Uttar Pradesh Rajarshi Tandon
open University

SBSCS-01

Discrete Mathematics

BLOCK

1

Language of Mathematics & its Application

Course Design Committee

Dr. Ashutosh Gupta — **Chairman**
Director-In-charge,
School of Computer and Information Science,
UPRTOU, Allahabad

Prof. R. S. Yadav — **Member**
Department of Computer Science and Engineering
MNNIT-Allahabad, Allahabad

Ms. Marisha — **Member**
Assistant Professor, Computer Science
School of Sciences, UPRTOU, Allahabad

Mr. Manoj Kumar Balwant — **Member**
Assistant Professor, Computer Science
School of Science, UPRTOU, Allahabad

Course Preparation Committee

Dr. A. K. Pandey — **Author**
Reader, Dept of Mathematics
ECC, Allahabad

Prof. D. P. Chaudhary — **Editor**
Ex-Professor, University of Allahabad
Allahabad, Uttar Pradesh

Dr. Ashutosh Gupta
Director (In-charge), School of Computer and Information Science,
UPRTOU, Allahabad

Ms. Marisha (Coordinator)
Assistant Professor, School of Sciences,
UPRTOU, Allahabad

Printed and Published by Vinay Kumar Registrar, Uttar Pradesh Rajarshi Tandon Open University, 2024.

Printed By : Chandrakala Universal Pvt. Ltd. 42/7 Jawahar Lal Neharu Road, Prayagraj.

Unit - 1

Mathematical Logic

Structure

1.1 Introduction

1.2 Objectives

1.3 Statements

1.4 Logical connectives

1.5 Truth functional rules

1.6 Elementary Logical Operations

- **(1) Conjunction**
- **(2) Disjunction**
- **(3) Negation**
- **(4) Implication**
- **(5) Double implication**

1.7 Tautology

1.8 Tautological equivalence

1.9 Law of Duality

1.10 Functionally Complete Set of Operations

1.11 Sentential form

1.12 Quantifiers

- ***(1) Universal quantifier***
- ***(2) Existential quantifier***

1.13 Negation of a quantifier

1.1 Introduction

This is most basic unit of this block as it introduces the concept of statements, statements, statement variables and the five elementary operations and associated logical connectives. We introduce the well formed statement formulae, tautologies and equivalence of formulae. The law of duality is explained and established. It has got tremendous application in almost every field, social, economy, engineering, technology etc. In computer science concept of logic is a major tool to learn to understand it more clearly. Mathematics has a language of its own like most other sciences, which is very precise and communicates just what is required-neither more nor less. Language basically consists of words and their combinations called 'expression' or 'sentences'. However in Mathematics any expression or statement will not be called a 'sentence'.

1.2 Objectives

After reading this unit we should be able to

1. Understand the concept of statement and statement variables

2. Use elementary operations like Conjunction, Disjunction, Negation, Implication, Double implication

3. Understand statement formulae, tautologies to equivalence of formulae

4. Use law of duality and functionally complete set of connectives

Logic is a field of study that deals with the method of reasoning Logic provides rules by which we can determine whether a given argument or reasoning is valid (correct) or not. Logical reasoning is used in Mathematics to prove theorems. In computer science logic is used to verify the correctness of programs.

1.3 Statements

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

Example1.1. Which of the following are statements?

(a) Indira Gandhi was one of the Prime Ministers of India.
(b) 8 is greater than 10.
(c) $2 + 4 = 6$
(d) Blood is green.
(e) It is raining

(f) The sun will come out tomorrow.

Solution:

(a) is a statement because it is true.
(b) is a statement because it is false.
(c) is a statement because it is true.
(d) is a statement because it is false.
(e) is a statement because the sentence " it is raining" is either true of false but not both a given time.
(f) is a statement since it is either true or false but not both. Although, we would have to wait until tomorrow whether it is true or false.

If a sentence is a question (interrogative type) or a command or not free of ambiguity then the sentence cannot be answered as true or false and therefore such sentences are not statements.

Example1.2: The following are not statements.

(a) Is the number 6 a prime?
(b) $2 - x = 6$
(c) What are you studying?
(d) Open the door.
(e) This statement is false.

Explanation:

(a) is not a statement because it is a question
(b) is not a statement because it is true or false depending on the value of x.
(c) is not a statement because it is a question.
(d) is a command and therefore it is not a statement.
(e) is not a statement because it is not possible to assign a definite true or false value to it. If we assume that sentence (e) is true then it says that statement (e) is false. On the other hand if we assume that sentence (e) is false then it implies that statement (e) is true. Hence it is not a statement.

1.4 Logical connectives:

There are some key words and phrases which are used to form new sentences from given sentences, as for example 'and' 'or', 'not', 'if.... then ...., if and only if' etc. They are called sentential or logical connectives. A Sentence with some logical connective is called a 'Compound sentence' and a sentence without logical connective is called an 'atomic sentence. As for example: A triangle is a plane figure. Water is cold, are atomic sentences. But the followings are the compound sentences.

(a) A triangle is a plane figure and is bounded by three straight lines.
(b) A real number is rational or irrational.
(c) 2013 is not a leap year.
(d) If a triangle is equilateral then it's all angles are equal.
(e) If a triangle is isosceles then two of its angles are equal.

A part of a compound sentence that itself is a sentence is called a component of the sentence – thus the components of the sentence are also sentence.

1.5 Truth functional rules or truth tables:

The rules by which the truth or falsity of a compound sentence is determined from the truth or falsity of its components are called *truth functional rules*. The table giving the truth or falsity of the compound sentence depending upon the truth or falsity of its components is called its *truth table*. We shall say that T or F according as the sentence is true or false respectively.

1.6 Elementary Logical Operations:

The formation of compound sentence from given sentences by using the logical connectives are called *elementary logical operations* which are five in number in accordance with the five logical connectives used. They are: **(1) Conjunction (2) Disjunction (3) Negation (4) Implication (5) Double implication.**

Note: When we form compound sentence by using any of the five logical connectives, it is not necessary that the components of compound sentence should be related in the nation however absurd is permitted. As for example consider the compound sentence 'Ram is a player and the earth revolves about the Sun. Here the components of the compound sentence are not related in the usual sense of conversation.

1. Conjunction : A sentence obtained by conjoining two sentences P,Q by using the connective 'and' is called the *conjunction* of the two sentences and will be denoted by $P \wedge Q$ (read as P and Q).

Example: Let P= U.S.A. sent Apollo 11 to the moon, Q = Russia sent Luna 15 to the moon. Then $P \wedge Q$= U.S.A. sent Apollo 11 and Russia sent Luna 15 to the moon.

Truth functional rule for conjunction:

$P \wedge Q$ is true if and only if both the sentences *P, Q* are true. How this truth functional rule is obtained is a matter of sophisticated logical reasoning and is beyond the purview of the present discussion.

Truth-Table for Conjunction: The following table gives the truth-values of $P \wedge Q$ for all possible truth values of P and *Q*:

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

2. Disjunction: A sentence obtained by joining two sentences *P, Q,* by the connective 'or' is called the *disjunction* of the two sentences and will be denoted by $P \vee Q$ (read as P or *Q*). For example:*P* = Ram is intelligent, *Q* = Ram is hard working, $P \vee Q$ = Ram is intelligent or hard working.

Truth functional rule for disjunction:

$P \vee Q$ is true if at least one of *P, Q* is true, that is, $P \vee Q$ is false only when both *P* and *Q* are false. Truth Table for disjunction:

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

3. Negation: A sentence which has a truth value opposite to that of a sentence *P* is called the negation of *P* and is denoted by $-P$ or ~ P. Negation of an atomic sentence is obtained by using the connective 'not' at proper place.

As for example: If *P*= The water is cold, Then $-P$ =The water is not cold. Negation of $P \wedge Q$ is $(-P) \vee (-Q)$, that is, $-(P \wedge Q) \equiv (-P) \vee (-Q)$. Thus the negation of 'Ram is poor and honest' is 'Ram is not poor or not honest. This can be verified by the following Truth Table:

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

The above table shows that the truth-values of $P\wedge Q$ (as given in the third column) are exactly opposite to those of $(-P)\vee(-Q)$ as given in the last column. The negation of $P\vee Q$ is $(-P)\wedge(-Q)$, that is, $-(P\vee Q)\equiv(-P)\wedge(-Q)$

The negation of 'Mohan or Sohan has failed' is 'neither Mohan nor Sohan has failed' that is, 'Mohan has not failed and Sohan has not failed'.

4. Implication or a conditional sentence:

A conditional sentence obtained by using the connective 'If ….then…' is called an implication. As for example: P = you read, Q = you will pass, By using the connective 'if ……… then' we get 'If you read then you will pass' which can be denoted by 'If P then Q'. It is also written as $P\Rightarrow Q$ (read as P implies Q). In the implication $P\Rightarrow Q$, P is called the *hypothesis* or antecedent and Q is called the *conclusion or consequent.*

The Truth functional rule for implication:

$P\Rightarrow Q$ is false if P is true and Q is false;' otherwise it is true. The Negation of $P\Rightarrow Q$ is $P\wedge(-Q)$ that is, $\sim(P\Rightarrow Q)\equiv P\wedge(-Q)$. This is proved by the following Truth Table:

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

Truth values of $P\Rightarrow Q$ as given in third column are exactly opposite to those of

$P\wedge(-Q)$ as given in the last column. Thus the Negation of the sentence 'If you read then you will pass' is 'You read and you will not pass. Note that 'If you do not read then you will not pass' is not the negation of the given sentence.

5. Double Implication:

A bi-conditional sentence obtained by using the connective 'If and only if'

(briefly written as *iff*) between two sentences *P*, *Q* is called a double implication and is written a 'P *iffQ*'. It is also written as $P \Leftrightarrow Q$ (read as P implies and implied by *Q*). Thus we find that $P \Leftrightarrow Q$ is precisely the conjunction of $P \Rightarrow Q$, $Q \Rightarrow P$, that is $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$. The double implication $P \Leftrightarrow Q$ is true only when both P and Q are true or both are false. This is proved by the following table:

P	*Q*	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$ *i.e.* $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
T	*T*	*T*	*T*	*T*
T	*F*	*F*	*T*	*F*
F	*T*	*T*	*F*	*F*
F	*F*	*T*	*T*	*T*

Note: If *P*= the Sun revolves about the earth, *Q*= The year consists of 400 days. Then '*P* iff Q' or $P \Leftrightarrow Q$ = the Sun revolves about the earth iff the year consists of 400 days – which statement is true though P and Q are both false. The Negation of $P \Leftrightarrow Q$ is $(P \wedge -Q) \vee (Q \wedge -P)$. Thus the Negation of the sentence 'One is good teacher iff one is a good scholar' is 'One is a good teacher and a bad scholar or one is a good scholar and a bad teacher'.

Example 1 : Construct the truth table for $\sim p \vee q$. We must consider all possible

combination of truth values of *p* and *q*. All possible combinations of the truth values of the statements *p* and *q* are listed in the first two columns of the table. The truth values of $\sim p$ are entered in the third column and the truth values of $\sim p \vee q$ are entered in the fourth column.

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

Truth table for $\sim p \vee q$

Example 2 : Construct the truth table for $p\wedge\sim p$.

Since the statement $p\wedge\sim p$ has only one distinct atomic statement. We have to consider 2 possible combinations of truth values. The truth table for $p\wedge\sim p$ is given below.

p	$\sim p$	$p\wedge\sim p$
T	F	F
F	T	F

Truth table for $p \wedge\sim p$

Example 3 : Construct the truth-table for $\sim(p\wedge\sim q)$.

In the first two columns, we list all the variable and the combinations of their truth values. In the third column, we write truth values for $\sim q$. The truth values of $p\wedge\sim q$ are listed in the next column. Finally we obtain the truth values of the proposition $\sim(p\wedge\sim q)$. Thus we have the following truth table:

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

Example 4 : Construct the truth-table for $(p \vee q) \wedge (p\vee r)$.

Here, we have three atomic statements. Therefore we shall require eight rows to list all possible combinations of the truth values of statements p, q and r. Rest of the procedure will be the same as above. We shall proceed in steps and in the final column we will have the truth values of the given statements.

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

T	F	F	T	T	T
F	T	T	T	T	T
F	T	F	T	F	F
F	F	T	F	T	F
F	F	F	F	F	F

Truth table for $(p\vee q)\wedge(p\vee r)$

Example 5 : Prove that the truth values of the following pairs of sentences are the same.

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

(b) $P\vee(Q\wedge R)$ and $(P\vee Q)\wedge(P\vee R)$

(c) $P\wedge(Q\wedge R)$ and $(P\wedge Q)\wedge R$

(d) $P\vee(Q\vee R)$ and $(P\vee Q)\vee R$

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

from columns fifth and eight we find that the truth values of $P\wedge(Q\vee R)$ ad $(P\wedge Q)\vee(P\wedge R)$ are the same in all cases. Solutions of other parts have been left as exercise.

Check your progress

1. Which of the following are statements?

   (a) Is 3 a positive number?
   (b) $x^2 - 5x + 6 = 0$
   (c) There will be snow in December.
   (d) Give me ten rupees.
   (e) Ramesh is poor but honest
   (f) No triangles are squares.

2. Let p be the proposition "Mathematics is easy" and let q be the proposition "five is greater than four." Write in English the proposition, which corresponds to each of the following:(a) $p \wedge q$ (b) $p \vee q$

   (c) $\sim(p \wedge q)$ (d) $\sim p \wedge \sim q$

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

3. Write the negation of each of the following statements:

   (a) $2+7 \leq 13$

   (b) 3 is an odd integer and 8 is an even integer.

   (c) No nice people are dangerous.

4. Let p be the statement "Ravi is rich" and let q be the statement "Ravi is happy." Write the following statements in symbolic form:

   (a) Ravi is poor but happy.
   (b) Ravi is rich or unhappy.
   (c) Ravi is neither rich nor unhappy.
   (d) Ravi is poor or he is both rich and unhappy.

5. Construct the truth-table for the following functions:

   (a) $(p'+q')'$ (b) $(p'q')'$

   (c) $p(p+q)$ (d) $pqr+p'q'r'$

   (e) $(p'+qr)'(pq+q'r)$

6. Given the truth values of p and q as true and those of r and s as false; find the truth values of the following:

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

Answers

1. (c),(e) and (f) are statements.
2. (a) Mathematics is easy and five is greater than four.

   (b) Mathematics is easy or five is greater than four.

   (c) Either Mathematics is not easy or five is not greater than four.

   (d) Mathematics is not easy and five is not greater than four.

   (e) Either Mathematics is easy and five is not greater than four or Mathematics is not easy and five is greater than four.
3. (a) It is false that $2 + 7 \leq 13$

   (b) Either 3 is not an odd integer or 8 is not an even integer.

   (c) Some nice people are dangerous.
4. (a) $\sim p \wedge q$ (b) $p \vee \sim q$

   (c) $\sim p \wedge q$ (d) $\sim p \vee (p \wedge \sim q)$
5. (a) True (b) True

Note: The symbols $\vee$, $\wedge$, $\sim$, $\rightarrow$ and $\leftrightarrow$ defined above are called **connectives.**

Converse, Inverse and Contrapositive of $p \rightarrow q$

Definition: Let $p \rightarrow q$ be any conditional statement. Then,

(a) the converse of $p \rightarrow q$ is statement $q \rightarrow p$.

(b) the inverse of $p \rightarrow q$ is the statement $\sim p \rightarrow \sim q$.

(c) the contrapositive of $p \rightarrow q$ is the statement $\sim q \rightarrow \sim p$.

Example1.15. Write the converse, inverse and contrapositive of the conditional statement "if $2 + 2 = 4$ then I am not the Prime Minister of India."

Let p: $2+2 = 4$ and q: I am not the Prime Minister of India.

Then the given statement can be written as $p \rightarrow q$. Therefore, the converse is $q \rightarrow p$. That is, if I am not the Prime Minister of India then $2+2 = 4$. The inverse of $p \rightarrow q$ is the statement $\sim p \rightarrow \sim q$. That is, if $2+2 \neq 4$ then I am Prime Minister of India.

The contra-positive of $p \rightarrow q$ is the statement $\sim q \rightarrow \sim p$. That is, contra-positive of the given statement is "if I am Prime Minister of India then $2+2 \neq 4$."

Propositional Functions and Propositional Variables

By a propositional variable, we mean a symbol which represents an arbitrary statement (proposition). Thus propositional variable is a variable that can be replaced by a statement. We shall use the symbols $p, q, r, \ldots$ or $p_1, p_2, p_3, \ldots$ to denote propositional variables.

Propositional function is a function or statement which is formed by using propositional variables and connectives. For example, compound statement such as $p \vee q$, $p \wedge q$, $p \to q$ and $p \wedge (q \to r)$ are propositional functions. More formally,

Definition: A propositional function is an expression, which is a combination of propositional variables and connectives. Propositional function are denoted as f $(p, q, r, \ldots)$, where $p, q, r, \ldots$ are the variable used in forming the function f. A propositional function f in n variables $p_1, p_2, p_3, \ldots p_n$ will be denoted as $f(p_1, p_2, p_3, \ldots p_n)$.

(1). $f(p, q) = \sim (p \wedge q)$ is a propositional function in propositional variables p and q

(2). $f(p, q, r) = p \to (p \to r)$ is propositional function in propositional variables p, q and r.

(3). $f(p_1, p_2, p_3) = (p_1 \to p_2) \wedge (p_2 \to p_3)$ is a propositional function in propositional variables p_1, p_2, and p_3. Thus we see that propositional functions are compound statements formed by using finite number of simple (atomic) statements and connectives. We shall often use the word statement for propositional functions.

1.1.7 Tautology

Definition 1: A compound sentence is called a tautology if it is always true irrespective of the truth values of its component parts. i.e. A statement (or propositional function) which is true for all possible truth values of its propositional variables is called a tautology.

Definition 2: A statement which is always false is called a contradiction. A simple method to determine whether a given statement is a tautology is to construct its truth table. If the statement is tautology then the column corresponding to the statement in the truth table contains only T. Similarly a statement is contradiction if the column corresponding to the statement contains only F.

For example $P \vee - P$ is a tautology, since one of P and $-P$ must be true and so $P \vee - P$ is always true. Similarly $(-P \Rightarrow Q) \wedge -Q \Rightarrow P$ is a tautology as proved by the following table.

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

If P $\Rightarrow Q$ is a tautology then we also say $P \Rightarrow Q$ tautologically. Thus in the preceding example we can say that $(-P \Rightarrow Q) \wedge - Q \Rightarrow P$ tautologically.

Note: $P \Rightarrow Q$ cannot be a tautology if both P and Q are atomic sentence.

1.1.8 Tautological equivalence

Two sentence P and Q are said to be *tautologically equivalent* if $P \Rightarrow Q$ tautologically. And also $Q \Rightarrow P$ tautological equivalence if $P \Rightarrow Q$ tautologically, and also $Q \Rightarrow P$ tautologically. P and Q are tautologically equivalent may be written as $P \equiv Q$. It is clear that two compound sentence P and Q are tautologically equivalent if they have the same truth values in all the cases. i.e. Two statement p and q are said to be logically equivalent or equal if they have identical truth values.

One method to determine whether any two statements are equal is to construct a column for each statement in a truth table and compare these to see if they are identical.

For example $P \Rightarrow Q$ is tautologically equivalent to $- Q \Rightarrow - P$ as proved by the following table:

P	Q	$P \Rightarrow Q$	$-Q$	$-P$	$-Q \Rightarrow -P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

We find that the truth values of $P \Rightarrow Q$ and $- Q \Rightarrow - P$ are the same in all the cases.
Hence $[P \Rightarrow Q] \Rightarrow [-Q \Rightarrow - P]$ and $[- Q \Rightarrow -P \Rightarrow [P \Rightarrow Q]$ are both tautologies.

The sentence $-Q\Rightarrow -P$ is called the contra-positive of the sentence $P\Rightarrow Q$. Hence very often to prove $P\Rightarrow Q$ we prove $-Q\Rightarrow -P$.

Note: If $P\Rightarrow Q$ is a tautology, hen if P is true then Q must be true, since the implication is always true except when P is true and Q false.

Example 1 : Show that each of the following is a tautology

(a) $[p\wedge(p\to q)]\to q$

(b) $[(p\to q)\wedge(q\to r)]\to(p\to r)$

(a) We shall construct truth-table for the function $p\wedge(p\to q)\to q$

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

Truth table for $p\wedge(p\to q)]\to q$

Since the column for $[p\wedge p\to q)]\to q$ contains only T, it is a tautology

(c) Here we construct the truth-table for $[(p\to q)\wedge(q\to r)]\to p\to r)]$

p	q	r	$p\to q$	$q\to r$	$p\to r$	$(p\to r)\wedge(q\to r)$	$[p\to r)\wedge[q\to r)]\to p\to r)$
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

Truth table for $[(p\to r)\wedge(q\to r)]\to(p\to r)$

Since the last column corresponding to $[(p \to q) \wedge (q \to r)] \to (p \to r)$ contains only T, it is a tautology.

Example 2 : Show that the statement $p \wedge \sim p$ is a contradiction. Consider the truth table for $p \wedge \sim p$.

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

Truth table for $p \wedge \sim p$

It follows from the table that $p \wedge \sim p$ is a contradiction.

Example 3 : Prove that $p \to q = \sim p \vee q$.

We shall construct truth table for statement $p \to q$ and $\sim p \vee q$.

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

Truth table for $p \to q$ and $\sim p \vee q$

We observe that the truth values in the columns for $p \to q$ and $\sim p \vee q$ are identical. Hence $p \to q = \sim p \vee q$.

Example 4 : Show that the statement $(p \wedge \sim p) \vee q$ and q are equal.

Consider the truth table for given statement.

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

F	*F*	*T*	*F*	*F*

Truth table for $(p \wedge \sim p) \vee q$ and q

From the truth table we see that columns for $(p \wedge \sim p) \vee q$ and q are identical. Hence they are equal.

Example 5 : Show that two statements p and q are equivalent if bi-conditional statement $p \leftrightarrow q$ is a tautology. From the definition of bi-conditional statement we know that $p \leftrightarrow q$ is true whenever both p and q have the same truth values. Thus $p = q$ if $p \leftrightarrow q$ is a tautology.

Note. (1) Some authors have used the symbol '$\Leftrightarrow$' to denote equivalent or equal statements and symbol $\leftrightarrow$ is used for bi-conditional statement. From Example 1.20, we have $p \Leftrightarrow q$ if $p \leftrightarrow q$ is tautology.

(2) Two equivalent statements may contain different variables as is clear from Example 1.19 above.

Example 6 : Show that $p \to (q \to r) = (p \wedge q) \to r$

Consider the following truth table.

p	q	r	$q \to r$	$p \wedge q$	$p \to (q \to r)$	$(p \wedge q) \to r$
T	*T*	*T*	*T*	*T*	*T*	*T*
T	*T*	*F*	*F*	*T*	*F*	*F*
T	*F*	*T*	*T*	*F*	*T*	*T*
T	*F*	*F*	*T*	*F*	*T*	*T*
F	*T*	*T*	*T*	*F*	*T*	*T*
F	*T*	*F*	*F*	*F*	*T*	*T*
F	*F*	*T*	*T*	*F*	*T*	*T*
F	*F*	*F*	*T*	*F*	*T*	*T*

Truth table for $p \to (q \to r) \& (p \wedge q) \to r$

We see that columns for $p \to (q \to r)$ and $(p \wedge q) \to r$ are identical hence given statement are equal.

PEPE-103/PEPE-144/ETH-108

Check your progress

(1) By constructing truth tables, show that the following are tautologies:

(a) $(P \wedge Q) \Rightarrow P$
(b) $(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$
(c) $(P \Leftrightarrow Q) \wedge (Q \wedge R) \Rightarrow (P \Leftrightarrow R)$
(d) $(P \vee Q) \wedge -Q \Rightarrow P$
(e) $[P \Rightarrow Q] \Leftrightarrow [-P \vee Q]$

(2) Show that the following are tautological equivalences:

(a) $(P \Leftrightarrow Q) \equiv (P \Rightarrow Q) \wedge (-P \Rightarrow -Q)$
(b) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
(c) $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
(d) $-(P \wedge Q) \equiv (-P) \vee (-Q)$
(e) $-(P \vee Q) \equiv (-P) \wedge (-Q)$
(f) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge (P \wedge R)$
(g) $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$

The following theorem contains various laws satisfied by propositions. We shall use these laws for simplification of propositions.

Theorem 1: The following laws are satisfied by statements:

1. Commutative laws:

(a) $p \vee q = q \vee p$. (b) $p \wedge q = q \wedge p$.

2. Associative laws:

(a) $p \vee (q \vee r) = (p \vee q) \vee r$ (b) $p \wedge (q \wedge r) = (p \wedge q) \wedge r$

3. Distributive laws:

(a) $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$ (b) $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$

4. Idempotent laws:

(a) $p \vee q = p$ (b) $p \wedge p = p$

5. Laws of absorption:

(a) $p \vee (p \wedge q) = p$ (b) $p \wedge (p \vee q) = p$

6. Involution laws:

(a) $\sim(\sim p) = p$

7. Complement laws:

(a) $p \vee \sim p = T$ (b) $p \wedge \sim p = F$

8.De Morgan's laws:

(a) $\sim(p \vee q) = \sim p \wedge \sim q$ (b) $\sim(p \wedge q) = \sim p \vee \sim q$

9. Operation with *T*

(a) $p \vee T = T$ (b) $p \wedge T = p$

10. **Operation with *F***

(a) $F \vee p = p$ (b) $F \wedge p = F$

Here *T* and *F* denote statements, which are tautology and contradiction respectively.

Proof: We shall prove 3(a) and 8(a). The remaining laws can be proved exactly in the same way by constructing truth tables.

To prove 3(a), consider the following truth-table

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

Since columns for $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are identical they are equal.

To prove 8(a), consider the following truth table:

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

T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

It follows from the table that $\sim(p \vee q) = \sim p \wedge \sim q$.

Theorem 2: Show that (a) $p \to q = \sim p \vee q$, (b) $p \leftrightarrow q = (p \to q) \wedge = (q \to p)$

Proof: Using the definitions of $\to$ and $\leftrightarrow$ we have,

p	q	$\sim p$	$p \to q$	$q \to p$	$p \leftrightarrow q$	$\sim p \vee q$	$(p \to q) \wedge = (q \to p)$
T	T	F	T	T	T	T	T
T	F	F	F	T	F	F	F
F	T	T	T	F	F	T	F
F	F	T	T	T	T	T	T

Since the truth values in columns (4) and (7) are identical, we have (a), Similarly, since the truth values in columns (6) and (8) are identical, we have (b).

Theorem 3 : Show that (a) $\sim(p \to q) = p \wedge \sim q$, (b) $\sim(p \leftrightarrow q) = p \leftrightarrow \sim q$

Proof : Using the definitions of $\to$ and $\leftrightarrow$, we construct the truth table

p	q	$\sim p$	$\sim q$	$p \to q$	$\sim(p \to q)$	$p \wedge \sim q$	$p \leftrightarrow q$	$\sim(p \leftrightarrow q)$	$p \leftrightarrow \sim q$
T	T	F	F	T	F	F	T	F	F
T	F	F	T	F	T	T	F	T	T
F	T	T	F	T	F	F	F	T	T
F	F	T	T	T	F	F	T	F	F

$\sim(p \leftrightarrow q) = p \leftrightarrow \sim q$ have identical truth values, so $\sim(p \leftrightarrow q) = p \leftrightarrow \sim q$

Example 7 : Prove that $\sim(p \wedge q) \to (\sim p \vee (\sim p \vee q)) = \sim p \vee q$, without constructing truth table.

Solution : We shall use theorems 1 and 2.

L.H.S = $\sim(p \wedge q) \rightarrow (\sim p \vee (\sim p \vee q))$

$= (p \wedge q) \vee (\sim p \vee (\sim p \vee q))$	Since $p \rightarrow q = \sim p \vee q$
$= (p \wedge q) \vee ((\sim p \vee \sim p) \vee q)$	by associative law
$= (p \wedge q) \vee (\sim p \wedge q)$	by idempotent law
$= ((p \wedge q) \vee \sim p) \vee q$	by associative law
$= (\sim p \vee (p \wedge q)) \vee q$	by commutative law
$= ((\sim p \vee p) \wedge (\sim p \vee q)) \vee q$	by distributive law
$= (T \wedge (\sim p \vee q)) \vee q$	by complement law
$= (\sim p \vee q) \vee q$	by 9(b) of Theorem 1
$= \sim p \vee (q \vee q)$	by associative law
$= \sim p \vee q$	by idempotent law
=R.H.S.	

Check your progress

1. Prove that each of the following is a tautology:

(a) $p \rightarrow p$ (b) $p \wedge q \rightarrow p$

(c) $p \rightarrow (p \vee q)$ (d) $(p \wedge (p \rightarrow q)) \rightarrow q$

(e) $(p \rightarrow q) \rightarrow [(p \vee (q \wedge r)) \leftrightarrow q \wedge (p \vee r)]$

2. Write in words the converse, inverse, contra positive and negation of the implication "if she works then she will earn money."

3. Construct truth tables to determine whether each of the following is tautology or a contradiction:

(a) $p \wedge \sim p$ (b) $p \rightarrow (q \rightarrow p)$

(c) $p \rightarrow q \wedge p$ (d) $q \vee (\sim q \wedge p)$

4. Prove the following:

(a) $p \vee q = q \vee p$ (b) $p \wedge (q \wedge r) = (p \vee q) \wedge r$

(c) $p\wedge(q\vee r)=(p\wedge q)\vee(p\wedge r$ (d) $p\vee p=p$

(e) $\sim(p\wedge q)=\sim p\vee\sim q$ (f) $\sim(p\leftrightarrow q)=\sim p\leftrightarrow q$

5. Write in English the negation of each of the following:

(a) The weather is bad and I will not go to work.

(b) I grow fat only if I eat too much.

6. Show the following equivalences:

(a) $p\to(q\to q)\Leftrightarrow\sim p\to(p\to q)$

(b) $\sim(p\leftrightarrow q)\Leftrightarrow(p\wedge\sim q)\vee(\sim p\wedge q)$

7. We define $p\Rightarrow q$ if and only if $p\to q$ is tautology. Prove the following:

(a) $p\to q\Rightarrow p\to(p\wedge q)$

(b) $(p\to q)\to q\Rightarrow p\vee q$

8. Prove that for any propositions p and q.

(a) $p\vee T=T$

(b) $p\wedge F=F$

(c) $\{(p\vee\sim q)\wedge(\sim p\vee\sim q)\}\vee q=T$

Answers

2. The converse of the statement is "if she earns money then the she works." The inverse is "if she does not work then she will not earn money." The contra-positive is "if she does not earn money then she does not work" The negation of the statement is "she works and she will not earn money."

3. (a) Contradiction

   (b) Tautology

   (c) Neither tautology nor contradiction

   (d) Neither tautology nor contradiction

5. (a) The weather is bad but I will go to work.

   (b) I grow fat and (although) I don't eat too much.

1.9. Law of Duality

In this section, we consider only those statements which contain the connectives $\wedge$, $\vee$ and $\sim$ only.

Definition: Two statement p and p^* are said to be duals of each other if either one can be obtained from the other by replacing $\wedge$ by $\vee$, $\vee$ by $\wedge$, T by F and F by T.

It is obvious from the definition that dual of a statement is the statement itself. We now state (without proof) the principle of duality.

Principle of Duality

It states that if any two statements are equal then their duals are also equal.

Example.8: Prove the following:

(a) $\sim(p \wedge q) = \sim p \vee \sim q$ (b) $\sim(p \vee q) = \sim p \wedge \sim q$

Solution: We shall only prove (a). The result stated in (b) will follow by principle of duality.

To prove (a), consider the following table:

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

From the table, it follows that $\sim(p \wedge q) = \sim p \vee \sim q$

1.10. Functionally Complete Set of Operations

Definition: A set of operations (connectives) is said to be functionally complete if every statement can be expressed entirely in terms of the operations in the set.

It is assumed that such a functionally complete set does not contain any connective which can be expressed in terms of the order connectives in the set.

Recall that so far, we have defined the connectives $\wedge, \vee, \sim, \rightarrow$ and $\leftrightarrow$. We know that $p \rightarrow q$ is equal to $\sim p \vee q$. Thus it is possible to replace each occurrence of $\rightarrow$ in any statement with an equivalent expression involving ~ and $\vee$. Similarly, we know that: $p \leftrightarrow q = (p \rightarrow q) \wedge (q \rightarrow p) = (\sim p \vee q) \wedge (\sim q \vee p)$

Thus the symbol $\leftrightarrow$ can be replaced by connectives $\vee, \wedge$ and ~,

By De Morgan's law, we know that $\sim (p \wedge q) = \sim p \vee \sim q$

Or, $p \wedge q = \sim (\sim p \vee \sim q)$. Similary, we have, $p \vee q = \sim (\sim p \wedge \sim q)$

Thus it is possible to replace $\wedge$ in any statement by connectives ~and $\vee$. Hence any statement can be expressed in an equivalent statement containing ~ and $\wedge$ only. This shows that $\{\wedge, \sim\}$ is functionally complete set of operations. Similarly, any statement can be expressed in an equivalent statement containing $\vee$ and ~only. Thus $\{\vee, \sim\}$ is also functionally complete set.

Example 9 : Write the statement $(p \vee \sim q) \rightarrow (p \wedge r)$ in terms of $\vee$ and ~only.

Solution: We know that $p \rightarrow q = \sim p \vee q$

Therefore, $(p \vee \sim q) \rightarrow (p \wedge r) \;=\; \sim (p \vee \sim q) \vee (p \wedge r)$

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

because $p \wedge r = \sim (\sim p \vee \sim r)$

Example 10 : Express $p \wedge (q \rightarrow r)$ in terms of $\wedge$ and ~.

Solution: $p \wedge (q \leftrightarrow r) = p \wedge [(q \rightarrow r) \wedge (r \rightarrow q)]$

$$= p \wedge [(\sim q \vee r) \wedge (\sim r \vee q]$$

$$= p \wedge \sim (q \wedge \sim r) \wedge \sim (r \wedge \sim q] \quad (\because p \vee q = \sim (\sim p \wedge \sim q))$$

Example 11 : Show that $\{\rightarrow, \sim\}$ is functionally complete set.

Solution : We know that $\{\vee, \sim\}$ is functionally complete set. Thus any statement can be expressed in an equivalent statement containing $\vee$ and ~, Since

$$p \vee q = (\sim p) \rightarrow q$$

Therefore we can replace the connective $\vee$ in any statement by ~ and $\rightarrow$. Hence the statement can be expressed in terms of $\rightarrow$ and ~. Thus $\{\rightarrow, \sim\}$ is functionally complete.

Example 12 : Show that $\{\wedge, \vee\}$ is not functionally complete.

Solution: Since the connective '~' can not be expressed entirely in terms of $\vee$&$\wedge$, therefore any statement containing ~ can not be expressed in an equivalent statement containing $\wedge$&$\vee$ only. Hence $\{\wedge, \vee\}$ is not functionally complete.

Connectives ↓ and ↑

We now introduce two more connectives, which have useful application in the design of computers. They are NAND and NOR. The connective NAND is denoted by the symbol ↑ and is defined by the following truth table:

p	q	$p \uparrow q$
T	T	F
T	F	T
F	T	T
F	F	T

Truth-table for $p \uparrow q$

The connective NOR is denoted by the symbol ↓ and is defined by the following table:

p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

Truth-table for $p \downarrow q$

For any two statements p and q, it can be shown by constructing truth tables that,

$$p \uparrow q = \sim(p \wedge q) \text{ and}$$

$$p \downarrow q = \sim(p \vee q).$$

Theorem 1 : Show that each of the sets $\{\downarrow\}$ and $\{\uparrow\}$ is functionally complete.

Proof: We know that the sets of connectives $\{\vee, \sim\}$ and $\{\wedge, \sim\}$ are functionally complete. Therefore, in order to show that $\{\downarrow\}$ and $\{\uparrow\}$ are functionally complete, it is sufficient to show that the connective $\wedge, \vee$ and $\sim$ can be expressed either in terms of $\uparrow$ alone or in terms of $\downarrow$ alone. From the definition of $\uparrow$, we see that

$$p \uparrow p = \sim(p \wedge p)$$

$$= \sim p \qquad \ldots\ldots\ldots\ldots(1)$$

Again,

$$(p \uparrow q) \uparrow (p \uparrow q) = \sim(p \uparrow q) \text{ since } p \uparrow q = \sim p \text{ by } (1)$$

$$= \sim(\sim(p \wedge p))$$

$$= p \vee q \qquad \ldots\ldots\ldots\ldots(2)$$

Finally,

$$(p \uparrow p) \uparrow (q \uparrow q) = (\sim p) \uparrow (\sim q)$$

$$= \sim(\sim p \wedge \sim q)$$

$$= p \vee q \qquad \ldots\ldots\ldots\ldots(3)$$

Thus $\sim$, $\vee$ and $\wedge$ have been expressed in term of $\uparrow$ alone. Hence $\{\uparrow\}$ is functionally complete. In a similar manner, we have

$$(p \downarrow p) = \sim(p \vee p)$$

$$= \sim p,$$

$$(p \downarrow q) \downarrow (p \uparrow q) = p \vee q$$

and $(p \downarrow p) \downarrow (q \uparrow q) = p \wedge q$

Thus $\{\downarrow\}$ is functionally complete.

1.11 Sentential form

Consider the following expressions or statements: (1) x is mortal (2) x is a fraction

They are not sentences, since we do not know their truth values. If we take x to be a number in (1) and x to be a man in (2), then these two statements (1), (2) become meaningless and hence they are not sentences. But if we restrict x in (1) to men and in (2) to numbers, then these statements will be sentences either true or false. Here x will be called a variable. Such statements which contain variables like x which are not specified are called open sentences or sentential from. Similarly expressions containing pronouns, as for example 'He is prime minister of India', 'It is a prime number' are open sentences, since we do not know their truth value without additional information specifying the unknown pronouns which behave like variables. The open sentence 'x is mortal' will be denoted by $P(x)$.

1.12. Quantifiers

In the discussion of logic, some very important statements contain quantifiers. The following are examples of statements which contain quantifiers:

(1) Some people are honest.

(2) No woman is a player.

(3) All Americans are crazy.

The words *some, no* and all are known as quantifiers. From quantifiers, we know "how many" of a certain set of things is being considered.

1.12 (a) Universal Quantifier

Let p be a statement. We define the symbol $\forall_x p$ to mean that for every value of x in the given set, the statement p is true. The symbol $\forall$ is called the universal quantifier. $\forall$ can also be read as 'for all' , ' for every' or 'for any.'

ILLustration: The statement "for all natural numbers, $n + 4 > 3$" can be expressed as $\forall_x p$, where x belongs to the set N of natural numbers and p is the statement '$n + 4 > 3$.'

1.12 (b) Existential Quantifier

Let p be a statement. We define the symbol $\exists_x p$ to mean that for one or more elements x of a certain set, the proposition p is true. The symbol $\exists$ is called existential quantifier and is usually read as "these exists" or "for at least one "for some".

Illustration : (1) The statement "there exists a number x such that $x^2 - 4x = 16$" may be written as $\exists_x (x^2 - 4x = 16)$

(2) The statement $\exists_x (n + 4 < 7)$, where n is in the set of natural numbers is true since there exists a natural number, namely I, such that $n + 4 < 7$ is true.

1.13 Negation of Quantifiers

It is important to know how the negations of statements having quantifiers are formed. Consider the statement"All Americans are crazy"

The negation of this statement would be

"It is false that all Americans are crazy" or equivalently,

"There exists at least one American who is not crazy."

In general, we have $\sim(\exists_x p) = \forall_x(\sim p)$ and $\sim(\forall_x p) = \exists_x(\sim p)$

Example: The function *f* is said to approach the limit *l* near *a* if (1) $\forall \in > 0$, $\exists \delta > 0$ such that $\forall x\ 0 < |x - a| < \delta \Rightarrow |f(x) - l| < \in$.

Putting *P*(*x*): $0 < |x - a| < \delta \Rightarrow |f(x) - l| < \in$. It can be written as $\forall \in > 0\ \exists \delta > 0$ such that $\forall(x)$ *P*(*x*). *Hence the negation of the above definition will be :*

The function *f* does not approach *l* at a if $\exists \in > 0$ s.t. $\forall \delta > 0\ \exists x(\sim P(x))$.

That is, if there exists some $\in > 0$, such that *for every* $\delta > 0$, there exists some *x* for which $0 < |x - a| < \delta$ and $|f(x) - l| \nless \in$.

Example: Write the negation of 'No teachers are wise'. Putting *P(x)*: x is wise (*x* is a teacher), the symbolic form of the above sentence is $\forall x$ (*x* is a teacher) *x* is not wise or $\forall x\ (\sim P(x))$ (*x* is a teacher). Hence its negation will be $\exists x P(x)$ that is, there exists a teacher *x* who is wise or' Some teachers are wise'.

Check your progress

(3). Given *P* is true, *Q* is false and *R* is true, find, find the truth values of:

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

(b) $(P \Rightarrow Q) \Rightarrow (P \wedge - Q)$

(c) $[(P \wedge Q) \wedge - R] \Rightarrow (Q \Rightarrow P)$ [Ans. (a) *T*, (b) *T*, (c) *T*]

(4). Write the Negations of the following

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

(b) $P \wedge (Q \Rightarrow -R)$,

(c) $P \Rightarrow (Q \Rightarrow R)$.

(d) $P \wedge - Q \Leftrightarrow R$,

(e) $\forall^x (x \neq 1, x \neq 2)$,

(f) $\exists^x(x^2<0)$

(g) $\forall x(x\neq 0) \Rightarrow (x^2> 0)$,

(h) $\exists x(x^2=1$ and $x^2-2x+3= 0)$

(i) Every Indian is honest.

(j) If there is a will then there is a way.

(5). State if the following are sentence, giving reasons of your answer.

(a) Do you think you will pass in the examination?

(b) Mathematics is black .

(c) Walk right in.

(d) He is a President of India.

(e) 2/5 is a integer .

(f) If you pass in the examination, then the sun will revolve about the earth.

(g) Oh! How sand he is.

(6). By constructing Truth-tables shows that the following are tautologies:

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

(b) $(P\vee Q) \wedge - Q\Rightarrow P$

(c) $[(P\Rightarrow Q) \wedge (Q\Rightarrow R)] \Rightarrow (P\Rightarrow R)$,

(d) $(- P\Rightarrow Q) \wedge - Q) \Rightarrow P$

(7). Prove the following tautological equivalences:

(a) $(P\Rightarrow Q) \vee (P\Rightarrow R)\equiv P \Rightarrow Q\vee R$.

(b) $(P\Rightarrow R)\wedge(Q \Rightarrow R)\equiv P \vee Q \Rightarrow R$

(c) $(P \Rightarrow Q) \wedge (P \Rightarrow R) \equiv P \Rightarrow Q \wedge R$,

(d) $(P \Rightarrow R) \vee (Q \Rightarrow R) \equiv P \wedge Q \Rightarrow R$.

(8). Prove that the following are tautologies

(a) $[(P \Rightarrow Q) \wedge (R \Rightarrow S)] \Rightarrow (P \wedge R \Rightarrow Q \wedge S)$.

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

(9) Find the dual of the following:

(a) $(p \vee q) \wedge r$ (b) $(p \wedge q) \vee T$

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

(10) Form the negation of each of the following:

(a) "For all positive integers x, we have $x+2>8$"

(b) "All men are honest or some man is a thief."

(c) "There is at least one person who is happy all the time."

(d) "The sum of any two integers is an even integer."

(e) At least one student does not live in the dormitories.

Solution: (9) (a) Interchanging $\vee$ and $\wedge$, we have, dual as $(p \wedge q) \vee r$.

(b) Dual is $(p \vee q) \wedge F$

(10) Dual is Negation of the statement are:

(a) There exists a positive integer x such that $x+2>8$.

(b) There exists a man who is not honest and all men are not thief.

(c) No person is happy all the time.

(d) There exists two integers such that their sum is not an even integer.

(e) All students live in the dormitories.

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983) Topic in Algebra, Vikas publishing house Pvt. Ltd.

Unit - 2

Arguments

Structure

2.1. Introduction

The main problem in logic is the investigation of the process of reasoning. In Mathematics, a certain set of statements (propositions) is assumed and from this set, other statements are derived by logical reasoning. In this section, we shall investigate those processes which can be accepted as valid in the derivation of a statement from the given set of statements. The given set of statements is called premises or hypothesis and the statement derived from the given statement is called conclusion.

2.2. Objectives

After reading this unit we should be able to

1. Understand the concept of Argument
2. Use Rule of Detachment
3. Understand Invalidity of an Argument
4. Use IndirectMethod of proof
5. Use Proof by Counter-Example

2.3. Argument

Definition: An argument is a process by which a conclusion is formed from a given set of statements called premises.

An argument is said to be **valid argument** if and only if the conjunction of the premises implies the conclusion. That is, the argument which yields a conclusion r from the premises p_1, p_2, p_3------,p_n is valid if and only if the statement is tautology.

An argument which is not valid is called a fallacy. An argument which is derived from the premises or hypothesis $p_1, p_2, -----, p_n$ is written as

$$\begin{array}{c} p_1 \\ p_2 \\ p_3 \\ - \\ - \\ p_n \\ \hline q \end{array}$$

That is, the premise or premises will be listed first and the conclusion will be written beneath a horizontal line.

Example: Prove that the following argument is valid:

$$\begin{array}{c} P \\ p \to q \\ \hline q \end{array}$$

Solution: Here p and $p \to q$ are two premises and q is the conclusion. To show that the argument is valid we show that conjunction of the given premises implies the conclusion is a tautology. That is, we show $[p \wedge (p \to q)] \to q$ is a tautology by constructing truth table.

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*

It follows from the truth table that $[p \wedge (p \to q)] \to q$ is a tautology. Thus the argument is valid.

2.4. Rule of Detachment or Modus Ponens

The valid argument

$$\begin{array}{c} P \\ \underline{p \to q} \\ q \end{array}$$

is called rule of detachment. Rule of detachment is also known as **modus ponens**.

Law of Syllogism The argument

$$\begin{array}{c} p \to q \\ q \to r \\ \hline p \to r \end{array}$$

is valid argument and is known as the **law of syllogism.**

Example: The validity of the law of syllogism is proved by constructing truth table for $[(p \to q) \wedge (q \to r)] \to (p \to r)$.

p	q	r	$p \to q$	$q \to r$	$p \to r$	$(p \to q) \wedge (q \to r)$	$[(p \to q) \wedge (q \to r)] \to (p \to r)$
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

Truth table for $[(p \to q) \wedge (q \to r)] \to (p \to r)$

It follows from the truth table that the law of syllogism is a valid argument.

Given an argument, there are, in general, three methods to check the validity of the argument. These methods are given below.

1. Validity using Truth Table

In this method, we construct a truth table as follows: $p_1 p_2 ----, p_n$ be all the premise and let q be the conclusion in the given argument. We construct truth table for the statement $(p_1 \wedge p_2 \wedge ---- \wedge p_n) \rightarrow q$

If we have all *T*s in the column of this statement then the statement is tautology and so the argument used is valid otherwise the argument is not valid.

2. Validity using Simplification Methods

In this method, we convert all the implication statement $p \rightarrow q$ to the equivalent statement $\sim p \vee q$ in the argument involved and then we simplify the resulting statement using rules of statement (Theorem 1 of § 1.9). If the statement

$$(p_1 \wedge p_2 \wedge p_3 \wedge ---- \wedge p_n) \rightarrow q$$

can be reduced to *T*, then we say that the argument is valid.

3. Validity using Rules of Inference

In this method, we reduce the given argument to a series of arguments each of which is known to be valid. Two of the most frequently used rules of inference (i.e. valid argument) are the rule of detachment and the law of syllogism.

Example: Show that the following argument is valid

$$\begin{array}{l} p \\ p \rightarrow q \\ \underline{q \rightarrow r} \\ \quad r \end{array}$$

Solution: We shall show the validity of the argument by all three methods.

First solution: We construct the truth table for the statement

$f = [p \wedge (p \to q) \wedge (q \to r)] \to r$

p	q	r	$p \to q$	$q \to r$	$p \wedge (p \to q)$	$p \wedge (p \to q) \wedge (q \to r)$	f
T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	T
T	F	T	F	T	F	F	T
T	F	F	F	T	F	F	T
F	T	T	T	T	F	F	T
F	T	F	T	F	F	F	T
F	F	T	T	T	F	F	T
F	F	F	T	T	F	F	T

Truth table for $f = [p \wedge (p \to q) \wedge (q \to r)] \to r$

Since the column for f contains only Ts, the argument is valid

Second solution: We shall simplify the statement

$f = [p \wedge (p \to q) \wedge (q \to r)] \to r$

since $p \to q = \sim p \vee q$

$= \sim p \vee (p \wedge \sim q) \vee (q \wedge \sim r) \vee r$ using $-(p \wedge q) = - p \vee - q$

$= (\sim p \vee p) \wedge (\sim p \vee \sim q) \vee (q \wedge \sim r) \vee r$ using distributive law.

$= T \wedge (\sim p \vee \sim q) \vee r \vee (q \wedge \sim r)$ since $\sim p \vee p = T$

$= (\sim p \vee \sim q) \vee \{(r \vee q) \wedge (r \vee \sim r)\}$ since $p \wedge T = p$

$= (\sim p \vee \sim q) \vee \{(r \vee q) \wedge T\}$ since $r \vee - r = T$

$= (\sim p \vee \sim q) \vee (r \vee q)$ since $p \wedge T = p$

$= \{(\sim p \vee \sim q) \vee q\} \vee r$ since $p \vee q = q \vee p$

$= \{\sim p \vee (\sim q \vee q)\} \vee r$ by associative law

$= \{\sim p \vee T\} \vee r$ since $\sim p \vee p = T$

$= T$

Since f reduces to T, so the argument is valid

Example : Check the validity of the argument

$$\begin{array}{c} p \to q \\ r \to \sim q \\ \hline p \to \sim r \end{array}$$

Solution : Since the statement $r \to \sim q$ is equal to $q \to \sim r$, we can replace the premise $r \to \sim q$ by $q \to \sim r$. Now $p \to q$

$$\begin{array}{c} q \to \sim r \\ \hline p \to \sim r \end{array}$$

is valid argument by the law of syllogism. Hence given argument is valid.

2.5. Invalidity of an Argument

A Short Method for Invalidity of an Argument

In checking a validity of a given argument, if it is found or suspected that the argument is not valid, a proof of invalidity can be given more easily than by constructing the entire truth table related to the argument. For proving that the argument is invalid, it is sufficient to exhibit a particular set of truth values for the statements involved for which the premises are all true and the conclusion is false. This is equivalent to demonstrating that one row in the truth table would contain F and hence the argument is invalid.

Example: Show that the following argument is not valid

$$\begin{array}{c} p \\ \sim p \vee r \\ \sim p \to q \\ \hline r \end{array}$$

Solution: If p is true, q is false and r is false then each of the premises is true but the conclusion is false. Hence the argument is invalid.

Example: Given the following statements as premises, all referring to an arbitrary meal:

(a) If he takes coffee, he doesn't drink milk.

(b) He eats crackers only if be drinks milk.
(c) He does not take soup unless he eats crackers.
(d) At noon today, he had coffee.

Whether he took soup at noon today? If so, what is the correct conclusion?

Solution: Let p: he takes coffee.

q: he drinks milk.

r: he eats crakers.

s: he takes soup.

Then we have, by condition (a) that $p \to \sim q$

by condition (b), we have $r \to q$, by condition (c), we have $\sim r \to \sim s$

and by condition (d), we have p

Since implication $r \to q$ is equivalent to its contrapositive $\sim q \to \sim r$., we have the following chain of argument:

$p \to \sim q$	a premise
$\sim q \to \sim r$	contrapositive of premise (b)
$\overline{p \to \sim r}$	a conclusion by law of syllogism
$\sim r \to \sim s$	a premise
$\overline{p \to \sim s}$	a conclusion by law of syllogism
$p / \sim s$	

Hence $\sim s$ is the conclusion. That is, he did not take soup at noon today.

2.6. Indirect Method of proof

An important proof technique called the indirect method follows from the fact that any implication $p \to q$ is equivalent to its contra-positive $\sim q \to \sim p$. Thus to prove $p \to q$ indirectly, we assume that q is false and show that p is then false.

More generally, to prove the validity of an argument with premises $p_1, p_2, p_3, ---, p_n$ and conclusion q by indirect method, we consider second argument with premises $\sim q p_1 p_2 p_3 \text{-------} p_{i-1} p_{i+1} --- p_n$ and conclusion p_i and prove the validity of this second argument.

Example : Show that the following argument is a valid argument.

$$\begin{array}{l} p \\ p \wedge q \rightarrow r \vee s \\ q \\ \underline{\sim s} \\ r \end{array}$$

Solution : We will take as premises for the indirect proof all given premises except $\sim s$ and the negation of the conclusion $\sim r$.*i.e.* we shall show that the following argument is valid: p

$$p \wedge q \rightarrow r \vee s$$

$$q$$

$$\sim r / s$$

Now, p a premise

q a premise

$\overline{}$ a conclusion because $p \wedge q \rightarrow p \wedge q$ is always a tautology.

$p \wedge q$

Now, $p \wedge q$ a valid conclusion

$\underline{p \wedge q \rightarrow r \vee s}$ a premise

$r \vee s$ a valid conclusion by *modus ponens*

$\sim r$ a valid conclusion because

$(r \vee s) \wedge -r \rightarrow s$ is a tautology

2.7. Proof by Counter-Example

If a statement claims that a property holds for all objects of a certain type, then to prove it, we must use steps that are valid for all objects of that type. To disprove such a statement, we need only show one counter example. That is one particular object for which the statement is false. Such a proof is called a proof by counter-example.

Example: Prove that the statement "if n is an integer, then $n^2 - n + 41$ is a prime number" is false.

Solution: We need only find one example for which the statement is false. If $n = 41$, then $n^2 - n + 41 = 41^2$ which is not a prime. Hence the statement is false.

Example: Rohan made the following two statement:

1. I love Vicky
2. If I love Vicky then I also love Vivian

Given that Rohan either told the truth or lied in both cases, determine whether Rohan really loves Vicky.

Solution : Let p: Rohan loves Vicky and q: Rohan loves Vivian

Consider the following truth table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

We are given that both p and $p \to q$ are either true or both of them are false. From the table, it is possible for both p and $p \to q$ to be true (row 1) but not possible for both p and $p \to q$ to be false. Hence Rohan must have told the truth and we conclude that Rohan really loves Vicky.

Example: An island has two tribes of natives. Any native from first tribe always tells the truth while any native from the second tribe always lies. Suppose you arrive at the island and ask a native if there is gold on the island. He answers "There is a gold on the island if and only if I always tell the truth." Determine whether there is gold on the island.

Solution: Let p&q be the following propositions:

p : He (the native from whom question is being asked) always tells the truth.

q : There is gold on the island.

Then his answer is the statement ‘ $p \to q$ ’. Suppose p is true then $p \leftrightarrow q$ is true. Consequently q must be true. If p is false then his statement $p \leftrightarrow q$ is false. Consequently q must be true. Thus in both cases we can conclude that there is gold on the island.

Example:A logician was captured by a certain gang. The leader of the gang blindfolded the logician and placed him in a locked room containing two boxes. He gave the following instruction "one box contains the key to the room and other a poisonous snake.

You are the reach into either box you choose and if you find the key, you can use it to go free. To help you, you can ask my assistant a single question requiring a yes or no answer. However, he does not have to answer truely, he may lie if he chooses." After a moment of thought, the logician asked a question, reached in to the box with the key and left. What question did the logician ask so that he was certain to go free?

Solution: Let p be the statement "the box on my left contains the key". Let q be the statement "you are telling the truth." Suppose we desire the answer "yes" if p is true and "no" if p is false. In the table given below, the first three columns represent the possible truth values of p and q and the desired answer. Then the required statement (i.e. a question requiring answer in 'yes' or 'no') must have column 4 as its truth values.

p	q	*Desired answer*	*Truth value of required statement*
T	T	Yes	T
T	F	Yes	F
F	T	Yes	F
F	F	Yes	T

We explain the reasoning used in forming the truth table by considering row 2. In this row truth value of statement p is T while that of q is F. Thus the key is in the left box and the man is lying. Consequently to obtain an affirmative answer the function must have the value F (because the value of the function in row 1 is T) The statement corresponding to this truth table is $p \leftrightarrow q$. Hence the proper question is "does the box on the left contain the key if and only if you are telling the truth?

Example: Given that the value of $p \rightarrow q$ is true, can you determine the value of $\sim p \vee (p \leftrightarrow q)$?

Solution: We shall construct the truth table having columns for $p \rightarrow q$ and $\sim p \vee (p \leftrightarrow q)$.

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

From the table it follows that if $p \to q$ is true then the value of $\sim p \vee (p \leftrightarrow q)$ is true.

Note: In the above example, we could determine the value of $\sim p \vee (p \leftrightarrow q)$ because corresponding to each possible choices of p and q for which the value of $p \to q$ is true, the value of $\sim p \vee (p \leftrightarrow q)$ is same as T.

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P.T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I.N. Herstein. (1983) Topic in Algebra, Vikas publishing house Pvt. Ltd.

Unit - 3

Boolean Algebra

Structure

3.1. Introduction

This is most basic unit of this block as it introduces the concept of statements, statements, statement variables and the five elementary operations and associated logical connectives. We introduce the well formed statement formulae, tautologies and equivalence of formulae. The law of duality is explained and established. It has got tremendous application in almost every field, social, economy, engineering, technology etc. In computer science concept of logic is a major tool to learn to understand it more clearly. Mathematics has a language of its own like most other sciences, which is very precise and communicates just what is required-neither more nor less. Language basically consists of words and their combinations called 'expression' or 'sentences'. However in Mathematics any expression or statement will not be called a 'sentence'.

3.2. Objectives

After reading this unit we should be able to

1. Understand the concept of statement and statement variables
2. Use elementary operations like Conjunction, Disjunction, Negation, Implication, Double implication
3. Understand statement formulae, tautologies to equivalence of formulae
4. Use law of duality and functionally complete set of connectives

Logic is a field of study that deals with the method of reasoning Logic provides rules by which we can determine whether a given argument or reasoning is valid (correct) or not. Logical reasoning is used in Mathematics to prove theorems. In computer science logic is used to verify the correctness of programs.

In this chapter, we shall study Boolean algebra as an abstract structure. The definition of a Boolean algebra which will be given now is one given by **Huntington** in 1904. In fact, Boolean algebra originated in the works of the English Mathematician **George Boole** (1813-1865). The original purpose of this algebra was to simplify logical statements and solve logic problems. Today it is the backbone of design and analysis of computer and other digital circuits.

3.3. Boolean Algbera

Definition: Let B be a none-empty set with two binary operations + and *, a unary operation′, and two distinct elements 0 and 1. They B is called a Boolean algebra if the following axioms hold for any a, b, c ∈ B.

[B_1] **Commutative laws:** The operations + and * are commutative. In other words,

$$a+b = b + a \text{ and } a + b = b+a \ \forall a, b \in B$$

[B_2] **Identity laws:** For any a∈B   a + 0 = a   and a*1 = a

That is, both operations + and * have identity elements denoted by 0 and 1 respectively.

[B_3] **DistributiveLaws:** Each binary operation is distributive over the other. That is, for any a, b, c ∈ B, a+ (b*c) = (a+b) * (a+c) and a* (b+c) = (a*b) + (a*c)

[B_3] **Complements laws:** For each a in B, there exists an element a in B such that a+a′ = 1 and a*a′=0

We sometimes denote a Boolean algebra by (B, +, *, ′ , 0, 1). The elements 0 and 1 are called zero element (identity for +) and unit element (identity for *) of B respectively while a′ is called complement of a in B.

We will usually drop the symbol * between a and b and write a * b simply as ab. Some authors use the symbols $\vee$ and $\wedge$ in place of the symbols + and * respectively and denote the complement of an element a by the symbol $\bar{a}$ instead of a′.

We mention here that there exist other sets of axioms which can equally well define a Boolean algebra, though, of course, each set is derivable from the other. Moreover, we shall also give all alternative definition of a Boolean algebra in terms of an associated partial ordering. The following example shows that the algebra of sets is a Boolean algebra.

Example : Let S be an non-empty set and P(S) be the power set of S. then P(S) is a Boolean algebra with respect to union and intersection as two binary operations + and * respectively and complement of a set with respect to S as unary operation′, ϕ and S will act as 0 and 1 respectively.

Solution : We shall show that the power set P(S) of a non-empty set S forms a Boolean algebra with respect to union and intersection as two binary operations + and * respectively and complement of a subset A of S with respect to S, i.e, S – A as unary operation′ on a.

1. Commutative laws : We know from set theory that

$A \cup B = B \cap A$ and $A \cap B = B \cap A \ \forall A, B \in P(S)$

Thus commutative laws are satisfied.

2. Identity laws: We know that ϕ and S belong to P(S) such that

$A \cup \phi = A$ and $A \cap S = A$ for any $A \in P(S)$.

Thus ϕ and S act as 0 and 1 respectively.

3. Distributive laws: From set theory, we know that

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and

$A \cap (B \cap C) = (A \cap B) \cup (A \cap C)$ for all $A, B, C \in P(S)$.

Hence both operations $\cup$ and $\cap$ distribute over each other.

4. Complement laws : For any $A \in P(S)$, $S - A \in P(S)$ such that

$$A \cup (S - A) = S \text{ and } A \cap (S - A) = \phi$$

Thus every element A in P(S) contains 2^n elements. The case when S contains three elements is considered in the following example.

Example: Let S = {a, b, c}. Then P(S) = {ϕ, {a}, {b}, {c}, {a}, {b, c}, {a, c}, S} is a boolean algebra in which +, * and ′ are taken as union ∪, intersection ∩ and complement with respect to respectively with 0 = ϕ and 1 = S.

Solution: This is a particular case of example 5.1 above. Students are advised to reproduce the solution.

Example: Show that the set B = {0, 1} together with the operatons +, * and ′ defined by the following tables is a Boolean algebra.

+	0	1
0	0	1
1		1

*	0	1
0	0	0
1	0	1

′	0	1
	1	0

Solution: It is clear from the tables that + and * are binary operations on B and that ′ is a unary operation on B. We show that all axioms for a Boolean algebra are satisfied.

1. **Commutative laws:** Since the table for + and * are symmetrical about main diagonals, both operations are commutative.
2. **Identity laws:** It is clear from the tables that a+0 = a and a * 1 = a ∀a∈B. Thus 0 is the identity for + and 1 is the identity for *
3. **Distributive laws:** It is easy to verify that both + and * are distributive over each other. That is, a+(b*c) = (a+b) * (a+c)and a* (b+c)=(a*b)+(a*c)∀a, b, c ∈B.
4. **Complement laws:** Given 0∈B, there exists 1 ∈B such that 0+1=1 and 0*1=0 and given 1∈B, we have 0∈B such that 1+0=1 and 1*0=0 Hence for every a in B, there exists a′=0 Thus (B, +, *, ′) is a Boolean algebra.

Example: let B = {1, 2, 5, 7, 10, 14, 35, 70}. For any a, b in B define +, * and ′ as follows: a+b = lcm (a, b), a*b = gcd (a, b) and $a = \frac{70}{a}$. Then it shows that B is a Boolean algebra with 1 as zero element and 70 as unit element.

