1. A triangle is always a complete polygon.
2. But for a quadrilateral to be a complete polygon we must have the two diagonals present.

Example

1. Let X = {ball, bed, dog, let, egg} and let the relation R be given by

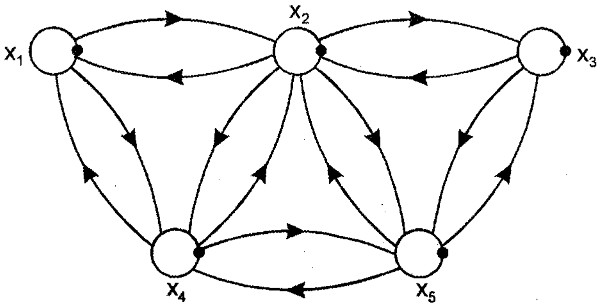
R = {<x, y> / x, y ∈ X ∧ xRy if x and y contain some common letter}.

Solution

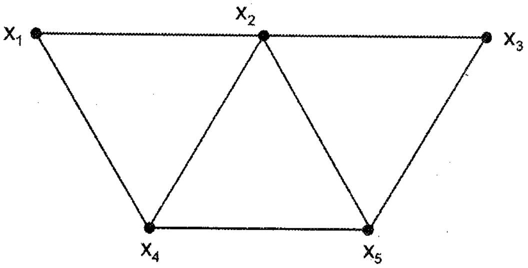
$$X = \left\{ \overset{x_1}{\text{ball}}, \overset{x_2}{\text{bed}}, \overset{x_3}{\text{dog}}, \overset{x_4}{\text{let}}, \overset{x_5}{\text{egg}} \right\}$$

R = $\{<x_1, x_1>, <x_1, x_2>, <x_1, x_4>, <x_2, x_2>, <x_2, x_1>, <x_2, x_3> <x_2, x_4>, <x_2, x_5> <x_3, x_3>,$

$<x_3, x_2>, <x_3, x_5>, <x_4, x_4>, <x_4, x_1>, <x_4, x_2>, <x_4, x_5>, <x_5, x_5> <x_5, x_2>, <x_5, x_3>, <x_5, x_4>\}$



G_R

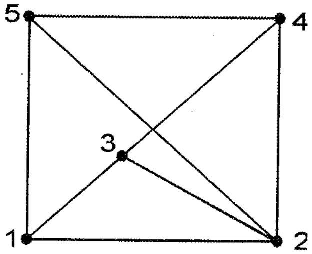


Simplified Graph

The maximal compatibility blocks are $\{x_1, x_2, x_4\}$, $\{x_2, x_4, x_5\}$, $\{x_2, x_3, x_5\}$

These sets are not mutually disjoint, they only define a covering of X.

2. **Consider the diagram given below for the compatible relation R on the set. A = {1, 2, 3, 4, 5}**



Solution

The maximal compatibility blocks are $M_1 = \{1, 2, 3\}$, $M_2 = \{2, 3, 4\}$, $M_3 = \{1, 2, 5\}$, $M_4 = \{2, 4, 5\}$.

$$A = M_1 \cup M_2 \cup M_3$$

Hence $\{M_1, M_2, M_3\}$ forms a covering for A $\{M_1, M_4\}$, $\{M_2, M_3\}$ forms a covering for A.

Note

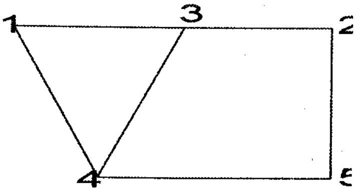
i. Any element of the set which is related only to itself forms a maximal compatibility block.

ii. Any two elements which are compatible to one another but to no other elements also form a maximal compatibility block.

3. **Let the compatibility relation on a set $\{x_1, x_2, \ldots, x_5\}$ be given by the matrix**

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

Solution



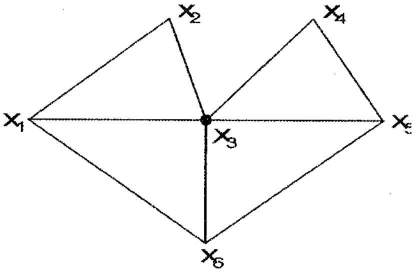
The maximal compatibility blocks are {1, 3, 4}, {2, 3}, {4, 5}, {2, 5}

4. Let the compatibility relation on a set {$x_1, x_2, \ldots, x_6$} be given by the matrix.

$$\begin{array}{c|ccccc}
x_2 & 1 & & & & \\
x_3 & 1 & 1 & & & \\
x_4 & 0 & 0 & 1 & & \\
x_5 & 0 & 0 & 1 & 1 & \\
x_6 & 1 & 0 & 1 & 0 & 1 \\
\hline
 & x_1 & x_2 & x_3 & x_4 & x_5
\end{array}$$

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

Solution



The maximal compatibility blocks are {x_1, x_2, x_3}, {x_1, x_3, x_6}, {x_3, x_4, x_5}, {x_3, x_5, x_6}

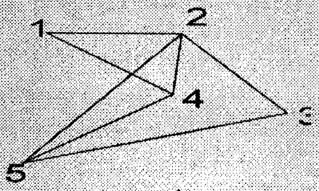
5. The compatibility relation on a set {1, 2, 3, 4, 5} be given by the following matrix.

1
PU
Oct. 2010 – *5M*

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

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

Solution



The maximal compatibility blocks are {1, 2, 4} {2, 4, 5}, {2, 3, 5}.

6. The compatibility relation on a set $\{x_1, x_2, \ldots\ldots x_6\}$ be given by the matrix.

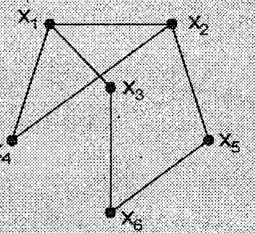
1

PU
Apr. 2010 – *5M*

$$\begin{array}{c|ccccc} x_2 & 1 & & & & \\ x_3 & 1 & 0 & & & \\ x_4 & 1 & 1 & 0 & & \\ x_5 & 0 & 1 & 0 & 0 & \\ x_6 & 0 & 0 & 1 & 0 & 1 \\ \hline & x_1 & x_2 & x_3 & x_4 & x_5 \end{array}$$

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

Solution



Maximal compatibility blocks of the relation are $\{x_1, x_2, x_4\}$, $\{x_1, x_3\}$ $\{x_2, x_5\}$ $\{x_3, x_6\}$ $\{x_5, x_6\}$

7. Let A = {a, b, c, d, e} and P = {{a, b}, {c}, {d, e}}. Show that the partition P defines an equivalence relation on A.

Solution

$$P = \{\overset{P_1}{\{a, b\}}, \overset{P_2}{\{c\}}, \overset{P_3}{\{d, e\}}\}$$

$R = (P_1 \times P_1) \cup (P_2 \times P_2) \cup (P_3 \times P_3)$ where

$P_1 = \{a, b\}, P_2 = \{c\}, P_3 = \{d, e\}$

$P_1 \times P_1 = \{a, b\} \times \{a, b\}$

$= \{<a, a>, <a, b>, <b, a>, <b, b>\}$

$P_2 \times P_2 = \{c\} \times \{c\}$

$= \{<c, c>\}$

$P_3 \times P_3 = \{d, e\} \times \{d, e\}$

$= \{<d, d>, <d, e>, <e, d>, <e, e>\}$

$R = \{<a, a>, <a, b>, <b, a>, <b, b>, <c, c>, <d, d>, <d, e>, <e, d>, <e, e>\}$

The relation is reflexive, symmetric and transitive and hence an equivalence relation.

8. Prove that the relation "congruence modulo m" given by $\equiv \{<x, y> / x - y$ is divisible by m$\}$ over the set of positive integers is an equivalence relation. Also show that if $x_1 \equiv y_1$ and $x_2 \equiv y_2$, then $(x_1 + x_2) \equiv (y_1 + y_2)$.

Solution

i. For any $a \in X$, $a - a$ is divisible by m; hence a R a or R is reflexive.

ii. For any $a, b \in X$, if $a - b$ is divisible by m, then $b - a$ is also divisible by m that is, $aRb \Rightarrow bRa$. Thus R is symmetric.

iii. For $a, b, c \in X$, if aRb and bRc, then both $a - b$ and $b - c$ are divisible by m so that $a - c = (a - b) + (b - c)$ is also divisible by m and hence aRc.

Thus R is transitive.

To prove that $(x_1 + x_2) \equiv (y_1 + y_2)$

Given that $x_1 \equiv y_1$ ....(1)

$x_2 \equiv y_2$ ....(2)

From (1) we will get $\dfrac{(x_1 - y_1)}{m}$

From (2) $\dfrac{(x_2 - y_2)}{m}$

Adding the above equations we will get

$$x_1 + x_2 \equiv y_1 + y_2$$

9. Let R denote a relation on the set of ordered pairs of positive integers such that<x, y> R <u, v> iff xv = yu. Show that R is an equivalence relation.

Solution

Reflexive: <x, y> R <x, y> iff xy = yx i.e., xy = xy

Symmetry: <x, y> R <u, v> iff xv = yu

Also yu = vx i.e., <u, v> R <x, y>

Transitive: <x, y> R <u, v> and <u, v> R <w, s> then

xv = yu and us = vw

Multiplying the corresponding terms

$$\langle x\ \cancel{v}\rangle \langle \cancel{u}\ s\rangle = \langle y\ \cancel{u}\rangle \langle \cancel{v}\ w\rangle$$

$$xs = yw$$

<x, y> R <w, s>

10. Given a set S = {1, 2, 3, 4, 5} find the equivalence relation on S which generates the partition { $\overline{1, 2}$, $\overline{3}$, $\overline{4, 5}$ }. Draw the graph of the relation.

Solution

$$S = \{\overset{S_1}{\{1, 2\}}, \overset{S_2}{\{3\}}, \overset{S_3}{\{4, 5\}}\}$$

$$R = (S_1 \times S_1) \cup (S_2 \times S_2) \cup (S_3 \times S_3) \text{ where } S_1 = \{1, 2\}, S_2 = \{3\}, S_3 = \{4, 5\}$$

$$S_1 = \{1, 2\}$$

$$S_1 \times S_1 = \{1, 2\} \times \{1, 2\} = \{<1, 1>, <1, 2>, <2, 1>, <2, 2>\}$$

$$S_2 \times S_2 = \{3\} \times \{3\} = \{<3, 3>\}$$

$$S_3 \times S_3 = \{4, 5\} \times \{4, 5\}$$

$$= \{<4, 4>, <4, 5>, <5, 4>, <5, 5>\}$$

$$R = \{<1, 1>, <1, 2>, <2, 1>, <2, 2>, <3, 3>, <4, 4>, <4, 5>, <5, 4>, <5, 5>\}$$

The relation is reflexive, symmetry and transitive and hence an equivalence relation.

1.10 Composition of Binary Relations

Let R be relation from X to Y and S be a relation from Y to Z. Then a relation denoted by $R \circ S$ is called a composite relation of R and S where,

$$R \circ S = \{<x, z> / x \in X \wedge z \in Z \wedge (\exists y)\,(y \in Y) \wedge <x, y> \in R \wedge <y, z> \in S\}$$

The operation of obtaining $R \circ S$ from R and S is called composition of relations.

Let P be a relation from X to Y, R be a relation from Y to Z and S be a relation from Z to W then $(P \circ R) \circ S$ and $P \circ (R \circ S)$ are binary relations from X to W and

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

Examples

1. **Let R = {<1, 2>, <3, 4>, <2, 2>} and S = {<4, 2>, <2, 5>, <3, 1>, <1, 3>}. Find R ∘ S, S ∘ R, R ∘ (S ∘ R), (R ∘ S) ∘ R, S ∘ S and R ∘ R ∘ R.**

Solution

$$R \circ S = \{<1, 5>, <3, 2>, <2, 5>\}$$

$$S \circ R = \{<4, 2>, <3, 2>, <1, 4>\}$$

$$R \circ (S \circ R) = \{<3, 2>\}$$

$$(R \circ S) \circ R = \{<3, 2>\}$$

$$R \circ R = \{<1, 2>, <2, 2>\}$$

$$S \circ S = \{<4, 5>, <3, 3>, <1, 1>\}$$

$$R \circ R \circ R = \{<1, 2>, <2, 2>\}$$

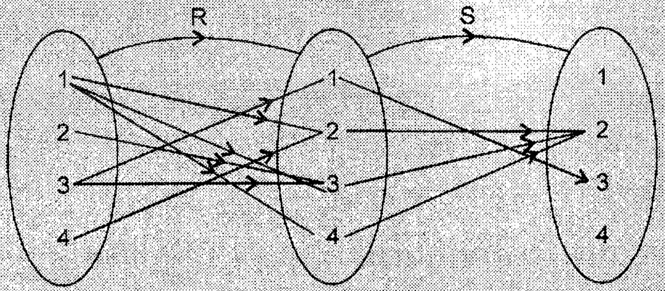
2. **Let A = {1, 2, 3, 4} Let R = {<1, 2>, <1, 3>, <1, 4>, <1, 4>, <2, 3>, <3, 3>, <4, 2>, and S={<1, 3>, <2, 2>, <3, 2>, <4, 2>} Find:**
   - **i. R ∘ (S ∘ S).**
   - **ii. Is R ∘ S = S ∘ R?**
   - **iii. R ∘ R ∘ R**

1

PU
Oct. 2008 – 6M

Solution

i. $R \circ (S \circ S)$.



$$S \circ S = \{(1, 2), (2, 2), (3, 2), (4, 2)\}$$

$$R \circ (S \circ S) = \{(1, 2), (2, 2), (3, 2), (4, 2)\}$$

ii. Is $R \circ S = S \circ R$?

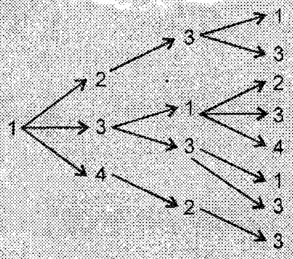
Now $R \circ S = \{(1, 2), (2, 2), (3, 3), (3, 2), (4, 2)\}$

$S \circ R = \{(1, 1), (1, 3), (2, 3), (3, 3), (4, 3)\}$

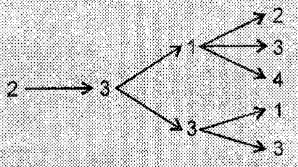
$\therefore R \circ S \neq S \circ R$.

iii. $R \circ R \circ R$

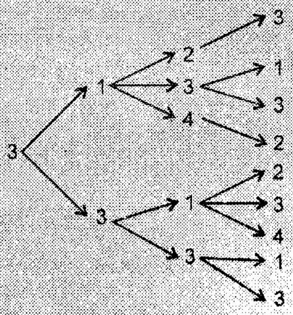
$R \circ R \circ R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (2, 1), (3, 1), (3, 2), (3, 3), (3, 4), (4, 3), (4, 1)\}$



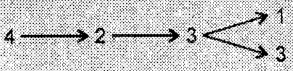
(1,1), (1,2), (1,3), (1,4)



(2,2), (2,1), (2,3), (2,4)



(3,1), (3,2), (3,3), (3,4)



(4,1), (4,3)

3. Let R and S be the following relations on B = {a, b, c, d}, R = {(a, a), (a, c), (c, b), (c, d) (d, b)} and S = {(b, a), (c, c), (c, d), (d, a)}

Find the following composite relations.

i. S o R ii. S o R o S

1
PU
Oct. 2010 – 5M

Solution

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

ii. S o R o S = (S o R) o S = {(b, c) (b, d), (c, a), (d, c) (d, d)}

4. Let R and S be two relations on a set of positive integers I:R = {<x, 2x>/ x ∈ I} S = {<x, 7x> / x ∈ I}. Find R o S, R o R, S o S, R o R o R and R o S o R.

Solution

$$R \circ S = \{<x, 14x> / x \in I\}$$

$$S \circ R = \{<x, 14x> / x \in I\}$$

$$\therefore \quad R \circ S = S \circ R$$

$$R \circ R = \{<x, 4x> / x \in I\}$$

$$S \circ S = \{<x, 49x> / x \in I\}$$

$$R \circ R \circ R = \{<x, 8x> / x \in I\}$$

$$R \circ S \circ R = \{<x, 28x> / x \in I\}$$

5. Let R = {<1, 2>, <3, 4>, <2, 2>} and S = {<4, 2>, <2, 5>, <3, 1>}. Obtain the relation matrices for R o S and S o R.

Solution

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

$$M_{R \circ S} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad M_{S \circ R} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

OR

$$R \circ S = \{<1, 5>, <3, 2>, <2, 5>\}$$

$$S \circ R = \{<4, 2>, <3, 2>\}$$

Put these relations in the matrices.

Converse of a Relation: Given a relation R from X to Y, a relation $\tilde{R}$ from Y to X is called the converse of R, where the ordered pairs of $\tilde{R}$ are obtained by interchanging the members in each of the ordered pairs of R. For $x \in X$ and $y \in Y$, that $xRy \Leftrightarrow y\tilde{R}x$.

Example

1. **Let M_R, M_S be the matrices given by**

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad M_S = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Show that $M_{\widetilde{RoS}} = M_{\tilde{S}o\tilde{R}}$.

Solution

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

$$M_{\widetilde{RoS}} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \text{Transpose of } M_{RoS}$$

$$M_{\tilde{S}} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad M_{\tilde{R}} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

$$M_{\tilde{S}o\tilde{R}} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = M_{\widetilde{RoS}}$$

1.11 Complement of a Relation

Given a relation R from X to Y the complement of R, $\bar{R}$ is referred to as the complementary relation, is a relation from X to Y that can be expressed in terms of R:

$X\bar{R}Y$ if and only if $X \not{R} Y$

For example: If $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c\}$

Let $R = \{(1,b), (1,c), (2,a), (2,c), (3,b), (4,a)\}$

Then $\bar{R} = \{(1,a), (2,b), (3,a), (3,c), (4,b), (4,c)\}$

Note that relation matrix of $\bar{R}$ ($M_{\bar{R}}$) is obtained from relation matrix of R (M_R) by replacing every 1 in M_R by a 0 and every 0 by a 1.

Thus in above example.

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

$$\text{Then } M_{\bar{R}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

And diagraph of $\bar{R}$ is a complement of diagraph of R.

1.12 Transitive Closure

Let X be any finite set and R be a relation in X. The relation $R^+ = R \cup R^2 \cup R^3 \cup \ldots$ in X is called the transitive closure of R in X.

Example

1. **Let A = {1, 2, 3, 4} and R = {<1, 2>, <2, 3>, <3, 4>} be a relation on A. Find R^+.**

Solution

R = {<1, 2>, <2, 3>, <3, 4>}

$R^2 = R \circ R$ = {<1, 3>, <2, 4>}

$R^3 = R \circ R^2$ = {<1, 4>}

$R^4 = \phi$

$R^+ = R \cup R^2 \cup R^3$ = {<1, 2>, <2, 3>, <3, 4>, <1, 3>, <2, 4>, <1, 4>}

2. **Given the relation matrix M_R of a relation R on the set {a, b, c}, find the relation matrices of $\tilde{R}$, R^2 = R o R, R^3 = R o R o R and R o $\tilde{R}$.**

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

Solution

R = {<a, a>, <a, c>, <b, a>, <b, b>, <c, a>, <c, b>, <c, c>}

$\tilde{R}$ ={<a, a>, <a, b>, <a, c>, <b, b>, <b, c>, <c, a>, <c, c>}

R^2 = {<a, a>, <a, c>, <a, b>, <b, a>, <b, c>, <b, b>, <c, a>, <c, c>, <c, b>}

R^3 = {<a, a>, <a, c>, <a, b>, <b, a>, <b, c>, <b, b>, <c, a>, <c, c>, <c, b>}

$R \circ \tilde{R}$ = {<a, a>, <a, b>, <a, c>, <b, a>, <b, b>, <b, c>, <c, a>, <c, b>, <c, c>}

1.13 Warshall's Algorithm

Finding the transitive closure of a relation, by computing various powers of R or product of relation matrix M(R) is quite impractical for large sets and relations. Warshall's Algorithm offers an alternative but efficient method for computing the transitive closure.

Working Steps of Warshall's Algorithms

Let R be a relation on a set A, where A = $(a_1,a_2,\ldots,a_n\}$

Let M(R) denote matrix of relation R.

Step 1: Set M(R) = W_0

Step 2 K = 1

Step 3: Transfer to W_k all 1's in W_{k-1}.

Step 4 List the locations r_1,r_2,----in column K of W_{K-1}, where the entry is 1 and the locations S_1,S_2,------ in row K of W_{K-1} where the entry is 1.

Step 5: Put 1's in all the position$(r_i, s_j)$of W_K(if they are not already there)

Step 6: K = K + 1

Step 7: Repeat steps 3, 4 and 5 until K = n.

Examples

1. **Let A = {1,2,3} and Let R = {(1,1),(1,2),(2,3),(1,3),(3,1)(3,2)}**

Find transitive closure of R using Warshall's algorithm.

Solution

We have a set A

A = {1, 2, 3} and the relation R

R = {(1, 1), (1, 2), (2, 3), (1, 3), (3, 1)(3, 2)} defined on A.

The matrix of relation R is

$$M(R) = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \end{array}$$

Set M(R) = W_0

K = 1, in W_0, We have in first column 1's in position 1 and 3.

Also in first row 1's in position 1,2, and 3 ⇒ so in W_1, We have 1's in position(1,1), (1,2), (1,3), (3,1), (3,2) and (3,3)

$$\therefore\ W_1 = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{array}$$

K = 2, In W_1, we have in second row 1's in position3 ⇒ so in W_2 we have 1's in position(1,3) and (3,3).

$$\therefore \quad W_2 = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{array}$$

We observe that $W_2 = W_1$

K = 3, In W_2 in third column 1's in the position 1, 2 and 3. Also in third row,1's in position 1, 2, 3 ⇒ In W_3, 1's in position (1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2) and (3,3).

$$\therefore \quad W_3 = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \end{array} = M(R^*)$$

∴ The transitive closure of given relation R is

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

2. Let A = {1, 2, 3, 4} and R = { <1, 2>, <2, 3>, <3, 4> }. Find R*, transitive closure and draw graph.

1

PU
Oct. 2008 – *6M*

Solution

We find transitive closure of relation R by Warshall's Algorithm as below.

Step 1: We find the Matrix of Relation R i.e.

$$M(R) = \begin{array}{c c} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Step 2: Set $W_0 = M(R)$ and $K = 1$.

Step 3: In W_0, we have in 1st column, '1' is in none of the position also in 1st row, '1' is in position 2. So here $W_1 = W_0$

$$\text{i.e. } W_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Step 4: K = 2, In second column we have '1' is in position 1 of W_1 and also in 2nd row '1' is in position 3. Thus we add '1' in the position (1, 3) for W_2.

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

Step 5: K = 3, In third column, we have '1' is in position '1' and '2' of W_2 and also in third row '1' is in position 4. Thus we add 1 in the position (1, 4) and (2, 4) for W_3.

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

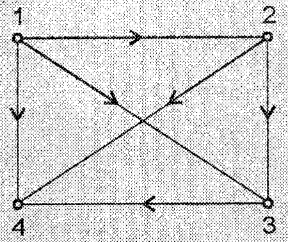
Step 6: K = 4, In fourth column we have '1' is in position 1,2 and 3 of W_3 and also in fourth row '1' is in none of position so here $W_4 = W_3$.

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

Thus, $M(R^*) = W_4$

Thus $R^* = \{(1, 2), (1, 3), (1; 4), (2, 3), (2, 4), (3, 4)\}$

Graph for R*



3. Let A = {1,2,3,4} and R = {(1,2), (2,1), (2,3), (3,4)}. Find R^+ by using Warshall's algorithm.

1
PU
Apr. 2010 – *5M*

Solution

The matrix of relation R is,

$$M(R) = \begin{array}{c|cccc|} & 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 \end{array}$$

Let $W_0 = M(R)$.

Step 1 : Let K = 1, in W_0, we have in first column 1's in position 2 and in first row, 1's in position 2 ⇒ so in W_1, we have 1's in position (2, 2)

$$\therefore \quad W_1 = \begin{array}{c|cccc|} & 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & 1 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 \end{array}$$

Step 2: K = 2 in W_1, we have in second column we have 1's in positions 1 and 2 and in second row we have 1's in 1, 2, 3, positions.

∴ We have 1 in positions (1, 1) (1, 2) (1, 3) (2, 1)(2, 2), (2, 3) of W_2.

$$\therefore \quad W_2 = \begin{array}{cc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Step 3: K = 3. In 3rd column we have 1's in positions 1 and 2 and in 3rd row we have 1's in position 4, so in W_3 we have 1's in positions (1, 4) and (2, 4).

$$\therefore \quad W_3 = \begin{array}{cc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Step 4: K = 4. In 4th column we have 1's in positions 1, 2, 3 and in fourth row we do not have any 1's so,

$W_4 = W_3 = M(R^+)$

$\therefore$ The transitive closure of given relation R is

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

2. Functions

A particular class of relations are called functions.

Definitions

Let X and Y be any two sets. A relation f from X to Y is called a function if for every $x \in X$ there is a unique $y \in Y$ such that $<x, y> \in f$

For a function $f : X \rightarrow Y$, if $<x, y> \in f$, then x is called an argument and the corresponding y is called the image of x under f. Instead of writing $<x, y> \in f$, it is customary to write $y = f(x)$ and to call y the value of the function f at x.

Definition

If f is a function from A to B, we say that A is the domain of f and B is the codomain of f. If f(a) = b, we say that b is the image of a and a is a pre-image of b. The range of f is the set of all images of elements of A. Also, if f is a function from A to B, we say that f maps A to B.

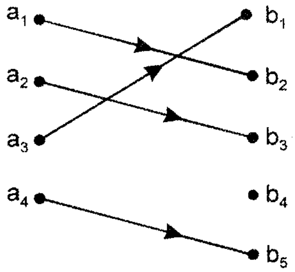
Example

1. **Let f be a function from A to B, where $A = \{a_1, a_2, a_3, a_4\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$ defined by $f = \{<a_1, b_2>, <a_2, b_3>, <a_3, b_1>, <a_4, b_5>\}$. Obtain D_f, R_f and co-domain.**

Solution

$$\begin{aligned} D_f &= \{a_1, a_2, a_3, a_4\} = A \\ R_f &= \{b_2, b_3, b_1, b_5\} \\ \text{Co-domain} &= \{b_1, b_2, b_3, b_4, b_5\} = B \end{aligned}$$

2.1 Graphical Representation of Function



Definition

Let f be a function from the set A to the set B and let S be a subset of A. The image of S is the subset of B that consists of the images of the elements of S. We denote the image of S by f(S), so that

$$f(S) = \{f(s) / s \in S\}$$

Example

1. **Let A = {a, b, c, d, e,} and B = {1, 2, 3, 4} with f(a) = 2, f(b) = 1, f(c) = 4, f(d) = 1 and f(e) = 1. Find the image.**

Solution

The image of the subset S = {b, c, d} is the set f(S) = {1, 4}

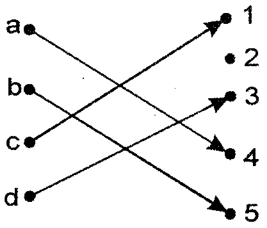
Definition

A function f is said to be **one-one or injective** if and only if f(x) = f(y) implies that x = y for all x and y in the domain of f. A function is said to be an injection if it is one-to-one.

Example

1. **Determine whether the function f from {a, b, c, d} to {1, 2, 3, 4, 5} with f(a) = 4, f(b) = 5, f(c) = 1 and f(d) = 3 is one-to-one.**

Solution



The function f is one-to-one since f takes on different values at the four elements of its domain.

Definition

A function f whose domain and codomain are subsets of the set of real numbers is called strictly increasing if f(x) < f(y) whenever x < y and x and y are in the domain of f. Similarly, f is called strictly decreasing if f(x) > f(y) whenever x < y and x and y are in the domain of f.

Note: For some functions the range and the codomain are equal. That is, every member of the codomain is the image of some elements of the domain. Functions with this property are called ONTO functions.

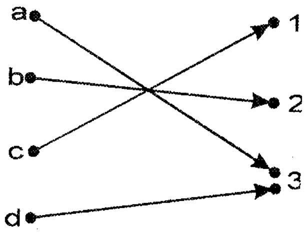
Definition

A function f from A to B is called **ONTO** or **surjective**, if and only if for every element b ∈ B there is an element a ∈ A with f(a) = b. A function f is called a surjection if it is ONTO.

Example

1. **Let f be the function from {a, b, c, d} to {1, 2, 3} defined by f(a) = 3, f(b) = 2, f(c) = 1 and f(d) = 3. Is f an ONTO function**

Solution



Since all three elements of the codomain are images of elements in the domain, f is ONTO.

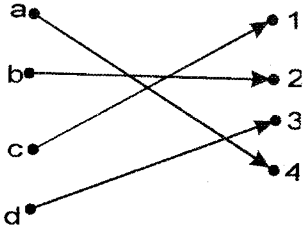
Definition

The function f is a one-to-one correspondence or a **bijection**, if it is both one-to-one and ONTO.

Example

1. **Let f be the function from {a, b, c, d} to {1, 2, 3, 4} with f(a) = 4, f(b) = 2, f(c) = 1 and f(d) = 3. If f a bijection?**

Solution



The function f is one-to-one and ONTO. It is one-to-one. Since the function takes on distinct values. It is ONTO since all four elements of the codomain are images of elements in the domain are images of elements in the domain. Hence, f is bijection.

Definition

Let f be a one-to-one correspondence from the set A to the set B. The **inverse function** of f is the function that assigns to an element b belonging to B the unique elements a in A such that f(a) = b. The inverse function of f is denoted by f^{-1}. Hence $f^{-1}(b) = a$ when f(a) = b.

Example

1. **Let f be the function from {a, b, c} to {1, 2, 3} such that f(a) = 2, f(b) = 3 and f(c) = 1. Is f invertible and if it is, what is its inverse?**

Solution

The function f is invertible since it is a one-to-one correspondence. The inverse function f^{-1} reverses the correspondence given by f, so that $f^{-1}(1) = c$, $f^{-1}(2) = a$ and $f^{-1}(3) = b$.

Left Inverse and Right Inverse

Let X be a set and f be a function f: X×X →X, then f is called a binary operation on X, Let $*$ be a binary operation on X with the identity element e. An element $a \in X$ is said to be left-invertible if there exists an element $x_l \in X$ such that $x_l * a = e$, x_l is *called* a left inverse of a.

Similarly, $a \in X$ is said to be right-invertible if there exists $x_r \in X$ such that $a * x_r = e$, x_r is called as right inverse of a.

Definition

Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The **composition** of the functions f and g, denoted by f∘g, is defined by

$$(f \circ g)(a) = f(g(a))$$

Example

1. **Let g be the function from the set {a, b, c} to itself such that g(a) = b, g(b) = c and g(c) = a. Let f be the function from the set {a, b, c} to the set {1, 2, 3} such that f(a) = 3, f(b) =2 and f(c) = 1. What is the composition of f and g, g and f.**

Solution

$$(f \circ g)(a) = f(g(a)) = f(b) = 2$$
$$(f \circ g)(b) = f(g(b)) = f(c) = 1$$
$$(f \circ g)(c) = f(g(c)) = f(a) = 3$$

g∘f is not defined because the range of f is not a subset of the domain of g.

2. **Let f and g be the functions from the set of integers defined by f(x) = 2x + 3 and g(x) = 3x + 2. What is the composition of f and g, g and f?**

Solution

$$(f \circ g)(x) = f(g(x) = f(3x + 2) = 2(3x + 2) + 3 = 6x + 7$$
$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = 6x + 11$$

Note: The commutative law does not hold for the composition of functions.

3. **Let X = {1, 2, 3} and f, g, h and s be functions from X to X given by**

f = {<1, 2>, <2, 3>, <3, 1>} **g = {<1, 2>, <2, 1>, <3, 3>}**

h = {<1, 1>, <2, 2>, <3, 1>} **s = {<1, 1>, <2, 2>, <3, 3>}**

Find f∘g, g∘f, f∘h∘g, s∘g, g∘s, s∘s and f∘s.

Solution

$f \circ g = \{<1, 1>, <2, 3>, <3, 2>\}$

$g \circ f = \{<1, 3>, <2, 2>, <3, 1>\}$

$h \circ g = \{<1, 2>, <2, 1>, <3, 1>\}$

$f \circ h \circ g = \{<1, 3>, <2, 2>, <3, 2>\}$

$s \circ g = \{<1, 2>, <2, 1>, <3, 3>\}$

$g \circ s = \{<1, 2>, <2, 1>, <3, 3>\}$

$s \circ s = \{<1, 1>, <2, 2>, <3, 3>\}$

$f \circ s = \{<1, 2>, <2, 3>, <3, 1>\}$

4. Let $f(x) = x + 2$, $g(x) = x - 2$ and $h(x) = 3x \ \forall\ x \in R$ where R is the set of real numbers. Find:

a. $f \circ g$ b. $g \circ f$ c. $f \circ f$ d. $g \circ g$
e. $h \circ g$ f. $h \circ f$ g. $f \circ h$ h. $f \circ h \circ g$

Solution

a. $f \circ g(x) = f(g(x)) = f(x - 2) = (x - 2) + 2 = x$

b. $g \circ f(x) = g(f(x)) = g(x + 2) = (x + 2) - 2 = x$

c. $f \circ f(x) = f(f(x)) = f(x + 2) = (x + 2) + 2 = x + 4$

d. $g \circ g(x) = g(g(x)) = g(x - 2) = (x - 2) - 2 = x - 4$

e. $h \circ g(x) = h(g(x)) = h(x - 2) = 3(x - 2) = 3x - 6$

f. $h \circ f(x) = h(f(x)) = h(x + 2) = 3(x + 2) = 3x + 6$

g. $f \circ h(x) = f(h(x)) = f(3x) = 3x + 2$

h. $f \circ h \circ g(x) = f(h(g(x))) = f(h(x - 2)) = f(3(x - 2)) = f(3x - 6) = 3x - 6 + 2 = 3x - 4$

Definition

A mapping $I_x : X \to X$ is called an identity map if

$$I_x = \{<x, x> / x \in X\}$$

▶Theorem

1. **If $f : X \to Y$ is invertible, then $f^{-1} \circ f = I_x$ and $f \circ f^{-1} = I_y$.**
2. **Let $f : X \to Y$ and $g : Y \to X$. The function g is equal to f^{-1} only if $g \circ f = I_x$ and $f \circ g = I_y$.**

Examples

1. Show that the functions $f(x) = x^3$ and $g(x) = x^{1/3}$ for $x \in R$ are inverses of one another.

Solution

$(f \circ g)(x) = f(x^{1/3}) = (x^{1/3})^3 = x$

$(g \circ f)(x) = g(x^3) = (x^3)^{1/3} = x$

Then $f = g^{-1}$ or $g = f^{-1}$

2. Let F_x be the set of all one-to-one ONTO mappings from X ONTO X, where X = {1, 2, 3}. Find all the elements of F_x and find the inverse of each element.

Solution

$f_1 = \{<1, 1>, <2, 2>, <3, 3>\}$

$f_2 = \{<1, 1>, <2, 3>, <3, 2>\}$

$f_3 = \{<1, 2>, <2, 1>, <3, 3>\}$

$f_4 = \{<1, 3>, <2, 2>, <3, 1>\}$

$f_5 = \{<1, 2>, <2, 3>, <3, 1>\}$

$f_6 = \{<1, 3>, <2, 1>, <3, 2>\}$

0	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_5	f_1	f_3	f_2
f_5	f_5	f_3	f_4	f_2	f_6	f_1
f_6	f_6	f_4	f_2	f_3	f_1	f_5

The elements of $F_X = \{f_1, f_2, f_3, f_4, f_5, f_6\}$ where $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$, $f_5^{-1} = f_6$ and $f_6^{-1} = f_5$.

3. Let f : R → R and g : R → R where R is the set of real numbers. Find f ∘ g and g ∘ f, where $f(x) = x^2 - 2$ and $g(x) = x + 4$.

Solution

$$f \circ g(x) = f(g(x)) = f(x + 4) = (x + 4)^2 - 2 = x^2 + 8x + 14$$

$$g \circ f(x) = g(f(x)) = g(x^2 - 2) = x^2 - 2 + 4 = x^2 + 2$$

4. If f : X → Y and g : Y → Z and both f and g are ONTO, show that g ∘ f is also ONTO. Is g ∘ f one-to-one if both g and f are one-to-one.

Solution

Let $f : X \to Y$ and $g : Y \to Z$ be ONTO, then $g \circ f : X \to Z$ also ONTO because for every, $z_1 \in Z$ there exists an y_1 such that $g(y_1) = z_1$ (as g is ONTO) and for every $y_1 \in Y$, there exists x_1 such that $f(x_1) = y_1$ (as f is ONTO).

$\therefore\ g(y_1) = g \circ (f(x_1)) = g \circ f(x_1) = z_1$

Thus for every $z_1 \in Z$, there is a $x_1 \in X$ such that $g \circ f(x_1) = z_1$

Let $f : X \to Y$ and $g : Y \to Z$ be one-one then $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ for $x_1, x_2 \in X$ and $g(y_1) = g(y_2) \Rightarrow y_1 = y_2$

Let $(g \circ f)(x_1) = (g \circ f)(x_2)$ for $x_1, x_2 \in X$

$g(f(x_1)) = g(f(x_2))$

$f(x_1) = f(x_2)$ (as g is one-to-one)

$x_1 = x_2$ (as f is one-to-one)

$g \circ f(x_1) = g \circ f(x_2) \Rightarrow x_1 = x_2$

Thus $g \circ f$ is one-one.

5. Let f : R → R be given by $f(x) = x^3 - 2$. Find f^{-1}.

Solution

Let $x^3 - 2 = y$ then $x = (y + 2)^{1/3}$

$\therefore$ $g(x) = (x + 2)^{1/3}$ is the inverse of f.

6. How many functions are there from X to Y for the sets given below? Find also the number of functions which are one-to-one, ONTO and one-to-one ONTO.

a. $X = \{1, 2, 3\}$ $Y = \{1, 2, 3\}$

b. $X = \{1, 2, 3, 4\}$ $Y = \{1, 2, 3\}$

c. $X = \{1, 2, 3\}$ $Y = \{1, 2, 3, 4\}$

Solution

a. There are Y^X distinct functions from X to Y.

$\therefore$ Number of distinct functions are $3^3 = 27$

Number of one-to-one mappings are $3.2.1 = 3! = 6$

Every one-to-one mapping from X → Y is ONTO and every ONTO mapping from X → Y is one-to-one and hence the number of ONTO mapping from X to Y is also 6.

$\therefore$ The number of bijective mappings from X to Y is also 6.

b. As X > Y it is not possible to have single one-to-one mapping from X to Y. Also a map is ONTO, if every element of Y is image of some element of X and no two elements of Y are the images of one element of X.

$\therefore$ The number of ONTO maps is $X (|X| - 1) (|X| - 2) \ldots |Y|$ factors

Thus number of ONTO mappings is equal to $4.3.2 = 24$. Also there is no bijective map from X to Y.

c. There are 4^3 distinct mapping of these $4.3.2 = 24$ mappings are one-to-one.

There is no ONTO mapping from X to Y and hence, there is no bijective maps from X to Y.

7. Show that there exists a one-to-one mapping from A × B to B × A. Is it also ONTO.

Solution

Let f: A × B to B × A be a mapping defined by $f <a, b> = <b, a>$ for $a \in A$ and $b \in B$. Clearly f is one-to-one because

$f <a_1, b_1> = f <a_2, b_2>$

$<b_1, a_1> = <b_2, a_2>$

$b_1 = b_2$ and $a_1 = a_2$

$\therefore\ \langle a_1, b_1\rangle = \langle a_2, b_2\rangle$

f is ONTO because for every element <b, a> ∈ B × A, there is an element <a, b> ∈ A × B such that f<a, b> = <b, a>. Thus f is a bijective map from A × B to B × A.

8. Let X = {1, 2, 3, 4}. Define a function

$f : X \to X$ such that $f \neq I_x$ and is one-to-one

Find $f \circ f = f^2$, $f^3 = f \circ f^2$, f^{-1} and $f \circ f^{-1}$.

Can you find another function which is one-to-one $g : X \to X$ such that $g \neq I_x$ but $g \circ g = I_x$?

Solution

Let $f : X \to X$ defined by f(1) = 2, f(2) = 3, f(3) = 4, f(4) = 1 then

$$f^2 = \{\langle 1, 3\rangle, \langle 2, 4\rangle, \langle 3, 1\rangle, \langle 4, 2\rangle\}$$

$$f^3 = \{\langle 1, 4\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle, \langle 4, 3\rangle\}$$

$$f^{-1} = \{\langle 2, 1\rangle, \langle 3, 2\rangle, \langle 4, 3\rangle, \langle 1, 4\rangle\}$$

$$f \circ f^{-1} = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 4, 4\rangle\}$$

It is possible to find a one-to-one function $g : X \to X$ such that $g \neq I_x$

Take $g = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 3, 4\rangle, \langle 4, 3\rangle\}$

$$g \circ g = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 4, 4\rangle\} = I_x$$

2.2 Characteristics Function of a Set

Let E be a universal set and A be a subset of E. The function

$\tau_A : E \to \{0, 1\}$ defined by

$$\tau_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

is called the characteristic function of the set A.

2.3 Hashing Function

Let this numerical value of a key be denoted by K, and let n be a fixed integer. Then the hashing function h defined by the division method is

$$h(K) = K(\text{mod } n)$$

where h(K) is the remainder of dividing K by n and is therefore an element of {0, 1, ..., n – 1}. Thus, the hashing function maps the set of keys to the set of n addresses, viz., the set {0, 1, ..., n – 1} which may be called the address set. The choice of n depends upon the fact that a good hashing function should uniformly distribute the records over the elements of the address set.

2.4 Floor and Ceil Functions

Let functions f and g be defined by:

$$f = \{<x, \lfloor x \rfloor> / x \in R \wedge \lfloor x \rfloor = \text{the greatest integer less than or equal to } x\}$$

$$g = \{<x, \lceil x \rceil> / x \in R \wedge \lceil x \rceil = \text{the least integer greater than or equal to } x\}$$

The function $f(x) = \lfloor x \rfloor$ is frequently called the floor of x and the function $g(x) = \lceil x \rceil$ is called the ceiling of x.

$$f(3.75) = \lfloor 3.75 \rfloor = 3$$

$$f(4) = \lfloor 4 \rfloor = 4$$

$$f(-3.75) = \lfloor 3.75 \rfloor = -4$$

$$g(3.33) = \lceil 3.33 \rceil = 4$$

$$g(4) = \lceil 4 \rceil = 4$$

$$g(-3.33) = \lceil -3.33 \rceil = -3$$

2.5 Partial Function

A function $f : D \rightarrow N$ where $D \subseteq N^n$, then f is called a partial function, i.e., if a function cannot be defined for every n-tuple in N^n is called a partial function.

For example, $f(x, y) = x - y$, which is defined for only those $x, y \in N$ which satisfy $x \geq y$ hence $f(x, y)$ is a partial function.

2.6 Infinite Sets

A set A is infinite if there exists an injection $f : A \rightarrow A$ such that f(A) is a proper subset of A. If no such injection exists, the set is finite.

Examples

i. The set of natural numbers N is an infinite set.

Consider $f : N \rightarrow N$, where $f(x) = 2x$

f(N) is the set of all positive even integers which is a proper subset of N.

ii. The set of real numbers R is an infinite set

Define $f : R \rightarrow R$ as

$$\begin{aligned} f(x) &= x + 1 && \text{if } x \geq 0 \\ &= x && \text{if } x < 0 \end{aligned}$$

Clearly f is an injective function.

If $y \in R$ such that $y = x + 1$ then $x = y - 1$.

Hence $x \geq 0$ implies $y \geq 1$

Range (f) = $\{y \in R / y < 0 \wedge y \geq 1\}$, which is a proper subset of R.

2.7 Bijection and Cardinality of Finite Sets

Cardinality

Two sets A and B are said to be equipotent (or equivalent or to have the same cardinality or to be similar) and written as $A \sim B$ if and only if there is one-to-one correspondence between the elements of A and those of B.

The concept of bijection is a powerful tool to compare the cardinalities of two sets, especially for infinite sets.

Countability

An infinite set A is said to be countable if there exists a bijection $f : N \rightarrow A$.

A countably infinite set is also called a denumerable set.

Definition

If A and B are sets and there exists a bijection $f : A \rightarrow B$, then A and B have the same cardinality.

We denote the cardinality of N by N_0. Hence if A is countably infinite then $|A| = N_0$.

2.8 Non-denumerable Sets

One should not however be misled in assuming that every infinite set is countable we shall now deal with some important sets that are not countable.

▶ Theorem

The set of real numbers R is non-denumerable

i. **What is the cardinality of the following sets:**

   a. **$I = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$.**

   b. **$N \times N$, N is the set of natural numbers.**

   c. **Union of finite number of countable sets.**

Solution

a. I is countably infinite

   $\therefore |I| = N_0$.

b. $N \times N$ is also countably infinite $|N \times N| = N_0$.

c. Countably infinite.

   Cardinality is N_0.

ii. **Classify the following into finite, denumerable and non-denumerable:**

a. **Number of trees in India.**

b. **Power set of a countably infinite set.**

c. **Number of songs sung by Lata Mangeshkar.**

Solution

a. Since the number of trees is not static but continues to increase, the set is denumerable.

b. Power set of N is non-denumerable. Hence power set of a countably infinite set is non-denumerable.

c. The set is finite.

EXERCISE

1. List all possible functions from A → A, where A = {a, b, c}. State which of these are into, onto, one-to-one and one-to-one and onto.

2. Define cardinality of the set. Show that the set of integers is countable.

3. Let A = {1, 2, 3, 4} and relation R : A → A is R = {(1, 2), (2, 1), (2, 3), (3, 4), (4, 1)} find transitive closure R.

4. Let A = {1, 2, 3}. Let R, S be relations on A whose matrices are

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

Find $M_{S \circ R}$. Is $S \circ R$ reflexive? Is it symmetric?

5. Use Warshall's algorithm, to find the transitive closure of the relation

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

6. Let A = {1, 2, 3, 4} and R = {(1, 1), (1, 4), (2, 2), (3, 3), (4, 1), (4, 4)}. Prove that R is an equivalence relation on A. Find the equivalence classes of elements of A.

7. Show that the set of all integers is a denumerable set.

8. Given the relation matrices M_R and M_S.

Find $M_{R \circ S}$, $M_{S \circ R}$,

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

9. Let X = {a, b, c, d, e} and C = {{a, b}, {c}, {d, e}}. Show that the partition 'c' defines an equivalence relation on X.

Collection of Questions asked in Previous Exams PU

1. Let A = {1, 2, 3, 4} and R = { <1, 2>, <2, 3>, <3, 4> }. Find R*, transitive closure and draw graph. **[Oct. 2008 – 6M]**

2. Let A ={1, 2, 3, 4.} Let R = {<1, 2>, <1, 3>, <1, 4>, <1, 4>, <2, 3>, <3, 3>, <4, 2>, and S={<1, 3>, <2, 2>, <3, 2>, <4, 2>} Find:

   i. R o (S o S) ii. Is R o S = S o R? iii. R o R o R **[Oct. 2008 – 6M]**

3. A relation R = { <1, 1>, <1, 2>, <1, 4>, <2, 1>, <2, 2>, <3, 3>, <4, 4>} defined over the set A = {1,2,3,4}. Is R an equivalence Relation? **[Oct. 2008 – 6M]**

4. For a set A = {1, 2, 3, 4, 5}, the relation matrix is **[Oct. 2009 – 5M]**

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

   Draw its diagraph.

5. Draw all non isomorphic graphs on 2 and 3 vertices. **[Oct. 2009 – 4M]**

6. Let Z be the set of integers and let aRb; b is a multiple of a. Determine which of the five properties are satisfied by R. **[Oct. 2009 – 5M]**

7. Define the term: Non-Denumerable sets. **[Oct. 2009 – 2M]**

8. Define the term: Matrix representation of a relation. **[Oct. 2009 – 2M]**

9. If {(1,3,5), (2,4)} is a partition set of the set A = {(1,2,3,4,5}. Determine the corresponding equivalence relation. **[Apr. 2010 – 5M]**

10. Let A = {1,2,3,4} and R = {(1,2), (2,1) (2,3), (3,4)}. Find R^+ by using Warshall's algorithm. **[Apr. 2010 – 5M]**

11. The compatibility relation on a set $\{x_1, x_2, \ldots\ldots x_6\}$ be given by the matrix. **[Apr. 2010 – 5M]**

$$\begin{array}{c|ccccc} x_2 & 1 & & & & \\ x_3 & 1 & 0 & & & \\ x_4 & 1 & 1 & 0 & & \\ x_5 & 0 & 1 & 0 & 0 & \\ x_6 & 0 & 0 & 1 & 0 & 1 \\ \hline & x_1 & x_2 & x_3 & x_4 & x_5 \end{array}$$

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

12. Let A = {1, 2, 3, 4, 5, 6, 7} Determine a relation R on A by aRb iff 3 divides (a – b). Show that R is an equivalence relation. Also determine the partition generated by R. **[Apr. 2010 – 5M]**

13. Let A = {1, 2, 3, 4, 5, 6}. Let R = {(a, b) | a ≡ b mod 2}. Is R an equivalence relation? **[Oct. 2010 – 5M]**

14. Let R and S be the following relations on B = {a, b, c, d}, R = {(a, a), (a, c) (c, b) (c, d) (d, b) and S = {(b, a), (c, c), (c, d), (d, a)}

Find the following composite relations.

i. $S \circ R$

ii. $S \circ R \circ S$ **[Oct. 2010 – 5 M**

15. The compatibility relation on a set {1, 2, 3, 4, 5} be given by the following matrix.

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

Draw the graph and find all the maximal compatibility blocks of the relation. **[Oct. 2010 – 5M**

16. Let f: A → B and A = B = R, $f(x) = x^4 + 1$. Find F^{-1}. **[Oct. 2010 – 5M**

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

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

3 Permutations and Combinations

1. Introduction

Many problems in probability theory can be solved simply by counting the number of different ways that a certain event can occur. The mathematical theory of **counting** is formally known as combinatorial analysis. Combinatorics is a branch of mathematics which deals with problems of existences, counting and generation of arrangements of a specified kind. Hence combinatorics has important applications to probability theory, computer science, operations research and many other fields.

2. Principles of Counting

Addition Principle (AP)

If a set S contains m objects and a set T contains n objects and S and T are disjoint sets then the total number of ways of choosing one object from S or T is m+n. In other words if S and T are two disjoint finite sets then number of objects in S $\cup$ T can be obtained by adding the number of objects in S and number of objects in T.

i.e., $|S \cup T| = |S| + |T|$

where |S| denotes the number of elements in a finite set S, known as cardinality of set S.

The addition principle also be stated as follows: If an event can happen in m possible ways and another event in n possible ways and both are mutually exclusive (both cannot happen simultaneously) then either the two events can be occurred in (m + n) ways.

The addition principle can be extended, by induction to any finite number of sets as follows:

Generalization of A.P.

If $S_1, S_2, \ldots, S_m$ are m pairwise disjoint finite sets and S_i contains n_i objects, then the number of ways to select an object from one of these sets is $n_1 + n_2 + \ldots + n_m$.

Example

1. **If there are 8 different books on mathematics and 6 different books on statistics then in how many ways student can select a book from these?**

Solution

Student has to choose one book, it can be a book on mathematics (8 choices) or a book on statistics (6 choices). All books are different, so by addition principle. The total number of ways of selecting is 8 + 6 = 14.

Multiplication Principle (MP)

If A and B are finite sets containing m and n objects respectively then the Cartesian product $A \times B = \{(x,y)/\ x \in A,\ y \in B\}$ contains mn ordered pairs.

This principle can also be stated as: *If an event can occur is in m way and if corresponding to each way of occurring this event another event can occur in n ways independent of the first, then the number of ways of happening both the events simultaneously (or sequentially) is $m \times n$.*

Example

1. **How many ways a captain and a vice-captain can be selected from team of 11 players?**

Solution

A captain from 11 players can be selected in 11 ways. After selecting a captain, a vice-captain from the remaining players can be selected in 10 ways, so total number of ways of selecting by multiplication principle is $11 \times 10 = 110$.

The multiplication principle can be extended, by induction to any finite number of events as follows:

Generalization of MP

If $E_1, E_2, \ldots, E_m$ are m events where i^{th} event can occur in n_i, different ways i = 1, 2, . . ., m then total number of ways of happening all the events either sequentially or simultaneously is $n_1 \cdot, n_2 \cdot, n_3 \cdots n_m$.

Bijection Principle (BP)

If finite sets S and T can be put into one – to – one correspondence with each other, then they contain the same number of elements i.e. $|S| = |T|$.

For example: Consider an n – set $S = \{a_1, a_2, \ldots, a_n\}$. Let A be the family of all subsets of S and B be the family of all binary words of length n. We define a correspondence between A and B thus: a subset T of S corresponds to the binary word t = $(x_1, x_2, \ldots, x_n)$ where $x_i = 1$ if a_i is in T and $x_i = 0$ if a_i is not in T. (*For example*, if n = 4, the subset $\{a_2, a_4\}$ corresponds to the binary word (0, 1, 0, 1) of length 4). Clearly the binary word t is uniquely defined when T is given. Conversely, every binary word of length n uniquely corresponds to a subset of S. Thus T → t is a one-to-one correspondence between the families A and B and so by BP,

$$|A| = |B|$$

3. Permutations

3.1 r Permutations of n-Elements

Definition

A linear r-permutation of a set S containing n different objects is an **ordered** arrangement of r of the n elements of S in a row.

▶Theorem I

The number of r-permutations of a set S contains n different objects is denoted by P(n, r) or ^nP_r and is given by,

$$^nP_r = n(n-1)(n-2)\ldots(n-r+1)$$

$$= \frac{n!}{(n-r)!}, \quad 0 \le r \le n$$

Proof

Constructing an r-permutation from the n objects in S, is equivalent to filling r places, in a row using these objects. The first place can be filled in n ways since any one of the n objects can be used. Then the second place can be filled in (n–1) ways using any one of the remaining (n–1) objects and so on. Having filled (r–1) places with (r+1) of the objects in this ways, the rth place can be filled in n–(r–1) = n–r+1 ways using any one of the remaining n–r+1 objects. Hence by multiplication principle, the total number of ways of filling the r places i.e. the total number of r-permutations in S is

$$^nP_r = n(n-1)(n-2)\ldots(n-r+1) = \frac{n!}{(n-r)!}$$

Note: In particular, if r = 0, then

$$^nP_0 = \frac{n!}{(n-0)!} = \frac{n!}{n!} = 1$$

If r = n, then

$$^nP_n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

If r = 2, then

$$^nP_2 = \frac{n!}{(n-2)!} = n(n-1)$$

Examples

1. **Find the number of Permutations of the letters of the word 'COMPUTER'. How many words can be formed from it by using only 5 letters?**

Solution

Here total number of letters n = 8, all are different. Permutation of the letters of the word 'COMPUTER is arrangement of 8 letters out of 8 letters, so number is

$^8P_8 = 8!$

If words of 5 letters are to be formed from given word, then we have to permute 5 letters out of 8 letters, which can be done in $^8P_5 = \frac{8!}{(8-5)!} = \frac{8!}{3!} = 6720$ ways.

2. **In how many ways can 10 persons be seated in a row? If 3 of these are women, how many ways can 10 people be arranged so that no two women sit side by side?**

1 PU Oct. 2009 – 5M

Solution

10 persons can be seated in a row in $^{10}P_{10} = 10!$ ways.

If 3 women are to be arranged so that no two women sit side by side then first we make arrangement of 7 men in $^7P_7 = 7!$ ways and in between these 7 men there are 8 places on which 3 women can be arranged the number of ways for this is

$$^8P_3 = \frac{8!}{5!}$$

$$= 8 \times 7 \times 6 = 336$$

Hence, total number of ways of arrangement with given condition is 336 × 7!.

3. **How many 3 digit numbers can be formed by using the 6 numbers 2, 3, 4, 5, 6 and 8 if:**
   i. **Repetition not allowed**
   ii. **Number must contain the digit 5 and repetitions are allowed.**

1 PU Apr. 2010 – 5M

Solution

i. Repetition is not allowed: The arrangement of 3 out of 6 without repetition is given by $^6P_3 = \frac{6!}{3!}$

$= 6 \times 5 \times 4$

$= 120.$

So total 120 numbers can be formed by using the given condition.

ii. Number must contain the digit 5 and repetitions are allowed: the digit 5 can be placed in any one the three places in $^3p_1 = 3$ ways, since repetitions are allowed, for remaining two places, the arrangements can be done in $6 \times 6 = 36$ ways. Hence total no. of ways of forming numbers $= 36 \times 3 = 108$.

3.2 Permutations with Repetitions from Distinct Objects

The number of permutations of r objects taken from a set S containing n different objects with repetitions is denoted by $^{n}p_{r}*$and is given by

$$^{n}p_{r}* = n^{r}, \quad 0 \leq r \leq n$$

Example

1. **How many strings of four letters followed by three digits can be formed if the letters and digits can be repeated any number of times?**

Solution

There are 26 letters and 10 digits since letters and digits can be repeated, the total number of ways in which string can be formed is,

$$\underbrace{26 \times 26 \times 26 \times 26}_{\text{(4 letters)}} \times \underbrace{10 \times 10 \times 10}_{\text{(3 digits)}} = 26^{4} \times 10^{3}$$

3.3 Circular Permutations

The permutations considered in earlier articles are called linear permutations for the objects as the objects are being arranged in a line. If instead of arranging objects in a line, we arrange them in a cycle, then the permutation is said to be *circular permutations*.

We know that if we arrange three different persons a, b, c in a row then there are 3! = 6 arrangements viz.

a, b, c   b, c, a   c, a, b ....(1)

a, c, b   c, b, a   b, a, c ....(2)

But suppose these persons are seated around a circular table and suppose the seats are not numbered then we observe the following arrangements.

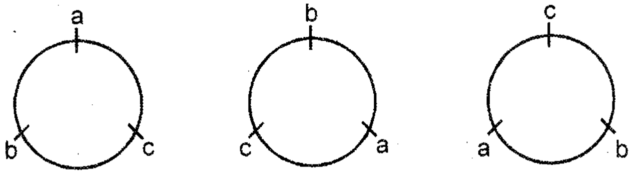


Figure 1

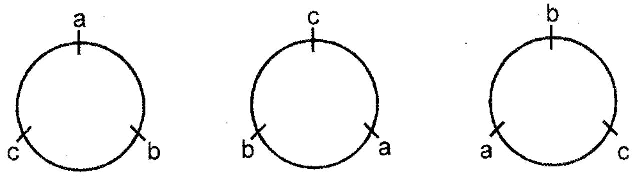


Figure 2

Figure 3.1

We note that since the seats are not numbered, only the relative positions of a, b, c are important. Hence we must regard a, b, c and b, c, a as equal circular permutations because in both of them the relative positions of a, b, c are exactly the same, in fact they are obtained from one another by rotation. Similarly a, b, c and c, a, b are equivalent. Thus all the three linear permutations in (1) correspond to one circular permutations a, b, c. Also we note that the permutations of a, b, c and a, c, b cannot be changed into one another by rotations. Hence a, b, c and a, c, b can taken as distinct permutation. Thus number of circular permutations is less than the number of linear permutations.

▶Theorem 2

The number of distinct circular permutations of n different objects is (n–1)!

Proof

Let a_1 , a_2, . . . , a_n denote n different objects. In a circular permutations only the relative positions of the objects are important. Also the relative positions are not changed by a rotation. Hence we may fix one particular object say a_1 in a position and count the number of different ways of arranging the remaining (n–1) objects relative to a_1. So in the place say r_1, to the right of a_1, we can put any one of the other (n–1) objects. Then in the place say r_2, to the right of r_1 we can put any of the remaining (n–2) objects.

Continuing in this anticlockwise way, we can successively place the objects in (n–1),(n–2),. . ., 2, 1 ways around the table.

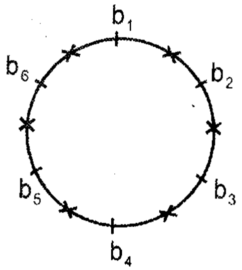
Hence by multiplication theorem, the number of distinct circular permutations n different object is $(n-1)\cdot(n-2)\ldots 2.1 = (n-1)!$.

Examples

1. **In how many ways can a party of 6 boys and 5 girls be seated at a round table so that no two girls are together?**

Solution

First we arrange for boys at a round table. As there are 6 boys, they can be arranged around the table in (6–1)! = 5! ways.



Now after arrangement of boys, there are six places for girls, one each between two boys. Hence girls can be seated in ${}^6P_5$ ways. Therefore required number of ways the arrangement can be done by multiplication principle is $5! \times {}^6P_5 = 5! \times 6! = 86,400$

2. In how many ways can 10 boys and 5 girls stand so that no two girls are next to each other if they are standing

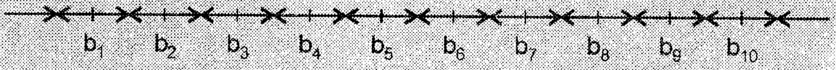
i. Along a straight line ii Around a circle.

1

PU
Apr. 2009 – 5M

Solution

i. Standing along a straight line first we make arrangement of 10 boys in a line, which can be done in $10p_{10} = 10!$ ways.



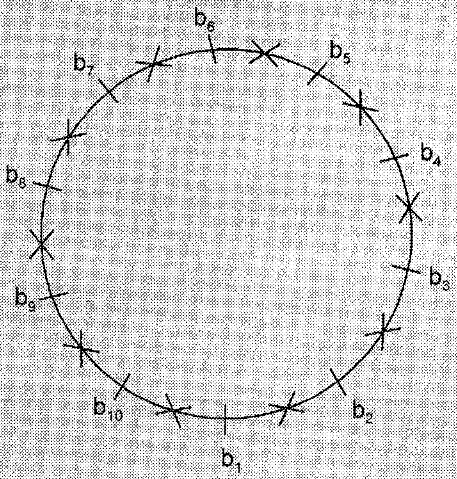
In between the boys there are 11 positions (marked with x) where girls can be arranged the number of ways for this is $11\ p_5$.

$\therefore$ Total number of ways $= 10! \times 11p_5$

$= 10! \times 3628800$

$= 2.011867 \times 10^{11}$

ii. Standing around a circle



First we arrange for boys around a circle. As there are 10 boys they can be arranged in $(10-1)! = 9!$ ways.

Now after arranging for boys there are 10 places for girls, one each between two boys. Hence girls one can be arranged in $10p_5$ ways.

$\therefore$ Total number of ways $= 9! \times 10p_5$

$= 9! \times 4320$

$= 1567641600$

3.4 Permutations with Repetitions of Objects

Here the objects in a set S are not all different and we want to make permutation of all these n objects.