Solution: We shall construct the composition tables for +, *, and ′,

+	1	2	5	7	10	14	35	70
1	1	2	5	7	10	14	35	70
2	2	2	10	14	10	14	70	70

5	5	10	5	35	10	70	35	70
7	7	14	35	7	70	14	35	70
10	10	10	10	70	10	70	70	70
14	14	14	70	14	70	14	70	70
35	37	70	25	35	70	70	35	70
70	70	70	70	70	70	70	70	70

+	1	2	5	7	10	14	35	70
1	1	1	1	1	1	1	1	1
2	1	2	1	1	2	2	1	2
5	1	1	5	1	5	1	5	5
7	1	1	1	7	1	7	7	7
10	1	2	5	1	10	2	5	10
14	1	2	1	7	2	14	7	14
35	1	1	5	7	5	7	35	35
70	1	1	5	7	10	14	35	70

′	1	2	5	7	10	14	35	70
	70	35	14	10	7	5	2	1

From the table we see that all the entries in the table are elements of the set B. Therefore both + and * are binary operations on B and ′ is a unary operation on B

1. **Commutative laws**: Since the composition tables for + and * are symmetrical with respect to main diagonals. Therefore operation + and * are commutative.
2. **Identity laws**: From the composition tables we see that a+1 =a and a*70= a ∀a∈B. Hence 1 and 70 are zero element and unit element of B, respectively.

3. **Distributive laws**: With the help of the composition tables for + and * it can be verified that a+(b*c)=(a+b)*(a+c) and a*(b+c)=(b+c)=(a*b)+(b*c)∀a,b,c∈b.

Complement laws: For each a∈B, there exist $a'=\frac{70}{a}$ in b such that a+a′=70 and a*a′=1. Thus complement of every element in B exists in B. Hence B is a Boolean algebra.

3.4. Principle of Duality: Observe the symmetry of the axioms [B_1] to [B_4] in the definition of a Boolan algebra b with respect to the two operations + an * and the two identities 0 and 1. For example, there are two complement laws and the second complement law can be obtained from the first complement law buy interchanging + and * and also interchange their identities 0 an 1. Because of this symmetry it follows that any statement deducible from the axioms of a Boolean algebra remains valid if the operations + and * are interchanged and also their identities 0 and 1 are interchanged throughout. The new statement so obtained (by interchanging + and * and also interchanging identies 0 and 1 in the given statement) is called dual of the given statement. Thus if a statement or algebraic identity holds in a Boolean algebra then its dual also holds. This result is known as Principle of Duality. We state this result as a theorem.

Theorem 1: (Principle of Duality) and theorem of Boolean algebra remains valid if + is interchanged with * and 0 is interchanged with 1 throughout in the theorem.

In the following theorem, each part contains two dual statements. In view of Principle of duality, it is sufficient to rove only one of them and the other will follow by the Principle of duality. However to illustrate the nature of duality, we shall give proofs of both statements in first part.

Theorem 2: The following holds in a Boolean algebra B.

1. **Idempotent laws:** a + a = a and a * a = a ∀ a∈b
2. **Boundedness laws :** a + 1 = 1 and a * 0 = 0 ∀a∈B
3. **Absorption laws:** a+ (a * b) = a and a*(a+b)=a ∀a, b∈B
4. **Associative laws:** (a+b)+c= a+(b+c) and (a*b) * c = a * (b * c) ∀a, b, c∈B

Proof. (1): We first show that a + a = a ∀a∈B

we have a = a 0 by B_2

= a + a * a′ by B_4

=(a + a) * (a+a′) by B_3

= (a+a) * 1 by B_4

= a * a by B_2. Hence a = a + a

To show $a * a = a$, we write $a = a * 1$ by B_2

$=a * (a+a')$ by B_4

$= a * a+a* a'$ by B_3

$=a * a +0$ by B_4

$= a * a$ by B_2. Thus $a = a * a$

Note that the step in the proof of $a * a = a$ is dual to the steps in the proof of $a+a = a$ and the justification for each steps is the same law in $a*a = a$ as in $a + a = a$.

(2) We shall only prove $a+1 = 1$. The other statement will be obtained by the principle of duality. We have

$1 = a + a'$ by B_4

$=a+a'*1$ by B_2 ($\because a'*1 = a'$)

$= (a+a')*(a+1)$ by B_3 $=1* (a+1)$ $=a+1$ by B_2. Thus $a+ 1 = 1$

To prove $a * 0 = 0$, by principle of duality, since $a + 1 =0$ holds in a Boolean algebra, therefore its dual $a * 0 = 0$, also holds in the Boolean algebra by the principle of duality

(3) We first show that $a + a * b = a$ $\forall a, b, \in B$

we have $a = a * 1$ by B_2

$= a * (1+b)$ by boundeness law, $1+b=1$

$=a*1+a*b$ by B_1 $=a+a*b$ by B_2. Thus $a+a*b = a$

To prove $a*(a+b) = a$, we use principle of duality. Since $a+a*b = a$

Also holds in B by the principle of duality

Note: Students are advised to prove the result $a * (a+b)=a$ without using the principle of duality.

(4) To prove $(a * b)* c = a * (b * c)$, we first prove that $a+(a*b)*c = a+a* (b *c)$ $\forall a, b, c \in b$. By absorption law, we have $a+a*(b*c) = a = a* (a+c)$

by absorption law $= (a+a*b)*(a+c)$

Thus $a+a*(b*c)=a+(a*b)*c$ by distributive laws .....(1)

Next, we will show that $a'+a* (b*c) = a'+(b+c)*c$

We have $a'+a*(b*c) = (a'+a) * (a'+b*c)$ by distributive law

$=1 * (a' + b * c)$ by complement law

$= a' + b * c$ by identity law $= (a'+b)*(a'+c)$ by distributive law

$= [1*(a'+b)] *(a'+c)$ by identity law

$= [(a'+a*b) * (a'+b)]*('+c)$ $\because a'+a = 1$

$=(a'+a*b)*(a'+c)$ by distributive law $= a'+(a*b)*c$ by distributive law

Thus $a'+a* (b*c)=a'+(a*B)*c$ ......(2)

Now, $(a*b)*c = 0 + (a*b)*c = a * a' + (a* b) * cx$

$= [a+(a* (a*b) *c]*[a'+(a*b)*c]$ by distributive law

$= [a+a* (b*c)]*[a'+a*(b*c)$ by equations (1) and (2)

$= a * a' + a* (b*c)$ by distributive law

$= 0 +a* (b * c) = a * (b * c)$. This completes the proof.

Applying principle of duality on the result $(a* b) * c = a* (b*c)$

We get $(a+b)+c = a+(b+c)$

In view of this results, we shall write both $a * (b *c)$ and $(a * b)* c$ as $a * b *$ and similarly, we shall write both $(a+b) + c$ and $a+(b +c)$ as $a +b +c$.

Theorem 3 : For each element a in a Boolean algebra B, a′ is unique. In other words, complement of an element a in Boolean algebra B is unique.

Proof : Let a by any element in a Boolean algebra B. If possible, suppose x and y be two complements o a in B. Then $a +x = 1$, $a* x = 0$ and $a + y = 1$, $a * y = 0$

now $x = x *1$ by identity law

$= x * (a+y)$ by assumption

$= x * a + x*y$ by distributive l= $0 + * y$ by assumption

$= x * y$ by identity law $= x * y + 0$ by identity law

$= x * y + a * y$ by assumption $= (x+a) *y$ by distributive law

$= 1 * y$ by assumption $= y$ by identity law

Thus complement of a is unique.

PEPE-103/PEPE-144/ETH-108

Theorem 4 : For any element a in a Boolean algebra B, $(a')' = a$ (this result is known as involution law)

Proof : Since a' is a complement of the element $a \in B$, therefore $a+a'=1$ and $a*a'=0$. But this is exactly the condition to be satisfied for a to be complement of a'. Now by uniqueness of the complement, we have $(a')'=a$

Theorem 5 : In any Boolean algebra, $0' = 1$ and $1' = 0$.

Proof: By theorem 2, we have $1+0 = 1$ and $1 * 0 = 0$

$\Rightarrow 0' = 1$ and $1' = 0$,

Theorem: The following are equivalent in a Boolean algebra B

(1) $a + b = b$ (2) $a * b = a$ (3) $a' + b = 1$ (4) $a * b = 0$

Proof: (1) $\Rightarrow$(2) By absorption law, we have $a = a + a * b = (a + a) * (a + b)$

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

(2) $\Rightarrow$ (1) Suppose that $a * b = a$. To show $a+b=b$.

We have $a + b = a*b+b$ by assumption $a = a*b$

$= b+a*b$ by commutative law $=b$ by absorption law

We now show (1) and (3) are equivalent.

(1) $\Rightarrow$ (3) Suppose (1) holds. Then

$a'+ b = a' + (a + b)$ $\because$ by (1), $a + b = b$

$= (a'+a) + b$ by associative law $= 1 + b$ by complement law

$= 1$ by theorem (2)

(3) $\Rightarrow$ (1) Suppose that $a'+ b = 1$. To show $a+b = b$.

We have, $a + b = 1 * (a+b)$ by identity law

$= (a'+a) * (a+b)$ by assumption

$= a'*a+b$ by distributive law

$= 0 + b$ by complement law

$= b$ by identity law

Thus (1) and (3) are equivalent.

Finally we show that (3) and (4) are equivalent.

(3) $\Rightarrow$ (4). Suppose that $a' + b = 1$. To show $a*b' = 0$

We have $0 = 1' = (a'+ b)' = (a*)' = b'$ by De Morgain's law

$= a * b'$ by involution law

Thus (3) $\Rightarrow$ (4)

Suppose that $a*b' = 0$. To show $a' + b = 1$

We have $1 = 0' = (* b')'$ by assumption

$= a' + (b')$ by De Morgain's law

$= a' + b$

Thus (3) and (4) are equivalent. Consequently, all four are equivalent.

3.5. Subalgebra

Definition: Let (B, +, *, ′, 0, 1) be a Boolean algebra. A non-empty subset S of B is said to be a sub algebra (or a sub Boolean algebra) if S itself is a Boolean algebra with respect to the operation +, * and ′ of B.

From the definition, it is clear that for any Boolean algebra B, the subsets {0, 1} containing identities of + and * and the set B are both sub algebras of B. Observe that the identities of + and * namely 0 and 1 must belong to every subalgebra. For if S is a subalgebra of a Boolean algebra B and $a \in S$ then by complement laws, $a' \in S$ and thus both $a+a' = 1$ and $a * a' = 0$ belong to S.

Theorem 1 : A non-empty subset S of a Boolean algebra B is subalgebra of B if and only if S is closed under the three operations of B, i.e., +, * and ′ .

Proof: Suppose that S is sub-algebra of a Boolean algebra B. Then S itself is a Boolean algebra under the three operations +, * and ′ defined on B. Hence S is closed under the three operations. Thus $a, b \in S \Rightarrow a+b \in S$ and $a' \in S$

Conversely, suppose S is closed under the operations +, * and ′ of B. That is,

$a, b \in S \Rightarrow a+b, a*b$ and $a' \in S$. To show S is a sub-algebra of B.

First of all, we show that both 0 and 1 are in S. Since S is non-empty suppose $a \in S$. We have $a \in S \Rightarrow a' \in S$ by assumption S is closed under ′

Now $a \in S$ and $a' \Rightarrow a + a' \in S$ and $a*a' \in S$ because S is closed under + and *./

$\Rightarrow 1 \in S$ and $0 \in S$. Thus both identities 0 and 1 are in S.

Now we show that all the four axions $[B_1]$ to $[B_4]$ are satisfied for S.

1. **Commutative law :** Let a, b $\in$ S then a, b $\in$ B and therefore $a+b=b+a$ and $a*b=b*a$
2. **Identity laws :** For any a $\in$ S, we have 0 and 1 $\in$ S, such that $a+0=a$ and $a*1=a$, $\forall a \in S$
3. **Distributive laws :** Since operations + and * are distributive over each other for elements of B, therefore they must also distributive over each other for all elements of S.
4. **Complement laws :** Let a $\in$ S. Then by assumption, $a' \in S$ such that $a+a' = 1$ and $a* a' = 0$. Hence S itself is a Boolean algebra under the operations of B. Thus S is a subalgebra of B.

Example: The subset S = (ϕ, {a}, {b,c}, {a,b,c}} of the Boolean algebra B = {ϕ, {a}, {b}, {c}, {a, b}, {a, c}, {b, c}, {a, b,c}} which respect to union intersection and complementation of sets is a sub-algebra of B.

Example: Consider the Boolean algebra B={1,2,5,7,10,14,35,70} discussed in Example 5.4 of 5.1 Then S = {1, 7, 70} is a sub algebra of B.

Example: Let B be any Boolean algebra and a $\in$ B such that $a \neq 1$. Then the subset S = {a, a', 0, 1} is sub-algebra of B.

Solution: We have to show that S is closed with respect to the operations +, * and ′ of B. We know that a+a=a, a*a, a+1=1 and a*0=0, $\forall a \in B$.

we construct composition tables for +, * and ′ for the element of S.

+	a	a′	0	1
a	a	1	A	1
a′	1	a′	a′	1
0	a	a′	0	1
1	1	1	1	1

*	a′	a′	0	1
a	a	0	0	a
a′	0	a′	0	a′
0	0	0	0	0
1	a	a′	0	1

′	a	a′	0	1
	a′	a	1	0

Since all entries in the tables are element of S, therefore S is closed with respect to operation +, * and ′.

Theorem 2: A non-empty subset S of a Boolean algebra (B, +, *, ′ 0, 1) is a sub-algebra of B, if and only if S is closed with respect to operations + and′.

Proof: If S is sub-algebra of (B, +, $*$, ′, 0, 1) then S is closed with respect to operations + and $*$ and′ by theorem 1. Therefore S is closed with respect to operation + and ′.

Conversely, suppose S is closed with respect to operations + and′. To show that S is a sub-algebra, we need to show that S is also closed with respect to $*$. That is, we must show a, b$\in$S.

$a, b \in S \Rightarrow a', b' \in S$ $\because$ S is closed w. r. to operation′.

$\Rightarrow a' + b' \in S$ $\because$ S is closed w.r. to operation +.

$= (a'+b')' = (a')' * (b')' = a*b$. Thus $a*b \in S$.

Hence S is closed w.r. to $*$ also. Thus S is a subalgebra.

Theorem 3: If S_1 and S_2 are two subalgebras of a Boolean algebra B then $S1 \cap S_2$ is also a subalgebra of B.

Proof: Let S_1 and S_2 be any two subalgebra of a Boolean algebra B. We show that $S_1 \cap S_2$ is closed with respect to the operations +, $*$ and ′ of B (although in view of theorem 2, we need to show only for + and ′).

Clearly $S_1 \cap S_2$ is non-empty because 0, $1 \in S_1 \cap S_2$. Let a, $b \in S_1 \cap S_2$. We have a, $b \in S_1 \cap S_2 \Rightarrow$ a, b$\in$ and a, $b \in S_2$

Now, a, b$\in$ $S_1$and S_2 is subalgebra $\Rightarrow a + b \in S_1$, $a * b \in S_1$ and $a' \in S_1$ similarly. $a*b \in S_1 \cap S_2$ and $a + b \in S_2 \Rightarrow a+b \in S_1 \cap S_2$. Similarly, $a*b \in S_1 \cap S_2$ and $a' \in S_1 \cap S_2$.

Thus $S_1 \cap S_2$ is a subalgebra of B.

3.6. Isomorphic Boolean Algebras

Definition: Two Boolean algebras B and B′and said to be isomorphic it there exists a bijective mapping f from B onto B′ such that

$f(a+b) = f(a) + f(b)$, $f(a*b) = f(a) * f(b)$ and $f(a') = [f(a)]'$ for all elements a, b of B.

In other words, two Boolean algebra's are said to be isomorphic if there exists a one-one, onto mapping f: B $\rightarrow$ B$\rightarrow$ which preserves that there operations in B and B′.

Note: In the above definition, we have used same symbols for operations in B and B′. If necessary, the students can use different symbols to denote the operations in B and B′.

If two Boolean algebras are isomorphic then they must have the same cardinality. If Boolean algebras B and B′ are isomorphic and one of them, say B, is finite then the Boolean algebra B′ must also be finite having the same number of elements as B.

Example: Let B = {0, 1} and operationis +, ∗ and ′ are defined on B as follows

+	0	1
0	0	1
1	1	1

∗	0	1
0	0	0
1	0	1

′	0	1
	1	0

Then B is a Boolean algebra. Also, consider the set B′ = {a, b} together with the operations +∗, ∗′ and – as follows

+′	a	b
a	a	b
b	a	b

a′	a	b
a	a	a
b	a	b

-	a	b
	b	a

Then B′ is also a Boolean algebra. The function f: B → B′ defined as f(0) = a and f(10 = b is a bijective mapping which preserves the three operations. Hence Boolean algebras B and B′ are isomorphic to each other.

Example : Consider Boolean algebra B of power set of {a, b, c} discussed in Example 5.2 and the Boolean algebra B′= {1, 2, 5, 7, 14, 35, 70}. B and B′ are isomorphic. In fact, the mapping f: B →B′ defined by

f(ϕ) = 1, f({a})= 2, f({b}) = 5, f({c})=7, f({a, b})=10, f({a, c}) =14, f({b, c})=35 and f({a, b, c})=70 is bijective mapping which preserves the three operations. Hence Boolean algebras b and B′ are isomorphic.

Theorem 4 : Let Boolean algebras B and B′ be ismorphic and let f: B→B′ be the isomorphic mapping, then

(i) If 0 is the identity for + in B then f(0) is the identity for + in B′.

(ii) If 1 is the identity for ∗ in B then f(1) is the identity for ∗ in B′.

Proof: **(i)** Let 0 be the identity for + in B and 0∗ be the identity for + in g′. Then

$f(0) = f(a * a')$ $\qquad \because a * a' = 0 \ \forall \ a \in B.$

$=f(a) * f(a')$ $\quad \because$ f is isomorphic mapping

$= f(a) * [f(a)]'$ $\quad \because$ f is isomorphic mapping

$= 0^*$ by complement law. Hence $0^* = f(0)$

(ii) Let 1 and 1* be the unit elements in B and B′. Then $f(1) = f(a+a')$ $\because$ $a+a' = 1$

$= f(a) * f(a')$ $\quad \because$ f is isomorphic mapping

$= f(a) + [f(a)]'$ $\quad \because$ f is isomorphic mapping

$= 1^*$ by complement law. Thus $1^* = f(1)$

Solved Examples

Example: Prove that no Boolean algebra can have three distinct elements.

Solution: Let B be a Boolean algebra having three elements. Then B must have two distinct elements 0 and 1 as identities ofr the operations + and * respectively. Let a b the third element of B. Since B in a Boolean algebra, there exists an element a′ in B such that $a + a' = 1$ and $a * = 0$

Now there are three cases : (i) $a' =$ (ii) $a' = 0$ (iii) $a' = 1$

Case (i) If $a'=a$ then $a+a' = 1 \Rightarrow a + a = 1 \Rightarrow a = 1$

And $a * a' = 0 \Rightarrow a * a = 0 \Rightarrow a = 0$. But a is different from 0 and 1.

Therefore $a' = a$ is not possible. Case (ii) if $a' = 0$. Then $a + a'\ 1 \Rightarrow a + 0 = 1 \Rightarrow a = 1$.But a is not equal to 1. Hence $a' = 0$ is not possible.

Case (iii) if $a' = 1$. Then $a * a' = 0 \Rightarrow a * 1 = 0 \Rightarrow a = 0$

Thus $a' \neq 1$ because a is not equal to 0.

Therefore B either has only two elements 0 and 1, or B has four elements because if there is an element a in B different from 0 and 1, then B must have another element f different from 0, 1 and a. Hence no Booleam algebra can have exactly three elements.

Example: Prove that for any, a, b and c in a Boolean algebra the following are equal. **(a)** $(a+b)(a'+c)(b+c)$ **(b)** $ac + a'b + bc$ **(c)** $(a + b)(a'+c)$ **(d)** $ac + a'b$

Solution: We have $(a+b)(a'+c)(b+c) = (a+v)(a'b+c)$ by distributive law

$=a(a'b+c)+b(a'b+c)$ by distributive law

$=aa'b+ac+ba'b+bc$ by distributive law

$=(aa')b+ac+a'bb+bc$ by commutative and associative law

$=0b + ac + a'b+bc$ $\because aa' = 0$ and $bb=b$ $=ac+a'b+bc$ $\because 0b=0$

Thus (a) and (b) are equal

Now we show that (c) is equal to (b).

$(a+b)(a'+c) = a(a'+c) + b(a'+c)$ by distributive law

$= aa' +ac+ba'+bc$ by distributive law

$= 0 + ac + a'b + bc$ by commutative and complement law

Thus (b) is equal to (c)

Finally, we show that (b) is equal to (d)

$ac+a'b+bc = ac + a'b + (a+a')$ be $\because a+a'=1$

$= ac+a'b+abc+a'bc$ by distributive law

$= (ac+abc)+(a'b+a'bc)$ by associative and commutative law

$= (ac+(ac)+(a'b+(a'b)c$ by associative and commutative law

$= ac + a'b$ by absorption law. Hence (b) and (d) are equal

Thus all the four are equal.

Example: In any Boolean algebra, show that

(1) $(a+b)(b+c)(c+a) = ab + bc + ca$
(2) $(a+b')(b+c')(c+a') = (a'+b)(b'+c)(c'+a)$

Solution (1) L.H.S $= (a+b)(b+c)(c+a)$

$= (a+b)[(b+c)(c+a)]$ by associative law

$= (a+b)[(c+b)(c+a)]$ by commutative law

$= (a+b)[c+ba]$ by distributive law

$= a(c+ba) + b(c+ba)$ by distributive law

$= ac + aba + bc + bba$ by distributive and associative laws

$= ac + (aa)b+bc+9bb)a$ by commutative and associative law $\because aa = a$

$= ac + ab = bc+ba$ by associative and commutative laws

$= ab+bc+ac$

R.H.S. (2) $(a+b')(b+c')(c+a') = [(a+b')(b+c')](c+a')$

$=[(a+b')b+(a+b')c'](c+a') = (ab + b'b+ac'+b'c')(c+a')$

$= (ab+0+ac'+b'c')(c+a') = (ab + ac'+b'c')(c+a')$

$=(ab + ac'+b'c')c+(ab+ac'+b'c')a'= abc+ac'c+b'c'c+aba'+ac'a'+b'c'a'$

$= abc+0+0+0+0+b'c'a' = abc + a'b'c'$

Similarly, we can show that $(a'+b)(b'+c)(c'+a) = abc + a'b'c'$

Hence we have $(a+b')(b+c')(c+a') = (a'+b)(b'+c)(c'+a)$

Example: in a Boolean algebra, if $a + x= b + x$ and $a + x' = b+x'$ then prove that $a = b$

Solution: We are given that $a + x = b + x$ ... (1)

and $a + x' = b + x'$ ... (2)

now $a = a + 0$ by identity law

$= a + xx'$ $\because xx' = 0$

$= (a+x)(a+x')$ by distributive law

$= (b+x)(b+x')$ by (1) and (2)

$= b+xx'$ by distributive law

$= b + 0,$ $\because xx' = 0$ $= b$ by identity law

Example: In anyBoolean algebra, prove that $b = c$ if and only of both $a+b = a+c$ and $ab= ac$ holds.

Proof: If $b = c$ then we have $a + b = a + c$ and $ab = ac$ both hold

Now we show that $a+b = a+c$ and $ab = ac \Rightarrow b = c$

$b = b(b+a)$ by absorption law

$=b(c+a)$ $\because a+b=a+c \Rightarrow b+a=c+a$

$= bc+ba$ by distributive law

$=bc+ab$ by commutative law

$=bc+ac$ by given conditioin

$= (b+a)c$ by distributive law

$= (c+a)c \Rightarrow b+a = c+a = c$ by absorption law

PEPE-103/PEPE-144/ETH-108

Check your progress

1. Write the dual of each of the following

   (a) $(a * 1) * (0 + a') = 0$, (b) $a + a'b = a + b$

2. Show that the set $B = \{0, a, b, 1\}$ together with the operation $\vee, \wedge$ and $'$ defined by

$\vee$	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

$\wedge$	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

$'$	
0	1
a	b
b	a
1	0

   is a Boolean algebra.

3. Show that algebra of sets is a Boolean algebra with respect to suitable operations.

4. Show that a non-empty subset S of a Boolean algebra is a sub algebra if it is closed under $*$ and $'$.

5. Show that a mapping f from a Boolean algebra B to another Boolean algebra B$'$ which preserves the operations + and $'$ also preserves the operation $*$.

6. If a and b are element of a Boolean algebra B then show that a=b if and only if $ab' + a'b = 0$

7. prove that in any Boolean algebra (a) $a+a'b = a+b$

   (b) if $ax = bx$ and ax' bx' then $a=b$, (c) $ab+ab'+a'b+a'b' = 1$

8. Let B_n be the set of n-tuples of the form $(a_1, a_2,\ldots a_n)$ where each a_1 is either 0 or 1. Define suitable operations on B_n so that it becomes a Boolean algebra.

[Hind ; Define $(a_1,a_2, \ldots,a_n)+(b_1,b_2,\ldots b_n) = (a_1,b_2, a_2,+b_2,\ldots, a_n,b_n)$, $(a_1, a_2,\ldots a_n) * (a_1,b_2,\ldots b_n) = (a_1, b_2, a_2 ,b_2\ldots, a_n,b_n)$ and $(a_1,a_2\ldots,a_n)'=(a'_1, a'_2,\ldots a'_n)$].

Solutions/Answer

(1) (a) $(a+0) + (1*a')=1$ (b) $a(a'+b) = ab$

3.7. Boolean Algebra as Lattices

Definition : Let B a Boolean algebra and $a, b \in B$. Then $a \leq b$ if and only if $a+b = b$.

Proof: We know that $ab'=0$ is equivalent to $a+b=b$. Thus $a \leq b$ if and only if $a+b = b$

Theorem 2: Let B be a Boolean algebra. Then the relation $\leq$ defined as $a \leq b$ if and only if $ab' = 0$ is a partial order on B.

Proof: $\leq$ is reflexive. Since $aa'=0$ therefore $a \leq a$ for all $a \in B$

$\leq$ is anti symmetric. Let $a, b \in b$ such that

$a \leq b$ and $b \leq a$. Then $ab'=0$ and $ba'=0$

Now $a = a.1 = a(b+b') = ab + ab' = ab+0 = ab + ba' = ba + ba' = b(a+a') = b.1 = b$

Thus $\leq$ is anti symmetric

$\leq$ is transitive. Suppose that $a \leq b$ and $b \leq c$. Then $ab'=0$ and $bc'=0$.

Now $ac' = a.1.c' = a(b+b')c' =(ab + ab')c' =a(bc') + (ab')c'$

$= a.0+0.c' = 0+0=0$. Hence $a \leq c$. Thus $\leq$ is a partial order on B.

Theorem 3: Let B be a Boolean algebra. Then $(B, \leq)$ where $\leq$ is defined as $a \leq b$ if and only if $ab' = 0$, is a lattice. Moreover the identities 0 and 1 are the least and the greatest elements of this lattice.

Proof: We have already shown that $(B, \leq)$ is a partial ordered set. To show that $(B, \leq)$ is a lattice, we will show that for any elements $a, b \in B$, join of a and b is a+b and meet of a and b is ab. That is, we will show that

Sup $\{a, b\} = a \vee b = a + b$ and inf $\{a, b\} = a \wedge b = ab$ $\forall a, b \in B$

Since $a (a+b)' = a(a'b') = (aa')b'=0b'=0$, $a \leq a + b$

Similarly, $b \leq a + b$

$a \leq a + b$ and $b \leq a + b \Rightarrow a + b$ is an upper bound of the set $\{a, b\}$.

Let c be any other upper bound of $\{a, b\}$. Then $a \leq c$ and $b \leq c$

$\Rightarrow ac' = 0$ and $bc' = 0 \Rightarrow ac' + bc' = 0$

$\Rightarrow (a + b) c' = 0 \Rightarrow a + b \leq c$

Thus a + b is the least upper bound of the set {a, b}, which by definition, in the joint of a abd be denoted by $a \vee b$. Similarly we can show (or by duality) that ab is the infimum of {a, b}. Thus inf {a, b} = $a \wedge b$ = ab.

Hence B is a lattice where + and ′ are join and meet operations.

Finally, if $a \in B$ then 0 a′=0 and hence $0 \leq a$. This shows that 0 is the least element of B. Similarly a. 1′ = a0 = 0 for all $a \in B$ implies that $a \leq 1$ for all $a \in B$. Thus 1 is the greatest element of B. Thus B is bounded lattice.

Theorem 4: Let (B, +, ., ′) be a Boolean algebra. Then the lattice ($B \vee, \wedge$), where $a \vee = a +$ b and $a \wedge b$ = ab is bounded, complemented and distributive. Conversely, if ($B, \vee, \wedge$) is a bounded, complemented and distributive lattice then (B, +, ., ′) is a Boolean algebra, where a+b = a $a \vee b$, ab = a $\wedge b$ and a′ is a complement of a in ($B, \vee, \wedge$).

Proof: Let (B, +, ., ′) be a Boolean algebra. Then ($B, \vee, \wedge$) is a bounded lattice. Since $\vee$ and $\wedge$ are precisely + and respectively, axioms B_2 and B_4 in definition of a Boolean algebra show that ($B, \vee, \wedge$) is also distributive and complemented.

Conversely suppose ($B, \vee, \wedge$) is bounded, complemented and distributive lattice with 0 and 1 as the least and the greatest elements. For a, $b \in B$, define

$a + b = a \vee b$ and $a . b = a \wedge b$

Then the binary operation + and . are commutative with 0 and 1 as their identities. The distributive laws follow from the definition of a distributive lattice. Thus the axioms B_1 to B_3 in the definitions for a Boolean algebra are verified. Since ($b, \vee, \wedge$) is a complemented lattice, we can find a complement of each $a \in B$. We denote this complement of a by a′. Now we have a+a′ = 1 and aa′ = 0

Thus axiom B_4 is also satisfied. Thus (B, +, . , ′) is a Boolean algebra.

Remark: Many authors define a Boolean algebra as a bounded, complemented and distributive lattice. The preceding theorem shows that the definition is equivalent to ours.

3.8. Representation Theorem for Finite Boolean Algebras

The partial order structure induced on the set B of a Boolean algebra (B, +, . , ′) also enables us to prove the representation theorem for finite Boolean algebras. By a finite Boolean algebra we mean a Boolean algebra with a finite number of elements. We shall show that a finite Boolean algebra has exactly 2^n elements for some n>0. Moreover, there is a unique Boolean algebra of 2^n elements for every n>0.

Let (B, + , . , ′) be a Boolean algebra. (Then (B, ≤) is lattice, where $a \le b$ if and only if $ab' = 0$. We recall that an element a in B is an atom if it covers 0. In other words, an elements a in B is called an atom if $0 < a$ and there is no element b in B such that $0 < b$ and $b < a$. For example, atoms of a power set Boolean algebra P(S), are precisely singleton subsets of S. As another example, consider the Boolean algebra B = {1, 2, 5, 7, 10, 14, 35, 70} of factors of 70 under the operations lcm (for +) and gcd (for.) The atoms of this Boolean algebra are precisely 2, 5 and 7.

In the following lemma, we give some simple properties about atoms in a finite Boolean algebra.

Lemma: Let (B, +, . , ′) be a finite Boolean algebra. Then

(i) For every noon-zero element b, there exists atleast one atom a such that $a \le b$.
(ii) If a and b are distinct aotms then $ab = 0$
(iii) If b is any non-zero element in B and $a_1, a_2, a_3, \ldots, a_4$ be all atoms of B such that $a_i \le b$, $i=1\ldots k$, then $b = a_1+a_2+\ldots+a_k$ and this representation in unique.

Proof: (i) Let (B, +, . , ′) be a finite Boolean algebra with 0 as the least element. Let b be any non-zero element of B. We shall show that there exists atleast one atoms a in B such that $a \le b$. If b itself is an atom then we have nothing to do. If b is not an atom then there exists b_1 in B such that $0 < b_1 < b$. If b_1 is an atom, we are done. Otherwise there exists b_2 in B such that $0 < b_2 < b_1 < b$. Continuing in this manner, since B is finite, there exists and atom b_i for some i such that $0 < b_i < \ldots\ldots b_2 < b_1 < b$. It follows that for every non-zero element b, there exists atleast one atom a such that $a \le b$.

(ii) Let a and be two distinct aotms of B. If $ab \neq 0$ then b (i), there exists an atom c such that $c \le ab$. Note $ab = a \wedge b = \inf \{a, b\}$ Therefore $c \le ab \le a$. Since a itself is an atom it follows that $a = c$. Similarly $b = c$. Hence $a = b$. In other words, if a and b are distinct atoms then $ab = 0$.

(iii) Let $a_1, a_2, \ldots, a_k$ be distinct atoms of B such that $a_1 \le b, a_2 \le b, \ldots, a_k \le b$

we claim that $b = a_1+a_2+\ldots+a_k$

since $a_i \le b$ for each $i = 1, 2, \ldots, k$ $\Rightarrow \sup \{a_1, a_2, \ldots. A_k\} \le b$

$\Rightarrow a_1 + a_1 + \ldots + a_k \le b$. We now show that $b \le a_1 + a_2 + \ldots + a_k$

for notational convenience , let $c = a_1 + a_2 + \ldots. a_k$.

To show $b \le c$, we shal show $bc'=0$. $b \le c$ will follow by (1). If possible, suppose $bc' \neq 0$. Then by (i), there exists an atom a such that $a \le bc'$

Since $bc' \le b$ and $bc'c'$ by transitive property of ≤, we have $a \le b$ and $a \le c'$

since a is an atom and $a \leq b$, therefore a must be equal t one of the atoms $a_1, a_2, \ldots, a_4$. Thus $a \leq a_1 + a_2 + \ldots + a_k = c$

Now $a \leq c'$ and $a \leq c \Rightarrow a \leq c \wedge c' = cc' = 0 \Rightarrow a = 0$, which is impossible because a is an atom. Thus $bc' = 0$ which implies $b \leq c$ by (i)

Now $b \leq c$, $c \leq b$ and $\leq$ is anti-symmetric give $b = c = a_1 + a_2 + \ldots a_k$

Uniqueness : suppose $b = b_1 + b_2 + \ldots . b_r$, where each b_i is an atom and $b_i \neq b_j$ be another representation of b.

$\Rightarrow b_i \leq b$ for each I, because b is the supremum of $b_1, b_2, \ldots .. b_r$

Now consider an atom b_i, $i \leq i \leq r$. Since $b_i \leq b$, we have $\inf\{b_i, b\} = b_i$

$\Rightarrow b_i\, b = b_i, 1 \leq i \leq r$

$\Rightarrow b_i\,(a_1 + a_2 + \ldots + a_k) = b_i \qquad \because a_1 + a_2 + \ldots a_k = b$

$\Rightarrow b_i\, a_1 + b_i\, a_2 + \ldots .. b_i\, a_k = b_i \qquad$ by distributive law

$\Rightarrow$ for some a_j, $1 \leq j \leq k$, $b_i\, a_j \neq 0 \Rightarrow b_i = a_j \qquad$ by (ii)

This shows that every b_i is equal to some a_j and hence representation of b as um of atoms is unique (except for order).

Corollary: (B, + , …., ′ , 0, 1) be a Boolean algebra, Then sum of all atoms in B equal 1. Now we state and prove representation theorem for finite boolan algebras.

Theorem: let (B, +, . , ′) be a finite Boolean aogebra. Let S be the set of atoms of b. Then (B, +, . , ′0 is isomorphic to the Boolean algebra (P(S), ∪, ∩-) of power set of S.

Proof: Let (B, +, . , ′) be a finite Boolean algebra and let $S = \{a_1, a_2, \ldots, a_n\}$ be the set of all distinct atoms of B. By the last lemma, every element $x \neq 0$ has a unique representation as a sum of atoms. That is,

$x = a_1 + a_2 + \ldots + a_k$, where a_i, s are atoms $f(0) = \phi$ and $f(x) = \{ a_1, a_2, \ldots .. a_k)$ where

$x = a_1 + a_2 + \ldots . + a_k$ is the unique representation of x as a sum of atoms.

Suppose x, y are any two elements in B. suppose

$x = a_1 + a_2 + \ldots . + a_r + b_1 + b_2 + \ldots . + b_s$

and $y = b_1 + b_2 + \ldots . + b_s + c_1 + c_2 + + \ldots . c_t$

where each a_i, $1 \leq i \leq r$, b_j, $1 \leq j \leq s$ and c_k, $1 \leq k \leq t$ are atoms of B.

Then $x+y = a_1 + a_2 + \ldots + a_r + b_1 + b_2 + \ldots b_s + c_1 + c_2 + \ldots + c_1$

And $xy = b_1 + b_2 + \ldots + b_s$

Because if a_i and a_j are distinct atoms then $a_i\, a_j = 0$ and

$a + a = a$ and $a.a = a$ for any $a \in B$.

Hence $f(x+y) = \{a_1, a_2, \ldots, a_r, b_1, b_2 \ldots, b_s, c_1, c_2 \ldots c_t\}$

$= \{a_1, a_2, .. a_r, b_1, b_2, \ldots b_s\} \cup \{b_1, b_2 \ldots b_s, c_1, c_2 \ldots c_1\} = f(xy) = \{b_1, b_2 \ldots b_s\}$

$= \{a_1, a_2, .. a_r, b_1, b_2, \ldots b_s\} \cap \{b_1, b_2 \ldots b_s, c_1, c_2 \ldots c_1\} = f(x) \cap f(y)$

Let $S - \{a_1, a_2, .. a_r, b_1, b_2, \ldots b_s\} = \{d_1, d_2, .. d_p\}$

We claim $z = d_1, d_2, .. d_p$ is the complement of x. For this, we shall show $x + z = 1$ and $xz = 0$. Clearly, $x + z = a_1 + a_2 + \ldots a_r + b_1 + b_2 + \ldots b_s + d_1 + d_2 + \ldots d_p$ is the sum of all atoms of B. Therefore, $x + z = 1$. Also $xz = 0$ because $a_i a_j = 0$ for distinct atoms a_i and a_j. Hence $z = x'$

Now $f(x') = \{d_1, d_2, \ldots, d_p\} = S - \{a_1, a_2, \ldots a_r, b_1, b_2, \ldots, b_s\} = S - f(x)$ complement of f(x) Further, by uniquenss of the representation, we see that f is one and onto.

(To show f in one-one, consider $x, y \in B$ such that $x \neq y$, we can write

$x = a_1 + a_2 + \ldots + a_m$, and $y = b_1, b_2, \ldots, b_k$ as sums of atoms

$x \neq y \Rightarrow a_1 + a_2 + \ldots a_m \neq b_1, b_2, \ldots, b_k \Rightarrow \{a_1 + a_2 + \ldots a_m\} \neq \{b_1, b_2, \ldots, b_k\}$

$\Rightarrow f(x) \neq f(y)$. Thus f in one-one

To show that f is onto, let $\{a_1 + a_2 + \ldots a_n\}$ be any subset of S. then $x = a_1 + a_2 + \ldots a_n$

is a unique element in B and $f(x) = \{a_1 + a_2 + \ldots a_n\}$. Hence f is onto.

Hence f is an isomorphism. Thus Boolean algebra (B, +, . , ') and (P (S), $\cup$,$\cap$,-) are isomorphic to each other.

Corollary: Every finite Boolean algebra has 2^n elements for some positive integer n.

Proof: Since, by above theorem, every finite Boolean algebra B is isomorphic to power set Boolean algebra P(S) and power set P(S) has 2^n elements, where n is the number of elements in S, the set of atoms of B. Hence B has 2^n elements for some n>0.

Example : Consider the Boolean algebra B = {1, 2, 5, 7, 10, 14, 35, 70} with + +, . and ' defined as follows: $a + b = \text{lcm}(a, b)$, $ab = \gcd(a, b)$ and $a' = 70/a$.

In this Boolean algebra, atoms are 2, 5 and 7 and B is isomorphic to the Boolean algebra (P(S), ∪, ∩, -), where S = {2,5,7}.

Example : in any Boolean algebra B, show that $a \leq b \Rightarrow a + bc = = b\,(a + c)$, where a, b, $c \in B$.

Proof: We have $a + b = a\,(b + b') + b$

$= ab + ab' + b$ by distributive law

$= ab + 0 + b$ $\because a \leq b \Leftrightarrow ab' = 0$

$= ab + b$ by identity law

$= b$ by absorption. Therefore, $a + bc = (a + b)(a + c)$ by distributive law

$= b(a+c)$ in view of the result just proved.

Example : Show that the lattice whose Hasse diagram is given below is not a Boolean algebra.

Solution: Observe that elements a and e are both complements of c. But theorem says that such an element is unique. Thus given lattice cannot be a Boolean algebra.

Example : Consider the lattice {1, 2, 4, 5, 10, 20} of all positive divisors of 20 under the divisibility relation.Then this lattice cannot be a Boolean algebra because it has six elements and $6 \neq 2^n$ for any integer $n > 0$. Thus we conclude that divisors of 20 is not a Boolean algebra.

3.9. Boolean Functions

Let (B, +, ·, ′) be a Boolean algebra. By a constant, we shall mean any symbol, such as 0 and 1, which represents a specified element of B. By a variable, we mean a symbol, which represents an arbitrary element of B.

A Boolean function or a Boolean polynomial is an expression derived from a finite number of applications of the operations +, ·, and ′ to the elements of a Boolean algebra. Expression such as ab, $(a' + b)' + ab'x + ab$, and $a' + b'$ are Boolean functions. In any Boolean algebra, we know that $2a = a + a = a$, $3a = a + a + a = a$ and in general $na = a$ where n is any positive integer.

Also $a^2 = a.\ a = a$, $a^3 = a\ .\ a.\ a = a$ and in general $a^k = a$, where k is any positive integer. Thus no multiples or powers appear in the Boolean polynomials.

Definition: A Boolean expression of n variables $x_1, x_2, \ldots\ x_n$ is said to be a minterm or a minimal polynomial if it is of the form $f_1(x_1) \cdot f_2(x_2) \cdot f_3(x_3) \ldots\ldots f_n(x_n)$

where $f_i(x_i) = x_i$ or x_i' for all $i = 1, 2, \ldots.n$

for example $x_1.x_2.x_1'.\ x_2,\ x_1.\ x_2'$ are min-terms in two variables x_1 and x_2. Similarly $x_1x_2'x_3$ and $x_1'\ x_2'$ is an example of minterms in three variables x_1,x_2 and x_3.

Theorem 1: There are exactly 2^n minterms in variables $x_1,x_2\ \ldots\ X_n$ is an expression of the form $f_1(x_1)\cdot f_2(x_2)\ \ldots, f(x_n)$, where each $f_i(x_i) = x_i$ or x_i' for all $i = 1, \ldots\ldots,n$

clearly, there are two ways of selecting $f_i(x_i)$ namely x_i or x_i' for each $i = 1, \ldots,n$. Thus there are 2^n different minterms in n variables.

3.10. Disjunctive Normal Form

Definition: A Boolean function in n variables $x_1, x_2, \ldots, x_n$, is said to be in disjunctive normal form (in short, D N form) if it is a sum of minterms. Also 1 and 0 are said to be in disjuncive normal form.

In other words, a Boolean function in n variables $x_1, x_2, \ldots,x_n$ is said to be in disjunctive normal form if the function is a sum of terms of the type $f_1(x_1)\ f_2(x_2)\ f_3(x_3)\ f_4(x_4)\ f_5(x_5)\ldots\ f_n(x_n)$ where $f_j(x_j) = x_j$ or x'_j for all $j=1, 2,\ldots n$ and no two terms are same. Also 1 and 0 are said to be in disjunctive normal from.

The disjunctive normal form is also called the (sum of products canonical form).

Observe that in a disjunctive normal form (sum of products canonical form) any particular minterm may or may not be present. Since there are 2^n minterms in n variables, we can have only 2^{2n}different DN forms. These DN forms include the DN form of 0 in which no minterm is present in the sum and also the DN form of 1 where all the minterms are present in the sum. In any case, every Boolean function given in DN form in n variables is equal to one of the 2^{2n} Boolean functions.

Example : Write the function $f=(xy' + zx)' + x'$ in DN form.

Solution: We have $f = (xy' + xz)' +x' = (xy')'(xz)\ '+x' = (x'+y)\ (x'+z')+x' = x'+yz'+x' = x' + (x'+yz')=yz'= x'(y+y')(z+z')+yz'(x+x')$

$=x'yz + x'\ yz'+x'y'z'xyz'+x'yz' = x'yz + xyz'+x'yz'+x'y'z+x'y'z'$

$= x'yz+xyz'+x'yz'+x'y'z+x'y'z'$, because the minterm $x'y'z'$ is appearing twice.

Example : Write the Boolean function $f - x_1+x_2$ in sum of products canonical form in three variables x_1,x_2 and x_3.

Solution: We have $f = x_1+x_2 = x_1(x_2+x'_2)\ (x_3+ x'_3)\ x_2+(x_1+ x'_1)\ (x_3+ x'_3)$

$= x_1\ x_2+ x_1\ x_2\ x'_3+ x_1\ x'_2\ x_1\ x'_2\ x'_3+ x_1x_2\ x_3+ x_1\ x_2\ x'_3+ x'_1\ x_2\ x_3 + x'_1\ x_2\ x'_3$

$= x_1\ x_2\ x_3+ x_1\ x_2\ x'_3+ x_1\ x'_2\ x'_3+ x'_1\ x_2\ x_3+ x'_1\ x_2\ x'_3$

Complete Disjunctive Normal Form

As seen earlier, if there are n variables, then the total number of minterms will be 2^n. Therefore any DN form can have at most 2^n minterms.

Definition : A disjunctive normal form in n variables, which contains all the 2n minterms is called the complete disjunctive normal form. For example, $f = xy + x'y + xy' + x'y'$ is the complete disjunctive normal form in two variables. It can be seen by simplification of the complete disjunctive normal form or by the following theorem that the complete disjunctive normal form is identically equal to 1.

Theorem 2 : If each of n variables is assigned the value 0 or 1 in an arbitrary, but fixed manner then exactly one minterm of the complete disjunctive normal form in the n variables will have the value 1 and all other minterms will have the value 0.

Proof: Consider the complete disjunctive normal form in n variables $x_1, x_2, \ldots, x_n$. Then it has all the 2^n minterms of the form $f_1(x_1)\ f_2(x_2) \ldots f_n(x_n)$ where $f_i(x_i)=x_i$ or x'_I for each $i = 1, 2, \ldots, n$. Now assign the values 0 or 1 to the variables $x_1, x_2, \ldots x_n$. Select a minterm from the complete normal form as follows: use x_i if x_i is assigned the value 1 and use x'_i if x_i is assigned the value 0 for each x_i, $i=1, 2, \ldots, n$. The term so selected is then a product of n ones and hence is equal to 1. All other terms in the complete normal form will contain at least one factor 0 and hence will be 0.

Corollary 1 : To functions with same minterms are obviously equal. Conversely, if two functions are equal, then they must have same value for every choice of value for each variable. In particular, they assume the same value for each set of values 0 and 1, which may be assigned to the variables. By theorem 2 above, the combinations of values of 0 and 1 which, when assigned to the variables, make the function assume the value 1 uniquely determine the terms which are present in the DN from for the function. Hence, both DN forms contain the same min-terms.

Corollary 2 : To establish any identity in Boolean algebra, it is sufficient to check the value of each function (on both sides of the identity) for all combination of 0 and 1, which may be assigned to the variables.

We have seen in the preceding theorems that a Boolean function is completely determined by the value it take for each possible assignment of 0 and 1 to the respective variables. This suggests that Boolean functions could be easily specified by giving a table to represent such properties. If such a table has been given, then the function, in disjunctive normal form, may be written down by inspection. We simply look at the conditions where the function takes the value 1 then the sum of corresponding minterms (where function takes the value1) gives the function, although the function so obtained may not be in simplest form. The following example will explain this method.

Example : Find and simplify the function specified by the table as given.

Row	X	y	z	f(x,y,z)
1	1	1	1	0
2	1	1	0	1
3	1	0	1	0
4	1	0	0	1
5	0	1	1	0
6	0	1	0	0
7	0	0	1	0

Solution : We observe that function f(x, y, z) takes the value 1 for the normal form of f will contain two minterms each corresponding to the conditions given in rows 2 and 4. In row 2, the values of x, y, z are given respectively as 1, 1, 0 and so the corresponding minterm will be xyz'. Similarly the other minterm will be $xy'z'$ which is taken with respect to row 4. Thus the function $f(x,y,z) = xyz' + xy'z'$.

We now simplify f(x, y, z) b using laws of Boolean algebra $\therefore f(x, y, z) = yz' (y + y') = xz'$. It may be verified that this function satisfies all the other rows also.

Rule for finding complement of a function in DN form

We can find by inspection the complement of any function given in disjunctive normal form. If a function f is given in disjunctive normal from then its complement f' is obtained by omitting from the complete disjunctive normal form the terms which appear in the function f.

Example : Find the complement of the following functions –

(a) $f = a'b = ab'$
(b) $f = a'bc + abc' + a'b'c+a'b'c'$

Therefore the complement of $f = a'b + ab'$ is given by $f' = ab + a'b'$

(b) The complete disjunctive normal form in three variables a, b, c is

$abc+abc'+ab'c+ab'c'+a'bc+a'bc'+a'bc'+a'b'c+a'b'c'$

Therefore the complement of $f = a'bc + abc' + a'b'c + a'b'c'$ is given by

$f' = abc + ab'c + ab'c + a'bc'$

Example: Find the function of three variables x, y and z which is I if either $x=y=1$ and $z=0$ or if $x = z = 1$ and $y = 0$ and is 0 otherwise.

Solution: By given conditions, the required function takes the value 1 at two points namely when $x = 1, y = 1, z = 0$ and when $x = 1, y = 0 = 1$. The corresponding minterms are xyz' and $xy'z$. Hence the required function f DN form is equal to sum of these two terms, i.e. $f = xyz'+xy'z$

Example: Express each of the following in DN from in the smallest possible number of variables

(i) $xy'+xz+xy$
(ii) $(x'+xyz'+xy'z+x'y'z't+t')'$

Solution: (i) Let $f = xy'+xz+xy = xy'+xy+xz$ by commutative law

$= x(y'+y) + xz$ by distributive law $= x + xz$ by complement law

$= x$ by absorption law. Now f contains only one variable. Hence $f = x$

is its disjunctive normal form in smallest possible variables.

(ii) Let $f = [x'y+xy'+xy'z+x'y'z't+t']'$

we first consider the expression without complement, i.e. $x'y+xyz'+xy'z+x'y'z't+t'$

and express it in disjunctive normal form in four variables x, y, z and t.

Now $x'y+xyz'+x'y'z't+t' = x'y(z+z')(t+t') + xyz'(t+t')xy'z$

$(t+t') + x'y'z't+t'(x+x')(y+y')(z+z') = x'y(zt+z't+zt'+z't'+) + xyz'(t+t')+$

$xy'z(t+t')+x''z't+t'(zyz+x'yz+xy'z+xyz'+x'y'z+x'yz'+xy'z'+x'y'z')$

Using the law $a+a = a$, we ge

$t= x'yzt+x'yz't+x'yzt'+x'yz't'+xyz't+xyz't'+xy'zt+ xy'zt'+ x'y'z't+$

$x'yzt'+ x'y'zt'+ xy'z't'+x'y'z't'$. Which contains 13 terms.

Now writing the missing terms from the complete DN form, we get the required function (which is complement of this function) as $f = xyzt+x'y'zt+xy'z't$

in DN form in three variables

Example: Solve f(x,y, z)= (x+yy′) (x′+z) using distributive law

Solution: We can write f(x,y, z)= (x+yy′) (x′+z) using distributive law

= x(x′+z) = xz = x(y+y′) z = xyz+zy′z

The table for above function is given DN from of the function is xyz+xy′z

x	y	z	f(x,y,z)
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

Example: In a Boolean algebra, show that f(x,y) = xf(1, y) +x′f(0,y)

Solution: The complete DN form of f(x,y) is f(x,y) = xy + xy′+x′y+x′y′=x(y+y′)+x′(y+y′) ....(1)

putting x = 1 and therefore x′ = 0, we get f (1, y) = y′

Again putting x = 0 and therefore x′ = 1, we get f(0, y) = y+y′

f(x,y)= x f(1, y) +x′f(0, y) by (1)

Example: Write all 16 possible functions of two variables x and y.

Solution: All possible 16 functions are listed in the following table:

x	y	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1	1	1	1	1	1	0	1	1	1	0	0	0	1	0	0	0	0
1	0	1	1	1	0	1	1	0	0	1	0	1	0	1	0	0	0
0	1	1	1	0	1	1	0	1	0	0	1	1	0	01	0	0	0
0	0	1	0	1	1	1	0	0	1	1	1	0	0	0	0	1	0

Therefore, the 16 functions are:

$f_1 = xy + x'y + xy' + x'y' = 1$, $f_2 = xy+x'y+xy' = x+x'y$

$f_3 = xy+x'y+x'y' = xy+x'$, $f_4 = xy+xy'+x'y' = xy+y'$

$f_5 = x'y+xy'+x'y' = x'y+y'$, $f_6 = xy + x'y = y$

$f_7 = xy + xy' = x$, $f_8 = xy + x'y' = xy + x'y'$

$f_9 = x'y + x'y' = x'$, $f_{10} = xy'+x'y' = y'$

$f_{11} = x'y + xy' = x'y + xy'$, $f_{12} = xy = xy$, $f_{13} = x'y = x'y$

$f_{14} = xy' = xy'$, $f_{15} = x'y' = x'y'$, $f_{16} = 0 = 0$

Check your progress

1. Express each of the following in DN from in the smallest possible number of variables (a). $x + x'y$ (b) $(u+v+w)(uv+u'w)'$
2. Write complete disjunctive normal form in three variables x, y and z. Determine which term equal 1 if (1) $x = 1, y = z = 0$, (b) $x = z = 1$ and $y = 0$
3. Write disjunctive normal form in the three variables x, y and y of the function $f = x + y'$.
4. Write the function f of x, y and z which is 1 if and only if any two or more of the variables are 1.
5. Find, by inspection, the complement of each of the following

   (a) $xy + x'y$, (b) $x'y'z' + x'yz + xy'z'$
6. Prove that there are exactly 2^{2n} distinct functions of n variables in a Boolean algebra.
7. Write and simplify the two functions f_1 and f_2 specified by the table

x	y	z	f_1	f_2
1	1	1	0	1
1	1	0	1	1
1	0	1	0	0
1	0	0	1	0
0	1	1	0	0
0	1	0	0	0
0	0	1	0	0
0	0	0	0	1

Answer

1. (a) $xy + xy' + x'y$ (b) $uv'w + u'vw' + uv'w'$
3. $Xyz + xyz' + xy'z + xy'z' + x'y'z + x'y'z'$
4. $xy + yz + zx$
5. (a) $xy' + x'y'$ (b) $xyz + xyz' + xy'z + x'yz'$
7. $f_1 = xz'$, $f_2 = xy + x'y'z'$

3.11. Conjunctive Normal Form

Conjunctive normal form is a dual of disjunctive normal form. Thus all the results that we proved for DN forms can be extended to this form by duality.

Definition : A Boolean function is said to be in conjunctive normal form (in short, CN form) in n variables $x_1, x_2, \ldots, x_n$, for $n > 0$ if the $f_1(x_1)f_2(x_2)+\ldots+f_n(x_n)$. Where $f_i(x_i) = x_i$ or x_i' for each $i = 1, 2, \ldots, n$, and no two terms are same. Moreover 0 and 1 are also said to be in conjunctive normal form. The terms of the type

$f_1(x_1)+f_2(x_2)+\ldots+f_n(x_n)$, where $f_i(x_i)= x_i$ or x_i' for each $i = 1, 2, \ldots, n$ are called max-terms or maximal polynomials.

Theorem 1 : Every function in Boolean algebra, which contains no constants is equal to a function in E/n form.

Proof : Let f be the Boolean function which contains no constant. If f contains an expression of the form $(x+y)'$ or $(xy)'$ for some variables x and y then De Morgan's rule may be applied to get $x'y'$ and $x'+y'$, respectively. This process may be continued until each′ which appears applies only to a single variable.

Next, by applying the distribution law, f can be reduced to products. Now suppose some term does not contain either x_i oo x_i' for some variable x_i. Then x_ix_i' may be added to this tem without changing the function. Continuing this process for each missing variable in each factors in f will give an equivalent function whose factors contain x_i or x_i' for each i = 1, 2, n. Finally, using aa=a, we can eliminate the duplicate terms and with this the proof is complete.

Example : Write the function $(xy'+xz)'+x'$ in CN form

Solution : Let $f= (xy'+xz)'+x' = (xy')(xz)'+x'$

$=(x'+y)(x'+z')+x' = x'+(x'+y)(x'+z')$

$= (x'+x'+y)\ (x'+x'+z)\ = (x'+y)\ (x'+z')$

$= (x'+y+zz')\ (x'+z'+yy')\ = (x'+y+z)\ (x'+y+z')\ (x'+y+z')\ (x'+y'+z')$

$= (x'+y+z)\ (x'+y+z')\ (x'+y'+z')$

Definition : (Complete conjunctive normal form): The conjunctive normal form in n variables which contains 2^{nd} factors (max-terms) is called complete conjunctive normal form in n variables.

Theorem 2 : Let f be a complete conjunctive normal form in n variable. The exactly one maxterm (factor) will have the value 0 and all other max-terms (factors0 will have the value 1.

Example : Find the Boolean function f in CN form that is given by the following table

x	y	z	f
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	1
0	0	0	0

Solution: To get the expression in CN form, we look at the values of f(x,y,z) when it is 0. We see from the table that f takes value 0 at 2^{nd}, 3^{rd}, 4^{th} and 8^{th} row thus

$f = (x'+y'+z)\ (x'+y+z')\ (x'+y+z)\ (x+y+z)$

Rule for finding complement of a function given in CN form

As in disjunctive normal form, we can use the conjunctive normal form to find complements of functions written in this form by inspection. The complement of any function written in CN form is that function whose factors are exactly those factors of the complete conjunctive normal form, which are missing from the given function.

Example: Find the complement of f= (x+y′) (x′+y)

Solution: The given function f is written in CN form of two variables. The complete conjunctive normal form in two variables is (x+y)(x+y′) (x′+y) (x′+y′)

Therefore the complement of f is (x+y) (x′ +y′)

Example: Find the conjunctive normal form for the function

f=xyz+x′yz+xy′z+x′yz′

Solution: We know that (f′)′ = f ∴ f = [(xyz + x′yz + xy′z′+x′yz′)′]′

=[(xyz) ′(x′yz) ′ (xy′z′)′ (x′yz′)]′ by De Morgain's law

= [(x′+y′+z′) (x+y′+z′) (x′+y+z) (x+y′+z′)]′ by De Morgain's law

= (x+y+z) (x′+y+z′) (x+y+z′) (x′+y′+z)

Check your progress

(1) Express each of the following in CN form in the smallest possible number of variable.(a) x+x′y (b) (u+v+w) (uv+u′w′) (c) (x+y(x+y′) (x′+z)

(2) Write the CN form in three variables x, y anx z (a) x+y′ (b) (x+y) (x′+′)

(3) Write the function of x, y and z which is 0 when any two or more of the variables are 0 otherwise it is 1.

(4) Find by inspection the complement of each of the following

(a) (x+y) (x′+y) (x′+y′) (b) (x+y+z) (x′+y′+z) (x′+y′+z′)

(5) Change the function f = uv + u′v + u′v′ from DN from to CN form

(6) Change the function f = (x+y′) (x′+y) (x′+y) from CN form to DN

(7) Let f $(x_1, x_2, x_3,)$ = $[(x_1+ x_1)' + x_1' x_1']'$ be a Boolean expression (function) over two valued Boolean algebra. Write $f(x_1, x_2, x_3)$ in both DN and CN form.

(8) Write the expression$(x_1, x_2, x_3) = x_1x_1+ x_1x_3+ x_2 x_3$in both DN and CN forms.

(9) Express the function given by the table below in both DN form and CN form

(x_1, x_2, x_3)	$f(x_1, x_2, x_3)$
(0,0,0)	1
(0,0,1)	0
(0,1,0)	1
(0,1,1)	0
(1,0,0)	0
(1,0,1)	1
(1,1,0)	0
(1,1,1)	1

(10) For any Boolean function f(x1, x2), show that

$f(x1, x2)=[\ x1+f(0, x2)][\ x1'+f(1, x2)]$

(11) Simplify the following Boolean function

(a) $ab + abc + bc$ (b) $(ab'+c)\ (a+b'+c)$

Answer

1. (a) $x + y$ (b) $(u+v+w)\ (u+v+w')\ (u+v'+w')\ (u'+v'+w)\ (u'+v'+w')$ (c) $(x+z)\ (x+z')\ (x'+z)$
2. (a) $(x+y'+z)\ (x+y'+z')$ (b) $(x+y+z)\ (x+y+z)\ (x+y+z')\ (x'+y'+z)\ (x'+y'+z')$
3. $(x+y+z)\ (x+y+z')\ (x+y+z')\ (x+y'+z)\ (x'+y+z)$
4. (a) $(x+y')$ (b) $(x+y+z')\ (x+y'+z)\ (x+y'+z')\ (x'+y+z)\ (x'+y+z')$
5. $u'+v$
6. $x'y'$
7. DN form of $f = x_1x_2x_3 + x_1x_2x_3' + x_1x_2'x_3 + x_1x_2'x_3' + x_1'x_2'x_3'$
   CN form of $f = (x_1x_2x_3)\ (x_1x_2x_3')(\ x_1x_2'x_3')$
8. DN form of $f = x_1x_2x_3 + x_1x_2x_3' + x_1x_2'x_3 + x_1'x_2'x_3$
   CN form of $f = (x_1+x_2+x_3)\ (x_1+x'_2+x_3)(\ x_1+x'_2+x'_3)(\ x'_1+x_2+x_3)$
9. $F\ (x_1,x_2,x_3) = (x_1+x_2+x'_3)\ (x_1+x'_2+x'_3)(\ x'_1+x_2+x_3)\ (x'_1+x'_2+x_3)$
10. (a) $ab+ac$ (b) $ac+b'c$

3.12. Minimization of Boolean Functions (Karnaugh Map)

In this section, we shall concern with the problem of obtaining a minimal Boolean function equivalent to a given Boolean function. These problems arise in the design of switching circuits because the cost of the circuit, to some extent, depends on the number of switches in the circuit. The goal of minimization is to reduce to minimum number of switches or gate required by a circuit. A general method of simplifying a Boolean function obtain a minimal form is to use basic laws and identities such as a+ab = a of a Boolean algebra.

Example: Simplifying the Boolean function

$f=ab'+cd+cb+cd'+ac'+a'bc+b'c'd'$

Solution : Here $f = ab'cd+cb+cd'+ac'+a'b\,c'+b'c'd'$

$= (ab'd+b+d')\,c+(a+a'b+b'd')c' = c(b+d'+ab'd)+c'[(a+a')\,(a+b)+b'd']$

using $a+a'b= (a+a')\,(a+b)$

$= c[(b+d'+b')\,(b+d'+ad)]+c'\,[a+b+b'd']$ using distributive law and $a+a'=1$

$= c\,(b+d'+a)\,(b+d'+d)+c'(a+b+b'0\,(a+b+d') =c\,(a+b+d')+c'(a+b+d')$

$\because d+d'1,\ b+b'=1\ =a+b+d'$

Form the above, it is clear that the choice of which Boolean laws to use in any particular simplification operation is primarily determined by the skill of the person performing Bolean manipulations and this skill is partly a matter of experience. Because of this difficulty in reducing a Boolean functions to its simplest (minimal) form, a method base on Karnugh maps has been developed.

Karnaugh Maps : The Karnaugh map is a pictorial representation of truth table of the Boolean functions. This method is easy to use when Boolean function has six or fewer variables. Since function of one variable can be simplified easily, there is no need to illustrate it. We illustrate the method when number of variables in a function is 2, 3 and 4.