▶Theorem 3

Suppose there are n objects, of which n_1 are identical of first type, n_2 are identical of second type, . . . n_k are identical of k^{th} type so that $n_1+n_2+...+n_k = n$. Then the number of permutations of these n objects, taken all at a time, is denoted by $P(n; n_1, n_2, ..., n_k)$ and is given by,

$$\mathbf{P(n; n_1, n_2, ..., n_k) = \binom{n}{n_1}\binom{n-n_1}{n_2}...\binom{n-n_1-n_2...-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!...n_k!}}$$

Proof

We have to fill n places in a row with the given objects. First we can choose n_1 of the n places in $\binom{n}{n_1}$ ways and place n_1 like objects of the first kind in these places uniquely. Then n_2 of the remaining in $(n-n_1)$ places can be choosen in $\binom{n-n_1}{n_2}$ ways and n_2 like objects of the second kind can be placed in these places uniquely.

In this way, having placed the objects of types $n_1, n_2, ..., n_{k-1}$, there remains $(n-n_1-n_2...-n_{k-1}) = n_k$ places and n_k of these can be chosen in $\binom{n-n_1-n_2-...-n_{k-1}}{n_k}$ ways and n_k like objects of the k^{th} kind can be placed in these places uniquely, so by multiplication theorem, total number of permutations is

$$P(n;n_1,n_2,...n_k) = \binom{n}{n_1}.\binom{n-n_1}{n_2}...\binom{n-n_1-n_2...-n_{k-1}}{n_k}$$

$$= \frac{n!}{n_1!(n-n_1)!} \times \frac{(n-n_1)!}{(n-n_1-n_2)!n_2!} \frac{(n-n_1-n_2)!}{(n-n_1-n_2-n_3)n_3!} \cdots = \frac{n!}{n_1!n_2!...n_k!}$$

Example

1. a. **How many arrangements are there of all the letters in 'SOCIOLOGICAL'?**

   b. **In how many of the arrangements in part (a) are there A and G adjacent.**

Solution

a. There are 12 letters A, L, L, S, G, I, I, D, O, O, C, C of these there are 3 unrepeated letters A, S, G, 3 letters each repeated twice (L, I, C) and one letter (O) repeated thrice.

i.e., $n = 12$, $n_1 = 2$ (L)

$n_2 = 2$ (I)

$n_3 = 2$ (C)

$n_4 = 3$ (O)

So total number of arrangements of the given word $= \frac{n!}{n_1!n_2!n_3!n_4!} = \frac{12!}{2!\ 2!\ 2!\ 3!} = 9979200$

b. If we treat A and G as a single letter say X then we have to permute X, S, L, L, I, I, C, C, O, O, O

then $n = 11$ $n_1 = 2\ (L)$
$n_2 = 2(I)$
$n_3 = 2\ (C)$
$n_4 = 3(O)$

So these 11 letters can be arranged in $\frac{11!}{2!\ 2!\ 2!\ 3!}$ also in the letter X, A and G can be arranged in 2! ways. Hence total number of ways of arranging by multiplication principle is

$$\frac{11!}{2!\ 2!\ 2!\ 3!} \times 2! = \frac{11!}{2!\ 2!\ 2!\ 3!} = 1663200$$

4. Combinations

4.1 r-Combination of n Elements

Definition

An **unordered** selection of r objects from a set S containing n different objects is a r-combination of n elements.

▶Theorem 4

The number of r-combinations of an n-elements set S is denoted by $\binom{n}{r}$ or ^nC_r or C(n, r) and is given by, $^nC_r = \frac{^nP_r}{r!} = \frac{n!}{(n-r)!r!}$, $0 \le r \le n$

Proof

Consider any one of the ^nC_r combinations of S, say x. Now by arranging the r objects in x, taken all at a time, in all possible ways in a row we get r! permutations. Doing this for each of the ^nC_r combinations we get in all $^nC_r \times r!$ different permutations. But every permutation containing r objects can be derived from the corresponding combination by the above process. Hence above process gives us all the ^nP_r permutations of S.

Hence $^nP_r = {^nC_r} \times r!$

$$\therefore\ ^nC_r = \frac{^nP_r}{r!} = \frac{n!}{(n-r)!\ r!}$$

Note: In particular if r = 0,

then $^{n}C_0 = \dfrac{n!}{(n-0)!0!} = 1$

If r = n

$^{n}C_n = \dfrac{n!}{(n-n)!0!} = 1$

If r = 2

$^{n}C_2 = \dfrac{n!}{(n-2)!2!} = \dfrac{n(n-1)}{2}$

Some properties of $^{n}C_r$ we list in the following theorem without proof.

▶ Theorem 5

For any positive integers n, r (r ≤ n) we have,

i. $^{n}C_r = {}^{n}C_{n-r}$, if $0 \leq r \leq n$

ii. $^{n}C_r + {}^{n}C_{r-1} = {}^{n+1}C_r$, if $1 \leq r \leq n$

iii. $^{n}C_r = \dfrac{n}{r} \times {}^{n-1}C_{r-1}$, if $1 \leq r \leq n$

iv. $^{n}C_0 + {}^{n}C_1 + \ldots + {}^{n}C_n = 2^n$.

v. $^{n}C_0 + {}^{n}C_2 + {}^{n}C_4 + \ldots = {}^{n}C_1 + {}^{n}C_3 + {}^{n}C_5 + \ldots = 2^{n-1}$

vi. $\sum\limits_{r=0}^{k} {}^{m}C_r \,.\, {}^{n}C_{k-r} = {}^{m+n}C_k$

vii. $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$

Examples

1. **There are three sections in a question paper each containing 5 questions. A candidate has to solve any 5 questions at least one question from each section. In how many ways can be make his choice?**

Solution

Since the candidate has to solve at least one question from 5 questions from each section, then the alternative ways for this can be tabulated as follows:

		Section I	Section II	Section III
	a)	1	1	3
or	b)	1	3	1
or	c)	3	1	1
or	d)	2	2	1
or	e)	2	1	2
or	f)	1	2	2

The number of ways for each of a), b) and c) are ${}^5C_1 \times {}^5C_1 \times {}^5C_3$ and those for each of d), e) and f) are ${}^5C_2 \times {}^5C_2 \times {}^5C_1$. Hence by addition theorem, total number of ways is $({}^5C_1 \times {}^5C_1 \times {}^5C_3)$ + $({}^5C_1 \times {}^5C_3 \times {}^5C_1)$.

Hence by addition theorem, total number of ways is

$$({}^5C_1 \times {}^5C_1 \times {}^5C_3) + ({}^5C_1 \times {}^5C_3 \times {}^5C_1) + ({}^5C_3 \times {}^5C_1 \times {}^5C_1) + ({}^5C_2 \times {}^5C_2 \times {}^5C_1)$$

$$+ ({}^5C_2 \times {}^5C_1 \times {}^5C_2) + ({}^5C_2 \times {}^5C_2 \times {}^5C_1)$$

$$= 3 \times ({}^5C_1 \times {}^5C_1 \times {}^5C_3) + 3 \times ({}^5C_2 \times {}^5C_2 \times {}^5C_1)$$

$$= 3 \times \left(5 \times 5 \times \frac{5.4}{2}\right) + 3\left(\frac{5.4}{2} \times \frac{5.4}{2} \times 5\right) = 2250$$

2. How many ways can a committee be formed from four men and six women with:

i. atleast 2 men and atleast twice as many women as men.

ii. four members at least 2 of which are women, and Mr. and Mrs. Baggins will not serve together.

Solution

i. Committee with atleast 2 men and at least twice as many women as men with the given condition the committee can consist.

	Men	Women
or	2	4
or	2	5
or	2	6
or	3	6

So the number of selection is

$$({}^4C_2 \times {}^6C_4) + ({}^4C_2 \times {}^6C_5) + ({}^4C_2 \times {}^6C_6) + ({}^4C_3 \times {}^6C_6)$$

$$= \left(6 \times \frac{6 \times 5}{2}\right) + (6 \times 6) + (6 \times 1) + (4 \times 1) = 136$$

ii. Committee with four members, at least 2 of which are womens and Mr. and Mrs. Baggins will not serve together.

The total number of ways of committees with at least 2 women is

Men	Women
2	2
1	3
0	4

$$n_1 = ({}^4C_2 \times {}^6C_2) + ({}^4C_1 \times {}^6C_3) + ({}^4C_0 \times {}^6C_4)$$

$$= \left(6 \times \frac{6 \times 5}{2}\right) + \left(4 \times \frac{6 \times 5 \times 4}{3 \times 2}\right) + \left(1 \times \frac{6 \times 5}{2}\right) \quad = \quad 185$$

and the ways in which Mr. and Mrs. Baggins serve together is for which

	Men	Women
or	1 man and Mr. Baggins	2 = 1 other woman and Mrs. Baggins
	Mr. Baggins	3 = 2 other women and Mrs. Baggins

$$n_2 = ({}^4C_1 \times {}^5C_1) + ({}^4C_0 \times {}^5C_2) \quad = \quad (4 \times 5) + \left(\frac{5 \times 4}{2}\right) \quad = \quad 10$$

Hence the number of ways of selecting committee with the given condition is

$$n_1 - n_2 \quad = \quad 185 - 10 \; = \; 175$$

4.2 Binomial Theorem

For every positive integer n, we have

$$(x+a)^n \quad = \quad {}^nC_0\, x^n + {}^nC_1\, x^{n-1}a + {}^nC_2\, x^{n-2}a^2 + \ldots + {}^nC_r x^{n-r}a^r + \ldots + {}^nC_n\, x^n.$$

$$= \sum_{r=0}^{n} {}^nC_r\, x^{n-r}\, a^r$$

The numbers ${}^nC_r = \dfrac{n!}{(n-r)!\,r!}$, are called the *binomial coefficients.*

4.3 Multinomial Coefficients

A set of n distinct items is to be divided into r distinct groups of respective sizes $n_1, n_2, \ldots, n_r$ where $\sum\limits_{i=1}^{n} = n$. Then these are $\binom{n}{n_1}$ possible choices for the first group; for each of choice of the first group there are $\binom{n-n_1}{n_2}$ possible choices for the second group; for each choice of the first two groups there are $\binom{n-n_1-n_2}{n_3}$ possible choices for the third group; and so on. Hence by generalized principle of multiplication principle it follows that there are

$$\binom{n}{n_1} \cdot \binom{n-n_1}{n_2} \cdot \binom{n-n_1-n_2}{n_3} \ldots \binom{n-n_1-n_2 \ldots -n_{r-1}}{n_r}$$

$$= \frac{n!}{(n-n_1)!n!} \times \frac{(n-n_1)!}{(n-n_1-n_2)!n_2!} \times \frac{(n-n_1-n_2)!}{(n-n_1-n_2-n_3)!n_3!} \times \ldots \frac{(n-n_1-n_2 \ldots - n_{r-1})!}{(n-n_1-n_2 \ldots -n_{r-1}- n_r)!\, n_r\,!}$$

$$= \frac{n!}{n_1!n_2! \ldots n_r!} \text{ possible divisions}$$

The number $\dfrac{n!}{n_1!n_2! \ldots n_r!}$ is denoted by $\binom{n}{n_1, n_2, \ldots, n_r}$ and are known as *multinomial coefficients.*

4.4 Multinomial Theorem

Let n, r be positive integers.

Then the expansion of $(x_1 + x_2 + \ldots + x_r)^n$ is given by

$$(x_1 + x_2 + \ldots + x_r)^n = \sum \frac{n!}{n_1!n_2!\ldots n_r!}\ x_1^{n_1} \cdot x_2^{n_2} \ldots x_r^{n_r}$$

where the sum is taken over all sequences $n_1, n_2, \ldots, n_r$ of non-negative integers such that $n_1 + n_2 + \ldots n_r = n$

Examples

1. Find the coefficient of $x^6y^6z^5$ in the expression of $(2x^2 - 3y^3 + 5z)^{10}$.

1 PU Oct. 2010 – *7M*

Solution

By using multinomial theorem,

Coefficient of $x^6y^6z^5$ is

$$= \frac{10!}{3!2!5!} 2^3 (-3)^2 \cdot (5)^5 = \frac{10 \times 9 \times 8 \times 7 \times 6}{3 \times 2 \times 2} \times \overset{4}{8} \times 9 \times 3125 = 567000000.$$

2. Find coefficient of x^7 in the expansion of $(1+3x-2x^3)^{10}$.

1 PU Apr. 2010 – *7M*

Solution

The general term in the expansion of $(1+3x-2x^3)^{10}$ is,

$$\frac{10!}{a!b!c!} 1^a (3x)^b (-2x^3)^c = \frac{10!}{a!b!c!} \cdot 3^b (-2)^c . x^{b+3c}$$

where $a+b+c = 10$ and the terms in x^7 are given by $b+3c = 7$. So we have to find the common non-negative integer solutions of the equations $a+b+c = 10$ and $b+3c = 7$ and $0 \leq a, b, c, \leq 10$. From second equation for $c = 0, 1, 2$ we have $b = 7, 4, 1$ and with these values from equation first, values of a are 3, 5, 7 respectively.

So the required coefficient is,

$$\frac{10!}{3!7!0!} 3^7 + \frac{10!}{5!4!1!} 3^4(-2)^1 + \frac{10!}{7!1!2!} 3(-2)^2$$

$$= \frac{10 \times 9 \times 8}{3 \times 2} \times 3^7 + (-2) \times \frac{10 \times 9 \times 8 \times 7 \times 6}{4 \times 3 \times 2} \times 3^4 + \frac{10 \times 9 \times 8}{2} \times 3 \times (-2)^2 = 62640$$

3. State and prove multinomial theorem and hence find the coefficient of $x^2y^4z^3$ in the expansion of $(x - 2y + 3z)^9$.

1 PU Oct. 2009 – *7M*

Solution

Multinomial theorem

For n, a positive integer, $(x_1 + x_2 + \ldots + x_k)^n$

$$= \sum_{n_i \geq 0} \binom{n}{n_1, n_2, \ldots n_k} x_1^{n_1} \cdot x_2^{n_2} \ldots x_k^{n_k}$$

Where summation is taken over all non-negative n_i's so that $\sum_{i=1}^{k} n_i = n$

and $\binom{n}{n_1, n_2, \ldots n_k} = \frac{n!}{n_1!\, n_2! \ldots n_k!}$ is the multinomial coefficient.

Proof: We prove the result by method of induction for k.

Step 1: When k =1, the result is obviously true.

Step 2: When k =2, the result is nothing but the binomial theorem.

Step 3: Assume that, the result is true for k = r i.e.

$$(x_1 + x_2 + \ldots + x_r)^n =$$

$$\sum \frac{n!}{n_1!\, n_2! \ldots n_r!} x_1^{n_1} x_2^{n_2} \ldots x_r^{n_r}$$

$$\sum_{i=1}^{r} n_i = n, \qquad n_i \geq 0.$$

Step 4: For k = r +1

$$(x_1 + x_2 + \ldots + x_r + x_{r+1})^n$$

where $y = x_1 + x_2 + \ldots + x_r$

$$= (y + x_{r+1})^n$$

$$= \sum_{s=0}^{n} {}^nC_s\, y^s \cdot x_{r+1}^{n-s} \quad \ldots \text{ by binomial theorem}$$

$$= \sum_{s=0}^{n} {}^nC_s \cdot [(x_1 + x_2 \ldots + x_r)^s]\, x_{r+1}^{n-s}$$

$$= \sum_{s=0}^{n} {}^nC_s \left[\sum_{n_i \geq 0} \frac{s!}{n_1!\, n_2! \ldots n_r!} x_1^{n_1} \cdot x_2^{n_2} \ldots x_r^{n_r} \right] x_{r+i}^{n-s} \; (n_1 + n_2 + \ldots + n_r = s)$$

$$= \sum \frac{n!}{s!\,(n-s)!} \frac{s!}{n_1!\, n_2! \ldots n_r!} x_1^{n_1} \cdot x_2^{n_2} \ldots x_r^{n_r} \cdot x_{r+1}^{n-s}$$

$$= \sum \frac{n!}{n_1!\, n_2! \ldots n_r!\,(n-s)!} x_1^{n_1} \cdot x_2^{n_2} \ldots x_r^{n_r} \cdot x_{r+1}^{n-s}$$

$$= \sum \frac{n!}{n_1!\, n_2! \ldots n_r!\, n_{r+1}!} x_1^{n_1} \cdot x_2^{n_2} \ldots x_r^{n_r} \cdot x_{r+1}^{r+1}$$

where $n_{r+1} = n - s$

and $n_1 + n_2 + \ldots + n_{r+1} = n$

so the result is true for k = r +1.

Hence, by induction the result is true for k-integers.

Coefficient of $x^2 y^4 z^3$ in $(x - 2y + 3z)^9$ is

$$= \frac{9!}{2!\,4!\,3!}(-2)^4 \cdot (3^3) = \frac{9 \times 8 \times 7 \times 6 \times 5}{2 \times 3 \times 2} \times 16 \times 27 = 544320$$

3. Find the co-efficient of $w^3x^2\,y\,z^2$ in $(2w - x + 3y - 2z)^8$.

1

PU
Oct. 2010 – 7M

Solution

We have $n_1 = 3$, $n_2 = 2$, $n_3 = 1$, $n_4 = 1$ with $n_1 + n_2 + n_3 + n_4 = 3 + 2 + 1 + 1 = 8 = n$

$\therefore$ By multinomial theorem. coefficient of $w^3x^2yz^2$ is

$$= \frac{8!}{3!\,2!\,1!\,2!}(-1)^2(-1)^2 = \frac{8!}{6\times2\times2} = 1680$$

4.5 Combinations with Repetitions

Suppose $S = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$ is a set containing 8 different objects. Then a 5-combination of S with repetitions allowed is $t = a_1a_2a_5a_5a_8$. To count the number of such five combinations, we first agree to pick the objects $a_1, a_2, \ldots$ in the order indicated by the suffixes 1, 2,. . .. Then we use a vertical line to separate the repeated occurrences of a_i, $i = 1,2, \ldots ,8$. Thus to separate 8 objects we need $8 - 1 = 7$ vertical lines and the combination t is written as

$$t = a_1|a_2|||a_5a_5|||a_8,$$

Here the three vertical lines between a_2 and a_5 indicate that a_3 and a_4 not included similarly three vertical lines between a_5 and a_8 indicate that a_6 and a_7 not included.

Since $a_1, a_2, \ldots ,$ are picked in succession, we need not use the suffixes for a's. Thus the combination t can be written as,

$$t = a|a|||aa|||a$$

Thus it is clear that any 5-combination s of S can be uniquely specified by arranging 5 a's in a row separated by 7 vertical lines in the following way: first a is written as many times as a_1 occurs in S then a vertical line is inserted then a is written as many times a_2 occurs in S and then a vertical line inserted and so on. Thus, each 5-combination uniquely corresponds to a permutation of 7 vertical lines and 5 a's. Conversely, every such permutation uniquely corresponds to a combination of S with repetition. *For example*, the permutation a||aa|||a||a corresponds to the 5-combination with repetition $a_1a_3a_3a_6a_8$. Now, there are $\frac{(7+5)!}{7!5!} = \binom{12}{5} = \binom{8-1+5}{5}$.

Permutations of 7 vertical lines and 5 a's. Hence the number of 5-combinations of S with repetitions and so it is $\binom{8-1+5}{5}$.

▶Theorem 6

Let $S = \{a_1, a_2, \ldots , a_n\}$ be a set with n distinct elements. Then any r combination t of S with repetitions allowed can be uniquely represented by a permutation of $(n - 1)$ vertical lines and r a's as follows: first a is written as many times as a_1 occurs in t and then a vertical line is inserted, then a is written as many times as a_2 occurs in t and then a vertical line is inserted, and so on. Conversely it is clear that every such permutations uniquely corresponds to an r-combination of S, with repetition. Hence the number of r-combinations of S, with repetitions allowed is the same as the number of such permutations and so it is $\frac{((n-1)+r)!}{(n-1)!r!} = \binom{n-1+r}{r}$.

4.6 Distributions

A distribution is defined as separation of a set into a number of classes; *for example*, the assignment of objects to boxes. Here we consider the following cases for distribution of objects.

Case i. Distinct objects in distinct cells

Suppose r different objects are to be assigned to n distinct boxes. Here again there are two possibilities; each of the boxes may hold

a. atmost one object or

b. any number of objects.

a. Suppose each box may hold at most one object. Let $n \geq r$. Then the first object may be put into any one of the n boxes, then the second object may be put into any one of the remaining (n–1) boxes and so on. Hence the number of ways of putting r different objects into n distinct boxes is,

$$n(n-1)\,(n-2)\ldots(n-r+1) = {}^nP_r$$

If $r \geq n$, then these are ${}^rp_n$ ways, since the object put in the first box may be any one of the r objects, the object put in the second box may be any one of the remaining (r–1) objects and so on.

b. Suppose each box may hold any number of objects. Then the first object may be put into any one of the n boxes, the second object may also be put into anyone of the n boxes. Hence the number of ways of distributed the objects is,

$$n.n.\,.\,.n = n^r$$

This is true whether $n \geq r$ or $n \leq r$.

Case ii. Indistinguishable objects in distinct cells

a. Suppose each box may hold atmost one object and let $n \geq r$. Suppose r objects to be distributed are not all distinct, but r_1 of them are alike of the first kind r_2 of them are alike of the second kind,. . . , r_k of them are alike of the k^{th} kind and $r = r_1+r_2+\ldots+r_k$

Now r of the n boxes can be chosen in $\binom{n}{r}$ ways. Then the r objects are distributed in the r chosen boxes, which is equivalent to a permutation with repetition. The number of such permutations is, $\frac{r!}{r_1!r_2!\ldots r_k!}$.

Hence the number of distribution is,

$$\binom{n}{r} \cdot \frac{r!}{r_1!r_2!\ldots r_k!} = \frac{n!}{(n-r)!r_1!\, r_2!\ldots r_k!}$$

In particular when the r objects are all alike, there is only one kind and $r_1 = r$, hence number of such distribution is,

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

b. Suppose we have r like objects and each box may hold any number of objects. Here there is no restriction on the number of objects put into any box. Hence distributing the r objects into n distinct boxes is equivalent to selecting r of the n boxes with repetition of boxes allowed, so the number of distribution is, $\binom{n-1+r}{r}$.

Case iii. Distinct objects in indistinguishable cells

For $m \geq n$ there are $\sum_{k=0}^{n} (-1)^k \binom{n}{n-k} \cdot (n-k)^m$

ways to distribute m distinct objects into n numbered (but otherwise identical) containers with no containers left empty. Removing the numbers on the containers so that they are now identical in appearance, we find that one distribution into these n (nonempty) identical containers corresponds with n! such distributions into the numbered containers. So the number of ways in which it is possible is to distribute the m distinct objects into n identical containers, with no container left empty is,

$$\frac{1}{n!} \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{n-k} \cdot (n-k)^m$$

For example, if A = {a, b, c, d} and B = {1,2,3} then there are

$\binom{3}{3}3^4 - \binom{3}{2}.2^4 + \binom{3}{1}.(1)^4 = 3^4 - 3.2^4 + 3 = 36$ onto functions from A to B i.e. there are 36 ways to distribute 4 distinct objects into three distinguishable cells. Among these distribution consider one of the six such possible collections of six, namely,

1. $\{a, b\}_1, \{c\}_2, \{d\}_3$
2. $\{a, b\}_1, \{d\}_2, \{c\}_3$
3. $\{c\}_1, \{a, b\}_2, \{d\}_3$
4. $\{c\}_1, \{d\}_2, \{a, b\}_3$
5. $\{d\}_1, \{a, b\}_2, \{c\}_3$
6. $\{d\}_1, \{c\}_2, \{a,b\}_3$

where *for example* $\{c\}_3$ means C is in the third container. Now if all these containers become identical, then 6 = 3! distributions become identical, so there are $\frac{36}{3!} = 6$ ways to distribute the distinct objects a, b, c, d into three identical containers, leaving no container empty.

Case iv: Indistinguishable objects in indistinguishable cells

Suppose we have n identical objects which are put into m identical boxes, so that no box is empty. Let $n_1, n_2, \ldots, n_m$ be the numbers of objects in these. The indexing here is purely arbitrary, since the boxes are identical we cannot call them as the first, one as the second. Each n_i is positive integer and obviously $n_1 + n_2 + \ldots + n_m = n$. Note that the integer n_i's (each counted with its multiplicity if any) completely determine the arrangement of the objects into boxes. Thus this problem reduces to partitioning the integer n, into m parts which we write as $P_{n, m}$.

The number of ways to put n indistinguishable objects into r indistinguishable boxes is

$$\sum_{m=1}^{n} P_{n, m} = P(n).$$

Examples

1. **How many ways are there to place 25 different flags on 10 numbered flagpoles if the order of the flags on a flagpole is**

   a. not relevant? b. relevant?

Solution

a. If order of flags on a flaghole is not relevant then first flag can be flied on any one of the 10 flagpoles in 10 ways after that second flag on any one of the 10 poles and so on.

So total number of ways $= \underbrace{10 \times 10 \times 10 \times \ldots \times 10}_{(25\text{ times})} = 10^{25}$.

b. If the order of flagpole is relevant then first flag can be flied on any one of the 10 poles in 10 ways. After that the second flag can be flied on 10 poles not in 10 ways put in 11 ways, i.e. 9 ways on other poles and one below and one above the pole on which first flag was flied. Similarly for the third flag there are 12 ways and so on for the 25th flag there are 34 ways, hence

Total number of ways $= 10 \times 11 \times 12 \times \ldots \times 34 = \frac{34!}{9!}$

2. **How many ways are there to invite 1 of 3 friends over for dinner on six successive nights such that no friend is invited more than 3 times?**

Solution

Let x, y, z denote friends and (a, b, c) denote the case where x is invited a times, y is invited b times and z is invited c times. Now we have following possibilities.

i. (a, b, c) = (1, 2, 3); (1, 3, 2); (2, 3, 1);
(2, 1, 3); (3, 1, 2); (3, 2, 1);

ii. (a, b, c) = (3, 3, 0); (3, 0, 3) (0, 3, 3)

iii. (a, b, c) = (2, 2, 2)

So total number of ways $= 6 \times \frac{6!}{1!\,2!\,3!} + 3 \times \frac{6!}{3!\,3!} + \frac{6!}{2!\,2!\,2!} \quad = 510$

EXERCISE

1. How many ways are there to roll two dice to yield a sum divisible by 3?
2. How many times the digit 0 written when listing all numbers from 1 to 3333?
3. i. How many ways can the letters of the word SOCIOLOGICAL be arranged?
   ii. In how many ways the arrangements in part (a) are A and G adjacent?
   iii. In how many ways to arrangements in part (a) are all vowels adjacent?
4. A student is to answer 7 out of 10 questions on an examination. In how many ways can be selection if
   i. there are no restrictions?
   ii. he must answer the first two questions?
   iii. he must answer atleast four of the first six questions?
5. How many ways can 12 identical white and 12 identical black pawns be placed on the black squares of an 8 × 8 board?
6. There are 12 members in a committee who sit around a table. There is one place specially designed for the chairman. Besides the chairman there are 3 people who constitute a subcommittee. Find the number of seating arrangements if
   i. the subcommittee sit together as a block, and
   ii. number 2 of the subcommittee sit next to each other.
7. Calculate the coefficient of $x^6 y^6 z^5$ in the expansion of $(2x^2-3y^3+5z)^{10}$.
8. How many ways are there to distribute 20 different toys among 5 children
   i. Without restrictions?
   ii. If 2 children get 7 toys and 3 children get 2 toys?
9. A shop sells 9 different flavours of ice-cream. In how many ways can a customer choose 5 ice-cream cones if
   i. they are all of different flavours;
   ii. they are not necessarily of different flavours;
   iii. they contain only 3 different flavours?
10. Find coefficient of
    i. x^5 in $(1+2x-\frac{1}{2}x^2)^9$ ii. a^2b^5d in $(a+b-c-d)^8$

Hints and Answers

1. (x, y) is required outcome iff (x+y) = 3 , 6, 9, 12. **Ans: 12 ways.**
2. We have to consider integers t such that $1 \leq t \leq 3333$. Clearly the largest t having 0 in the units place is 3330. So there are 333 numbers t having 0 in the units place viz 10, 20, 30, . . ., 3330. Similarly the numbers having 0 in the tens place will be the type x0y where x can be any one among 1,2,. . .,33, So such numbers are 33 × 10 = 330. In the same way there are $3 \times 10^2 = 300$ numbers with 0 in the hundreds place. So the total number of times 0 is the written is 333+330+300 = 963
3. i. 12! / (3! 2! 2! 2!) ii. 2[11! / (3! 2! 2! 2!)] iii. [7!/(2!2!)][6!/(3!2!)]

4. i. 120 ii. 56 iii. 100

5. There are 32 black squares of these 12 can be chosen to put white pawns in $\binom{32}{12}$ ways. Then out of 20 remaining black squares 12 can be chosen to put 12 black pawn in $\binom{20}{12}$ ways. So total ways $= \binom{32}{12}\binom{20}{12} = \frac{32!}{(12!)^2 8!}$.

6. i. $9! \times 3!$ ii. $8! \times {}^9P_3$

7. 567000000

8. i. 5^{20} ii. 2 children of 5, who get 7 toys each can be chosen in $\binom{5}{2}$ways.

Now the first gets 7 toys in $\binom{20}{7}$ ways and second gets 7 toys in $\binom{13}{7}$ ways and remaining 3 children get 2 toys in number of ways is $\binom{6}{2} \times \binom{4}{2} \times \binom{2}{2}$.

$\therefore$ Total number of ways $= \binom{5}{2} \times \binom{20}{7} \times \binom{13}{7} \times \binom{6}{2} \times \binom{4}{2} \times \binom{2}{2} = \binom{5}{2} \times \frac{20!}{(7!)^2 \times (2!)^3}$

9. i. $\binom{9}{5} = 126$

ii. $\binom{9-1+5}{5} = \binom{13}{5} = 1287$

iii. The number of ways of choosing 5 cones of exactly 3 flavours with repetitions = (the number of ways of choosing 3 flavours out of 9) × (number of ways of choosing 5 cones of 3 choosen flavours) $= \binom{9}{3} \times 6 = 504$.

because for each choice say a, b, c there are 6 ways of choosing 5 cones namely, aabbc, abbcc, aabcc, aaabc, abbbc, abccc.

10. i. 2142 ii. –168

Collection of Questions asked in Previous Exams PU

1. In how many ways can 10 boys and 5 girls stand so that no two girls are next to each other if they are standing **[Apr. 2009 – 5M]**
   i. Along a straight line ii Around a circle.
2. Find the co-efficient of $w^3x^2 y z^2$ in $(2w–x+3y–2z)^8$. **[Apr. 2009 – 5M]**
3. In how many ways can 10 persons be seated in a row? If 3 of these are women, how many ways can 10 people be arranged so that no two women sit side by side? **[Oct. 2009 – 5M]**
4. How many 3 digit numbers can be formed by using the 6 numbers 2, 3, 4, 5, 6 and 8 if:
   i. Repetition not allowed
   ii. Number must contain the digit 5 and repetitions are allowed. **[Apr. 2010 – 5M]**
5. State multinomial theorem and find the coefficient of x^7 in $(1 + 3x – 2x^3)^{10}$. **[Apr. 2010– 7M]**
6. Find the coefficient of $x^6y^6z^5$ in the expression of $(2x^2 – 3y^3 + 5z)^{10}$. **[Oct. 2010– 7M]**

4 Number of Non-Negative Integer Solutions

1. Introduction

To find the number of integer solutions is a corollary to theorem to count the number of r-combinations out of n distinct objects. In this chapter we also discuss various binomial identities.

2. Integer Solutions of Linear Equations

2.1 Non-negative Integer Solutions

▶Theorem 1

Let n, r be given positive integers. Then the number $A_{n,\, r}$ of non negative integer solutions $(x_1, x_2, \ldots, x_n)$ of the equation,

$$x_1 + x_2 + \ldots + x_n = r \quad \text{...(1)}$$

is $\binom{n-1+r}{r}$

Proof

Let S = $\{a_1, a_2, \ldots, a_n\}$ be a set with n distinct elements. Given any r-combination t of S, with repetitions allowed, (say $t = a_2a_2a_2a_5a_7$, $n = 7$, $r = 5$). Let x_i be the number of times a_i occurs in t.