Case of two variables :

We consider the case when the Boolean function f is of two variables, say x and y, in the first figure below, we have constructed a 2×2 matrix of squares with each square containing one possible input combination of variable x and y. The Karnaugh map of the function is the 2×2 matrix obtained by placing 0s and 1s in the square according to whether the functional value is 0 or 1 or the input combination associated with that square. For example, the Boolean function $f=xy+x'y$ is represented by the Karnaugh map as shown I second figure below

	x	x′
y	xy	x′y
y′	xy′	x′y′

	x	x′
y	1	1
y′	0	0

Karnaugh map of $f=xy + x'y$

We now consider the method to obtain minimal form of the function by using Karnaugh map. The application of the Boolean law $xy+x'y=x$, when seen in the context of a Karnaugh map, becomes the replacement of two adjacent squares (squares having one side in common) containing 1s by a rectangle containing two squares. The absorption law $x+xy =x$ has its counterpart on a Karnaugh map as well. It is simply the grouping of adjacent squares into the largest possible rectangle of such squares and we still use the largest rectangle instead of individual squares. Of find minimal form of the function, we first consider all largest rectangles composed of the adjacent squares with 1s in them. From the set of these largest rectangles, the minimum number of rectangles are taken such that every square with 1 is part of atleast one such rectangle.

Example: use the karnaugh map method to find a minimal DN form (sum of products form) of the following functions

(a) $f(x, y) = xy + xy'$

(b) $f(x,y) = xy + x'y+x'y'$

(c) $f(x,y) = xy +x'y'$

Solution: (a) We first represent f(x, y) by a Karnaugh map. The Karnaugh map representation of $f(x, y) = xy = xy'$ is the following

	x	x′
y	1	0
y′	1	0

We have represented two adjacent squares with 1s in them by a rectangle. This rectangle represents x, Hence $f(x,y) = x$.

(b) The representation of f(x,y0=xy+x'y+x'y' by Karnaugh map is as follows:

	x	x'
y	1	1
y'	0	1

The function f(x,y) contains two pairs of adjacent squares with 1 (indicated by two rectangles) which includes all the squares of f(x,y) which contain 1. The horizontal pair (rectangle) represents y and vertical pair (rectangle) represents x′, Hence.

$f(x,y)= y+x'=x'+y$ is its minimal form.

(c) The Karaugh map representation of $f(x, y)=xy+x'y'$ is given below

	x	x'
y	1	0
y'	0	1

Observe that f(x,y) consider of two rectangles as shown in the figure. Thus $f(x,y) = xy+x'y'$ is the minimal form.

Case of three Variables

We now turn to the case of a function of three variables, say x, y and z. The Kanaugh map corresponding to Boolean functions f(x, y, z0 is shown in figure 3(a)

	xy	xy′	x′y′	x′y
z				
z′				

Fig. 3(a)

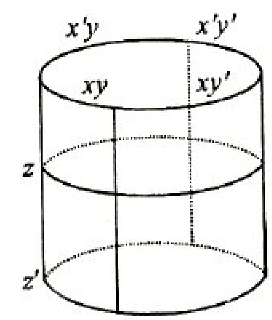


Fig. 3(b)

In figure 3(a), each square represents the minterm corresponding to the column and row intersecting in that square. In order that every pair of adjacent product in figure 39a) are geometrically adjacent, the right and left edge of the must be identified. This is equivalent to cutting out, bending and gluing the map along the identified edge to obtain the cylindrical figure as shown in figure 3(b), by a basic rectangle in Karnaugh map with three variables, we mean a square, two adjacent squares or four squares which form 1×4 or a 2×2 rectangle.

Suppose that the Boolean function f(x,y,z) has been represented in the Karnaugh map by placing 0s and 1s in the appropriate squares. A minimal form of f(x, y, z0 will consist of the least number of maximal basic rectangles (a basic rectangle which is not contained in any larger basic rectangle) of f which together include all the squares with 1 (in them) of f.

Example: Find using Karaugh maps a minimal form for each of the following Boolean functions

(a) f(x, y, z) = xyz + xyz′ + x′yz′+ x′y′z′

(b) f(x, y, z) = xyz + xyz′ + xy′z+x′yz+x′y′z

(c) f(x, y, z) = xyz + xyz′+xy′z′+x′y′z′+x′y′z

Solution: (a) The Karnaugh map corresponding to the given function is given below

	xy	xy'	$x'y'$	$x'y$
z	1	0	1	0
z'	1	0	0	1

From the Karnaugh map, we see that f(x, y, z) has three maximal basic rectangles containing squares with 1 which are shown by rectangles. Observe that squars corresponding to xyz′ and x′yz′ are adjacent. Thus the symbols are left open ended to signify that they join in one rectangle. The resulting minimal Boolean function is xy+yz′+x′y′z

(b) The Karnaugh map corresponding to the function f=xyz+xyz′+xy′z+x′yz+x′y′z

is given below which has five squares with 1s in them corresponding to the five

	xy	xy'	$x'y'$	$x'y$
z	1	1	1	1
z'	1	0	0	0

miniterms of f.

From the Karnaugh map, we see tht f(x, y, z) has two maximal basic rectangles containing all the squares with 1, which are shown by rectangles. One of the maximal basic rectangle is the two adjacent squares which represents xy and the other is the 1×4 square which represent z. Both are needed to cover all the squares with 1. So, the minimal form of f(x,y,z) is given by f(x,y,z) = xy +z

(c) The Karnugh map corresponding to the function

f(x,y,z) = xyz + xyz′+x′yz′+x′y′z′+x′y′z is given below which has five squares with 1s in the corresponding to the five minterms of f.

	xy	xy'	$x'y'$	$x'y$
z	1	0	1	0
z'	1	0	1	1

As shown by the rectangles, f (x, y, z) has four maximal basic rectangles. To cover all squares with 1s in them, it is necessary here to include basic rectangles which represent xy and x′y′ and only one of two rectangles which correspond to x′z′ and yz′. Thus f(x, y, z) has two minimal forms: f (x, y, z) xy + x′y′+x′z′

and f (x, y, z) = xy + x′y′ + yz′

Case of four variables :

The Karnaugh map corresponding to Boolean function f(x, y, z, w) with four variables x, y, z and w is shown below. Each of the 16 squares corresponds to one of the 16 min-terms with four variables xyzw, xyzw′,….,x′yz′w

	xy	xy'	$x'y'$	$x'y$
zw				
zw'				
$z'w'$				
$z'w$				

Here again, we consider the first and last column to be adjacent and the first and last rows to be adjacent, both by wrap around.

A basic rectangle in a four variable Karnaugh ma is a square, two adjacent squares, four squares which form a 1×4 or 2×2 rectangle or eight squares which form a 2× 4 rectangle. The minimization technique for a Boolean function f(x, y, z, w) is the same as for three variables function.

Example: Use Karnaugh maps to find a minimal form for the following Boolean functions

(a) $f(x, y, z, w) = x'yzw + xy'zw' + x'y'zw' + xyz'w' + xy'z'w'$

(b) $f(x, y, z, w) = xy' + xyz + x'y'z' + x'yzw'$

Solution: (a) The Karnaugh map representation of the given function is shown below which has five squares with 1s in the corresponding to the five minterms of f

	xy	xy'	$x'y'$	$x'y$
zw	0	0	0	1
zw'	0	1	1	0
$z'w'$	1	1	0	0
$z'w$	0	0	0	0

in the corresponding to the five min-terms of f. A minimal cover of all 1s of the map consists of the three maximal basic rectangles as shown in the figure. Thus the minimal form is $f(x, y, z, w) = y'zw' + xz'w' + x'yzw$

(b) The Karanugh map representation of the given function is shown below. Observe that there are four squares with 1s in them representing xy'. Similarly, there are two squares with 1 representing xyz and so on

	xy	xy'	$x'y'$	$x'y$
zw	1	1		
zw'	1	1		1
$z'w'$		1	1	
$z'w$		1	1	

The minimum number of maximal basic rectangles to cover all 1s of the map is 3 as shown in the figure. Thus the minimal form is $f(x, y, z) = xz + y'z' + yzw'$

observe that the upper left 2×2 rectangle represent xz while the other 2×2 rectangles represents $y'z'$.

Example: Use a Karnaugh map to find a minimal form of the function

$f(x, y, z, w) = xyzw + xyzw' + xy'zw' + x'y'zw + x'y'zw'$

Solution: The Karnaugh map of the given function is shown below

	xy	xy'	$x'y'$	$x'y$
zw	1	0	1	0
zw'	1	1	1	0
$z'w'$	0	0	0	0
$z'w$	0	0	0	0

As shown by the rectangles, f(x, y, z, w0 has four maximal basic rectangles of 1×2 size. To cover all 1s, it is necessary to include basic rectangles which represents xz and $x'y'z$ and only one of the two dotted rectangles which cover 1 at the square corresponding to $xy'zw'$. Hence we obtain two minimal forms, namely

$f(x,y,z,w) = xyz+x'y'z+xzw'$ and $f(x, y, z, w) = xyz + x'y'z+y\,zw$.

Check your progress

1. Describe the Karnaugh maps for three and four variables.
2. Use the Karnaugh map representation to find a minimal form of each of the following functions: (a) $f(x,y) = x'y + xy$

(b) $f(x, y, z) = xyz + xy'z + x'yz + x'y'z$

(c) $f(x, y, z) = xyz' + xy'z + x'y'z' + x'y'z' + x'yz+x'yz'$

3. Use the Karnaugh map to find a minimal form of each of the following functions:
   a. $f = xyz'w'+xyz'w+xyz'w+xy'zw'+x'y'zw+x'y'zw'+x'yw'z'$
   b. $f = xyzw'+xy'zw'+xy'z'w'+xy'z'w+x'y'zw+x'y'zw'+x'y'z'w'+x'yz'w'$
4. Find the minimal form of the Boolean function of four variables represented by the Karnaugh map given below:

	xy	xy′	x′y′	x′y
zw	1	0	0	1
zw′	0	0	0	0
z′w′	0	0	0	0
z′w	1	0	0	1

Answer

2. (a) $f = y$ (b) $f = z$ (c) $f = z' + x'z$

3. (a) $f = y'z + xyz' + yz'w'$ (b) $f = xzw' + xy'z' + x'y'z + x'z'w$ (4). $f = yw$

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983) Topic in Algebra, Vikas publishing house Pvt. Ltd.

Unit - 4

Unit – 04 Switching Circuits and Logic Circuits

Structure

4.1. Introduction

This is most basic unit of this block as it introduces the concept of statements, statements, statement variables and the five elementary operations and associated logical connectives. We introduce the well formed statement formulae, tautologies and equivalence of formulae. The law of duality is explained and established. It has got tremendous application in almost every field, social, economy, engineering, technology etc. In computer science concept of logic is a major tool to learn to understand it more clearly. Mathematics has a language of its own like most other sciences, which is very precise and communicates just what is required-neither more nor less. Language basically consists of words and their combinations called 'expression' or 'sentences'. However in Mathematics any expression or statement will not be called a 'sentence'.

4.2. Objectives

After reading this unit we should be able to

1. Understand the concept of statement and statement variables
2. Use elementary operations like Conjunction, Disjunction, Negation, Implication, Double implication

3. Understand statement formulae, tautologies to equivalence of formulae

4. Use law of duality and functionally complete set of connectives

Logic is a field of study that deals with the method of reasoning Logic provides rules by which we can determine whether a given argument or reasoning is valid (correct) or not. Logical reasoning is used in Mathematics to prove theorems. In computer science logic is used to verify the correctness of programs.

One of the major applications of Boolean algebra is to the switching circuits (an electrical network consisting of switches) that involve two-state devices. The simplest example of such a device is a switch or contact. The theory introduced here holds equally well for such two state devices as rectifying diodes, magnetic cores, transistors, various type of election tubes etc. With the advent of computers, the algebra of circuits is receiving more attention because of the significant use of Boolean algebra in the design and simplification of complex circuits which are involved in electronic computers, dial telephone switching system etc.

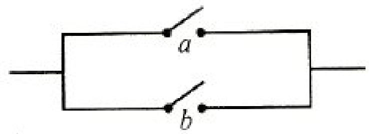
4.3. Switching Circuits

By a switch we mean a contact or a device which permits or stops the flow of

electric current.The switch can assume two state 'closed' or 'open' (ON or OFF).When the switch is closed the current flows in the circuit.When the switch is open current does not flow. We will sue a, b, c…. x, y, z …. etc to denote switches in a circuit. If two switches operate so that they open and close simultaneously we denote them by the same letter. Again, if two switches be such that one is open if and only if the other is closed, we represent them by a and a'.There are two basic ways in which switches are generally interconnected. These are referred to as 'in series' and in 'parallel'.

Definition 1 : Two switches a and b are said to be connected 'in series' if the current flows only when both are closed and current does not flow if any one or both are open.Two switches a and b connected in series a circuit is denoted by ab and is represented as shown in the following diagram.

Definition 2 : Two switches a and b are said to be connected in parallel if current flows when any one or both are closed and current does not flow when both are open. Two switches a and b connected in parallel in a circuit is denoted by a+b and is represented as shown in the following diagram:



We assign the value 1 to a switch which is always closed and the value 0 to a switch which is always open. If two switches a and a′ both open then a is 1 if and only if a′=0

Theorem: The algebra of switches is a Boolean algebra.

Proof: We know that the set B = {0, 1} with operations +, · and ′ defined by the following tables for ns a Boolean algebra of two elements

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

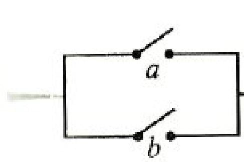
a	a′
0	1
1	0

Consider the following correspondence between the element and operations of the switching algebra and the Boolean algebra B of two elements described above.

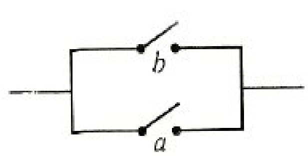
Boolean algebra of x	x′	x	+	·	0	1
	↕	↕	↕	↕	↕	↕
Switching algebra	x	x′	connected in parallel	connected in series	open	closed
			(+)	(·)		

With the help of this correspondence, every series-parallel circuit corresponds to a Boolean function and conversely every Boolean function corresponds to a circuit. Two circuits S_1 and S_2 are defined to be equivalent if both are open (current does not pass through either) or both are closed (current passes through both) for any given position of switches involved. We now verify that switching algebra satisfies all the axioms of Boolean algebra.

[B_1] **Commutative laws:** since circuits are equivalent, we have a+b=b+a

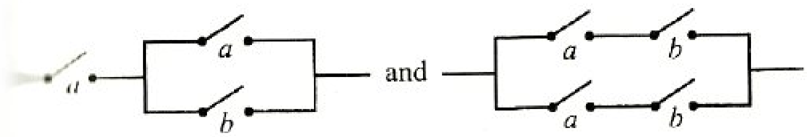


and

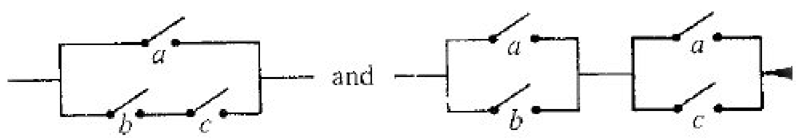


similarly, circuits are equivalent, we have $a \cdot b = b \cdot a$

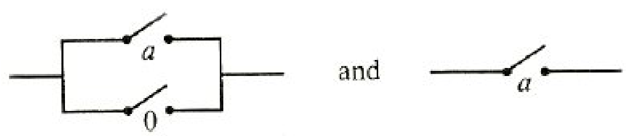
[B_2] **Distributive laws :** Since circuits



are equivalents, we have $a.(b+c) = ab+bc$. Similarly, we have, $a+b \cdot c = (a+b) \cdot (a+c)$ because both circuits are equivalent



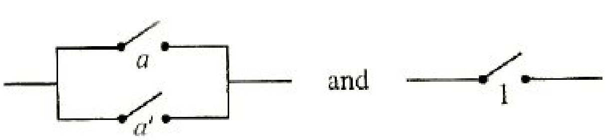
[B_3] **Identity laws:** Since circuits



Where 0 represents a switch which is always open, are equivalent therefore, we have, $a+0=a$. Similalry, circuits where 1 denotes a switch which is always closed,

are equivalent. Thus $a, 1=a$

[B_4] **Complement laws:** Since the circuits are equivalent, we have $a+a'=1$.

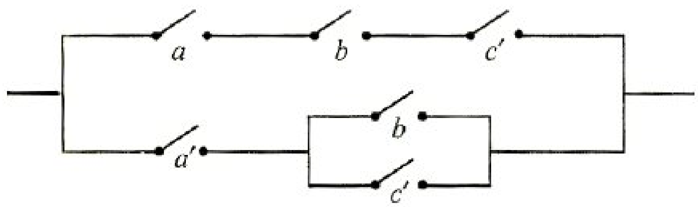


Similarly, the circuits are equivalent, we have $a+a'=1$

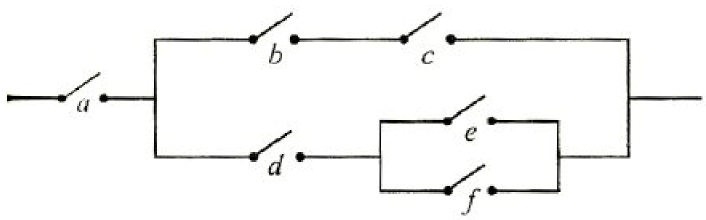
Thus algebra of switches is a Boolean algebra. In view of the above theorem, all results of Boolean algebra can be applied to switching algebra.

Example : Draw a circuit which realizes (represents) the Boolean function $f=abc'+a'(b+c')$

Solution : The circuit is given by the diagram

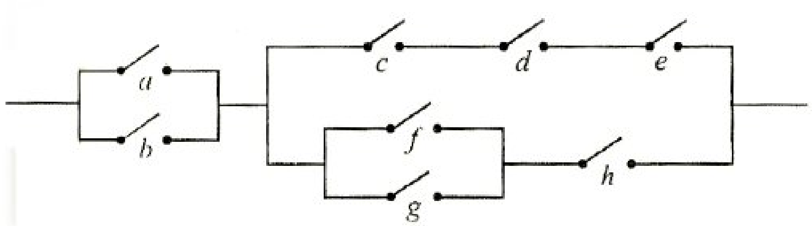


Example 6.2 : Find the function that represents the circuit



Solution : The function f which represents the circuit is given by $f = a\,(b\,c+d(e+f))$

Example : Find the function that represents the circuit and hence find a circuit



which would be open (closed) if and only if the above circuit is closed (open).

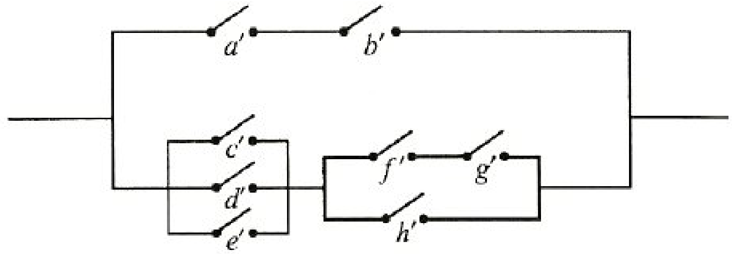
Solution : The given circuit is represented by function $f= (a+b)(cde+(f+g)h)$

The required circuit which will be open if and only if the given circuit is closed will be given by the complement of f. Now,

$f' = [a+v)\,(cde + (f+g)\,h)]' =(a+b)'+[cde+ (f+g)\,h]'$

$= a'b'+ (c'+d'+e')\,[(f+g)g'+h'\,] = a'b'+(c'+d'+e')\,[f'\,g' + h']$

Thus the required circuit is the following



Example : Constructthe tale for closure properties for the functioin f= x'z+z(x+y')

Solution : A table of closure properties for a function is identical to a truth table for a propositional function. Therefore, the table of closure properties for the function f = x'z+z(x+y') is given below

x	y	z	x'y	x+y'	z(x+y')	x'y+z(x+y')
1	1	1	0	1	1	0
1	1	0	0	1	0	0
1	0	1	0	1	1	1
1	0	0	0	1	0	0
0	1	1	1	0	0	1
0	1	0	1	0	0	1
0	0	1	0	1	1	1
0	0	0	0	1	0	0

Check your progress

1. Draw circuits which realize each of the following expressions without simplifyi the expression.

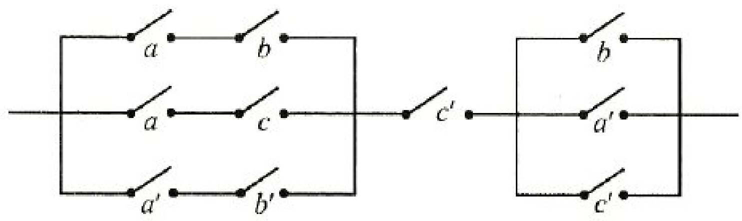
   (a) abc + a (dc + ef)

   (b) (+b′ +c) (a+bc′) + c′d+d(vb′+c)

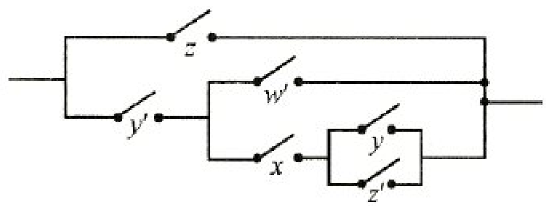
   (c) x[y (z+w) + z(u+v)

2. Find the functions which represent each of the circuits given below

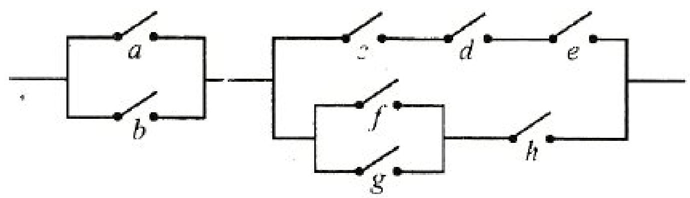
(a)



(b)



3. Find a circuit which is closed when the following circuit is open and open when the given circuit is closed.

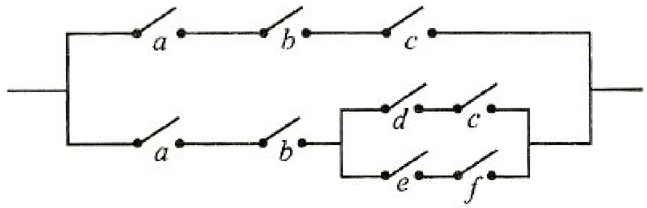


4. Find circuits which realize each of the functions given in the following table

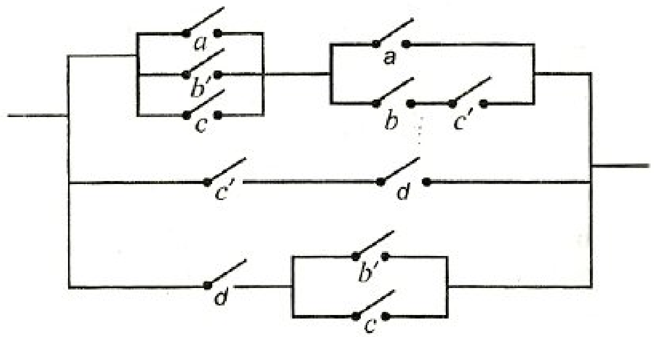
x	y	z	f_1	f_2	f_3
1	1	1	0	1	1
1	1	0	1	0	1
1	0	1	1	0	0
1	0	0	0	1	1
0	1	1	0	1	1
0	1	0	0	1	0
0	0	1	0	0	0
0	0	0	1	1	0

Answers

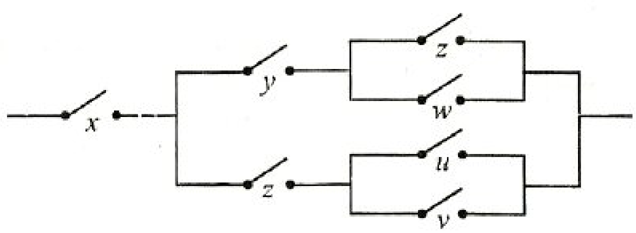
1(a)



(b)

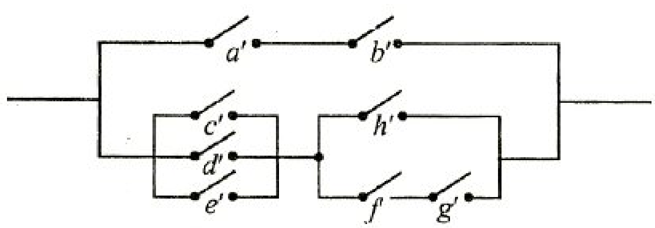


(c)

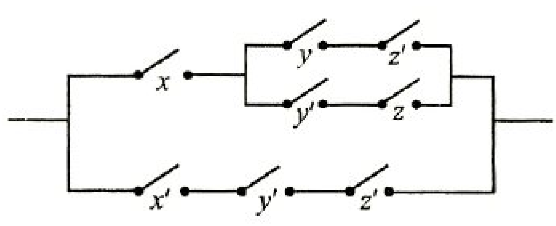


2. (a) $(ab+ac+a'b')c'(b+a'+c')$ (b) $z + {}' [w'+x\,(y+z')]$

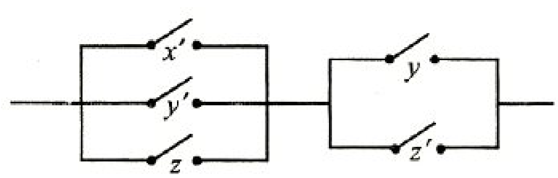
3

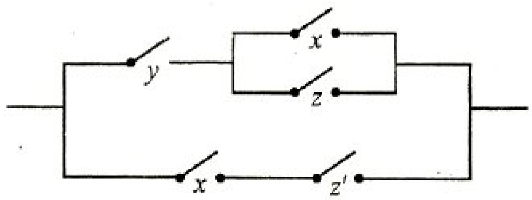


4 Circuit for f_1 is



Circuit for f_2 is



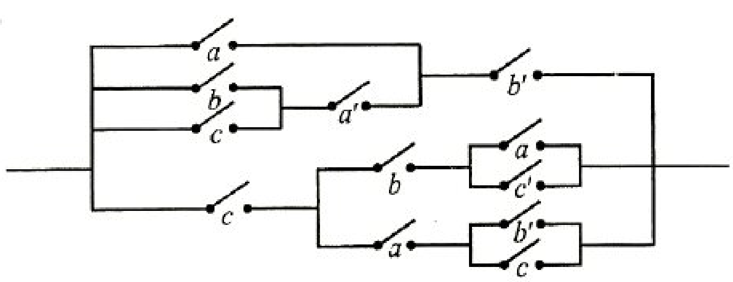
Circuit for f_3 is 

4.4. Simplification of circuit

We have seen in last chapter that Boolean expression can be simplified by algebraic method using Boolean theorems. Since algebra of circuits (net work) is a Boolean algebra, we can use theorems and rules of Boolean algebra in algebra of circuits also. But the drawback of this technique is that there are no specific rules for proceeding step by step to manipulate the process of simplification. Even if minimum is obtained, one may not be sure that it is minimum. Another method is the Karanaugh map method which provieds a simple straight forward technique of simplification of Boolean functions. The simplification is essential to minimize the cost of the circuit. By simplification of a given circuit we mean a circuit which is equivalent to the given circuit and which has fewer switch.

A general method of simplifying a circuit is first to find the Boolean function which represent the circuit, then to simplify the function by the Karnauh map method and finally to draw a new circuit diagram realizing the simplified function.

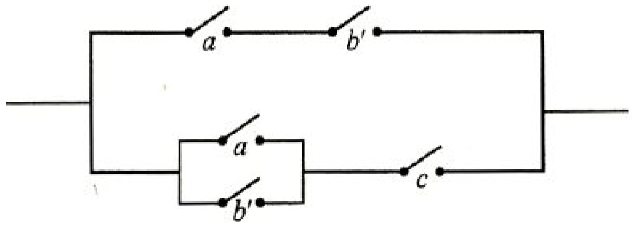
Example: Simplify the circuit



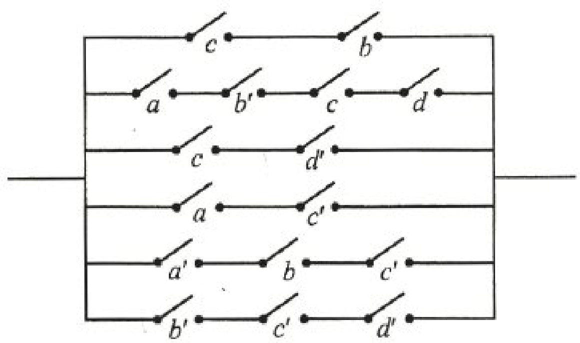
Solution: The Boolean function f representing the given circuit is
$f = [a + (b + c)a']\, b' + c[b\,(a + c') + a(b' + c)] = ab' + a'b'c + abc + ab'c + ac$
The Karnaugh map corresponding to f is

	ab	ab'	$a'b'$	$a'b$
c	1	1	1	
c'		1		

The simplified function is $f = ab'+ac+b'c$. This expression is the minimal sum of products. The circuit corresponding to this form will contain 6 switches. But if it is expressed as $f = ab'+(a+b')c$ then the corresponding circuit will contain five switches. Thus we see that we have to see both forms of the simplified expression before constructing the circuit. Hence we get the following circuit.



Example: Simplifying the circuit given below –

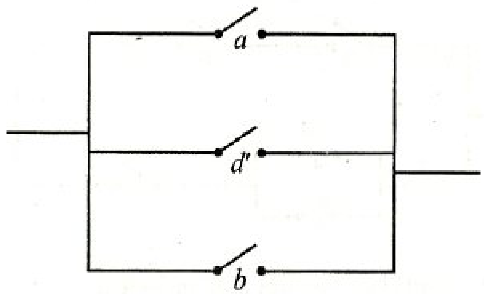


Solution: The circuit is represented by the function

$f = bc + ab'cd + cd' + ac' + a'bc' + b'c'd'$

	ab	ab'	$a'b'$	$a'b$
cd	1	1	0	1
cd'	1	1	1	1
$c'd'$	1	1	1	1
$c'd$	1	1	0	1

The function contains four variables. The Karnaugh map of f gives (to find simplified form of f). There are three basic rectangles each of the type 2×4. The simplified functions $f = a+d'+b$. Hence the simplified circuit is



Note: Karnaugh map method can also be used find function in product of sums form. For this we have to consider squares with 0 in them only. Consider the Karnaugh map shown in example 6.6 above. The entry in square at 1st row and 3rd row column will be zero if a+b+c'+d=0. Similarly, the sum term for the 4th row and 3rd column will be a+b+c+d'. The two squares with 0 in them have common variables a, b and d'. The simplified function is (a+b+c'+d')(a+b+c+d') = a+b+d'

Don't Care Condition

Boolean functions describe the behavior of circuits. Each square of a Karnaugh map represents the output of the circuit corresponding to a combination of values of the input variable. Sometimes it happens that certain input combinations never occur. In such situations the output of the circuit network, is not specified. These situations are referred to as don't care condition. The square on the Karnaugh map corresponding to a don't care conditions is indicated by – or × and such square is known as don't care square. A don't care square may be assumed either as a square with 1 or a square with0 as desired while forming the basic rectangles for simplification. Any one of such squares or some of them may be included or may not be included while forming basic rectangles.

Example: Suppose a circuit is defined by the following table where × denotes don't care condition. Draw the circuit as simplified as possible

x	*y*	*z*	*f(x,y,z)*
0	0	0	1
1	0	0	1
0	1	0	0
0	0	1	×
1	1	0	0
1	0	1	1
0	1	1	0
1	1	1	0

Solution: We can directly represent the function f given by the table in Karnaugh map as follows –

	xy	xy′	x′y′	x′y
z	0	1	×	0
z′	0	1	1	0

$$f = xy' + z'z'$$

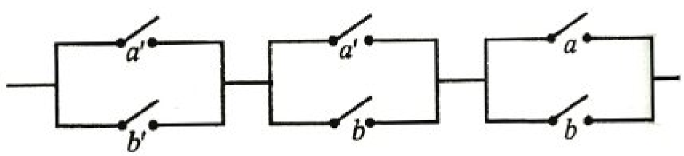
But if we take 1 in the don't care square then we have one basic rectangle of the type 2×2 and the corresponding Boolean function will be f = y′

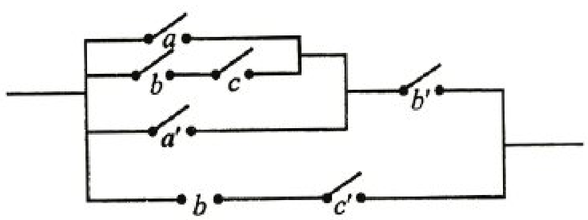
Hence simplified circuit is 

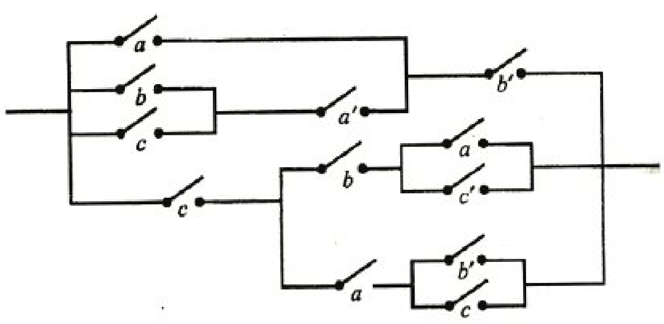
Thus the addition of don't care condition has made our circuit simpler.

Check your progress

1. Simplify the following circuits:

(a) 

(b) 

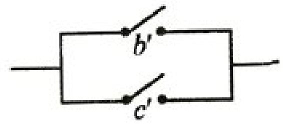
(c) 

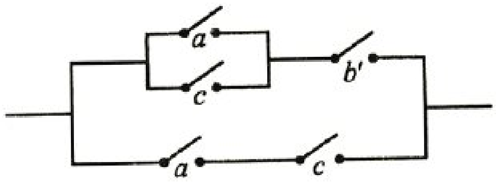
2. Suppose that we have a circuit defined by the function f = a(b′+c) + a′b′c′

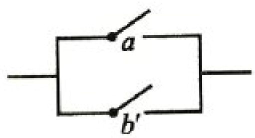
Suppose further that abc′ and a′b′c′ are impossible to occur. Draw the circuit with least switches.

Answer

1(a) 

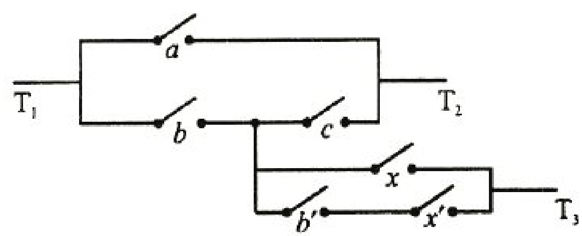
(b) 

(c) 

2 

4.5. Non-Series Parallel Circuits

In the previous sections, we have discussed circuits which have two terminals. Such circuits are called 2-terminal circuits. We now study the concept of n-terminal circuits. The following diagram shows a 3- terminal circuits.

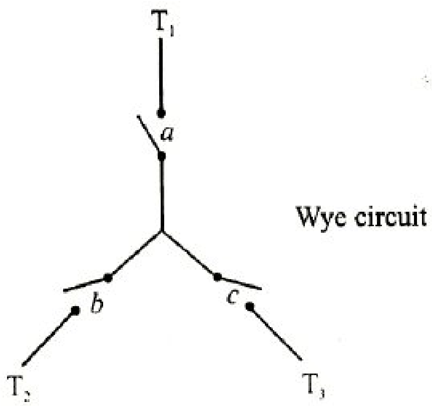


This circuit is a combination of three 2-termainal circuits joining terminal points T_1 and T_2, T_2 and T_3, and T_1 and T_3. The Boolean function corresponding to the 2-terminal circuit joining terminals T_i and T_j will be denoted by f_{ij} for each i and j, where $i \neq j$. In general, an n-terminal circuit can be defined as a configuration of switches connected by wire in which n points are designated as terminals. The $n(n - 1)/2$ possible Boolean functions corresponding to the 2 terminal circuit joining T_i to T_j for each i and j, $i \neq j$, will be denoted as f_{ij}.Two n-terminal circuits are said

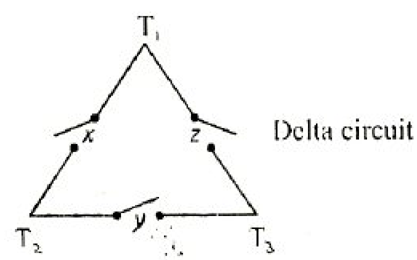
to be **equivalent** if each pair of 2 terminal circuits are equivalent or, as well as,

if the functions representing the pairs of corresponding circuits are equal.

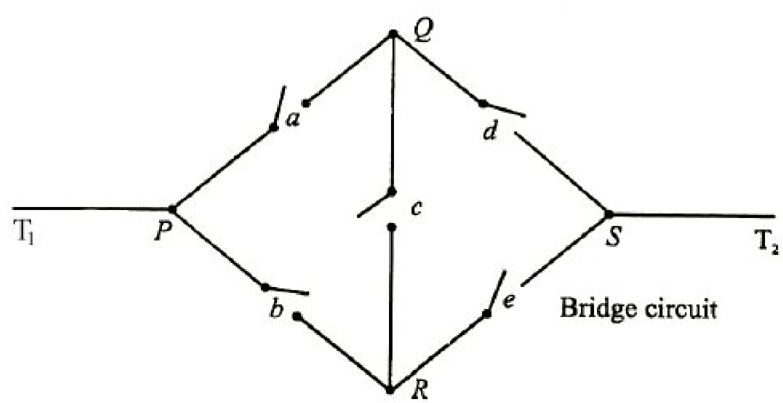
wye Circuit: A -3terminal circuit is said to be a wye circuit if the three 2-terminals circuits involved have common point other than a terminal. Such a circuit is called wye circuit because of its resemblance with the letter y.



Delta Circuit : A 3-terminal circuit in which they only common point of any pair of the three 2-terminal circuits are the three terminals, each of which is common to exactly two of the terminal circuits is known as delta circuit.

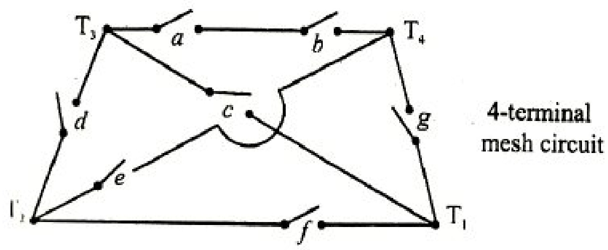


Bridge Circuit: A non-series-parallel circuit of the type shown below is known as bridge circuit. The vertices of the circuit are labeled with capital letters for reference. The point Q is the central point of a wye circuit with terminals P, R, and S.

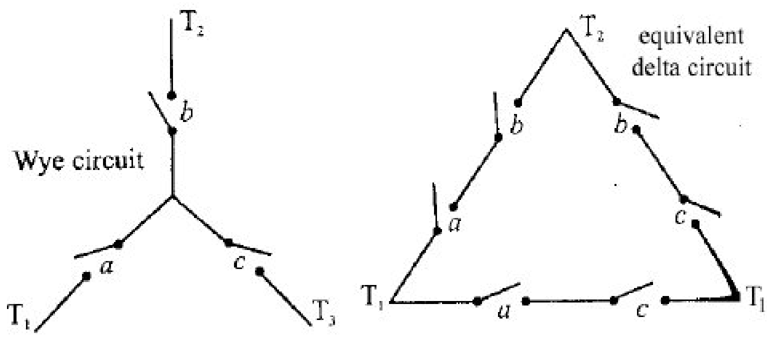


Star Circuit: An n-terminal circuit is said to be a start if it has a common central point other than the terminal points. Clearly start circuit is a generalization of wye circuit.

Mesh Circuit: An n-terminal circuit is called a mesh if in this circuit only common points of any pair of $\frac{1}{2}$n(n- 1), 2-teminal circuits are the terminals only, each of which is common to exactly (n – 1) 2-terminal circuits. If n = 3, then mesh circuit is simply a delta circuit.

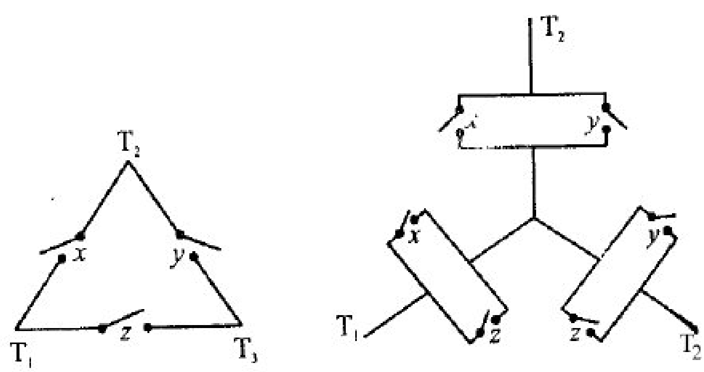


Why-to-delta and delta-to-wye Transformation: As in ordinary circuit theory, there exist wye-to-data and delta-to-wye transformation. We introduce these transformations to develop a method for reducing a non-series-parallel circuit to an equivalent circuit of series-parallel type. The wye-to-delta transformation is shown below:



Wye-to-delta transformation

Clearly, wye-to-delta transformation gives an equivalent 3-terminal since 2-terminal circuits formed in each case are series connections of the same pair of switches. A delta-to-wye transformation is given below.

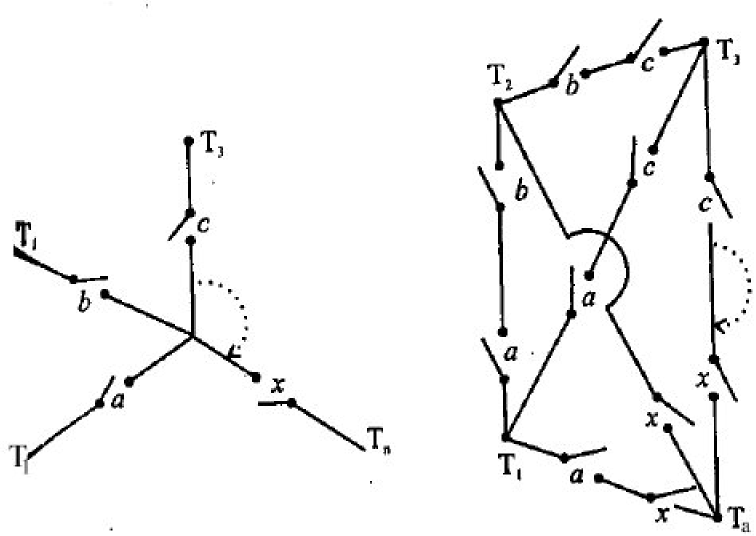


Delta-to-wye transformation

Now to see that the circuits in figure (b) above are equivalent to the circuits in (a), we note that the 2-terminal circuit from T_1 to T_2 in (b) is nothing but the circuit given by the Boolean functions. (x+z) (x+y) which is equivalent to the function

x+yz in view of the distribution law. Note that circuit from T_1 to T_2 in figure (a) is given by x + yz. Similarly, we can check the other two circuits.

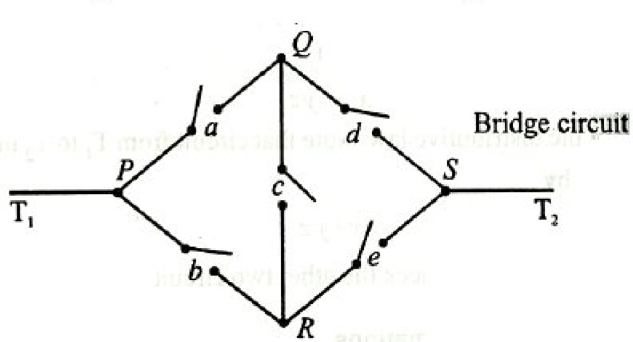
Star-to- Mesh Transformation: Star and mesh circuits are generalizations of wye and delta circuits respectively. Therefore wye-to-delta and delta-to-wye transformation may be generalized to a star-to-mesh and mesh-to-star transformation respectively. Figure below suggest the method employed.



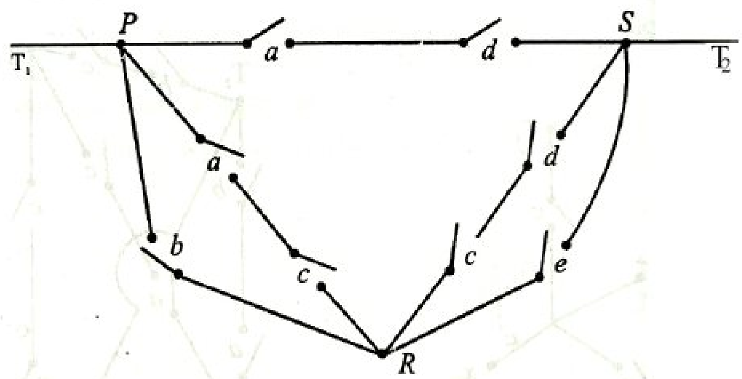
Start-to-mesh transformation

To find series-parallel circuit equivalent to a bridge circuit

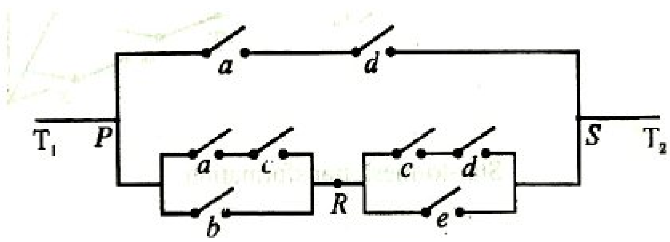
We can use wye-to-delta transformation to obtain a Boolean function to represent the bridge circuit (which is not a series parallel circuit) to represent the bridge circuit) given below and thus obtain a series parallel circuit which is equivalent



to the given bridge circuit. Consider the bridge circuit given above. The point Q can be taken as central point of a wye circuit with terminals P, R and S. applying the wye-to-delta transformation we get an equivalent circuit shown below:



We can redraw this circuit as sows below



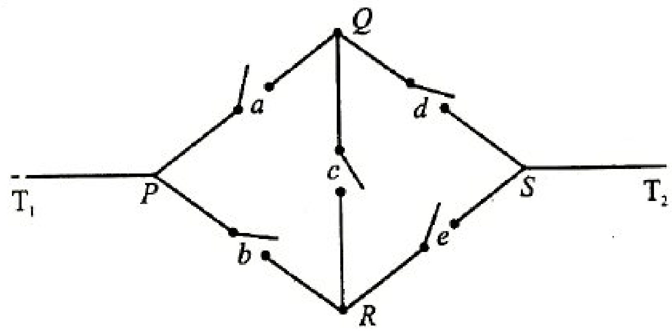
From this figure, it follows that the given bridge circuit is represented by the Boolean function f = ad + (ac + b) (cd+e)

Conversely, any Boolean function of the form f= ad + (ac + b) (cd + e)

can be realized by a bridge circuit. For this, we first locate the delta circuit and then transform it into a wye circuit.

Alternative method: We now explain two alternative methods of obtaining the Boolean function for a circuit. These methods are eaiser to use in simple cases but have the disadvantage of being essentially trial and error methods and hence error may occur in complicated cases.

The first of these methods consosits of examining the circuit for all possible combinations of closed switches which allow a current through the circuit. To illustrate the method we consider again the bridge circuit.



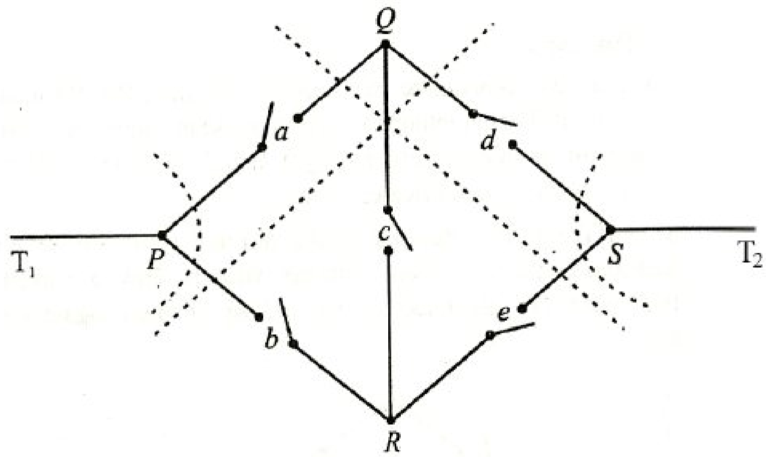
From the circuit it is clear that there are only 4 possible paths from T_1 to T_2, namely T_1 – P – Q – S – T_2, T_1 – P – Q – R – S T_2,

T_1 – P – R – Q – S – T_2, and T_1 – P – R – S – T_2,

through which current can flow from T_1 to T_2.These paths corresponds to the comination ad, ace, bcd and be. Hence the required Boolean function is

$$f = ad + be + ace + bcd$$

The second alternative method is to consider all ways in which the circuit ma be broken (by a combination of open switches)

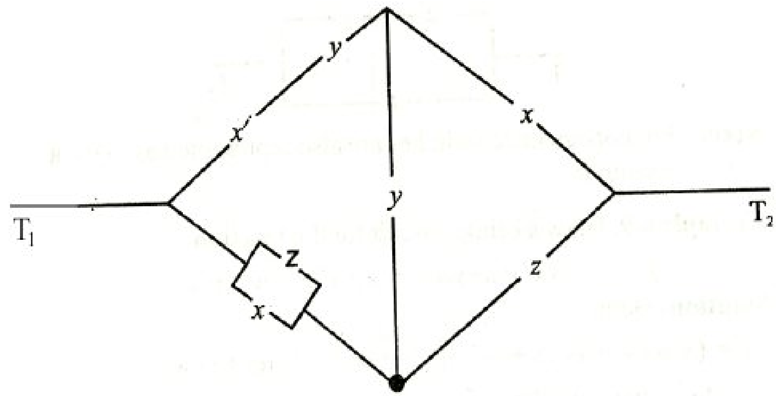


In this method, broken lines are drawn in all possible ways in which the circuit may be broken as shown above. These combinations are a and b, a, c and e, b, c and d, and d and e. Now the required Boolean function is given by

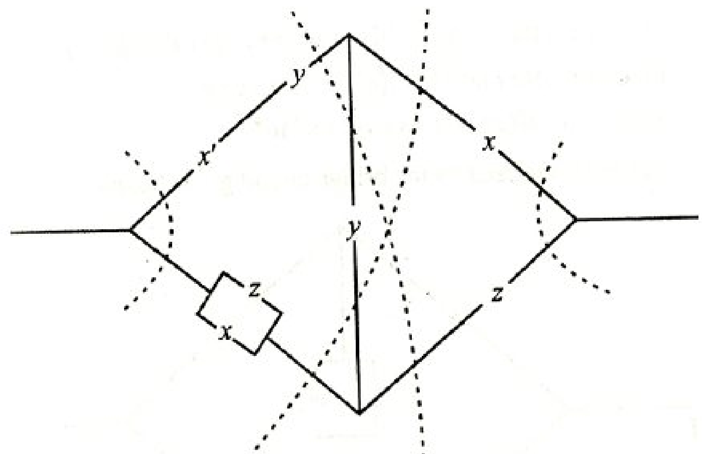
$$f = (a+b)\,(a+c+e)\,(b+c+d)\,(d+e)$$

which has the value 0 if any of the four sets of switches is open. It can be easily seen that the three Boolean functions ad + (ac+b) (cd+e). ad+be+bcd and (a+b) (a+c+e) (b+c+d) (d+e) are equivalent.

Example: Simplify the circuit given below



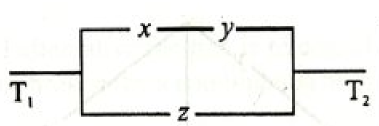
Solution: We draw broken lines though the circuit in all possible ways in which the circuit could be broken by a combination to open switches as shown below :



Now we can write the Boolean function f representing this circuit:

$f = (x'y + x+z)\ (x+z)\ (x'y+y+z)\ (x+z+y+z)\ = (x'y+z+xy)\ (x+z)$

$= (y+z)\ (x+z) = xy+z$. Therefore, the circuit equivalent to the given circuit is



Note: For convenience switches are also represented as in the above example.

Example : Draw a bridge circuit for the function

$f = (x'u+x'v'\ s+yu+yv's)\ (x'+z+w'+v's0(y+z+w'+u)$

Solution: here, $f = (x'u+x'v's+yu+yv's0\ (x'+z+w'+v''(y+z+w'+u)$

$= (x'+y)\ (u+v's)\ [z+w'+(x'+v's)\ (y+u)]$

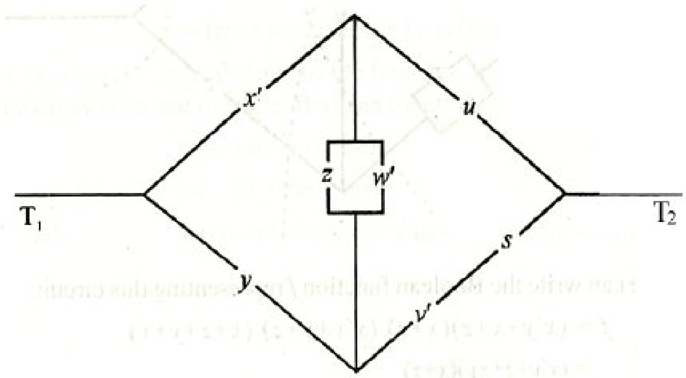
$=(x'+y)\ (u+v's)\ (z+w') + (x'+z)\ (\ x'+v's)\ (\ u+v's)\ (y+u)$

$=(x'+y)(u+v's)(z+w')+(x'+yv's)(u+yv's)=(x'+y)(u+v's)(z+w')+(x'y+yv's)$

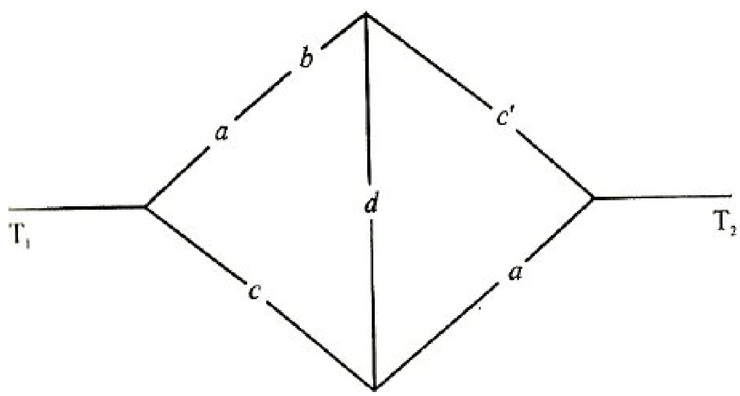
$=(x'u+yv's)(z+w')+(x'v's+yu)(z+w')+(x'u+yv's)$

$=(x'u+yv's)(z+w'+1)+(x'v's+yu)(z+w')=x'u+yv's+x'(z+w')v's+(z+w')u$

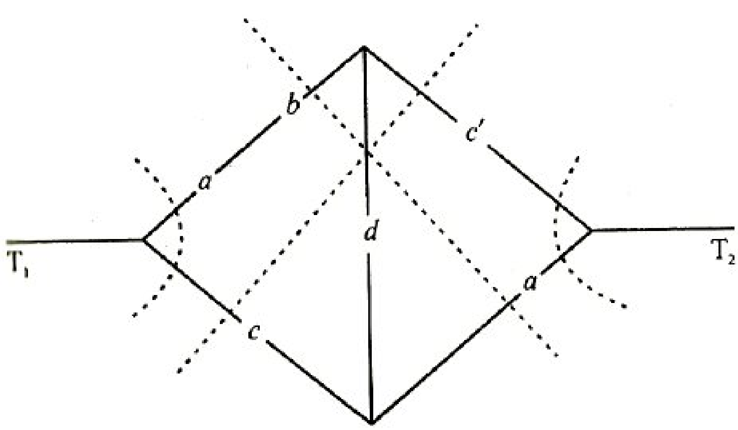
Hence f is realized by the bridge circuit given below



Example: find the Boolean function which represents bridge circuit given below. Simplify, if possible



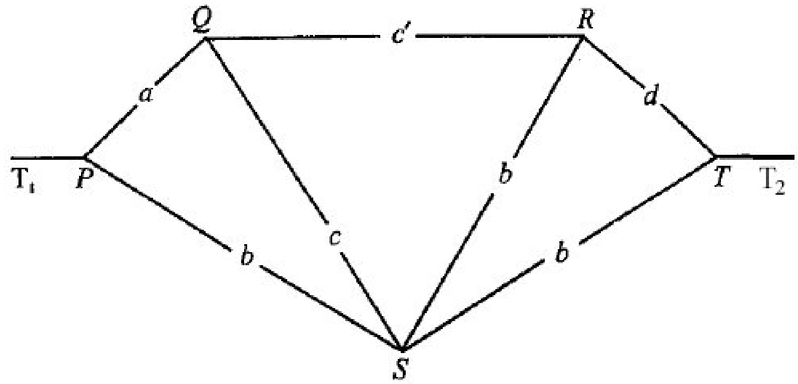
Solution: We draw broken lines as shown below through the circuit in all possible ways in which the circuit could be broken by a combination of open switches.



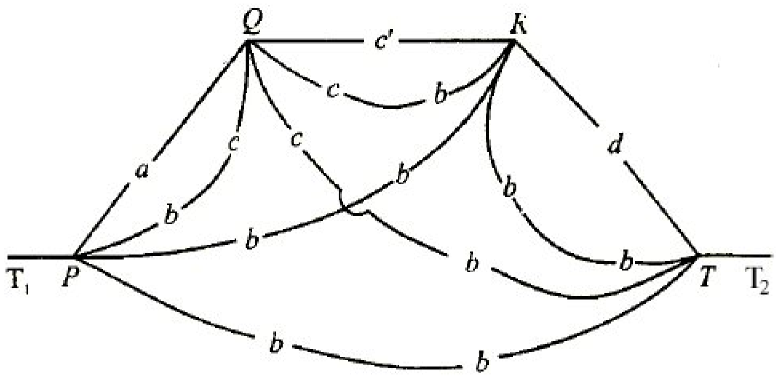
Hence the required Boolean function will be f = (ab+c) (ab+d+a) (c+d+c′) (c′+a)
=(ab+c) (ab+d+a) (1+d)(c′+a) =[ab+c(d+a)](c′+a)
=abc′+cc′(d+a)+ab+ac(d+a) =abc′+ab+ac+acd = ab + ac = a(b+c0

Note: The Boolean function f in the above example can also be simplified with the help of Karnaugh map.

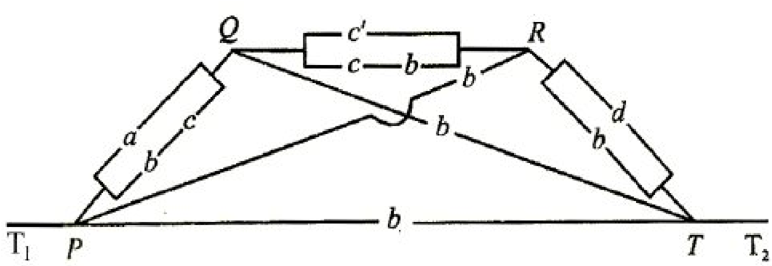
Example: Simplify the circuit given below



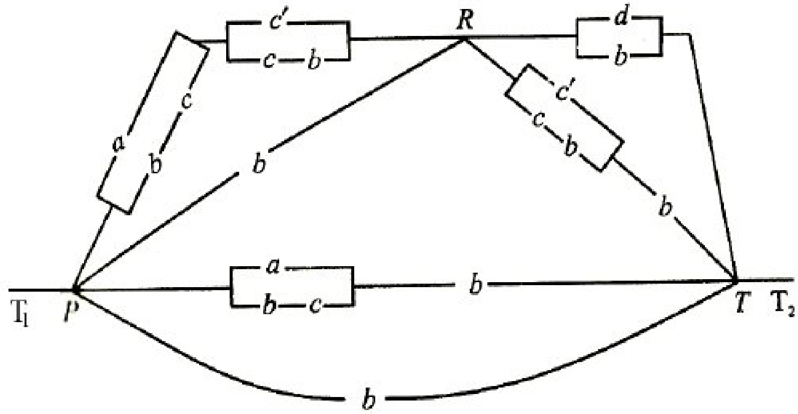
Solution: The point S is central point of the star circuit with terminals P,Q,R and T. Applying the start to mesh transformation, we get an equivalent circuit shown below:



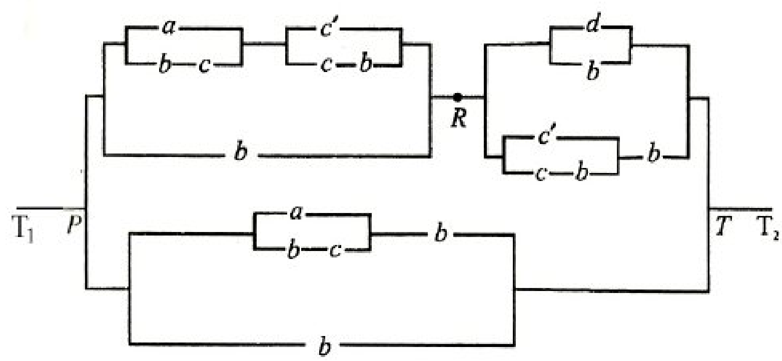
which is equivalent to



Now taking Q as the central point of a wye circuit with terminals P, R and T and applying the wye-to-delta transformation, we get an equivalent circuit shown below

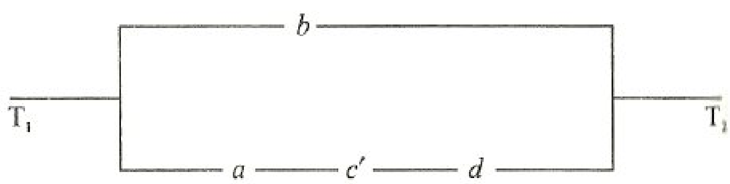


We redraw this circuit as follows:



From this figure, it follows that the Boolean function representation the given circuit is $f = [(a+bc)(c'+bc)]\,[(b+d)+b(c'+cb)]+(a+b+c)b+d]=b+ac'd$

Hence the circuit equivalent to the given circuit is

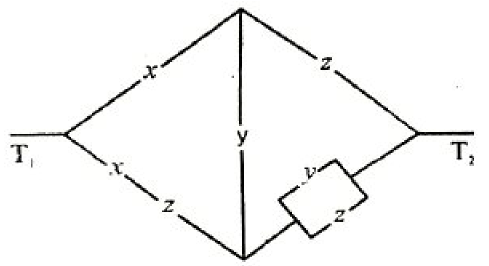


Check your progress

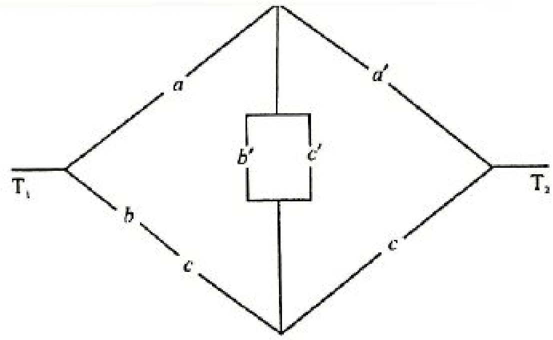
1. Construct a bridge circuit which realizes the function $f = xw'+y'uv+(xz+y')(zw'+uv)$.