Then t corresponds to the solution $(x_1, x_2, \ldots, x_n)$ of (1). (Thus the above 5-combination $t = a_2\, a_2\, a_2\, a_5\, a_7$ corresponds to the solution (0, 3, 0, 0, 1, 0, 1) of the equation $x_1 + x_2 + \ldots + x_7 = 5$).

Conversely, every non-negative integer solution of (1) corresponds to a unique r-combination of S, with repetitions allowed. Hence by the theorem of r-combinations out of n distinct objects, with repetitions allowed, $A_{n,\,r} = \binom{n-1+r}{r}$.

1. How many solutions are there to equation $x_1 + x_2 + x_3 = 17$ where x_1, x_2 and x_3 are non-negative with $x_1 < 6$ and $x_3 > 5$?

1
PU
Apr. 2010 – 8M

Solution

The number a_r of non-negative integer solutions of $x_1 + x_2 + x_3 = 17$, where x_1, x_2 x_3 are non-negative with $x_1<6$ and $x_3>5$ is obtained from the generating function.

$$f(x) = (1 + x + x^2 + x^3 + x^4 + x^5)\,(1 + x + x^2 + \ldots)\,(x^5 + x^6 + \ldots)$$

$$= [(1 - x^6)\,(1 - x)^{-1}]\,(1 - x)^{-1} \cdot x^5[1 + x + x^2 + \ldots]$$

$$= (1 - x^6)\,(1 - x)^{-2} \cdot x^5 \cdot (1 - x)^{-1}$$

$$= x^5\,(1 - x^6)\,(1 - x)^{-3} = x^5\,(1 - x^6) \sum_{r=0}^{\infty} \binom{3 + r - 1}{r} x^r = x^5\,(1 - x^6) \sum_{r=0}^{\infty} \binom{2 + r}{r} x^r$$

Hence, the number of required solutions of $x_1 + x_2 + x_3 = 17$ is the coefficient of x^{17} in f(x) which is,

$$\left[\binom{2+12}{12} - \binom{2+6}{6}\right] = \binom{14}{12} - \binom{8}{6} = \frac{14 \times 13}{2} - \frac{8 \times 7}{2} = 63$$

2. An elevator starts the basement with 8 people (excluding the elevator operator) and discharges them all by the time it reaches the top floor, number 6.

i. In how many ways could the operator have perceived the people leaving the elevator if all people look alike to him?

ii. What if the 8 people consist of 5 men and 3 women and operator could tell a man from a woman?

1
PU
Oct. 2010 – 8M

Solution

i. Let x_1, x_2, x_3 . . .x_6 be number of people discharged at floor number 1, 2, 3, . . .6 respectively, $x_i \geq 0$, i= 1, 2 . . .6. Since there are 8 people excluding the operator, the values of x_i's are nothing but a non-negative solution to the equation

$$x_1 + x_2 + \ldots + x_6 = 8$$

and the solution is given by

$$\binom{n-1+r}{r} = \binom{6-1+8}{8} = \binom{13}{8}$$

$$= \frac{13!}{8!\,5!} = \frac{13 \times 12 \times 11 \times 10 \times 9}{5 \times 4 \times 3 \times 2} = 1287$$

i.e., the operator can perceive people in 1287 ways.

3. If 8 identical black boards are to be divided among 4 schools, how many divisions are possible?

i. with no restriction

ii. each school must get at least 1 blackboard.

1

PU
Oct. 2009 – *4M*

Solution

Let x_i denote the number of black boards received by ith school, i = 1, 2, 3, 4.

i. Here we have $x_1 + x_2 + x_3 + x_4 = 8$; $x_i \ge 0$. And required no. of divisions is a non-negative solution of $x_1 + x_2 + x_3 + x_4 = 8$ and is given by

$$\binom{n-1+r}{r} = \binom{4-1+8}{8} = \binom{11}{8} = \frac{11!}{8!\,3!} = \frac{11 \times 10 \times 9}{3 \times 2} = 165.$$

ii. Let y_i denote number of black board received by ith school, i = 1, 2, 3, 4 and $y_i \ge 1$ $\forall$ i, i.e., y_i is the positive integer. Solution of the equation

$y_1 + y_2 + y_3 + y_4 = 8$ ....(1)

Let $y_i = x_i + 1$ and $x_i \ge 0$

i.e. $x_i = y_i - 1$, $x_i \ge 0$

$\therefore$ $(x_1 + 1)(x_2 + 1) + (x_3 + 1) + (x_4 + 1) = 8$

or $x_1 + x_2 + x_3 + x_4 = 4$ ....(2)

Hence x_i is a non-negative solution of (2) and is given by

$$\binom{n-1+r}{r} = \binom{4-1+4}{4} = \binom{7}{4} = \frac{7!}{3!\,4!} = \frac{7 \times 6 \times 5}{3 \times 2} = 35$$

2.2 Positive Integer Solutions

▶Corollary I

Let $r \ge n > 0$ be integer. The number $B_{n,\,r}$ of solutions $(x_1, x_2, \ldots, x_n)$ of equation (1) in positive integers is $\binom{r-1}{n-1}$.

Proof

Let $(y_1, y_2, \ldots, y_n)$ be any solution of (1) in positive integers, so that $y_1 + y_2 + \ldots + y_n = r$. Let $x_i = y_i - 1$. Then the last equation becomes

$$x_1 + x_2 + \ldots x_n + n = r$$

$$\therefore \; x_1 + x_2 + \ldots + x_n = r - n \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Hence $(x_1, x_2, \ldots, x_n)$ is non-negative integer solution of (2). Conversely, every non-negative integer solution of (2) corresponds to a unique positive integer solution $(y_1, y_2, \ldots, y_n)$ of (1) with $y_i = x_i + 1$. Hence by above theorem

$$B_{n,\,r} = \binom{n-1-(r-n)}{r-n} = \binom{r-1}{n-1}$$

2.3 Integer Solution with Conditions

▶**Corollary 2**

Let r, n > 0 be integers. Let $a_1, a_2, \ldots, a_n$ be given integers. Then the number of integer solutions of equation (1) such that $x_i > a_i$, $1 \le i \le n$ is $\binom{r - a_1 - a_2 \ldots - a_{n-1}}{n-1}$.

Proof

Given any solution $(y_1, y_2, \ldots, y_n)$ of equation (1) in integers such that $y_i > a_i$, $1 \le i \le n$, so that $y_1 + y_2 + \ldots + y_n = r$. Let $x_i = y_i - a_i$, $i = 1,2,\ldots,n$ then substituting for y's we get,

$$(x_1 + a_1) + (x_2 + a_2) + \ldots + (x_n + a_n) = r$$

$$\therefore\ x_1 + x_2 + \ldots + x_n = r - a_1 - a_2 \ldots - a_n.$$

So that $(x_1, x_2, \ldots, x_n)$ is a positive integer solution of the last equation and conversely. So the required number by corollary 1 is, $\binom{r - a_1 - a_2 \ldots - a_{n-1}}{n-1}$.

Examples

1. **Find number of non-negative solutions of the equation $x_1 + x_2 + x_3 = 24$ subject to the conditions.**

   i. $x_1, x_2, x_3 \ge 0$ **ii.** $x_1 > 1, x_2 > 2, x_3 > 3$ **iii.** $x_1 \ge 3, x_2 \ge 2, x_3 \ge 5$.

Solution

i. Here n =3, r = 24 and integers are non negative, hence the number of non-negative integers solutions is $\binom{n+r-1}{r} = \binom{3+24-1}{24} = \binom{26}{24} = 325$

ii. Let y_1, y_2, y_3 be the required solution to $y_1 + y_2 + y_3 = 24$

Put $x_1 = y_1 - 1, x_2 = y_2 - 2, x_3 = y_3 - 3$

then $y_1 + y_2 + y_3 = 24$ becomes

$(x_1 + 1) + (x_2 + 2) + (x_3 + 3) = 24$

$\therefore\ x_1 + x_2 + x_3 = 18$ and we want positive integer solution, so the number of solutions is,

$$\binom{r-1}{n-1} = \binom{18-1}{3-1} = \binom{17}{2} = 136$$

iii. If (y_1, y_2, y_3) is the solution of the required type, then put $x_1 = y_1 - 3$, $x_2 = y_2 - 2$, $x_3 = y_3 - 5$ then (x_1, x_2, x_3) is non negative solution of $x_1 + x_2 + x_3 = 24 - (3+2+5) = 14$ and so number of such solutions if,

$$\binom{n-1+r}{r} = \binom{3-1+14}{14} = \binom{16}{14} = 120$$

2. **How many different collections of 3 coins can be formed if the coins can be pennies, nickels, dimes, quarter or halt dollars? How many different collections of 5 coins can be formed with the same types of coins?**

Solution

Let x, y, z, w, t be number of coins of pennies, nickels, dimes, quarter or half dollars respectively.

We have to form a collection of 3 coins. Then required number is non-negative integer solution of $x + y + z + w + t = 3$ which is $\binom{5-1+3}{3} = \binom{7}{5} = 35$.

If 5 different collects are to be formed with the same coins then it is a non-negative integer solution of $x + y + z + w + t = 5$. And the number of such collection is $\binom{5+5-1}{5} = \binom{9}{5} = 126$.

3. In how many Rs. 20,000 could be invested in denomination of Rs. 1,000 among 4 different investment opportunities if

i. All money need not be invested?

ii. All investment opportunities must be used?

1

PU
Apr. 2009 – *5M*

Solution

i. Let $x_1, x_2, x_3\ x_4$ be number of units of Rs. 10,000/- in 4 different investments. Let x_5 be amount which is not invested where $x_5 > 0$. Let $y_5 = x_5 - 1$ then, $x_5 > 0 \Rightarrow y_5 \geq 0$ then number of ways Rs. 20,000 should be invested if all money need not be invested is the non-negative integer solution to

$$x_1+x_2+x_3+x_4+x_5 = 20$$

i.e., $x_1+x_2+x_3+x_4+y_5+1 = 20$

i.e., $x_1+x_2+x_3+x_4+y_5 = 19$, with $x_{i,}\ y_5 \geq 0$

which is

$$= \binom{n+r-1}{r} = \binom{4+20-1}{19} = \binom{23}{19}$$

$$= 8855.$$

ii. If all investment opportunities must be used then number of ways for this number of positive solutions to $x_1+x_2+x_3+x_4 = 20$

which is $\binom{r-1}{n-1}$ with $r = 20, n = 4$

$$= \binom{19}{3} = 969$$

where $x_1, x_2, x_3\ x_4$ are the number of units of Rs. 1000/- in 4 different investments.

3. Binomial Identities

In this section we consider some identities involving binomial coefficients. These can be deduced from the binomial theorem or can be proved using a combinatorial argument.

Identity 1: $\binom{2n}{2} = 2 \cdot \binom{n}{2} + n^2$

1

PU
Apr. 2009 – *21/2M*

Proof

Let S be a finite set having 2n elements viz. $S = \{1, 2, \ldots, n, n+1, \ldots 2n\}$

The set S is partitioned into two subsets X and Y each having cardinality n say

$X = \{1, 2, \ldots, n\}$, $Y = \{n+1, n+2, \ldots, 2n\}$.

Every subset of S with 2 elements belongs to one of the following three mutually exclusive classes.

i. The class of all 2-elements subsets of X, there are $\binom{n}{2}$ subsets in this class.

ii. The class of all 2 elements subsets of Y, there are $\binom{n}{2}$ subsets in this class.

iii. The class of all subsets $\{x, y\}$ $x \in X, y \in Y$, there are n^2 subsets in this class.

So $\binom{2n}{2} = \binom{n}{2}+\binom{n}{2}+n^2 = 2 \cdot \binom{n}{2}+n^2$

Identity 2: $\sum\limits_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}$

Proof

Consider the identity

$$(1+x)^m (1+x)^n = (1+x)^{m+n} \quad \text{.......................................}\mathbf{(1)}$$

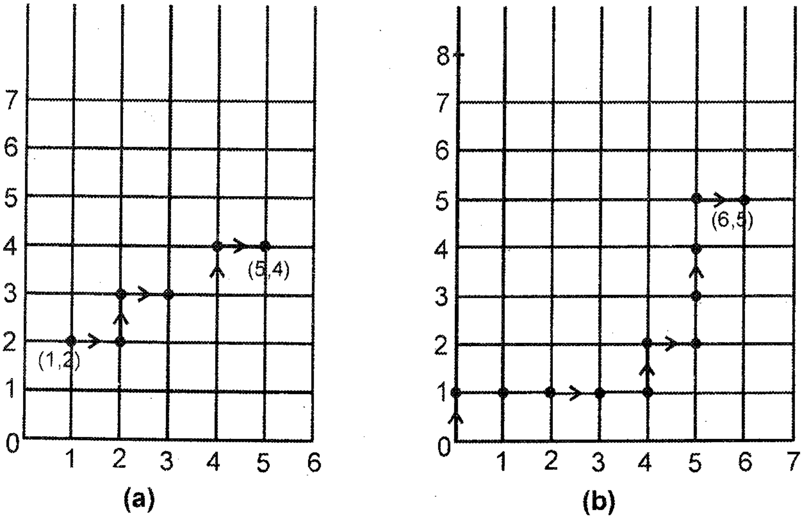
The coefficient of x^r in the left side of (1), namely,

$$\left[\binom{m}{0} + \binom{m}{1}x + \binom{m}{2}x^2 + \ldots + \binom{m}{m} x^m\right] \cdot \left[\binom{n}{0} + \binom{n}{1}x + \ldots + \binom{n}{n} x^n\right]$$

is $\binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \binom{m}{2}\binom{n}{r-2} + \ldots + \binom{m}{r}\binom{n}{0} = \sum\limits_{k=0}^{r}\binom{m}{k}\binom{n}{k-r}$, while the coefficient of x^r on the right side of (1) is, $\binom{m+n}{r}$. Hence we get,

$$\sum_{k=0}^{r} \binom{m}{n}\binom{n}{k-r} = \binom{m+n}{r}$$

Increasing Paths



(a)

(b)

Figure 4. 1

In the XY-plane we consider points whose both coordinates are integers. An increasing path (simply, a path) is a sequence of steps where each step is a move one unit to the right or a move one unit upward. No moves to the left or downward are allowed. *Figure 4.1 (a)* shows such a path from (1,2) to (5,4).

Let m, n be non negative integers. Now we will find the number of paths from the origin O(0,0) to the point P(m, n).

For example, let us count the number of paths from (0,0) to (6,5) as shown in *figure 4.1 (b)*. Let 0 stand for a move one unit to the right and 1 stand for a move one unit upward, then each path will correspond to a sequence of 0's and 1's. In this example, the sequence 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0 corresponds to the path shown in *figure 4.1 (b)*.

Now each path from O to P(6,5) must contain 6 moves to the right and 5 moves upward. Hence each path corresponds to a unique binary sequence of 6 zeros and 5 ones. Conversely, every such binary sequence corresponds to a unique path from O to P(6,5). Hence the number of required paths equals the number of binary sequences of length 6+5 and containing 6 zeros and 5 ones. This number is

$$\frac{(6+5)!}{6!\,5!} = \binom{6+5}{5}$$

The same argument shows the number of path from O to P(m, n) equals the number of binary sequences of length (m+n) and containing m zeros and n one. This number is $\frac{(m+n)!}{m!n!} = \binom{m+n}{n}$.

In particular, the number of paths from (a, b) to the point (m, n) is $\binom{m-a+n-b}{n-b}$ and the number of paths from (0, 0) to (n–r, r) is

$$\binom{n-r+r}{r} = \binom{n}{r}$$

This interpretation of the binomial coefficients can be used to prove many binomial identities.

Identity 3: $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$

1

PU
Apr. 2009 – 21/2 M

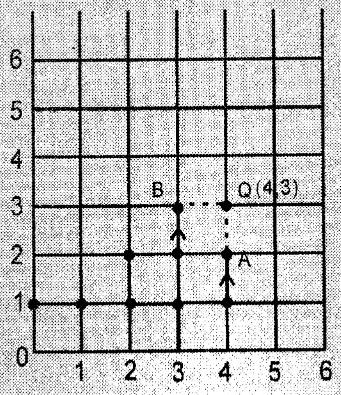


Figure 4. 2

Refer *figure 4.2* clearly each of the $\binom{m}{n}$ paths from O to Q must pass through exactly one of the points A (n–r, r–1) and B(n–r–1, r). Also a path reaching A can be continued to Q in only one-way, namely along AQ. Similarly a path reaching B uniquely proceeds along BQ. Hence the set S of paths from O to Q is the disjoint union of the sets S_1 from O to A and S_2 of paths from O to B.

Since $|S_1| = \binom{n-1}{r-1}$ and $|S_2| = \binom{n-1}{r}$

So by, addition principle,

$$|S| = |S_1| + |S_2|$$

$$\therefore \binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

Identity 4: $\binom{r}{r} + \binom{r+1}{r} + \ldots + \binom{n}{r} = \binom{n+1}{r+1}$

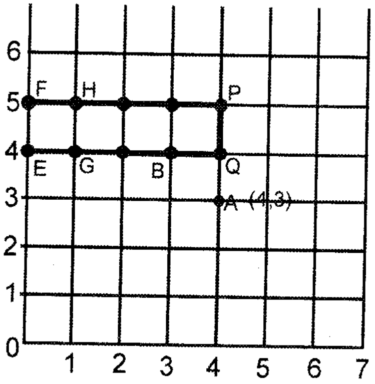


Figure 4.3

Refer *figure 4.3*, each path from O to P(n–r, r+1) must meet the y = r in some points.

Let T_i be the set of those paths whose last common point with the line y = r is (i, r) $0 \leq i \leq n - r$. *For example*, the set T_o contains paths having E as the last common point with the line y = r and these paths must proceed along EFP, T_1, contains paths having G as the last common point with the line y =r and they must proceed along GHP and so on.

Also all paths, i.e., |S| is the disjoint union of the sets T_i and $|T_i| = \binom{i+r}{i} = \binom{i+r}{r}$

Hence

$$|S| = \sum_{i=0}^{n} |T_i|$$

$$\therefore \binom{n+1}{r+1} = \binom{r}{r} + \binom{r+1}{r} + \ldots + \binom{n}{r}$$

Identity 5: $\binom{n}{0}+\binom{n+1}{1}+\binom{n+2}{2}+\ldots+\binom{n+r}{r}=\binom{n+r+1}{r}$

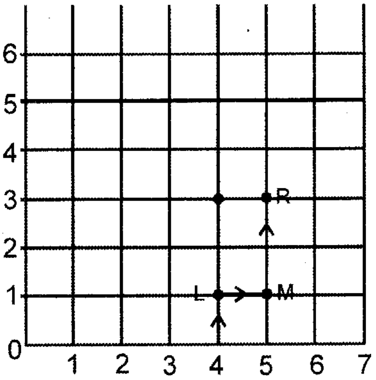


Figure 4. 4

Refer *figure 4.4*, note that each path from O to the point R(n+1, r) must meet the line x = n in some points. (In *figure 4.4* n = 4, r = 3) Let W_i be the set of paths from O to R having (n, i), $0 \le i \le r$, as the last common point with the line x = n. Then $|W_i| = \binom{n+i}{i}$ and the set of paths from O to R is the disjoint union of the sets W_i.

$$\therefore\ |S| = \binom{n+1+r}{r} = \sum_{i=0}^{r} |W_i| = \binom{n}{0}+\binom{n+1}{1}+\ldots+\binom{n+r}{r}$$

Identity 6: For integer n, k, r with $0 \le r \le k \le n$.

$$\binom{n}{k}-\binom{n}{k-1}+\binom{n}{k-2}-\binom{n}{k-3}+\ldots+(-1)^r\binom{n}{k-r} = \binom{n-1}{k}+(-1)^r.\binom{n-1}{k-r-1}$$

Proof

In the expansion of $(1+x)^n$, $\binom{n}{k-i}$ is coefficient of x^{k-i}, $\forall i = 0, 1, \ldots, r$

Also $\binom{n}{k-i}$ = coefficient of x^k in the expansion of $x^i\,(1+x)^n$.

$$\begin{aligned}\therefore \text{L.H.S.} &= \binom{n}{k}-\binom{n}{k-1}+\binom{n}{k-2}+\ldots+(-1)^r\binom{n}{k-r}\\ &= \text{coefficient of } x^k \text{ in } \Sigma\,(-x)^i\,(1+x)^n\\ &= \text{coefficient of } x^k \text{ in } \Sigma(-x)^i\,(1+x)^n\\ &= \text{coefficient of } x^k \text{ in } (1+x)^n\left[\frac{1-(-1)^{r+1}.\,x^{r+1}}{1+x}\right]\\ &= \text{coefficient of } x^k \text{ in } [(1+x)^{n-1}+(-1)^r\,x^{r+1}\,(1+x)^{n-1}]\end{aligned}$$

$$= \text{coefficient of } x^k \text{ in } (1+x)^{n-1} + (-1)^r.\ \text{Coefficient of } x^k \text{ in } x^{r+1}\,(1+x)^{n-1}$$

$$= \binom{n-1}{k} + (-1)^r \cdot \binom{n-1}{k-r-1}$$

Examples

1. Show that $\sum_{k=0}^{m} \binom{n}{k}\binom{n-k}{m-k} = 2^m \cdot \binom{n}{m}$, m < n

Solution

Note that

$$\binom{n}{k}\cdot\binom{n-k}{m-k} = \frac{n!}{(n-k)!k!} \times \frac{(n-k)!}{(n-m)!(m-k)!}$$

$$= \frac{n!}{m!(n-m)!}\ \frac{m!}{(m-k)!k!} \quad = \binom{n}{m}\cdot\binom{m}{k}$$

$$\therefore \text{L.H.S.} = \sum_{k=0}^{m}\binom{n}{k}\binom{n-k}{m-k} = \sum_{k=0}^{m}\binom{n}{m}\cdot\binom{m}{k}$$

$$= \binom{n}{m}\cdot\sum_{k=0}^{m}\binom{m}{k} = \binom{n}{m}\cdot 2^m \quad (\because \text{Sum of binomial coefficients of order m is } 2^m)$$

$$= 2^m \cdot \binom{n}{m} = \text{R.H.S.}$$

2. Let m, n be positive integers where $m \le n$, then sum of series $\sum_{k=0}^{m} (-1)^k \cdot \binom{n}{k}\binom{n}{m-k}$

Solution

$$\text{The expansion of } (1+x)^n = \sum_{k=0}^{n}\binom{n}{k} x^k$$

$$\text{and the expansion of } (1-x)^n = \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} \cdot x^k$$

$$\therefore \sum_{k=0}^{n} (-1)^k \binom{n}{k}\cdot\binom{n}{m-k} = \text{coefficient of } x^m \text{ in the expansion of } (1+x)^m \times \text{coefficient of } x^m \text{ in the expansion of } (1-x)^m.$$

$$= \text{coefficient of } x^m \text{ in } (1+x)^n\,(1-x)^n$$

$$= \text{coefficient of } x^m \text{ in } (1-x^2)^n$$

$$= \text{coefficient of } x^m \text{ in } \sum_{k=0}^{n} (-1)^k \cdot \binom{n}{k} x^{2K}$$

$$= (-1)^{m/2} \cdot \binom{n}{m/2}, \quad \text{if m is even}$$

$$= 0\ , \quad \text{if m is odd}$$

Solved Examples

1 PU Apr. 2009 – 7M

1. Father wants to divide 601 rupees to three children, so that no one child gets more than the other two children. How many ways can he do this distribution.

Solution

Let a,b,c denote the amount received by the three children. Then we require that a+b+c = 601. Now if for example, a = 0 , i.e., first child receives 0 amount then since 601 is an odd integer, the larger of b, c must be ≥ 301 and the corresponding child gets more amount than the other two. Therefore each of a,b,c must be ≥ 1. Further if a ≥ 301 say then b ≤ 300 and 3 ≤ 300, since a+b+c = 601 so that first child will get more amount than the other two. Hence each of a, b, c must be ≤ 300. Thus the number n say of required distributions is the number of integer solutions of the equation a+b+c = 601 with 1 ≤ a,b,c ≤ 301. So, n is the coefficient of x^{601} in the enumerator

$$\begin{aligned}
& (x + x^2 + \ldots + x^{300})^3 \\
= \;& x^3 (1 + x + \ldots + x^{299})^3 \\
= \;& x^3 (1 - x^{300})^3 (1 - x)^{-3} \\
= \;& x^3 (1 - 3x^{300} + 3x^{600} - x^{900}) (1 - x)^{-3} \\
= \;& x^3 (1 - 3x^{300} + 3x^{600} - x^{900}) \sum_{r=0}^{\infty} \binom{r+2}{2} x^r \\
= \;& (x^3 - 3x^{303} + 3x^{603} - x^{903}) (1 + 3x + 6x^2 + \ldots + {}^{300}C_2 x^{298} + {}^{600}C_2 x^{598} + \ldots)
\end{aligned}$$

Coefficient of x^{601} in above expansion is,

$$ {}^{600}C_2 - 3 \times {}^{300}C_2 = \frac{600 \times 599}{2} - 3 \times \frac{300 \times 299}{2} = 45150. $$

1 PU Oct. 2009 – 8M

2. Prove:

i. $\binom{n}{1} + \binom{n}{3} + \ldots = \binom{n}{0} + \binom{n}{2} + \ldots = 2^{n-1}$

ii. $\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$

Solution

i. The expansion of,

$$\begin{aligned}
(1 + x)^n &= \sum_{k=0}^{n} \binom{n}{k} x^k \\
&= \binom{n}{0} x^0 + \binom{n}{1} x + \binom{n}{2} x^2 + \ldots + \binom{n}{n} x^n
\end{aligned}$$

If we put x=1, we get

$$2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} \quad \ldots\ldots\ldots\ldots (1)$$

and if we put x= –1, we get

$$0 = \binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\ldots+(-1)^n\binom{n}{n}$$

$$\therefore \binom{n}{0}+\binom{n}{2}+\ldots = \binom{n}{1}+\binom{n}{3}+\ldots \quad \ldots\ldots(2$$

Hence from(1) and (2) we get,

$$\binom{n}{0}+\binom{n}{2}+\ldots = \binom{n}{1}+\binom{n}{3}+\ldots = 2^{n-1}$$

ii. Consider expansion,

$$(1+x)^n\,(x+1)^n = (1+x)^{2n}$$

$$\text{i.e., } \sum_{r=0}^{n}\binom{n}{r}x^r\cdot\sum_{r=0}^{n}\binom{n}{n-r}x^{n-r} = \sum_{r=0}^{2n}\binom{2n}{n}x^r$$

Comparing coefficient of x^n on both sides we get,

$$\binom{n}{0}\binom{n}{n}+\binom{n}{1}\cdot\binom{n}{n-1}+\binom{n}{2}\cdot\binom{n}{n-2}\ldots+\binom{n}{n}\cdot\binom{n}{0} = \binom{2n}{n}$$

$$\text{but } \binom{n}{r} = \binom{n}{n-r}$$

$$\therefore \binom{n}{0}\cdot\binom{n}{0}+\binom{n}{1}\cdot\binom{n}{1}+\binom{n}{2}\cdot\binom{n}{2}+\ldots\binom{n}{n}\cdot\binom{n}{n} = \binom{2n}{n}$$

$$\text{i.e., } \binom{n}{0}^2+\binom{n}{1}^2+\ldots\binom{n}{n}^2 = \binom{2n}{n}.$$

3. Prove $\boldsymbol{\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\ldots+\binom{n}{n}^2=\binom{2n}{n}}$

1
PU
Apr. 2010 – 4M

Solution

Consider the identity,

$$(1+x)^n\,(1+x)^n = (1+x)^{2n} \quad \ldots\ldots(1)$$

The coefficient of x^n on the left side of (1) namely

$$\left[\binom{n}{0}+\binom{n}{1}x+\binom{n}{2}x^2+\ldots\right]\left[\binom{n}{0}+\binom{n}{1}x+\ldots\right]$$

is,

$$\binom{n}{0}\cdot\binom{n}{n}+\binom{n}{1}\cdot\binom{n}{n-1}+\binom{n}{2}\cdot\binom{n}{n-2}+\ldots+\binom{n}{n}\cdot\binom{n}{0}$$

$$= \binom{n}{0}\cdot\binom{n}{0}+\binom{n}{1}\cdot\binom{n}{1}+\binom{n}{2}\cdot\binom{n}{2}+\ldots\binom{n}{n}\cdot\binom{n}{n} \qquad \because\ {}^nC_r = {}^nC_{n-r}$$

$$= \binom{n}{0}^2+\binom{n}{1}^2+\ldots\binom{n}{n}^2$$

While the coefficient of x^n on the right side of (1) is $\binom{2n}{n}$.

Hence the result follows by equating these coefficients.

$$\binom{m+n}{n} = \binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \ldots + \binom{m}{n}\binom{n}{n}$$

4. **Prove** $\binom{m+n}{n} = \binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \ldots + \binom{m}{n}\binom{n}{n}$

1 PU Oct. 2010 – 4M

Solution

Proof

Consider the identity,

$$(1+x)^m (1+x)^n = (1+x)^{m+n} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

The coefficient of x^n in the left side of (1) viz.

$$\left[\binom{m}{0} + \binom{m}{1}x + \binom{m}{2}x^2 + \ldots + \binom{m}{m}x^m\right] \times$$

$$\left[\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \ldots + \binom{n}{n}x^n\right]$$

$$\text{is } \binom{m}{0}\binom{n}{n} + \binom{m}{1}\binom{n}{n-1} + \binom{m}{2}\binom{n}{n-2} + \ldots + \binom{m}{n}\binom{n}{0}x^0$$

$$= \binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \binom{m}{2}\binom{n}{2} + \ldots + \binom{m}{n}\binom{n}{n}$$

$$\left(\because \binom{n}{r} = \binom{n}{n-r}\right)$$

While coefficient of x^n on the right side of (1) is, $\binom{m+n}{n}$. Hence we get,

$$\binom{m+n}{n} = \binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \ldots + \binom{m}{n}\binom{n}{n}.$$

5. **How many solutions are there to equation $x_1 + x_2 + x_3 = 17$ are non-negative integers with $x_1 < 4$, $x_2 < 3$ and $x_3 > 5$.**

1 PU Oct. 2009 – 7M

Solution

For integer $r = 17$, the number a_r of non-negative integer solutions of $x_1 + x_2 + x_3 = 17$ is obtained from the generating function

$$f(x) = (1 + x + x^2 + x^3)(1 + x + x^2)(x^6 + x^7 + \ldots)$$

since $x_1 < 4$, $x_2 < 3$ and $x_3 > 5$

$$\begin{aligned} \therefore\ f(x) &= x^6(1 + x + x^2 + \ldots)(1 - x^4)(1-x)^{-1}(1 - x^3)(1-x)^{-1} \\ &= x^6(1-x)^{-1}(1-x^4)(1-x)^{-1}(1-x^3)(1-x)^{-1} \\ &= x^6(1-x^4)(1-x^3)(1-x)^{-3} \end{aligned}$$

$$= x^6(1-x^4)(1-x^3)\sum_{r=0}^{\infty}\binom{r+2}{2}x^r$$

$$= x^6(1-x^4-x^3+x^7)\sum_{r=0}^{\infty}\binom{r+2}{2}x^r$$

Hence, the number of required solutions of $x_1 + x_2 + x_3 = 17$ is the coefficient of x^{17} in f(x) which is

$$= \underset{(\text{for } r = 11)}{\binom{13}{2}} - \underset{(\text{for } r = 7)}{\binom{9}{2}} - \underset{(\text{for } r = 8)}{\binom{10}{2}} + \underset{(\text{for } r = 4)}{\binom{6}{2}}$$

$$= \frac{13\times 12}{2} - \frac{9\times 8}{2} - \frac{10\times 9}{2} + \frac{6\times 5}{2} = 78 - 36 - 45 + 15 = 12$$

EXERCISE

1. How many ways are there to distribute 40 identical jelly beans among 4 children?

   i. Without restrictions? ii. With each child getting 10 beans
   iii. With each child getting at least 1 bean?