2. Simplify the circuits given below:

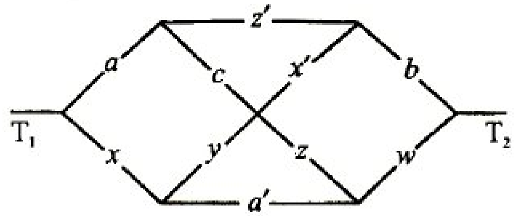
(b)



(a)

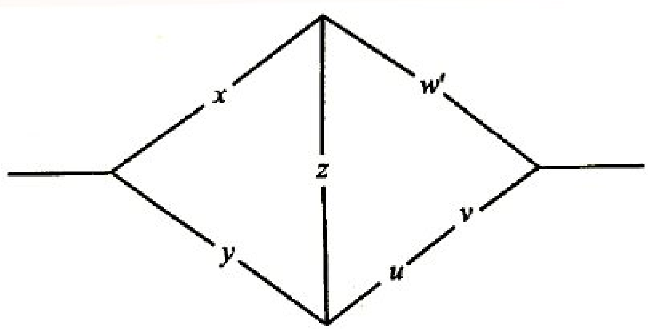


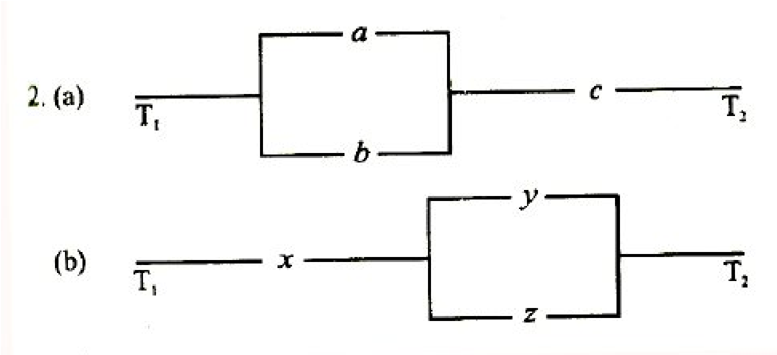
3. Find series-parallel circuit equivalent to the circuit given below

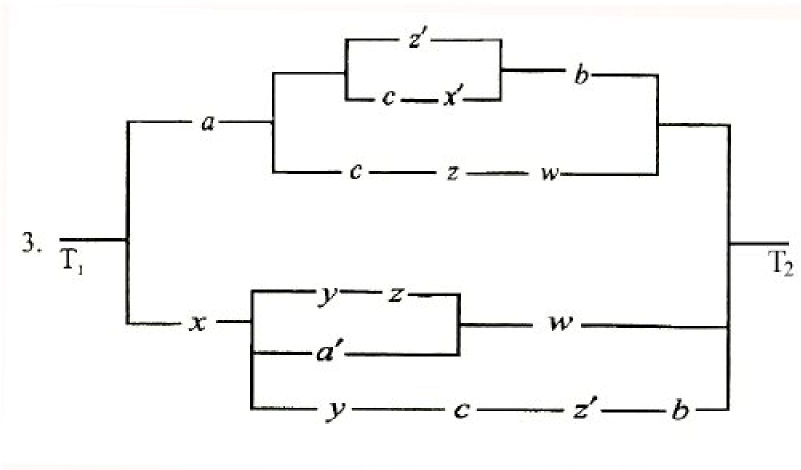


Answer

1.

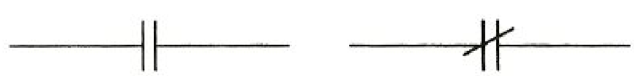






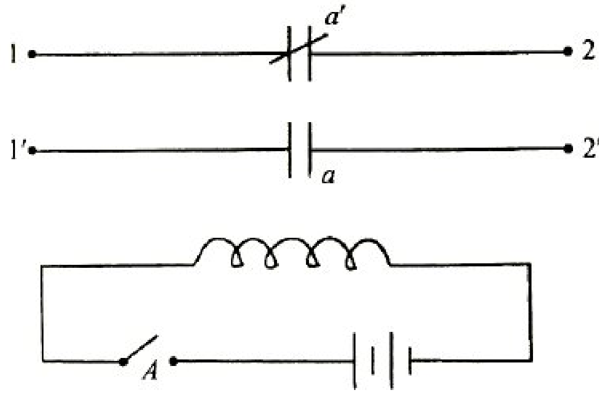
4.6. Relay Circuits:

In Practice, an on-off switch is usually replaced by a relay. A relay is a combination of a certain set of contacts all operated by a single electromagnet. The term contact carries essentially the same meaning as switch in that it is a device between two leads, which may be open o closed. When no electric current flows through the coil of the magnet, the relay is said to be in rest state. When current flows in the coil the relay is activated and said to be in its operate state. It will continue to be in this state as on as currant flows in the coil.By a normally open contact (also called make contact), we mean a contact that is open when the relay is in rest state and is closed when the relay is activated. By a normally closed contact (also known as break contact), we mean a contact that is closed when the relay is at rest and is open when the relay is activated (i.e inoperative state). Symbolically, normally open contacts and normally closed contact are represented as follows –



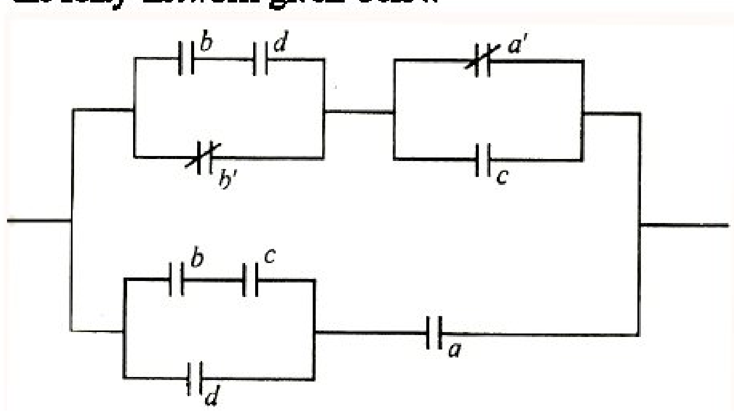
Normally open contact (a) Normally closed contact (b)

The following figure indicates a typical relay. The on-off switch



Controlling the electromagnetic coil will be denoted by a capital letter, say A, and all normally open contacts by a and all normally closed contacts by a′. It may be noted that a normally open contact and a normally closed contact on the same relay will always be in opposite states, whether the relay is at rest or is activated. We can connect relay contacts in parallel and in series in exactly the same manner as on-off switches are interconnected and all the results of Boolean algebra can be applied to the analysis and synthesis of relay network.

Example: Simplify the relay network given below

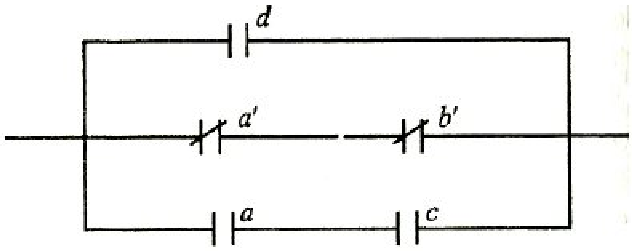


Solution: The Boolean function corresponding to the given circuit is $f=(bd+b')(a'+c)+(bc+d)a$. Representing f by a Karnaugh map, we have

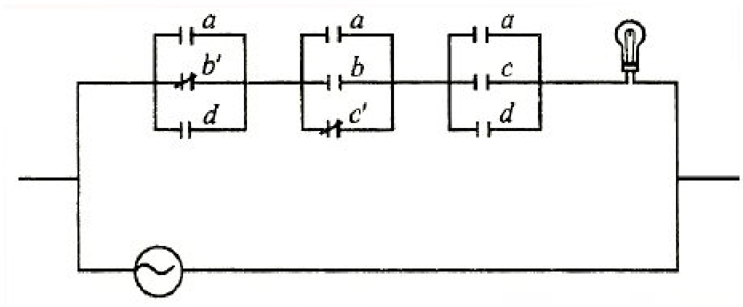
	ab	ab'	$a'b'$	$a'b$
cd	1	1	1	1
cd'	1	1	1	0
$c'd'$	0	0	1	0
$c'd$	1	1	1	1

As shown in the Karnaugh map, f has four maximal basic rectangles. Thus the minimal form of f is given by $f = d + a'b' + ac$.

The simplified network is given below



Example: A light is controlled by the switching circuit shown in the figure given below, simplify the circuit



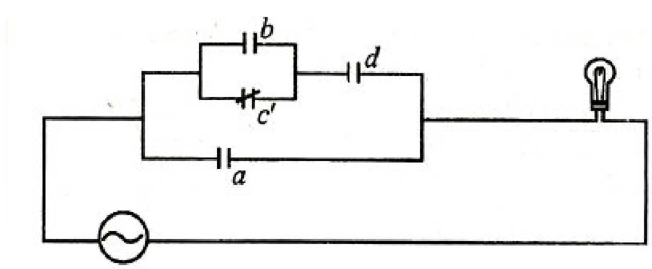
Solution: The above circuit can be described by the Boolean function

$$f = (ab'+d)\,(a+b+c)\,(a+c+d)$$

The simplified form of f is obtained from the Karanugh map of f given below

	ab	ab'	$a'b'$	$a'b$
cd	1	1	0	1
cd'	1	1	0	0
$c'd'$	1	1	0	0
$c'd$	1	1	1	1

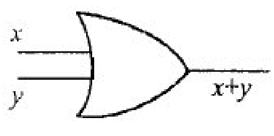
As shown in the Karnaugh map, there are three maximal basic rectangles, namely, 2×4, 1×4 and 2×2 rectangles. Hence $f = a + c'd + bd = a+(b+c')d$. Thus equivalent circuit which will perform the same control function is given below



4.7. Logic Circuits:

A digital computer used binary number system for its operation. In the binary number system, there are only two digits 0 and 1 called bits. The computer receives, stores, understands and manipulates information composed of only 0s and 1s. Logic circuits (also known as logic network) are constructed using certain elementary circuits called logic gates. Each logic circuit may be viewed as a machine which contains one or more input devices and exactly one output device. There are three basic logic gates namely OR gate, AND gate, and NOT gate. By connecting these gates indifferent ways, we can build circuit called logic circuits the perform arithmetic and other operations associated with the human brain. We first define logic gates.

Or gate: An OR gate has two or more inputs but it has only one output. Let x and y be two inputs. The output of OR gate is denoted by x+y, where x+y is defined by the table (b) given below –

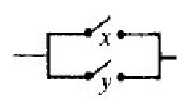


OR gate

(a)

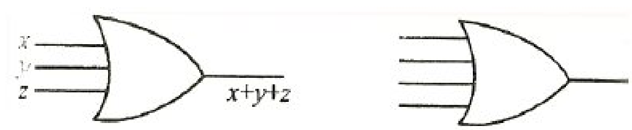
x	y	x+y
1	1	1
1	0	1
0	1	1
0	0	0

(b)



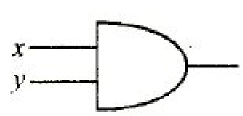
(c)

Thus output of OR gate is 1 if one of the input is 1 otherwise it is zero. The logical operation of an OR gate can easily be explained with the help of two switches connected in parallel as shown in figure (c) above. The figure (a) shows standard symbol for two input OR gate an OR gate can have as many inputs as desired. The OR gate with 3 input and 4 input are shown below:



3-input OR gate   4-input OR gate

And Gate: An AND gate is a circuit that has two or more inputs and one output. If x and y are two inputs then the output of AND gate is xy where multiplication is defined by truth table (b) below:

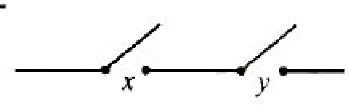


AND gate

(a)

x	y	xy
1	1	1
1	0	0
0	1	0
0	0	0

(b)

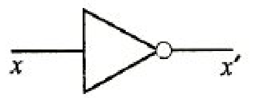


(c)

Thus output of AND gat is 1 if both the inputs are 1 otherwise it is zero. The logical operation of an AND gate can easily be explained with the help of two switches connected in series as shown in figure (c) above. The figure (a) shows standard symbol for two input and AND gate. An AND gate can have as many inputs as desired. The AND gate with 3-input and 4-input are shown below:

3-input AND gate   4-input AND gate

NOT Gate: A NOT gate is a circuit that has one input and one output. If x is the input then output of NOT gate is denoted by x′ where x′ is defined by the truth table (b) below. A NOT Gate is also called inverter Thus the output of NOT gate is complement of the input. The output is 1 if input is 0, and output is 0 if the input is



(a)

x	x'
1	0
0	1

(b)

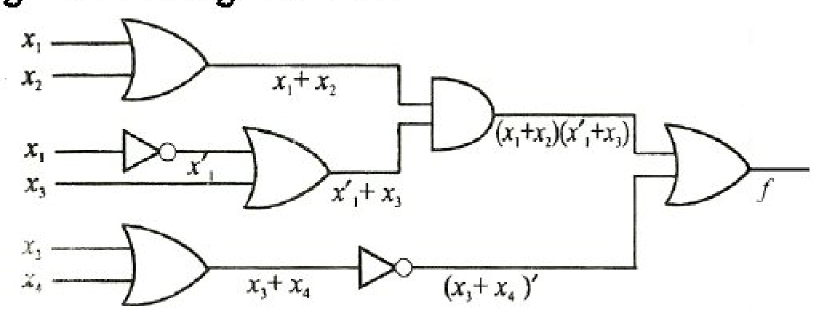
1 if input is 0, and output is 0 if the input is 1.

It is quite obvious that the above gate can be interconnected to form an electronic circuit that realizes any given Boolean expression

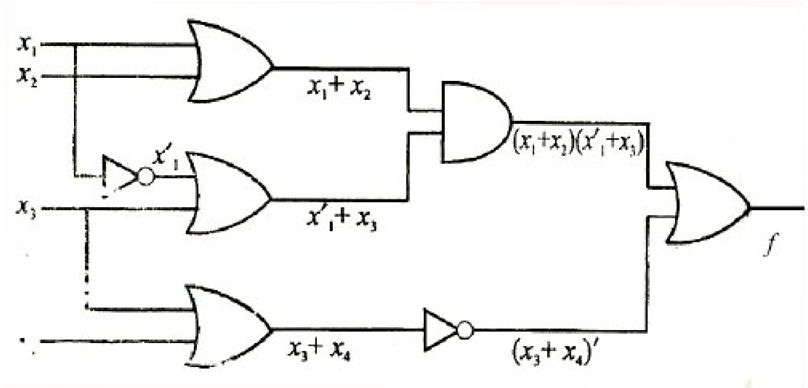
Example: Construct a circuit using gates to realize the Boolean expression

$$f = (x_1+x_2)\,(x_1'+x_3) + (x_3+x_4)'$$

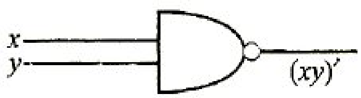
Solution: The logic network is given below:



Alternatively, invertors on x_1 input line may produce the complemented variable x_1' and x_3 input line may be combined as shown in the figure below. Observe that this network has 4 input corresponding to four variable x_1, x_2, x_3 and x_4.



NAND and NOR gates: There are two additional gates frequently used in computer known as NAND gates and NOR gates. Figure (a) below represents a NAND gate and its associated truth table. NAND gate is equivalent to an **AND** gate followed by a **NOT** gate.



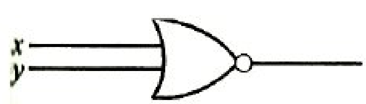
NAND gate

x	y	NAND
1	1	0
1	0	1
0	1	1
0	0	1

(a)

NAND Gate has two or mores inputs and one output. Further the output of a NAND gate is 0 if and only if all inputs are 1.

NOR gate is equivalent to an OR gate followed by a NOT gate. Figure (b) below represents a NOR gate and its associated truth table



NOR gate

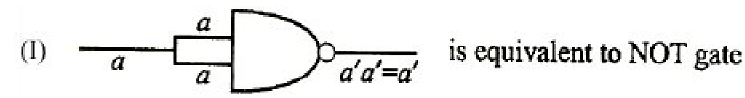
x	y	NOR
1	1	0
1	0	0
0	1	0
0	0	1

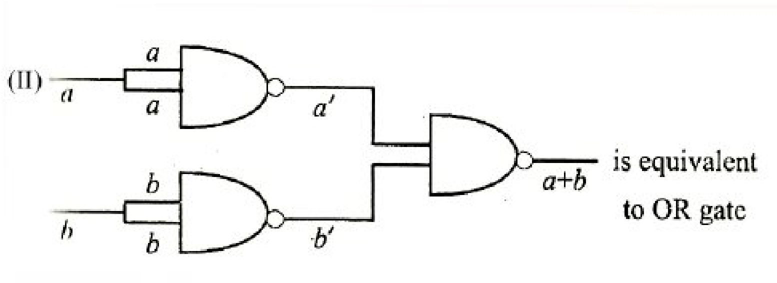
(b)

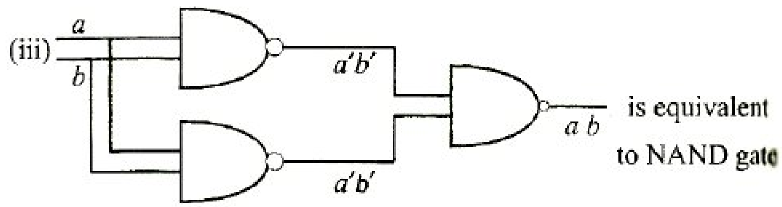
NOR gate also has two or more inputs and one output. The output of a NOR gate is 1 if and only if all the inputs are 0.

Example: Show that logic circuit corresponding to any Boolean expression can be realized by using NAND gates alone.

Solution: Since logic circuits corresponding to any Boolean expression are constructed using AND, OR and NOT gates, therefore it is enough to show that AND, OR and NOT gates can be replaced by NAND gates only. The following figures show how OR gates, And gates and NOT gates can be replaced by suitable interconnection of NAND gates.



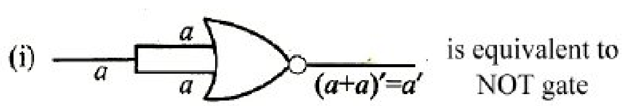


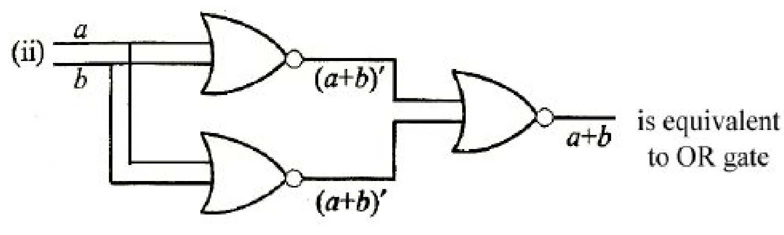


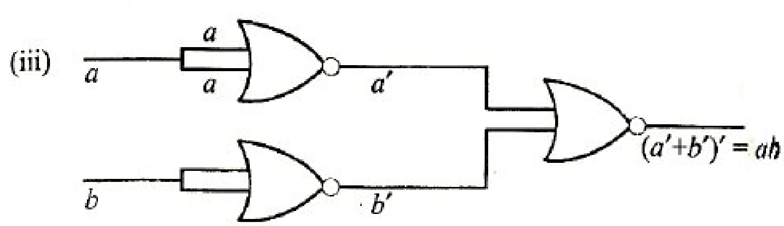
Thus logic circuit corresponding to any Boolean expression can be constructed using NAND gate only.

Example: Show that logic circuit to realize any Boolean expression can be constructed using NOR gates alone.

Solution: As in above example, we shall show that OR gate, AND gate and NOT gate can be replaced by suitable inter connectioin of NOR gates.





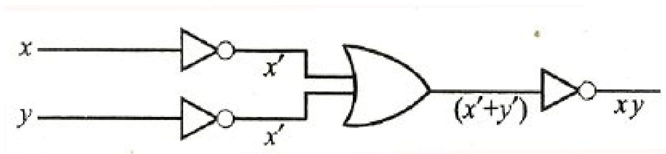


Thus logic circuit corresponding to any Boolean expression can be constructed using NOR gates only.

Example: Show thatthe set of gates (OR, NOT) is functionally complete.

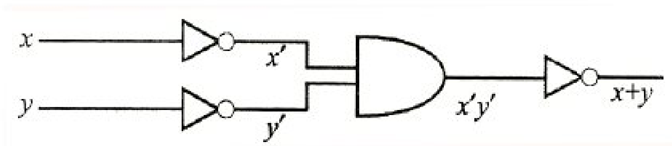
Solution: Since by DeMorgan's law xy = (x'+y')'

Therefore an AND gate can be replaced by one OR gate and three NOT gates. The logic circuit is given below

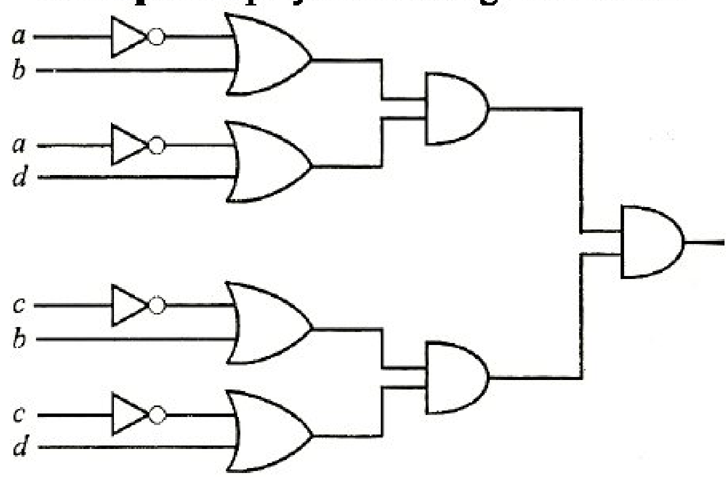


Example: Show that on OR gate can be replaced by a suitable interconnection of AND gates and NOT gates. x+y=(x'y')'

Thus an OR gate can be replaced by one And gate and three NOT gates as shown below



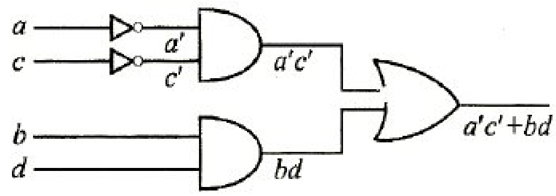
Example: Simplify the circuit given below –



Solution: Clearly the output of first, second, third, and fourth OR gates are a'+b, a'+d, c'+b and c'+d respectively. Thus the inputs first (upper) AND gate are a'+b and a'+d and inputs of second (lower) AND gate are c'+b and c'Hence inputs of last AND gate are (a'+b) (a'+d) and (c'+d). Therefore, the Boolean expression corresponding to given circuit is f = (a'+b) (a'+d) ('+b) (c'+d)

= (a'+bd) ('+bd) = a'c'+bd by distributive law

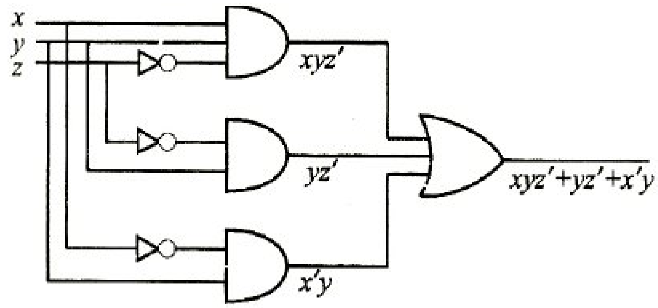
The simplified circuit corresponding to f=a'c'+bd is given below



Example: Construct a logic circuit corresponding to Boolean function

$$f = xyz' + yz' + x'y$$

Solution: Clearly the logic circuit will contain 3 AND gate and one OR gate. The inputs of the first AND gate will be x, y and z′, inputs of second And gate will be and z′ and inputs of last AND gate will be x′ and . The logic circuit is given as



4.9. Design of circuits from given properties

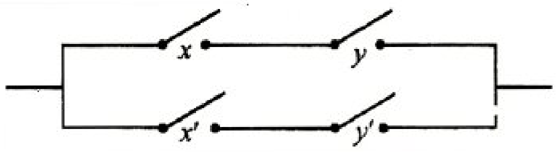
We shall now design a circuit that has given properties. For this, we first construct the tale which gives the desired state of the circuit for each possible combination of states for the separate switches. The Boolean function corresponding to the table is then written and if possible simplified. From the simplified expression a circuit is drawn.

Example: Design a circuit connecting two switches and a light bulb in such a way that either switch may be used to control the light independently of the other. It means that the change in the state of either one of them must cause a change in the state of the lamp. We arbitrarily set the lamp 'on' when x and y are both closed. We then get the table of values for the closure function, say f of the lamp shown in table below:

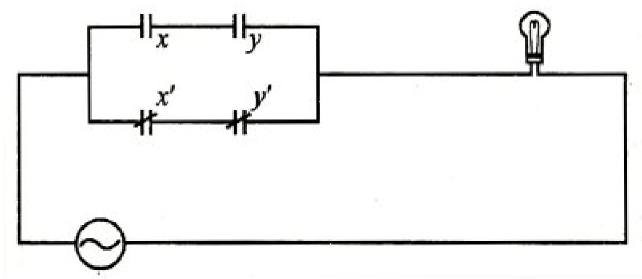
Row	x	y	f
1	1	1	1
2	1	0	0
3	0	1	0
4	0	0	1

Note that either row 2 or row 3 represents a change of state of a single switch and thus is required to change the state of the light. Hence function must take the value 0 for rows 2 and 3. Finally, row 4 represents a change of state of a single switch from the state of either row 2 or row 3. Hence the function f must assume the value 1 in row 4. From the tale we can write the function as $f = xy + x'y'$

A circuit realizing this function is given below



Alternatively, the diagram may also be given as below



Example: Design as simply as possible a series-parallel circuit for the operation of alight independently from three switches x, y and z.

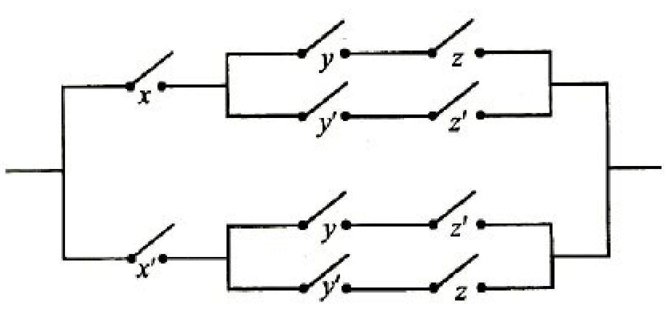
Solution: As discussed in Example 6.20 above, we arbitrarily set the lamp 'on' when x, y and z are closed. We then get the table of values for the closure function, say f of the lamp as given below:

row	x	y	z	f
1	1	1	1	1
2	1	1	0	0
3	1	0	1	0
4	1	0	0	1
5	0	1	1	0
6	0	1	0	1
7	0	0	1	1
8	0	0	0	0

From this table, we get the function f as follows

$f = xyz+xy'z'+x'yz'+x'y'z \; = x(yz+y'z'(\; + x'(yz'y'z)$

Hence the circuit corresponding to f is



Example: An aircraft has three engines. Each engine is provided with a switch which closes as soon as there is any mechanical fault in that engine. Although the aircraft can run with just one engine operating, it is desired to have a red lamp appear when there is a fault in any one of the engine and an alarm to ring when there is a fault in any two of them. Design a two terminal circuit for this, sharing switches whenever possible.

Solution: We denote the three switches by x, y and z. Let f and g denote the closure functions for the red lamp (R) and the alarm (A) respectively. The table of value for the closure function f and g of lamp and alarm is given below:

row	x	y	z	f	g
1	1	1	1	1	1
2	1	1	0	1	1
3	1	0	1	1	1
4	1	0	0	1	0
5	0	1	1	1	1
6	0	1	0	1	0
7	0	0	1	1	0
8	0	0	0	0	0

From the table, we see that $f = x+y+z$

$g = xyz+xyz'+xy'z+x'yz = xy+xy'z+yz$

$= xy+z(xy'+y) = xy+z(x+y)(y'+y) = xy + yz + xz$

If we draw separate circuits for red lamp and alarm, we need 8 occurrences of switches. To see that whether the sharing of switches is beneficial we first see if f and g have any common factors. For this we take their conjunctive normal forms. f is already in its CN form while from table we can write

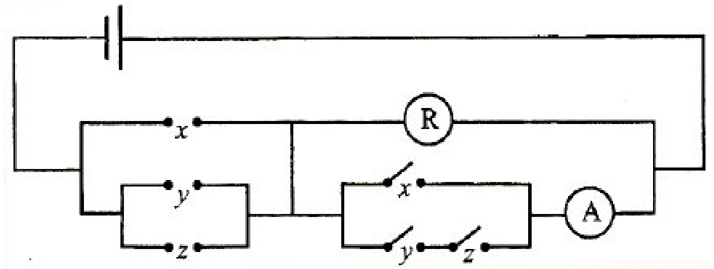
$g = (x+y+z)\,(x+y+z')\,(x+y'+z)\,(x'+y+z)$

Here although $x+y+z$ is a common factor in f and g, it will not result in any saving to share it because the remaining three factors of g, even upon simplification would require at least five occurrence of switches. So we write f as f_1+f_2 where f_1+x and $f_2=y+z$. Then

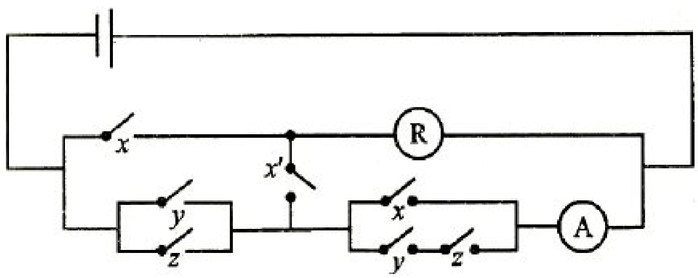
$g = (y+z+xx')\,[x+(y+z')\,(y'+z)]$

$= (y+z)\,(x+yz+y'z') = (y+z)\,(x+yz)$

Now we may try to use the factor $y+z$ common in f_2 and g. The resulting circuit is as follows:



But in this circuit the alarm will also ring even when only x is closed which is not desired. To avoid this we insert switch x′ as shown in figure below which is a correct solution.



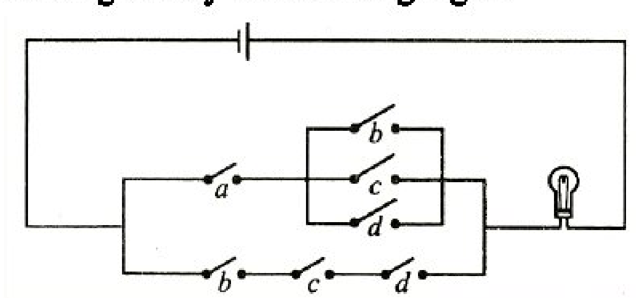
Note that there is a saving of switches because 7 occurrence are needed.

Example: Suppose there is committee of four persons A, B, C and D. Any motion is taken as passed by the committee if and only if either A and any of B, C, D say yes or at least three out of four members say yes. Any member who says yes press a button. A light is to shine only when a motion is passed. Draw the circuit.

Solution: Let a, b, c and d denote the four switches (buttons) given to membes A, B, C and D respectively. Now the light should shine when a and any of b, c, d are closed. That is when a(b+c+d0 is 1. Similarly light should shine when any three of a,b,c,d, are 1. That is, when any of abc, bcd, acd, abd is 1. Thus the closure function for the lamp is given by

$f = a(b+c+d) + abc+bcd+acd+abd = ab+ac+ad+bcd = a\ (b+c+d)+bcd$

Hence the required circuit is given by the following figure



Example: Design a 4-terminal circuit to realize the following three function using common switches wherever possible. $f = xy'z+(xy'+x'y)\ zw$

$g = xy'zw'+x'yzw'$, $h = x'y+(xy'+x'y)\ (z'+w')$

Solution: We first write each function in product form to find common factor. Since g can be most easily factored, we begin by writing it in the form

$g = (xy'+x'y)zw'$. Examining f and h for possible factors in common with g, we find

$f = z[xy'+(xy'+x'y)w] = z[xy'y'+x'y'+(xy'+x'y)w]$

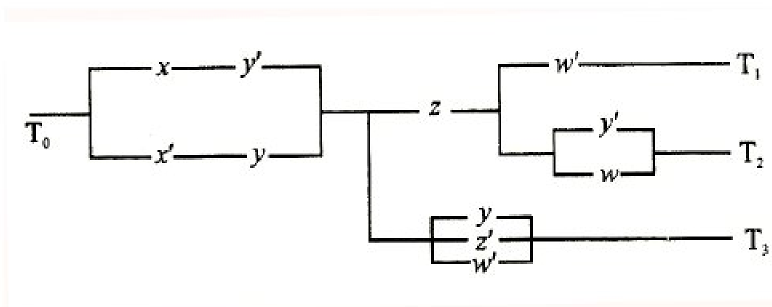
$=z[xy'+x'z)y'+(xy'+x'y)w] = z(xy'+x'y)(y'+w)$

Similarly, $h = x'y+(xy'+x'y)(z'+w')$

$= x'yy+xy'y+(xy'+x'y)(z'+w') = (x'y+xy')y+(xy'+x'y)(z'+w')$

$= (x'y+xy')(y+z'+w')$

Hence the required circuit is given below where circuits between T_0 and T_1, T_0 and T_2 and T_3 realize functions g, f and h respectively.



Example: Construct a 4-terminal circuit to realize the functions f, g, and h with properties given by the following table:

(x,y,z)	f	g	h
(0,0,0)	1	0	1
(0,0,1)	1	0	1
(0,1,0)	0	1	1
(0,1,1)	1	0	0
(1,0,0)	0	0	0
(1,0,1)	1	1	1
(1,1,0)	0	1	1
(1,1,1)	1	0	0

Solution: We first write each function in conjunctive normal form:

$f = (x+y'+')(x'+y+z)(x'+y'+z)$

$g = (x+y+z)(x+y+z')(xy'+z')(x'+y+z)(x'+y'+z')$

$h = (x+y'+z')(x'+y+z)(x'+y'+z')$

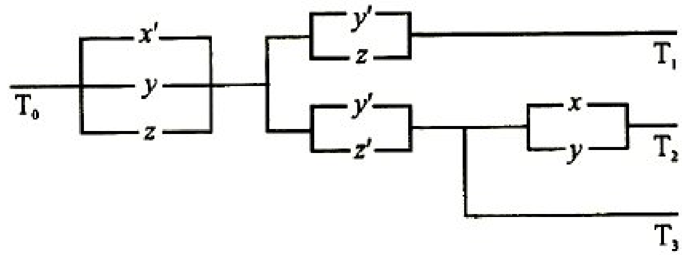
The common factor in f, g and h are noted and are indicated below with dotted vertical lines. Simplification are made where possible

$f = (x'+y'+z) \quad (y'+z)$

$g = (x'+y'+z) \quad (y'+z') \quad (x+y)$

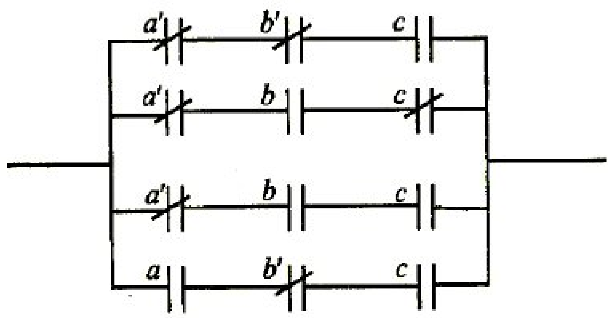
$h = (x'+y'+z) \quad (y'+z')$

The required circuit is given below where circuits between T_0 and T_1, T_0 and T_2, T_0 and T_3 are corresponding to functions f, g and h respectively

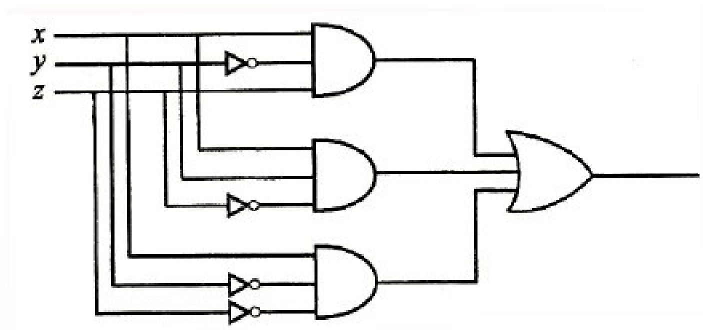


Check your progress

1. Simplify the relay network given below



2. Use Karnaugh maps to redesign logic circuit given below so that it becomes a minimal AND-O circuit.



3. Construct a 3-terminal circuit to realize both the following functions

   $f = xzw + y'zw$, $g = xzw + y'zw + x'y'z$

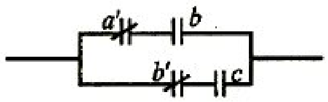
4. Construct a 4-terminal circuit to realize the following three functions with minimum number of switches $f = a(b+cd)(x+y)$

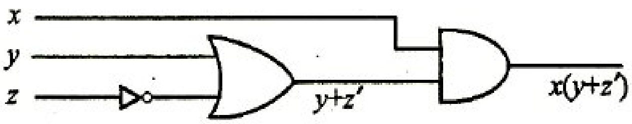
   $g = a(bc+cd)$, $h = a(bc'+b'cd)$

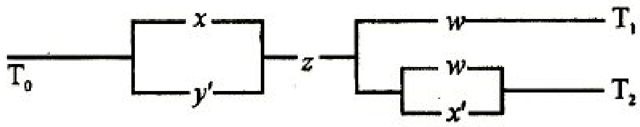
5. Design a circuit which connects two switches at the two entrances of a room to light a bulb in the room. The switches work independently so that any of the switch may be used to operate the bulb.

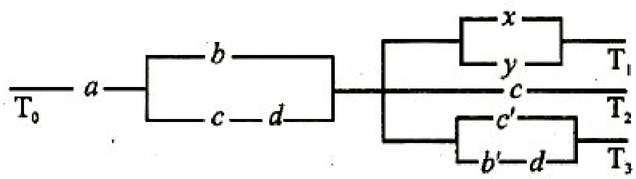
6. A digital system has 4-bit input from 0000 to 1111. Desing a decimal input is greater than 13.

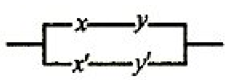
Answers

1 

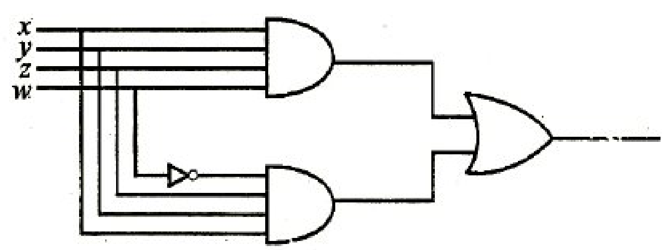
2 

3 

4 

5 

5. The function is given by f = xyzw + xyzw



Uttar Pradesh Rajarshi Tandon open University

SBSCS-01

Discrete Mathematics

BLOCK

2

SET THEORY AND ITS APPLICATION

Course Design Committee

Dr. Ashutosh Gupta — **Chairman**
Director-In-charge,
School of Computer and Information Science,
UPRTOU, Allahabad

Prof. R. S. Yadav — **Member**
Department of Computer Science and Engineering
MNNIT-Allahabad, Allahabad

Ms. Marisha — **Member**
Assistant Professor, Computer Science
School of Sciences, UPRTOU, Allahabad

Mr. Manoj Kumar Balwant — **Member**
Assistant Professor, Computer Science
School of Science, UPRTOU, Allahabad

Course Preparation Committee

Dr. A. K. Pandey — **Author**
Reader, Dept of Mathematics
ECC, Allahabad

Prof. D. P. Chaudhary — **Editor**
Ex-Professor, University of Allahabad
Allahabad, Uttar Pradesh

Dr. Ashutosh Gupta
Director (In-charge), School of Computer and Information Science,
UPRTOU, Allahabad

Ms. Marisha (Coordinator)
Assistant Professor, School of Sciences,
UPRTOU, Allahabad

Unit – 1

Set theory

Structure

1.1 INTRODUCTION

A word either belongs to this collection or not, depending on whether it is listed in the dictionary or not. This collection is an example of a set. When we start studying any part of mathematics, we will come into contact with one or more sets. This is why we want to spend some time in discussing some basic concepts and properties concerning sets.

In this unit we will introduce various examples of sets. Then we will discuss some operations on sets. We will also introduce you to Venn diagrams, a pictorial way of describing sets. Knowledge of the material covered in this unit is necessary for studying any mathematics course, so please study this unit carefully.

1.2 Objectives

After reading this unit we should be able to:

- identify a set;
- represent sets by the listing method, property method and Venn diagrams;
- perform the operations of complementation, union and intersections on sets;
- prove and apply the distributive laws;
- prove and apply De Morgan's laws;

1.3 Sets

The concept of set is used in all branches of mathematics.The word 'set' in mathematics was first of all used by **George Cantor**. According to him, **'A set is any collection into a whole of definite and distinct objects of our intuition or thought'**. However, Cantor's definition faced controversies due to the forms like 'definite' and 'collection into a whole'. Later on, a single word 'distinguishable' used to make the definition acceptable. **'A set is any collection of distinct and distinguishable objects around us'.** By the form 'distinct', we mean that no object is repeated and some lack the term 'distinguishable' we mean that whether that object is in our collection or not. The objects belonging to a set are called as elements or members of that set. For example, say A is a set of stationary used by any student i.e.

A = {Pen, Pencil, Eraser, Sharpener, Paper}

A set is a well-defined collection of object. By a well-defined collection we mean that there exists a rule with the help of which it is possible to determine whether a given object is a member of the given collection or not. Each object belonging to a set is called an element or a member of the set. We generally use capital letters *A, B, C, X, Y, Z* etc. to denote sets and lower case letters *a, b, c, x, y* etc. to denote elements of a set. If x is an element of a set A, we write $x \in A$ (read as '*x* belongs to *A*'). If *x* is not an element of A, we write $x \notin A$ (read as x does not belong to *A*). Examples:

(i) Let A = {4, 2, 8, 2, 6}. The elements of this collection are distinguishable but not distinct, hence A is not a set.

(ii) Let B = {*a, e, i, o, u*} i.e. *B* is set of vowels in English. Here elements of B are distinguishable as well as distinct. Hence *B* is a set.

1.3.1 Methods of Describing Sets

There are essentially two methods to specify a given set

1. Roster Method: A set may be described by listing all its elements. For example, the set of vowels in the English alphabet is

$$A = \{a, e, i, o, u\}$$

Here the elements are separated by commas and are enclosed in a pair of braces {}. This method of describing a set is called the roster method or the tabular form of the set.

Sometimes, it is not convenient to list all the elements of a set. For example, the set of natural numbers may be written as

$$N = \{1, 2, 3, \ldots..\}$$

2. Property Method (Set Builder Form): The roster method of specifying a set is not always convenient and sometimes it is not possible to use this method to describe a set. A set can also be defined by some property which characterizes all the elements of the set. For example,

$$A = \{x : x \text{ is vowel in the English alphabet}\}$$

which reads "A is the set x such that x is a vowel in the English alphabet. This method of describing a set is called property method (or set builders form).

Examples: (a) $N = \{n : n \text{ is a natural number}\}$ (b) $E = \{x : x \text{ is an even integer}\}$

1.3.2 Equality of Sets

Two sets A and B are said to be equal if they contain the same elements. This statement is also known as the *axiom of extension*. We write $A = B$ if the sets A and B are equal and $A \neq B$ if the set A and B are not equal. For example,

1. $\{a, b, c\} = \{b, a, c\}$
2. $\{2, 3, 5\} \neq \{2, 3, 7\}$

Remark: If $A = \{a, a, b, c\}$ and $B = \{a, b, c\}$ then it is clear that $A = B$. Thus $\{a, a, b, c\}$ is a redundant representation of the set $\{a, b, c\}$. For this reason, some authors defined a set to be a well-defined collection of distinct object.

1.4 Subsets

Let A and B be two sets. If every element of A is also an element of B then A is called a subset of B. We also say that A is contained in B or that B contains A. In symbols, we write '$A \subseteq B$'or '$B \supseteq A$'.We say A is not a subset of B if at least one element of A does not belong to B and we write it as $A \subseteq B$. It is clear that two sets A and B are equal if and only if $A \subseteq B$ and $B \subseteq A$.

Examples: Consider the set $A = \{1, 3, 4, 5\}$, $B = \{1, 2, 3, 5\}$ and $C = \{2, 3\}$. Then $C \subseteq B$ but $C \not\subset A$.

Proper Subset of a Set: Set A is said to be a proper subset of a set B if

(a) Every element of set A is an element of set B, and

(b) Set B has at least one element which is not an element of set A.

This is expressed by writing $A \subset B$ and read as A is a proper subset of B , if A is not a proper subset of B then we write it as $A \not\subset B$.

(i) Let $A = \{4,5,6\}$ and $B = \{4, 5, 7, 8, 6\}$ So, $A \subset B$

(ii) Let $A = \{1, 2, 3\}$, and $B = \{3, 2, 9\}$ So, $A \not\subset B$.

From the definition of a subset it is clear that every set is a subset of itself. Briefly, B is a proper subset of A if $B \subseteq A$ and $B \neq A$ and write $B \subseteq A$.

Empty Set

The set which contains no element is called the empty set (or null set or the void set) and is denoted by $\{\}$. The empty set is also denoted by the symbol ϕ. Since ϕ has no element, therefore, empty set is subset of every set. A set which is not empty is called non-empty set.

Disjoint Sets

Two sets A and B are said to be disjoint if they have no elements in common.

For example, the sets $A = \{1,2,3,4\}$ and $B = \{0,5,6\}$ are disjoint while the sets $A = \{1,2,3,4\}$ and $C = \{1,2,6\}$ are no disjoint.

Comparability of Sets: Two sets A and B are said to be comparable if either one of these happens.

(i) $A \subset B$

(ii) $B \subset A$

(iii) $A = B$

Similarly if neither of these above three exist i.e. $A \not\subset B$, $B \not\subset A$ and $A \neq B$, then A and B are said to be incomparable. **Example** $A = \{1, 2, 3\}$, and $B = \{1, 2\}$. Hence set A & B are comparable. But $A = \{1, 2, 3\}$ and $B = \{2, 3, 6, 7\}$ are incomparable

Singleton Set

A set which contains exactly one element is called a singleton. For example, $\{2\}$ is a singleton.

Universal Set

In any mathematical discussion, we usually consider all the sets to be subsets of a fixed set called the universal set. Universal set is sometimes referred to as the universe or the universe of discourse.

For example, in studying human population the universal set consists of all human in the world and while discussing plane geometry we may consider the universal set to be the set consisting of all the points in the plane.

Power Set

If X is any set then the set of all subsets of X is called the power set of X. denoted by $P(X)$. Thus $P(X)=\{A : A \subseteq X\}$. If X contains n elements then $P(X)$ contains 2^n elements.

Example: Let $X=\{1,2,3\}$ then

$P(X)=\{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Since X has three elements, $P(X)$ has $2^3 = 8$ elements.

Finite and Infinite Set

A set is said to be finite if it contains a ***finite*** number of distinct elements. A set is said to be **infinite** if it is not finite.

Example: Let $A = \{1,3,5,7,9\}$. Then A is finite because it contains 5 distinct elements.

Example: Let $B = \{1,2,3,4....\}$. Then B is an infinite set

1.5. Operations on Sets

We introduce and study some basic operations in the section. Using these operation, we can construct new sets by combining the elements of given sets.

Union of sets

Let A and B be two sets. The *union of A* and B is the set of all elements which are in the set A or in the set B. The union of two sets A and B is denoted by the symbol $A \cup B$

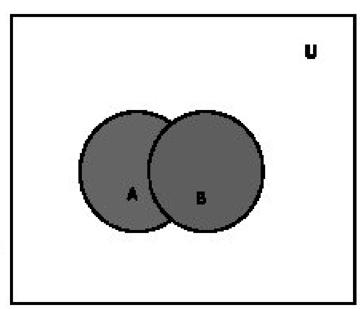
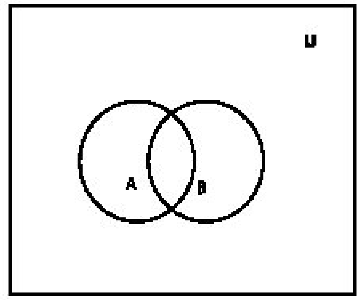


Fig. 2.1: $A \cup B$ is shaded

which is read as 'A union B'. Symbolically, $A \cup B = \{x : x \in A$ or $x \in B\}$

In the adjoining Venn-diagram, the union of A and B is shown by the shaded area.



Intersection of Sets

Let A and B be two sets. The *intersection* of A and B is the set of all elements which are both in A and B. We denote the intersection of A and B by $A \cap B$, which is read as 'A intersection B'. Symbolically, $A \cap B = \{x : x \in A$ and $x \in B\}$

In the adjoining venn diagram the intersection of two sets A and B is shown by the shaded region.

Complement of a Set

Let A be a subset of a universal set U. The set of all those elements of U which are not in A is called the complement of A and is denoted by U-A or simply A'. Symbolically, $A' = U - A = \{x : x \in U$ and $x \notin A\}$

Difference of Sets

The difference A-B of two sets A and B is the set of elements which belong to A but which do not belong to B. Thus,

A-B $= \{x : x \in A$ and $x \notin B\}$

The shaded region represents A-B in the adjoining diagram.

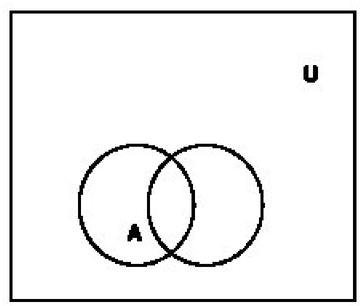


Fig. 2.3: A-B is shaded

Example: Let U= $\{a, b, c, d, e, f\}$, $A = \{a, b, c, d\}$ and

$B = \{b, d, f\}$. Then $A - B = \{a, c\}$, $B - A = \{f\}$

$A \cup B = \{a, b, c, d, f\}$, $A \cap B = \{b, d\}$ and $U - A = \{e, f\}$

1.6. Law of Algebra of Sets

Theorem: Let A, B and C be subsets of an universal set U. Then the operations defined on sets satisfy the following properties:

1. ***Commutative laws:***

(a) $A \cup B = B \cup A$
(b) $A \cap B = B \cap A.$

2. ***Associative laws:***

(a) $A \cup (B \cup C) = (A \cup B) \cup C$

(b) $A \cap (B \cap C) = (A \cap B) \cap C$

3. ***Idempotent laws:***

(a) $A \cup A = A$ (b) $A \cap A = A$

4. ***Distributive law:***

(a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

5. ***Identity Laws:***

(a) $A \cup \phi = A$ (b) $A \cap \phi = \phi$

6. ***Involution laws:***

$(A')' = A$

7. ***De-Morgan's laws:***

(a) ($(A \cup B)' = A' \cap B'$) (b) $(A \cap B)' = A' \cup B'$

8. ***Complement laws:***

(a) $A \cup A' = U$ (b) $A \cap A' = \phi$

Proof : We will prove 4(a) and 7 only and leave proofs of remaining laws as exercises for the reader. We first prove 4(a), i.e. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Let $x \in A \cup (B \cap C)$ then we have,

$x \in A \cup (B \cap C) \Leftrightarrow \quad x \in A$ or $x \in B \cap C$

$\Leftrightarrow \quad x \in A \text{ or } (x \in B \text{ and } x \in C) \Leftrightarrow \quad (x \in A \text{ or } x \in B) \text{ and } (x \in A \text{ or } x \in C)$

$\Leftrightarrow \quad x \in A \cup B \text{ and } x \in A \cup C \Leftrightarrow \quad x \in (A \cup B) \cap (A \cup C)$

Hence $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Proof : 7(a) If $x \in (A \cup B)' \Rightarrow x \notin (A \cup B) \Rightarrow x \notin A$ and $x \notin B \Rightarrow x \in A'$ and $x \in B' \Rightarrow x \in A' \cap B' \Rightarrow x \in (A \cup B)' \Rightarrow x \in A' \cap B$ So, $(A \cup B)' = A' \cap B'$

(b) Say $x \in (A \cap B)' \Rightarrow x \notin A \cap B \Rightarrow x \notin A$ or $x \notin B \Rightarrow x \in A'$ or $x \in B'$

So $x \in (A \cap B)' = A' \cup B'$ Hence $(A \cap B)' = A' \cup B'$.

Check your progress

1. Determine whether each of the following is true or false:

   (a) $\phi \subseteq \phi$ (b) $\phi \in \phi$ (c) $\phi \in \{\phi\}$ (d) $\{\phi\} \in \{\phi\}$

   (e) $\{a,b\} \subseteq \{a,b,c,\{a,b,c\}\}$ (f) $\{a,b\} \in \{a,b,c,\{a,b,c\}\}$

   (g) $\{a,b,c\} \in \{a,b,c,\{a,b,c\}\}$ (h) $\{a,b,c\} \subseteq \{a,b,c,\{a,b,c\}\}$

2. Determine the following sets:

   (a) $\{\phi\} \cup \{a,\phi,\{\phi\}\}$ (b) $\{\phi\} \cap \{a,\phi,\{\phi\}\}$

3. Give an example of sets *A*, *B* and *C* such that $A \subseteq B$, $B \in C$ and $A \notin C$.

4. Write the power set of the set = $\{\phi,\{\phi\}\}$.

5. For $A = \{a,b,\{a,c\},\phi\}$, determine the following sets:

   (a) $A-\{a\}$ (b) $A-\{\phi\}$ (c) $A-\{\{a,b\}\}$

   (d) $A-\{\{a,c\}\}$ (e) $\{\phi\}-A$

6. Prove that $A-B = A \cap B'$.

7. Given that $A \cap B = A \cap C$ and $A' \cap B = A' \cap C$. Is it necessary that $B = C$? Justify your answer.

(8) Represent the set $A = \{a, e, i, o, u\}$ in set builder form.

(9) Represent the set $B = \{x: x$ is a letter in the word 'STATISTICS'$\}$ in tabular form.

(10) Represent the set $A = \{x: x$ is an odd integer and $3 \leq x < 13\}$ in tabular form.

(11) Are the following sets equal?

$A = \{x: x$ is a letter in the word 'wolf'$\}$
$B = \{x: x$ is a letter in the word 'follow'$\}$
$C = \{x: x$ is a letter in the word How$\}$

(12) Find the proper subset of following sets

(i) ϕ
(ii) $\{1,2,3\}$
(iii) $\{0,2,3,4\}$

(13) Find the power sets of the following sets

(i) $\{0\}$
(ii) $\{1, 2,3\}$
(iii) $\{4,1,8\}$

(14) If $A = \{2,3,4,5,6\}$, $B=\{3,4,5,6,7\}$, $C= \{4,5,6,7,8\}$, then find

(i) $(A\cup B) \cap (A\cup C)$
(ii) $(A\cap B) \cup (A\cap C)$
(iii) $(A-B)$ and $(B-C)$
(iv) $A\Delta B$

Solution

(1) (a) True. (b) False. (c)True. (d) False.

(e) True. (f) False. (g)True. (h) True.

(2) (a) $\{a, \phi, \{\phi\}\}$ (b) $\{\phi\}$

(3) $A=\{a,b\}, B=\{a,b\}\}, C=\{a,b,\{a,b,\{a,b\}\}\}$

(4) $P(X) = \{\phi, \{\phi\}, \{\{\phi\}\}, \{\phi, \{\phi\}\}\}$

(5) (a) $\{b,\{a,c\}\},\phi\}$ (b) $\{a,b,\{a,c\}\}$ (c) A (d) $\{a,b,\phi\}$ (e) ϕ

(7) Yes. (8) A = {x: x is vowel of English alphabets}

(9) B = {A, C, I, S, T}. (10) A = {3, 5, 7, 9, 11}.

(11) A and B are equal sets.

(12) (ii) {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}.

(iii) {0}, {2}, {3}, {4}, {0, 2}, {0, 3}, {0, 4}, {2, 3} {2, 4}, {3, 4}, {0, 2, 4}, {0, 2, 3}, {0, 3, 4}, {2, 3, 4}.

(13) (i) {{}, {0}}, (ii) {{}, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}

(iii) {{}, {1}, {4}, {8}, {1, 4}, {1, 8}, {4, 8}, {1, 4, 8}}

(14) (i) {2, 3, 4, 5, 6,7}. (ii) {3, 4, 5, 6}. (iii) {2}, {3} (iv) {2, 7}

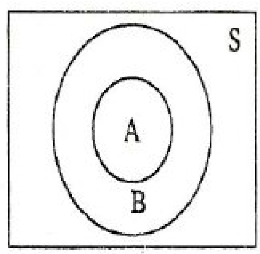
1.7 Venn diagram

Here we will learn the operations on sets and its applications with the help of pictorial representation of the sets. The diagram formed by these sets is said to be the Venn diagram of the statement.

A set is represented by circles or a closed geometrical figure inside the universal set. The Universal Set S, is represented by a rectangular region.

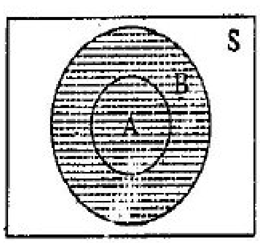
First of all we will represent the set or a statement regarding sets with the help of Venn diagram. The shaded area represents the set written.

(a) Subset :

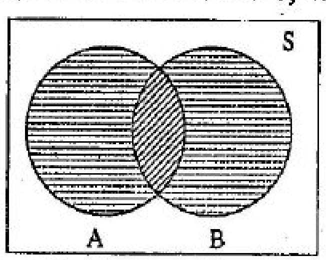


$A \subset B$

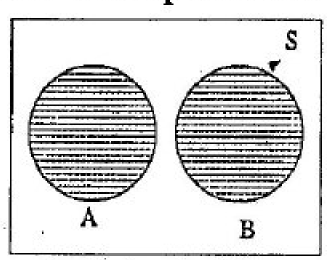
(b) Union of sets: Let $A \cup B = B$. Here, whole area represented by B represents $A \cup B$.



$A \subset B$ when $A \subset B$

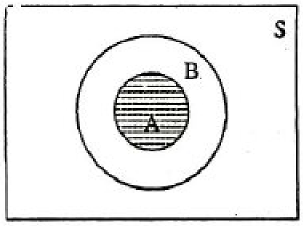


$A \subset B$ when neither $A \subset B$ nor $B \subset A$

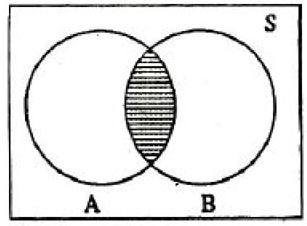


$A \cup B$ when A and B are disjoint events

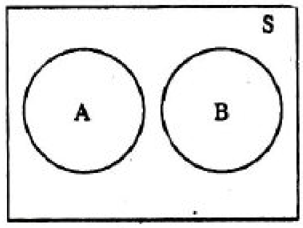
(c) Intersection of Sets ($A \cap B$): $A \cap B$ represents the common area of A and B.



A ∩ B when A ⊂ B and
A ∩ B = A

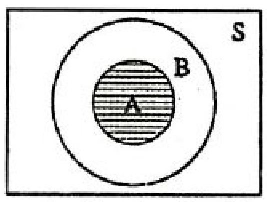


A ∩ B when neither A ⊂ B nor
B ⊂ A

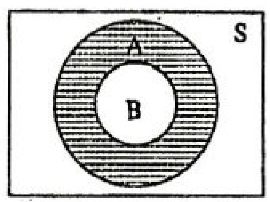


A ∩ B = ϕ

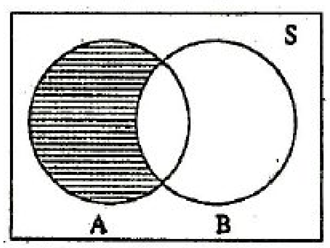
(d) Difference of sets: (A – B) represents the area of A that is not in B.



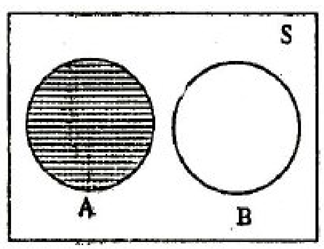
A – B, when A ⊂ B
(A – B = ϕ)



A – B, when B ⊂ A

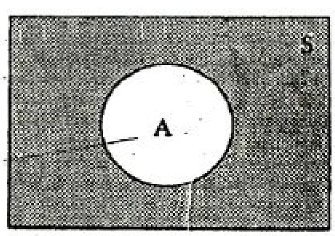


A – B when neither
A ⊂ B nor B ⊂ A



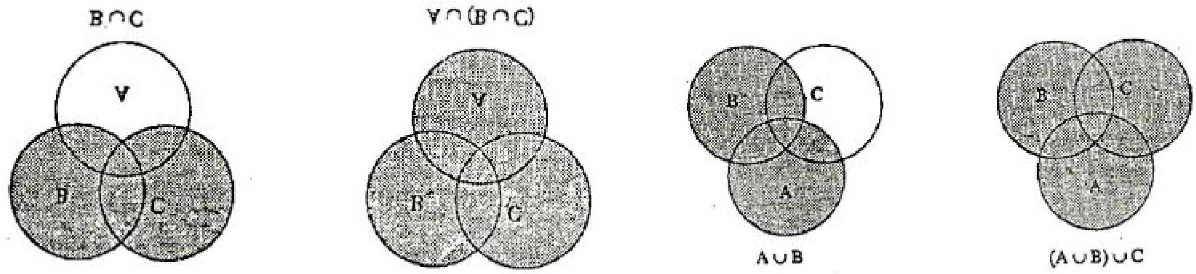
A – B when A and B are
disjoint sets
(A – B ⊂ A)

(e) Complement of Sets(A′): A′ or A° is the set of those elements of Universal Set S which are not in A.

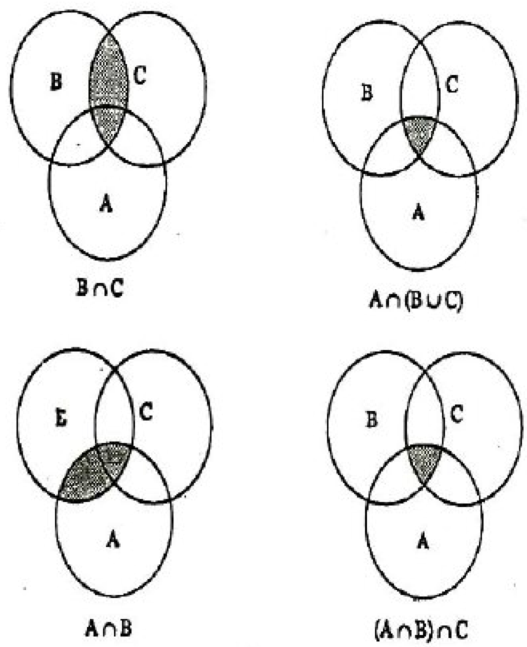


A′

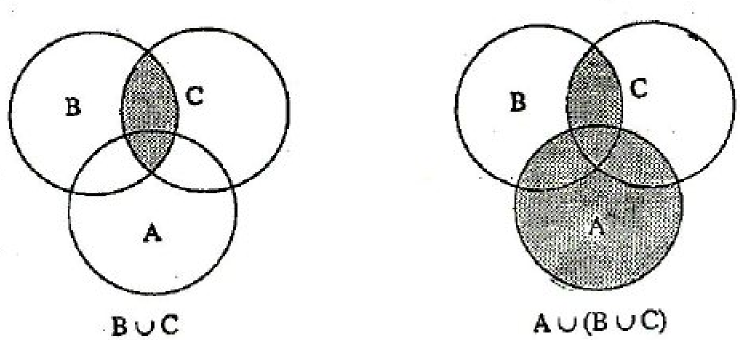
(f) A ∪ (B ∪ C) and (A ∪ B) ∪ C

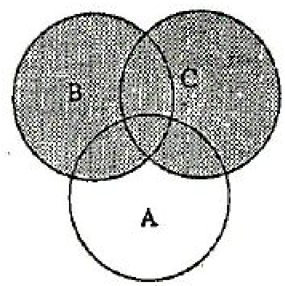


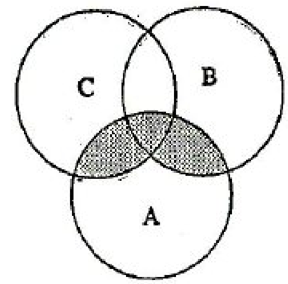
(g) A ∩ (B ∩ C) and (A ∩ B) ∩ C



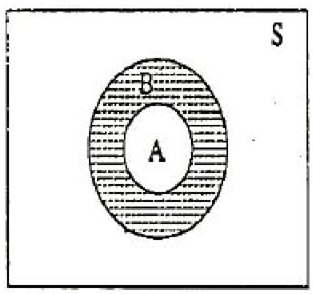
(h) A ∪ (B ∩ C) and A ∩ (B ∪ C)



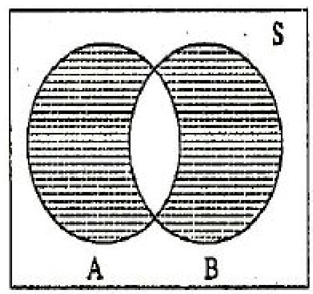




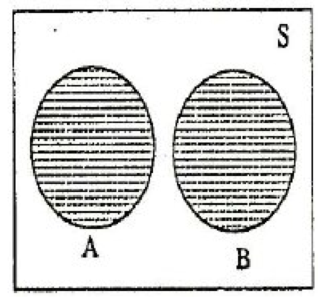
Symmetric difference(A∆ B):



A ∆ B = (A – B) ∪ (B – A)

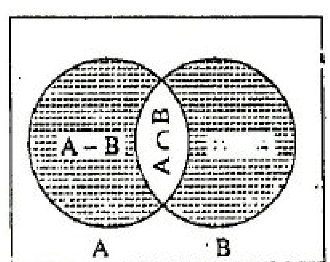


A ∆ B
When neither A ⊆ B nor B ⊆ A
and A and B are not disjoint



A ∆ B = (A – B) ∪ (B – A) = A ∪ B
When A and B are disjoint

Note: The number of distinct elements of a finite set A is denoted by $n(A)$. Let $n(A)$, $n(B)$ and $n(A \cap B)$, where A and B are non-empty sets. Then $n(A \cup B) = n(A) + n(B) - n(A \cap B)$



In case A and B are disjoint sets, so we have $A \cap B = \phi$, then $n(A \cup B) = n(A) + n(B)$

From the above Venn-Diagram, the following results are clearly true $n(A) = n(A - B) + n(A \cap B)$

(a) $n(B) = n(B - A) + n(A \cap B)$
(b) $n(A) \cup B) = n(A - B) + n(B - A) + n(A \cap B)$

Then result, $n(A \cap B) = n(A) + n(B) - n(A \cap B)$ can be generalized as,

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(B \cap C) - n(A \cap C) + n(A \cap B \cap C)$$

Example: If 63% of persons like orange where 76% like apples. What can be said about the percentage of persons who like both oranges and apple?

Let n(s) = total number of persons = 100

$A = \{x: x \text{ likes oranges}\}$, $B = \{x: x \text{ likes apples}\}$

$n(A) = 63$, $n(B) = 76$, $A \cap B = \{x: x \text{ likes oranges and apples both}\}$

Now, $n(A \cup B) = n(A) + n(B) - n(A \cap B)$

$\therefore n(A \cap B) = n(A) + n(B) - n(A \cup B) = 63 + 76 - 100 = 39 = n(A \cap B) = 39$

Hence, 39% people like both oranges and apples.

Example: In a group of 1000 people, there are 750, who can speak Hindi and 400, who can speak Bengal. How many can speak Hindi only? How many can speak Bengali only? How many can speak?

Solution: Let $A = \{x: x \text{ speaks Hindi}\}$ and $B = \{ x: x \text{ speaks Bengali})$

$\therefore A - B = \{x: x \text{ speaks Hindi and can not speak Bengali}\}$

$B - A = \{x: x \text{ speaks Bengali and can not speak Hindi}\}$

$A \cap B = \{x: x \text{ speaks Hindi and Bengali both}\}$

Given, $n(A) = 750$, $n(B) = 400$ $n(A \cup B) = 1000$

$\therefore n(A \cup B) = n(A) + n(B) - n(A \cap B) = 750 + 400 - 100 = 1150 - 1000 = 150$

So, 150 people are speaking Hindi and Bengali both.

Again, $n(A) = n(A - B) + n(A \cap B)$, $n(A - B) = n(A) - n(A \cap B) = 750 - 150 = 600$

Hence, 600 people are speaking Hindi only,

Finally, $n(S - A) = n(B) - n(A \cap B) = 400 - 150 = 250$ So, 250 people are speaking Bengali only.

1.8 Cartesian product of Sets

An ordered pair (a, b) consists of two objects a the b in a given fixed order.

We call a and b as the first and second coordinates respectively of the ordered pair (a, b). a and b may have equal values. Two ordered pairs (a, b) and (x, y) are said to be equal if $a = x$ and $b = y$ and we write $(a, b) = (x, y)$. Thus $(1,2) \neq (2,1)$. A distinction between the ordered pair $(1,2)$ and the set $\{1,2\}$ is that $(1,2) \neq (2,1)$ but $\{1,2\} = \{2,1\}$.

Definition: Let A and B be two sets. The set of all ordered pairs (a, b), where the first coordinate a of (a, b) is an element of A and the second coordinate b is an element of B is called the Cartesian product or simply product of sets A and B and is written as $A \times B$.

Symbolically, $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$

Example: Let $A = \{1,2\}$ and $B = \{a, b, c\}$. Find $A \times B$, $B \times A$, and $A \times A$.

Solution: $A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$

$B \times A = \{(a,1),(a,2),(b,1),(b,2),(c,1),(c,2)\}$. And $A \times A = \{(1,1),(1,2),(2,1),(2,2)\}$

The Cartesian product $A \times A$ is written as A^2 and we see from the above example that in general $A \times A \neq B \times A$

Generalizing the definition of the cartesian product of two sets, we define the cartesian product of n sets $A_1, A_2, \dots, A_n$ as follows:

$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2 \dots a_n) : a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$

Example: Find x, y if $(2x-3, 3y-1) = (5,5)$

Solution: We know that $(2x-3, 3y-1) = (5,5)$ if $2x-3=5$ and $3y-1=5$

$\Rightarrow x = 4$ and $y = 2$

Example: Let $A = \{1,2,4\}, B = \{2,5,7\}$ and $C = \{1,3,7\}$. Show that

$$A \times (B \cap C) = (A \times B) \cap (A \times C)$$

Solution: $B \cap C = \{7\}$ $\therefore A \times (B \cap C) = \{(1,7),(2,7),(4,7)\}$

Again $A \times B = \{(1,2),(1,5),(1,7),(2,2),(2,5),(2,7),(4,2),(4,5),(4,7)\}$ and

$A \times C = \{(1,1),(1,3),(1,7),(2,1),(2,3),(2,7),(4,1),(4,3),(4,7)\}$

$\therefore (A \times B) \cap (A \times C) = \{(1,7),(2,7),(4,7)\}$ Hence $A \times (B \cap C) = (A \times B) \cap (A \cap C)$

<u>Check your progress</u>

(1) If $A = \{2,3,4,5,6\}$, $B = \{3,4,5,6,7\}$, $C = \{4,5,6,7,8\}$, then find

(i) $(A \cup B) \cap (A \cup C)$ (ii) $(A \cap B) \cup (A \cap C)$ (iii) $(A - B)$ *and* $(B - C)$ (iv) $A \Delta B$

(2) Show the following sets by Venn-Diagram.

(i) $(A-B)'$

(ii) $A - A'$

(iii) $A' \cap B$

(3) In a group of 45 students, 22 can speak Hindi only, 12 can speak English only. How many can speak both Hindi and English?

(4) If $A = \{2, 4, 5\}$, $B = \{1, 3, 6, 7\}$, $C = \{7, 8\}$ Find $\{A \times B\} \cup \{B \times C\}$

Answer/Solution

(1) (i) $\{2, 3, 4, 5, 6, 7\}$. (ii) $\{3, 4, 5, 6\}$. (iii) $\{2\}$ and $\{3\}$ (iv) $\{2, 7\}$

(3) $n(H \cup E) = 45$, $n(H) - n(H \cap E) = 22$, $n(E) - n(H \cap E) = 12$.

$n(H \cup E) = n(H) + n(E) - n(H \cap E) = 22 + 12 + n(H \cap E)$

$45 - 34 = n(H \cap E) = 11.$

(4) $\{A \times B\} \cup \{B \times C\} = \{(2,1), (2,3), (2,6), (2,7), (4,1), (4,3), (4,6), (4,7), (5,1), (5,3), (5,6), (5,7)\} \cup \{(1,7), (1,8), (3,7), (3,8), (6,7), (6,8), (7,7), (7,8)\} = \{(2,1), (2,3), (2,6), (2,7), (4,1), (4,3), (4,6), (4,7), (5,1), (5,3), (5,6), (5,7)\} \cup \{(1,7), (1,8), (3,7), (3,8), (6,7), (6,8), (7,7), (7,8)\}$

Suggested Further Readings

(1) Felix. H. (1978), Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983),Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S.Ganguly and M.N.Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

Unit – 2

Relation

Structure

2.1 Introduction

Relation has got tremendous application in almost every field, social, economy, engineering, technology etc. In computer science concept of relation is a major tool to learn to understand it more clearly.

2.2 Objectives

After reading this unit we should be able to

- recall the basic properties of relations
- derive other properties with the help of the basic ones
- identify various types of relation
- Relationship between equivalence classes and partition.

2.3 Relation

The word "relation" suggests some familiar examples of relations between two people such as the relation of father to son, mother to son, brother to sister, etc. If A is the set of real numbers then there are many commonly used relations between two real numbers such as "less than", "greater than" or that of "equality". These examples suggest relationship between two objects. A relation, which describes relationship between two objects is called a *binary relation*. If a relation describes relationship among three objects then it is called *ternary relation*. For example, the relation described as "three integers $a,b,$ and c in the set $\{1,2,3,\ldots,15\}$ are related if their sum $a+b+c$ is divisible by 5", is a ternary relation on the set $\{1,2,3,\ldots,15\}$. In this relation, the integers 2,3 and 5 are related because their sum is divisible by 5 but the integers 1,2 and 4 are not related. The relation between parents and child on the set of human beings is also ternary relation. In general, an n-ary relation among the sets $A_1+A_2+A_3,\ldots A_n$ is a set of n-tuples in which first coordinate is an element of A_1, the second coordinate is an element of $A_2\ldots$, and the n^{th} element of A_n.

Here, we shall only consider binary relations. Such a relation between two objects can be defined by listing the two objects as an ordered pair. A set of all such ordered pairs, in each of which first elements is related to the second elements describes a binary relation. We shall call a binary relation simply as relation.

Definition: Let A and B be two sets. A binary relation (or simply a relation) from A to B is a subset of $A\times B$. Symbolically, R is a relation from A to B if $R\subseteq A\times B$.

If R is a relation from A to B and if the ordered pair $(a,b)\in R$ then we say that the element a is related to the element b by R and we also write aRb which is read as "a is R-related to b". If x is not related by y, we write $(x,y)\notin R$.

Relation on a Set: Let R be a relation from A to B. If $A=B$ then we say that R is a relation on the set A instead of saying that R is a relation from A to A. Thus a relation on a set A is a subset of $A\times A$.

Example: Let $A=\{1,2,3\}$ and $B=\{p,q\}$

Then $R=\{(1,p),(2,q),(3,q)\}$ is a relation from A to B.

Example: Let I be the set of integers. Define the following relation (less than) on I. xRy if and only if $x < y$. Then $R = \{(x, y) : x, y \in \text{I and} x < y$

Example: Let $A = \{1, 2, ..., 12\}$. Define the following relation R on A:

a, R, b if and only if a divides b. Then

R={(1,1),(1,2),(1,3),(1,4),(1,5),(1,6),(1,7),(1,8),(1,9),(1,10),(1,11),(1,12),(2,2),(2,4),(2,6),(2,8),(2,10),(2,12),(3,3),(3,6),(3,9),(3,12),(4,4),(4,8),(4,12),(5,5),(5,10),(6,6),(6,12)}.)

Example: Let S be a set. Let R be a relation in $p(S)$, $R \subseteq p(S) \times p(S)$ given by

$R = \{(A, B) : A, B \in p(S) \text{ and } A \subseteq B\}$, Now $(A, B) \in R \Rightarrow A \subseteq B$. Or $ARB \Rightarrow A \subseteq B$.

Example: Let X be a set and let Δ is called the *relation of equality or diagonal relation in X and we write* $x \Delta y$ iff $x = y$.

Example: If $R = X \times X - \Delta$. Then $(x, y) \in R \Rightarrow (x, y) \in X \times X$, $(x, y) \notin \Delta$ i.e. xRy iff $x \neq y$

R is called the relation of inequality in X. Thus we can say that the relation R of inequality in a set X is the complement of the diagonal relation Δ in $X \times X$.

Example: Let R be a relation in the set Z of integers given by $R = \{x, y): x < y, x, y \in Z\}$ where '<' has the usual meaning in Z. Since $3 < 4$, therefore $(3, 4) \in R$ or $3R4$. But $(4, 3) \notin R$, since $4 > 3$.

Example: Let A and B be two finite sets having m and n elements respectively. Find the number of distinct relations that can be defined from A to B. The number of distinct relations from A to B is the total number of subsets of $A \times B$.

2.4 Binary Relations in a Set

A binary relation R is said to be defined in a set A if for any ordered pair $(x, y) \in A \times A$, it is meaningful to say that xRy is true or false. In other words, $R = \{(x, y) \in A \times A: xRy$ is true}.That is, a relation R in a set A is a subset of $A \times A$. So, the binary relation is a relation between two sets, these sets may be different or may be identical, For the sake of convenience a binary relation will be written as a relation.

2. 5 Domain and Range of a Relation

The domain D of the relation R is defined as the set of elements of first set of the ordered pairs which belongs to R, i.e., $D = \{(x, y) \in R, \text{ for } x \in A\}$.

The range E of the relation R is define as the set of all elements of the second set of the ordered pairs which belong to R, i.e., $E = \{y: (x, y) \in R, \text{for } y \in B\}$. Obviously, $D \subseteq A$ and $E \subseteq B$.

Example: Let $A = \{1, 2, 3, 4\}$ and $B = \{a, b, c\}$. Every subset of $A \times B$ is a relation from A to B. So, if $R = \{(2, a), (4, A), (4, c)\}$, then the domain of R is the set $\{2,4\}$ and the range of R is the set $\{a, c\}$

Representation of a Relation by a Matrix and a Graph

A relation from a finite set A to a finite set B can also be represented by a matrix called *relation matrix* of R.

Let $A = \{a_1, a_2, ... a_m\}$ and $B = \{b_1, b_2, ... b_n\}$ and R be a relation from A to B. Define an $m \times n$ matrix whose m rows correspond to the m elements in A and the n columns correspond to the n elements in B as follows: The matrix element

$$r_{ij} \begin{cases} 1 & \text{if } a_i R b_j \\ 0 & \text{if } a_i R b_j \end{cases}$$

where r_{ij} is the element in the i^{th} row and j^{th} column.

Example: Let $A = \{a, b, c, d\}$ and $B = \{\alpha, \beta, \gamma\}$. Then $R = \{(a,\alpha),(b,\gamma),(c,\gamma),(d,\beta)\}$ can be represented in relation matrix as:

$$\begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \alpha\ \beta\ \gamma \\ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \end{array}$$

A relation can also be represented pictorially by drawing its graph. Here we shall use the term graphs only as a tool to represent relations. Let R be a relation in a set $A = \{a_1, a_2, ... a_m\}$. The elements of A are represented by small circles called vertices or nodes. The vertices corresponding to the element a_i is labeled as a_i. If $a_i\ Ra_j$, that is, if $(a_i, a_j) \in R$, then we join vertices a_i and a_j by means of an are called edge and put an arrow on the edge in the direction from a_i to a_j. When all the vertices corresponding to the ordered pairs in R are connected by edges with proper arrows, we get a graph of the relation R.

Example: Let $A=\{1,2,3,4,5,\}$ and

Let $R=\{(1,2),(1,3),(1,4),(1,5),(2,3),(2,4)(2,5),(3,4)(3,5),(4,5)\}$ .Then the relation R can be represented in graph.

Domain and Range of a Relation: Let R be a relation from A to B. That is , $R \subseteq A \times B$. The *domain* D of the relation R is the set of all first elements of the ordered pairs which belong to R. Symbolically,

$D=\{x : x \in A$ and $(x,y) \in R$ for some $y \in B\}$

The *range* E of the relation R is the set of all second elements of the ordered pairs which belong to R. Symbolically,

$E=\{y : y \in B$ and $(x,y) \in R$ for some $x \in A\}$.

Obviously, for any relation $R \subseteq A \times B$, domain $\subseteq A$ and range $\subseteq B$.

Example: Let $A=\{1,2,3,4\}$ and $B=\{\alpha,\beta,\gamma\}$.

Let $R=\{(2,a),(4,a),(4,b)\}$ be a relation. Then domain of R is the set $\{2,4\}$ and range of R is the set $\{\alpha,\beta\}$.

2.6 Types of Relations

(1) Power Set :

Suppose that the set A has m elements and the set B has n elements. Then the product $A \times B$ has mn elements. Therefore the power set of $A \times B$, that is, $P(A \times B)$ will have 2^{mn} elements. Thus $A \times B$ have 2^{mn} different subsets. Now since every subset of $A \times B$ is a relation from A to B, therefore we shall have 2^{mn} different relation from A to B.

(2) Inverse relation :

Let R be a relation from A to B. The inverse relation of R, denoted by R^{-1}, is a relation from B to A defined by:

$R^{-1}\{(y,x) : y \in B, x \in A$ and $(x,y) \in R\}$. In other words, $(x,y) \in R$ if and only if $(y,x) \in R^{-1}$.

Example : Let $A=\{a,b,c\}, B=\{1,2,3\}$ and $R=\{(a,1),(a,3),(b,3)\}\{c,3\}$.Then

$$R^{-1}=\{(1,a),(3,a),(3,b)\}\{3,c\}$$

Example : Let $A = \{1,2,3\}$, $B=\{a, b\}$ and $R=\{(1,a), (1, b), (3,a), (2, b)\}$ be a relation from A to B. The inverse relation of R is $R^{-1} = \{(a,1), (b, 1), (a, 3), (b,2)\}$

Example : Let $A= \{2,3,4\}$, $B=\{2,3,4\}$ and $R=\{(x,y) : |x - y| = 1\}$ be a relation from A to B. That is, $R =\{(3,2), (2,3), (4,3), (3, 4)\}$. The inverse relation of R is $R^{-1}=\{(3, 2), (2, 3), (4, 3), (3, 4)\}$. It may be noted that $R=R^{-1}$.

Note : every relation has an inverse relation. If R be a relation from A to B, then

R^{-1} is a relation from B to A and $(R^{-1})^{-1}=R$.

Theorem 2.3.1 : If R be a relation from A to B, then the domain of R is the range of R^{-1} and the range of R is the domain of R^{-1}.

Proof : Let $y\in$ domain of R^{-1}. Then there exist $x\in A$ and $y\in B$, $(y, x)\in R^{-1}$. But $(y, x)\in R^{-1} \Rightarrow (x, y)\in R$. $\Rightarrow y\in$ range of R.

Therefore, $y\in$ domain $R^{-1} \Rightarrow y\in$ range of R. Hence domain of $R^{-1} \subseteq$ range of R. In a similar way we can prove that range of $R \subseteq$ domain of R^{-1}. Therefore, domain of R^{-1}= range of R. In a similar manner it can be shown that domain of R=range of R^{-1}.

Identity Relation: A relation R in a set A is said to be identity relation, if $I_A=\{x,x) : x\in A\}$. Generally it is denoted by I_A.

Example : Let $A = \{1,2,3\}$ then $R=A\times A=\{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2),(3,3)\}$ is a universal relation in A.

Void (empty) Relation : A relation R in a set A is said to be a void relation if R is a null set, i.e., if $R= \phi$.

Example: Let $A = \{2,3,7\}$ and let R be defined as 'aRb if and only if 2a = b ' then we observe that $R=\phi\subset A \times A$ is a void relation.

Example: Let $A = \{1, 2, 3\}$. We consider several relations on A.

(i) Let R_1 be the relation defined by $m<n$, that is, mR_1n if and only if $m<n$.
(ii) Let R_2 be the relation defined by mR_2n if and only if $|m - n| \leq 1$.
(iii) Define R_3 by $m = n \pmod 3$, so that mR_3n if and only if $m = n \pmod 3$.
(iv) Let E be the 'equality relation' on A, that is, mEn if and only if $m=n$.

Example : Let $A = \{1,2,3,4,5\}$ and $B=\{a, b, c\}$ and let $R= \{(1, a), (2,a), (2, c), (3, a,), (3, b), (4, a), (4, b), (4, c), (5, b)\}$.

2.7. Difference between relation and functions

Suppose A and B are two sets. Let f be a function from A to B. Then f is a subset of $A\times B$ satisfying the following two conditions:

1. For each $a\in A$, the ordered pair $(a,b)\in f$ for some $b\in B$.
2. If $(a,b)\in f$ and $(a,c)\in f$ then $b=c$.

On the other hand, every subset of $A\times B$ is a relation from A to B. Thus every function is a relation but every relation is not necessarily a function. In a relation from A to B an element of A may be related to more than one element in B. Also there may be some elements of A which may not be related to any element of B. But in a function from A to B each element of A must be associated to one and only one element of B.

Example: Let $A=\{1,2,3,4\}$ and $B=\{a,b,c\}$. Then $R=\{(1,a),(2,a),(3,a)\}\{4,a\}$

is both relation and function from A to B. But $S=\{(1,a),(2,b),(1,c),(3,a)\}$

is a relation from A to B but not a function from A to B because the element 1 of A is associated to two different elements a and c of B.

2.8 Composition of Relations

Let A,B and C be sets and let R be a relation from A to B and let S be a relation from B to C, that is , $R\subseteq A\times B$ and $S\subseteq B\times C$. Then the composition of R and S, denoted by $R\circ S$, is the relation from A to C defined by setting $(a,c)\in R\circ S$ is any only if there exists an element $b\in R$ such that $(a,b)\in R$ and $(b,c)\in S$.

Suppose the R is a relation on a set A, that is $R\subseteq A\times A$. Then $R\circ R$, the composition of R with itself is always defined and $R\circ R$ is sometimes denoted by R^2 .Similarly, $R^3=R^2\circ R=R\circ R\circ R$ and so on. Hence R^n is defined for all positive integers n.

Example: Let $A=\{1,2,3,4\},B=\{a,b,c,d\},C=\{x,y,z\}$

And let $R=\{(1,a),(2,d),(3,a),(3,b),(3,d)\}$ and $S=\{(b,x),(b,z),(c,y),(d,z)\}$.

Then $R\circ S=\{(2,z),(3,x),(3,z)\}$.

Example: Let $X\Rightarrow$Set of all women, Y=Set of all men, Z=Set of all human beings.

Let R_1 be a relation from X to Y given by $R_1=\{(x, y) : x\in X, y\in Y$ and x is wife of $y\}$

And let R_2 be a relation from Y to Z given by $R_2 = \{(y, z): y \in Y, z \in Z$ and y is father of $z\}$. Therefore $R_2 o R_1 = \{(x, z) \in X \times Z$: for some $y \in Y$ $(x, y) \in R_1$ and $(y, z) \in R_2\}$. Here $R_2 o R_1$ is the relation 'is mother of' provided a man can have only wife.

Example: If R_1 be a relation form the set X to the set Y, R_2 a relation from the set Y to the set Z and R_3 a relation from the set Z to the set W. Then $R_2 o (R_2 o R_1) = (R_2 o R_2) o R_1$, that is **composition of relation is associative :**

Now $R_2 o R_1 \subseteq X \times Z$ and $R_2 \subseteq Z \times W$. Therefore $R_2 o (R_2 O R_1) \subseteq X \times W$, that is, a relation from X to W. Similarly $(R_2 o R_1) o R_1 \subseteq X \times W$; that is, a relation from X to W. Now $(x, w) \in R_2 o (R_2 o R_1) \Leftrightarrow \exists z \in Z | (x,z) \in R_1$ and $(R, z) \in R_2$ & $(z, w) \in R_2 \Leftrightarrow \exists z \in Z, y \in Z, y \in Y (x, y) \in R_1$ and $(y, z) \in R_2$ & $(z, w) \in R_2$

(Since $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$) $\Leftrightarrow \exists y \in Y | (x, y) \in R_1$ and $(y, w) \in R_3 o R_2$. $\Leftrightarrow (x, w) \in (R_2 o R_2) o R_1$. Therefore $R_3 o (R_2 o R_1) = (R_2 o R_2) o R_1$.

Check your progress

(2.1) Prove that $(R^{-1})1 = R$.

(2.2) Prove that $(R_2 o R_1)\text{-}1 = R_1^{-1} o R_2^{-1}$.

Reversal Rule: From the above we get the inverse of the composite of two relations is the composite of their inverse in the reverse order

Solution :

(2.1). Let $R \subseteq X \times Y$. then $R^{-1} \subseteq Y \times Y$. Therefore $(R^{-})^{-1} \subseteq X \times Y$. Now $(x, y) \in R \Leftrightarrow (y, x) \in R^{-1} \Leftrightarrow (x, y) \in (R^{-1})\text{-}1$ Hence $R = (R^{-1})^{-1}$.

(2.2). Let $R_1 \subseteq X \times Y, R_2 \subseteq Y \times Z$. then $R_2 o R_1 \subseteq X \times Y$. Hence $(R_2 o R_1)^{-1} \subseteq Z \times X$. Now $R_1^{-1} o R_2^{-1} \subseteq Z \times Y$ (prove). Now $(z, x) \in (R_2 o R_1)^{-1} \Leftrightarrow (x, z) \in R_2 o R_1 \Leftrightarrow (x, y) \in R_1$ and $(y, z) \in R_2$ for some $y \in Y \Leftrightarrow (y, x) \in R_1^{-1}$ and $(z, y) \in R_2^{-1}$ for some $y \in Y \Leftrightarrow (z, y) \in R_2^{-1}$ and $(y, x) \in R_1^{-1}$ for some $y \in Y \Leftrightarrow (z, x) \in R_1^{-1} o R_2^{-1}$. Hence $(R_2 o R_1)^{-1} = R_1^{-1} o R_2^{-1}$.

To find composition of Relations using Matrices

There is another way of finding $R \circ S$ using matrix representations of R and S. Let M_R and M_S denote matrices of the relations R and S respectively. Consider the matrix M obtained by multiplying M_R and M_S. That is $M = M_R M_S$. Then the elements corresponding to the non-zero entries in M are related by $R \circ S$. In other words $M = M_R M_S$ and $M_{R \circ S}$ have the same non-zero entries. That is $(i, j)^{th}$ element in M is non-zero if and only if $(i, j)^{th}$ element in $M_{R \circ S}$ is non-zero. Note that the non-zero entries in M and $M_{R \circ S}$ may not have the same values.

Example : Let us consider the above example. Then

$$M_R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array} \quad \text{and} \quad M_S = \begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

Multiplying M_R and M_S we obtain the matrix

$$M = M_R M_S = \begin{array}{c} \begin{array}{ccc} x & y & z \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

Corresponding to non-zero entries in M, we obtain the relation

$$R \circ S = \{(2,z),(3,x),(3,z)\}.$$

2.9 Properties of Relations on a Set

Consider the given set A. In this section we discuss a number of important types of relations, which are defined on A.

Reflexive relation : A relation R on a set is said to be reflexive relation if

$(a,a) \in R \;\; \forall a \in A$. Thus relation R is reflexive if we have $aRa, \; \forall a \in A$.

A relation is not reflexive if there exists an $a \in A$ such that $(a,a) \notin R$.

Example : Let A be the set of positive integers. Define a relation R on A as follows: aRb if and only if a divides b.

Since every integer always divides itself, R is a reflexive relation.

Example : Let $A=\{1,2,3,4\}$. Then $R=\{(1,1),(2,3),(2,4),(3,3),(4,1),(4,4)\}$ on *A* is not reflexive since $2\in A$ but $(2,2)\notin R$.

Clearly a relation on a set *A* represented by a matrix will be reflexive if and only if all the entries on the main diagonal of the matrix are 1.

Symmetric relation : A relation *R* on a set *A* is said to be symmetric relation if $(a,b)\in R \Rightarrow (b,a)\in R$. Thus *R* is symmetric if whenever *aRb* then *bRa*.

A relation *R* is not symmetric if there exists $a,b\in A$ such that $(a,b)\in R$ but $(b,a)\notin R$.

Example: Let $A=\{a,b,c\}$

$$R_1 = \{\ \}$$
$$R_2 = \{(a,a),(b,b)\}$$
$$R_3 = \{(a,b),(b,a)\} \text{ and}$$
$$R_4 = A\times A$$

Then all four R_1, R_2, R_3, and R_4 are symmetric relations. The relation R_1 is called empty relation or the void relation on *A*, while the relation R_4 which is eaual $A\times A$ is called universal relation on *A*.

Example : Let *A* be the set of positive integers. Define a relation *R* on *A* as follows: $(a,b)\notin R$ if and only if $a\geq b$.

Then the relation *R* is not symmetric because (10,9) $\in R$ but (9,10) is not in *B*.

Clearly, a relation on set *A* represented by a matrix will be symmetric if the entries in the matrix are symmetrical with respect to the main diagonal.

Anti-symmetric relation : A relation *R* on a set *A* is said to be anti-symmetric relation if (a, b) $\in R$ and $(b,a)\in R$ then $a=b$. Thus *R* is anti-symmetric if (a,b) in *R* implies that (b,a) is not in *R* unless $a=b$.

A relation *R* on a set *A* is not anti-symmetric if there exists elements a,b in *A* such that aRb, bRa but $a\neq b$

Example : Let N be the set of natural numbers. Let R be the relation on N defined by "x is a divisor of y". Then R is anti-symmetric since a divides b and b divides a implies $a = b$.

Example : Let A be the set of positive integers and R be a relation on A such that (a,b) is in R if and only $a \geq b$. Then R is an anti-symmetric relation.

Example : Let $A = \{a,b,c\}$ and let relation R on A is given by R=$R = \{(a,b),(a,c),(c,a)\}$. Then R is not anti-symmetric.

Transitive relation : A relation R on a set A is said to be transitive relation if

$(a,b) \in R$ and $(b,c) \in R \Rightarrow (a,c) \in R$. Thus R is transitive if aRb, bRc then aRc.

A relation R on a set A is not transitive if there exists elements a, b and $c \in A$, not necessarily distinct, such that: $(a,b) \in R$, $(b,c) \in R$ but $(a,c) \notin R$

If R is transitive relation on A then it is clear that $R \circ R \subseteq R$.

Example : The relation $\leq$ is a transitive relation on the set of real numbers.

Example : Let A be set of positive integers. Define a relation R on A as follows: aRb if and only if a divides b. Then R is a transitive relation because if a divides b and b divides c then a divides c.

Example : Let A = the set of all lines in the plane. Define the following relation R on A: $l_1 R l_2$ and only if l_1 is perpendicular to l_2, where l_1 and l_2 are lines in the plane. Then R is not a transitive relation.

Transitive Extension and Transitive Closure of a rotation : Let R be a relation on A. Then the *transitive extension* of R is a relation R_1 on A defined by $R_1 = R \cup (R \circ R)$, where $R \circ R$ is the composition of relation R with itself. Thus R_1 contains R and moreover if (a,b) and (b,c) are in R then (a,c) is also in R_1.

It is obvious that a relation R on A is transitive if and only if the transitive extension R_1 of R is equal to R. That is $R_1 = R$.

Difinition: Let R be a relation on A. The transitive closure R^* of R is the relation on A such that.

1. R^* is transitive
2. $R \subseteq R^*$
3. R^* has the fewest possible elements.

Thus the transitive closure of relation R is the smallest transitive relation on A containing R. Given a relation R on a set A, the transitive closure R^* can be determined as follows:

Step1. Calculate $R_1 = R \cup (R \circ R)$ and $R_{i+1} = R_i \cup (R_i \circ R_i)$, where the relation R_{i+1} is the transition extension of the relation R_i and so on.

Step2. If $R_1 = R$ then R is transitive and relation R itself is the transitive closure of R. If $R_1 \neq R$, calculate R_2.

Step3. If $R_{i+1} \neq R_i$ calculate next R_i.

Step4. if $R_{i+1} = R_i$ stop. The transitive closure R^* of R is the relation R_i. That is, $R^* = R_i$.

Example: Let $A = \{1,2,3,4\}$ and let R be a relation on A defined by $R = \{(1,1),(1,2),(2,4),(3,2),(4,3)\}$. Find the transitive closure of R.

Solution: The matrix of the relation R is given by

1 2 3 4

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

Multiplying M_R with itself, we obtain,

$$\begin{array}{c} \quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad 1\;2\;3\;4 \end{array}$$

$$M = M_R M_R \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Corresponding to non-zero entries in M, we obtain $R \circ R = \{(1,1),(1,2),(1,4),(2,3),(3,4),(4,2)\}$

$\therefore R_1 = R \cup (R \circ R) = \{(1,1),(1,2),(1,4),(2,3),(2,4),(3,2),(3,4),(4,2),(4,3)\}$.

Since $R_1 \neq R$, we will calculate $R_2 = R_1 \cup (R_1 \circ R_1)$.

The matrix of relation R_1 is given by

$$M_{R_1} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

Multiplying M_{R_1} with itself, we obtain

$$M' = M_{R_1} M_{R_1} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 2 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Corresponding to non-zero entries in M', we obtain

$(R_1 \circ R_1) = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3),(4,4)\}$

$\therefore R_2 = R_1 \cup (R_1 \circ R_1) = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3),(4,4)\}$

Again since $R_2 \neq R_1$, we will calculate $R_3 = R_2 \cup (R_2 \circ R_2)$.

The matrix of relation R_2 is given by

$$M_{R_2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Multiplying M_{R_2} with itself, we obtain $M'' = M_{R_1} M_{R_2} \begin{bmatrix} 1 & 4 & 4 & 4 \\ 0 & 3 & 3 & 3 \\ 0 & 3 & 3 & 3 \\ 0 & 3 & 3 & 3 \end{bmatrix}$

Since non-zero entries in M_{R_2} and M'' are same, therefore $R_2 \circ R_2 = R_2$. Thus $R_3 = R_2$.

Since $R_3 = R_2$, the transitive closure R^* of R is the relation R_2.

Hence $R^* = \{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,2),(3,3),(3,4),(4,2),(4,3),(4,4)\}$.

2.10 Partially Ordered Sets

Definition : A relation R on a set A is said to be partial order if R is reflexive, anti symmetric and transitive. Thus a relation R on a set A is partial order relation if the following conditions hold:

1. **Reflexivity** : aRa $\forall$ a$\in$A
2. **Anti-symmetry** : if aRb, bRa then a = b.
3. **Transitivity** : If aRb, bRc then aRc

The set A together with the partial order R is called partially ordered set.

For convenience, we generally denote a partial order by the symbol $\leq$ in place of R. We read $\leq$ as less than or equal to. The symbol $\leq$ does not necessarily mean usual "less than or equal to" as is used for real numbers. If $\leq$ is partial order on A, then the ordered pair (A, $\leq$) is called a partially ordered set or simply a poset.

Example : Let A be a collection of subsets of a set S. the relation $\subseteq$ of set inclusion is a partial order on A. Theu (A, $\subseteq$) is poset.

Example : The relation $\leq$ of divisibility is partial order on the set N of natural numbers. Here a $\leq$ b means a | b (a divides b).

Example : The relation < on N is not a partial order, since it is not reflexive.

Example : In the set [*R* of real numbers, the relation $\leq$ having its usual meaning in *R* is a total order relation. The proof is left as an exercise.

Example : If S be a set, then the relation in *p* (*S*) given by : for *A, B*$\in$*p*(*S*). *A*$\leq$*B*, is a partial order relation but not a total order relation. The proof is left as an exercise.

Definition : Let (A, $\leq$) be a poset. The elements a and b of A are said to be comparable if a$\leq$ b or b$\leq$ a.Thus a and b are non comparable if neither a$\leq$ b nor b$\leq$ a.

Example : Consider the poset in Example 2.51. The elements 1 and 5 are not comparable since neither 2 divides 5 nor 5 divides 2. Thus in a poset every pair of elements need not be comparable.

Let (A, $\leq$) be a poset. We say a < b if a$\leq$ b and a$\neq$b. We also say b in larger than or equal to a and write b$\leq$ a a if a $\leq$ b.

Definition : Let (*S*, $\leq$) be a partially ordered set. If $x\leq y$ and $x\neq y$, then x is said to be strictly smaller than or strictly predecessor of y. We also say that y is strictly greater than or strictly successor of y. denote it by $x<y$.

An element $a\in S$ is said to be a least or first (respectively greatest or last) element S if $a\leq$(respectively $x\leq A$)$\forall x\in S$).

An element $a \in S$ is called minimal (respectively maximal) element of S is $x \leq a$ (respectively $a \leq x$) implies $a=x$ where $x \in S$.

Example : $(N, \leq)$, (the relation $\leq$ having its usual meaning) is a partially ordered set. 2 is strictly smaller than 5 or $2 < 5$. 1 is the least or first element of N. since, $1 \leq m \forall m \in N$, There is no greatest or last element of N. 1 is the only minimal element since if $x \in N$, Then $x \leq 1 \Rightarrow x = 1$.

Example : Consider the set S = {1, 2, 3, 4, 12}. Let $\leq$ be defined by $a \leq b$ if a divides b. Then 2 is strictly smaller than 4 or $2 < 4$. 12 is strictly greatest than 4 or $4 < 12$. Since I divides each of the number 1,2,3,4,12 so $1 \leq x \forall x \in S$, hence 1 is the least element of S. Again since $x \leq 12 \forall x \in S$ i.e. each element of S divides 12, so 12 is the greatest or last element of S. Here also I is the only minimal element, since $x \in S$, then $x \leq 1$ i.e. x divides 1 implies $x = 1$.

Example : Let S be a set. Then $(p\ (S), \leq)$ where $\leq$ is the set inclusion relation $\subseteq$, is a partially ordered set. Then ϕ is the least element, since $\phi \subseteq A \forall A \in p(S)$, and S is the greatest element since $A \subseteq S \forall A \in p\ (S)$. Every singleton is a minimal element. For if $a \in S$, $\{a\} \in p\ (S)$ and if $X \in p\ (S)$, then $X \subseteq \{a\} \Rightarrow X = \{a\}$.

Definition : Infimum and Supermum : Let $(S, \leq)$ be a partially ordered set and A a subset of S. An element $a \in S$ is said to be a lower bound (respectively upper bound) of A if $a \leq x$ (respectively $x \leq a$) $\forall x \in A$.

In case A has a lower bound, we say that A is bounded below or bounded on the left. When A has an upper bound we say that A is bounded above or bounded on the right. Let $L(\neq \phi)$ be the set of all lower bounds of A, then greatest element of L if it exists is called the greatest lower bound ($g\ 1\ b$) or infimum of A. Similarly if $U(\neq \phi)$ be the set of all upper bounds of A, then the least element of U if it exists is called the least upper bounded ($l.u.b.$) or supremum of A

Example : Consider the partially ordered set $(N, \leq)$, where $m \leq n$ if m divides n. Consider the subset $A = \{12, 18\}$. 2 is a lower bound of A since 2 divides both 12 and 18. i.e. $2 \leq 12$ and $2 \leq 18$. The set of al lower bounds of A viz L={1,2,3,6} and 6 is the greatest element of L. Hence $g.l.b.$ or infimum of A=6. It is called the greatest common divisor ($g.c.d$) of A. Now 36, 72, 108 etc. are upper bounds of A since x divides 36 or 72 or 108 $\forall x \in A$ thus $x \leq 36$ or 72 or 108 $\forall x \in A$. Now the set of upper bounds of A viz U = {36, 72, 108, ...}, the lest element of U= 36. Hence the $l.u.b$ or supremum of A= 36. It is also called the L.C.M. of 12 and 18.

Example : Set S be a non-empty set which is not a singleton, consider the set $Y=P\ (\phi, S\}$ partially ordered by the inclusion relation. Now Y has no least or no greatest element. Each singleton as in Ex. (5.6) is the minimal element.

Let $A \subseteq Y$, $G = \cap \{X_\alpha : X\alpha \in A\}$. If $G \neq \phi$, then G is *g.l.b* of A. Similarly $L = U \{X_\alpha : X\alpha \in A\}$ is the *l.u.b* of A and exists if $L \neq A$.

Theorem : The least (respectively greatest) element of a partially set $(s, \leq)$, if it exists, is unique.

***Proof*:** If possible let l and l' be two least element of S. Since l is the least element, so $l \leq x \forall x \in S$ hence $l \leq l'$ since $l' \in S$. Similarly taking l' as lest element $l' \leq l$. Hence $l \leq l'$ and $l' \leq l$. Therefore by anti-symmetry $l = l'$. Similar proof can be given for the greatest element.

Remark : In contrast to the above theorem, maximal and minimal elements of a partially ordered set X need not be unique. In example (5.6) or (5.8)* we have shown that every singleton is a minimal element. Sometimes minimal element can also be a maximal element. For example consider the partially ordered set $\{X\Delta\}$ where Δ is the diagonal relation. Every element of X is a minimal as well as a maximal element of X. For let $a \in X$. Then $x\Delta a \Rightarrow x = a$, $a\Delta x \Rightarrow x \Rightarrow a$.

Definition : A partially ordered set $(S, \leq)$ is said to be well ordered if every non empty subset of S has a least element.

Theorem : A well ordered set $(S, \leq)$ is always totally ordered or linearly ordered or a chain.

***Proof*:** Let x, y be any two element of S. Consider the subset $\{x, y\}$ of S, which is non empty and hence has a least element either x or y, then $x \leq y$ or $y \leq x$. Hence every two element of S are comparable and so S is totally ordered. We now state two important statements without proof.

Well ordering principle : Every set can be well ordered.

Zorn's Lemma: Let S be a non empty partially ordered set in which every chain i.e. every totally ordered subset has an upper bound, then S contains a maximal

Totally ordered set or chain : Let $(A, \leq)$ be a poset. $(A, \leq)$ is called chain or totally ordered set if every two elements in A ae comparable. That is, if $a, b \in A$ then $a \leq b$ or $b \leq a$. Totally ordered sets are also called linearly orderly sets. ***Example 1:*** Let R be a relation in the set of natural numbers N defined by 'x is a multiple of y', then R is a partial order in N. 6 and 2, 15 and 3, 20 and 20 are all comparable but 3 and 5, 7 and 10 are not comparable. So N is not a totally ordered set.

Example : Let A and B be totally ordered sets. Then Cartesian product $A \times B$ can be totally ordered as follows: $(a,b) < (a', b')$ if $a < a'$ or if $a = a'$ and $b < b'$. This order is called the lexicographical order of $A \times B$, since it is similar to the way words are arranged in a dictionary.

Theorem : Every subset of a well-ordered set is well-ordered.

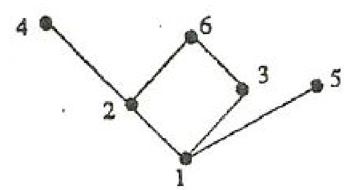
Illustration:

Let R the set of real numbers and let $\leq$ be the usual less than or equal to relation on R. Then (R, $\leq$) is poset which is a chain whereas the posets in Example 2.50 and example 2.51 are not chain.

Hasse Diagram

It is possible, at least in principle, to draw a diagram which shows at a glance the order relation on a finite poset. Let $(S, \preceq)$ be a poset. Define a relation $\preceq$ on S by 'a $<b$ if and only if $a \leq b$ but $a \neq b$', $a, b \in S$. given a partial order $\leq$ on S, b is said to cover a if $a<b$ and there is no element c in S such that $a \preceq c \preceq b$ holds. A Hasse diagram of a poset $(S, \leq)$ is a graphical representation consisting of points labeled by the members of S, with a line segment directed generally upward from a to wherever b covers a.

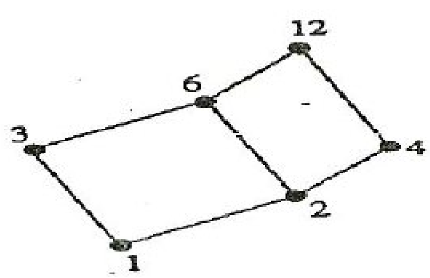
Example : Let $S = \{1, 2, 3, 4, 5, 6\}$. We define $\leq$ as $m \leq n$ if 'm divides n', that is, n is an integer multiple of m. The diagram in Figure 6 is a Hasse diagram of the poset $(S, \leq)$.



Hasse diagram of Example 1

There is no segment between 1 and 6 because 6 does not cove 1. From diagram we see that 2 covers 1 and 6 covers 2. Similarly, 4 does not cover 1 because 4 covers 2 and 2 covers 1.

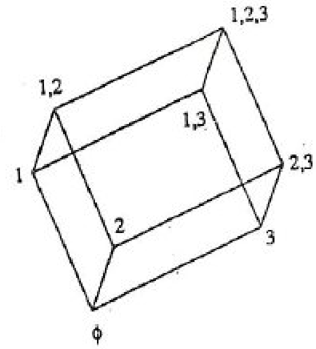
Example: S be the set of all positive divisors of 12. That is, $S = \{1, 2, 3, 4, 5, 6, 12\}$.$(S,<)$ is a poset where $a \leq b$ means 'a is a divisor of b' for $a, b \in S$.



Hasse diagram of Example 2

There is no segment between 6 and 1, because 6 does not cover 1, as 1 < 2 < 6 and 1 prec 3 < 6. Similarly, 12 does not cove 2 as 2 < 4 < 12 and 2 < 6 < 12.

Example : Let S be the power set of {1, 2, 3}. That is S = {ϕ, {1}, {2}, {3},1,2}, {1,3}, {2,3}, {1,2,3}.



Hasse diagram of Example 3

The Hasse diagram of the poset (S, ≤), where $A \leq B$ is $A \subseteq B$ for $A, B \in S$, is shown in figure

.

Example: Let X = {2, 3, 6, 12, 24, 36} and the relation ≤ be such that x≤ y if x divides y (written as x|y). Draw the Hasse diagram of (X, ≤).

Example: Let = {1, 2, 3}. Then power set of X, P(X) = {ϕ, {1}, {2}, {3}, {1,3}, {2,3}, {1,2,3}. Let ⊆ be the inclusion relation on P(X). Draw Hasse diagram of (P(X), ⊆).

Example:: Let X be the set of factors of 12 and let ≤ be the relation divides, i.e., x≤ y if and only if x|y. Draw the Hasse diagram of (X, ≤).

Example: Let P = {1, 2, 3, 4, 5} and ≤ be the relation "less than or equal to". Draw the Hasse diagram of (P, ≤).

Since any two elements of P are comparable, (P, ≤) is a totally ordered set. A totally ordered set would always have the Hasse diagram consisting of circles (or dots) one below the other as shown in the Hasse diagram of this poset. This justifies the name "chain" for a totally ordered set.

Check your progress

(1) Let R be the relation in A = {1, 2, 3, 4, 5} which is defined by 'x and y are relative prime'. Find the solution set of R and draw R on a coordinate diagram of $A \times A$.

(2) Let R be the relation in the natural numbers N defined by '$x - y$ is divisible 8'. Prove that R is an equivalence relation.

(3) Let L be the set of lines in the Euclidean plane and let

a. R be the relation in L defined by 'x is parallel to y'.

b. *R*' be the relation in L defined by '*x* is perpendicular to *y*'. State whether or not *R* and *R'* are equivalence relation.

(4) Each of the following relations in the natural number *N*

a. "$x>y$"

b. "*x* is a multiple of *y*"

c. "$x + 3y = 12$"

d. "$x \leq Y$"

e. "$x^2=y^2$"

f. "*x* is the husband of *y*"

whether or not each of the relations are (a) reflexive (b) symmetric 9c) anti-symmetric (d) transitive.

(5) Let *Z* be the set of all integers. Define a relation *R* on *Z* in the following way. $R = \{a, b\} \in Z \times Z$: $(a - b)$ is divisible by 7}.Show that *R* is an equivalence relation. Find all the distinct equivalence classes of the relation R.

(6) Show that if *R* and *S* be transitive relations on a set *A*, then $R \cup S$ is not transitive on *A*.

(7) Prove that a relation *R* on a set *A* is symmetric if and only if $R^{-1}=R$.

(8) Find the equivalence classes determined by the equivalence relation *R* on *Z* defined by '*aRb* if and only if $a - b$ is divisible by 5' for $a, b \in Z$, the set of integer.

(9) Prove that an equivalence relation *R* on a set *S* determines a partitions of *S*. Conversely, each partitions of *S* yields and equivalence relation on *S*.

(10) Find all of the partitions of $S = \{p, q, r, s\}$

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

Unit - 3

Partitions and distributions

Structure

3.1 Introduction

This is most basic unit of this block as it introduces the concept of statements,

Statement variables and the five elementary operations and associated logical connectives.

We introduce the well formed statement formulae, tautologies and equivalence of formulae. The law of duality is explained and established. It has got tremendous application in almost every field, social, economy, engineering, technology etc. In computer science concept of logic is a major tool to learn to understand it more clearly. Mathematics has a language of its own like most other sciences, which is very precise and communicates just what is required-neither more nor less. Language basically consists of words and their combinations called 'expression' or 'sentences'. However in Mathematics any expression or statement will not be called a 'sentence'.

3.2 Objectives

After reading this unit we should be able to

1. Understand the concept of statement and statement variables
2. Use elementary operations like Conjunction, Disjunction, Negation, Implication, Double implication

3. Understand statement formulae, tautologies to equivalence of formulae

4. Use law of duality and functionally complete set of connectives

Logic is a field of study that deals with the method of reasoning Logic provides rules by which we can determine whether a given argument or reasoning is valid (correct) or not. Logical reasoning is used in Mathematics to prove theorems. In computer science logic is used to verify the correctness of programs

3.3 Equivalence Relations

Let A be a non-empty set and let R be relation on A. Then R is said to be equivalent relation if it is

1. *Reflexive*. That is, for every $a \in A$, aRa.
2. *Symmetric*. That is, aRb, then bRa.
3. *Transitive*. That is, if aRb and bRc then aRc

   The equivalence relation is usually denoted by the symbol~.

Illustrations: The following are some examples of equivalence relations:

1. Equality of numbers on the set of real numbers
2. Equality of subsets a universal set
3. Congruency of triangles on the set of triangles.
4. Relation of lines being parallel on the set of lines in a plane.

Example : Let I be the set of integers. Define a relation R on I as follows: xRy if and only if $x-y$ is divisible by 5, $\forall x, y \in \text{I}$. Show that R is an equivalence relation on I.

Solution : 1. R is reflexive: Since for any $a \in \text{I}, a-a=0$ which is divisible by 5, therefore aRa. Thus R is reflexive.

2. R is *symmetric*: For any $a,b \in \text{I}$, if $a-b$ is divisible by 5, then $b-a$ is also divisible by 5. Thus, $aRb \Rightarrow bRa$. Hence R is symmetric.

3. R is *transitive*: Suppose aRb and bRc for any $a,b,c \in \text{I}$

$\Rightarrow$ both $a-b$ and $b-c$ are divisible by 5

$\Rightarrow$ $(a-b)+(b-c)$ are divisible by 5

$\Rightarrow$ $a-c$ is divisible by 5

$\Rightarrow$ aRc. Thus R is transitive.

Since R is reflexive, symmetric and transitive, therefore R is an equivalence relation.

Example : The diagonal or the equality relation Δ in a set S is an equivalence relation in S. For if $x, y \in S$ the $x\Delta y$ iff $x=y$. Thus

(α) $x\Delta x \forall x \in S$ (reflexivity)

(β) $x\Delta y \Rightarrow x = y \Rightarrow y = x \Rightarrow y\Delta x$ (Symmetry)

(γ) for $x, y, z \in S$, $[x\Delta y, y\Delta z] \Rightarrow [x=y, y=z \Rightarrow x = \Rightarrow x\Delta z$.

Hence $[x\Delta y$, and $y\Delta z] \Rightarrow \Delta$ (transitivity).

Example : Let N be the set of natural numbers. Consider the relation R in $N \times N$ given by $(a, b) R(c, d)$ if $a+d=b+c$, where $a, b, cd \in N$ and + denotes addition of natural numbers, R is an equivalence relation in $N \times N$.

(α) $(a, b)R(a, b)$ since $a+b=b+a$ (Reflexivity)

(β) $(a, b)R(c, d) \Rightarrow a+d=b+c \Rightarrow c+b=d+a \Rightarrow (c,d)R(a, b)$ (Symmetry)

(γ) $[(a, b)R(c, d), (c, d)R(e, f)] \Rightarrow [a+d=b+c, c+f=f=d+e]$

$\Rightarrow (a+d+c+f=b+c+d+e) \Rightarrow a+f=b+e$ (By cancellation laws in N) $\Rightarrow (a, b)R(e, f)$ (transitivity)

Example : Let a relation R in the set N of natural numbers be defined by: If m, $n \in N$, then mRn if m and n are both odd. Then R is not reflexive, since 2 is not related to 2. Thus $xR x$ $\forall x \in N$. But R is symmetric and transitive as can be verified.

Example : Let X be a set. Consider the relation R in $p(x)$ given by : for $A, B \in p(X)$. ARB if $A \subseteq B$. Now R is reflexive, since $A \subseteq A$, $\forall A \in p(X)$ R is transitive, since $[A \subseteq B, B \subseteq C]$ $\Rightarrow A \subseteq C$ where $A, B, C \in p(X)$. But R is not symmetric, since $A \subseteq B \not\Rightarrow B \subseteq A$.

Example : Let S be the set of all lines L in three dimensional space. Consider the relation R in S given by; for $L_1, L_2 \in S$, L_1RL_2 if L_1 is coplanar with L_2. Now R is reflexive, since L_1 is coplanar with L_1, R is symmetric, since L_1 coplanar with $L_2 \Rightarrow L_2$ coplanar with L_1. But R is not transitive, since (L_1 coplanar with L_2 and L_2 coplanar with L_3) $\not\Rightarrow L_1$ coplanar with L_3.

Example : (a) Let $X = \{x, x_2, x_3, x_4\}$. Define the following relations in X :

$R_1 = \{(x_1, x_1), (x_2, x_2), (x_3, x_3), (x_2, x_3), (x_3, x_2)\}$

$R_2 = \{ x_1, x_1), (x_2, x_2), (x_3, x_3), (x_4, x_4), (x_2, x_3), (x_2, x_4), (x_2, x_4)\}$

$R_3 = \{(x_1, x_1), (x_2, x_2), (x_3, x_3), (x_4, x_4), (x_2, x_3), (x_3, x_2), (x_3, x_4), (x_4, x_3)\}$

R_1 is symmetric, transitive but not reflexive since $(x_4, x_4) \notin R_1$

R_2 is reflexive, transitive but not symmetric since $x_3 R x_4$ but $(x_4, x_2) \notin R2$

R_3 is reflexive, symmetric but not transitive since $x_2 R x_3$ and $x_3 R x_4$ but $(x_2, x_4) \notin R2$.

Note : Examples prove that the three properties of an equivalence relation viz. reflexive, symmetric and transitive are independent of each other, i.e. no one of them can be deduced from the other two.

Example : Let A be the set of all people on the earth. Let us define a relation R in A, such that xRy if and only if 'x is father of y', Examine R is (i) reflexive, (ii) symmetric, and (iii) transitive. We have

(i) For $x \in A$, xRx does not holds, because, x is not the father of x. That is R is not reflexive.

(ii) Let xRy, i.e., x is father of y, which does not imply that y is father of x. Thus yRx does not hold. Hence R is not symmetric.

(iii) Let xRy and yRz hold. i.e., x is father of y and y is father of z, but x is not father of z, i.e., xRz does not holds. Hence R is not transitive.

Example : Let A be the set of all people on the earth. A relation R is defined on the set A by aRb if and only if a loves b' for $a, b \in A$.Examine R is (i) reflexive, (ii) symmetric, and (iii) transitive. Here,

(i) R is reflexive, because, every people loves himself. That is, aRa holds.

(ii) R is not symmetric, because, if a loves b then b not necessarily loves , i.e., aRb does not always imply bRa. Thus, R is not symmetric.

(iii) R is not transitive, because, if a loves b and b loves c then a not necessarily loves c, i.e., if aRb and bRc but not necessarily aRc. Thus R is not transitive. Hence R is reflexive but not symmetric and transitive.

Example : Let N be the set of all natural numbers. Define a relation R in N by 'xRy if and only if $x + y = 10$'. Examine R is (i) reflective, (ii) symmetric, and (iii) transitive. Here,

(i) Since $3 + 3 \neq 10$ i.e., $3R3$ does not hold. Therefore R is not reflexive.

(ii) If $a + b = 10$ then $b + a = 10$, i.e., if aRb hold then bRa holds. Hence R is symmetric.

(iii) We have, 2+8=10 and 8+2=10 but $2+2 \neq 10$, i.e. $2R8$ and $8R2$ holds but $2R2$ does not hold. Hence R is not transitive therefore R is not reflexive and transitive but symmetric.

Example : Let I be the set of all integers and R be a relation defined on I such that 'xRy if and only if $x>y$'. Examine R is (i) reflexive, (ii) symmetric and (iii) transitive. Here,

(i) R is not reflexive, because, $x > x$ is not true, i.e., xRx is not true.

(ii) R is not symmetric also, because, if $x>y$ then $y \ngtr x$. i.e., R is not symmetric

(iii) *R is transitive because* if xRy and yRz holds then xRz hold. Therefore R is not reflexive and symmetric but transitive.

Example : Let A be the set of all straight lines in 3-space. A relation R is defined on A by 'lRm if and only if l lies on the plane of m' for $l.\ m \in A$. Examine R is (i) reflexive, (ii) symmetric and (iii) transitive. Here,

(i) Let $l \in A$. then l is coplanar with itself. Therefore lRl holds for all $l \in A$. Hence R is reflexive.

(ii) Let $l, m \in A$ and lRm hold. Then l lies on the plane of m. Therefore m lies on the plane of l. Therefore $lRm \Rightarrow mRl$. Thus R is symmetric.

(iii) Le $l, m, n, \in A$ and lRm and mRn both hold. The l lies on the plane of m and m lies on the plane of n. This does not always imply that l lies on the plane of n. e.g., if l is a straight line on the $x - y$ plane and m be another straight line parallel *to* y axis and n be a line on the y – z plane then lRm and mRn hold but lRn does not hold because l and n lie on $x - y$ plane and $y - z$ plane respectively. Thus R is not transitive.

Hence R is reflexive and symmetric but not transitive.

Example : Let A be a family of sets and let R be the relation in A defined by 'A is a subset of B'. Examine R is (i) reflexive, (ii) symmetric and (iii) transitive. Then R is

(i) Reflexive, because, if $A \in A$ the $A \subseteq A$ is true.

(ii) Not symmetric, because if $A \subseteq B$ then B is not necessarily a subset of A.

(iii) Transitive, because, if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$., i.e., if ARB and BRC hold then ARC holds. Thus R is reflexive and transitive but not symmetric.

Example : A relation R is defined on the set I, the set of integers, by 'aRb if and only if $ab>0$' for $a \neq 0$, b$\neq 0 \in I$.Examine R is (i) reflexive, (ii) symmetric and (iii) transitive. Here,

(i) Let $a \in R$. Then $a.a.>0$ holds. Therefore aRa holds for all $a \in I$. Thus R is reflexive.

(ii) Let $a,\ b \in I$ and aRb holds. If $ab>0$ then $ba>0$. Therefore, $aRb \Rightarrow bRa$. Thus R is symmetric.

(iii) Let $a, b, c \in I$ and aRb, bRc hold. Then $ab > 0$ and be > 0. Therefore, $(ab)(bc) > 0$. This implies $ac > 0$ since $b^2 > 0$. So aRb and $bRc \Rightarrow aRc$. Thus **R** is transitive. Hence R is reflecsive, symmetric and transitive, hence R is an equivalence relation.

Example : Let R be a relation in a set S which is symmetric and transitive. Then $aRB \Rightarrow bRa$ (by symmetry) $[aRb$ and $bRa] \Rightarrow aRa$ (by Transitivity)

From this it may not be concluded tht fefelxivity follows from symmetry and transitivity. The fallacy involved in the above argument is:

for $a \in S$, to prove aRa, we have started with $aRb \Rightarrow bRa$.

Now it might happen that $\exists$ no element $b \in S$ such that aRb.

Example : Examine whether each of the following relations is an equivalence relation in the accompanying set –

(i) The geometric notion of similarity in the set of all triangles in the Euclidean plane.

Hint : It is an equivalence relation

(ii) The relation of divisibility of a positive integer by another, the relation being defined in the set of all positive integers as follows:

a is divisible by b if $\exists$ a positive integer c such that $a=bc$.

Hint : The relation is reflexive, transitive but not symmetric.

(iii) The relation $\leq$ in the set R of all real numbers defined as follows :

$a \leq b$ if $\exists$ a non-negative number c such that $a+c=b$.

Hint : The relation is reflexive, since $a+0=a \, \forall a \in R$.So the relation is not symmetric for $a \leq b \neq\Rightarrow b \leq a$ (prove)

The relation is transitive for $a \leq b$ and $b \leq c \Rightarrow a \leq c$ (Prove)

(iv) The relation $<$ in the set of natural Numbers N is defined as follows :

(a) $a < a$ since $a + x = a$ has no solution in N. Hence $<$ is non-reflexive

(b) $a < b$ not implies $a < b$. Hence $<$ is not-symmetric

(c) $a < b$ and $b < c \Rightarrow a < c$ Hence $<$ is transitive.

Example : R is a relation in Z defined by: if $x, y, \in Z$, then xR_1 if $10+xy>0$. Prove that R is reflexive, symmetric but not transitive.

Hint : $2R3$ nd $3R6$ but $-2R6$

Definition : Let m be a fixed integer. Two integers a and b are said to be congruent module m, written as $a = b(\text{mod}\, m)$

if any only if m divides $a-b$. That is, $a \equiv b\ (\text{mod}\, m)$ if and only if $a-b = km$ for some integer k.

The relation $a \equiv b(\text{mod}\, m)$ defined on the set of integers is called the relation of 'congruence modulo m'

3.4 Equivalence Classes

Definition : Let R be an equivalence relation on A. For any a∈A, the set of all x∈A which are related to a is called equivalence class of a. We denote equivalence class of a by the symbol [a]. Thus symbolically [a] = {x : x∈A and aRx}

Example : Let A = {1, 2, 3, 4} and let relation R on A be given by R = {(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (4, 4)}. Find the equivalence classes of relation R.

Solution : It is easy to verify that R is an equivalence relation. The equivalences class of l∈A is [1] = {x: x∈A and lRx}= {1, 2, 3}

Similarly, [2] = {1, 2, 3}, [3] = {1, 2, 3} and [4] = {4}

Example : Let R be the relation of congruence module 3' on the set I of integers. Find equivalence classes of R.

Solution: We start with the element 0∈I. The equivalence class of 0 is

[0] = {x: x∈I and 0Rx} = {x: x∈I and x ≡ 0 (mod 3)}

= {x: x∈ I and x is multiple of 3= {…., - 6, - 3, 0, 3, 6,…..}

Since [0] ≠ I, we take an element in I which is not in [0]. Let us choose l∈I. Now we compute, equivalence class of l,

[1] = {x: x∈ I and lRx} = {x: x∈I and x ≡ 1 (mod 3)}

= {x: x∈ I and x = 3k+1, when k∈I} = {…., -5 , -2, 1, 4, 7,……}

Since [0] ∪ [1]≠ I, we choose in an element in I which is not in [0] ∪ [1]. Let us choose 2∈I. The equivalence class of 2 is [2] = {.... – 4, - 1, 2, 5, 8,.....).