2. How many ways are there to distribute 18 chocolate doughnuts, 12 cinnamon doughnuts and 14 powdered doughnuts among 4 school principals if each principal demands atleast 2 doughnuts of each kind?

3. How many ways are there to distribute 15 identical objects into 4 boxes if the number of objects in box 4, must be multiple of 3?

4. In how many ways 10 (identical) dimes be distributed among 5 children if

   i. there are no restrictions? ii. each child gets at least one dime?
   iii. the oldest child gets atleast 2 dimes?

5. Determine the number of integer solutions of $x_1 + x_2 + x_3 + x_4 = 32$ where

   i. $x_i \geq 0,\ 1 \leq i \leq 4$ ii. $x_i > 0, 1 \leq i \leq 4$ iii. $x_1, x_2 \geq 5,\ x_3, x_4, \geq 7$
   iv. $x_i \geq 8, 1 \leq i \leq 4$ v. $x_i \geq -2,\ 1 \leq i \leq 4$

6. Twenty thousand rupees are to be invested in four different investments in units of Rs. 1000, how many different ways it can be invested a) entire amount is to be invested b) entire amount may not be invested.

7. Seven people enter the lift. The lift stops at all three-floors. At each of the floors no one enters the lift but atleast one person leaves the lift. After the three floor stops, the lift is empty. In how may ways can this happen?

8. Using combinatorial argument prove that

   i. $\binom{2n}{2} = 2.\binom{n}{2} + n^2$ ii. $\binom{n-1}{r-1} + \binom{n-1}{r} = \binom{n}{r}$

   iii. $\binom{r}{r} + \binom{r+1}{r} + \ldots + \binom{n}{r} = \binom{n+1}{r+1}$ iv. $\binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \ldots + \binom{n+r}{r} = \binom{n+r+1}{r}$

9. Show that

i. $\sum_{k=0}^{r} \binom{m}{k} \cdot \binom{n}{r-k} = \binom{m+n}{r}$ ii. $\binom{r}{0}^2 + \binom{r}{1}^2 + \ldots + \binom{r}{r}^2 = \binom{2r}{r}$

iii. $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$ iv. $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots = 2^{n-1}$

v. $\sum_{k=0}^{n} 2^K \binom{n}{k} = 3^n$

Hints and Answers

1. i. Let each child gets x_i jelly beans so that $x_1+x_2+x_3+x_4= 40$. Required number is non negative integer solutions to $x_1+x_2+x_3+x_4=40$ i.e. $\binom{43}{3} = 12341$

ii. Since the beans are identical, there is only one way to distribute 10 beans to each child.

iii. Required number is positive integer solution is $x_1+x_2+x_3+x_4 = 40$ which $\binom{39}{3} = 9139$.

2. Let x_1, x_2, x_3, x_4 denote the number of doughnuts of one kind given to the four principals respectively. We want number of integer solutions of the equation $x_1+x_2+x_3+x_4 = k$, where $x_i \geq 2 \ \forall$ i. Put $x_i = y_i +2$, then we want get number of non-negative solutions to the equations $y_1+y_2+y_3+y_4 = k-8$ for chocolate doughnuts $k = 18$. ∴ number of ways of distributions chocolate doughnuts is $\binom{4-1+10}{10}$.

Similarly the ways of distributing other doughnuts can be obtained and total ways

$$= \binom{4-1+10}{10} . \binom{4-1+4}{4} . \binom{4-1+6}{6} = 840840$$

3. Let $x_1, x_2, x_3, 3k$ denote the number of objects put into 4 boxes respectively $k = 0, 1,2,3,4,5$.

∴ Number of non-negative solutions to

$x_1+x_2+x_3+3k = 15$ i.e. $x_1+x_2+x_3 = 15-3k$ is $\sum_{k=0}^{5} \binom{3-1+15-3k}{15-3k}$

4. i. $\binom{14}{10} = 100!$ ii. $\binom{9}{4} = 126$ iii. $\binom{12}{8} = 495$

5. i. $\binom{35}{32} = 6545$ ii. $\binom{31}{3} = 4495$ iii. $\binom{11}{8} = 165$

iv. 1 v. $\binom{43}{40} = 12341$

6. i. Let x_1, x_2, x_3, x_4 be number of units of Rs. 1000/- in 4 different investments then required ways = number of non-negative integer solution to $x_1+x_2+x_3+x_4 = 20$ which is $\binom{23}{20} = 1771$.

ii. Let along with 4 investments (x_1, x_2, x_3, x_4), x_5 the amount not to be invested, where $x_5 > 0$ then required number of ways is non-negative integer solution to $x_1+x_2+x_3+x_4+x_5 = 19$ which is $\binom{23}{19} = 8855$

7. Let x_1, x_2, x_3 people living at three floors respectively, $x_i > 0$, $1 \leq i \leq 3$ and required answer is positive integer solution to $x_1+ x_2+x_3 = 7$ which $\binom{6}{2} = 15$.

Collection of Questions asked in Previous Exams PU

1. In how many Rs. 20,000 could be invested in denomination of Rs. 1,000 among 4 different investment opportunities if **[Apr. 2009 – 5 M]**
   i. All money need not be invested?
   ii. All investment opportunities must be used?

2. Show the following by using combinatoric arguments: **[Apr. 2009 – 5 M]**
   i. $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ ii. $\binom{2n}{2} = 2\binom{n}{2} + n^2$.

3. Father wants to divide 60 1 rupees to three children, so that no one child gets more than the other two children. How many ways can he do this distribution? **[Apr. 2009 – 5 M]**

4. Prove: **[Oct.2009 – 8 M]**
   i. $\binom{n}{1} + \binom{n}{3} + \ldots = \binom{n}{0} + \binom{n}{2} + \ldots = 2^{n-1}$ ii. $\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$

5. If 8 identical black boards are to be divided among 4 schools, how many divisions are possible?
   i. with no restriction
   ii. each school must get at least 1 blackboard. **[Oct.2009 – 4 M]**

6. How many solutions are there to equation $x_1 + x_2 + x_3 = 17$ are non-negative integers with $x_1 < 4$, $x_2 < 3$ and $x_3 > 5$. **[Oct.2009 – 7 M]**

7. How many solutions are there to equation $x_1 + x_2 + x_3 = 17$ where x_1, x_2 and x_3 are non-negative with $x_1 < 6$ and $x_3 > 5$? **[Apr. 2010 – 8 M]**

8. Prove: **[Apr. 2010 – 7M]**
   i. $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$ ii. $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$

9. An elevator starts the basement with 8 people (excluding the elevator operator) and discharges them all by the time it reaches the top floor, number 6.
   i. In how many ways could the operator have perceived the people leaving the elevator if all people look alike to him?
   ii. What if the 8 people consist of 5 men and 3 women and operator could tell a man from a woman? **[Oct 2010 – 5M]**

10. Prove: **[Oct. 2010 – 8 M]**
    i. $\binom{2^n}{2} = 2\binom{n}{2} + n^2$ ii. $\binom{m+n}{n} = \binom{m}{0}\binom{n}{0} + \binom{m}{1}\binom{n}{1} + \ldots + \binom{m}{n}\binom{n}{n}$

5 Principles of Inclusion and Exclusion

1. Introduction

In this chapter we will discuss the topic like principle of inclusion and exclusion, which is generalization of the addition principle, formula derangement and generating functions.

2. Principle of Inclusion and Exclusion

▶Theorem 1

Let A and B be subsets of a finite universal set U, then principle of Inclusion and Exclusion (PIE) states that $|A \cup B| = |A| + |B| - |A \cap B|$

Proof

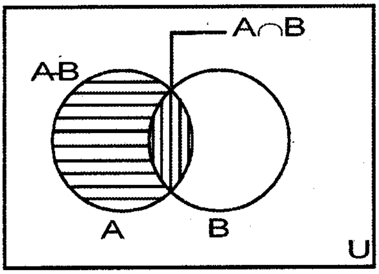


Figure 5.1

We prove the result by using venn-diagram. In the *figure 5.1* the area marked with horizontal lines is the set A–B and the area marked with vertical lines is the set $A \cap B$. Thus A is union of the disjoint sets A–B and $A \cap B$. Hence by addition principle, we have,

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

$$\therefore\ |A-B| = |A| - |A \cap B| \quad \text{...} \mathbf{(1)}$$

Also, $A \cup B$ is the union of the disjoint sets B and (A–B); hence by addition principle,

$$\begin{aligned} |A \cup B| &= |B| + |A-B| \\ &= |B| + |A| - |A \cap B| \qquad \text{(from (1))} \end{aligned}$$

and hence

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

Extension of Principle of Inclusion and Exclusion

Let $S_1, S_2, \ldots, S_n$ be finite sets and let

$$S = S_1 \cup S_2 \cup \ldots \cup S_n$$

Then $$|S| = \sum_{i=1}^{n} |S_i| - \sum_{1 \le i < j \le n} |S_i \cap S_j| + \sum_{1 \le i < j < k \le n} |S_i \cap S_j \cap S_k| + \ldots + (-1)^n |S_1 \cap S_2 \cap \ldots \cap S_n|$$

Examples

1. Among the integer 1 to 1000

i. How many of them are not divisible by 3, nor by 5, nor by 7?

ii. How many are not divisible by 5 and 7 but divisible by 3?

Solution

Let A, B, C denote respectively the set of integers from 1 to 1000 divisible by 3, 5, and by 7.

i. Then $A' \cap B' \cap C'$ denote the set of integers not divisible by 3, nor by 5, nor by 7.

By De Morgan's law $A' \cap B' \cap C' = (A \cup B \cup C)'$

$$\begin{aligned} \therefore\ |A' \cap B' \cap C'| &= n(U) - |A \cup B \cup C| \\ &= 1000 - |A \cup B \cup C| \\ &= 1000 - \big[|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|\big] \end{aligned}$$

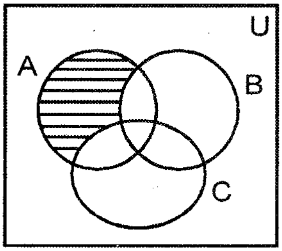
Now $|A| = \left[\frac{1000}{3}\right] = 333,\quad |B| = \left[\frac{1000}{5}\right] = 200,\quad |C| = \left[\frac{1000}{7}\right] = 142,$

$|A \cap B| = \left[\frac{1000}{15}\right] = 66,\quad |B \cap C| = \left[\frac{1000}{35}\right] = 28,\quad |A \cap C| = \left[\frac{1000}{21}\right] = 47$

$|A \cap B \cap C| = \left[\frac{1000}{105}\right] = 9$

Hence $|A' \cap B' \cap C'| = 1000 - [333 + 200 + 142 - 66 - 28 - 47 + 9] = 457$

ii. $A \cap B' \cap C'$ denotes the set of integers not divisible by 5 and 7 but divisible by 3.



The shaded region is $A \cap B' \cap C'$.

From venn diagram it is clear that

$|A \cap B' \cap C'| = |A| - |A \cap B| - |A \cap C| + |A \cap B \cap C| = 333 - 66 - 47 + 9 = 229$

2. How many integers between 999 and 9999 either begin or end with 3?

Solution

Let S be the set of 4-digit numbers and

$A = \{x \in S \,/\, x \text{ begins with } 3\}$

$B = \{x \in S/ \, x \text{ ends with } 3\}$

Now, we want to find $|A \cup B|$. If a 4 –digit number begins with 3 then each of its remaining three digits can be chosen in 10 ways, so by multiplication theorem, $|A| = 10^3$; and it a 4-digit number ends with 3, then its leading digit, being non-zero can be chosen in 9 ways and each of its remaining two digits can be chosen in 10 ways, so by multiplication principle, $|B| = 9 \times 10^2 = 900$ and if a 4 –digit begins and ends with 3 then each of its remaining two digits can be in 10 ways and so $|A \cap B| = 10^2$.

Hence $|A \cup B| = |A| + |B| - |A \cap B| = 1000 + 900 - 100 = 1800$

3. Derangements

Derangements means nothing is in its right place. Consider n distinct object a_i, $1 \leq i \leq n$ arranged in a row in the order: $a_1, a_2, \ldots a_n$. Then a derangement of these objects is a permutation in which no object is in its original position i.e. a_1 is not in the first place, a_2, is not in the second place, . . ., a_n is not in the nth place. Thus, if a, b, c, d are arranged in the order x = abcd, then compared to x, y = dcab is a derangement but z = dacb is not because in z the object c is in its original place.

Now for considering derangements, the nature of the objects is not important. So denote the n objects by integers, 1, 2, . . ., n written in natural order. Let D_n denote the number of derangements of these n integers. Then $D_1 = 0$, since the only permutation of 1 is 1 and so no derangements are possible. $D_2 = 1$, since the only derangement of 1, 2 is 2, 1. $D_3 = 2$, since the only derangements of 1,2,3 are 3,1,2 and 2, 3, 1.

$D_4 = 9$, since there are exactly of derangements of 1,2,3,4 namely

2,1,4,3 2,3,4,1 2,4,1,3
3,1,4,2 3,4,1,2 3,4,2,1
4,3,2,1 4,3,1,2 4,1,2,3

▶Theorem 2

The number D_n of derangements of n distinct objects is given by

$$D_n = n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}\right]$$

Proof

Let the given objects be denoted by the integers 1, 2, . . ., n and suppose that these are arranged in their natural order. Let U be the set of all permutations of these integers. Let A_i denote the set of those permutations in each of which the integer i is in the ith place. Then it is clear that

$$D_n = |A'_1 \cap A'_2 \cap \ldots \cap A'_n|$$

Now for each $i = 1, 2, \ldots n$, $|A_i| = (n-1)!$,

because after putting i in ith place, the remaining (n–1) integers can be arranged in the remaining places in (n–1)! ways. So $S_1 = \Sigma\, |A_i| = {}^nC_1 \times (n-1)! = n(n-1)!$

Next, for $1 \le i < j \le n$, we have $|A_i \cap A_j| = (n-2)!$ because after putting the integers i, j in their respective original places, the remaining (n–2) integers can be arranged in (n–2) places in (n–2)! ways. Since there are ${}^nC_2$ pairs A_i, A_j we have $S_2 = \Sigma|A_i \cap A_j| = {}^nC_2\,(n-2)!$. Similarly, for any set

$$T = \{i_1, i_2, \ldots, i_r\} \text{ of r integers such that } 1 \le i_1 < i_2 < \ldots < i_r \le n \text{ we get}$$

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_n}| = (n-r)! \text{ and there are } {}^nC_r \text{ different r- sets T.}$$

Hence

$$|S_r| = \Sigma\, |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_n}| = \binom{n}{r} . (n-r)!$$

$$S_n = 1$$

∴ By generalized principle of inclusion and exclusion,

$$\begin{aligned} D_n &= |U| - S_1 + S_2 - S_3 + \ldots + (-1)^n S_n. \\ &= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \ldots + (-1)^n. \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \ldots + (-1)^n \\ &= n!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}\right] \end{aligned}$$

and hence the proof.

Note

$$D_4 = 4!\left[1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}\right] = 4!\left[1-1+\frac{1}{2}-\frac{1}{6}+\frac{1}{24}\right] = 24\left[\frac{12-4+1}{24}\right] = 9$$

Example

1. **Eight envelopes are opened and the letters are removed. How many ways can the letters be replaced so that**

   i. **no letter is put in its original envelope**

   ii. **exactly one letter is put in its original envelope.**

   iii. **atleast one letter is put in its original envelope.**

   iv. **atleast two letters are put in their original envelopes?**

Solution

Here number of objects are 8.

i. **No letter is put in its original envelope**: This means it is a derangement of 8 objects, the number of ways for which is

$$\begin{aligned}D_8 &= 8!\left[1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\frac{1}{5!}+\frac{1}{6!}-\frac{1}{7!}+\frac{1}{8!}\right]\\ &= 8!\left[\frac{20160-6720+1680-336+56-8+1}{8!}\right]\\ &= 14833\end{aligned}$$

ii. **Exactly one letter is put in its original envelope:** In this case, out of 8 any one letter will in its original envelope which can be done in ${}^8C_1 = 8$ ways and remaining 7 letters are derangements, the number of ways for which is

$$D_7 = 7!\left[1-\frac{1}{1!}+\frac{1}{2!}-\frac{1}{3!}+\frac{1}{4!}-\frac{1}{5!}+\frac{1}{6!}-\frac{1}{7!}\right]$$

$$\begin{aligned}\therefore \text{ Total number of ways} &= 8 \times D_7\\ &= 8 \times [2520-840+210-42+7-1]\\ &= 14832\end{aligned}$$

iii. **At least one letter is put in its original envelope:** In this case either 1 letter is placed properly or 2 letters or 3 letters . . . or all 8 letters are placed properly. The number of ways

$$\begin{aligned}&= D_7+D_6+D_5+D_4+D_3+D_2+D_1+D_0\\ &= |\cup|-D_8 = 8!-14833 = 25487\end{aligned}$$

iv. **Atleast two letters are put in their original envelopes**

Here either 2, 3, 4, 5, 6, 7, or 8 letters are placed properly which means $D_6+D_5+D_4+D_3+D_2+D_1+D_0$ which is equivalent to $|\cup|-D_8-D_7$

$$= 8!-14833-14832 = 10655$$

4. Find the probability that in a group of 100 letters.

i. No letter is put into the correct envelope.

ii. Exactly 98 letters are put into correct envelope.

1

PU
Oct. 2010 – 5M

Solution

Total number of ways of arranging 100 letters in 100 envelops is, $n = {}^{100}P_{100} = 100!$

i. Let A: No letter is put into the correct envelope. This means it is a de-arrangement of 100 objects, the number of ways for which is,

$$\begin{aligned} m &= D_{100} \\ &= 100!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \cdots + \frac{1}{100!}\right) \end{aligned}$$

$$\begin{aligned} \therefore\ P(A) &= \frac{m}{n} \\ &= \frac{D_{100}}{100!} \\ &= 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \cdots + \frac{1}{100!} \end{aligned}$$

ii. Let B: Exactly 98 letters are not put into correct envelope. In this case out of 100, any 2 letters will be in their original envelops, which can be done in ${}^{100}C_2 = \dfrac{100 \times 99}{2} = 4950.$

Remaining 98 letters are de-arrangements, the number of ways for which is,

$$D_{98} = 98!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ \ldots + \frac{1}{98!}\right]$$

$\therefore$ Favourable ways for B are $m = 4950 \times D_{98}$

$$\begin{aligned} \therefore\ P(B) &= \frac{m}{n} = \frac{4950 \times 98!\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ \ldots + \frac{1}{98!}\right]}{100!} \\ &= \frac{4950\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ \ldots + \frac{1}{98!}\right]}{100 \times 99} \\ &= \frac{\left[1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ \ldots + \frac{1}{98!}\right]}{2} \end{aligned}$$

Solved Examples

1. **A man has 6 friends. At dinner in a certain restaurant, he has met each of them 12 times, every two of them 6 times, every three of them 4 times, every four of them 3 times, every five of them twice and all of them only once. He has dined out without meeting any of them 8 times. How many times has he dined out altogether?**

1 PU Apr. 2010 – 5M

Solution

Let A denote the man has dined out; A_i denote the ith friend of the man has dined i = 1, 2, . . . 6.

Now,

$$\begin{aligned}|A| &= |A \cap A_1' \cap A_2' \cap A_3' \cap A_4' \cap A_5' \cap A_6'| + \sum_{i=1}^{6} |A \cap A_i| + \sum_{i \neq j}\sum |A \cap A_i \cap A_j| + \\ &\quad \sum_{i<j<k}\sum\sum |A \cap A_i \cap A_j \cap A_k| + \sum_{i<j<k<l}\sum\sum\sum |A \cap A_i \cap A_j \cap A_k \cap A_l| + \\ &\quad \sum_{i<j<k<l<m}\sum\sum\sum\sum |A \cap A_i \cap A_j \cap A_k \cap A_l \cap A_m| + \left(\bigcap_{i=1}^{6} A_i \cap A\right) \\ &= 8 + 12 + 6 + 4 + 3 + 2 + 1 \quad = \quad 36.\end{aligned}$$

EXERCISE

1. How many integers between 1 and 567 are divisible by either 3 or 5?
2. The students in a hostel were asked whether they had a TV set or a computer in their rooms. The result showed that 650 students had a TV set; 150 did not have a TV set; 175 had a computer and 50 had neither a TV set nor a computer. Find the number of students who i) live in the hostel ii) have both a TV set and a computer iii) have only a computer.
3. A survey of 500 television watchers produced the following information;285 watch Cricket, 195 watch Hockey, 115 watch Tennis, 45 watch Cricket and Tennis, 70 watch Cricket and Hockey, 50 watch Hockey and Tennis and 50 do not watch any of the 3 games.
   i. How many people in the survey watch all the 3 games?
   ii. How many people watch exactly 1 of the 3 games?
4. 5 gentlemen attend a party, they leave their overcoats in a clock room. After the party they pick at random the overcoats and leave. Find the number of ways they do not carry their own overcoats.
5. 4 letters and 4 corresponding addressed envelops are to be prepared. Place the letters in the envelops in such a way that no letter goes in correctly addressed envelope. How many ways it can be done?
6. One publisher wants two reviews per book for 7 books published. So he hires 7 people to review them. He gives each person one book to read in the first week and then redistributes the books at the start of the second week. In how many ways can be make these two distributions so that he gets two reviews (by different people) of each book?

Hints and Answers

1. 265

2. i. 800 ii. 75 iii. 100

3. i. 20 ii. 325

4. $D_5 = 44$

5. $D_4 = 9$

6. Publisher can distribute the books in 7! ways in the first week. Numbering both the books and the reviewers (for the first week) as 1, 2, . . . , 7. For the second week he must arrange these numbers so that none of them is in its natural position, which he can do in D_7, ways. Hence total number of ways = $7! \times D_7$.

Collection of Questions asked in Previous Exams PU

1. State and prove Derangement theorem. **[Apr. 2009 – 5M]**

3. A man has 6 friends. At dinner in a certain restaurant, he has met each of them 12 times, every two of them 6 times, every three of them 4 times, every four of them 3 times, every five of them twice and all of them only once. He has dined out without meeting any of them 8 times. How many times has he dined out altogether? **[Apr. 2009 – 5M]**

4. State and prove principles of Exclusion and Inclusion. **[Oct. 2009 – 5M]**

5. If 8 identical black boards are to be divided among 4 schools, how many divisions are possible?
   - i. with no restriction
   - ii. each school must get at least 1 blackboard. **[Oct. 2009 – 5M]**

8. State and prove derangement theorem. **[Apr. 2010 – 5M]**

10. State and prove principles of Exclusion and Inclusion. **Oct. 2010 – 5M]**

11. Find the probability that in a group of 100 letters. **[Oct. 2010 – 5M]**
   - i. No letter is put into the correct envelope
   - ii. Exactly 98 letters are put into correct envelope.

6 Algebraic Structures

1. Introduction

We study sets with additional structures, induced by one or more binary operations on the elements of the set. These discrete structures are called as algebraic systems as they obey a set of rules or axioms which are similar to the rules of addition and multiplication of numbers in elementary algebra.

An important application of groups is in coding theory where techniques are developed for detecting and correcting errors in transmitted data. Besides coding theory, algebraic systems are also widely applied in the design of computer hardware and development of software especially formal language theory and finite state machines.

2. Algebraic System

Let us first define an operation on the elements of a set, such that the resulting element is also an element of the set.

Definition

Let X be a set and f be a mapping f: $X \times X$. Then f is called a binary operation on X. In general, a mapping f: $X^n \rightarrow X$ is called an n-ary operation and n is called the order of the operation.

If $n = 1$, f is called unary.

If $n = 2$, f is called binary.

If $n = 3$, f is called ternary and so on.

Examples

i. The function $f : Z \to Z$, where $f(x) = -x$, is unary.

ii. $f : Z \times Z \to Z$, defined as $f(x, y) = x + y$, is binary.

iii. $f : Z \times Z \times Z \to Z$, defined as

$$f(x, y, z) = \begin{cases} y & \text{if } x \neq 0 \\ z & \text{otherwise} \end{cases}$$

is ternary

Definition

An algebraic system is an ordered pair (A, F) where:

i. A is a set of elements, called as the carrier of the algebra.

ii. F is a finite set of a m-ary operations on the carrier, m being a variable.

In the notation for an algebraic system, the carrier set A is first specified, followed by the elements of F, which are actually listed, viz. (A, f_1) or (A, f_1, f_2) etc.

Examples

i. Let $E = \{0, 2, 4, \ldots\}$ then E with the binary operation of addition + represents an algebraic system (E, +).

ii. The set of integers Z with the two binary operations of addition + and multiplication × is an algebraic system and denoted as $(Z, +, \times)$.

iii. The set of real numbers R, with a single unary operation minus – and two binary operations of addition and multiplication is an algebraic system denoted by $(R, -, + \times)$.

2.1 Properties of Binary Operations

i. A binary operation $*$ on A is said to be **commutative** if $a * b = b * a$, for all elements $a, b \in A$.

Examples: The binary operation of addition and multiplication on the set of integers is commutative, but the operation of subtraction on the set of integers is not commutative.

ii. A binary operation $*$ on A is said to be **associative** if

$a * (b * c) = (a * b) * c$, for all elements $a, b, c \in A$

Example: The binary operation of addition and multiplication on the set of integers is associative, whereas the binary operation of subtraction is not associative.

iii. A binary operation $*$ on A is said to satisfy the **idempotent property** if $a * a = a$, for all $a \in A$.

Example: Let L be a lattice with the operators $\wedge$ (meet) and $\vee$ (join). Then $\wedge$ and $\vee$ are binary operations and we know that

$$a \vee a = a$$
$$a \wedge a = a, \quad \text{for all } a \in A$$

Hence both $\wedge$ and $\vee$ satisfy the idempotent property.

For each of the following, determine whether the binary operation $*$ is commutative or associative.

1. **N is the set of natural numbers and $a * b = a + b + 2$, for $a, b \in N$.**

Solution

$*$ is commutative since

$$\begin{aligned} a * b &= a + b + 2 \\ b * a &= b + a + 2 \end{aligned}$$

Hence both are equal

$$\begin{aligned} a * (b * c) &= a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4 \\ (a * b) * c &= (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4 \end{aligned}$$

Hence $*$ is associative.

2. **On N, where $a * b = \min(a, b + 2)$**

Solution

$*$ is not commutative.

$$\begin{aligned} 2 * 3 &= \min(2, 3 + 2) = \min(2, 5) = 2 \\ \text{whereas } 3 * 2 &= \min(3, 2 + 2) = \min(3, 4) = 3 \end{aligned}$$

$*$ is also not associative since

$$\begin{aligned} 4 * (3 * 1) &= 4 * 3 = 4 \text{ while} \\ (4 * 3) * 1 &= 4 * 1 = 3 \end{aligned}$$

3. **Show that $x * y = x^y$ is a binary operation on set of positive integers. Determine whether**

i. $*$ is commutative ii. $*$ is associative

1 PU Oct. 2008 – 7 M

Solution

$\therefore x * y = x^y$ is a binary operation on set of positive integers (Z^+).

Let $x, y \in Z^+$

$\therefore x^y$ is a positive integer.

$\therefore x * y = x^y$ is a positive integer.

$\therefore x * y \in Z^+$. $\forall x, y \in Z^+$

i.e., $*$ is a function from $Z^* \times Z^+$ to Z^+

$\therefore$ $*$ is a binary operation on set Z^+.

i. To check $*$ is commutative

i.e., $x * y = y * x \ \forall x, y \in Z^+$.

Now $x * y = x^y$

Also $y * x = y^x$

$x^y \neq y^x$

$\therefore x * y \neq y * x$

$\therefore$ $*$ is not commutative.

ii. To check $*$ is associative

i.e., $x * (y * z) = (x * y) * z \quad \forall x, y, z \in Z^+$

c.n.s. $x * (y * z) = x * (y^z)$

$= x^{y^z}$

r.n.s. $(x * y) * Z = x^y * z$

$= (x^y)^z$

$= x^{yz}$

$\therefore x * (y * z) \neq (x * y) * z$

Hence $*$ is not Associative.

2.2 Semi-groups

Let $(A, *)$ be an algebraic system, with a binary operation $*$ on A. Then $(A, *)$ is called semi-group if $*$ is **associative**, i.e.,

$$a * (b * c) = (a * b) * c, \text{ for all } a, b, c \in A$$

The semi-group is further said to be **commutative** if $*$ is commutative.

Examples

i. $(Z, +)$ is a commutative semi-group.

ii. $(Z, \times)$ is a commutative semi-group.

iii. $(Z, -)$ is not a semi-group, since.

Subtraction is not associative.

Definition

i. An element e in $(A, *)$ is called as left identity element if for each element $x \in A$, $e * x = x$.

ii. e is called a right identity if $x * e = x$, for all $x \in A$.

An element e in a semi-group (A, $*$) is called an identity element if $a * e = e * a = a$, for all $a \in A$, i.e., e is both a left identity and right identity. It is clear that e is unique.

Examples

i. The semi-group (Z, +) has the identity element which is the number zero.

ii. The semi-group (Z, ×) has the identity element which is the number one.

iii. The semi-group (N, +) has no identity element, where the set N is the set of natural numbers, excluding zero.

Monoid

A monoid is a semi-group (A, $*$) that has an identity element.

Examples

i. Let $E = \{0, 2, 4, 6, \ldots\}$ then (E, +) is a monoid, with the number zero as the identity element.

ii. Let E* be the set of all words over the alphabet set E = {a, b}. Let concatenation be the binary operation. The empty word $\wedge$ is the identity for E*. Hence E* under concatenation is a monoid.

Example

1. **Define monoid. Show that the set of N natural numbers is a semigroup under the operation $x * y = \max\{x, y\}$ is it monoid?**

1

PU
Oct. 2010– *6 M*

Solution

An algebraic system (A, $*$) is said to be monoid if

i. $*$ is associate in A

i.e., $a * (b * c) = (a * b) * c$, for all a, b, c $\in$ A.

ii. There exists an identity element 'e' in A so that

$a * e = e * a = a, \ \forall a \in A.$

Let x, y, z $\in$ N

$$x * (y * z) = x * \max\{y, z\}$$

$$= \max\{x, \max\{y, z\}\} \quad \ldots\ldots\ldots (1)$$

and $$(x * y) * z = (\max\{x, y\}) * z$$

$$= \max\{\max\{x, y\}, z\} \quad \ldots\ldots\ldots (2)$$

From (1) and (2) it is clear that we have to get maximum number of x, y, z

$$x * (y * z) = (x * y) * z$$

$\therefore$ $*$ Associative on N and hence N is a semi-group.

Let e be an element such that

$$x * e = e * x = x$$

Since $x * e = \max\{x, e\} = x$

If and only if e = 1, for all $x \in N$. Hence N is monoid under '$*$'.

2.3 Sub semi-group

Let (A, $*$) be a semi-group and let B be a non-empty subset of A, such that B is closed under $*$. Then (B, $*$) is itself a semi-group and is called a sub semi-group of (A, x).

Submonoid

Let (A, $*$) be a monoid and let B be a non-empty subset of A. Then (B, $*$) is called a submonoid of (A, $*$) if:

i. B is closed under $*$.

ii. The identity element $e \in B$.

Example

Let E = {0, 2, 4, 6, ...} Then (E, +) is a submonoid of (Z, +).

The concepts of semi-groups and monoids are used in finite state machines.