Since [0] ∪ [1] ∪ [2] = I, we see that these are the only distinct equivalence classes with respect to the relation 'congruence modulo 3'.

3.5 Properties of Equivalence Classes

The following theorem contains some important properties of an equivalence relation.

Theorem : Let A be a non-empty set and let R be an equivalence relation on A. For a, b∈ A.

1. a∈[a]
2. if b∈[a] then[b] = [a],
3. [a] = [b] if and only if (a, b)∈R.
4. Either [a] = [b] or [a] ∩ [b] = ϕ. That is, two equivalence classes are ether disjoint or identical.

Proof : (1) Since R is reflexive, we have aRa. Thus a∈[a].

(2) Suppose b∈[a], then bRa. Let x be any element of [a]. Then xRb, but R is transitive, therefore xRb and bRa ⇒ xRa ⇒x∈[a]. Thus [b] ⊆ [a].

Again let y be any element of [a], then yRa. Since R is symmetric, therefore bRa ⇒ aRb.Now yRa and aRb ⇒yRb ⇒y∈[b] Thus [a] ⊆ [b]. Hence [a] ⊆ [b] and [b] ⊆ [a]⇒[a]=[b]

(3) Suppose [a] = [b]. We show that aRb. Since R is reflexive, we have aRa now aRa ⇒a∈[a] ⇒a∈[b] (since [a]=[b]) ⇒aRb

Conversely, suppose that aRb. Then we show that [a] = [b]. Let x be any element of [a]. Then xRa. But it is given that aRb. Therefore,xRa and aRb ⇒ xRb [since R is transitive] ⇒x∈[b]. Therefore, [a] ⊆ [b]. Again let be any element of [b]. then y∈[b] ⇒yRb. Now we are given that aRb. ⇒bRa[since R is symmetric]

Now, yRb and bRa⇒ yRa [since R is transitive] ⇒ y∈[a]. Therefore [b] ⊆ [a].

Finally, since [a] ⊆ [b] and [b] ⊆ [a], we have [a] = [b].

(4) If [a] ∩ [b] and [b] = ϕ, hence we are nothing to prove. So let us suppose that [a] ∩ [b] ≠ϕ.Since [a] ∩ [b] ≠ϕ, suppose x∈[a]∩[b]. Now x∈[a] ∩[b]

$\Rightarrow x\in[a]$ and $x\in[b]\Rightarrow xRa$ and $xRb \Rightarrow xRx$ and $xRb \Rightarrow aRb \Rightarrow [a] = [b]$ [by part (iii)] Thus $[a]\cap[b]\neq\phi\Rightarrow[a]=[a]$.

Thus two equivalence classes [a] and [b] are either identical or disjoint.

3.6 Quotient set of a Set S :

The set of equivalence classes obtained from an equivalence relation in a set *S* is called the quotient set of *S* which is denoted by $\bar{s}$ or by $S|\sim$, or by $S|R$ when the equivalence relation is denoted by *R*.

Example : Let S be the set of all points in the x.y plane. We define a relation R in S by: For a, $b\in S$, aRb if the line through the point a parallel to the X-axis passes through the point b.It can easily be proved that R is an equivalence relation in S. Now the equivalence class $\bar{a}$ determined by the point a is the line through the point a parallel to the x-axis and the quotient set $\bar{S}$= set of all straight lines in the x-y plane parallel to the x-axis.

Example : The diagonal relation or the relation of equality in a set S is an equivalence relation proved in). If $a\in S$, then $\bar{a}=\{a\}$. i.e. each equivalence class is a singleton and $\bar{S}$=set of all singletons.

Example : If *S* is a set, then $R=S\times S$ is an equivalence relation in *S* and the only equivalence class is the set *S*. $\bar{S}=\{S\}$.

Example : If *X* be the set of points in a plane and *R* is a relation on *X* defined by $A, B\in X$, ARB if *A* and *B* are equidistant from the origin. prove that *R* is an equivalence relation. Describe the equivalence classes.

Hint : The equivalence class R_A=Set of points on the circle with centre as origin *O* and radius *OA*. Hence the quotient set $X|R$ is the set of circles on the plane with centre as *O*.

3.7 Partition

Definition : Let S be non-empty set. A collection P =$\{A_1, A_2, \ldots.)$ or non empty subsets of S is called a partition of S if

1. $A_1\cup A_2\ A_3\ldots\ldots=S$.
2. If $A_i\neq A_j$ then $A_i\cap A_j=\phi$.

Example: Let I=$\{\ldots., -5, -4, -2, -1, 0, 1, 2, 3, 4,\ldots\}$. Then the collection $\{A_1, A_2, A_3\}$, where

$A_1=\{\ldots, -6, -3, 0, 3, 6, 9, \ldots.\}$

$A_2 = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$ and $A_3 = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}$

is a partition of I because $A_1 \cup A_2 \cup A_3 = I$ and $A_i \cap AA_j = \phi$ when $A_i \neq A_j$.

It may be seen that every equivalence relation on a set determines a unique partition of the set and every partition of a set defines an equivalence relation on the set.

Example: Let A = {1, 2, 3 4} and consider the partition P={{1, 2}, {3, 4}} of A. Find the equivalence relation R on A determined by P.

Solution: The disjoint sets in P are {1, 2} and {3, 4}. Each elements in a disjoint set is related to every other element in the same disjoint set and only to those elements. Thus R ={(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)}.

Quotient Set : Let A be a non-empty set and R be an equivalence relation on A. The set of all equivalence classes is called the quotient set of A modulo R and is denoted by A/R.

Check your progress

1. Give an example of a relation on the set {a, b, c} which is
   a. Reflexive but is neither symmetric nor transitive.
   b. Reflexive, symmetric but not transitive.
   c. Symmetric and transitive but not reflexive.
2. (a) Let A = {1, 2, 3} and B = {r, s}. Then write the matrix of the relation R from A to B given by R={(1, r), (2, s), (3, r)}

   (b) Let A = {1, 2, 3, 4}. Give the relation R on A that has relation matrix

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

3. Let A = {1,2,3,4), B={1,4,6,8,9}. Let R be relation from A to B defined by aRb I and only if $b = a^2$. Find the domain and range of R.
4. Let A be the set of real numbers. Consider the following relation R on A;

   $(a, b) \in R$ if and only if $a^2+b^2=25$. Find the domain and range of R.
5. (a) Let A be a set with 10 distinct elements. How many relation are there on A? How mahy of them are reflextive?

   (b) Let $A = \{1,2,3\} \times \{a,b\}$. How many relations are there on A?

6. Let R be the following relation on A= {1, 2, 3, 4}:

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

   (a) Find the matrix M_R of R.
   (b) Find the domain and range of R.
   (c) Find the R^{-1}.
   (d) Draw the graph of R.
   (e) Find the composition relation RoR.
7. If relation R and S are reflexive, symmetric and transitive them show that R∩S is also reflextiv, symmetric and transitive.
8. Given A = {a, b, c} and a relation R on A is defined by R ={(a, a), (a, b), (, c), (c, c). Find transitive closure of R.
9. Let A = [1, 2, ...,9} and let ~ be the relation on A×A defined by (a,b)~(c,d) if a+d=bc. Prove that ~ is an equivalence relation. Also find the equivalence class of (2, 5).
10. Let R be the relatioin on N defined by the equation x+3y=12 That is, R={(x, y) : x+3y = 12}. Write R as a set of ordered pairs. Also find RoR.
11. Let A= {1, 2, 3, 4} and R = {(x, y}. Draw the graph of R and also given its matrix.
12. If {{1, 2, 3}, {4}} is a partition of the set A= {1, 2, 3, 4} then determine the corresponding equivalence relation R on A.
13. For a given partition of a set A, define a relation R on A such that R is an equivalence relation corresponding to the partition.

Answers

1. (a) R = {(a, a), (b, b), (c, c), (a, b), (b, c)

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

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

2. (a) $M_r = \begin{matrix} 1 \\ 2 \\ 3 \end{matrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$ (b) R = {(1, 1), (1, 2), (1, 4), (2, 2), (2, 3), (3, 3), (3, 4), (4, 1)}.

3. Domain of R = {1, 2, 3} and range of R = {1, 4, 9}

4. Domain of R = {x : $-5 \le x \le 5$}, Range of R = {x : $-5 \le x \le 5$}

5. (a) number of relation on A=2^{100}, number of reflexive relation on A= 2^{90}.

(b) Since A contains 6 elements, number of relation on A = 2^{36}.

6. (a) $M_R \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

(b) Domain ={1, 3}. Range ={2, 3, 4}; (c) R^{-1}= {(3, 1), (4, 1), (2, 3), (3, 3), (4, 3)};
(e) RoR = {(1, 2), (1, 3), (1, 4), (3, 2), (3, 3), (3, 4)}.

8. Transitive closure of R = {a, a), (a, b), (b, c), (c, c), (a, c)}.

9. [(2, 5)] = {(1, 4), (2, 5), (3, 6), (4, 7), (5, 8), (6, 9)}

10. R = {(9, 1), (6, 2), (3, 3)}, RoR = {(3, 3)}.

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

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

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P.T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I.N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

Unit - 4

Fuctions

Structure

4.1 INTRODUCTION

As we know fuction is one of the most fundamental concept in mathematics and is used knowingly or unknowingly to our day to day life at every moment. Computer Science is an area where a number of applications of function can be seen.We thought it would be a good idea to acquaint with some basic results about the function. Perhaps, we are already familiar with these results. But, a quick look through the pages will help us in refreshing our memory, and we will be ready to tackle the course. We will find a number of examples of various types of functions,

4.2 Objectives

After reading this unit you should be able to:

- Describe function of its different forms
- derive other properties with the help of the basic ones
- define a function and examine whether a given function in one–one/onto
- investigate whether a given function has an inverse or not
- define sum, difference, product, quotient of the given function and
- determine whether a given function is quotient map.

4.3 Functions

Definition : Let X and Y be two sets. A function f from X to Y is a rule which associates to each element x in X a unique element y of Y. The function f from X to Y is denoted by $f: X \to Y$

The terms such as mapping transformation or correspondence are also used for function.

If f is a function from X to Y, i.e., $f: X \to Y$, then the set X is called the domain of the function f and Y is called co-domain of f. The element $x \in X$ is called an argument of the function and the element $y \in Y$ which the function f associates to $x \in X$ is denoted by $f(x)$ and is called the image of x under f or the value of the function f at x. The set $\{f(x): x \in X\}$ is called the range of f. If $A \subseteq X$ then $f(A) = \{f(x): x \in A\}$.

Functions as Sets of Ordered Pairs

If X and Y be any two sets, then a function f from X to Y is a subset f of $X \times Y$ satisfying the following two conditions:

(1) For each $x \in X, (x, y) \in f$ for some $y \in Y$.

(2) If $(x, y) \in f$ and $(x, z) \in f$ then $y = z$

The first condition ensures that every x in X is associated with some y in Y and the second condition guarantees that the image of each x in X is unique.

Equal function **:** Two functions f and g are said to be equal if their domains are same and $f(x) = g(x)$ for all x in the domain.

Example 1: Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3\}$. Then $f = \{(a,1), (b,2), (a,3), (c,3)\}$

Is not a function from X to Y because the second condition is not satisfied for $a \in X$ as both $(a,1)$ and $(a,3)$ are in f.

2. Let $X = \{1, 2, 3\}$. Then $f = \{(1,2), (3,1)\}$

is not a function from X to X because $2 \in X$ is not the first coordinate of any pair in f and so f does not assign any image to 2.

3. Let $X = \{1, 2, 3, 4\}, Y = \{a, b, c, d\}$ and let $f = \{(1, a), (2, a)(3, d), (4, c)\}$.

Then f is a function from X to Y. Here, we have

$f(1) = a, \quad f(2) = a,$
$f(3) = d, \quad f(4) = c.$ and range of $f = \{a, c, d\}$

We observe that the element $a \in Y$ appears as the second coordinate of two different ordered pairs in *f*. This does not violate the definition of a function.

Note (1.3) : Mapping of set *X* to a set *Y*, when *X* and *Y* are sets of numbers are also called functions.

Example : Let Z_+ be the set of positive integers and E the set of even positive integers. Let map $f: Z_+ \to E$ be defined by $f(m)=2m\ \forall m \in Z_+$. Hence range $f = f(Z_+) = E$.

Example : Let *R* be the set of real numbers. Let function $f: R \to R$ be given by $f(x) = e^x$, $x \in R$ since $e^x > 0$ for $\forall x \in R$, therefore range $f = R_+$(set of positive real numbers).

Example : Let *X* = set of all students of Allahabad University, *Y* = Set of ages in years. Since every student has some unique age, so we can define a map

$f: X \to Y$ by $f(x)= y$. Where x is student and *y* is his age in years.

Example : $f: R \to R$ defined by $f(x) = \log x$, $x \in R$ is not a map or function, since

$f(-3) = \log(-3)$ is not a real number. But $f: R^+ \to R$ where R^+ is the set of positive real numbers defined by $f(x)=\log x$ is a map.

Example : $f: R^+ = R$ defined by $f(x) = \sqrt{x}$ is not a map, since $f(4) = \sqrt{4} = \pm 2$. Thus 4 has two *f*-images. But $f(x) = +\sqrt{x}$ (positive value of the square root of x) will be a map or function from R^+ to R.

Types of Function

Definition: A function $f: X \to Y$ is called *onto* (or surjective) if range of $f = Y$. That is, each element of *y* is the image of some element of *X*.

If $f: X \to Y$ is not onto then it is called *into*.

Definition: A function $f: X \to Y$ is called *one-to-one* (or injective or 1-1) if distinct elements of X have distinct images under *f*. In other words, *f* is one-to-one if $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ Or equivalently, $f(x_1) = f(x_2) \Rightarrow x_1 \neq x_2$

A mapping $f: X \to Y$ is said to be *many-one* if at least two distinct elements in X have the same image in *Y* under *f*, i.e., $x_1 \neq x_2$ but $f(x_1) = f(x_2)$

Definition : A mapping $f: X \to Y$ is said to be *bijective* if f is one-to-one and onto. A bijective mapping is also called one-to-one correspondence.

Example : Let $f: R \to R$ be defined by $f(x_1) = x^2$. Then f is neither one-to-one nor onto. f is not one-to-one because both 2 and −2 are mapped on 4. f is not onto because range of $f = \{x^2 : x \in R\} = R^+ \cup \{0\} \neq R$, where R^+ denotes the set of all positive real numbers.

Example : Let $f: \{1,3,5,7,9\} \to \{2,4,6,8,10\}$ be given by $f(x) = x+1$. Then f is one-to-one and onto. Thus f is bijective.

Example : The map $f: Z_+ \to E$ given in example (6.1) is injective, because for m, $n \in Z_+$, $f(m)=f(n) \Rightarrow 2m = 2n \Rightarrow m = n$. f is surjective also, since for $\forall y \in E \exists y/2 \in Z_+$ such that $f(y/2)=y$. Thus f is a bijection or one-one correspondence from Z_+ to E.

Example : The map $f: R \to R$ given by $f(x)=e^x$, $x \in R$ is injective but not surjective for if x, $y \in R$ then $f(x) = f(y) \Rightarrow e^x = x^y \Rightarrow x = y$ therefore f is *injective.*

Again $e^x > 0$ $\forall x \in R$, hence 0 or any negative real number is not the f-image of any real number of the domain set, and so f is not *surjective.*

Example : Let C be the set of complex numbers and R the set of real numbers. The map f: C → R given by $f(x + iy) = \sqrt{(x^2 + y^2)}$ is neither injective nor surjective for $f(x+iy) = f(x - iy) = \sqrt{(x^2+y^2)}$.

Example : The function f: R → R given by $f(x) = \sin x$ is neither injective nor surjective for $f(x) = f(\pi - x) = \sin x$ and there does not exist $x \in R$ such that $f(x) = \sin x = 2$.

Example : If A and B are two finite sets having the same number of elements, then prove that $f: A \to B$ is injective (one-one) iff it is surjective (onto). Let A and B both have n elements, If $f: A \to B$ is injective then the n elements of A will have n distinct images in B which will be the n elements of B and hence every element of B is the image of some element of A and so f is surjective.

Again if f is surjective, then ach of the n element of B will be the image of at least one element of A, but any element of B cannot be the image of more than one element of A, for in that case A must have more than n elements. Hence each element of B is the image of exactly one element of A. So f is injective.

Example : Show that there exists a bijection between the set N of natural numbers and the set Z of integers. Define $f: N \to Z$ as follows:

$f(m) = m/2$ when m is an even natural number,

$f(m) = -(m-1)/2$ when m is an odd natural number.

This map is one-one correspondence (bijective).

Identity function : A function 1: $X \rightarrow X$ is called an identity function if $I(x) = x \forall x \in X$.

Under identity function, each element is mapped on itself.

Remainder function : Let m be any positive integer and k be any integer. We define a function f_m from the set of integers Z to $\{0,1,2,\ldots,m-1\}$ as follows:

$$f_m(k) = k(\text{mod } m)$$

where $k(\text{mod } m)$ denotes the remainder r, $0 \leq r < m$ when k is divided by m. This functions is known as remainder function (or the **mod *m*-function**)

Given any integer k and a fixed positive integer m, the value of $k(\text{mod } m)$ is obtained as follows: If k is positive then divide k by m to obtain the remainder r. For example,

1. 25(mod 7) = 4 because when we divide 25 by 7 then we get the remainder as 4.

2. 25(mod 5) = 0 because when we divide 25 by 5, then the remainder is 0.

3. 3(mod 8) = 3 because when we divide 3 by 8 the remainder is 3.

If k is negative then divide $|k|$ by m to obtain remainder r', then $k(\text{mod } m) = m - r'$

For example, –26(Mod 7) = 7–5 = 2 and –371 (mod 8) = 8–2 = 5.

Example : The remainder function is onto but not one-to-one.

Solution : Let m be any position integer. Define $f_m : Z \rightarrow \{0,1,\ldots,m-1\}$ as follows:

$$f_m(k) = r = k(\text{mod } m).$$

Suppose $k \in Z$ is mapped on r. Then we see that $k+m, k+2m, \ldots$ are also mapped on r. Thus f_m is not one-to-one but f_m is onto. Let $r \in \{0,1,2,\ldots,m-1\}$. Then $r \in Z$ and $f_m(r) = r$. Thus f_m is onto.

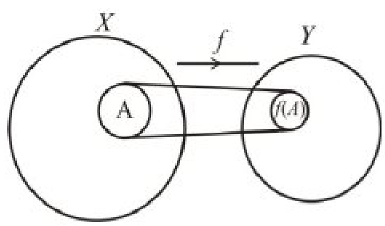
Inclusion and Identity Maps : Let $X \subseteq Y$ and let $f: X \rightarrow Y$ be given by $f(x) = x$. $\forall x \in X$. Then f is called inclusion map of X into Y. An inclusion map is generally denoted by I_x in place of f. the inclusion map of X into X is called the identity map on X and is denoted by I_x, Thus $I_x: X \to X$ is given by $I_x(x) = x \ \forall x \in X$.

Equality of Mapping : Let f and g be two maps from X to Y, that is both f and g map the set X to the set Y. We define $f = g$ if $f(x) = g(x) \ \forall x \in X$.

If $f; R \to$ is defined as $f(x) = \dfrac{x^2 - 4}{x - 2}$ when $x \neq 2$ and $f(2) = 4$ and g; $R \to R$ is defined as $g(x) = x + 2 \ \forall x \in R$. then $f = g$.

Direct and Inverse image : Let f: $X \to Y$ be a map and let $A \subseteq X, B \subseteq Y$, then the direct image of A under f denoted $f(A)$ is given by

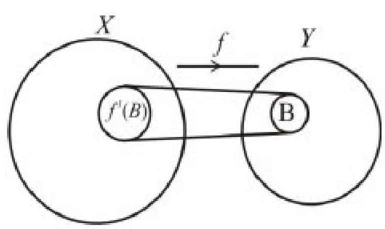
$f(A) = \{y \in Y : \exists x \in A$ with $f(x) = y\}$,



that is $f(A)$ is the set of images of all the elements of A. the above diagram illustrates it. Thus $x \in A \Rightarrow f(x) \in f(A)$ the reserve implication viz $f(x) \in f(A) \Rightarrow x \in A$ is only true when f is injective. If $x \in X$, then $f(\{x\}) = \{f(x)\}$ and $f(X)$ = range f and $f(\phi) = \phi$. The inverse image of B under f denoted $f^{1}(B)$ is given by

$f^{1}(B) = \{x \in X : f(x) \in B\}$ thus $x \in f^{1}(B) \ \exists f(x) \in B$.

The reserve implication viz $f(x) \in B \Rightarrow x \in f^{1}(B)$ is also true.



In case there is no element $x \in X$ such that $f(x) \in B$ (which may happen when f is not surjective), then $f^{1}(B) = \phi$.

Example : Let f: R→R be given by $f(x) = x^2, x \in$ R.

Let $A = \{x \in R: 1 \leq x \leq 2\} = [1, 2] \subset R$.

Then $f(A) = \{y \in R: 1 \leq y \leq 4\} = [1, 4]$. [since $1 \leq x \leq 2 \Rightarrow 1 \leq x^2 \leq 4$]

Let $B = \{y \in R: 4 \leq y \leq 9\} = [4, 9]$. Then $f^{1}(B) = [-3, -2] \cup [2, 3]$.

If $C = [-4, -1]$, then $f^{1}(C) = \phi$, since $x \in R$ such that $f(x) = x^2 \in [-4, -1]$, does not exist.

Example : Let $A = \{n\pi: n$ is an integer$\}$ and R be the set of real numbers.

Let $f: A \to R$ be defined by $f(\alpha) = \cos \alpha \, \forall \alpha \in A$ Find $f(A)$ and $f^{1}\{0\}$.

Now $f(n\pi) = \cos n\pi = +1$ or -1, Hence $f(A) = \{-1, 1\}$. If $f(\alpha) = 0$ or

$\cos \alpha = 0$ or $\alpha = (2n+1)\frac{\pi}{2}$ Hence $f^{1}\{0\} = (2n+1)\frac{\pi}{2}$.

Now $(2n+1)\frac{\pi}{2} \notin \{n\pi\}$, So, $f^{1}(0) = \phi$.

Example : Let $f: X \to Y$ be a map and let A and B be subsets of X, then

(i) $A \subseteq B \Rightarrow f(A) \subseteq f(B)$

(ii) $f(A \cup B) = f(A) \cup f(B)$

(iii) $f(A \cap B) \subseteq f(A) \cap f(B)$. Equality holds when f is injective.

Proof (i) If $A \subseteq B$, then $x \in A \Rightarrow x \in B$. Now $y \in f(A) \Rightarrow \exists x \in A$ s.t. $f(x) = y$. $\Rightarrow x \in B$ s.t. $y = f(x)$. $\Rightarrow y = f(x) \in f(B)$ since $x \in B \Rightarrow f(x) \in f(B))$

Therefore , $y \in f(A) \Rightarrow y \in f(B)$ hence $f(A) \subseteq f(B)$.

(ii) $\in f(A \cup B) \Rightarrow \exists x \in A \cup B$ s.t. $y = f(x) \Rightarrow \exists x \in A$ or $x \in B$ s.t. $y = f(x) \Rightarrow y = f(x) \in f(A)$ or $y = f(x) \in f(B)$. (since $x \in A \Rightarrow f(x) \in f(A)$ and $x \in B \Rightarrow f(x) \in |(B)$).

Hence $y \in f(A \cup B) \Rightarrow y \in f(A) \cup f(B)$. Therefore $f(A \cup B) \subseteq f(A) \cup f(B)$.

Again $A \subseteq A \cup B$, $B \subseteq A \cup B$ therefore by (i) $f(A) \subseteq f(A \cup B)$, $f(B) \subseteq f(A \cup B)$ therefore $f(A) \cup f(B) \subseteq f(A \cup B)$.

From the above we get $f(A \cup B) = f(A) \cup f(B)$.

(iii) $A \cap B \subseteq A$, $A \cap B \subseteq B$, therefore by (i) $f(A \cap B) \subseteq f(A)$, $f(A \cap B) \subseteq f(B)$.

Hence $f(A \cap B) \subseteq f(A) \cap f(B)$.

Note: $f(A) \cap f(B) \subseteq f(A \cap B)$ is not true. Since $y \in f(A) \cap f(B) \Rightarrow y \in f(A)$ and $y \in f(B) \Rightarrow \exists x_1 \in A \mid f(x_1) = y$ and $\exists x_2 \in B \mid f(x_2) = y \not\Rightarrow \exists x \in A \cap B \mid f(x) = y$. Since $x_1 \in A$ but x_1 may not be an element of B, similarly $x_2 \in B$ but x_2 may not be an element of A, so there may not exist a common element x of A and B such that $f(x) = y$.

But if f is injective, then $f(A)\cap f(B) \subseteq f(A\cap B)$ will be true and hence in that case $f(A\cap B)=f(A)\cap f(B)$.

Example: When $f(A)\cap f(B)\not\subseteq f(A\cap B)$. Consider map $f: R\to R$ given by $f(x)= x^2$, It is clear f is not injective.

Let A= {-1, - 2, -3, 4} and B= {1, 2, -3} be subsets of Dom f. Then $A\cap B$ = {-3}.

So, $f(A\cap B)=\{-3^2\}$. Now $f(A)=\{1^2,2^2,-3^2,4^2\}$, $f(B)=\{1^2,2^2,-3^2\}$

So, $f(A)\cap f(B)=\{1^2,2^2,-3^2\} \not\subseteq \{-3^2\}$. So $f(A)\cap f(B) \not\subseteq f(A\cap B)$

Example: Let $f: X\to Y$ be a map and let A and B be subsets of Y.

Then (i) $A\subseteq B\Rightarrow f^{1}(A)\Rightarrow f^{1}(B)$

(ii) $f^{1}(A \cup B) = f^{1}(A) \cup f^{1}(B)$ (iii) $f^{1}(A\cap B) = f^{1}(A) \cap f^{1}(B)$.

Proof. (i) $x\in f^{1}(A)\Rightarrow(x)\in A\Rightarrow f(x) \in B$ (since $A\subseteq B$) $\Rightarrow x\in f^{1}(B)$,

Therefore $f^{1}(A) \subseteq f^{1}(B)$.

(ii) $x\in f^{1}(A \cup B)\Leftrightarrow f(x)\in A \cup B\Leftrightarrow f(x) \in A$ or $f(x) \in B\Leftrightarrow x\in f^{1}(A)$ or $x\in f^{1}(B)$

$\Leftrightarrow x\in f^{1}(A) \cup f^{1}(B)$. Therefore $f^{1}(A \cup B) = f^{1}(A)\cup f^{1}(B)$.

(iii) $x\in f^{1}(A\cap B) \Leftrightarrow f(x) \in A\cap B\Leftrightarrow f(x) \in A$ and $f(x) \in B\Leftrightarrow x\in f^{1}(A)$ and $x\in f^{1}(B) \Leftrightarrow x\in f^{1}(A) \cap f^{1}(B)$. Therefore $f^{1}(A\cap B) = f^{1}(A) \cap f^{1}(B)$.

Thus (ii) and (iii) show that union and intersection are pre served under inverse image.

Check your progress

(1.1) Prove that $f: X\to Y$ is injective iff $f^{1}(\{y\}) = \{x\}$ $\forall y\in f(X), x\in X$

(1.2) Prove that $f: X\to Y$ is sujrective iff $f^{1}(B) \neq \phi$ where $B\subseteq Y$ and $B \neq \phi$.

(1.3) Prove that $f: X\to Y$ is bijective iff $\forall y\in Y, f^{1}(\{y\}) = \{x\}, x\in X$.

(1.4) give examples when (i) $f(f^{1}(B))$ is a proper subset of B

(ii) A is a proper subset of $f^{1}(f(A))$

(1.5) If $f: X\to Y$ and $A\subseteq X$, $B\subseteq Y$, prove that

(a). If $(f^{1}(B)) \subseteq B$.

(b). f^{1}(f(A)) $\supseteq A$.

(c). $f^{1}(Y) = X$.

(d) let $f: X \to Y$ and let $A \subseteq Y$, then prove $f^{1}(Y - A) = X - f^{1}(A)$.

Inverse map : Let $f: X \to Y$ be a map. Let us define a map

$\phi : Y \in X$ given by if $y \in Y$, then $\phi(y) = x$ where $f(x) = y$.

if ϕ is to be map, then every $y \in Y$ must be f image of some $x \in X$, that is f must be surjective. Further two different elements x_1 and x_2 of X must not have the same f-image $y \in Y$, for in that case $\phi(y) = x_1$ also x_2, so ϕ cannot be a map. Hence f must be injective. Thus when f is bijective we can define the above map ϕ which is called inverse of f and will be denoted by f^{1}. Thus the inverse of f is defined as: $f^{1} : Y \to X$ given by $\forall y \in Y, f^{1}(y) = x \in X$ such that $f(x) = y$.

Remarks (1.1) : Inverse map of f should not be confused with the inverse image of a subset under f, denoted by the same symbol viz f^{1}.

(1.2) Inverse of the map $f: X \to Y$ only exists when f is bijective and the inverse map f^{1}: $X \to Y$ only exdists when f is bijective and the inverse map f^{1}: $Y \to X$ is such that $f^{1}((y) = \Leftrightarrow f(x) = y$.

Example : Let $X = [-\pi/2, \pi/2]$, $Y = [-1, 1]$. Let $f: X \to Y$ be given by $f(x) = \sin x$, $x \in X$. It can be easily proved that f is a bijection. So f^{1}: $Y \to X$ given by $f^{1}(y) = \sin^{-1} y = x \in X$. such that $\sin x = y$. Thus $\sin^{-1} y = x. \Leftrightarrow \sin x = y$.

Example: If $f: X \to Y$ is a bijection, then the inverse map f^{1}: $Y \to X$ is also a bijection. For let $f^{1}(y_1) = x_1$, $\in Y$ and $x_1 \in Y$ and $x_1 \in X$. Then $f(x_1) = y_1 f^{1}(y_a) = x_2$, $y_2 \in Y$ and $x_2 \in X$. Then $f(x_2) = y_2$. Now $f^{1}(y_1) = f^{1}(y_2) \Rightarrow x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$[since f is map] $\Rightarrow y_1 = y_2$. Therefore f^{1} is surjective. Again since f is bijective, every element $y \in Y$ is the f-image of a unique element $x \in X$. Hence every $x \in X$ is the f^{1} image of an element $y \in Y$. Therefore f^{1} is surjective.

Composite of Maps: Let $f: X \to Y$ and $g: Y \to Z$ be two maps. Their composite denoted by gof is the map $gof: X \to Z$ given by such that for some $y \in Y f(x) = y$ and $g(y) = z$. Thus we get $(gof)(x) = z = g(y) = g(f(x))$.

Note (1.1): For the composite gof of maps f and g, range $f \subseteq dom\ g$.

Note (1.2): In general $gof \neq fog$.

Note (1.3): The maps being particular types of relations composite of maps has been defined exactly in the same way as composite of relations.

Example: let f: $\mathbf{R}\to\mathbf{R}$ be given by $f(x) = e^x$, $x\in\mathbf{R}$ and

g: $\mathbf{R}\to\mathbf{R}$ be given $g(y) = \sin y, y\in\mathbf{R}$. Then go: $\mathbf{R}\to\mathbf{R}$ given by

$(gof)(x) = g(f(x)) = g(e^x) = sin(e^x)$.

Here Range $f = f(\mathbf{R}) = \mathbf{R}^+$ (the set of positive real numbers) $\subseteq R$.

Thus range $f \subset domg$. Here fog is also defined, viz

$fog: R\to R$ given by $(fog)(y) = f(g(y)) = f(\sin y) = e^{\sin y}$, $y\forall\in\mathbf{R}$.

Hence $(fog)(x) = e^{\sin x}$. So, fog maps x to $\sin(e^x)$, and fog maps x to $e^{\sin x}$.

Thus $gof \neq fog$.

Example: Let f: $\mathbf{R}\to\mathbf{R}$ be given by $f(x) = x^3 + 3$ and g: $R\to R$ be given by

$g(x) = x^2 - 7$. Then gof: $\mathbf{R}\to\mathbf{R}$ given by $(gof(x) = g(f(x)) = g(x^3+3)$

$= (x^2+3)^3 - 7$. Now fog: $R\to R$ given by $(fog)(x) = f(g(x))$

$= (x^3 - 7) = (x^3 - 7)^2+3$. Thus $gof \neq fog$.

Remarks : If gof is defied, then fog need not be defined.

Example : Let $X = \{1,2,3\}$ and f and g be functions from X to X given by:

$f = \{(1,2),(2,3),(3,1)\}$ and $g = \{(1,1),(2,2),(3,1)\}$

Find fog and gof and also show that $fog \neq gof$.

Solution: $f: X\to X$ and $g: X\to X$

$\therefore$ $gof: X\to X$ defined by $(gof)(x) = g(f(x))$

$\therefore$ $(gof)(1) = g(f(1)) = g(2) = 2$, $(gof)(2) = g(f(2)) = g(3) = 1$

$(gof)(3) = g(f(3)) = g(1) = 1 \therefore$ $gof = \{(1,2),(2,1),(3,1)\}$

Similarly, $fog = \{(1,2),(2,3),(3,2)\}$. We see that $gof \neq fog$

Example: Let f: $X\to Y$, g: $Y\to Z$, h: $Z\to W$ be three maps. Then ho $(gof) = (hog)$ of, that is composition of maps is associative just like the composition of relations, as shown below. Both $ho(gof)$ and (hog) of maps from $X\to W$.

Now $(ho\,(gof)\,(x) = h\,((gof)x) = h(g\,(f\,(x))$ and $((hog)\,of)\,x = (hog)\,(f\,(x)) = h(g\,(f\,(x)))$. Hence $ho\,(gof) = (hog)\,of$.

Example: Let $f: X \to Y$ be a bijection, prove that $f^{1} \circ f = I_x$ and $fof^{1} = I_x$.

Solution: Let $f(x) = y, x \in X$. Then $x = f^{1}(y)$. Now $f^{1} \circ f : X \to X$, given by

$(f^{1}\, of)\,(x) = f^{1}(f(x)) = f^{1}(y) = x = I_x(x)$. Therefore $(f^{-1}of)\,(x) = I_x(x)\ \forall x \in X$.

Hence $f^{-1}\, of = I_x$. The other part can similarly be proved.

Example: Let f: $X \to Y$ and g: $Y \to Z$ be both bijections. Prove that gof is bijection and $(gof)^{-1} = f^{-1}og^{-1}$ (Reversal rule)

Solution: If $x_1, x_2 \in X$, then $(go\,f)\,(x_1) = (go\,f)\,(x_2) \Rightarrow g(f(x_1) = g\,(f\,(x_2))$

$\Rightarrow f\,(x_1) = f(x_2)$ (since g is injective) $\Rightarrow x_1 = x_2$ (since f is injective). Hence gof is injective. Now we prove gof is surjective.

Now gof : X→ Z. and $(gof)\,(X) = g\,(f\,(X)) = g(Y)$ (since $f\,(X) = Y, f$ being surjective) $= Z$ (since $g\,(Y) = Z$, (g being surjective)

Therefore, gof is sujrective. Hence gof is bijective.

Now both $(gof)^{-1}$ and $f^{1}\, og^{-1}$ map from $Z \to X$. Let $(gof)^{-1}(z) = x$ where $z \in Z$, $x \in$ z. Then $(gof)\,(x) = z$. Let $f(x) = y$ and $g(y) = z$. Now $(f^{-1}og^{-1})\,(z) = f^{1}(g^{-1}(z))$

$= f^{1}(y)$[since $g(y) = z \Rightarrow g^{-1}\,(z) = y$] $= x$. [since $f\,(x) = y \Rightarrow f^{1}(y) = x$].

Hence $(gof)^{-1}\,(f^{1}og^{-1})\,(z)\ \forall z \in Z$. Consequently, $(gof)^{-1} = f^{1}\, og^{-1}$.

Check your progress

(1) Let $f: X \to Y$ and $g: Y \to X$ be both bijectioin such that $gof = Ix$ and $fog = Ix$. Prove that $g = f^{1}$ and $f = g^{1}$. Also prove that

(i) gof injective $\Rightarrow f$ is injective and (ii) gof sujrective $\Rightarrow g$ is sujrective.

(2) Let Z be the set of integers. Define $f: Z \to Z \times Z$ by $f\,(m) = (m - 1, 1), m \in Z$. $g: Z \times Z \to Z$ by $g\,(m, n) = m + n, m, n \in Z$. Prove that $gof = I_z$. Discuss the mapping fog.

4.5 Connection between Equivalence relation and mapping.

Natural map or quotient map : Let S be a set and $\bar{S}$ the quotient set of S relative to an equivalence relation.~. We define a map $v: S \to \bar{S}$ given by $v(a) = \bar{a}$, where $a \in S$ and $\bar{a}$ is the equivalence class determined by a. The map v is called the natural map or the quotient map or the canonical map of S to $\bar{S}$. The map v is surjective but in general not injective as proved below –

Let $\bar{a}\in\bar{S}$, then a$\bar{a}$ since $a \sim a$. Thus, $\forall\bar{a}\in\bar{S}$, $\exists$ a$\in$S such that $v(a) = \bar{a}$. Hence map v is surjective. If $a_1 \neq a_2 \in \in S$ s.t. $a_1 \sim a$, then $v(a_1) = v(a_2) = \bar{a}$. Hence map v is not injective.

Equivalence relation induced by map : Let f: $S\rightarrow T$ be a map for A, $b\in S$, we define a relation ~ in $S a \sim b$ if $f(a) = f(b)$. It can be easily proved that ~ is an equivalenc relation in S. Then ~ is called an equivalence relation in S induced by the map F. The equivalence class $\bar{a} = \{x\in S: f(x) = f(a)\}$.

Theorem (2.1): Let f: $S\rightarrow T$ be a map and R the equivalence relation in S induced by f. Define a correspondence $\bar{f}$: $S|R\rightarrow T$ by $\bar{f}(R_x) = f(x)$ where Rx denoted the equivalence class of $x\in S$. Prove that. (i). $\bar{f}$ is a map. (ii). $\bar{f}$ is injective (iii). $\bar{f}$ is surjective if f is surjective. (iv) $f = \bar{f} o v$ where $v : S\rightarrow S|R$ is the natural map. (v) $\bar{f}$ is unique.

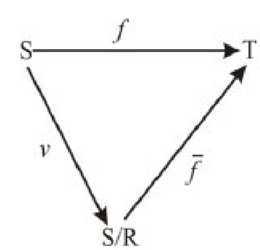
Proof. *(i)* $R_x = R_y \Rightarrow xRy \Rightarrow f(x) = f(y) \Rightarrow \bar{f}(Rx) = \bar{f}(Ry)$. Hence $\bar{f}$ is a map.

(ii). $\bar{f}(R_x) = \bar{f}(Ry) \Rightarrow f(x) = f(y) \Rightarrow xRy \Rightarrow Rx = Ry$. Hence $\bar{f}$ is injective.

(iii). Let $y\in T$, then $\exists x\in S \mid f(x) = y$ (since f is sujrective)

Now $f(x) = \bar{f}(R_x) = y$. Thus $\forall y\in T$, $\exists R_x \in S|R$ s.t. $\bar{f}(R_x) = y$. Hence $\bar{f}$ is surjective.

(iv). v: $S\rightarrow S|R$ and $\bar{f}$: S|R $\rightarrow$ T. Therefore, $\bar{f} o v$: $S\rightarrow T$, given by if x$\in$S, then ($\bar{f}$ ov) (x) $\bar{f}$ v (x))= $\bar{f}$ (R_x)=f(x). Consequently, $\bar{f}$ ov=f. This can be represented by diagram as follows:



Since $fov = f$, the image of each element of S along the two ways viz. $S\rightarrow T$ or $S \rightarrow S \mid R\rightarrow T$ is the same. Such a diagram is said to be commutative.

(v). Now we prove that $\bar{f}$ is unique. Let $\bar{f}_1$: $S|R\rightarrow T$ be another map such that $\bar{f}_1\ ov = f$. Let, $R_x \in S|R$ be the equivalence class determined by $x\in S$. Then $f(x) = f(\bar{f}_1\ ov)\ (x) = \bar{f}_1(v(x)) = \bar{f}_1(R_x)$. Now $f(x) = \bar{f}(R_x)$. Hence, $\bar{f}_1(R_x) = \bar{f}(R_x \in S|R$. Consequently, $\bar{f}_1 = \bar{f}$.

Corollary : Let $f: S \to T$ be a map and let R be the equivalence relation in S induced by F. Let R' be any other equivalence relation in S with quotient set $S|R'$ and $v': S|R'$ be the natural map. Then there exists a unique map. $\bar{f}: S|R' \to T$ such that $f = \bar{f} o v'$ iff $R \subseteq R$.

Proof. Let $R' \subseteq R$. Define $\bar{f}: S|R' \to T$ by $\bar{f}\left(\frac{x}{R'}\right) = f(x)$. Now $\bar{f}$ is a map. For

$\frac{x}{R'} = \frac{y}{R'} \Rightarrow xR'y \Rightarrow x\,Ry$ {since $R \subseteq R \Rightarrow [(x, y) \in R \Leftrightarrow (x, y) \in R] \Rightarrow xRy$, $\Rightarrow f(x) = f(y) \Rightarrow$ f $\left(\frac{x}{R'}\right) = \bar{f}\left(\frac{y}{R'}\right)$ Now $\bar{f}$ov: S $\to$ T given by $(\bar{f} o v')(x) = \bar{f}(v'(x)) = \bar{f}\left(\frac{x}{R'}\right) = f(x), \forall x \in s$.
Therefore, $\bar{f} o v' = f$.

Uniqueness of $\bar{f}$ can also be proved as in the above theorem.

Conversely, let $\bar{f}: S|R' \to T$ be the unique map such that $\bar{f} o v' = f$. Then $xR'y \Rightarrow \frac{x}{R'} = \frac{y}{R'}$ $\Rightarrow \bar{f}\left(\frac{x}{R'}\right) = \bar{f}\left(\frac{y}{R'}\right) \Rightarrow \bar{f}(v'(x) = \bar{f}(v'(y))$, [Since $\bar{f} o v' = f$] Hence, $(x, y) \in R' \Rightarrow (x, y) \in R$.
Therefore, $R' \subseteq R$.

Example: Let S be the set of points in the x-y plane and T, the set f points on the x-axis. Consider the map $\pi_x: S \to T$ given by $\pi_x(a) = a'$

where $a \in S$ and a' is the projection of a on the x axis. The equivalence relation ~ in S induced by the map π_x is given by $a \sim b$ if $\pi_x(a) = \pi_x(b)$, that is, if projections of a and b on the x-axis are the same. Hence the equivalence class $\bar{a}$ = straight line through a perpendicular to x-axis. The natural map $v: S \to \bar{S}$ is given by $v(a) = \bar{a}$ that is, the straight line through a perpendicular. to x-axis. Let $\overline{x_x}: \bar{S} \to T$ be given by $\overline{x_x}(\bar{a}) = \pi_x(a) = a'$ that is $\overline{x_x}$ send a line perpendicular to x-axis to its intersection point with x-axis. Clearly π_x is injective and $\pi_x = \overline{x_x}$ ov.

Invertible functions: Let $f: X \to Y$ be a one-to-one and onto mapping. Let y be any element of Y. Since the mapping f is onto, therefore there exists an element $x \in X$ such that $Y = f(x)$.

Since the mapping f is also one-to-one, there will be only one element $x \in X$ such that $Y = f(x)$. Let us denote x by $f^{-1}(y)$. Thus we see that if $f: X \to Y$ is one-to-one and onto then we can define a new mapping called the inverse of f and denoted by f^{-1} from Y to X which associates to each element y of Y a unique element in X. It can be seen that only one-to-one and onto (i.e. bijective) mappings possess inverse mappings. In other words, if $f: X \to Y$ is not bijective then f^{-1} does not exist.

Inverse map: Let $f:X\rightarrow Y$ be a bijective mapping. Then the mapping $f^{-1}:Y\rightarrow X$ defined by $f^{-1}(y)=x$, where $f(x)=y$ is called the inverse mapping of *f*.

It can be seen easily that if *f* is bijective then $f^{-1}$is also bijective Moreover f^{-1}o*f* and *f*o f^{-1} both are identity mappings on *X* and and *Y* repectively.

Example: Let *Q* be the set of rational number. Let $f:Q\rightarrow Q$ be defined by $f:(x)=2x+3$. Show that *f* is bijective. Also find a formula that defines the inverse function f^{-1}.

Soultion: Let x_1 and x_2 be two distinct elements in *Q*, then $x_1\neq x_2\Rightarrow 2x_1+3\neq 2x_2+3$

$\Rightarrow f(x_1)\neq f(x_2)$. Hence *f* is one-to-one

Let y be any element in *Q*. If $y=f(x)$ then $y=2x+3$ and therefore

$$f\left(\frac{y-3}{2}\right)=2\left(\frac{y-3}{2}\right)+3=y$$

Hence *f* is onto. Solving $y=f(x)$, we get $=x=\frac{y-3}{2}$ Thus $f^{-1}(y)=x=\frac{y-3}{2}$ defines the inverse function $f^{-1}Q\rightarrow Q$

4.6 Binary Operations or Binary Compositions

We are familiar with operations like addition, subtraction and multiplication. Wherever we add two natural numbers we get a unique natural number. In other words, addition is mapping for $N\times N\rightarrow N$, where N is the set of natural numbers.

Definition: Let *X* be a set. Then a mapping $f:X\times X\rightarrow X$ is called a binary operation (or binary composition) on *X*.

Thus binary operations on *X* is a mapping from $X\times X$ to X. In other words, binary operation on *X* is a mapping which associates to each pair *a,b*, of elements of *X*, a unique element *c* of *X*. We use symbols like *,+,o,⊕,∧,∨ etc. for binary operations.

Illustration

1. Addition is a binary operation on the set of integers because addition of two integers is again a unique integer.
2. Multiplication is a binary operation on the set *N* of natural number.
3. Subtraction is a binary operation on the set *Z* of integers because subtraction of two integers is again a unique integer but subtraction is not a binary operation on the set *N* of natural numbers because subtraction of two natural numbers is not necessarily a **natural numbers.** For example $3-4\notin N$.

4. A set X is said to be closed under operation * if * is a binary operation on the set X. That is, $a*b$ is a unique element of X for all a, b in X. This property is often called the closure property.

Properties of Binary Operations

Now we shall discuss some general properties of binary operations.

Commutative operation: A binary operation * on a set X is said to be commutative $x*y = y*x \quad \forall x, y \in X$.

Example : Addition and multiplication are commutative binary operations on the set R of real numbers. But subtraction is not a commutative binary operation on R because $a-b \neq b-a$ in general.

Associative operation: A binary operation * on a set X is said to be associative if

$$x*(y*z) = (x*y)*z \quad \forall x, y, z \in X.$$

Example : Since $x+(y+z) = (x+y)+z \quad \forall x, y, z \in \boldsymbol{R}$. Therefore addition is associative binary operation on $\boldsymbol{R}$. Similarly multiplication is also associative binary operation on $\boldsymbol{R}$.

Distributive operations : Let * and o be two binary operations on a set X. We say * is left distributive over o if $a*(b \circ c) = (a*b) \circ (a*c) \quad \forall a, b, c \in X$ ....(1)

We say * is right distributive over o if $(b \circ c)*a = (b*a) \circ (c*a) \quad \forall a, b, c \in X$ ....(2)

When both (1) and (2) hold, we say that * is distributive over o.

Example: On the set R of real numbers, multiplication is distributive over +, since $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$

But + is not distributive over $(\cdot)$ because $a + b \cdot c \neq (a+b) \cdot (a+c)$ for every $a, b, c \in R$

Identity Element for a Binary Operation

Given a binary operation * on a set X, we now define identity element of X for the operation *. Identity element may or may not exist.

Definition: Let * be a binary operation on X. If there exists an element $e \in X$ such that $a*e = e*a = a \quad \forall a \in X$. Then e is called identity element for *.

Example: Addition is a binary operation on $\boldsymbol{R}$, the set of real number. Since

$a+0 \quad 0+a=a \quad \forall a \in R$, therefore, the element 0 is the identity for +.

Example: We know that addition is a binary operation on N, the set of natural numbers. But N has no identity element for + because there exists no natural number e such that $a+e \;=\; e+a=a \quad \forall a \in N$

Invertible elements: Let * be a binary operation on the set X with the identity element e. An element $a \in X$ is said to be invertible if there exists an element $b \in X$ such that: $a*b \;=\; b*a=e$

Moreover, b is then said to be inverse of a and is denoted by a^{-1}. The identity element is always invertible because $e*e=e*e=e$.

Example: We know the operation of addition is a binary operation on R and 0 is the identity for +. Since for each $a \in R$, $-a$ also belongs to R such that $a+(-a)=(-a)+a=0$. Therefore, every real number has inverse for the operation of addition.

Example: Consider the operation of multiplication on R. 1 is the identity for multiplication and for every non-zero real number $a \in R$, 1/a is also a real number such that: $a\frac{1}{a}=\frac{1}{a}a=1$

Hence every non-zero real number is invertible. But 0 is not invertible with respect to multiplication. Similarly the operation of multiplication on N has identity element, namely 1 but no element except 1 is invertible.

Composition Table

A binary composition on a finite set can be defined by means of a table called *composition table* which may be described as follows:

Let $A \;=\; \{a_1, a_2, a_3, ...a_n\}$ be a finite set. We write the elements of the set A in a horizontal row as well as in a vertical column. The element $a_i * a_j$ is entered at the intersection of the i^{th} row and j^{th} column

Example: Let $A \;=\; \{1,5,7,11\}$. We define the operation of multiplication module 12 denoted x_{12} on A as follows: $a x_{12} b \;=\; r \qquad 0 \le r < 12$

where r is the least non-negative remainder when the product $a \cdot b$ is divided by 12.

The composition table for $\times_{12}$ on A is given below:

$\times_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

In the body of the table, the second entry of the third row is 11 which is obtained as follows: $7 \times_{12} 5 = 11$ since $7 \times 5 = 35 = 2(12) + 11$

Similarly other entries of the table are obtained.

Example : Let * : I×I→I, where I is the set of integers, be defined as $x * y = x + y - xy$

Show that the binary operation * is commutative and associative. Find the identity element and indicate the inverse of each element.

Solution : Let x and y be two integers. Then $x+y$ and xy are also integers. Now since subtraction of two integers is also are integer, we have $x+y-xy$ is an integer. Thus $x * y \in$ I. Hence * is binary operation on I.

*** is commutative :**

Since $x * y = x + y - yx$

$= x + y - yx$ the operation * is commutative

$= y * x,$

*** is associative :** For any x, y and z in I, we have

$$\begin{aligned} x*(y*z) &= x*(y+z-yz) \\ &= x+(y+z-yz)-x(y+z-yz) \\ &= x+y+z-yz-xy-xz+xyz \end{aligned}$$

Similarly, $(x*y)*z = x+y+z-yz-xy-xz+xyz$

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

Identity element : If e is the identity element for * then $a*e=e*a=a \quad \forall a \in X$

$\Rightarrow \quad a+e-ae=a$

$\Rightarrow \quad e=0$

Inverse of an element : Let a be any element of X. Let b the inverse of a. Then

$a*b = 0$

$\Rightarrow \quad a+b-ab = 0$

$\Rightarrow \quad b = a/(a-1) \text{ if } a \neq 1$

Thus if $a \neq 1$, then $a^{-1} = a/(a-1)$.

Example : Let I_+ be the set of positive integers. Let

$*: I_+ \times I_+ \to I_+$ be defined as follows: $x*y =$ lcm of x and y.

Show that * is commutative and associative. Find the identity element.

Solution: We know that the least common multiple of two positive integers is again a positive integer. Hence * is binary operation on I_+.

*** is commutative:** We know that lcm of x and y = lcm of y and x. Hence $x*y = y*x$. Thus * is commutative:

*** is associative:** For any three positive integers x, y and z,

$x*(y*z) = x*(\text{lcm of } y \text{ and } z)$ = lcm of x, y and z

= (lcm of x and and y) *z = (x *y) *z. Thus * is associative.

Identity Element : We know that for any positive integer x, the least common multiple of x*1=x, Hence $1 \in I$, such that $x*1 = 1*x \, \forall x \in I_+$. Thus 1 is the identity element.

Example : Let X={0,1,2,3,4} and x_5 be the operation "multiplication modulo 5". Give composition table for the operation x_5. Show that x_5 is commutative, Also indicate the identity element.

Solution : For $a,b \in X$, $a \times_5 b = ab(\text{mod } 5) = r$, Where r is the remainder when ab is divided by 5. The composition table is given below:

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the table, we see that $a \times_5 b$ for any $a, b \in X$ is again in the set X. Hence the set is closed under the operation $\times_5$. Since the entries in the table are symmetrical about main diagonal, the operation is commutative. From the table it is evident that 1 is the identity element.

Check your progress

1. Show that $x * y = x - y$ is not a binary operation over the set of natural numbers but it is binary operation on the set of integers. Is it commutative or associative?
2. How many distinct binary operations can be defined on the set $\{0,1\}$.

[Hint: Every binary operation * on $\{0,1\}$ can be described by the table

*	0	1
0		
1		

3. Consider the binary operation * defined on the set $A = \{a, b, c, d\}$ by the following table:

*	a	b	c	d
a	a	c	b	d
b	d	a	b	c
c	c	d	a	a
d	d	b	a	c

Compute $c * d$, $d * c$, $b * d$ and $d * b$. Is * commutative?

4. Show that $x * y = xy$ is a binary operation on the set N of natural numbers. Determine whether $*$ is commutative or associative.
5. Fill in the following table so that the binary operation $*$ is commutative.

$*$	a	b	c
a	b		
b	c	b	a
c	a		c

6. Let $I_5 = \{0,1,2,3,4\}$. Give composition table for the operation $+_5$ defined by $x +_5 y = (x + y)(\text{mod } 5)$. Indicate the identity element.

7. Let $*$ denote a binary operation on N given by $x * y = x$. Show that $*$ is not commutative, but is associative.

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers-Kolkata.

Uttar Pradesh Rajarshi Tandon open University

SBSCS-01

Discrete Mathematics

BLOCK 3

Counting Process

Course Design Committee

Dr. Ashutosh Gupta — **Chairman**
Director-In-charge,
School of Computer and Information Science,
UPRTOU, Allahabad

Prof. R. S. Yadav — **Member**
Department of Computer Science and Engineering
MNNIT-Allahabad, Allahabad

Ms. Marisha — **Member**
Assistant Professor, Computer Science
School of Sciences, UPRTOU, Allahabad

Mr. Manoj Kumar Balwant — **Member**
Assistant Professor, Computer Science
School of Science, UPRTOU, Allahabad

Course Preparation Committee

Dr. A. K. Pandey — **Author**
Reader, Dept of Mathematics
ECC, Allahabad

Prof. D. P. Chaudhary — **Editor**
Ex-Professor, University of Allahabad
Allahabad, Uttar Pradesh

Dr. Ashutosh Gupta
Director (In-charge), School of Computer and Information Science,
UPRTOU, Allahabad

Ms. Marisha (Coordinator)
Assistant Professor, School of Sciences,
UPRTOU, Allahabad

Unit-1

Mathematical Induction

Structure

1.1 Introduction

(1) This is most basic unit of this block as it introduces the concept of The principle of Mathematical induction is of great help in proving results involving a natural member for every n or for every $n \geq$ some positive integer m. If $P(n)$ is a statement involving a positive integer n. If $P(l)$ is true $\Rightarrow$ truth of $P(l+1)$ $\forall$ $l \geq$ m.

Then $P(n)$ is true for every $n \geq m$. The particular case of this result for $m = 1$ is usually referred to as the principle of mathematical induction and in fact the general version stated above can be obtained from version stated above can be obtained from this particular case. The above principle is popularly stated as if a statement holds for $n = 1$ and whenever it is true for $n = t$, it holds for $n = t + 1$, then it holds for all natural numbers n. There was a reason for looking the further generalization, apart from mathematical interest. The reason was the many applications. Apart from the ones we mentioned at the beginning, the binomial theorem has several applications in probability theory, calculus and approximating numbers like $(1.02)^{15}$. We shall discuss a few of them in this unit.

1.2 Objectives

After reading this unit we should be able to

1. Understand the Principle of Mathematical Induction

2. Understand Second Principle of Induction

4. Understand the Well ordering property

1.3 Mathematical Induction

The principle of Mathematical induction is of great help in proving results involving a natural member for every n or for every $n \geq$ some positive integer m.

Principle of Mathematical Induction: If $P(n)$ is a statement involving a positive integer n for which

(2) $P(m)$ is true for some integer m.
(3) Truth of $P(l) \Rightarrow$ Truth of $P(l+1)\ \forall\ l \geq$ m.

Then $P(n)$ is true for every $n \geq m$. The particular case of this result for $m = 1$ is usually referred to as the principle of mathematical induction and in fact the general version stated above can be obtained from version stated above can be obtained from this particular case. The above principle is popularly stated as if a statement holds for n=1 and whenever it is true for $n = t$, it holds for $n = t + 1$, then it holds for all natural numbers n.

Example: $2^n > n^2$ for all $n \geq 5$. Clearly the statement does not hold for $n = 2, 3, 4$.

$2^5 = 32 > 25 = 5^2$ & so if holds for n = 5.

Take any $l \geq 5$ and assume that $2^l > l^2$.

Then $2^{l+1} = 2.2^l = 2^l + 2^l. > l^2 + l^2$ (by hypothesis)

$\geq l^2 + 5l \quad (\because l \geq 5)$

$= l^2 + 2l + 3l \leq l^2 + 2l + 3 \times 5\ (\because l \geq 5)$

$> l^2 + 2l + 1\ (\because\ 15 > l)$

$= (l+1)^2$ i.e. $2^{l+1} > (l+1)^2\ \ \forall\ l \geq 5$.

$\therefore$ Assumption of truth of the statement for $l \geq 5$ implies its truth for $l + 1$. $\therefore$ the above statement is true for every $l \geq 5$ by the above result.

Example: Show that for all integers greater than zero : $2^n >= n+1$.

Solution:
For n = 1, the above equation evaluates to:

2 >= 1+ 1, which is true.

Now assume that the property is valid for n=k

Thus p(k) evaluates to:

$2^k >= k+1$.

Now, we have to prove that property is valid for n = k+1

p(k+1): $2^{k+1} >= k+2$

Now, multiplying p(k) by 2 on both sides we get,

$2^k.2 >= (k+1).2$

=> $2k+2 >= k+2$

Also, we know that, $2^{k+1} = 2^k . 2$

Thus, $2^{k+1} >= k+2$

Thus, the property is true for p(k+1) and hence, true for all n.

Example: Apply mathematical induction rule to prove 1 + 2 + 3 +... + n = n (*n*+1)/2 for all positive integers n

Solution:

Let p(n) be 1 + 2 + 3 +... + n = n (*n*+1)/2

Step 1: First, we show p(1) is true

Left side = 1

Right side = 1 (1+1)2 = 1

Both sides are equal, hence p(1) is true

Step 2: Let us assume p(k) is true

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

Show that p(k + 1) is true by adding a(k + 1) on both the sides at the above statement

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

taking (k+ 1) as common we get,

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

The above statement can be rewritten as

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

which is the statement for p(k + 1).

Hence, proved.

Example: Apply mathematical induction rule to prove $1^3 + 2^3 + 3^3 + ... + n^3 = [n(n+1)/2]^2$ for all positive integers n.

Solution:

Let p(n) be $1^3 + 2^3 + 3^3 + ... + n^3 = n^2 (n+1)24$

Step 1: First, we show p(1) is true.

Left side = $1^3 = 1$

Right side = 1^2 (1+1)24 = 1

Both sides are equal. Hence, p(1) is true.

Step 2: Let us assume p(k) is true

$1^3 + 2^3 + 3^3 + \ldots + k^3 = k^2 (k+1)/24$

Adding $(k + 1)^3$ on both the sides

$1^3 + 2^3 + 3^3 + \ldots + k^3 + (k + 1)^3 = [k (k+1)/2]^2 + (k + 1)^3$

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

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

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

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

Thus, the above statement can be rewritten as

$1^3 + 2^3 + 3^3 + \ldots + k^3 + (k + 1)^3 = [(k + 1) (k+2)/2]^2$

which is the statement for p(k + 1)

Hence, proved.

Example:

Prove that **n ! > 2** ^{n} for all positive integers n greater than or equal to 4. (Note: n! is n factorial and is given by 1 * 2 * ...* (n-1)*n.)

Solution:

Statement P (n) is defined by $n! > 2^n$

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

4! = 24

$2^4 = 16$

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

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

$k! > 2^k$

Multiply both sides of the above inequality by k + 1

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

The left side is equal to $(k + 1)!$. For $k >, 4$, we can write
$k + 1 > 2$

Multiply both sides of the above inequality by 2^k to obtain
$2^k (k + 1) > 2 * 2^k$

The above inequality may be written
$2^k (k + 1) > 2^{k+1}$

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

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

Example:
Prove that for any positive integer number n, $\mathbf{n^3 + 2n}$ is divisible by 3

Solution

Statement P (n) is defined by
$n^3 + 2n$ is divisible by 3

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

Hence, p (1) is true.

STEP 2: We now assume that p (k) is true
$k^3 + 2k$ is divisible by 3
is equivalent to
$k^3 + 2k = 3M$, where M is a positive integer.

We now consider the algebraic expression $(k + 1)^3 + 2(k + 1)$; expand it and group like terms
$(k + 1)^3 + 2(k + 1) = k^3 + 3k^2 + 5k + 3$
$= [k^3 + 2k] + [3k^2 + 3k + 3]$
$= 3M + 3[k^2 + k + 1] = 3[M + k^2 + k + 1]$

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

Example: Prove 6^n+4 is divisible by 5 by mathematical induction.

Step 1: Show it is true for $n=0$.

$6^0+4=5$, which is divisible by 5

Step 2: Assume that it is true for $n=k$.

That is, $6^k+4=5M$, where $M \in I$.

Step 3: Show it is true for $n=k+1$.

That is, $6^{k+1}+4=5P$, where $P \in I$.

$6^{k+1}+4=6\times 6^k+4=6(5M-4)+4 \quad 6^k=5M-4$

by Step 2, $30M-20=5(6M-4)$, which is divisible by 5

Therefore it is true for $n=k+1$ assuming that it is true for $n=k$.

Therefore 6^n+4 is always divisible by 5.

Example: Prove $5^n + 2\times 11^n$ is divisible by 3 by mathematical induction.

Solution

Step 1: Show it is true for $n=0$. 0 is the first number for being true.

$5^0+2\times 11^0=3$, which is divisible by 3.

Therefore it is true for $n=0$.

Step 2: Assume that it is true for $n=k$.

That is, $5^k+2\times 11^k=3M$.

Step 3: Show it is true for $n=k+1$.

That is, $5^{k+1}+2\times 11^{k+1}$ is divisible by 3.

$5^{k+1}+2\times 11^{k+1}=5^{k+1}+2\times 11^k\times 11$

$=5^{k+1}+(3M-5^k)\times 11 \quad (2\times 11^k=3M-5^k$ by assumption at Step 2)

$=5^k\times 5+33M-5^k\times 11=33M-5^k\times 6$

$=3(11M-5^k\times 2)$, which is divisible by 3

Therefore it is true for $n=k+1$ assuming that it is true for $n=k$.

Therefore $5^n+2\times 11^n$ is always divisible by 3 for $n\geq 0$.

3.4 Second Principle of Induction :

If $P(n)$ is a statement involving a natural number n and Truth of $P(l)$ $\forall\, l < m \Rightarrow$ Truth of $P(m)$, then the statement is true for all natural numbers n. We shall illustrate its uses later in this unit. The second principle of induction is a consequence of the well ordering property of the set $\mathbb{N}$ of natural number or of $\mathbb{N} \cup \{0\}$.

3.5 Well ordering property :

Every non empty subset A of $\mathbb{N}$ (or of $\mathbb{N} \cup \{0\}$ has a least element i.e. there is an element $l \in A$ for which $l \leq a$ for every $a \in A$.

We are omitting the proof but the reader may satisfy himself by considering various subsets of $\mathbb{N}$ and obtain least elements of them.

This result does not hold for $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$.

<u>Check your progress</u>

1. Prove that $|m + n| = |m| + |n|$ occurs if and only if m and n have same sign (positive or negative) or one of them at least in zero and that

   $|m + n| < |m| + |n|$ if and only if they are of opposite sings.

2. Prove that $||a| - |b|| \leq |a - b|$ for any $a, b \in \mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$.

3. Prove that $3^n > 2^n + 1$ for all $n \geq 2$.

4. Prove that $1^3+2^3+\ldots.. n^3= \dfrac{n^2(n+1)^2}{4}$ $\forall\, n \geq 1$.

5. Prove that for any real number $x > -1$, $(1 + x)^n \geq (1 + nx)$ $\forall\, n \geq 1$.

6. Prove that $n! > 2^n$ $\forall\, n \geq 4$.

7. Prove that $n! > 4^n$ $\forall\, n \geq 9$.

8. Let $a_1 = 1$ and $a_n = \sqrt{3a_{n-1} + 1}$ $\forall\, n \geq 2$. Prove that $a_n < \dfrac{7}{2}$ $\forall$ integer $n \geq 1$.

9. Prove that $2^n > n^3$ for all $n \geq 10$

10. Show that $n! > 3n$ for $n \geq 7$.

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

Unit-2

Combinatorics

Structure

2.1 INTRODUCTION

Whole of the discipline of Mathematics evolved but of "counting" so much so as in Indian language. The word for Mathematics is ***Ganita*** which literally means counting or counted. All the types of numbers like integers, rational, real or couplex numbers have there origin in the concept of natural or counting numbers: 1,2,3,……..

In this unit we are primarily interested in counting certain finite sets arising in day to day situations. We all want to know how but as the sets which we want to count become more and more complicated, we have to be more precise and systematic. We first enunciate certain "basic counting principle" by the help of which we can tackle most of the situations we shall be interested in counting

2.2 Objectives

After reading this unit you should be able to

- Recall the basic counting principles
- Recall Principle of Disjunctive counting
- Recall Principle of Sequential counting
- Identify Ordered and Unordered Partitions

2.3 Basic counting principles

2.3.1. Principle of Disjunctive counting (Sum Rule)

It simply states that if $s_1, s_2, \ldots.. s_n$ are finite sets which are paraise disjoint (i.e. two of them have a common element, then $|S_1 \cup S_2 \cup \ldots.. \cup S_n| = |S_1| + |S_2| + \ldots. + |S_n|$

Where we use the symbol $|s|$ to denote the number of elements in a finite set s. ($n(s)$ or # (s) are other standard notations for $|s|$).

The above principle hardly needs a proof becomes in counting $s_1 \cup \ldots. \cup s_n$ ww first count the elements of s_1 followed by those of s_2 etc and became these sets are pair wise disjoint, we element will be counted move than once and so R.H.S. gives $|s_1 \cup \ldots \cup s_n|$

Example: If $s_1 = \{1, 2, \ldots\ldots 7\}$, $s_2 = \{a, b, \ldots\ldots z\}$, $s_3 = \{\alpha, \beta, r, \pi \in\}$ then clearly these are finite pairwise disjoint sets

$\therefore |s_1 \cup s_2 \cup s_3| = |s_1| + |s_2| + |s_3| = 7 + 26 + 5 = 38$

Example: If a certain farmer has six cows, seven goats and four dogs then we first form the sets of the respective animals, observe that these are pairwise disjoint, and then we can find the total number of livestocks in his household.

This principle apparently is restrictive in the sense of pairwise disjointness, but we shall see later n that we can derive the"**Inclusion Exclusion principle**" from the principle stated above using which we can count the number of element of a finite union of overlapping finite sets.

2.3.2. Principle of Sequential counting (Profit Rule)

We known that certain product of two, three or more sets are defined as the sets of ordered pairs, triples or in general n sets (which are not necessarily distinct):

$A \times B = \{(a, b) \mid a \in A, b \in B\}$. $A \times B \times C = \{(a, b, c) \mid a \in A, b \in B, c \in C\}$

$A_1 \times A_2 \times \ldots. \times A_n = \{(a_1, a_2, \ldots.. a_n) \mid a_i \in A_i \ \forall\ 1 \le i \le n)$. Here the sets A, B, A_i, A_j etc are necessarily pairwise disjoint. This principle states that if $A_1, A_2, \ldots\ldots A_n$ are finite sets then $|A_1 \times A_2 \times \ldots\ldots. \times A_n| = |A_1| |A_2| \ldots. |A_n|$. This is because we observe that to count the ordered notables $(a_1, a_2, \ldots. a_n)$ with $a_1 \in A_1$ for $1 \le I \le n$, we note that a_1 can be any of the

$|A_1|$ element of A, and for each of the $|A_1|$ choice of a_1, a_2 can be chosen in $|A_2|$ ways and hence a_1 and a_2 can be chosen in $|\lambda_1|\lambda_2|$ way and so on. Indirectly we see that there are altogether $|A_1|A_2|\ldots|A_n|$ such elements in $A_1\times \ldots\times A_n$.

Example: If S is a set having n elements, then S has 2^n subsets.

Let $S = \{a_1, a_2, \ldots a_n\}$ each subset $A\subseteq S$ is a collection of some of the elements of S. Here 'some' include the cases 'none' and 'all' also. We associate with A, a unique sequence (i.e. ordered list or ……….) of length of o's and 1's in the sense that the with element of this sequence is taken as 1 in case are $\in A$ and o if $\in A$. For example, the subset $\{a_2, a_4\}$ is associated with the sequence $010\underbrace{100\ldots0}_{zero}$ Φ is associated with $\underbrace{00\ldots0}_{all\ zeros}$ and s with of $T = \{0, 1\}$ then the set of all such 'binary' sequences is $T^n = T\times T \ldots \times T$ (n copies). By this principle $|T^n| = |T| \ldots |T|$ {n times}

$= 2 \times 2\times2 \ldots 2$ (n times) $= 2^n$

By the one to one correspondence between the set of all subsets and the set of all binary segment of length n we se that there are altogether 2^n subset of s i.e.

$|O(s)| = 2$ Where $O(s)$ is the set of all subsets of s (called the power set of s).

Exercise: Find the number of distinct positive integer <1000 which are even and have distinct digit.

Note: All integer are of the form $(a_2, a_1 a_0)_{,0}$ ($= 100a_2+10_a, a_0$) in which $a_0\in \{0, 2, 4, 6, 8\}$, $a_, \in \{0, 1, \ldots, a\}$, $a_2\in \{0, 1, \ldots a\}$ a_0 has s choices, a_1 has $(10 - 2)= 8$ choices $\equiv$ { $a_2\neq a, a_0$) by the principle of sequencial counting (product role) there are $s\times a\times b = 360$ such sequences. the are 360 such positive integers.

Notations: 1. The product 1.2.3… $(n - 1)n$ of the first n positive integers is called the <u>factorial</u> of n or n <u>factorial</u> and denoted by $n!$. It appears naturally in counting number of arrangements of n distinct objects and many other situations. We have already encountered in the definition of determinant of ordre $n\times n$. It is customary to put $0! = 1$.

2. For integers $1 \leq .. \leq n$, we define the binomial coefficient $\binom{n}{r}$ or ${}^nc_r$ or c (n, *r*) as

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

As we shall see that it appears naturally in counting the number of ways of selecting *r* distinct objects from a collection of *n* objects. Also it arises as coefficients of terms when we expand $(a+b)^n$ as a sum of terms of the form $\alpha\ a^i b^j$ where $\alpha,\ i,\ j$ are non negative integers and *a, b* come from some number sets within which addition, multiplication etc are possible like. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ etc.

In case the partition blocks A_1, A_2, ….. a_1 are all of equal size q (say) i.e. $|A_i| = q\ \forall \leq I \leq +$ then n = qt and we have the following result.

2.4. Ordered and Unordered Partitions

Theorem: The number t-part unordered partition each of cell size is $\frac{n!}{t!(q_1)^t}$

This is because each such partition gives on arranging the t-subsets, t! ordered partition whose total number is $\frac{n!}{q!\,q!.....qi} = \frac{n!}{(q!)^t}$

Example: In how many ways 15 persons from a given set of 20 persons can be distributed into four teams where the first team has 6 persons, the second has 4 persons respectively.

Solution: We may first choose 15 persons from a setup 20 in C(20, 15) = C(20, 5)=20, 19, 18, 17, 16 / 2,3,4,5 = 3,17,19=969 ways and then the number of 4-part ordered partition of type (6,4,3,2) is $\frac{13!}{6!\ 4!\ 3!\ 2!}$

$\therefore$ the total number required is $C(20{,}5) = \frac{15!}{6!\ 4!\ 3!\ 2!}$

Example: If instead, we want the number of ways of forming 5 team of 3 persons each, then the number is $C(20,5)=\frac{15!}{5!(3!)^5}$. These are unordered partition as we have not called the teams first second etc.

Check your progress

1. Find the number of 5-part ordered partition of the set $\{a_1, a_2 \ldots\ldots a_{12}\}$ of the type (5,3,2,1,1)

2. Find the number of all unordered 4-part partitions of set in the preceding exercise into blocks of 3 each.

3. Find the number of arrangement of the letters of the word Book. Make a list of them and slow the correspondence between these and the set of all 3 part ordered partitions of the type (1,1,2) of the set $\{a_1, a_2, a_3, a_4\}$.

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

Unit-3

Permutation

Structure

3.1 Introduction

Permutation is a counting problem which comes under the branch of mathematics called combinatorics. Let $n \geq 1$ be an integer and $r \leq n$, then the number of ways of arranging r objects out of n objects, is denoted by P(n, r). Since each of the r objects can be arranged in r! ways. The number of ways of arranging r objectsis r!. Thus by the counting principle, the number of ways of choosing r objects and arranging the r objects chosen can be done in C(n, r).r! ways. But this is precisely P(n, r). In other words, we have P(n, r) = r!C(n, r). That is by permutation we mean an arrangement of objects in a particular order. The total number of permutations of n objects is n(n-1)(n-2)……..3.2.1 = n!.

In this unit we shall discuss some simple counting methods and use them in solving such simple counting problems.

3.2 Objectives

After reading this unit we should be able to

1. Understand the concept of P(n, r).
2. Permutations with Repetitions
3. Destinguish between Concept of permutation and combination.
4. Derive the formula C(n, r).r! = P(n, r).

3.3 Definition of Permutation

Definition: A permutation is an arrangement of a finite set of objects in a particular order.

For example, there are six different permutations of the set {a, b, c}. They are abc, acb, bac, bca, cab and cba.

Any arrangement on n distinct object taken r at a time (r □ n) is called r-permutation. The number of permutations of n distinct objects taken r at a time is given by

$$^{n}P_{r} = n\,(n - a)\,(n - 2)\;....\;(n - r + 1) = \frac{n!}{(n - r)}$$

Permutations with Repetitions

If out n objects in a set, p objects are exactly alike of one kind, q objects exactly alike of second kind and r objects exactly alike of third kind and the remaining objects are all different then the number of permutation of n objects taken all at a time is $= \frac{n!}{p!q!r!}$

(a) $\underline{|n} = n! = !n =$ Factorial of any quantity n is a factor of that quantity in descending order of integral n upto unity from right to left.

$$\underline{|n} = n(n-1)(n-2).....3.2.1$$

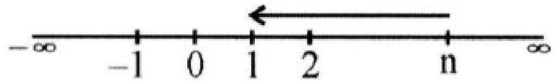


Fig. 1.10

$$\underline{|k} = k(k-1)(k-2).......3.2.1, \text{if } k \geq 1$$
$$= \text{meaningless, if } k < 0, k \notin I$$
$$= 1, \text{if } k = 0, 1$$

(b) (i) $^{n}P_{r} =$ A process to arrange n different things taking r different things at a time

$= \frac{\lfloor n}{\lfloor n-r} \qquad [n \geq r] \qquad$ **[r≥ 0, n > 0]**

(ii) Number of permutations (arrangement) of n different things $= \lfloor n$.

(iii) Number of permutations of n different things out of which P are alike but of same type, q are alike but are of same type, r are alike but are of same type and rest all are different $= \frac{\lfloor n}{\lfloor p \lfloor q \lfloor r}$

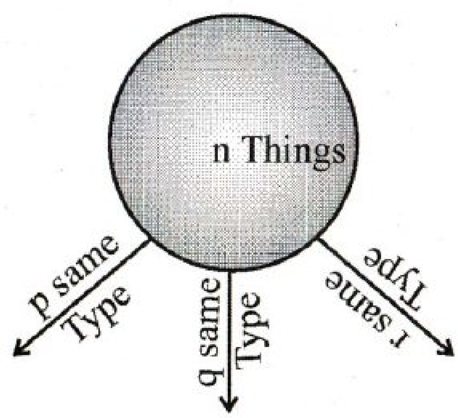


Fig. 1.11

(iv) ^nC_r = A process to select n different things taking r different things at a time

$= \frac{\lfloor n}{\lfloor n-r \lfloor r}$.

(v) Number of selection of r things ($r \leq n$) out of n identical things is only one.

(vi) Number of permutations of n different things taking r at a time when things can be repeated any number of times $= n.n.n.....r \text{ times} = n^r$

(vii) Total number of selection of zero or more than zero things from P identical thins = P + 1

Example: Calculate

1. $^4P_2$

$^4P_2 = 4! / (4 - 2)! = 24/2 = 12$

2. ${}^{6}P_{5}$

$^{6}P_{5} = 6! / (6 - 5)! = 6*5*4*3*2*1 / 1! = 720$

3. ${}^{4}P_{4}$

$^{4}P_{4} = 4! / (4 - 4)! = 4! / 0! = 4! = 4*3*2*1 = 24$

Example: How many two digit numbers can be formed using the digits 1, 2, 3 and 4 without repeating the digits?

Solution: Here we want to use 2 digits at a time to make 2 digit numbers. For the first digit we have 4 choices and for the second digit we have 3 choices (4 - 1 used already). Using the counting principle, the number of 2 digit numbers that we can make using 4 digits is given by

4 * 3 = 12

Example 5: How many 3 letter words can we make with the letters in the word **LOAD**?

Solution: There are 4 letters in the word load and making 3 letter words is similar to arranging these 3 letters and order is important since LOA and AOL are different words because of the order of the same letters L, O and A. Hence it is a permutation problem. The number of words is given by $_{4}P_{3} = 4! / (4 - 3)! = 24$

Example: How many ways are there to arrange the nine letters in the word **'ALLAHABAD'**

Solution : Since the word ALLAHABAD contains 4A's and 2L's, therefore there are

$$= \frac{9!}{4!2!} = 7560 \text{ ways.}$$

Example: Find the number of words, with or without meaning, which can be formed with the letters of the word **'CHAIR'**.

Solution: 'CHAIR' contains 5 letters.

Therefore, the number of words that can be formed with these 5 letters = 5! = 5*4*3*2*1 = 120.

Example: Find the number of words, with or without meaning, which can be formed with the letters of the word '**INDIA**'.

Solution: The word 'INDIA' contains 5 letters and 'I' comes twice.

When a letter occurs more than once in a word, then the permuation is obtained by dividing the factorial of the number of all letters in the word by the number of occurrences of each letter.

Therefore, the number of words formed by 'INDIA' = 5!/2! = 60.

Example: How many different words can be formed with the letters of the word '**SUPER**' such that the vowels always come together?

Solution: The word 'SUPER' contains 5 letters.

In order to find the number of permutations that can be formed where the two vowels U and E come together.

In these cases, we group the letters that should come together and consider that group as one letter.

So, the letters are S, P, R, (UE). Now the number of letters is 4.

Therefore, the number of ways in which these 4 letters can be arranged is 4!

In U and E, the number of ways in which U and E can be arranged is 2!

Hence, the total numbers of ways in which the letters of the 'SUPER' can be arranged such that vowels are always together are 4! * 2! = 48 ways.

Example: Find the number of different words that can be formed with the letters of the word '**BUTTER**' so that the vowels are always together.

Solution: The word 'BUTTER' contains 6 letters.

The letters U and E should always come together. So the letters are B, T, T, R, (UE).

Number of ways in which the letters above can be arranged = 5!/2! = 60 (since the letter 'T' is repeated twice).

Number of ways in which U and E can be arranged = 2! = 2 ways

Therefore, total number of permutations possible = 60*2 = 120 ways.
Example: Find the number of permutations of the letters of the word '**REMAINS**' such that the vowels always occur in odd places.

Solution: The word 'REMAINS' has 7 letters.

There are 4 consonants and 3 vowels in it.

Writing in the following way makes it easier to solve these types of questions.

(1) (2) (3) (4) (5) (6) (7)

No. of ways 3 vowels can occur in 4 different places = $^4P_3$ = 24 ways.

After 3 vowels take 3 places, no. of ways 4 consonants can take 4 places = $^4P_4$ = 4! = 24 ways.

Therefore, total number of permutations possible = 24*24 = 576 ways.

Check your progress

(1) Find the of ways in which 12 diffferent beads can be arranged to form a necklace.

(2) In how many different ways can five boys and five girls form a circle such that the boys and girls are to be alternate.

(3) How many permutations can be made out the letters of the word "TRINGLE"? How many of these will begin with T and end with E?

(4) How many permutations can be made out the letters of the word "INSURANCE", so that the vowels are never separated?

(5) How many permutations can be made out the letters of the word "PATALIPUTRA" without changing the relative positions of the vowels and consonants?

(6) How many permutations can be made out the letters of the word "OMEGA"

(i) O and A can occupying end places, (ii).E being alawasys in the middle,

(iii) Vowels occupying odd places, (iv).Vowels being never together.

(7) Consider 21 different pearls ona necklace. How many ways can be pearls be placed in on this necklace such that 3 specific pearls always remain together?

(8) In how many ways can 24 personsbe seated round a table, if there are 13 sets?

(9) How many necklaceof 12 beads each can be made from 18 beads of various colours?

(10) Find the number of ways in which candidates A_1, A_2, ...,A_{10} can be ranked if (i) A_1 *and* A_2 are next to each other (ii) A_1 is always above A_2.

(11) Find the number of ways in which four different letters can be put in their four addressed envelopes so that (i) at least two of them are in the wrong envelopes. (ii) all the letters in the wrong envelopes.

(12) Find the number of ways in which four friends can put up in 8 hotels of a town, if (i) there is no restriction. (ii) no two friends can stay together. (iii) all the friends do not stay in same hotel.

(13) Prove that P(n, r) = P(n-1, r) + rP(n-1, r-1).

(14) P(1,1) + 2P(2,2) + 3P(3,3) + 4P(4,4) + ...+ nP(n,n) = P(n+1,n+1) – 1,

(15) If P(56, r+6) : P(54, r+3) = 30800 : 1, find P(r, 2).

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P.T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I.N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

UNIT – 4

Combination

Structure

4.1 Introduction

4.2 Objectives

4.3 Definition of Combinations

4.1 Introduction

Combonation is a counting problem which comes under the branch of mathematics called combinatorics. Let $n \geq 1$ be an integer and $r \leq n$, then the number of ways of choosing r objects out of n objects, is denoted by c(n, r). Since each of the r objects choosen can be arranged in r! ways. The number of ways of arranging r objectsis r!. Thus by the counting principle, the number of ways of choosing r objects and arranging the r objects chosen can be done in C(n, r).r! ways. But this is precisely P(n, r). In other words, we have P(n, r) = r!C(n, r).

In this unit we shall discuss some simple counting methods and use them in solving such simple counting problems.

4.2 Objectives

After reading this unit we should be able to

1. Understand the concept of C(n, r).

2. Destinguish between Concept of permutation and combination.

3. Derive the formula C(n, r) = C(n, n-r).

4.3 Definition of Combination

Any selection which can be made by taking some or all of the objects at a time out of a given number of objects is called a combination.

Example: A term of two player selected out of five players is a combination of 5 players taken 2 at a time.

In the case of a combination, the order of the objects does not matter. The objects in a combination when arranged give rise to a permutation. The number of combination of n distinct objects taken r (r≤n) at a time is given by ${}^nC_r = \frac{n!}{r!(n-r)!}$

It is clear from the definitions or ${}^nP_r$ and ${}^nC_r$ that ${}^nP_r = {}^nC_r \times r!$

Note: (i).Total number of selection of zero or more things from n different things $= {}^nC_0 + {}^nC_1 + {}^nC_2 + {}^nC_3 + ... + {}_nC_n = 2^n$.

(ii) Number of ways of distributing n identical things among r persons when each person may get any number of things $= {}^{n+r-1}C_{r-1}$.

(iii) Number of ways of dividing (m + n) different things in two groups containing m and n things respectively.

$$= {}^{m+n}C_m \times {}^nC_n = \frac{\underline{|m+n}}{\underline{|n}\,\underline{|m}}$$

(iv) Number of ways of dividing 2m different things in two groups each containing m things

$$= {}^{2m}C_m \times {}^mC_m \times \frac{1}{\underline{|2}} = \frac{\underline{|2m}}{\underline{|m}\,\underline{|m}\,\underline{|2}}$$

(v) Number of ways of dividing 3m different things in three groups each having m things

$$= {}^{3m}C_m \times {}^{2m}C_m \times {}^mC_m \times \frac{1}{\underline{|3}} = \frac{\underline{|3m}}{\underline{|m}\,\underline{|m}\,\underline{|m}} \times \frac{1}{\underline{|3}}$$

(vi) Number of circular arrangements of n different things $= \frac{\underline{|n-1}}{2}$.

(vii) Number of circular arrangements of n different things where both the directions – clockwise and anticlockwise occur $= \frac{\lfloor n-1}{2}$.

Example: Find the number of diagonals which can be drawn by joining the angular points of a heptagon.

Solution: A heptagon has seven angular points (vertices) and seven sides. The join of two angular points is either a side or a diagonal. The number of lines joining the angular points. $^7C_2 = \frac{7!}{2!5!} = 21$. Since this number includes the seven sides,

therefore, number of diagonals = 21 – 7 =14.

Example: In how many ways can a committee of 5 persons be formed from 6 men and 4 women so as the include at least 2 women?

Solution: There are the following three cases. The committee may consist of

(i) 3 men and 2 women,

(ii) 2 men and 3 women,

(iii) 1 man and 4 women.

We can select 3 men and 2 women in $^6C_3 \times {}^4C_2 = 20 \times 6 = 120$ ways

We can select 2 men and 3 women in $^6C_2 \times {}^4C_3 = 15 \times 4 = 60$ was

We can select 1 men and 4 women in $^6C_1 \times {}^4C_4 = 6 \times 1 = 6$ ways.

Since all the three cases are disjoint, hence by sum rule, the required number of ways = 120 + 60 + 6 = 186.

Example: There are 10 balls in a bag numbered from 1 to 10. Three balls are selected at random. How many different ways are there of selecting the three balls?

$$^{10}C_3 = \frac{10!}{3!\,(10-3)!} = \frac{10 \times 9 \times 8}{3 \times 2 \times 1} = 120$$

Example: In how many ways can a committee of 1 man and 3 women can be formed from a group of 3 men and 4 women?

Solution: No. of ways 1 man can be selected from a group of 3 men = $^3C_1$ = 3! / 1!*(3-1)! = 3 ways.

No. of ways 3 women can be selected from a group of 4 women = $^4C_3$ = 4! / (3!*1!) = 4 ways.

Example: Among a set of 5 black balls and 3 red balls, how many selections of 5 balls can be made such that at least 3 of them are black balls.

Solution: Selecting at least 3 black balls from a set of 5 black balls in a total selection of 5 balls can be

3 B and 2 R

4 B and 1 R and

5 B and 0 R balls.

Therefore, our solution expression looks like this.

$^5C_3 * {}^3C_2 + {}^5C_4 * {}^3C_1 + {}^5C_5 * {}^3C_0 = 46$ ways.

Example: How many 4 digit numbers that are divisible by 10 can be formed from the numbers 3, 5, 7, 8, 9, 0 such that no number repeats?

Solution: If a number is divisible by 10, its units place should contain a 0.

After 0 is placed in the units place, the tens place can be filled with any of the other 5 digits.

Selecting one digit out of 5 digits can be done in $^5C_1 = 5$ ways.

After filling the tens place, we are left with 4 digits. Selecting 1 digit out of 4 digits can be done in $^4C_1 = 4$ ways.

After filling the hundreds place, the thousands place can be filled in $^3C_1 = 3$ ways.

Therefore, the total combinations possible = 5*4*3 = 60.

Example: Ten people go to a party. How many different ways can they be seated?

Solution: In this case, the anti-clockwise and clockwise arrangements are the same. Therefore, the total number of ways is ½ (10-1)! = 181 440

Example: In how many ways can a selection of 3 men and 2 women can be made from a group of 5 men and 5 women?

Solution: $^5C_3 * {}^5C_2 = 100$

Example:

Six friends want to play enough games of chess to be sure everyone plays everyone else. How many games will they have to play?

Solution: There are 6 players to be taken 2 at a time.

Using the formula:

They will need to play 15 games.

Example: How many numbers are there between 99 and 1000 having 7 in the units place?

Solution: First note that all these numbers have three digits. 7 is in the unit's place. The middle digit can be any one of the 10 digits from 0 to 9. The digit in hundred's place can be any one of the 9 digits from 1 to 9. Therefore, by the fundamental principle of counting, there are $10 \times 9 = 90$ numbers between 99 and 1000 having 7 in the unit's place.

Example: How many numbers are there between 99 and 1000 having at least one of their digits 7?

Solution: Total number of 3 digit numbers having atleast one of their digits as 7 = (Total numbers of three digit numbers) – (Total number of 3 digit numbers in which 7does not appear at all).

$= (9 \times 10 \times 10) - (8 \times 9 \times 9)$

$= 900 - 648 = 252.$

PERMUTATIONS AND COMBINATIONS 117

Example:

In how many ways can 5 children be arranged in a line such that

(i) Two particular children of them are always together

(ii) Two particular children of them are never together?

Solution:

(i) We consider the arrangements by taking 2 particular children together as one and hence the remaining 4 can be arranged in $4! = 24$ ways. Again two particular children taken together can be arranged in two ways. Therefore, there are $24 \times 2 = 48$ total ways of arrangement.

(ii) Among the $5! = 120$ permutations of 5 children, there are 48 in which two children are together. In the remaining $120 - 48 = 72$ permutations, two particular children are never together.

Example: If all permutations of the letters of the word AGAIN are arranged in the order as in a dictionary. What is the 49^{th} word?

Solution :

Starting with letter A, and arranging the other four letters, there are $4! = 24$ words. These are the first 24 words. Then starting with G, and arranging A, A, I and N in different ways, there are

$\frac{4!}{2!1!1!} = 12$ words. Next the 37^{th} word starts with I. There are again 12 words starting with I. This accounts up to the 48^{th} word. The 49^{th} word is NAAGI.

Example

In how many ways 3 mathematics books, 4 history books, 3 chemistry books and 2 biology books can be arranged on a shelf so that all books of the same subjects are together.

Solution :

First we take books of a particular subject as one unit. Thus there are 4 units which can be arranged in $4! = 24$ ways. Now in each of arrangements, mathematics books can be arranged in $3!$ ways, history books in $4!$ ways, chemistry books in $3!$ ways and biology books in $2!$ ways. Thus the total number of ways $= 4! \times 3! \times 4! \times 3! \times 2! = 41472$.

Example

A student has to answer 10 questions, choosing atleast 4 from each of Parts A and B. If there are 6 questions in Part A and 7 in Part B, in how many ways can the student choose 10 questions?

Solution

The possibilities are:

4 from Part A and 6 from Part B

or

5 from Part A and 5 from Part B

or

6 from Part A and 4 from Part B.

Therefore, the required number of ways is

$$^6C_4 \times {}^7C_6 + {}^6C_5 \times {}^7C_5 + {}^6C_6 \times {}^7C_4 = 105 + 126 + 35 = 266.$$

Example

A boy has 3 library tickets and 8 books of his interest in the library. Of these 8, he does not want to borrow Mathematics Part II, unless Mathematics Part I is also borrowed. In how many ways can he choose the three books to be borrowed?

Solution

Let us make the following cases:

Case (i)

Boy borrows Mathematics Part II, then he borrows Mathematics Part I also.

So the number of possible choices is

$^6C1 = 6$.

Case (ii)

Boy does not borrow Mathematics Part II, then the number of possible choices is $7C3 = 35$.

Hence, the total number of possible choices is $35 + 6 = 41$.

Check your progress

(1) Prove that

(i) $C(n, r) = C(n, n-r)$.

(ii) $C(n, r) + C(n, n-r) + C(n+1, r)$.

(iii) $nC(n-1, r-1) = (n+1-r)\ C(n, r-1)$.

(iv) $C(n, r) = n/r\ C(n-1, r-1)$.

(v) $C(n, r)/C(n, r-1) = n-r+1/r$.

(2) If $C(n, r-1) = 36$, $C(n, r) = 84$ and $C(n, r+1) = 126$, then find r and n.

(3) From a class of 60 students, 11 to be chosen for a cricket tournament. In how many ways can this be done?

(4) In how many ways can a cricket 11 by chosen out of a batch 15 players if (i) a particular is always chosen. (ii) a particular player is never chosen?

(5) How many different selections of 6 books can be made from11 different books, if (i) two particular books are always selected. (ii) two particular books are never selected?

(6) Mohan has 8 friends, in how many ways he invite one or more of them for dinner?

(7) Find the number of combinations that can be formed with 5 oranges, 4 mangoes and 3 bananas when it is essential to take (i) at least one fruit (ii) one fruit of each kind (iii) all bananas are taken together.

(8) In how many ways can a pack of 52 cards be divided equally among 4 players in order?

(9) In how many ways can a pack of 52 cards be formed into 4 groups of 13 cards each?

(10) In how many ways can a pack of 52 cards be divided equally among 4 sets, 3 of them having 17 cards each and fourth just one card?

(11) In how many ways can 12 balls be divided between two boys, one receiving 5 and the other 7 balls? Also in how many ways can thase 12 balls be divided into groups of 5, 4 and 3 balls respectively?

(12) In how many ways can 5 different balls can be arranged into 3 different boxes so that no box remains empty?

(13) In how many ways can 5 different balls can be distributed into 3 different boxes so that no box remains empty?

(14) In how many ways can 5 identical balls can be distributed into 3 different boxes so that no box remains empty?

(15) Four boys pickedup 30 mangoes, in how many ways can they divide them if all mangoes be identical?

(16) Find the positive number of solutionsof $x + y + z + w = 20$ under the following conditions: (i) zero values of x, y, z, w are included. (ii) zero values are excluded.

(17) Find the number of non- negative integral solutions of $3x+ y +z = 24$.

(18) In how many ways can three persons, each throwing a single dice once, make a sum of 15?

(19) Find the numer of combinations and permutationsof 4 letterstaken from the word "EXAMINATION".

(20) Find the number of positive eunequal integral solution of the equation $x+ y+z+w=20$.

(21) Find the number of rectangles excluding squares from a rectangle of size 9×6.

(22) Find the exponentof 3 in100!

(23) Find the number of zeros at the end of 100!

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P.T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

Uttar Pradesh Rajarshi Tandon
open University

SBSCS-01

Discrete Mathematics

BLOCK

4

Probability theory and application

Course Design Committee

Dr. Ashutosh Gupta Director-In-charge, School of Computer and Information Science, UPRTOU, Allahabad	**Chairman**
Prof. R. S. Yadav Department of Computer Science and Engineering MNNIT-Allahabad, Allahabad	**Member**
Ms. Marisha Assistant Professor, Computer Science School of Sciences, UPRTOU, Allahabad	**Member**
Mr. Manoj Kumar Balwant Assistant Professor, Computer Science School of Science, UPRTOU, Allahabad	**Member**

Course Preparation Committee

Dr. A. K. Pandey Reader, Dept of Mathematics ECC, Allahabad	**Author**
Prof. D. P. Chaudhary Ex-Professor, University of Allahabad Allahabad, Uttar Pradesh	**Editor**

Dr. Ashutosh Gupta
Director (In-charge), School of Computer and Information Science,
UPRTOU, Allahabad

Ms. Marisha (Coordinator)
Assistant Professor, School of Sciences,
UPRTOU, Allahabad

UNIT-1

Binomial Theorem

Structure

1.1 Introduction

Suppose we need to calculate the amount of the interest we will get after 6 years on a sum of moneythat we have invested at the rate of 12%compound interest per year.Suppose we need to find the size of the populationof a country after 15 years if we know that the annual grouth rate. A result that will help in finding these quations is the **binomial theorem.** This theorem as we will see, helping us to calculate the rational powers of any real binomial expression, that is any expression involving two terms.

The binomial theorem, was known to Indian and to greek mathematician in the 3rd century B.C. for some cases. The credit for the result for natural exponents goes to the Arab poet and mathematician **Omar Khayyam** (A.D. 1048– 1122). Further generalisationto rational exponents was done by the British mathematician **Newton**(A.D. 1642– 1727).

There was a reason for looking the further generalization, apart from mathematical interest. The reason was the many applications. Apart from the ones we mentioned at the beginning, the binomial theorem has several applications in probability theory, calculus and approximating numbers like $(1.02)^{15}$. We shall discuss a few of them in this unit.

1.2 Objectives

After reading this unit we should be able to

1. Understand the concept of binomial theorem for integral index and rational index for two variables
2. Write the binomial expression for expressions like $(x + y)^n$ for different values of x and y using binomial theorem.
3. Write the general term and middle term of the binomial expression.
4. Apply the binomial theorem for finding the approximate values of the nth roots of real numbers.

1.3 Binomial theorem for a natural index

We must have multiplied a binomial by itself, or by another binomial. Let us use this knowledge to do some expenssions.

(1) $(x + y)^1 = x+y$

(2) $(x + y)^2 = x^2+y^2 + 2xy$

(3) $(x + y)^3 = x^3+y^3 + 3x^2y + 3y^2x$

(4) $(x + y)^4 = x^4+y^4 + 4x^3y + 4y^3x + 6x^2y^2$ and so on

(5) $(x+y)^n = {}^nC_0\,x^n + {}^nC_1\,x^{n-1}\cdot y + {}^nC_2\cdot x^{n-2}\cdot y^2 + \ldots\ldots + {}^nC_n\,y^n$

In each of the equations above, the right hand side is called the binomial expansion of the left hand side.

Note: In each of the expansions, we have written the powers of the binomial in the expanded form in such a way that the terms are in descending powers of the first term of the binomial and the terms are in ascending powers of the second term of the binomial expansion. The sum of the powers of the first term and the powers of the second term is equal to the exponent of the binomial. If we use the combinatorial co-efficients, we can write the above expansions as

(1) $(x + y)^1 = C(1, 0)x + C(1, 1)y$

(2) $(x + y)^2 = C(2,0)x^2 + C(2, 2)y^2 + C(2, 1)xy$

(3) $(x + y)^3 = C(3,0)x^3 + C(3, 3)y^3 + C(3, 1)x^2y + C(3, 2)y^2x$

(4) $(x + y)^4 = C(4,0)x^4 + C(4, 4)y^4 + C(4, 1)x^3y + C(4, 3)y^3x + C(4, 2)x^2y^2$ and so on.

Most generally, we can write the binomial expansion of $(x + y)^n$, where n is a positive integer, as given in the binomial theorem

$$(x+y)^n = {}^nC_0\, x^n + {}^nC_1\, x^{n-1} \cdot y + {}^nC_2 \cdot x^{n-2} \cdot y^2 + \ldots\ldots + {}^nC_n\, y^n$$

Example : $(x + 3y)^4 = C(4,0)x^4 + C(4, 4)3^4y^4 + C(4, 1)x^3 3y + C(4, 3)3^3y^3x + C(4, 2)x^2 3^2y^2 = x^4 + 81y^4 + 12x^3y + 108y^3x + 36x^2y^2$

Example : $(1+a)^n = {}^nC_0 + {}^nC_1 \cdot a + {}^nC_2 \cdot \cdot a^2 + \ldots\ldots + {}^nC_n\, a^n$

Example : $(y/x + 1/y)^4 = C(4,0)\left(\frac{y}{x}\right)^4 + C(4, 4)\left(\frac{1}{y}\right)^4 + C(4, 1)\left(\frac{y}{x}\right)^3(1/y) + C(4, 2)\left(\frac{y}{x}\right)^2(1/y)^2 + C(4, 3)\left(\frac{1}{y}\right)^3\left(\frac{y}{x}\right).$

$= 1.\left(\frac{y}{x}\right)^4 + 1.\left(\frac{1}{y}\right)^4 + 4.\left(\frac{y}{x}\right)^3(1/y) + 6.\left(\frac{y}{x}\right)^2(1/y)^2 + 4.\left(\frac{1}{y}\right)^3\left(\frac{y}{x}\right).$

$= \left(\frac{y}{x}\right)^4 + \left(\frac{1}{y}\right)^4 + 4.\left(\frac{y}{x}\right)^3(1/y) + 6.\left(\frac{y}{x}\right)^2(1/y)^2 + 4.\left(\frac{1}{y}\right)^3\left(\frac{y}{x}\right).$

Example: The population of a city grows at the annual rate of 3%. What percentage increase is expected in 5 years? Give the answer upto 2 decimal places.

Solution: Suppose the population is a presently. By using of binomial theorem we have

$a(1+3/100)^5 = a[1+ c(5, 1).03 + c(5, 2)(.03)^2 + c(5, 3)(.03)^3 + c(5, 4)(.03)^4 + c(5, 5)(.03)^5]$.

$= a[1+ 5\times.03 + 10\times(.03)^2 + 10\times(.03)^3 + 5\times(.03)^4 + 1\times(.03)^5]$.

$= a[1+ 5\times.03 + 10\times(.03)^2]$.

$= a[1+ 5\times.03 + 10\times(.0009)]. = a\times 1.159$.

Example: Using binomial theorem, evaluate (i) $(102)^4$, (ii) $(97)^3$

Solution: (i). $(102)^4 = (100+2)^4 = c(4,0)(100)^4 + c(4,1).2(100)^3 + c(4,2)\,4(100)^2 + c(4,3)(2)^3.100 + c(4,4)(2)^4$

$= 100000000 + 4\times2\times1000000 + 6\times4\times 10000 + 4\times8\times100 + 1\times16$

$= 100000000 + 8000000 + 240000 + 3200 + 16 = 108343216$

(ii). $(97)^3 = (100-3)^3 = c(3,0)(100)^3 + c(3,1).(-3)(100)^2 + c(3,2)\,9(100) + c(3,3)(-3)^3$.

$= 1\times1000000 + -\,3\times3\times 10000 + 3\times9\times100 - 1\times27$

$= 1000000 - 90000 + 2700 - 27 = 912673$

Check your progress

1. Write the expansion of each of the following:

   (i). $(2x+3y)^4$ (ii). $(x-3y)^6$ (iii). $(4a-5b)^4$ (iv). $(ax+by)^6$

2. Write the expansion of each of the following:

   (i). $(1-y)^7$ (ii). $(1+x/y)^9$ (iii). $(1+2x)^5$ (iv). $(a/3+b/2)^5$ (v). $(3x-5/y)^4$

   (vi). $(x+1/x)^9$ (vii). $(x/y+y/x)^4$

3. Suppose I invest Rs. 100000 at 18% per year compound interest. What sum will I get back after 10 years? Give your answer up to 2 decimal places.

4. The population of bacteria increases at the rate of 2% per hour> If the count of bacteria at 9 a.m. is 150000, find the number at 1p.m. on the same day.

5. Using binomial theorem, evaluate each of the following:

(i). $(101)^4$ (ii). $(99)^7$ (iii). $(1.02)^5$ (iv). $(0.98)^7$ (v). $(12)^8$

1.4 General term and middle term in a binomial expansion:

Let us examine various terms in this expansion

$$(x+y)^n = {}^nC_0 x^n + {}^nC_1 x^{n-1} \cdot y + {}^nC_2 \cdot x^{n-2} \cdot y^2 + \ldots\ldots + {}^nC_n y^n$$

The first term is ${}^nC_0 x^n = x^n$

The second term is ${}^nC_1 x^{n-1} \cdot y = nx^{n-1}y$

The third term is ${}^nC_2 \cdot x^{n-2} \cdot y^2 =$ n (n-1)/2 $x^{n-2} \cdot y^2$

And so on. From the above, we can generalise that the (r+1)th term is **c(n, r) $x^{n-r} y^r$**

i.e. T_{r+1} = c(n, r) $x^{n-r} y^r$. T_{r+1} is called **the general term** of the binomial expansion.

Example: Find the fifth term in the expansion of $(x/y + y/x)^6$

Here n= 6, r= 5, the general term is $T_{4+1} = c(6,4)(x/y)^{6-4}(y/x)^4 = 15y^2/x^2$

We see that number terms in the binomial expansion is always one greater than the exponent of the binomial. This implies that if the exponent is even, the number of terms is odd, and if the exponent is odd, the number of terms is even. Thus, while finding the middle term in a binomial expansion, we come across two cases:

Case1: When n is even.

The number of terms is odd, the middle term is $(\frac{n}{2} + 1)^{th}$ term

Case 2: When n is odd.

The number of terms is even, the middle terms are $(\frac{n+1}{2})^{th}$ term and $(\frac{n+3}{2})^{th}$

Example: Find the middle term of the expansion of $(x^2 + y^2)^8$.

Solution: Here n= 8, so the number of terms (8+1)= 9. Hence middle term is $(\frac{8}{2} + 1)^{th}$

$= 5^{th}$ *term of the expantion.* Middle term is T_{4+1} = c(8, 4) $x^{2^4} y^{2^4}$ = 70 $x^8 y^8$.

Example: Find the middle term of the expansion of $(2x^2 + 1/x)^9$.

Solution: Here n= 9, so the number of terms (9+1)= 10. Hence middle terms are $(\frac{9+1}{2})^{th}$ term and $(\frac{9+3}{2})^{th}$

$= 5^{th}$ *term and* 6^{th} *term of the expantion.* Middle terms are T_{4+1} = c(9, 4) $(2x^2)^5(1/x)^4 = 4032x^{10}1/x^4 = 4032x^6$ and

T_{5+1} = c(9, 5) $(2x^2)^4(1/x)^5 = 2016\,x^8 1/x^5 = 2016x^3$.

Check your progress

1. Write the $(r+1)^{th}$term of the expansion of each of the following:

   (i). $(2x + y)^n$ (ii). $(x - 3y)^n$ (iii). $(4a - 5b)^n$ (iv). $(ax + by)^n$

2. Write the specified term of the expansion of each of the following:

   (i). $(1 - y)^7$, 5^{th}term (ii). $(1 + x/y)^9$, 7^{th}term (iii). $(1 + 2x)^5$, 4^{th}*term*

   (iv). $\left(\frac{a}{3} + \frac{b}{2}\right)^5$, 4^{th} *term*(v). $\left(3x - \frac{5}{y}\right)^4$, 4^{th}*term*

   (vi). $(x + 1/x)^9$, 7^{th}term (vii). $(x/y + y/x)^4$, 3^{rd} term

3. Find the middle term in the expansionof each of the following:

   (a). $(2x^2 + 1/x)^{10}$ (b). $(2x^2 + y)^9$ (c). $(x \quad + 1/x)^9$ (d). $(ax + by)^{12}$

4. Find the middle term in the expansionof each of the following:

   (i). $(1 - y)^{10}$ (ii). $(1 + x/y)^9$ (iii). $(1 + 2x)^{10}$ (iv). $\left(\frac{a}{3} + \frac{b}{2}\right)^{15}$ (v). $\left(3x - \frac{5}{y}\right)^{14}$

   (vi). $(x + 1/x)^9$ (vii). $(x/y + y/x)^{11}$

1.5 Binomial expansion for rational exponants

If n be rational number and x is a real number such that |x|< 1, then

$$(1 + x)^n = 1 + nx + n(n-1)x^2/2! + n(n-1)(n-2)x^3/3! + \dots\dots\dots\dots$$

Example: 1. $(1-x)^{-1} = 1+x+x^2+x^3+......\text{to}\infty$

2. $(1-x)^{-2} = 1+2x+3x^2+4x^3+......\text{to}\infty$

3. $(1-x)^{-3} = 1+3x+6x^2+10x^3+......\text{to}\infty$

4. $(1+x)^{-1} = 1+x+x^2+x^3+......\text{to}\infty$

5. $(1+x)^{-2} = 1-2x+3x^2-4x^3+......\text{to}\infty$

6. $(1+x)^{-3} = 1-3x+6x^2-10x^3+......\text{to}\infty$

7. $(1-3)^{-1} = 1+3+3^2+3^3+......\text{to}\infty$

8. $(1+2)^{-1} = 1+2+2^2+2^3+......\text{to}\infty$

9. $(1+2)^{-2} = 1-2{,}2+3.2^2-4.2^3+......\text{to}\infty$

10. $(1+5)^{-3} = 1-3.5+6.5^2-10.5^3+......\text{to}\infty$

Note: It is very useful to find n^{th} root of any real number up to some decimal places value

Use of Binomial applications on harder questions where identical things occur.

(i) $(a+x)^n = {}^nC_0\, a^n + {}^nC_1\, a^{n-1}\cdot x + {}^nC_2\cdot a^{n-2}\cdot x^2 + ... + {}^nC_n\, x^n$

(ii) ${}^nC_0 + {}^nC_1 + {}^nC_2 + ... + {}^nC_n = 2^n$

(iii) ${}^nC_1 + {}^nC_3 + {}^nC_5 + ...\text{uptooddof } n = 2^{n-1}$

(iv) ${}^nC_0 + {}^nC_2 + {}^nC_4 + ...\text{uptoevenof } n = 2^{n-1}$

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.
(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

UNIT-2

Probability

Structure

2.1 Introduction

Indaytodaylifeweseethatbeforestartingacricketmatchorgamblingorplayingofludo, diceetcallthesearea partofprobability Tossing of a coin is an activity and getting either a "Head" or a "Tail"are two possible outcomes. If we throw a die the possible outcomesof this activity could be any one of its faces having numeral, namely 1, 2, 3, …at the top face.

An activity that yields a result or an occurance is called an experiment. Normaly there are variety of outcomes of an experiment and it is a matter of chance as to which one of these occurs when an experiment is performed. In this unit, we propose to study various experiments, their outcomes and its Probability.

2.2 Objectives

After reading this unit we should be able to

1. Understand the meaning of a random experiment
2. Explain a sample space corresponding to an experiment.
3. Differentiatebetwwen various types of events as equally likely
4. Apply the binomial theorem for finding the approximate values of the nth roots of real numbers.

2.3 Some fundamental definitions of probability

(A) Random Experiment:

it is an experiment by which its outcome is not known in advance, however, the possible outcome of the experiment is known.

For example, if we toss a coin, we can't say definitely that it will turn up a head or a tail but we can say that it will turn up any of head or tail. So tossing a coin is a random experiment. Similarly, if we throw a die randomly then it can't be said in advance that the number appeared is 1 or 2 or 3 or 4 or 5 or 6, so it can be said that the number throwing of die is a random experiment.

(B) Sample Space:

The set of all possible outcomes of an experiment or a trial is called a sample space. It is denoted by S. Each outcome is a point of the sample space and it is called the sample point. For example, we consider the following trails:

(i) For tossing a coin, S = {H, T},
Where H and T denote Head and Tail, respectively.

(ii) For two coins, S = {(H, H), (H, T), (T, T)}
Here the outcome (H, T) stands for the ordered pair, first Head and the Tail or "Head on first coin, Tail on the second.

(iii) For a die, S = {1, 2, 3, 4, 5, 6}
Here 1, 2, 3, 4, 5 or 6, represent the number that appeared on die.

(iv) A person is selected at random and is asked about the day of the week on which he was born.
S = {Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday}.

(v) From a pack of cards, one card is selected then the outcome may be as
   (a) S = {Red, Black}
   (b) S = {Spade, Club, Heart, Diamond}
   (c) S = {A, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K}

(vi) A positive integer is selected at randome and is divided by 5 then the outcome as remainder may be S = {0, 1, 2, 3, 4}

All the above outcomes are as sample spaces.

(C) Discrete Sample Space :

A sample space having finite number of sample points, is said to be 'Discrete Sample Space'. All the above examples of sample space are Discrete Sample space. While a sample space containing non-enumerable number of points is said to be a continuous space.

(D) Event :

A subset of a sample space 'S' of the experiment E is said to be an 'Event' so that an event may be defined as the subset of a containing no outcome is a null or void set.

It represents an event which is impossible to occur. However, an event containing all sample points is an event that is certain to occur. Thus S itself is an event and so the empty set ϕ.

Example:

1. If S = {1, 2, 3, 4, 5, 4, 6} and A = {1, 3, 5}

   A is the subset of S and is, therefore, an event. Events are usually denoted by capital alphabet A, B, C, ...

2. Consider the tossing of a fair coin twice. The possible outcomes are (HH), (HT), (H,H), (T,T). The sample space S consists of four points

   $\{e_1, e_2, e_3, e_4\}$.

   The event A of getting at least one head is the set of outcomes.

   $\{(H,H), (H,T), (T,H)\} = \{e_1, e_2, e_3\}$

3. Consider a single throw of a die. There are six possible outcomes, the sample space S consists of six points $\{e_1, e_2, e_3, e_4, e_5, e_6\}$, where e_1 corresponds to the appearance of the number i. The event A: The outcome is even, is the set of points $\{e_2, e_4, e_6\}$.

4. Consider an experiment in which a pair of dice are thrown. The sample space S of this experiment consists of 36 points.

A : Event having score of the number appeared is > 12 equals ϕ.

B: Event having "sum of numbers on the faces is 9"

$= \{(6, 3), (5, 4), (4, 5), (3, 6)\}$

Since the events are sets, it is clear that statements concerning events can be translated. Thus, if A and B are events

(i) $A \cup B$ is the event, read as "Either A or B or Both".

(ii) $A \cap B$ is the event, read as "Both A and B".

(iii) $A' = \overline{A} = A^c = A^0 \rightarrow$ read as "A dash" or "A bar" or "A complement" or "A not".

(iv) A – B is the event, read as "A but not B".

(E) Simple Event or Elementary Event:

Every singleton subset of a sample space is a Simple Event or Elementary Event, But a subset of the sample space which has more than one element is said to be a mixed event.

e.g. $E \subset S$

For tossing a coin, {H} and {T} are Simple Events.

(F) Mixed Event:

Event subset of the sample space which has more than one element is called "Mixed Event".

Example: In case of throwing a die, appearing of odd numbers up is a Mixed Event. E = {1, 3, 5} which has three elements. All the above definitions can be considered by the figure drawn for throwing a die.

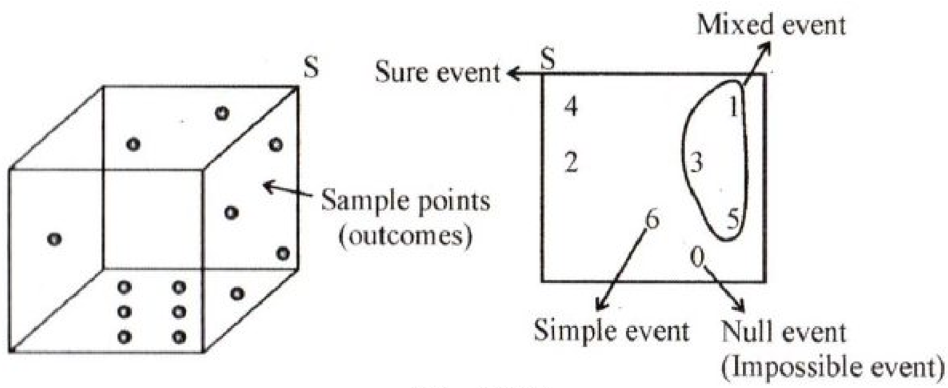


Fig. 1.12

(G) Equally Likely Event:

Two or more than two events are said to be Equally likely if any one of them can not be expected to occur in preference to the other but probability of occurrence of one is equal to probability of occurrence of the other.

Those events, the chances of whose happening is neither less nor greater than others are said to be "Equally likely Events".

e.g. (i) In tossing a coin, Head and Tail are equally likely to come up.

(ii) In throwing a die, any number may appear up so number appearing 1 is equally likely to any of 2, 3, 4, 5, and 6.

(H) Mutually Exclusive Events:

If the occurrence of one event prevents the occurrence of all other events then the events are said to be mutually exclusive events or two or more than two events are said to be mutually exclusive if these events can not occur simultaneously i.e. no member of these events is common.

Consider the experiment of throwing a die. Let A be the event "the number appeared is greater than zero but less than 4". Then A = {1, 2, 3}. Let B be the event, the number appeared is at least 5. Then B = {5, 6}. Clearly

$A \cap B = \phi$. The joint occurrence of A and B is thus an impossible event. The event A and B are said to be "Mutually Exclusive Events".

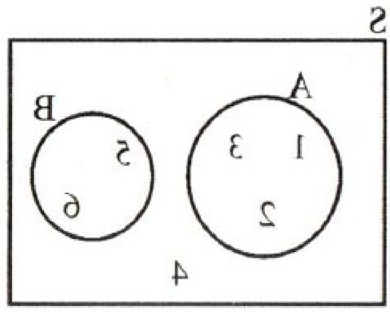


Fig. 1.13

In general, if A and B are any two events defined on a sample space S and $A \cap B = \phi$, then the events A and B are said to be mutually exclusive. If A is any event and A' is the complementary event of A, then $A \cap B = \phi$. Thus any event A and its complement A' are mutually exclusive events.

If $A \cap B = \phi$, then $P(A \cap B) = 0$.

(I) Exhaustive set of Events:

The totality of all possible events of a random experiment is known as the exhaustive set of events of the experiment.

For example: (1). In case of one, two and three tosses of a fair coin, the exhaustive set of events are respectively.

$$(H, T); \begin{pmatrix} HH & HT \\ TH & TT \end{pmatrix} \text{and} \begin{bmatrix} HHH & HHT \\ HTH & THH \\ HTT & THT \\ TTH & TTT \end{bmatrix}$$

$$(\text{one coin}), (\text{two coins}), (\text{three coins})$$

(2). In case of throwing a die only 1, 2, 3, 4, 5 and 6 may turn up but not any other number. For a single die 1, 2, 3, 4, 5 $\therefore$ S = {1, 2, 3, 4, 5, 6}

(J) Borel field of events:

If there exists a family T of certain subsets (the events) of S (the same space) satisfying the following axioms

(i) $S \in T$ and $\phi \in T$

(ii) $\bigcup_{i=1}^{n} Ai \in T$ if $Ai \in T, i=1,2,3,.......$

(iii) $A \in T \Rightarrow \overline{A} = S - A \in T$

Then the family of subsets T of subsets of S is said to be Borel field of events on S.

(K) Impossible Event:

As stated earlier, the null set is also a subset of the sample space and such an event is said to be "impossible Event" denoted by ϕ. It does not contain any sample point and hence cannot happen. Since $S \cup \phi = S$

and these are mutually exclusive $P(S \cup \phi) = P(S) + P(\phi) = P(S)$,

we get $P(\phi) = 0$, the probability of an impossible event is always zero.

(L) Complementary Event:

If A denotes an event, A' denotes an event which includes all the sample points not included in A. The complementary event of an odd number falling up in the throw of a die is the turning up of an even number.

e.g. For a single throw of a die S = {1, 2, 3, 4, 5, 6}

if A = {1, 3, 5}, then A' = {2, 4, 6}.

By pictorial representation,

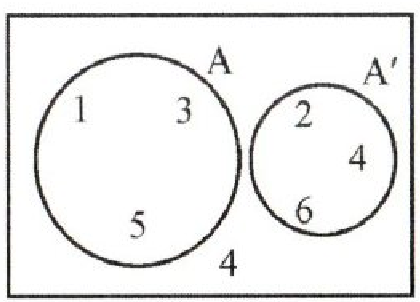


Fig. 1.14

(M) Probability of at least one event:

If A_1, A_2, ..., A_n are independent events with probabilities of success P_1, P_2, P_3, ..., P_n respectively then the probabilities of their failures are $(1-P_1)$, $(1-P_2)$, ..., $(1-P_n)$ and hence the probability of all failures is $(1-P_1)$. $(1-P_2)$... $(1-P_n)$ therefore the probability of at least one success is

$$1-(1-P_1)(1-P_2)...(1-P_n).$$

2.4 Definition of probability

(C) Mathematical or a Priori Definition of Probability:

If there are n exhaustive, mutually exclusive and equally likely events and m of which are favourable to an event A, then the probability that the event. A happens is given by

$$P(A)=\frac{m}{n}=\frac{n(A)}{n(S)} \qquad [\text{where } m \le n]$$

This gives the numerical measure of probability. Clearly, P i.e. P(A) is a positive number not greater than unity and never less than zero.

So that, $0 \le P(A) \le 1$.

(D) Statistical or Empirical Definition of Probability:

If trails be repeated a great number of times under the same conditions then the limit of the ratio of the number of times that an event happens to the total number of trails as the number of trails increases infinitely is said to be the probability of the happening of that event. It is assumed that the ratio approaches a finite and a unique limit.

Symbolically, if m be the number of times in which the event A happens in a series of n trials, then the probability, P, of the happening of this event is given by

$$P(A)=P=\lim_{n\to\infty}\frac{m}{n}$$

provided that the limit is finite and unique.

(E) Axiomatic definition of Probability or Probability measures:

If for a given sample space S and Borel field T, we consider a set function P on T. i.e. to every $A_i \in T$, we ascribe a real number P(A), such that

(i) $0 \le P(A) \le 1$

(ii) For mutually exclusive event, $A_1, A_2, A_3, \ldots, A_n$

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) = P(A_1) + P(A_2) + \ldots + P(A_n)$$

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i)$$

(iii) $P(S) = 1$

Then $P(A_i)$ is called the probability measure on T or simply the probability of the event A_i.

The above are said to be three axioms of probability. From the first axiom we see that the probability of an event can not be negative and also can not exceed unity the second axiom states that the probability of union of mutually exclusive event is sum of the probabilities of the component events. The third axiom states that the totality of probability of a sample space. i.e. the probability of the whole sample space is unity.

Although the above axioms give us the restrictions upon the probability measure, they do not clearly state what could be the probability of an event, since in any experiment, the above conditions are satisfied by an infinite number of values of P(A). The probability of an event is determined by intuition, mathematical reasoning or past experience. In most of the cases we take ideal situations. Thus, in the roll of die, we regard the die to be perfectly cubical so that there is no reason to suspect that one face should ordinarily come more frequently upwards than any other. Since there are six possibilities and the total probability is 1, we take the probability of each face coming up as 1/6. Similarly, in the toss of a symmetrical coin, the probability of head turning up is 1/2. It may be cautioned that all events are not equally probable. Thus, if a fan is hung up in a ceiling and there are two possibilities, one the fan is remaining hanging up and the other falling down, the two events are not equally probable and we should be wrong in deducing that the probability of the falling down is 1/2.

The probability of an event is the sum of the probabilities of the sample points contained in the subset.

Remarks: (i). If the sample space s is the union of the distinct simple events E_1, E_2, ..., it follows from axions II and III that $P(S)=P(E_1)+P(E_2)+...=1$.

(ii). It is easy to conclude from axiom II that if E1 and E2 are mutually exclusive events, so that $E_1 \cap E_2 = \phi$, then $P(E_1 \cup E_2)=P(E_1)+P(E_2)$.

Limitations of mathematical definitions

In the mathematical definition of probability, the !term 'equally likely' is involved. Hence when the cases are not equally likely the probability, in general, according to mathematical definition can not be calculated.

For example: If a die is so based that it gives even numbers more often than odd numbers, then occurrence of numbers on the die is not at all equally likely.

The mathematical definition, therefore, does not serve our purpose when

(i) all the cases are not equally likely.

(ii) when total number of cases are infinite.

(iii) when probability is not a rational number.

(iv) when equally likely cases cannot be easily enumerated.

Difference between mathematical probability and statistical probability

The two definitions are apparently different. Mathematical probability is the relative frequency of favourablecases to the total number of cases while according to statistical definition probability is the limit of the relative frequency of happening of the event.

Theorems on simple probability and formulated results

Theorem 1: Probability of the impossible event is zero i.e. $P(\phi)=0$.

Proof: For any event A, we have $A\cup\phi=A$

$$P(A\cup\phi)=P(A)$$

Since A and ϕ are mutually exclusive it follows from Axioms

$$P(A)+P(\phi)=P(A) \text{ or } P(\phi)=0$$

i.e. the probability of the impossible event ϕ is zero.

Theorem 2: Probability of a sure event S is always unity. i.e. P(S) = 1.

Proof: Let S be the sample space

$$P(S)=\frac{n(S)}{n(S)}=1 \qquad \Rightarrow P(S)=1$$

Theorem 3: The probability of an event lies between 0 and 1.

Proof: Let S be the sample space and let

E be any event. Then by set theory $\phi\subseteq E\subseteq S$

$$\Rightarrow \quad n(\phi)\leq n(E)n(S) \qquad \Rightarrow \quad 0\leq\frac{n(E)}{n(S)}\leq\frac{n(S)}{n(S)}$$

$$\Rightarrow \quad 0\leq P(E)\leq 1$$

i.e. the probability of any event lies between 0 and 1.

Theorem 4: The sum of the probabilities of an event and its complementary event is unity i.e. $P(A)+P(\bar{A})=1$

Proof: Let A and $\bar{A}$ be disjoint events, then by set theory,

$$A\cup\bar{A}=S \qquad \therefore n(A\cup\bar{A})=n(S)$$

$$\Rightarrow \quad n(A)+n(\bar{A})=n(S) \qquad [\because n(A\cap\bar{A})=0]$$

$$\Rightarrow \quad \frac{n(A)}{n(S)}+\frac{n(\bar{A})}{n(S)}=1 \qquad \Rightarrow \quad P(A)+P(\bar{A})=1$$

Theorem 5: If two events A and B are such that if A occurs, B necessarily occurs i.e. if $A\subseteq B$, then $P(A)\leq P(B)$.

Proof:
$$\because \quad A\subseteq B$$
$$\therefore \quad B=A+(B-A)=A\cup(B-A)$$

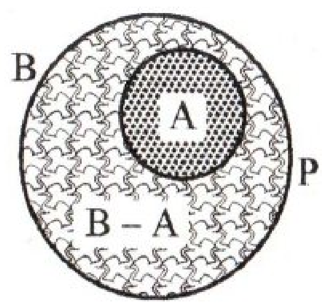


Fig. 1.15

A and B – A being mutually exclusive events so that

$$n(B)=n[A\cup(B-A)]=n(A)+n(B-A)$$

$$\Rightarrow \quad \frac{n(B)}{n(S)}=\frac{n(A)}{n(S)}+\frac{n(B-A)}{n(S)}\Rightarrow P(B)\geq P(A) \quad [\because 0\leq P(B-A)\leq 1]$$

Theorem 6: If A and B are two equivalent events then P(A) = P(B).

Proof: Let S be the sample space and let A and B two equivalent events. By definition of equivalent events, $A \subseteq B$ and $B \subseteq A$

$$\therefore \quad n(A) \leq n(B) \text{ and } n(B) \leq n(A)$$
$$\therefore \quad n(A) = n(B)$$
$$\text{or} \quad \frac{n(A)}{n(S)} = \frac{n(B)}{n(S)} \text{ or } P(A) = P(B)$$

Notations in set form:

We have $A \cup B =$ At least one of the events A and B occurs or occurrence of event either A or B or both. $= \{e \in S : e \in A \text{ or } e \in B\}$ i.e. $e \in A \cup B$.

$A \cup B =$ Both the events A and B occur.