Definition

Let (A, $*$) be a monoid with identity element e. Let B be a non-empty subset of A. Then the monoid generated by B, denoted by <B> is defined as follows:

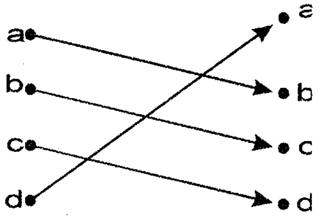
i. $e \in$ <B> and if $b \in B$, then b also is in <B> that is $B \subseteq$ <B>.

ii. <B> is closed under $*$.

iii. The only elements of <B> are those obtained from steps (i) and (ii).

Examples

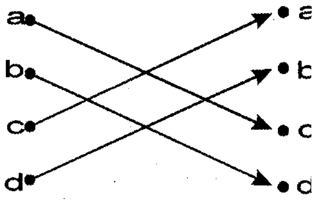
1. **Let A = {a, b, c, d} and let C(A) denote the set of all functions on A. Let f: A → A be defined by the following diagram.**



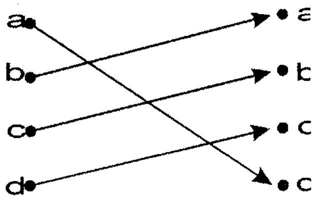
Find the submonoid of (C(A), o), where o denotes composition of functions, generated by f.

Solution

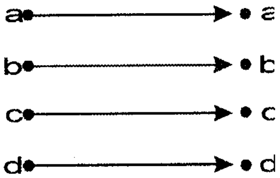
The identity element is 1_A consider $f \circ f = f^2$ which is defined by the following diagram:



$f \circ f \circ f = f^3$ is defined as



f^4 is defined as



$\therefore f^4 = 1_A$

Hence, the submonoid generated by f is the set $\{1_A, f, f^2, f^3\}$

2. Let A = {a, b} which of the following tables define a semi-group of A? monoid on A?

i.

*	a	b
a	a	b
b	a	a

ii.

*	a	b
a	a	b
b	b	b

Solution

i. $\ast$ is not associative.

Consider

$b \ast (a \ast b) = b \ast b = a$

$(b \ast a) \ast b = a \ast b = b$

$\therefore$ (A, $\ast$) is not a semi-group and hence, not a monoid.

ii. $a \ast (b \ast b) = a \ast b = b$

$(a \ast b) \ast b = b \ast b = b$

$a \ast (a \ast b) = a \ast b = b$

$(a \ast a) \ast b = a \ast b = b$

$a \ast (b \ast a) = a \ast b = b$

$(a \ast b) \ast a = b \ast a = b$

Similarly $\ast$ is associative for the remaining combinations.

The identity element is a. Hence, (A, $\ast$) is not only a semi-group, but it is also a monoid.

3. Let Z_n denote the set of integers {0, 1, 2, ..., n – 1}. Let $\odot$ be binary operation on Z_n such that $a \odot b$ = the remainder of ab divided by n:

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

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

Solution

i. $Z_4 = \{0, 1, 2, 3\}$

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

ii. Let $a \odot b = r$, where $ab = pn + r$ .... **(1)**

Then $(a \odot b) \odot c = r \odot c$

$= s$, where $rc = qn + s$ .... **(2)**

$b \odot c = t$, where $bc = ln + t$ .... **(3)**

$a \odot (b \odot c) = a \odot t = k$, where $at = mn + k$ .... **(4)**

we have to prove s = k

$a(bc) = aln + at$

$= aln + mn + k$ .... **(5)**

$(ab)\, c = (pn + r)\, c = pnc + rc$

$= pnc + qn + s$ .... **(6)**

Since equations (5) and (6) are equal, it follows that s = k.

$(a \odot b) \odot c = a \odot (b \odot c)$

Hence, $(Z_n, \odot)$ is a semi-group for any n.

Groups

A group (G, ∗) is a monoid, with identity e, such that for every element $a \in G$ there exists an element $a^{-1} \in G$, called the inverse of a, such that $a * a^{-1} = a^{-1} * a = e$.

Thus, a group is a set G together with binary operation ∗ on G such that

i. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$ (i.e., ∗ is associative).

ii. There is a unique element e in G such that
$a * e = e * a$, for $a \in G$ (Identity element).

iii. For each $a \in G$, there exists an element $a^{-1} \in G$, such that $a * a^{-1} = a^{-1} * a = e$ (Inverse element).

Definition

A group (G, $*$) is called an **Abelian group** if $a * b = b * a$, for all $a, b \in G$.

Examples

i. The set of all integers Z with the operation of addition is a group. The identity element is the number 0 and for every $n \in Z$, its inverse is $-n$.

ii. The set of all non zero real numbers under the operation of multiplication is a group, with the number 1 as the identity element and inverse of each number a is $\frac{1}{a}$.

iii. Let n be any positive integer ($n > 0$). For elements $x, y \in Z$, define a relation $\equiv$ on them as $x \equiv y$ or $x = y \pmod n$ if $x - y$ is divisible by n. The relation is an equivalence relation and for each element $x \in Z$, we obtained the corresponding equivalence class [x].

There are in all n distinct equivalence classes. Let Z_n denote the set of all equivalence classes, Z_n is called as set of residue classes modulo n, where $[x] = [y]$ implies $x = y \pmod n$.

For any two elements $[x], [y] \in Z_n$ define $[x] + [y] = [x + y]$ one can easily see that + is both associative and commutative. The identity element is [0] and for each $[x] \in Z_m$, its inverse is $[m - x]$, since $[x] + [m - x] = [x + m - x] = [m] = [0]$.

Thus $(Z_m, +)$ is an abelian group.

Example

1. Consider the set Q of rational numbers and let * be the operation on Q defined by a * b = a + b – ab. Is (Q, *) a group?

1

PU
Oct. 2010 – 7 *M*

Solution

i. For $\forall$ a, b $\in$ Q.

$a * b = a + b - ab \in Q$

$\therefore$ $*$ is defined on Q.

ii. Let a, b, c $\in$ Q.

Consider

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

$$\text{and} \quad (a * b) * c = (a + b - ab) * c$$
$$= (a + b - ab) + c - (a + b - ab)\, c$$
$$= a + b - ab + c - ac - bc + abc$$
$$= a + b + c - bc - ab - ac + abc \quad \text{..........} (2)$$

From (1) and (2) we have

$$a * (b * c) = (a * b) * c \ \forall a, b, c \in Q.$$

$\therefore$ * is associative.

iii. Let e be an element such that $a * e = a$

$$\begin{aligned} \text{i.e., } \quad a + e - ae &= a \\ \text{i.e., } \quad e(1 - a) &= 0 \\ \text{i.e., } \quad e &= 0 \in Q \end{aligned}$$

$\therefore$ Identity element belong to Q.

iv. Let b be an element such that

$$\begin{aligned} a * b &= b * a = e \\ \text{i.e., } \quad a * b &= 0 \\ \text{i.e., } \quad a + b - ab &= 0 \\ \text{i.e., } \quad a + b(1 - a) &= 0 \\ \text{i.e., } \quad b(1 - a) &= -a \\ \text{i.e., } \quad b &= \frac{-a}{1-a} \in Q \text{ if and only if } a \neq 1 \end{aligned}$$

i.e. for a = 1, inverse of a does not exist. Hence (Q, *) is not a group.

2.4 Order of an Element of a Group

Let e be the identity in a group G. An element $a \in G$ is said to be of order (or period) n if n is the least positive integer such that $a^n = e$.

Note

1. In any group the identity element is always of order 1.
2. $o(a) = 1, a \in G \Rightarrow a^1 = a = e$ for multiplicative composition.
3. $a^n = e \Rightarrow o(a) \leq n$

Example

1. Show that the set of integers {1, 5, 7, 11} is a group under multiplication modulo 12.

Solution

Let G = {1, 5, 7, 11}. Let $a, b, c \in G$ be arbitrary. We define an operation $\times_{12}$ on G as follows:

$$a \times_{12} b = r, \quad 0 \leq r \leq 12$$

where r is the least non-negative integer when ordinary product ab is divided by 12 we form the composition table as:

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Closure property

Since all the entries in the composition table are the elements of G and hence G is closed w.r.t $\times_{12}$.

Associative law

$(a \times_{12} b) \times_{12} c = a \times_{12} (b \times_{12} c)$

LHS = Least positive remainder when ordinary product (ab)c is divided by 12.

= Least positive remainder when product a(bc) is divided by 12

= $a \times_{12} (b \times_{12} c)$ = RHS

Existence of inverse

From the composition table it is clear that:

$$5 \times_{12} 5 = 1,\ 7 \times_{12} 7 = 1,\ 11 \times_{12} 11 = 1$$

Inverse of 1, 5, 7, 11 are 1, 5, 7, 11 respectively.

All these belongs to G.

Existence of identity

$1 \in G$ is identity of $1 \times_{12} a = a$

$\therefore (G, \times_{12})$ is a group

2. Verify that the totality of all positive rationals forms a group under the composition defined by $a * b = \frac{ab}{2}$.

1

PU
April 2009 – 5 M

Solution

Let Q^+ denote the set of all positive rationals. Let $a, b, c \in Q^+$ be arbitrary. We define an operation $*$ on Q^+ as follows:

$$a * b = \frac{ab}{2}$$

Our claim is to show that $(Q^+, *)$ is a group.

Closure property

$a, b \in Q^+ \Rightarrow a * b \in Q^+$

$a, b \in Q^+ \Rightarrow \frac{ab}{2} \in Q^+$

Associativity

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

For $(a * b) * c = \left(\frac{ab}{2}\right) * c = \left(\frac{ab}{2}\right)\left(\frac{c}{2}\right) = \frac{abc}{4}$

$= \frac{a}{2}\left(\frac{bc}{2}\right) = a * \left(\frac{bc}{2}\right) = a * (b * c)$

Existence of identity

e will be identity for Q^+ if $a * e = a$, i.e. if $\frac{ae}{2} = a$

$$\frac{ae}{2} = a \Rightarrow a(e-2) = 0 \Rightarrow e-2 = 0 \qquad \because a > 0$$

$$\Rightarrow e = 2$$

Also $2 \in Q^+$. Thus $\exists$ identity element $2 \in Q^+$.

Existence of inverse

If p is the inverse of a, then we must have

$p * a = e = 2$ or $\frac{pa}{2} = 2$ or $p = \frac{4}{a}$

$a \in Q^+ \Rightarrow \frac{4}{a} > 0 \Rightarrow P \in Q^+$

Inverse of every element a is $\frac{4}{a} \in Q^+$

$(Q^+, *)$ is a group

Remark

$a * b = \frac{ab}{2}$ $\qquad b * a = \frac{ba}{2}$

Hence, $(Q^+, *)$ is a commutative group.

3. The set of integers Z is an infinite abelian group for the operation * defined by:

$a * b = a + b + 1 \quad \forall\, a,\ b \in Z$

Solution

We have $Z = \{0, \pm 1, \pm 2, \ldots,\}$

For arbitrary elements $a, b \in Z$ we define

$$a * b = a + b + 1$$

To prove that $(Z, *)$ is an infinite abelian group...**(1)**

Closure property

$a, b \in Z \Rightarrow a * b \in Z$

For $a, b \in Z \Rightarrow a + b + 1 \in Z$

$\Rightarrow a * b \in Z$ according to (1)

Associativity

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

$$(a * b) * c = (a+b+1) * c = (a+b+1)+c+1 = a+b+c+2$$

$$a * (b * c) = a * (b+c+1) = a+(b+c+1)+1 = a+b+c+2$$

Existence of identity

If $e \in Z$ is the identity, then we must have $e * a = a,$

$$e+a+1 = a$$

$$e+1 = 0$$

$$e = -1$$

observe that $(-1) * a = -1+a+1 = a$

Also $-1 \in Z$

Thus $\exists$ identity element $-1 \in Z$

Existence of inverse

Let b be the inverse of a so that

$$b * a = e = -1$$

$$b+a+1 = -1$$

$$b = -a-2 \in Z \quad \text{by } (1)$$

$$(-a-2) * a = -a-2+a+1 = -1 = e$$

Hence $-a-2 \in Z$ is the inverse of a.

Every element of Z is inversible

Commutative law

$$a * b = a+b+1$$

$$= b+a+1 \text{ by } (1)$$

$$= b * a$$

4. **Show that the set $G = \{1, w, w^2\}$ is a group w.r.t ordinary multiplication, w being an imaginary cube root of unity.**

Solution

Cube roots of unity are obtained by solving the equation.

$$1^{1/3} = x$$

This gives $x^3 - 1 = 0$ or $(x-1)(x^2+x+1) = 0$

$$\Rightarrow x = 1, \quad \frac{-1 \pm i\sqrt{3}}{2}$$

$$w = \frac{-1 + i\sqrt{3}}{2}, \quad \text{then } w^2 = \frac{1 - i\sqrt{3}}{2}, \quad w^3 = 1$$

$$G = \{1, w, w^2\}$$

We are required to prove that (G, .) is a group, where (.) denotes ordinary multiplication.

$$w^2 . w^2 = w$$

$$w . w^2 = 1$$

.	1	w	w^2
1	1	w	w^2
w	w	w^2	1
w^2	w^2	1	w

Closure property

Since all the entries in the composition table are elements of G and hence G is closed w.r.t multiplication.

Associative and commutative laws

Since elements of G are complex numbers. Hence multiplication in G is associative as well as commutative.

$$(1 . w) w^2 = w . w^2 = 1$$

$$1 . (w . w^2) = 1 . w^3 = w^3 = 1$$

$$(1 . w) . w^2 = 1. (w . w^2)$$

$$(w^2 . w) . 1 = w^2 (w . 1)$$

It can be easily proved that

$$ab = ba \ \forall \ a, b \in G$$

Existence of identity

$1 \in G$ and 1 is the identity in G.

Existence of inverse

Every element of G is inversible then inverse of $a \in G$ is $a^{-1} = \frac{1}{a}$

For $1^{-1} = 1 \in G \quad w^{-1} = \frac{1}{w} = \frac{w^2}{w} = w^2 \in G$

$$(w^2)^{-1} = \frac{1}{w^2} = \frac{w^3}{w^2} = w \in G$$

$o(G) = 3$

For G contains 3 elements

$\therefore$ (G, .) is an abelian group

5. Prove that the four fourth roots of unity namely 1, i, –1, –i form an abelian multiplicative group of order 4.

Solution

Let $G = \{1, -1, i, -i\}$

To prove (G, .) is an abelian group of order 4. We form the composition table as:

.	1	–1	i	–i
1	1	–1	i	–i
–1	–1	1	–i	i
i	i	–i	–1	1
–i	–i	i	1	–1

Closure property

Since all the entries in the composition table are the elements of G and hence G is closed w.r.t multiplication.

Associative Law

$(ab)c = a(bc) \ \forall\ a, b, c \in G$

$1[(-1)i] = [1(-1)]\, i$ as each side is equal to –i.

Commutative law

$ab = ba \ \forall a, b \in G$

From the composition it is clear that elements in each row are the same as elements in the corresponding column so that ab = ba.

Existence of identity

$1 \in G$ is identity as $1 \cdot a = a \cdot 1 = a$

It follows from the first row and first column.

Existence of inverse

The inverse of a is $a^{-1} = \frac{1}{a}$.

Inverse of 1, –1, i, –i are 1, –1, i, –i respectively.

All these belongs to G.

$o(G) = 4$

Since G contains 4 elements.

$\therefore$ (G, .) is an abelian group.

6. Is the set {1, 2, 3, 4, 5} a group under

i. addition modulo 6 **ii. multiplication modulo 6**

Solution

Let G = {1, 2, 3, 4, 5}. The operations addition modulo 6 and multiplication modulo 6 are denoted by $+_6$ and $\times_6$ respectively.

i. To test the nature of $(G, +_6)$

$2 +_6 5 = 1$ for $2 + 5 = 7 = 1 \times 6 + 1$

$1 +_6 4 = 5$ for $1 + 4 = 5$

$3 +_6 5 = 2$ for $3 + 5 = 8 = 1 \times 6 + 2$

We prepare the composition table as

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Since all the entries in the composition table do not belong to G, in particular $0 \notin G$.

Hence G is not closed w.r.t $+_6$ consequently, $(G, +_6)$ is not a group.

ii. To test the nature of the system $(G, \times_6)$

$2 \times_6 5 = 4$ for $2 \times 5 = 10 = 1 \times 6 + 4$

$3 \times_6 4 = 0$ for $3 \times 4 = 12 = 2 \times 6 + 0$

In this way we prepare the composition table as:

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

From the composition table, it is clear that all the entries in the composition table do not belong to G, in particular $0 \notin 6$. Hence, G is not closed w.r.t $\times_6$.

$(G, \times_6)$ is not a group.

7. Find the following is a group under multiplication modulo 11: {1, 2, 3, 4, 5, 9}.

1

PU
Oct. 2010 – *5 M*

Solution

$\times_{11}$	1	2	3	4	5	9
1	1	2	3	4	5	9
2	2	4	6	8	10	7
3	3	6	9	1	4	5
4	4	8	1	5	9	3
5	5	10	4	9	3	1
9	9	7	5	3	1	4

Since the operation: Multiplication modulo 11 is not closed on A, it is not a group.

8. Prove that if G is an abelian group, then for all a, b $\in$ G and for all integers n,$(ab)^n = a^n b^n$

Solution

Let a, b be arbitrary elements of a commutative group G so that ab = ba ....(1)

Let n be any integer, a $\in$ G $\Rightarrow$

$a^2 = a . a \in G$ by closure property

$a^3 = a . a . a \in G$

$a^n \in G$ by induction

Similarly b $\in$ G$\Rightarrow$ $b^n \in G$

In view of (1) we have

$a^n b^n = b^n a^n$, $a^n b = ba^n$, $ab^n = b^n a$ ....(2)

claim : $(ab)^n = a^n b^n$

Case 1: When n = 0

By definition of identity element

$a^0 = e$, $b^0 = e$, $(ab)^0 = e$, $a^0 b^0 = e$, e = e

Thus $(ab)^0 = e = a^0 b^0$

(or) $(ab)^n = a^n b^n$ if n = 0

Hence, the required result is true if n = 0

Case 2: When n > 0

$(ab)^1 = ab = a^1 b^1$ or $(ab)^1 = a^1 b^1$

$\therefore (ab)^n = a^n b^n$ if n = 1

Hence the required result is true for n = m so that

$(ab)^m = a^m b^m$

$$\begin{aligned}(ab)^{m+1} &= (ab)^m (ab) = (a^m b^m)(ab) = a^m (b^m a)b \\ &= a^m(ab^m)\, b \qquad \text{by (2)} \\ &= (a^m a)(b^m b) \\ &= a^{m+1} b^{m+1}\end{aligned}$$

This shows that the required result is true for n = m + 1 if it is true for n = m. Hence, the result is true by mathematical induction.

$$(ab)^n = a^n b^n \quad \forall\, n > 0$$

Case 3: When $n < 0$ (n is a negative integer)

$n = -m$, where m is a positive integer,

$$\begin{aligned}(ab)^n &= (ab)^{-m} = [(ab)^m]^{-1} = (a^m b^m)^{-1} \qquad \text{by case (2)} \\ &= (b^m a^m)^{-1} \qquad \text{by(2)} \\ &= (a^m)^{-1} (b^m)^{-1} \ \text{since } (ab)^{-1} = b^{-1} a^{-1} \\ &= a^{-m} b^{-m} \\ &= a^n b^n \\ \therefore (ab)^n &= a^n b^n\end{aligned}$$

From cases (1), (2) and (3) it follows that $(ab)^n = a^n b^n \ \forall\, n \in Z$

2.5 Isomorphism of Groups

Definition

Let (G, ∗) and (G', ∗') be two groups. Any map $f : (G, *) \to (G', *')$ is called a homomorphism if $f(x * y) = f(x) *' f(y)$

The homomorphism f is called isomorphism if f is one-one onto or one-one into.

Definition

Let (G, ∗) and (G', ∗') be any two groups. A one-one onto map.

$f : (G, *) \to (G', *')$ is called an isomorphism

iff $f(a * b) = f(a) *' f(b) \quad \forall a, b \in G$

In this case we say that G is isomorphic to G' and write as $G \cong G'$

We also say that G is isomorphically mapped onto G' and G' are isomorphic groups.

Alternately isomorphism is defined as one-one onto map.

$f : (G, *) \to (G', *')$

which preserves the group structures.

Example

If R is the additive group of real numbers and R^+ the multiplicative group of positive real numbers, then the mapping $f : R \to R^+$ defined by $f(x) = e^x, \forall x \in R$ is an isomorphism.

Automorphism

Definition

An isomorphism of a group onto itself is called an automorphism of the group.

A one-one onto map $f : (G, *) \rightarrow (G, *)$ is called an automorphism of the group, $(G, *)$ if $f(x * y) = f(x) * f(y) \quad \forall x, y \in G$.

Examples

Let $(G, *)$ be a group

A map of $f : (G, *) \rightarrow (G, *)$ given by $f(x) = x \ \forall \ x \in G$ is an automorphism of G.

Inner automorphism

Let $(G, *)$ be a group and $a \in G$ be arbitrary but fixed. A map $f_a : (G, *) \rightarrow (G, *)$ given by $f_a(x) = a^{-1} xa, \forall x \in G$ is an automorphism of G, a^{-1} being the inverse of a. This automorphism is called inner automorphism.

Outer automorphism

An automorphism is called outer automorphism if it is not inner automorphism.

Properties of Isomorphic groups

i. Let G and G' be groups. If the mapping $f : G \rightarrow G'$ is isomorphism, show that the identities correspond.

ii. Let $(G, *)$ and $(G', *')$ be groups. If the mapping $f : (G, *) \rightarrow (G', *')$ is an isomorphism, show that inverses correspond.

iii. If $f : (G, .) \rightarrow (G', .)$ is an isomorphism of groups, show that the order of an element $a \in G$ is equal to order of the f-image of a, i.e., $o(a) = o[f(a)]$.

iv. The relation of isomorphism in the set of all groups is an equivalence relation.

v. Transference of group structures: Suppose G is a group and G' is a set with multiplicative composition. Also suppose that there exists one-one map $f : G \xrightarrow{\text{onto}} G'$ such that $f(xy) = f(x) f(y); x, y \in G$.

Examples

1. **Show that the group of non-zero integers multiplications modulo 5 is isomorphic to the group of integers under addition modulo 4.**

OR

Show that the group $[\{0, 1, 2, 3\}, +_4]$ is isomorphic to the group$[\{1, 2, 3, 4\}, \times_5]$.

Solution

Let $G = \{0, 1, 2, 3\}$ and $G' = \{1, 2, 3, 4,\}$

To prove that $(G, +_4) \cong (G', +_5)$

Define a map $f : G \rightarrow G'$ by requiring that $o(a) = o[f(a)] \ \forall \ a \in G$

0 is the identity in G and 1 is the identity in G'.

We know that order of identity element in every group is one.

Hence.

$o(0) = 1,\ o(1) = 1$

For elements of G : $o(a) = n \Rightarrow na = e = 0$

$1 \cdot 1 = 1, 2 \cdot 1 = 2, 3 \cdot 1 = 3, 4 \cdot 1 = 0 = e$

$o(1) = 4$

$1 \cdot 2 = 2, 2 \cdot 2 = 0 = e, o(2) = 2$

$1 \cdot 3 = 3, 2 \cdot 3 = 2, 4 \cdot 3 = 0 = e, o(3) = 4$

For elements of G': $o(a) = n \Rightarrow a^n = e = 1$

$2^1 = 2, 2^2 = 4, 2^3 = 3, 2^4 = 1 = e$

$o(2) = 4$

$3^1 = 3, 3^2 = 4, 3^3 = 2, 3^4 = 1 = e$

$o(3) = 4$

$4^1 = 4, 4^2 = 1$

$o(4) = 2$

Order of elements $0, 1, 2, 3 \in G$ are 1, 4, 2, 4 respectively.

Order of elements $1, 2, 3, 4 \in G'$ are 1, 4, 4, 2 respectively.

$f(0) = 1, f(1) = 2, f(2) = 4, f(3) = 3$

f is one-one onto map.

$$\begin{aligned} \text{Moreover,}\quad f(2 +_4 3) &= f(1) && \text{for } 2 + 3 = 5 = 1 \times 4 + 1 \\ &= 2 \\ &= 4 \times_5 3 && \text{for } 4 \times 3 = 12 = 2 \times 5 + 2 \\ &= f(2) \times_5 f(3) \end{aligned}$$

$f(2 +_4 3) = f(2) \times_5 f(3)$

Similarly, $f(1 +_4 2) = f(1) \times_5 f(2)$

$\Rightarrow$ f is order preserving.

Thus we have proved that f is an isomorphism.

Hence, $G \cong G'$

2. If R is the additive group of real numbers and R^+ is the multiplicative group of positive real numbers, then the map $f : R \to R^+$ defined by $f(x) = e^x, \forall x \in R$ is an isomorphism.

Solution

Consider the map $f : (R, +) \to (R^+, .)$ such that $f(x) = e^x, \forall\ x \in R$

f is one-one.

For $f(x) = f(y);\ x, y \in R \Rightarrow e^x = e^y$

$\Rightarrow x = y$

f is ONTO.

Given any $y \in R^+$, $\exists \log y \in R$ such that $f(\log y) = e^{\log y} = y$

Hence, f is onto.

f preserves compositions in R and R^+.

For if $x, y \in R$ then

$$f(x+y) = e^{x+y} = e^x \cdot e^y$$
$$= f(x)\, f(y)$$

i.e., $f(x+y) = f(x) \cdot f(y)$

Hence f is an isomorphism.

3. **The additive group G of integers is isomorphic to the multiplicative group G', where: $G' = \{\ldots, 3^{-3}, 3^{-2}, 3^{-1}, 3^0, 3^1, 3^2, \ldots\}$.**

Solution

$$G = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$$
$$G' = \{3^0, 3^{\pm 1}, 3^{\pm 2}, 3^{\pm 3}, \ldots\}$$

Define a map $f : (G, +) \rightarrow (G', .)$ given by $f(x) = 3^x$

f is one-one

For $f(x_1) = f(x_2);\ x_1, x_2 \in G$

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

$\Rightarrow x_1 = x_2$

f is onto.

For given $3^n \in G'$, $\exists n \in G$ such that $f(n) = 3^n$

f preserves compositions in G and G'.

$$f(x+y) = 3^{x+y} = 3^x \cdot 3^y$$
$$= f(x)\, f(y)$$

$\therefore$ f is an isomorphism.

4. **If a is a fixed element of a group G, then the map $G \rightarrow G$ such that $f(x) = a\,x\,a^{-1}$, $\forall x \in G$ is an isomorphism of G onto itself.**

Solution

Let $x, y, a \in G$ be arbitrary but a is fixed. Let G be a group with identity. Suppose $f : G \rightarrow G$ such that $f(x) = axa^{-1}$

i. f is one-one

For $f(x) = f(y) \Rightarrow axa^{-1} = aya^{-1}$

$\Rightarrow xa^{-1} = ya^{-1}$

$\Rightarrow x = y$ by cancellation law

ii. f is onto

For given any $z \in G$, $\exists a^{-1} za \in G$ such that

$f(a^{-1} za) = a(a^{-1} za) a^{-1} = (aa^{-1}) z aa^{-1}$

$= e z e = z$

iii. f is composition preserving

For $f(xy) = a (xy)a^{-1} = (ax) (ya^{-1})$

$= (ax) (a^{-1} a) (ya^{-1})$

$= (axa^{-1}) (aya^{-1}) = f(x) f(y)$

These facts prove that f is isomorphism onto.

5. Let T be the set of all even integers. Show that the semigroups (Z, +) and (T, +) are isomorphic?

1

PU
April 2010 – 7 *M*

Solution

$T = \{\ldots -4, -2, 0, 2, 4, 6, \ldots\}$

$Z = \{\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

T and Z are associative under '+.

We can define bijective function from T to Z.

So that $f: T \to Z$

$0 \to 0$

$2 \to 1$

$4 \to 2$

$6 \to 3$

.
.
.

and $t \in T \ \exists\ z \in Z$
so that t = 2 Z
Hence semigroups (Z, +)
and (T, +) are isomorphic.

2.6 Cyclic Groups

A group is said to be cyclic if it is capable of being generated by a single element. The single element is called the generator of the group.

If a cyclic group G is generated by an element a, then we shall write G = {a}. It is not necessary that all the elements of a cyclic group are distinct.

Examples

i. The group (Z, +) is cyclic and its generator is 1. Another generator is –1.

ii. The multiplicative group $\{1, w, w^2\}$ is cyclic and generators are w and w^2.

Properties

i. Every cyclic group is necessarily abelian.

ii. If a is generator of a cyclic group G, then a^{-1} is also a generator of G.

iii. Every infinite cyclic group is isomorphic to the additive group of integers.

iv. The order of a cyclic group is equal to the order of any generator of the group.

v. A cyclic group of finite order n is isomorphic to the additive group of residue classes.

vi. A cyclic group G with a generator of finite order n, is isomorphic to the multiplicative group of n, nth root of unity.

vii. Every isomorphic image of a cyclic group is cyclic.

viii. A finite group of order n containing an element of order n must be cyclic.

ix. If a cyclic group G is generated by an element a of order n, then a^m is a generator of G iff m and n are relatively primes.

Examples

1. **Show that the group $(G, \times_7)$ is cyclic, where G = {1, 2, 3, 4, 5, 6}. How many generators are there?**

Solution

Firstly we shall prove that if ∃ an element a ∈ G such that o(a) = 6 = o(G) then G will be a cyclic group and a will be the generator of G.

If e is the identity in G, then e = 1 observe that

$3^1 = 3, 3^2 = 3 \times_7 3 = 2$

$3 \times 3 = 9 = 1 \times 7 + 2$

$$3^3 = 3^2 \times_7 3^1 = 2 \times_7 3 = 6$$

$$3^4 = 3^3 \times_7 3^1 = 6 \times_7 3 = 4$$

$$3^5 = 3^4 \times_7 3 = 4 \times_7 3 = 5$$

$$3^6 = 3^5 \times_7 3 = 5 \times_7 3 = 1 = 2 \times 7 + 1$$

$$3^6 = e \text{ and } 3^6 \neq e \text{ for } r < 6$$

o(3) = 6 = o(G)

3 is a generator of G

Since $3^6 = 1, 3^5 = 5, 3^4 = 4, 3^3 = 6, 3^2 = 2, 3^1 = 3$

Hence G is expressible as

$G = \{3^6, 3^5, 3^4, 3^3, 3^2, 3\}$

This shows that G is cyclic.

Now we are to determine the number of generators of G.

If d is HCF of m and n, then we write (m, n) = d.

An element $3^m \in G$ is also a generator of G if (m, 6) = 1.

(1, 6) = 1

(5, 6) = 1

There are only two generators of G namely $3, 3^5$.

2. **Show that the set of non-zero residue classes modulo 5 is a cyclic group under multiplication modulo 5.**

Solution

G = {[1], [2], [3], [4]}

and (G, .) is a group. Here e = [1]

Here $o(a) = n \Rightarrow a^n = e$

$[2]^1 = [2], [2]^2 = [4], [2]^3 = [3]$

$[2]^4 = [1] = e$

o([2]) = 4 = o(G)

[2] is generator of G.

$\Rightarrow$ G is cyclic group.

3. Groups Permutations

Transformation

Let $x \neq \phi$. Any map $f : x \to x$ is called a transformation i.e., any map from a set onto itself is a transformation of the set.

Permutation

Let X be a non-empty finite set. A one-one onto map $f : x \to x$ is called a permutation.

The number of elements in the finite set X is known as degree of the permutation.

Symbol for Permutation

Let $X = \{a_1, a_2, \ldots, a_n\}$ such that $a_i \neq a_j$

for $i \neq j$. Then X contains n distinct elements $f(a_i) = b_i$ for $1 \leq i \leq n$.

The elements $b_1, b_2, \ldots, b_n$ are nothing but a rearrangement of n elements of X.

We shall use a special symbol to denote a permutation.

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ f(a_1) & f(a_2) & f(a_3) & \ldots & f(a_n) \end{pmatrix}$$

Equality of two Permutations

Let f and g be two permutations on a set X. Then we define $f = g$ iff $f(x) = g(x)\ \forall\ x \in X$

Example

1. **Let f and g be given by**

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \qquad g = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

Solution

$f(1) = 2, f(2) = 4, f(3) = 3, f(4) = 1$

$g(2) = 4, g(1) = 2, g(4) = 1, g(3) = 3$

$f(1) = 2 = g(1), f(2) = 4 = g(2)$

$f(3) = 3 = g(3), f(4) = 1 = g(4)$

$\Rightarrow f(x) = g(x) \qquad \forall\ x \in \{1, 2, 3, 4\}$

$\Rightarrow f = g$

Total Number of Distinct Permutations

Let X be a set consisting of n distinct elements. Then the elements of X can be permuted in n! distinct ways, i.e., n! distinct arrangement of the elements belonging to X are possible. If P_n be the set consisting of all permutations of degree n, then the set P_n will have n! distinct permutations of degree n.

This set P_n is called the symmetric set of permutations of degree n. Sometimes it is also denoted by S_n. Thus

$P_n = \{f : f \text{ is a permutation of degree } n\}$

Example

The set P_3 of all permutations of degree 3 will contain $3! = 6$ permutations given as below.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Identity Permutation

If a permutation I of degree n is such that the I-image of every element is the same element i.e., $I(x) = x, \forall\ x$

then I is called identity permutation.

Example

$$I = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

Inverse Permutation

Since a permutation is one-one ONTO map and hence it is inversible, i.e., every permutation f on a set P = $\{a_1, a_2, \dots, a_n\}$ has a unique inverse permutation denoted by f^{-1}. Thus if;

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \text{ then } f^{-1} = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

Product or Composition of Two Permutations

Let X = $\{a_1, a_2, \dots, a_n\}$. Let $f : x \to x$ and $g : x \to x$ be one-one onto maps. Then f and g are permutations of degree n. Clearly $g \circ f : x \to x$ and $f \circ g : x \to x$ are one-one onto maps. Hence $f \circ g$ and $g \circ f$ are permutations of degree n.

Examples

1. If f $= \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$, **g** $= \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$

Solution

$$fg = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

2. Let f $= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, **g** $= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Let I denote identity permutation. Find gf, fg, f^{-1}, g^{-1}. Also verify that $ff^{-1} = gg^{-1}$ = I. Hence prove that multiplication of permutation is not commutative, in general.

Solution

We know that interchange of columns will not change the nature of the permutation.

$$fg = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$gf = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$fg \neq gf$$

$$fI = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 1 & 2 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f$$

$$fI = f$$

Similarly, $gI = g$

$$f^{-1} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}, \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$ff^{-1} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\begin{pmatrix}3 & 1 & 2\\ 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = I$$

$$gg^{-1} = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 1 & 2 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}= I$$

Cyclic Permutation

The permutation which replaces n objects cyclically is called a cyclic permutation.

The number of distinct objects permuted by a cyclic is known as the length of the cycle.

Examples

i. $\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$ is a cyclic permutation of length 3.

ii. $\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix}$ is a cyclic permutation of length 4.

Disjoint Cycles

Two cycles are said to be disjoint iff they have no elements in common.

Examples

i. (1 2) and (5 6) are disjoint cycles.

ii. (1 3 5) and (5 4 1) are not disjoint cycles.

Symmetric Group of Permutations

The set P_n of all permutations of degree n forms a finite non-abelian group w.r.t permutation multiplication as composition.

Transposition

A cycle of length 2 is known as transposition. Thus a transposition is a cycle of the form $(a_i\ a_j)$ in which the symbols a_i, a_j are interchanged and other symbols remain unchanged.

Even and Odd Permutations

Let $P = \begin{pmatrix}1 & 2 & 3 \ldots n\\ a_1 & a_2 & a_3 \ldots a_n\end{pmatrix}$

be a permutation of degree n. The pair (i, k) is said to be regular if i – k and $a_j - a_k$ both have the same sign; otherwise irregular. Thus for irregularity of any pair (i, k), (i–k) and $(a_i - a_k)$ are of opposite signs. The number of irregular pairs denotes number of inversions.

A permutation of a set of integers onto itself is even or odd according as it contains an even or odd number of **inversions**.

Example

i. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ no inversion; permutation is even

ii. $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ 3 inversions; permutation is odd

iii. $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ 2 inversions; permutation is even

iv. $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ 1 inversion; permutation is odd

Cayley's Theorem

Every finite group G is isomorphic to permutation group G'.

The permutation group G' is called a regular permutation group.

Theorems Related to Permutation

i. The set P_n of all permutations on n symbols is a finite non-abelian group or order n! w.r.t. composition of mapping as the operation.

ii. A permutation P cannot be both even and odd i.e., if a permutation P is expressible as a product of s transpositions and also a product of t transpositions, then either both s and t are even or both are odd.

iii. Of the n! permutations on n symbols, $\frac{n!}{2}$ are even permutations and $\frac{n!}{2}$ are odd permutations.

iv. The set A_n of all even permutations of degree n forms a finite non-abelian group of order $\frac{n!}{2}$ w.r.t permutation multiplication as composition.

Example

1. Find the regular permutation group isomorphic to the multiplicative group G = {1, w, w²}

Solution

By Cayley's theorem, G is isomorphic to the regular permutation group G' consisting of f_1, f_w, f_{w^2} given by:

$$f_1 = \begin{pmatrix} 1 & w & w^2 \\ 1.1 & 1.w & 1.w^2 \end{pmatrix} = \begin{pmatrix} 1 & w & w^2 \\ 1 & w & w^2 \end{pmatrix} = I$$

$$f_w = \begin{pmatrix} 1 & w & w^2 \\ w.1 & w.w & w.w^2 \end{pmatrix} = \begin{pmatrix} 1 & w & w^2 \\ w & w^2 & 1 \end{pmatrix} = (1\ w\ w^2)$$

$$f_{w^2} = \begin{pmatrix} 1 & w & w^2 \\ w^2.1 & w^2.w & w^2.w^2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & w & w^2 \\ w^2 & 1 & w \end{pmatrix} = \begin{pmatrix} 1 & w^2 & w \\ w^2 & w & 1 \end{pmatrix} = (1\ w^2\ w)$$

$\therefore \{I, (1\ w\ w^2), (1\ w^2\ w)\}$

4. Subgroups

4.1 Introduction

Let (G, $*$) be group and $H \subset G$ be arbitrary such that $H \neq \phi$.

By properties of a group.

$$\forall\, a, b \in H \;\Rightarrow a, b \Rightarrow G \qquad \text{for } H \subset G$$

$$\Rightarrow a * b \in G$$

$$\Rightarrow a * b \in H \text{ or } a * b \notin H$$

If $a * b \in H$, then we say that H is stable for the composition in G and the composition in G has induced a composition in H. Now there are two possibilities:

i. H is itself a group relative to the operation $*$.

ii. H is not a group w.r.t. the operation $*$.

Definitions

Let (G, $*$) be a group. Then any non-empty subset H of G is called a complex of G.

Let H be any complex of a group (G, $*$). Then H is said to be stable for the composition in G iff

$$\forall\, a, b \in H \;\Rightarrow a * b \in H$$

Suppose a complex H of a group (G, $*$) is stable for the composition in G. Then we say that the composition in G has induced a composition in H. This composition in H is called induced composition.

Definition of a subgroup

Any non-empty subset H of a group (G, $*$) is called a subgroup of (G, $*$) iff

i. H is stable for the operation $*$.

ii. (H, $*$) is a group.

The two subgroups (G, $*$) and ({e}, $*$) of the group (G, $*$) are called improper (or trivial) subgroups of G. Any subgroup other than these two subgroups is called a proper (or non-trivial) subgroup.

Examples

i. $[\{1, -1\}, *]$ is a subgroup of $[\{1, -1, -i\}, *]$.

ii. (Z, +) is a subgroup of (Q, +).

iii. (Q, +) is a subgroup of (R, +).

Theorems

i. A non-empty subset H of a group G is a subgroup of G iff

a. $a, b \in H \Rightarrow ab \in H$

b. $a \in H \Rightarrow a^{-1} \in H$ where a^{-1} is the inverse of a in G.

ii. A necessary and sufficient condition for a non-empty subset H of a finite group G to be a subgroup is that:

$a \in H, b \in H \Rightarrow ab \in H$.

iii. A necessary and sufficient condition for a non-empty finite subset H of a group G to be a subgroup is that H must be closed.

iv. A necessary and sufficient condition that a non-empty subset of a group G to be a subgroup is a $\in H, b \in H \Rightarrow ab^{-1} \in H$.

v. If H is a subgroup of a group G, then $H^{-1} = H$ but the converse is not true.

vi. If H and K are any two complexes of a group G $(HK)^{-1} = K^{-1} H^{-1}$.

vii. A necessary and sufficient condition of a non-empty subset H of a group G to be a subgroup is $HH^{-1} \subset H$.

viii. A necessary and sufficient condition for a non-empty subset H of a group G to be a subgroup is that $HH^{-1} = H$.

ix. If H, K are subgroups of a group G, then HK is a subgroup of G iff HK = KH.

x. The intersection of any two subgroups of a group G is a subgroup of G.

xi. The union of two subgroups of a group G is a subgroup of G iff one is contained in the other.

Examples

1. Prove that the set of all multiple integers by a fixed integers m, is a subgroup of (Z, +).

Solution

$$H = \{mn; n \in Z\}$$
$$= \{0, \pm m, \pm 2m, \pm 3m, \ldots\}$$

where $m \in Z$ is fixed.

To prove that H is a subgroup of (Z, +)

Any $a, b \in H \Rightarrow \exists\, r, s \in Z$ such that $a = mr, b = ms$

$\Rightarrow a - b = m\,(r - s)$, $r - s$ is an integer

$\Rightarrow a - b \in H$

i.e., Any $a, b \in H \Rightarrow a - b \in H$

H is a subgroup of (Z, +)

2. If a is any element of a group G, then $\{a^n : n \in Z\}$ is a subgroup of G.

Solution

Let a be an arbitrary element of a group G. Let $H = \{a^n : n \in Z\}$

To prove that H is a subgroup of G.

Any $h_1, h_2 \in H \Rightarrow h_1 = a^x, h_2 = a^y$ where $x, y \in Z$

$\Rightarrow h_1 h_2^{-1} = a^{x-y}$ where $x - y \in Z$

$\Rightarrow h_1 h_2^{-1} \in H$ by definition of H.

3. Let $(Z_6, +)$ be a group and $S = \{[0], [3]\}$ be a subgroup. Is a normal subgroup?

1 PU April 2010 – 5 M

Solution

We have $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$

and $[0]^{-1} = [0] \qquad [3]^{-1} = [3]$

$[1]^{-1} = [5] \qquad [4]^{-1} = [2]$

$[2]^{-1} = [4] \qquad [5]^{-1} = [1]$

By definition, S will be normal subgroup of Z_6 if $xhx^{-1} \in S \; \forall \; x \in z_6$ and $h \in S$.

Now $[0] +_6 [0] +_6 [0] = [0] \in S$

$[1] +_6 [0] +_6 [5] = [6] = [0] \in S$

$[2] +_6 [0] +_6 [4] = [6] = [0] \in S$

$[3] +_6 [0] +_6 [3] = [6] = [0] \in S$

$[4] +_6 [0] +_6 [2] = [6] = [0] \in S$

$[5] +_6 [0] +_6 [1] = [6] = [0] \in S$

and $[0] +_6 [3] +_6 [0] = [3] \in S$

$[1] +_6 [3] +_6 [5] = [9] = [3] \in S$

$[2] +_6 [3] +_6 [4] = [9] = [3] \in S$

$[3] +_6 [3] +_6 [3] = [9] = [3] \in S$

$[4] +_6 [3] +_6 [2] = [9] = [3] \in S$

$[5] +_6 [3] +_6 [1] = [9] = [3] \in S$

$\therefore$ S is a normal subgroup of Z_6.

4.2 Cosets

These cosets are also called residue classes modulo the subgroup

Definition

Suppose H is a subgroup of a group $(G, *)$. Let $a \in G$ be arbitrary. We define

$aH = \{ah; h \in H\}, Ha = \{ha; h \in H\}$

$aH \subset G, Ha \subset G$

aH is called left coset of H in G generated by a. Ha is called right coset of H in G generated by a.

If e is the identity for G, then $e \in H$ is also identity for H.

$a = ae \in aH$, $a = ea \in Ha$

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

$He = H = eH$

Hence H itself is right as well as left coset.

If the group $(G, *)$ is abelian, then $ah = ha \ \forall h \in H$ so that $aH = Ha \ \forall a \in G$

Examples

1. Let $H = \{3n : n \in Z\}$ be subgroup of commutative group $(Z, +)$. Then $H = \{0, \pm 3, \pm 6, \ldots\}$.

Solution

$$1 \in Z,\quad H + 1 = \{h + 1 : h \in H\} = \{3n + 1 : n \in Z\}$$
$$= \{1, 4, 7, 10, \ldots, -2, -5, -8, -11, \ldots\}$$

For any $h \in H \Rightarrow \exists n \in Z$ such that $h = 3n$

$$2 \in Z,\quad H + 2 = \{3n + 2 : n \in Z\}$$
$$= \{2, 5, 8, 11, \ldots; -1, -4, -7, \ldots\}$$
$$3 \in Z,\quad H + 3 = \{3n + 3 : n \in Z\} = \{3(n + 1) : n \in Z\}$$
$$= \{3, 6, 9, \ldots; 0, -3, -6, \ldots\} = H$$
$$H + 3 = H, 3 \in H$$
$$H + 4 = H + 1, 4 \in H + 1$$

Generalising this result we have

$$H + n = H + a \text{ if } n \in H + a$$

$\exists$ three disjoint right cosets namely H, H + 1, H + 2.

2. Find the left cosets of $\{[0], [3]\}$ in the group $\langle Z_6, +_6\rangle$.

1

PU
Oct. 2008 – 7 M

Solution

$G = \langle Z_6, +_6\rangle \qquad H = \{[0], [3]\}$ and $Z_6 = \{[0], [1], [2], [3], [4], [5]\}$.

The left coset of H in G generated by $a \in G$ w.r.t. $+_6$ is defined as.

$$a + H = \{a + h; h \in H\}.$$

Now $a = [0]$ which is identity element of $(Z_6, +_6)$ $\therefore$ $a + H = [0] + H = H$. $[e + H = H]$

$$a = [1]$$
$$[1] + H = \{[1] + [0], [1] + [3]\} = \{[1], [4]\}$$

$$a = [2]$$

$$[2] + H = \{[2] + [0], [2] + [3]\} = \{[2], [5]\}$$

$$a = [3], \in H$$

$$\therefore\ a + H = H \qquad [\because \text{If } a \in H \text{ then } a + H = H].$$

i.e., $[3] + H = H$

$$a = [4]$$

$$[4] + H = \{[4] + [0], [4] + [3]\} = \{[4], [1]\}$$

i.e., $[4] + H = [1] + H$

$$a = [5]$$

$$[5] + H = \{[5] + [0], [5] + [3]\} = \{[5], [2]\}$$

i.e., $[5] + H = [2] + H$

$\therefore$ There are three distinct left coset of H in G w. r. t $+_6$ i.e., H, [1] +H, [2] + H.

3. Let G = {a, b, c, d} and * is the operation on G defined by Cayley table. Is G an abelian group?

1

PU
April 2010 – *7 M*

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Solution

i. We note that $\forall$ a, b, $\in$ G,

$a * b \in G$

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

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

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

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

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

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

$\therefore$ * is associative.

iii. Identity element e = 'a'

iv. Inverse of a = a

$b^{-1} = d$

$c^{-1} = c$

$d^{-1} = b$

Inverse of each element exists.

v. $a * b = b$

$b * a = b \quad \therefore a * b = b * a$

$a * c = c = c * a$

$a * d = d = d * a$

$b * c = d = c * b$

$b * d = a = d * b$

$*$ is commutative

$\therefore$ G is an abelian group.

4. Consider the group G = {0, 1, 2, 3, 4, 5, 6} under addition modulo 7.

i. Find the addition table of G.

ii. Obtain the left and right coset of G.

1

PU
Oct. 2010 – *7 M*

Solution

i. Find the addition table of G.

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

ii. Obtain the left and right coset of G.

Note: To obtain left and right cosets of G, subgroup of G is not provided. Even then if we find right and left cosets of G.

$aG = Ga = G, \ \forall a \in G.$

Lagrange's Theorem

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

Examples

1. If G is a group, then show that C = {c ∈ G, cx = xc ∀ x ∈ G} is a subgroup of G.

Solution

Suppose G is a group and $C = \{c \in G, cx = xc, \forall x \in G\}$

To prove that C is a subgroup of G. For this we shall show that:

i. Any $a \in C \Rightarrow a^{-1} \in C$

$a \in C \Rightarrow ax = xa, \forall x \in G$

$\Rightarrow x = a^{-1}xa$

$\Rightarrow xa^{-1} = a^{-1}x, \forall x \in G$

$\Rightarrow a^{-1} \in C$

ii. Any $a, b \in C \Rightarrow ab \in C$

$a, b \in C \Rightarrow ax = xa, bx = xb, \forall x \in C$

$\Rightarrow (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$

$\Rightarrow (ab)x = x(ab), \forall x \in G$

$\Rightarrow ab \in C$

2. **If G is a group and $a \in G$, then show that $N(a) = \{x \in G : ax = xa\}$ is a subgroup of G.**

Solution

Let a be an arbitrary element of a group G and let

$N(a) = \{x \in G : ax = xa\}$

To prove N(a) is a subgroup of G, we have to show that

i. $x \in N(a) \Rightarrow x^{-1} \in N(a)$

ii. $x, y \in N(a) \Rightarrow xy \in N(a)$

iii. $x \in N(a) \Rightarrow ax = xa$

$\Rightarrow a = xax^{-1}$

$\Rightarrow x^{-1}a = ax^{-1}$

$\Rightarrow x^{-1} \in N(a)$

iv. $x, y \in N(a) \Rightarrow xa = ax, ay = ya$

$\Rightarrow (xy)a = x(ya) = x(ay) = (xa)y$

$\Rightarrow (ax)y = a(xy)$

$\Rightarrow (xy)a = a(xy)$

$\Rightarrow xy \in N(a)$

3. **Show that the set of inverses of the elements of a right cosets is a left cosets i.e., $(Ha)^{-1} = a^{-1}H$.**

Solution

Let Ha be a right coset of a Subgroup H in a group G, where $a \in G$.

To prove $(Ha)^{-1} = a^{-1}H$

Any $x \in (Ha)^{-1}$, $\exists\, h \in H$ s.t. $x = (ha)^{-1} = a^{-1}h^{-1}$

$\Rightarrow x = a^{-1} h^{-1}, h^{-1} \in H$

$\Rightarrow x = a^{-1} h^{-1} \in a^{-1} H$

$\Rightarrow x \in a^{-1} H$

Again any $x \in a^{-1} H \Rightarrow x = a^{-1}h, h \in H$

$\Rightarrow x = a^{-1}(h^{-1})^{-1} = (h^{-1}a)^{-1} \in (Ha)^{-1}$

$\Rightarrow x \in (Ha)^{-1}$

Any $x \in a^{-1} H \Leftrightarrow x \in (Ha)^{-1}$

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

4. **Let H = {1, a²} be a subgroup of a cyclic group G = {a} which is of order 4. Find all left cosets of H in G. Further show that the union of all these cosets is equal to G and any two cosets are either identical or disjoint.**

Solution

Given: $G = \{a\}, o(G) = 4$

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

$G = \{a, a^2, a^3, a^4 = 1 = a^0\}$

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

$aH = \{a, a^3\}$

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

$a^3H = \{a^3, a^5\} = \{a^3, a\} = aH$

$a^4H = \{a^4, a^6\} = \{1, a^2\} = H$

Distinct coset of H are H, aH

$H \cap aH = \{1, a^2\} \cap \{a^1, a^3\} = \phi$

$H \cup aH = \{1, a^2\} \cup \{a, a^3\} = \{1, a, a^2, a^3\} = G$

4.3 Normal Subgroup

Definition

A subgroup H of a group G is called a normal subgroup of G iff $xhx^{-1} \in H \quad \forall x \in G$ and $\forall h \in H$ i.e., iff $xHx^{-1} \subset H, \forall x \in G$

The symbol "H Δ G" is read as, "H is a normal subgroup of the group G".

Every group G possesses two normal subgroups namely G and {e} e being identity in G. These two normal subgroups are called improper normal subgroups of G.

A normal subgroup H of a group G is called a proper normal subgroup of G iff $H \neq G, H \neq \{e\}$

A group having only improper normal subgroups is called a simple group.

4.4 Normalizer of an Element

$a \in G$ is the set of those elements of G which commute with a and is denoted by N(a). Symbolically $N(a) = \{x \in G : ax = xa\}$.

Remark

i. N(a) is a subgroup of G.

ii. N(a) is not a normal subgroup of G.

iii. $N(e) = G$ for $ex = xe \ \forall \ x \in G$.

iv. $N(a) = G$ iff G is abelian.

4.5 Centre of a Group

The centre of a group G is defined as an abelian part of a group and is denoted by Z.

$Z = \{x \in G : xy = yx \ \forall \ y \in G\}$

4.6 Conjugate Element

Let G be a group. An element $a \in G$ is called conjugate to an element $b \in G$ iff $a = x^{-1} bx$ for some $x \in G$.

If $a = x^{-1}bx$, then we sometimes say that a is the transform of b by x. The element x is not unique for the ordered pair a, b.

The symbol "$a \overset{c}{=} b$" is read as "a is conjugate to b".

4.7 Quotient Group

Let G be a group and N be its normal subgroup. Then

$$\frac{G}{N} = \{Nx : x \in G\}$$

is group w.r.t multiplication of cosets: $(Nx)(Ny) = N(xy), \ \forall \ x, y \in G$

The group $\frac{G}{N}$ is called quotient group.

Examples

1. **Show that every subgroup of an abelian group is normal.**

Solution

Let H be a subgroup of an abelian group G.

To prove that H is normal in G.

Let $h \in H$, $x \in G$ be arbitrary. Let e be an identity in H.

G is abelian $\Rightarrow xhx^{-1} = (hx)x^{-1}$

$$= h(xx^{-1}) = he = h \in H$$

$$\Rightarrow xhx^{-1} \in H$$

Any $x \in G$, any $h \in H \Rightarrow x\,hx^{-1} \in H$

This proves that H is normal in G.

2. **Suppose M and H are normal subgroups of a group G such that $M \cap H = \{e\}$. Then show that every element M commutes with every element H, mh = hm.**

Solution

Let M and H be normal subgroups of group G s.t. $M \cap H = \{e\}$. Let $m \in M$ and $h \in H$ be arbitrary.

To prove that every element of M commutes with every element of H, we have to show that mh = hm.

Consider the element

$$(hm)(mh)^{-1} = (hm)(h^{-1}m^{-1})$$

or $$(hm)(mh)^{-1} = (hmh^{-1})m^{-1} \quad \text{.......(1)}$$

$$= h(mh^{-1}m^{-1}) \quad \text{.......(2)}$$

By property of subgroup,

$$m \in M \Rightarrow m^{-1} \in M \text{ and } h \in H \Rightarrow h^{-1} \in H$$

By property of normal subgroup

$$hmh^{-1} \in M,\ mh^{-1}m^{-1} \in H$$

Using closure property, we get

$$(hmh^{-1})m^{-1} \in M,\ h(mh^{-1}m^{-1}) \in H$$

Using this in (1) and (2) we see that

$$(hm)(mh)^{-1} \in M,\ (hm)(mh)^{-1} \in H$$

$$\Rightarrow (hm)(mh)^{-1} \in M \cap H = \{e\}$$

$$\Rightarrow (hm)(mh)^{-1} = e \Rightarrow hm = mh$$

3. **Suppose H is the only subgroup of finite order n in the group G. Prove that H is a normal subgroup of G.**

Solution

Suppose H is the only subgroup of a group G s.t. o(H) = n(finite)

To prove that H is normal in G

$$o(H) = n \Rightarrow H \text{ is expressible as}$$

$$H = \{h_i : i = 1, 2, \dots, n\} \text{ s.t. } h_i \neq h_j \text{ for } i \neq j$$

Let $x \in G$ be arbitrary

$xHx^{-1} = \{xh_i x^{-1} : h \in H\} = \{xh_i x^{-1} : i = 1, 2, ..., n\}$

To prove xHx^{-1} is a subgroup of G.

Let $a, b \in xHx^{-1}$, then $a = xh_1 x^{-1}$, $b = xh_2 x^{-1}$

where $h_1, h_2 \in H$

$$\begin{aligned} ab^{-1} &= (xh_1x^{-1})(xh_2x^{-1})^{-1} \\ &= xh_1(x^{-1}x)h_2^{-1}x^{-1} = xh_1 . e . h_2^{-1}x^{-1} \\ &= xh_1h_2^{-1}x^{-1} \\ &= xh_3x^{-1}; \quad h_3 = h_1h_2^{-1} \end{aligned}$$

or $ab^{-1} = xh_3x^{-1}$ ....(1)

$h_1, h_2 \in H \Rightarrow h_3 = h_1 h_2^{-1} \in H$, by property of subgroup

$\Rightarrow ab^{-1} \in xHx^{-1}$ by(1)

$\therefore a, b \in xHx^{-1} \Rightarrow ab^{-1} \in xHx^{-1}$

$\therefore xHx^{-1}$ is a subgroup of G.

$o(xHx^{-1}) = n$

For $xh_i x^{-1} = xh_j x^{-1} \Rightarrow h_i = h_j$, by cancellation law. All the elements of xHx^{-1} are distinct. Thus $o(H) = n = o(xHx^{-1})$

By assumption, H is the only subgroup of G s.t. $o(H) = n$. Consequently $xHx^{-1} = H \;\forall\; x \in G$. This proves that H is normal in G.

4. Show that a subgroup H of a group G is normal iff the set $\frac{G}{H}$ of all its left cosets is closed under multiplication.

Solution

Let H be a subgroup of group G.

Also let $\frac{G}{H} = \{aH : a \in G\}$

Step 1: Let H be normal in G so that

$Ha = aH, \;\forall\; a \in G$ ....(1)

To prove $\frac{G}{H}$ is closed under multiplication.

Let $aH, bH \in \frac{G}{H}$ so that $a, b \in G$

$a, b \in G \Rightarrow ab \in G$. For G is a group

$$\Rightarrow (ab)\,H \in \frac{G}{H} \text{.....................} (2)$$

$$\begin{aligned}(aH)\,(bH) &= a(Hb)H = a(bH)H \ \text{ by } (1)\\ &= (ab)\,(HH)\\ &= (ab)H \quad \text{for } HH = H\end{aligned}$$

$$(aH)\,(bH) = (ab)H \in \frac{G}{H} \qquad \text{by } (2)$$

$(aH)\,(bH) \in \frac{G}{H}$ is closed.

Step 2: Let $\frac{G}{H}$ be closed under multiplication of left cosets of H.

To prove H is normal in G.

Let $a \in G$. Then aH and $a^{-1}H$ both are left cosets of H in G. Also $\frac{G}{H}$ is closed under multiplication. Hence $(aH)\,(a^{-1}H) \in \frac{G}{H}$. Since H is a subgroup and so $e \in H$. Then $(ae)\,(a^{-1}e) = aa^{-1} = e$ is an element of $(aH)\,(a^{-1}H)$. Hence e is common to both left cosets H and $(aH)\,(a^{-1}H)$. We know that any two left cosets are either identical or disjoint. Consequently

$$H = (aH)\,(a^{-1}H)\ \forall a \in H$$

$(ah)\,(a^{-1}h_1) \in (aH)\,(a^{-1}H) = H$ and $h, h_1 \in H$

$(aha^{-1})\,h_1 \in H$

$(aha^{-1}h_1)h_1^{-1} \in Hh_1^{-1} = H$

for $h_1 \in H \Rightarrow Hh_1^{-1} = H = h_1^{-1}H$

for $h_1 h_1^{-1} = e$

$\Rightarrow aha^{-1} \in H$

Thus $aha^{-1} \in H\ \forall\, h \in H$ and $\forall a \in G$

This prove that H is normal in G.

5. If G = {a} is a cyclic group of order 8, then find the quotient groups corresponding to the subgroup generated by a^2 and a^4 respectively.

Solution

Let $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$

$H_1 = \{a^2, a^4, a^6, a^8 = e\}$

$H_2 = \{a^4, a^8 = e\}$

G is abelian $\Rightarrow$ the subgroups H_1 and H_2 are normal in G.

$$O'\left(\frac{G}{H_1}\right) = \frac{8}{4} = 2, \quad O'\left(\frac{G}{H_2}\right) = \frac{8}{2} = 4$$

$$\frac{G}{H_1} = \{H_1, H_1a\} \text{ where } H_1a = \{a^3, a^5, a^7, a\}$$

$$H_1a^3 = H_1a$$

$$H_1a^2 = H_1a^4 = H_1a^6 = H_1a^8 = H_1 \text{ etc.,}$$

$$\frac{G}{H_2} = \{H_2, H_2a, H_2a^2, H_2a^3\}$$

6. If N is a normal subgroup of group G, then prove that $\frac{G}{N}$ is abelian iff $\forall$ x, y $\in$ G, $xyx^{-1}y^{-1} \in N$.

Solution

Let N be a normal subgroup of a group G. Let x, y $\in$ G be arbitrary. Then

$$\frac{G}{N} = \{Nx : x \in G\} \quad \text{.......................(1)}$$

is a quotient group w.r.t multiplication defined as

$$(Nx)(Ny) = N(xy), \ \forall x, y \in G \quad \text{.......................(2)}$$

Step 1: Let $\frac{G}{N}$ be abelian, then

$$(Nx)(Ny) = (Ny)(Nx) \quad \text{.......................(3)}$$

Aim: $xyx^{-1}y^{-1} \in N$ ....**(4)**

Using (2) in (3), we find that

$$N(xy) = N(yx) \text{ or } N(xy)(yx)^{-1} = N$$

$\Rightarrow (xy)(yx)^{-1} \in N \Rightarrow xyx^{-1}y^{-1} \in N$

Step 2: Let $xyx^{-1}y^{-1} \in N$ ....**(5)**

Aim: $\frac{G}{N}$ is abelian

$(5) \Rightarrow Nxyx^{-1}y^{-1} = N \Rightarrow N(xy)(yx)^{-1} = N$

$\Rightarrow N(xy) = N(yx) \Rightarrow (Nx)(Ny) = (Ny)(Nx)$

$\Rightarrow \frac{G}{N}$ is abelian.

5. Group Code

5.1 Coding of Binary Information and Error Detection

The basic unit of information called a message, is a finite sequence of characters from a finite alphabet. We shall choose our alphabet as the set B = {0, 1}. Every character or symbol that we want to transmit is now represented as a sequence of m elements from B. That is, every character or symbol is represented in binary form. Our basic unit of information called a word, is a sequence of m 0's and 1's.

The set B is a group under the binary operation +.

+	0	1
0	0	1
1	1	0

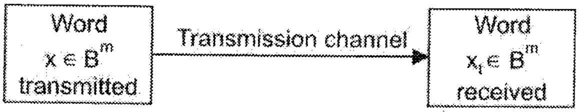
If we think of B as the group Z_2, then + is merely mod 2 addition.

$$B^m = B \times B \times \ldots \times B \text{ (m factors) is a group under the operation } \oplus \text{ defined by}$$

$$(x_1, x_2, \ldots, x_m) \oplus (y_1, y_2, \ldots, y_m)$$

$$= (x_1 + y_1, x_2 + y_2, \ldots, x_m + y_m)$$

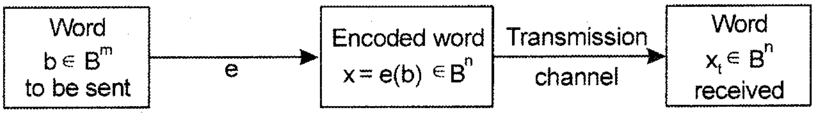
An element in B^m will be written as $(b_1, b_2, \ldots, b_m)$. B^m has 2^m elements. The order of the group B^m is 2^m.



The basic process of sending a word from one point to another point over a transmission channel. An element $x \in B^m$ is sent through the transmission channel and is received as an element $x_t \in B^m$. In actual practice, the transmission channel may suffer disturbances, which are generally called noise, due to weather interference, electrical problems and so, on that may cause a 0 to be received as a 1, or vice versa. This erroneous transmission of digits in a word being sent may give rise to the situation where the word received is different from the word that was sent; that is, $x \neq x_t$. If an error does occur, then x_t could be any element of B^m.

The basic task in the transmission of information is to reduce the likelihood of receiving a word that differs from the word that was sent. This is done as follows. We first choose an integer n > m and a one-to-one function $e : B^m \rightarrow B^n$. The function e is called an (m, n) **encoding function** and we view it as a means of representing every word in B^m as a word in B^n. If $b \in B^m$, then e(b) is called the code word representing b. The additional 0's and 1's can provide the means to detect or correct errors produced in the transmission channel.

We now transmit the code words by means of a transmission channel. Then each code word x = e(b) is received as the word x_t in B^n.



We want an encoding function e to be one-to-one so that different words in B^m will be assigned different code words.

If the transmission channel is noiseless, then $x_t = x$ for all x in B^n. In this case x = e(b) is received for each $b \in B^m$ and since e is a known function, b may be identified. In general, errors in transmission do occur we will say that the code word x = e(b) has been transmitted with k or fewer errors if x and x_t differ in atleast 1 but no more than k positions.

Let $e : B^m \to B^n$ be an (m, n) encoding function we say that e detects k or fewer errors if whenever x = e(b) is transmitted with k or fewer errors, then x_t is not a code word (thus x_t could not be x and therefore could not have been correctly transmitted). If $x \in B^n$, then the number of 1's in x is called the **weight of x** and is denoted by $|x|$.

Example

1. Find the weight of each of the following words in B^5:

a. x = 01000 b. x = 11100 c. x = 00000 d. x = 11111

Solution

a. $|x| = 1$ b. $|x| = 3$ c. $|x| = 0$ d. $|x| = 5$

5.2 Parity Check Code

The following encoding function $e : B^m \to B^{m+1}$ is called the parity (m, m + 1) check code: If $b = b_1, b_2, \ldots, b_m \in B^m$, define

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

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

b_{m+1} is zero if and only if the number of 1's in b is an even number. It then follows that every code word e(b) has even weight. A single error in the transmission of a code word will change the received word to a word of odd weight and therefore can be detected. In the same way we see that any odd number of errors can be detected.

Example

1. Consider the encoding function, let m = 3. Then

$$\left.\begin{array}{l} \mathbf{e(000) = 0000} \\ \mathbf{e(001) = 0011} \\ \mathbf{e(010) = 0101} \\ \mathbf{e(011) = 0110} \\ \mathbf{e(100) = 1001} \\ \mathbf{e(101) = 1010} \\ \mathbf{e(110) = 1100} \\ \mathbf{e(111) = 1111} \end{array}\right\} \textbf{Code words}$$

Solution

Now suppose b = 111 then x = e(b) = 1111. If the transmission channel transmits x as x_t = 1101 then $|x_t| = 3$ and we know that an odd number of errors (atleast one) has occurred.

2. Let m = 2, n = 5 and $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

Determine the group code eH: B2 → B5.

1

PU
April 2010 – 6 M

Solution

The parity check matrix

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

It is of order 5 × 3. Hence the length of the code words is 6 in which last 3 digits are parity check bits. The information digits are 5 – 3 = 2. The matrix H will generate $2^2 = 4$ code words. They are the solutions of $XH^t = 0$.

$$[x_1\, x_2\, x_3\, x_4\, x_5] \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0\,0\,0]$$

$$\text{or} \quad x_1 + x_3 = 0$$

$$x_1 + x_2 + x_4 = 0$$

$$x_2 + x_5 = 0$$

$$\text{i.e.,} \quad x_3 = -x_1$$

$$x_4 = -x_1 - x_2$$

$$x_5 = -x_2$$

as $(-1) \equiv 1 \pmod 2$, the above equations become

$$x_3 = x_1$$

$$x_4 = x_1 + x_2$$

$$x_5 = x_2$$

By giving different combinations of 0 and 1 we get the following code words

x_1	x_2	x_3	x_4	x_5
0	0	0	0	0
0	1	0	1	1
1	0	1	1	0
1	1	1	0	1

Hence the group code

$$C = \{(00000), (01011), (10110), (11101)\}.$$

5.3 Hamming Distance

Let x and y be words in B^m. The hamming distance δ(x, y) between x and y is the weight, $|x \oplus y|$, of $x \oplus y$. Thus the distance between $x = x_1, x_2, \ldots, x_m$ and $y = y_1, y_2, \ldots, y_m$ is the number of values of i such that $x_i \neq y_i$, that is, the number of position in which x and y differ.

Examples

1. Find the distance between x and y:

a. x = 110110, y = 000101 b. x = 001100, y = 010110

Solution

a.

$$\begin{array}{rcl} x & : & 110110 \\ y & : & \underline{000101} \\ x \oplus y & : & 110011 \end{array}$$

so $|x \oplus y| = 4$

b.

$$\begin{array}{rcl} x & : & 001100 \\ y & : & \underline{010110} \\ x \oplus y & : & 011010 \end{array}$$

so $|x \oplus y| = 3$

2. Define Hamming Distance between two words X and Y, state properties of Hamming Distance. Define Minimum distance of a code. Give illustration.

1 PU Oct. 2008 – 6 M

Solution

Let A denote the set of all binary sequence of length n. For X and Y in A the Hamming distance d(X,Y) between X and Y is defined by the number of positions where the code words have the different symbols.

Thus the distance between $x = x_1, x_2 \ldots\ldots x_n$ and $y = y_1, y_2 \ldots\ldots y_n$ is the number of values of i such that $x_i \neq y_i$, i.e., the number of positions in which x and y differs. *Example:* d(1011,1111) = 1 and d(1110000, 0001111) = 7.

Properties of Distance function

Let X, Y, and Z be elements of B^m (set of all binary m tuples). Then

i. d(X,Y) = d(Y, X) (symmetric property)

ii. d(X,Y) ≥ 0 (non negativity)

iii. d(X, Y) = 0 iff X=Y

iv. d(X + a, Y + a)= d(X,Y) i.e. distance between two words is unaltered if we add the same word to both of them.

v. d(X, Y) ≤ d(X, Z) + d(Z, Y).

Minimum Distance of a code

The minimum distance of an encoding function $E : B^m \rightarrow B^m$ is the minimum of the distance betwee all distinct pairs of code words.

i.e., $\min \{d(E(x), E(y)) : X, Y \in B^m\}$.

▶ Theorem

Let x, y and z be elements of B^m. Then

i. $\delta(x, y) = \delta(y, x)$

ii. $\delta(x, y) \geq 0$

iii. $\delta(x, y) = 0$ **if and only if** $x = y$

iv. $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$

Proof

i. $\delta(x, y) = w(x \oplus y)$

$= w(y \oplus x)$ $(\because x + y$ is commutative)

$= \delta(y, x)$

ii. $\delta(x, y) = w(x \oplus y)$

$=$ no. of 1's in $x \oplus y$

≥ 0

iii. **Case 1:** If $x = y$

$x \oplus y = \bar{0}$

$\therefore w(x \oplus y) = w(\bar{0}) = 0$

$\delta(x, y) = 0$ iff $x = y$

Case 2: If $\delta(x, y) = 0$ then $w(x \oplus y) = 0$

$\Rightarrow$ no. of 1's in $x \oplus y = 0$

$\Rightarrow x \oplus y = \bar{0}$

$\Rightarrow$ either $x_i = y_i = 1$ or $x_i = y_i = 0$

$\Rightarrow x = y$

$\therefore \delta(x, y) = 0$ iff $x = y$

iv. $\delta(x, y) = w(x \oplus y)$

$= w(x \oplus \bar{0} \oplus y)$

$= w(x \oplus (z \oplus z) \oplus y)$

$\leq w(x \oplus z) \oplus w(z \oplus y)$ $(\because w(a \oplus b) \leq w(a) + w(b))$

$\leq \delta(x, z) + \delta(z, y)$

The minimum distance of an encoding function $e : B^m \to B^n$ is the minimum of the distance between all distinct pairs of code words; that is,

$$\min\{\delta(e(x), e(y)) / x, y \in B^m\}$$

Example

1. **Consider the following (2, 5) encoding function**

$$\left.\begin{aligned} \mathbf{e(00) = 00000} \\ \mathbf{e(10) = 00111} \\ \mathbf{e(01) = 01110} \\ \mathbf{e(11) = 11111} \end{aligned}\right\} \textbf{Code words}$$

Solution

$e(00) \oplus e(10) = 00111 = 3$

$e(00) \oplus e(01) = 01110 = 3$

$e(00) \oplus e(11) = 11111 = 5$

$e(10) \oplus e(01) = 01001 = 2$

$e(10) \oplus e(11) = 11000 = 2$

$e(01) \oplus e(11) = 10001 = 2$

The minimum distance is 2, as can be checked by computing the minimum of the distances between all six distinct pairs of code words.

▶Theorem

An (m, n) encoding function $e : B^m \to B^n$ can detect k or fewer errors if and only if its minimum distance is atleast $k + 1$.

Example

1. **Consider the (3, 8) encoding function $e : B^3 \to B^8$ defined by**

$$\left.\begin{aligned} \mathbf{e(000) = 00000000} \\ \mathbf{e(001) = 10111000} \\ \mathbf{e(010) = 00101101} \\ \mathbf{e(011) = 10010101} \\ \mathbf{e(100) = 10100100} \\ \mathbf{e(101) = 10001001} \\ \mathbf{e(110) = 00011100} \\ \mathbf{e(111) = 00110001} \end{aligned}\right\} \textbf{Code words}$$

How many errors will e detect?

Solution

$e(000) \oplus e(001) = 4$

$e(000) \oplus e(010) = 4$

$e(000) \oplus e(011) = 4$

$e(000) \oplus e(100) = 3$

$e(000) \oplus e(101) = 3$

$e(000) \oplus e(110) = 3$

$e(000) \oplus e(111) = 3$

$e(001) \oplus e(010) = 4$

$e(001) \oplus e(011) = 4$

$e(001) \oplus e(100) = 3$

$e(001) \oplus e(101) = 3$

$e(001) \oplus e(110) = 3$

$e(001) \oplus e(111) = 3$

$e(010) \oplus e(011) = 4$

$e(010) + e(100) = 3$

$e(010) + e(101) = 3$

$e(010) + e(110) = 3$

$e(010) + e(111) = 3$

$e(011) + e(100) = 3$

$e(011) + e(101) = 3$

$e(011) + e(110) = 3$

$e(011) + e(111) = 3$

$e(100) + e(101) = 4$

$e(100) + e(110) = 4$

$e(100) + e(111) = 4$

$e(101) + e(110) = 4$

$e(101) + e(111) = 4$

$e(110) + e(111) = 4$

The minimum distance of e is 3, as can be checked by computing the minimum of the distance between all 28 distinct pairs of code words. By the above theorem, the code will detect k or fewer errors if and only if its minimum distance is atleast k + 1. Since the minimum distance is 3, we have $3 \geq k + 1$ or $k \leq 2$. Thus the code will detect two or fewer errors.

Generation of Codes by Using Parity Checks

The first complete error detecting and error correcting encoding procedure developed by Hamming in 1950. This procedure has been frequently used in computer system and it is very popular.

Hamming constructed the codes called Hamming codes, by introducing redundant digits called parity digits. In a message that is n digits long m digits (m < n) are used to represent the information part of the message and the remaining k = n – m digits are used for the detection and correction of errors. The later digits are called parity checks.

Hamming's single error detecting codes can be described as follows. The actual message is contained in the first (n – 1) digits of a code word of length n and the last digit position is set to 0 or 1, so as to make the entire message contain an even numbers of 1's. Such an encoding procedure is called an even parity check. An odd parity check can also be used by making the entire message containing an odd number of 1's.

For example, the message {00, 01, 10, 11} become {000, 011, 101, 110} when a single even parity check digit is added. For odd parity check it becomes {001, 010, 100, 111}. Hamming developed an error-correcting method, based on these parity checks, that enabled the detection of the position of erroneous digits. For codes involving check digits, the distance between each pair of code words is not necessarily the same so that the factor determining the error detecting and error correcting capabilities of the code is the minimum of the distance between pair of code words.

The code words of length n in which information is contained in m digits (m < n) and the remaining k = n – m digits are parity checks, can be generated by using a k × n matrix H. This matrix H is called a parity check matrix where elements are zeros and ones. A single error correcting code of length n generated by H will have k parity check bits given by

$$\begin{aligned} 2^k &\geq n+1 \\ 2^k &\geq (m+k)+1 \\ m &\leq 2^k - k - 1 \end{aligned}$$

The number of code words generated by H is $2^m = 2^{n-k}$ and the code generated in this way is called Hamming code.

For example, consider the parity check matrix.

$$H = \begin{bmatrix} 11 & 10 & 100 \\ 11 & 01 & 010 \\ 10 & 11 & 001 \end{bmatrix}$$

It is of order 3 × 7 and it will generate a code words of length 7 in which 3 digits are parity checks. Each code word will have m = 7 – 3 = 4 information bits. Also H will generated $2^4 = 16$ code words.

The parity check matrix H of order k × n can be partitioned into two submatrices Q and I_k as follows:

$$H = (Q|I_k)$$

where I_k is a k × k identity matrix and Q is any arbitrary k × m matrix chosen in such a way that H generate a single error correcting code.

▶ Theorem

Let H be a parity check matrix which consists of k rows and n columns. Then the set of words $X = (x_1, x_2, \ldots, x_n)$ which belong to the following set:

$C = \{X : XH^t = 0 \pmod 2\}$ is a group code under the operation ⊕ (addition modulo 2) where H^t is the transpose of the matrix H.

Proof

We know that C is group code if it is a group under the operation ⊕ (addition modulo 2). Let X, Y ∈ C.

$\Rightarrow X \,.\, H^t = 0$ and $Y \,.\, H^t = 0$

Consider $(X \oplus Y) \,.\, H^t = (X.\, H^t) \oplus (Y \,.\, H^t) = 0$

$\Rightarrow (X \oplus Y) \in C$

Hence C is closed under the operation $\oplus$.

For associativity,

$$\begin{aligned} (X \oplus Y) \oplus Z &= (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n) \oplus (z_1, z_2, \ldots, z_n) \\ &= (x_1 \oplus y_1 \oplus z_1, x_2 \oplus y_2 \oplus z_2, \ldots, x_n \oplus y_n \oplus z_n) \\ X \oplus (Y \oplus Z) &= X \oplus \ (y_1 \oplus z_1, y_2 \oplus z_2, \ldots, y_n \oplus z_n) \\ &= (x_1, x_2, \ldots, x_n) \oplus (y_1 \oplus z_1, y_2 \oplus z_2, \ldots, y_n \oplus z_n) \\ &= (x_1 \oplus y_1 \oplus z_1, x_2 \oplus y_2 \oplus z_2, \ldots, x_n \oplus y_n \oplus z_n) \end{aligned}$$

Hence $X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z$

Observe that $0.H^t = 0$. Hence $0 \in C$. Also $X \oplus 0 = X$. Therefore, identity element is $0 \in C$.

$$X \oplus X = (x_1 \oplus x_1, x_2 \oplus x_2, \ldots, x_n \oplus x_n) = (0, 0, \ldots, 0)$$

Hence every element in C is its own inverse.

We conclude that (C, $\oplus$) is a group and hence a group code.

▶ Theorem

A code can correct all combinations of k or fewer errors if and only if the minimum distance between any two code words is atleast 2k + 1.

Example

1. **The parity check matrix**

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

i. **Find the minimum distance of the code generated by H. How many errors it can detect and correct?**

ii. **Find the number of code words generated by the parity check matrix H, also find all the code words generated.**

Solution

i. **Find the minimum distance of the code generated by H. How many errors it can detect and correct?**

Consider the columns

$$h_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \quad h_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \text{and } h_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

of H.

The sum of these three column is

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

The minimum number of columns that have zero sum is 3. Hence the minimum weight of the code is 3 and thus, the minimum distance is 3. The code can detect k errors or less if its minimum distance is k + 1. Therefore, the code generated by H can detect 2 errors or less. Also it can correct k errors if the minimum distance is 2k + 1. In this case, the code can correct only single error.

Therefore it is a single error correcting code.

ii. Find the number of code words generated by the parity check matrix H, also find all the code words generated.

The parity check matrix

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

It is of order 3 × 6. Hence, the length of the code words is 6 in which last 3 digits are parity check bits. The information digits are 6 – 3 = 3. The matrix H will generate $2^3 = 8$ code words. They are the solutions of $X H^t = 0$

$$(x_1\ x_2\ x_3\ x_4\ x_5\ x_6)\begin{bmatrix}1 & 0 & 1\\1 & 1 & 0\\0 & 1 & 1\\1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix} = (0\ 0\ \ 0)$$

$$\text{or} \quad x_1 + x_2 + x_4 = 0$$

$$x_2 + x_3 + x_5 = 0$$

$$x_1 + x_3 + x_6 = 0$$

$$x_4 = -(x_1 + x_2)$$

$$x_5 = -(x_2 + x_3)$$

$$x_6 = -(x_1 + x_3)$$

As $(-1) \equiv 1 \bmod (2)$, the above equations become

$$x_4 = x_1 + x_2$$

$$x_5 = x_2 + x_3$$

$$x_6 = x_1 + x_3$$

By giving different combinations of 0 and 1, we get the following code words:

x_1	x_2	x_3	x_4	x_5	x_6
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	1	1	0
0	1	1	1	0	1
1	0	0	1	0	1
1	0	1	1	1	0
1	1	0	0	1	1
1	1	1	0	0	0

Hence the code c = {(000000), (001011), (010110), (011101), (100101), (101110), (110011), (111000)}.

3. Write code words generated by H where:

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

1

PU
Oct.2008 – 7 M

What is the minimum weight of the non-zero code word in the above code words? How many errors are detected by this group code?

Solution

i. The parity check matrix

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

It is of order 3 × 7. Hence the length of the code word is 7 in which last 3 digits are parity check bits. The information digits are 7–3= 4. The matrix H will generate 2^4= 16 code words. They are solution of XH^t =0.

$$(x_1x_2x_3x_4x_5x_6x_7) \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (0\ 0\ 0)$$

$$\begin{aligned} \text{or} \quad x_1 + x_2 + x_3 + x_5 &= 0 \\ x_1 + x_2 + x_4 + x_6 &= 0 \\ x_1 + x_3 + x_4 + x_7 &= 0 \\ \text{i.e.,} \quad x_5 &= -(x_1 + x_2 + x_3) \end{aligned}$$

$$x_6 = -(x_1 + x_2 + x_4)$$
$$x_7 = -(x_1 + x_3 + x_4)$$
$$\text{As } (-1) \equiv 1 \text{ mode } (2).$$

The above equation becomes.

$$x_5 = x_1 + x + x_3$$
$$x_6 = x_1 + x_2 + x_4$$
$$x_7 = x_1 + x_3 + x_4$$

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	0	1
0	1	0	0	1	1	0
1	0	0	0	1	1	1
0	0	1	1	1	1	0
0	1	1	1	1	0	1
1	0	0	1	1	0	0
0	1	1	0	0	1	1
1	0	1	0	0	1	0
1	1	0	0	0	0	1
0	1	1	1	0	0	0
1	0	1	1	0	0	1
1	1	0	1	0	1	0
1	1	1	0	1	0	0
1	1	1	1	1	1	1

Hence code C = { (0000000), (0001011), (0010101), (0100110), (1000111), (0011110), (0101101), (1001100), (0110011), (1010010), (1100001), (0111000), (1011001), (1101010), (1110100), (111111111)}

The minimum weight of the nonzero code word in the above code words is 3. Since the minimum no. of columns in H that have zero sum is 3.

i.e.

$$h_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \quad h_2 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \quad h_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \text{ of H.}$$

The sum of the three column is.

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

Hence minimum distance is also 3. We know by thm, the code will detect k or fewer errors iff its minimum distance is 3. We have $3 \geq K + 1$ or $K \leq Z$. Thus code will detect two or fewer errors.

4. Write the code words generated by H, where]

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

1

PU
Oct.2009 – *7 M*

If the received word is (0101000), what is the transmitted word?

Solution

The parity check matrix

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

is of order 3 × 7. Hence the length of code words is 7 in which last 3 digits are parity check bits. The information digits are 7 – 3 = 4. The matrix H will generate $2^4 = 16$ code words. They are solution, of $Hx^t = 0$.

$$\text{i.e.,} \quad \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{aligned} \text{i.e.,} \quad x_1 + x_3 + x_4 + x_5 &= 0 \\ x_1 + x_2 + x_3 + x_6 &= 0 \\ x_2 + x_3 + x_4 + x_7 &= 0 \end{aligned}$$

$$\begin{aligned} \text{or} \quad x_5 &= -(x_1 + x_3 + x_4) \\ x_6 &= -(x_4 + x_2 + x_3) \\ x_7 &= -(x_2 + x_3 + x_4) \end{aligned}$$

As $(-1) \equiv 1 \pmod 2$ the above equations become

$$\begin{aligned} x_5 &= x_1 + x_3 + x_4 \\ x_6 &= x_1 + x_2 + x_3 \\ x_7 &= x_2 + x_3 + x_4 \end{aligned}$$

By giving different combination of 0 and 1 we get the following code words:

x_1	x_2	x_3	x_4	x_5	x_6	x_7
0	0	0	0	0	0	0
0	0	0	1	1	0	1
0	0	1	0	1	1	0
0	0	1	1	0	1	0
0	1	0	0	0	1	1
0	1	0	1	1	1	0
0	1	1	0	1	0	0
0	1	1	1	0	0	1
1	0	0	0	1	1	0
1	0	0	1	0	1	1
1	0	1	0	0	0	1
1	0	1	1	1	0	0
1	1	0	0	1	0	1
1	1	0	1	0	0	0
1	1	1	0	0	1	0
1	1	1	1	1	1	1

Hence the code,

C = {(0000000), (0001101), (0010110), (0011010),(0100011), (0101110), (0110100), (0111001), (1000110), (1001011), (1010001), (1011100), (1100101), (1101000), (1110010), (1111111)}

The decoding table for this code is coset leader

0000000	0001101	0010110	0011010	0100011	0101110	0110100	0111001
1000110	1001011	101000	1011100	1100101	**1101000**	1110010	1111111
1000000	1001101	1010110	1011010	1100011	1101110	1110100	1111001
0000110	0001011	001000	0011100	0100101	**0101000**	0110010	0111111

If the received word is 0101000 then transmitted word is 1101000.

6. Decoding

The process of passing from a message word to its corresponding codeword is referred to as **encoding** and the converse process as **decoding.** After transmission, the received string in Σ^n may not be a codeword or it may be the wrong codeword, but the decoding scheme (or method for decoding) will make the best guess it can for what the message word was.

Optional Decoding

We now consider the problem of optimizing the decoding of a given group encoding, that is we shall be minimizing the probability that an error will be made. We do this with the following two assumptions.

i. That all message words are equally probable and

ii. That the communication is through a binary symmetric channel.

The decoding method is dependent on a decoding table which lists all possible words which can be received. The decoding table is constructed by using Lagrange's theorem. The code words form a subgroup B of the set of all receivable words C.

To construct a table C of all receivable words, the first step in the procedure is to construct a row of elements consisting of all code words in C with the zero code word in its left most position; thus

$$O = c_1\, c_2\, c_3 \ldots . c_2^m$$

where, it is assumed that $c_1 = <0, 0, \ldots, 0>$ for convenience.

In the second step, we select $y_i \in S_n$ but not in C and construct a new row or coset $y_j + c$; for all $1 \leq i \leq 2^m$; that is we add each code word c_i to y_j. We now have the following two rows of the desired table.

$0 = c_1$	c_2	c_3	.....	c_2^m
$y_j + 0$	$y_j + c_2$	$y_j + c_3$	......	$y_j + c_2^m$

This second row, it required is rewritten such that the elements of least weight is in the left most position. This element is called the **coset leader.** Let this coset leader be denoted by y_2 (y_1=0 is the coset leader of the first row); then two rows obtained will be as follows.

$0 = c_1 \quad c_2 \quad c_3 \quad \ldots.. \quad c_2^m$

We now form a third row by selecting some $y_k \in S_n$ which is not in the preceding two rows. This third row is also rewritten with its leftmost element being the word in that row with the least weight. This coset leader is called y_3.

This process is continued until all elements in S_n are accounted for the table.

The complete decoding table has the form

$0 = c_1$	c_2	c_3	.....	c_2^m
y_2	$y_2 + c_2$	$y_2 + c_3$	......	$y_2 + c_2^m$
y_3	$y_3 + c_2$	$y_3 + c_3$	......	$y_3 + c_2^m$
....				
y_2^{n-m}	$y_2^{n-m} + c_2$	$y_2^{n-m} + c_3$	.....	y2 n−m + c_2^m

A received word x can be decoded by first finding x in a row of the decoding table. Let it be the kth row. Then the decoded word c_i is given by $c_i = y_k + x = x + y_k$

where y_k is the coset leader for that row.

For example, let n=3, n =6 and the parity-check matrix be

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

The parity-check positions can be obtained from the equations

$$\left.\begin{aligned} x_4 &= x_1 + x_2 \\ x_5 &= x_1 + x_3 \\ x_6 &= x_1 + x_2 + x_3 \end{aligned}\right\} \text{all mod 2}$$

The single error correcting code generated by H is

C {<0, 0, 0, 0, 0, 0>, <0, 0, 1, 0, 1, 1>, <0, 1, 0, 1, 0, 1>, <0, 1, 1, 1, 1, 0>, <1, 0, 0, 1, 1, 1>, <1, 0, 1, 1, 0, 0>, <1, 1, 0, 0, 1, 0>, <1, 1, 1, 0, 0, 1>}

The decoding table for this code is coset leader

Row of code words→	000000	001011	010101	011110	100111	101100	110010	111001
	100000	101011	110101	111110	000111	001100	010010	011001
	010000	011011	000101	001110	110111	111100	100010	101001
	001000	000011	011101	010110	101111	100100	111010	110001
	000100	001111	010001	011010	100011	101000	110110	111101
	000010	001001	010111	011100	100101	101110	110000	111011
	000001	001010	010100	011111	100110	101101	110011	111000
	000110	001101	010011	011000	100001	101010	110100	111111

If 000011 is received then code word transmitted is taken to be 001011 and If 101110 is received then the code word transmitted is taken to be 101100.

EXERCISE

1. Define: Semi-group, Sub semi-group, Monoid, Sub-monoid, Group, Sub-group, Left coset, Right coset, Normal sub-group.
2. Let < G, $*$ > be a group and a $\in$ G. Let f: G $\to$ G be given by $f(x) = a * x * a^{-1}$ for every x $\in$ G. Prove that f is an isomorphism of G onto G.
3. Let $H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix. Decode the following words relative to a maximum likehood decoding function associated with e_H.
   i. 011001 ii. 101011 iii. 111010
4. What is group code? Write the code words generated by H, where
   $$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$
   What is the minimum weight of non-zero code word in above code words? How many errors are detected by this group code?
5. Show that the Hamming distance H(x, y) satisfies the following properties for all x, y, z $\in S_n$.
   i. $H(x, y) > 0$ ii. $H(x, y) = 0 \Rightarrow x = y$
   iii. $H(x, y) = H(y, x)$ iv. $H(x, y) + H(y, z) > H(x, z)$
6. Let G be a group a $\in$ G. Show that $H = \{a^n \mid n \text{ is an integer}\}$ is a subgroupof G.
7. Show that the set N of natural numbers is a semigroup under the operation x $*$ y = max {x, y}. Is it a monoid?
8. Let $G = \{e, a, a^2, a^3, a^4, a^5\}$ be a group under the operation $a^i * a^j = a^r$, where, $i + j = r \pmod 6$. Show that $f : (G, *) \to (Z_6, +_6)$ defined isomorphism.

Collection of Questions asked in Previous Exams PU

1. Define Hamming Distance between two words X and Y, state properties of Hamming Distance. Define Minimum distance of a code. Give illustration. **[Oct. 2008 – 5M]**
2. Write code words generated by H where: **[Oct. 2008 – 7M]**

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

What is the minimum weight of the non-zero code word in the above code words? How many errors are detected by this group code?

3. Find the left cosets of {[0], [3]} in the group $<Z_6, +_6>$. **[Oct. 2008 – 7M]**
4. Show that $x * y = x^y$ is a binary operation on set of positive integers. Determine whether
   i. * is commutative ii. * is associative **[Oct. 2008 – 7M]**
5. Verify that the totality of all positive rationals forms a group under the composition defined by $a * b = \frac{ab}{2}$. **[Apr. 2009 – 5M]**
6. Write the code words generated by H, where **[Oct. 2009 – 7M]**

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

If the received word is (0101000), what is the transmitted word?

7. Write short note on Hamming code. **[Oct. 2009 – 5M]**
8. Let $(Z_6, +)$ be a group and S = {[0], [3]} be a subgroup. Is a normal subgroup? **[Apr. 2010 – 5M]**
9. Let G = {a, b, c, d} and * is the operation on G defined by Cayley table. Is G an abelian group? **[Apr. 2010 – 7M]**

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

10. Let T be the set of all even integers. Show that the semigroups (Z, +) and (T, +) are isomorphic? **[Apr. 2010 – 7M]**
11. Let m = 2, n = 5 and $H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Determine the group code $e_H: B^2 \to B^5$. **[Apr. 2010 – 6M]**
13. Find the following is a group under multiplication modulo 11 {1, 2, 3, 4, 5, 9}. **[Oct. 2010 – 5M]**
14. Consider the set Q of rational numbers, and let * be the operation on Q defined by: a * b = a + b – ab is (Q, *) a group? **[Oct. 2010 – 7M]**
15. Consider the group G = {0, 1, 2, 3, 4, 5, 6} under addition modulo 7. **[Oct. 2010 – 7M]**
    i. Find the addition table of G. ii. Obtain the left and right coset of G.
16. Define monoid. Show that the set of N natural numbers is a semigroup under the operation x * y = max {x, y} is it monoid? **[Oct. 2010 – 6M]**

Suggestive Readings:

1. Elements of Discrete mathematics: C.L Lieu , Mc Graw Hill
2. Discrete Mathematical Structure with Application to Computer Science: Trembly J.P Mc Graw Hill
3. Operations Research- An Introduction (Eighth Edition); Hamdy A. Taha; Pearson Education, Prentice Hall, Delhi, (2008).
4. Operations Research; A.M. Natarajan, P. Salasubramani, A. Tamilarasi; Pearson Education (Singapore) Pvt. Ltd., Delhi, (2005).
5. Operations Research (Second Edition), Schaum's Outlines; Richard Bronson, GovindasamiNaadimuthu; Tata McGraw Hill Education Private Limited; New Delhi (2010)