$= \{e \in S : e \in A \text{ and } e \in B\}$ i.e. $e \in A \cap B$.

$\overline{A} =$ Complementary event of A. $= \{e \in S : e \notin A\}$ i.e. $e \in (S - A)$

$\overline{A} \cap \overline{B} =$ Neither A nor B occur. $= \{e \in S : e \notin A \text{ and } e \notin B\}$ i.e. $e \in \overline{A} \cap \overline{B}$.

$A \cap \overline{B} =$ A occurs but B does not $= \{e \in S : e \in A \text{ but } e \notin B\}$ i.e. $e \in A \cap \overline{B}$

$A - B = \{e \in S : e \in A \text{ but } e \notin B\} = e \in A \cap \overline{B}$. $A \subset B = \forall e \in A, e \in B$

i.e. if A occurs so does B.A and B are disjoint or mutually exclusive

$\Rightarrow \quad A \cap B = \phi$ where $A \cup B = A + B$ [here $A \Delta B = (A - B) \cup (B - A)$]

Not more than one of the events A or B occurs

$\Rightarrow \quad e \in \{(A \cap \overline{B}) \cup (\overline{A} \cap B) \cup (\overline{A} \cap \overline{B})\}$

Out of three events A, B, C only A occurs $\Rightarrow \quad e \in A \cap \overline{B} \cap \overline{C}$

A and B occur but C does not $\Rightarrow \quad e \in A \cap B \cap \overline{C}$.

A, B and C all three occur $\Rightarrow \quad e \in A \cap B \cap C$.

Out of A, B and C at least one occurs $\Rightarrow \quad e \in A \cup B \cup C$

$\Rightarrow \quad e \in 1-\left(\bar{A} \cap \bar{B} \cap \bar{C}\right)$ [If all three are independent]

Out of A, B and C at least two occur

$\Rightarrow \quad e \in \left(A \cap B \cap \bar{C}\right) \cup \left(A \cap \bar{B} \cap C\right) \cup \left(\bar{A} \cap B \cap C\right) \cup \left(A \cap B \cap C\right)$

Out of A, B and C only one occurs $\Rightarrow \quad e \in \left(A \cap \bar{B} \cap \bar{C}\right) \cup \left(\bar{A} \cap B \cap \bar{C}\right) \cup \left(\bar{A} \cap \bar{B} \cap C\right)$

Out of A, B and C only two occur $\Rightarrow \quad e \in \left(A \cap B \cap \bar{C}\right) \cup \left(A \cap \bar{B} \cap C\right) \cup \left(\bar{A} \cap B \cap C\right)$

None of A, B and C occurs $\Rightarrow \quad e \in \left(\overline{A \cap B \cap C}\right)$ i.e. $\bar{A} \cap \bar{B} \cap \bar{C}$

Fact and results:

(i) If E be any event and S be the sample space, then

$$P(E)=\frac{n(E)}{n(S)}=\frac{m}{n}=\frac{\text{Fav.no.of cases}}{\text{Total no.of cases}}$$

(ii) $P(\phi)=0, P(S)=1$

(iii) $0 \le P(E) \le 1$

(iv) $P(A)+P(\bar{A})=1 \qquad \Rightarrow P(A)=1-P(\bar{A})$

2.5 Addition law for counting:

If Any work A can be done in m ways and another work B can be done in n ways and C is a work which is done only when either A or B is done then number of ways of doing the work C = m + n.

2.6 Product law for counting :

If any work A can be done in m ways and another work B can be in n ways and C is a work which is done only when both A and B are done then number of ways of doing the work C = m × n.

Designation of cards:

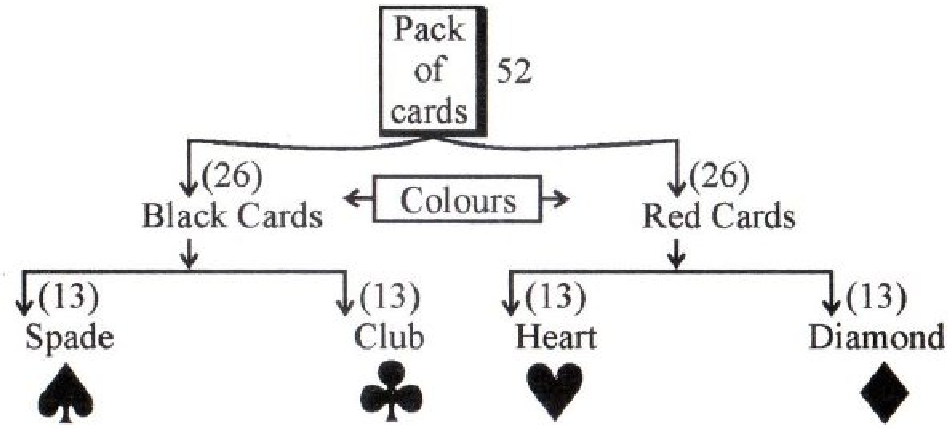


Fig. 1.16

- Colours: There are two colours.
- Suits: There are four (4) suits (types).
- Each suit contains 13 cards.

Recognition of cards:

	K King	Q Queen	J Jack	A Ace
♥	1	1	1	1
♦	1	1	1	1
♠	1	1	1	1
♣	1	1	1	1
	4	4	4	4

Fig. 1.17

(i) **Face cards:**

Face cards contain 12 cards all of K, Q and J having designed a figure of a person.i.e. Face cards = 4 + 4 + 4 = 12

(ii) **Honours Cards:**

It contains all face cards also a card marked A.

i.e. Honours cards = (4 + 4 + 4) + 4 = 16 cards.

(iii) **Knave Cards:** (10, J, Q) = 4 + 4 + 4 = 12 cards

Note: (A) For kanve cards, there has always been confusion to the students along with guides. Knave does not have a meaning like Jack. For Jack, it is always considered as a card of value J.

But for knave, it is considered as a slave card. Why the denomination (value) 10 is included in slave i.e. knave card? Answer is nation (value) 10 is included in slave i.e. knave card? Answer is because J is alphabetically in order 10. However J and Q are always considered by knave cards.

(B) What is the game 'Bridge'?

It is a game in which there are four players and each player gets thirteen cards to operate the game.The first person gets thirteen cards out of total fifty two (52) cards by ${}^{52}C_{13}$ ways. Similarly the 2nd, 3rd and 4th players get cards by ${}^{39}C_{13}$, ${}^{26}C_{13}$ and ${}^{13}C_{13}$ ways.

(C) In the support of cards if a person has to draw two cards of:

(a) The same colour (i) at once he can draw as the favourable cases by ${}^{26}C_2 \times 2$ ways (ii) one by one he can draw as the favourable cases by ${}^{26}C_1 \times {}^{25}C_1 \times 2$ or ${}^{52}C_1 \times {}^{25}C_1$ ways.

(b) Of the different colour (i) at once he can draw as the favourable cases by ${}^{26}C_1 \times {}^{26}C_1$ ways. (ii) one by one he can draw as favourable cases by ${}^{52}C_1 \times {}^{26}C_1$ or ${}^{26}C_1 \times {}^{26}C_1 \times 2$ ways.

Example : If three coins are tosed randomly, then represent the sample space and the event to turn up head and tail alternately.

Solution : Here, $S \rightarrow$ sample space

$S = \{(H, H, H), (H, H, T), (H, T, H), (T, H, H),(H, T, T), (T, H, T), (T, T, H), (T, T, T)\}$

Let, E be the event that head and tail turn up alternately.

$E = \{(H, T, H), (T, H, T)\}$

Example: There are 30 tickets numbered consecutively as 1, 2, 3, ...30. Represent the sample space and the event of drawing a ticket containing number which is the multiple of 2.

Solution : If S represents the results of drawing all possible tickets numbered then,

$S = \{1, 2, 3, 4, ...30\}$ and event to draw a number multiple of 2 will be

$E = \{2, 4, 6, ...30\}$.

Example : If three coins are tossed randomly then the probability of getting

(i) all three tails

(ii) at least one head

(iii) one head and two tails

(iv) exactly two tails

Solution : For a single coin, $S_1 = \{(H, T), n(S_1) = 2$

For two coins, $S_2 = \{(H, H), (H, T), (T, H), (T, T)\}, n(S_2)=2^2=4$

For three coins, $S= \{H, T\} \times \{(H, T), (H,T), (T,H) (T,T)\}$

$=\{(H, H, H), (H, H, T), (H, T, H), (T, H, H),(H, T, T), (T, H, T)\}(T, T, H), (T, T, T)\},$

$\therefore \quad n(S)=2^3=8$

(i) Let E_1 = Event of getting all three tail {(T, T, T), $n(E_1)$ =1

$$\therefore \quad P(E_1) = \frac{n(E_1)}{n(S)} = \frac{\text{Fav. case}}{\text{Total case}} = \frac{1}{8}$$

(ii) Let E_2 = Event of getting at least one head.

E_2 = {(H, H, H), (H, H, T), (H, T, H), (T, H, H), (H, T, T), (T, H, T), (T, T, H)}

$n(E_2)$=7

$$\therefore \quad P(E_1) = \frac{n(E_2)}{n(S)} = \frac{7}{8}.$$

(iii) Let E_3 = Event of getting one head and two tails.

E_3 = {(H, T, T), (T, H, T), (T, T, H)}, $n(E_3)$ = 3

$$\therefore \quad P(E_3) = \frac{n(E_3)}{n(S)} = \frac{3}{8}.$$

(iv) Let E_4 = Event of getting exactly two tails.

E_4 = {(H, T, T), (T, H, T), (T, T, H)}.$n(E_4)$ = 3

$$\therefore \quad P(E_4) = \frac{n(E_4)}{n(S)} = \frac{3}{8}$$

Example: If two dice are thrown at a time. Find the probability of the following events:

(i) numbers shown are equal.

(ii) the sum of numbers shown is 6.

(iii) the difference of the numbers shown is 2.

(iv) the sum of numbers shown is $\geq$ 10.

(i) Let E_1 = Event that numbers shown are equal.

E_1 = {(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)}, $n(E_1)$ = 6

$$\therefore \quad P(E_1) = \frac{n(E_1)}{n(S)} = \frac{6}{36} = \frac{1}{6}$$

(ii) Let E_2 = Event that sum of numbers shown is 6.

$E_2 = \{(1, 5), (2, 4), (3, 3), (4, 2), (5, 1)\}$, $n(E_2) = 5$

$$\therefore \quad P(E_2) = \frac{n(E_2)}{n(S)} = \frac{5}{36}$$

(iii) Let E_3 = Event that differences of the numbers shown is 2.

$E_3 = \{(1, 3), (2, 4), (3, 5), (4, 6), (3, 1), (4, 2), (5, 3), (6, 4)\}$, $n(E_3) = 8$

$$\therefore \quad P(E_3) = \frac{n(E_3)}{n(S)} = \frac{8}{36} = \frac{2}{9}$$

(iv) Let E_5 = Event that sum of numbers shown is ≥ 10.

$E_5 = \{(4, 6), (5, 5), (5, 6), (6, 4), (6, 5), (6, 6)\}$, $n(E_5) = 6$

$$\therefore \quad P(E_5) = \frac{n(E_5)}{n(S)} = \frac{6}{36} = \frac{1}{6}$$

Example : If three fair and unbaised dice are rolled on the ludo board at once. Find the probability that

(i) numbers shown are equal.

(ii) numbers shown are (totally) different.

(iii) sum of numbers is 10.

(iv) sum of numbers is 15.

Solution : Here, $n(S) = 6^3 = 216$

(i) E_1 = Event to show equal number on each.

$E_1 = \{(1, 1, 1), (2, 2, 2), (3, 3, 3), (4, 4, 4), (5, 5, 5), (6, 6, 6)\}$, $n(E_1) = 6$

$$\therefore \quad P(E_1) = \frac{n(E_1)}{n(S)} = \frac{6}{216} = \frac{1}{36}$$

(ii) E_2 = Event to show different number on each.

$n(E_2) = {}^6P_3$ = To arrange any three different face out of six faces.

$$\therefore \quad P(E_2) = \frac{n(E_2)}{n(S)} = \frac{{}^6P_3}{216} = \frac{5}{9}$$

(iii) E_3 = Event to have sum of all three dice appeared as 10.

$$\left.\begin{array}{lll} E_3 \to (1,3,6) & \to & \underline{|3} = 6 \\ \quad\;\; (1,4,5) & \to & \underline{|3} = 6 \\ \quad\;\; (2,2,6) & \to & \underline{|3}/2 = 6 \\ \quad\;\; (2,3,5) & \to & \underline{|3} = 6 \\ \quad\;\; (2,4,4) & \to & \underline{|3}/2 = 3 \\ \quad\;\; (3,3,4) & \to & \underline{|3}/2 = 3 \end{array}\right\} n(E_3) = 27$$

$$P(E_3) = \frac{n(E_3)}{n(S)} = \frac{27}{216}$$

Example : If one card is drawn from the pack of 52 cards at random. What is the probability that it is(i) Red, (ii) Black, (iii) Heart, (iv) Red or Black, (v) Heart or spade, (vi) King or Queen, (vii) Queen or Jack or King, (viii) Queen of Heart.

Solution : Here, $n(S) = {}^{52}C_1$ (we have to select one card out of 52 cards)

(i) Required probability (for red card)

$$= \frac{\text{Fav.no.of cases}}{\text{Total no.of cases}} = \frac{{}^{26}C_1}{{}^{52}C_1} = \frac{1}{2}$$

(ii) Required probability (for black card)

$$= \frac{\text{Fav.no.of cases}}{\text{Total no.of cases}} = \frac{{}^{26}C_1}{{}^{52}C_1} = \frac{1}{2}$$

(iii) Required probability

$$= \frac{\text{Fav.no.of cases}}{\text{Total no.of cases}} = \frac{{}^{13}C_1}{{}^{52}C_1} = \frac{13}{52} = \frac{1}{4}$$

(iv) Required probability

$$=\frac{\text{Fav.no.of cases}}{\text{Total no.of cases}}=\frac{{}^{13}C_1+{}^{26}C_1}{{}^{52}C_1}=\frac{52}{52}=1$$

(v) Required probability

$$=\frac{\text{Fav.no.of cases}}{\text{Total no.of cases}}=\frac{{}^{13}C_1+{}^{13}C_1}{{}^{52}C_1}=\frac{26}{52}=\frac{1}{2}$$

(vi) Required probability

$$=\frac{\text{Fav.no.of cases}}{\text{Total no.of cases}}=\frac{{}^{4}C_1+{}^{4}C_1}{{}^{52}C_1}=\frac{8}{52}=\frac{2}{13}$$

(vii) Required probability

$$=\frac{\text{Fav.no.of cases}}{\text{Total no.of cases}}=\frac{{}^{4}C_1+{}^{4}C_1+{}^{4}C_1}{{}^{52}C_1}=\frac{12}{52}=\frac{3}{13}$$

(viii) Required probability

$$=\frac{\text{Fav.no.of cases}}{\text{Total no.of cases}}=\frac{1}{52}$$

Example : If three cards are drawn from a well shuffled pack of 52 cards randomly. What is the probability that it has

(i) all three Kings?

(ii) no King at all?

(iii) exactly one King?

(iv) oneKing and two Queens?

(v) one King, one Queen and one Jack?

(vi) all three of same colours?

(vii) all three of different honours?

(viii) all three of different honours?

(ix) all three of different suits?

(x) all three of same face?

(xi) all three of same honours?

(xii) all three of same suit?

(xiii) all three of same denomination?

(xiv) all three of different denominations?

(xv) at least one King?

Solution: Since, three cards can be drawn out of 52 cards = $^{52}C_3 = 22100$,

$n(S) = 22100$

(i) All three King cards can be drawn out of four Kings by $^4C_3$ ways.

Required probability $= \frac{^4C_3}{22100} = \frac{4}{22100} = 0.0002$

(ii) Three non-King cards can be dawn out of 48 non-King cards by $^{48}C_3$ ways.

Required probability $= \frac{^{48}C_3}{52C3} = \frac{4324}{5525} = 0.782$

(iii) For exactly one King card; we can draw a King card out of 4 King cards and other two non-King cards out of 48 cards by $^4C_1 \times {}^{48}C_2$ ways. Required probability $= \frac{^4C_1 \times {}^{48}C_2}{^{52}C_3} = \frac{1125}{5525} = 0.203$

(iv) One King card can be drawn out of 4 Kings by $^4C_1$ ways and two Queen cards can be drawn out of 4 Queen cards by $^4C_2$ ways.

Required probability $= \frac{^4C_1 \times {}^4C_2}{^{52}C_3} = \frac{6}{5525} = 0.001$

(v) Number of ways of drawing a King, a Queen and a Jack

$= {}^4C_1 \times {}^4C_1 \times {}^4C_1$. Required probability $= \frac{^4C_1 \times {}^4C_1 \times {}^4C_1}{^{52}C_3} = \frac{16}{5525} = 0.00028$

(vi) All three cards of same colour can be drawn by ${}^{26}C_3 \times 2$

$$\text{Required probability} = \frac{{}^{2}C_1 \times {}^{26}C_3}{{}^{52}C_3}$$

(vii) All three cards of different faces i.e. one King, one Queen and on Jack card can be drawn by ${}^{4}C_1 \times {}^{4}C_1 \times {}^{4}C_1$ ways.

$$\text{Required probability} = \frac{{}^{4}C_1 \times {}^{4}C_1 \times {}^{4}C_1}{{}^{52}C_3}$$

(viii) Taking all three cards of different honours by ${}^{4}C_3 \times {}^{4}C_1 \times {}^{4}C_1 \times {}^{4}C_1$ ways.

$$\text{Required probability} = \frac{\text{Fav. no. of cases}}{\text{Total no. of cases}} = \frac{{}^{4}C_3 \times {}^{4}C_1 \times {}^{4}C_1 \times {}^{4}C_1}{{}^{52}C_3}$$

(ix) Taking all three cards of different suits by ${}^{4}C_3 \times {}^{13}C_1 \times {}^{13}C_1 \times {}^{13}C_1$ ways.

$$\text{Required probability} = \frac{\text{Fav. no. of cases}}{\text{Total no. of cases}} = \frac{{}^{4}C_3 \times {}^{13}C_1 \times {}^{13}C_1 \times {}^{13}C_1}{{}^{52}C_3}$$

(x) Taking all three cards of the same face by ${}^{3}C_1 \times {}^{4}C_3$ ways.

$$\text{Required probability} = \frac{\text{Fav. no. of cases}}{\text{Total no. of cases}} = \frac{{}^{3}C_1 \times {}^{4}C_3}{{}^{52}C_3}$$

(xi) Taking all three cards of same honours by ${}^{4}C_1 \times {}^{4}C_3$ ways.

$$\text{Required probability} = \frac{\text{Fav. no. of cases}}{\text{Total no. of cases}} = \frac{{}^{4}C_1 \times {}^{4}C_3}{{}^{52}C_3}$$

(xii) Taking all three cards of same suit by ${}^{4}C_1 \times {}^{13}C_3$ ways.

$$\text{Required probability} = \frac{\text{Fav. no. of cases}}{\text{Total no. of cases}} = \frac{{}^{4}C_1 \times {}^{13}C_3}{{}^{52}C_3}$$

(xiii) Taking all three cards of same denomination by ${}^{13}C_1 \times {}^{4}C_3$ ways.

$$\text{Required probability} = \frac{\text{Fav. no. of cases}}{\text{Total no. of cases}} = \frac{{}^{13}C_1 \times {}^{4}C_3}{{}^{52}C_3}$$

(xiv) Taking all three cards of different denomination by $^{13}C_3 \times {}^4C_1 \times {}^4C_1 \times {}^4C_1$ ways.

Required probability $= \dfrac{\text{Fav.no.of cases}}{\text{Total no.of cases}} = \dfrac{^{13}C_3 \times {}^4C_1 \times {}^4C_1 \times {}^4C_1}{^{52}C_3}$

(xv) Required probability $= \dfrac{\text{Fav.no.of cases}}{\text{Total no.of cases}}$

$$= \frac{^4C_1 \times {}^{48}C_2 \times {}^4C_2 \times {}^{48}C_1 + {}^4C_3 \times {}^{48}C_0}{^{52}C_3}$$

Example : If five cards are drawn randomly from a pack of 52 cards. What is the chance that these five cards will contain

(i) Just one ace?
(ii) At least one ace?

Solution : Total no. of ways to draw 5 cards out of 52 cards = $^{52}C_5$ = 2598960.

(i) Here, we have to draw 5 cards among these just one ace out of 4 aces and 4 other cards out of remaining 48 cards by $^4C_1 \times {}^{48}C_4$ ways.

Required probability $= \dfrac{\text{Fav.no.of cases}}{\text{Total no.of cases}}$

$= \dfrac{^4C_1 \times {}^{48}C_4}{^{52}C_5} = \dfrac{778320}{2598960} = 0.2995$

(ii) No. of ways in which no ace card is drawn = $^{48}C_5$ = 1712304

Probability of drawing no ace $= \dfrac{\text{Fav.no.of cases}}{\text{Total no. of cases}}$

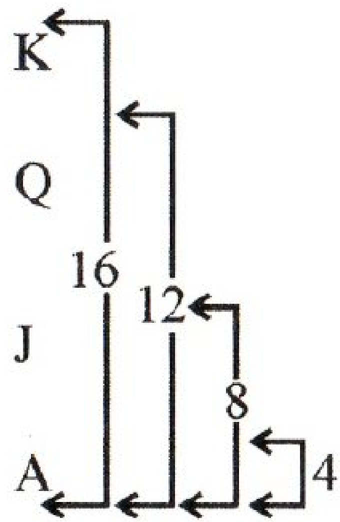
$= \dfrac{1712304}{2598960} = 0.6588$ Required probability = 1 – 0.6588 = 0.3412

Example : If four cards are drawn one by one without replacement method. What is the probability that these are

(i) all aces?

$$= \frac{^{52}C_1}{^{52}C_1} \cdot \frac{^{39}C_1}{^{51}C_1} \cdot \frac{^{26}C_1}{^{50}C_1} \cdot \frac{^{13}C_1}{^{49}C_1} = \frac{2197}{20825} = 0.1054$$

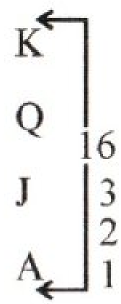
(iv)



Required probability $= \frac{n(E)}{n(S)} = \frac{^{16}C_1 \times {}^{12}C_1 \times {}^{8}C_1 \times {}^{4}C_1}{^{52}C_1 \times {}^{51}C_1 \times {}^{50}C_1 \times {}^{49}C_1}$

$= \frac{768}{812175} = 0.00095$

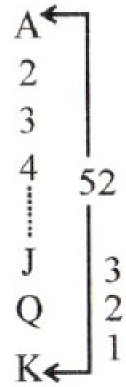
(v) Since, 1st honours card can be drawn by any of 16 cards by $^{16}C_1$ ways, then the rest of three cards can be drawn out of remaining same honours of three cards by $^{3}C_1 \times {}^{2}C_1 \times {}^{1}C_1$ ways.



Required probability $= \frac{n(E)}{n(S)} = \frac{^{16}C_1 \times {}^{3}C_1 \times {}^{2}C_1 \times {}^{1}C_1}{^{52}C_1 \times {}^{51}C_1 \times {}^{50}C_1 \times {}^{49}C_1}$

$= \frac{96}{6497400} = 0.000015$

(vi) Since, 1^{st} card can be drawn out of any of 52 cards by $^{52}C_1$ ways, then the rest of three cards of the same denomination can be drawn by $^{3}C_1 \times {}^{2}C_1 \times {}^{1}C_1$ ways.

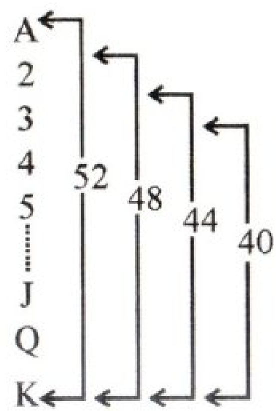


Required probability $= \frac{n(E)}{n(S)}$

$$= \frac{^{52}C_1 \times {}^{3}C_1 \times {}^{2}C_1 \times {}^{1}C_1}{^{52}C_1 \times {}^{51}C_1 \times {}^{50}C_1 \times {}^{49}C_1} = \frac{312}{6497400} = 0.000048$$

(vii) By graph, we see

$$n(E) = {}^{52}C_1 \times {}^{48}C_1 \times {}^{44}C_1 \times {}^{40}C_1$$



Required probability $= \frac{n(E)}{n(S)} = \frac{^{52}C_1 \times {}^{48}C_1 \times {}^{44}C_1 \times {}^{40}C_1}{^{52}C_1 \times {}^{51}C_1 \times {}^{50}C_1 \times {}^{49}C_1}$

$$= \frac{4392960}{6497400} = 0.6761$$

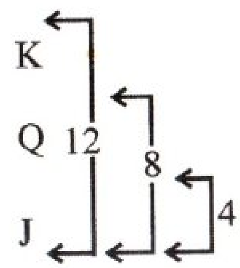
Example: Find the chance of drawing an ace, a king, a queen and a jack in order an ordinary pack in four consecutive draws

After dropping two cards there remain 50 cards of which 26 are of suit, different from those of dropped ones, so the chance of dropping a card of different suit in third missing $= \frac{^{26}C_1}{^{50}C_1} = \frac{26}{50} = \frac{13}{25}$.

Here, events being dependent,

Require probability $= 1 \times \frac{13}{17} \times \frac{13}{25} = \frac{169}{425} = 0.3976$

(ii) By similar fashion, the three missing cards are one by one in condition of dependent.



Hence, required probability

$$= \frac{12}{52} \times \frac{8}{51} \times \frac{4}{50} = \frac{384}{132600} = 0.00289$$

(iii) Required probability (same face) $= \frac{^{12}C_1}{^{52}C_1} \times \frac{^{3}C_1}{^{51}C_1} \times \frac{^{2}C_1}{^{50}C_1}$.

OR, Required probability $= \frac{^{4}C_1}{^{52}C_1} \times \frac{^{3}C_1}{^{51}C_1} \times \frac{^{2}C_1}{^{50}C_1} \times 3$

(iv) Required probability that missing cards are of the same suit

$$= \frac{^{13}C_1}{^{52}C_1} \times \frac{^{12}C_1}{^{51}C_1} \times \frac{^{11}C_1}{^{50}C_1} \times 4 = \frac{6864}{132600} = 0.0517$$

Or, Required probability $= \frac{^{52}C_1}{^{52}C_1} \times \frac{^{12}C_1}{^{51}C_1} \times \frac{^{11}C_1}{^{50}C_1} = \frac{6864}{132600} = 0.0517$.

Example: From a pack of cards two cards are drawn, the first being replaced before the second is drawn. Find the probability that the first is a diamond and the second is a king.

Solution : Let A denote the event of drawing a diamond and B that of drawing a king in the second draw, when the first drawn card has been replaced. Hence, there being 13 diamond cards and 4 king cards out of 52 cards, we have

$$P(A) = \text{Probability of drawing a diamond} = \frac{^{13}C_1}{^{52}C_1} = \frac{1}{4}$$

$$P(B) = \text{Probability of drawing a king} = \frac{^{4}C_1}{^{52}C_1} = \frac{4}{52} = \frac{1}{13}.$$

$$\text{Required probability} = P(A).P(B) = \frac{1}{4}\cdot\frac{1}{13} = \frac{1}{52} = 0.019$$

Example : If all face cards are removed from a well defined full pack. If 4 cards are drawn at random from remaining 40 cards. Find the probability that these belong to

(a) different suits

(b) different suits and different denominations

Solution : After removal of 12 face cards, the remaining 40 cards consist of 10 cards of each suit.

(a) The chance of drawing a card in the first draw $= \frac{^{40}C_1}{^{40}C_1} = 1.$

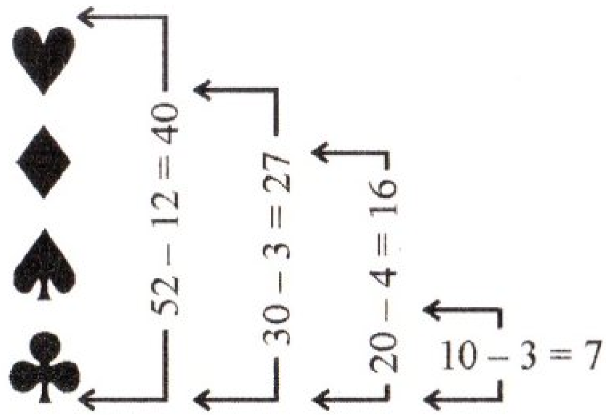
Having drawn a card, there remain 39 cards of which 30 are of different suits from that of drawn one. Therefore the chance of drawing a card of different suit in second draw $= \frac{^{30}C_1}{^{30}C_1} = \frac{10}{19}.$

Having drawn 3 cards, there remain 37 cards of which 10 are of suits, different from that drawn ones.So the chance of drawing a card of different suit in fourth draw $= \frac{^{10}C_1}{^{37}C_1} = \frac{10}{37}$

.All the events being dependent.

Required probability $=1\times\frac{10}{13}\times\frac{10}{19}\times\frac{10}{37}=\frac{1000}{9139}$

(b) The chance of drawing a card in the first draw $=\frac{{}^{40}C_1}{{}^{40}C_1}=1$.



Having drawn a card, there remain 39 cards of which 9 are of same suit and 3 are of the same denomination. So that 27 cards out of 39, are such as these are of different colours and different denominations from that of the drawn one.

$\therefore$ The chance of drawing a card in second draw $=\frac{{}^{27}C_1}{{}^{39}C_1}=\frac{27}{39}=\frac{9}{13}$.

Similarly, chance of drawing a card in 3rd draw $=\frac{{}^{16}C_1}{{}^{38}C_1}=\frac{16}{38}=\frac{8}{19}$.

And the chance of drawing a card in 4th draw $=\frac{{}^{7}C_1}{{}^{37}C_1}=\frac{7}{37}$.

All event, being mutually dependent,

Required probability $=1\times\frac{9}{13}\times\frac{8}{19}\times\frac{7}{37}=\frac{504}{9139}=0.055$.

Example: In a hand of bridge, what is the chance that all four queens out of 13 cards are held by a particular players?

Solution: Since a particular player will have 1 cards out of 52 cards by $^{52}C_{13}$ ways, he will have 4 queens and 9 other cards by $^{4}C_{4} \times {}^{48}C_{9}$ ways.

$$\text{Required probability} = \frac{^{4}C_{4} \times {}^{48}C_{9}}{^{52}C_{1}} = 0.0026.$$

Example: What is the probability of getting 9 cards of the same suit in one hand in a game of bridge?

Solution: The particular player can get 9 cards out of thirteen of one suit in $^{13}C_{9}$ways and 4 cards of some other suit in $^{39}C_{4}$ ways. Since, there are four suits in a set of cards, the number of ways in which he can get nine cards of the same suit = $^{13}C_{9} \times {}^{39}C_{4} \times 4$.

Also, the number of ways in which 13 cards can be given to the player = $^{52}C_{13}$.

$$\text{Required probability} = \frac{^{13}C_{9} \times {}^{39}C_{4} \times 4}{^{52}C_{13}}.$$

Example: In a deal for "bridge" the player A has to receive two aces. Find the probability for each of the possible number of aces that may have been dealt to his partner.

Solution: Since, A has to receive all his thirteen cards, his partner can have 13 cards out of 39 cards.

In case, his partner does not have any ace, the partner can have 13 cards out of 37 only. Since he can not have any card out of A's and rest two aces.

Hence, the probability that A's partner does not have any ace. $= \frac{^{37}C_{13}}{^{39}C_{13}} = \frac{28}{57}$.

Then probability that A's partner has one ace $= \frac{^{37}C_{12} \times {}^{2}C_{1}}{^{39}C_{13}} = \frac{26}{57}$.

Since, he can have one ace out of the remaining two and twelve cards out of the remaining 37.Similarly, the probability that the partner has two aces.

$$=\frac{^{37}C_{11}\times{}^{2}C_{2}}{^{39}C_{13}}=\frac{2}{19}$$

Note: (i) When two dice are thrown, the number of ways of getting total 'r' is

(b) $r-1$, if $2\le r\le 7$;

(c) $13-r$, if $8\le r\le 12$

(ii) When three dice are thrown, the number of ways of getting total 'r' is

(a) $\frac{(r-1)(r-2)}{2}$, if $3\le r\le 8$

(b) $\frac{(19-r)(20-r)}{2}$, if $13\le r\le 18$

(c) 25, if $r=9$ or 12

(d) 27, if $r=10$ or 11

(iii) Out of n pairs of shoes, if k shoes are selected at random the probability that there is no pair is $p=\frac{^{n}C_{k}-2k}{^{2n}C_{k}}$ and the probability that there is at least one pair is $1-p$.

(iv) If 'r' squares are selected at random from a chees board, the probability that they lie on a diagonal is $\frac{4\left(^{7}C_{r}+{}^{6}C_{r}+...{}^{r}C_{r}\right)+2\left(^{8}C_{r}\right)}{^{64}C_{r}}$, $1\le r\le 7$.

(v) If there are n letters and n addressed envelopes

(a) Probability of keeping n letters in all wrong envelopes

$$p=\frac{1}{2!}-\frac{1}{3!}+...+\frac{(-1)^{n}}{n!}$$

(b) Probability of at least one in right envelope = $1-p$

(c) Probability of all in right envelope $=\frac{1}{n!}$.

(d) Probability of at least one in wrong envelope $= 1 - \frac{1}{n!}$.

Check your progress

1. If two dice are thrown simultaneously. Represent the sample space and the following events.
   (i) numbers shown are equal.
   (ii) sum of numbers turned up is 10.
   (iii) sum of numbers appeared up is greater than 10.
   (iv) number appeared on 1st dice is even no.
   (v) number appeared on 1st die is multiple of 2 and on second is multiple of 3.
2. A bag containing 20 tickets numbered consecutively. If a tickets is drawn at random. Represent the sample space and the event that the ticket drawn has a prime number.
3. There are 3 red 5 black balls in an urn. If one ball is taken out at random from this urn, then represent, the sample space and the event of this ball being black.
4. If two coins are tossed randomly, what is the chance that the turnings are
   (i) both head?
   (ii) at least one head?
   (iii) one head and one tail?
   (iv) at most one head?
   (v) no head at all?
5. If three coins are tossed simultaneously, find the probability of getting
   (i) all three heads.
   (ii) one head and two tail.
   (iii) head and tail alternately.

(iv) at least one head.

(v) at least two heads.

(vi) exactly two heads.

(vii) at most two heads.

(viii) no heat at all.

6. If five coins are tossed randomly, find the chance that there are exactly four heads.

7. If n coins are tossed randomly, find the chance that head will turn up odd number of times.

8. If two dice are thrown simultaneously, then find the chance of getting

   (i) numbers shown are equal.

   (ii) numbers shown are different.

   (iii) sum of the numbers appeared is 7.

   (iv) total score is a prime.

   (v) sum is 10.

   (vi) sum is 5.

   (vii) sum of the numbers appeared is less than 6.

   (viii) sum of the numbers shown is ≥ 7.

   (ix) sum of the numbers shown is ≥ 10.

   (x) sum of the numbers shown at the bottom of the dice is 7.

9. A pair of fair dice are thrown simultaneously. Find the probability that

   (i) no appeared on first is > 3.

   (ii) no appeared on second is < 4.

   (iii) difference of the number shown is one.

   (iv) difference of the numbers shown is 2.

   (v) sum is neither 7 nor 11.

   (vi) first is a multiple of 2 and the other is a multiple of 3.

(vii) one is multiple of 2 and the other is multiple of 3.

(viii) sum of the numbers at the bottom of the dice is 7.

10. What is the probability of getting eight points with 2 dice in a single throw?

11. If three dice are rolled randomly. Find the probability that the number appeared on the dice are

    (i) equal no. on each.

    (ii) different number on each.

    (iii) sum is 10.

    (iv) sum is 15.

    (v) sum is 12.

12. If three pairs of fair dice are rolled randomly, find the probability that numbers appeared on the dice are as

    (i) equal number on each.

    (ii) different number in each.

    (iii) sum is 15.

    (iv) sum is 24.

13. If three identical dice are rolled, find the chance that the same number will appear on each of them.

14. If two pairs of fair dice are casted, find the chance that

    (i) different numbers appears on the dice.

    (ii) sum of the numbers shown is 18.

    (iii) sum of the numbers shown is 20.

    (iv) sum of the numbers shown is 15.

15. A card is drawn at random from a pack of cards. Find the probability of getting.

    (i) a king

    (ii) no king

    (iii) a spade

(iv) a black

(v) king or queen

(vi) heart or spade

(vii) king or queen or jack

(viii) a two of heart

(ix) a queen of spade

(x) either a queen of heart of king of spade.

16. From a well shuffled pack of 52 card, two cards are drawn at random. Find the chance that.

(i) both are aces.

(ii) both are queens.

(iii) both are red.

(iv) both are spade.

(v) one is a king and the other is a queen.

(vi) one is a spade and the other is a heart.

(vii) both of different colour.

(viii) at least one black.

(ix) at least one king.

(x) exactly a king.

(xi) one is an ace and the other is honours.

(xii) one is red and the other one is spade.

(xiii) none of the faces is drawn.

(xiv) neither knave nor honours cards are selected.

17. During shuffling of the pack of cards if two are misplaced, find the chance that in the misplaced cards there will be.

(i) at least one jack but no club.

(ii) queen must not be misplaced.

(iii) at least one is ace of heart.

18. From a well shuffled pack of 52 cards, two cards are drawn one by one, the first being replaced before the second is drawn, find the probability that

    (i) The first is a diamond and the other is a king.

    (ii) at least one jack is drawn, but no club.

    (iii) at least one knave is drawn, but no spade.

19. If two cards are drawn one after another from a pack of 52 ordinary cards, find the chance that the first card is an ace and the second is an honours card. The first card is not replaced while drawing the second.

20. If three cards are drawn from a well shuffled ordinary pack, find the probability that cards drawn are

    (i) all three kings.

    (ii) all of different faces.

    (iii) all of the same face.

    (iv) of the same value.

    (v) of the same honours.

    (vi) of different honours.

    (vii) of different knave.

    (viii) exactly two kings.

    (ix) 2 kings and 1 jack.

    (x) atelast one king.

    (xi) at most two queens.

    (xii) one is red and two are kings.

21. If four cards are drawn from a pack of 52 cards randomly, find the probability that cards drawn are

    (i) all four queens or kings.

    (ii) all of the same denomination.

(iii) all of different denominations.

(iv) of different suits.

(v) of the same suit.

(vi) of the same honours.

(vii) of different honours.

(viii) at least two kings.

(ix) at most two jacks.

(x) two are of red colour and two are kings.

(xi) one is an honours and the other three are queens.

(xii) one is an honours and the other three of different faces.

22. If four cards are drawn at random from the full pack. Find the chance that these will be

(i) fourhonours of the same suit.

(ii) fourhonours of different suits.

23. Two cards are drawn simultaneously from the same set. Find the probability that at least one of them will be the ace of hearts.

24. One card is drawn from each one of the two ordinary sets of 52 cards. Find the probability that at least one of them will be the ace of hearts.

25. Find the probability of drawing either the ace of spade or ace of hearts from a pack of cards in a single draw.

26. If 7 cards are drawn at random from a pack of well shuffled 52 cards, what is the chance that 3 will be red and 4 black?

27. A card manufacturer has supplied an incomplete pack of 50 cards. If two cards are drawn at random. What is the chance that they will be diamond?

28. In shuffling a pack of playing cards, four are accidently dropped. Find the chance that the missing cards should be one from each suit.

29. A deck of cards contains 4 kings, 4 aces, 4 queens and 4 jacks. Two cards are drawn at random. Find the probability that one of these is an ace.

30. From a well shuffled pack of cards, 2 cards are drawn at random and kept aside, then one card is drawn from the remaining 50 cards. Find the chance that, it is an ace.

31. From a pack of 52 cards, two cards are drawn one after another without replacement. Find the probability that
    (i) the first is a king and the other is a queen.
    (ii) one is a king and the other is honours card.

32. Find the chance of drawing an ace, a king, a queen and a jack in order from an ordinary pack in four consecutive draws, the card drawn being
    (i) not replaced.
    (ii) replaced.

33. Two cards drawn one after the other without replacement method. What is the chance that they will be of different colours and different denominations.

34. A person draws a card from a pack of playing cards, replaces it and shuffles the pack. He continues this until he draws a spade. Find the chance that he will be successful in the third attempt.

35. Two cards are drawn successfully and successively with replacement from a well shuffled deck of 52 cards. Find the probability of drawing two aces.

36. If 4 cards are drawn one by one without replacement, find the probability that cards drawn are
    (i) all aces.
    (ii) of the same value.
    (iii) of the same suit.
    (iv) of the same honours.
    (v) of the same faces.
    (vi) of different denominations.
    (vii) of different suits.
    (viii) of different honours.

(ix) allhonours of the same suit.

(x) allhonours of different suits.

37. (A) If two cards are drawn from a pack of 52 cards one after another without replacement, find the chance that one of these is an ace and the other is a queen of opposite shade.

(B) A deck of 36 cards is divided at random into two equal parts. What is the probability that both parts will have an equal number of red and black cards?

38. In a hand at whist, what is the probability that the four king are held by a specified player?

39. In a game of bridge, 4 players are distributed one card each by turn so that each player gets 13 cards. Find the chance of a player getting a black ace and a king.

40. What is the probability of getting 9 cards of the same suit in one hand in a game of bridge?

41. What is the chance that at least one of the players in a game of bridge will get a complete suit of cards?

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.
(2) P.T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.
(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.
(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.
(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

UNIT - 3

General Counting Methods

Structure

3.1 Introduction

This is most basic and useful unit of this block as it introduces the concept of sum rulefor counting the numbers,the concept of product rule for counting the numbers, elementary operations and associated logical connectives. We introduce the Pigeonhole Principleand its applications in counting.

3.2 Objectives

After reading this unit we should be able to

1. Understand the concept of statement of sum rule and statement of product rulefor counting
2. Understand the statement ofPigeonhole Principleand its applications in counting.

Logic is a field of study that deals with the method of reasoning Logic provides rules by which we can determine whether a given argument or reasoning is valid (correct) or not. Logical reasoning is used in Mathematics to prove theorems. In computer science logic is used to verify the correctness of programs. Combinatorics is a branch of mathematics that deals with counting. In this chapter, we shall study some topic which various combination of objects can arise. The sum rule and the product rule give us the method for counting. Pigeonhole Principle states that if there are more pigeons (objects) than the pigeon holes (boxes), then some pigeonhole (box) must contain two or more pigeons (objects). It is more useful in counting.

3.3 Sum and Product Rules

We begin by stating two basic principles for counting the number of ways events can happen.

Sum Rule : If one job can be done in m ways and another job cab be done in n ways and if there is no way common to both jobs then the total number of ways in which either of the two jobs can be done is equal to m+n.

In set-theoretic notatins, sum rule states that if A and B are two finite sets such that $A \cap B = \phi$ then $|A \cup B| = |A| + |B|$

Where |X| denotes then number of elements in X.

Product Rule : If one job can be done in m ways and following this another ob can be done in n ways then the total number of ways in which both the jobs can be done in the stated order is $m \times n$.In set-theoretic notations, product rule says that

$|A \times B| = |A| \times |B|$,where A and B are finite sets.

Example : Suppose an institute offers seven different courses in the morning shift and six different courses in the evening shift.

(a) How many ways are there for students who want admission in one course only?

(b) How many ways are there for students who want admission in one course in the morning shift and one in the evening shift?

Solution

(a) By sum rule, students will have $8+6 = 13$ choices if they want admission in only one course.

(b) By product rule there will be 7Ø6=42 choices for students who want to take admission in one course in the morning shift and one in the evening shift.

Example : There are five different Hindi books, six different English books and eight different Sanskrit books. How many ways are there to pick two books not both in the same language?

Solution : There are three cases:

(i) 1 Hindi and 1 English book

(ii) 1 Hindi and 1 Sanskrit book

(iii) 1 English and 1 Sanskrit book

Since there are five Hindi books and six English books, we can select one Hindi and one English book in 5×6 ways. Similarly, one Hindi and one Sanskrit books can be chosen in $5\times8=40$ ways and one English and one Sanskrit book can be chosen in $6\times8=48$ ways. Since the above three types of selections are disjoint, therefore by sum rule, there are $30+40+48=118$ ways in all.

Example : If A and B are finite sets then

1. $|A - B| = |A| - |A \cap B|$
2. $|A - B| = |A| - |B|$ if $B \subset A$

Solution :

1. We know from set theory that

$$(A - B) \cup (A \cap B') = (A \cap B') \cup (A \cup B)$$

$$= A \cap (B \cup B') = A$$

and $(A - B) \cap (A \cap B) = (A \cap B') \cap (A' B) = A \cap B \cap B' = \phi$

Therefore, by sum rule, $|A| = |(A - B) \cup (A \cap B)| = |A - B| + |A \cap B|$

$\Rightarrow \quad |A - B| = |A| - |A \cap B|$

2. It follows from (1) because $B \subset A$ implies $A \cap B = B$. Substituting $A \cap B = B$ in (1), we get $|a - B| = |A| - |B|$.

3.4 The Pigeonhole Principle

It states that if there are more pigeons (objects) than the pigeon holes (boxes), then some pigeonhole (box) must contain two or more pigeons (objects).

In set-theoretic terms, pigeonhole principle is equivalent to the following:

Let A and B be finite sets. Of $|A| > |B|$ then any function $f : A \rightarrow B$ cannot be one-to-one. That is, there exists at least 2 elements x and y and A such that $f(x) = f(y)$.

Although the pigeonhole principle itself is trivial but when applied cleverly, it can yield nontrivial results. The pigeonhole principle is also called the Dirichlet drawer principle. To apply the pigeonhole principle, we must identify pigeons (object) and pigeonholes (categories of the desired charactersitcs) and be able to count the number of pigeons and the number of pigeonholes.

Example: Show that among 13 people, there are at least two people who were born in the same month.

Solution: If we take 13 people as pigeons and the 12 months (January, February, March, ……., December) as the pigeonholes then by the pigeonhole principle there will be at least two people who were born in the same month.

Example : Show that in a set of five distinct integers, there must exist two integers with the same remainder when divided by 4.

Solution : We know that when any integer is divided by 4 then the possible remainders are 0,1,2 and 3. Assuming 5 given integers as pigeons and 4 remainders as pigeonhole, we get, by the pigeonholes principle, that there are at least two integers with same remainder (when divided by 4).

Example : Suppose 14 students in a class appear at an examination. Prove that there exist at least two among them whose seat numbers differ by a multiple of 13.

Solution : Let A be the set of seat numbers of 14 students. We know that when we divide any integer by 13 then the remainder can only have the values 0,1,2,…..,12. So, we define a function f : A → {0, 1, 2, …., 12} by

f(x) = remainder when x is divided by 13.

Since |A| = 14 and | {0, 1, 2, …., 12}|=13, therefore by the pigeonhole principle, function f cannot be one-to-one. Thus, there exists two distinct seat numbs x and y such that f (x0 = f(y). Now x and y can be written as (by Euclidean algorithm)

X = 13a+f(x) and y = 13b + f(y) .Where a and b are integers.

$\Rightarrow x - y = 13\ (a - b)\ \ \because f(x) = f(y)$

Since a – b is an integer, x – y is a multiple of 13.

Hence, there exist at least two tudents whos seat numbers differ by a multiple of 13.

Example : If any 51 integers are chosen from that set (1,2,3,….., 100} then show that among the chosen integers there exist two integers such that one is multiple of the other.

Solution : We know that every positive integer x can be written as = 2^p.r, where r I odd integer r the odd part of integer x.

If x is in {1,2,…,100} then its odd part r can oly be in 1,3,5,…..,99}.

Let s be any se of 51 integers chosen from the set {1,2,3….,100). Define a function

f: s → {1,3,5,7,….,99} byF (x) = odd part of x.

Since |S| = 51 and | {1,3,5,7,……,99)}|=50, it follows from the pigeonhole principle that f cannot be one-to-one. Thus, there exist two integers x and is S such that their odd parts f(x) and f(y) are same. That is, f(x) = f(y). Therefore, we have

$$x = 2^p.r \text{ and } y2^q.r \text{ for some integes p and q.}$$

If p > q then $x = 2^{p-q}.y$ and therefore x is a multiple of y. If q < q then y is a multiple of x. Thus, either x is multiple of y or y is multiple of x.

Example : Find the minimum number of elements to be chosen from the set S = {1,2,3,…..,9} such that two of them should add up to 10.

Solution : We first construct all possible different set {x, y} of two element from the given set S such that x + y = 10. They are {1, 9], {2, 8}, {3, 7], {4, 7}. Now consider the following partition of S : {1, 9} {2, 8}, {3, 7}, {4, 6} and {5}

Observe that each element of S belongs to one and only one of the above five sets. If we choose any six elements of the set S then it follows by the pigeonhole principle that two of them must belong to the same set which add up to 10.

To Pigeonhole Principle can be generalized in many way. We give below two generalizations. Another generalization is given in problem set.

Theorem 1 : if r □ 2 is an integer and if n(r – 1) + 1 objects are placed inn boxes, then there exists a box with at least r objects.

Proof : Suppose if possible, every box contains less then r objects. Then there wllbe atmost n.(r – 1) objects. But this is contradiction to our assumption that there are n(r –1) +1 objects. Hence, there exists a box with atleast r objects. Then there will be atmost n (r – 1) objects.

But this is a contradiction to our assumption that there are n(r – 1) + 1 objects. Hence, there exists a box with atleast r objects.

Theorem 2 : (Generalized pigeonhole principle). If there are n pigeons and m pigeonholes $(n > m)$ then some pigeonols must contain at least $\left[\frac{(n-1)}{m}\right]+1$ pigeons.

Then there will be atmost $m\left[\frac{(n-1)}{m}\right] \le m.\frac{(n-1)}{m} = n-1$ pigeons.

This is a contradiction to the assumption that there are n pigeons.

Corollary : if pigeons are more than k times the pigeonhole then some pigeonhole must contain at least k+1 pigeons.

Proof : Put $n > km$ in the above theorem to get the result.

Example : Show that if seven colours are used to paint 50 cars, at least eight cars will have the same colour.

Solution : Here 50 cars (Pigeons) are to assign 7 colours (pigeonholes). Hence, b the generalized pigeonhole principle, at least $\left[\frac{(50-1)}{7}\right]+1=8$ cars will have the same colour .

Example : How many letters one must choose from the set of 15A's, 20B's and 25C's so that 12 identical letters will always be include in the selection.

Solution : Here there are three types of letters (pigeonholes) each having more than 12 letters. We have to find minimum number of letters (pigeons) n such that

$$\left[\frac{(n-1)}{3}\right]+1=12 \Rightarrow \left[\frac{(n-1)}{3}\right]=11 \Rightarrow n = 11 \times 3 + 1 = 34$$

Thus, 34 is the minimum number of letters to be selected from the set having 15 A's, 20B's and 25C's so that 12 identical letter will always be included in the selection.

Example : Show that at any party with six people, thee either exists a set of three mutual friends or a set of three mutual strangers.

Solution : Let x be any person at the party. Let S_1 be the set of persons who are friends of x and S_2 be the set of persons who are strangers to x. Then the remaining 5 persons (pigeons) can be either in S_1, or in S_2. By the generalized pigeonhole principle either S_1 or S_2 contains at least $\left\lceil \frac{5-1}{2} \right\rceil + 1 = 3$ persons. We first consider the case when S_1 contains 3 persons a, b and c. If any two of a, b care friends then these two together with x form a set of three mutual friends. On the other hand if no two of a, b, c are friends of each other then {a, b, c} is a set of mutual strangers. In the second case suppose S_2 contains 3 persons a, b and c. If two of a, b, c are strangers to each other then these two together with x form a set of tree mutual strangers. If no two of a, b, c are strangers to each other then they from a set of three mutual friends.

Example : Show that anyset of seven distinct integers contains two integers x any y such that either x+y or x – y is divisible by 10.

Solution : Let A = $\{a_1, a_2, \ldots, a_7\}$ be any set of seven distinct integers. Let r_i be the remainder when any element a_i of A is divided by 10. Consider the following partition of A. $S_1 = \{a_i : a_i \in A \text{ and remainder } r_i = 0\}$

$S_2 = \{a_i : a_i \in A \text{ and remainder } r_i = 5\}$

$S_3 = \{a_i : a_i \in A \text{ and remainder } r_i = 1 \text{ or } 9\}$

$S_4 = \{a_i : a_i \in A \text{ and remainder } r_i = 2 \text{ or } 8\}$

$S_5 = \{a_i : a_i \in A \text{ and remainder } r_i = 3 \text{ or } 7\}$

$S_6 = \{a_i : a_i \in A \text{ and remainder } r_i = 4 \text{ or } 6\}$

We know that when we divide any integer by 10, then the remainder can only have the values 0,1,2,….,9. Therefore, if we divide any integer by 10 then its remainder must belong to one of the sets S_i, i = 1,2,…..,6.

Taking seven distinct integers a_i, i = 1,2,……,7 as pigeons and six sets S_i, i=1,2,…6 as pigeonholes we conclude from the pigeonholes principle that some S_i must contain at least two integers a_i and a_j from A. If both a_i and a_j are in S_1 or S_2 then $a_i + a_j$ and $a_i - a_j$ both are divisible by 10. If a_i and a_j are in one of the other four subsets then

$a_i = 10x+r_i$ and $a_j = 10\,y + r_j$,where r_i and r_j are in one of the sets S_3, S_4, S_5, S_6.

Now $a_i - a_j = 10\,(x - y) + (r_i - r_j)$ and $a_i + a_j = 10\,(x+y) + (r_i + r_j)$.

If r_i and r_j are equal then $a_i - a_j$ is divisible by 10. If $r_i \neq r_j$ then. Thus either $a_i - a_j$ or $a_i + a_j$ in divisible by 10.

Example : In a tournament in which each player against every other player, and each player wins at least once, show that there are at least two palyers having the same number of wins.

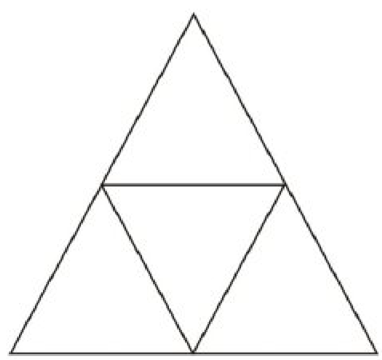
Solution : Let the number of players in a tournament be n. Since each players wins at least once, the number of wins for a player is at least 1 and at most n – 1. Let us define a function f from the set of players to the set {1, 2, …, n} by f (x) = number of wins of the player x. Since there are n players, it follows from the pigeonhole principle that atleast two players have the same number of wins.

Example : Show that any sequence of n^2+1 distinct integers contains an increasing subsequence of length n + 1 or a decreasing sequence of length n + 1

Solution : Let a_1, a_2, a_3,……. $A_n{}^2$+1 be a sequence of n^2+1 distinct (x_k, y_k), where x_k is the length of a longest increasing subsequence starting at a_k and y_k be the length of a longest decreasing subsequence starting at a_k. Suppose if possible there is no increasing or decreasing subsequence of length n+1 in the sequence a_i of n^2+1 integers. Then the set $\{(x_k, y_k)\}$ has atmost n^2 distinct ordered pairs. It follows the pigeonhole principle that there must exist two elements a_i and a_j in the sequence which corresponds to the same ordered pair. It follows by the pigeonhole principle that there must exist two element a_i and a_j in the sequence which correspond to the same ordered pair. In other words $(x_i, y_j) = (x_j, x_j)$. But this is not possible because if $a_i < a_j$ then we must have $x_i > x_j$ and if $a_i > a_j$ then we must have $y_i > y_j$. Contradiction proves that there is either an increasing subsequence or a decreasing subsequence of length n + 1.

Example : Given any five points in the interior of an equilateral triangle of side 1, show that there exists two points with in a distance of at most ½.

Solution : Divide the given equilateral triangle into four equal triangles as shown in the figure. Now the given five points will be placed in these four triangles. By the pigeonhole principle at least two of them must belong to one of the four small triangles. The distance between these two points cannot exceed the side of the triangle which is ½. Thus, thee exists two points within a distance of atmost ½.



<u>Check your progress</u>

1. Prove that if $q_1 \geq 1$, $q_2 \geq 1, \ldots, q_n \geq 1$ are integers and if $q_1+q_2+\ldots q_n - n + 1$ objects are put into n boxes, then either the first box contains atleast q_1 objects or

the second box contains at least q_2 objects, ….., or the n^{th} box contains at least q_n objects.

2. Show that at a party of an people ($n > 1$), there are 2 people who have the same number of friends.

   (**Hint**: Note that friendship is a symmetric relation. A person can have 0, 1, 2,…. upto $n - 1$ friends. If any person at the party has 0 friends of a person are either {0, 1, 2, ……, n – 2) or {1, 2, …., n – 1). In either case we have n people and n – 1 choice for number of friends).

3. Show that any subset of n+1 different integers between 1 and 2n (n□2) always contains pair of integers with no common divisor.

4. Given 10A's, 20B's, 8C's, 15D's and 25E's, how may letters must be chosen to guarantee that there are 12 identical letters.

5. A professor tells three jokes in his class each year. How many jokes does the professor require in order to never repeat the exact same triple of jokes over a period of 12 years. [Ans.6]

6. Find the minimum number of elements to be chosen from {1,2,3,…..8) such that two of them will add up to 9. [ans.5]

7. A student want to prepare for his final examination by solving some unsolved questions papers in 77 days. He decides to solve at least one paper a day but not more than132 papers altogether. Show that there is a period of consecutive day with in which he solves exactly 21 papers.

8. How many times must we throw two dice order to be sure that we obtain the same total score atleast 7 times. [Ans 67]

9. How many cards must be drawn from a pack 52 cards to be sure that you have seven cards of one suit. [Ans 25]

10. Given any five points inside a square of side 1, show that there exists two points within a distance of at most $1/\sqrt{2}$.

11. Given any ten points inside an equilateral triangle of side 1, show that there are two points within a distance of at must 1/3.

    [**Hint**. Divide the given triangle into 9 equal triangles]

12. If p is prime number then show that there exists integers a and b such that p divides a^2+b^2+1.

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

UNIT - 4

The Inclusion – Exclusion Principle

Structure

4.1 Introduction

This is most basic and important unit of this block as it introduces the concept of counting, the inclusion-exclusion principleand the elementary operations and associated connections. We introduce the well formed formulae for finding of onto maps,

4.2 Objectives

After reading this unit we should be able to

1. Understand the concept of the inclusion-exclusion principle

2. Understand the formulae for finding of onto maps

Logic is a field of study that deals with the method of reasoning Logic provides rules by which we can determine whether a given argument or reasoning is valid (correct) or not. Logical reasoning is used in Mathematics to prove theorems. In computer science logic is used to verify the correctness of programs. If $A \cap B \neq \phi$, then sume rule$|A \cup B| = |A|+|B|$

does not hold. For example if $A = \{a, b, c\}$, $B=\{c, d, e, f\}$

then $|A| = 3$ and $|B| = 4$ but $|A \cup B| = 6$ not 7. The general formula which is true for any finite sets A and B is $|A \cup B| = |A| + |B| - |A \cap B|$ ....(1)

Here to find $|A \cup B|$ we included (added) $|A|$ and $|B|$ and we excluded (subtracted) $|A \cap B|$. We shall see that formula (1) is a special case of the inclusion -exclusion principle. Before stating the general inclusion-exclusion principle for n sets we give it for three set.

Theorem: for any finite sets, A, B, C we have

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

Proof: $|A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$

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

$= |A| + |B| + |C| - |A \cap B| - \{|A \cap C| + |B \cap C| - |A \cap B \cap C|\}$

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

We now state and prove the inclusion-exclusion principle.

4.3 The inclusion-exclusion principle

Let $A_1, A_2, \ldots, A_n$ be an n finite sets. Then

$$|A_1 \cup A_2 \cup A_3 \ldots\ldots \cup A_n| \sum_{i=1}^{n} |A_i| - \sum_{1 \le j < j \le n} |A_i \cap A_j|$$

$$+ \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| \ldots + 9\ 1)^{n-1} |A_1 \cap A_2 \cap A|.$$

Proof. We shall prove the formula by showing that each element of $A_1 \cup A_2 \cup \ldots \cup A_n$ is counted exactly once on the right hand side of the equation. Let x be any element in $A_1 \cup A_2 \cup \ldots \cup A_n$. Suppose x belongs in exactly m sets, 1□m□n. Now, in $\sum_{i=1}^{n} |A_i|$ it is counted m times. In $\sum_{1 \le j < n} |A_i \cap A_j|$, x is counted ${}^mC_2$ times and so on. Thus, the element x is counted exactly $m - {}^mC_2 + {}^mC_3 \ldots\ldots + (-1)^{m-1} . {}^mC_m$

$= {}^mC_0 - [{}^mC_0 - {}^mC_1 + {}^mC_2 + \ldots\ldots (-1)^m\, {}^mC_m] = 1 - 1 = 0$

Because ${}^mC_0 - {}^mC_1 + {}^mC_2 - {}^mC_3 + \ldots . (-1)^m\, {}^mC_m = 0.$

Thus, each element of $A_1 \cup A_2 \ldots\ldots \cup A_n$ is counted exactly once on the right-hand side of the equation. This completes the proof.

Note: The above principle can also be proved by induction on n.

4.4 Alternative form of the inclusion-exclusion principle

Let S be a finite set and $A_1, A_2, \ldots, A_n$ be subsets of S. Let A_1' denote the complement of A_i. Then we have the following theorem.

Theorem : If $A_1, A_2, \ldots, A_n$ are subsets of a finite set S then

$$|A_1' \cap A_2' \cap A_3' \ldots \cap A_n'| = |S| - \sum_{i=1}^{n} |A_i| + \sum_{1 \le i < j \le n} |A_i \cap A_j|$$

$$+ \ldots + (-1)^n |A_1 \cap A_2 \cap \ldots \cap A_n|$$

Proof : by De Morgan's laws, we have $\bigcap_{i=1}^{n} A_i' = S - \bigcup_{i=1}^{n} A_i$

$$\Rightarrow \left|\bigcup_{i=1}^{n} A_i'\right| = |S| - \left|\bigcup_{i=1}^{n} A_i\right| \because [A \subset X \Rightarrow |X - A| = |X| - |A|]$$

If we substitute the value of $\left|\bigcup_{i=1}^{n} A_i\right|$ from theorem 2, we get the result.

Example: Find the number of integers between 1 and 250 that are divisible by any of the integers 2,3 and 7.

Solution : Let A_1 denote the set of all integers between 1 and 250 that are divisible by 2, A denote the set of integers that are divisible by 3 and A_3 denote th set of integers that are divisible by 7. Then

$$|A_1| = \left[\frac{250}{2}\right] = 125, |A_2| = \left[\frac{250}{3}\right] = 83 \text{ and } |A_3| = \left[\frac{250}{7}\right] = 35,$$

Where [x] denote the largest integer not greater than x.

Now $|A_1 \cap A_2|$ = no. of integers between 1 and 250 that are divisible b both 2 and 3.

$$= \text{no. of integers that are divisible by 6.} = \left[\frac{250}{6}\right] = 41$$

Similarly, $|A_1 \cap A_3| = \left|\frac{250}{2 \times 7}\right| = 17$ and $|A_2 \cap A_3| = \left|\frac{250}{3 \times 7}\right| = 11$

$$|A_1 \cap A_2 \cap A_3| = \left|\frac{250}{2 \times 3 \times 7}\right| = 5$$

$$\therefore |A_1 \cup A_2 \cup A_3| = 125+83+35-41-17-11+5 = 179$$

Example : How many integer solutions are there to the equation $x_1+ x_2+ x_3+ x_4=13$, $0 \leq x_i \leq 5$

Solution : Let S be the set of all integer solutions of the given equation with each $x_i \geq 0$ and let A_i be the set of integer solutions with $x_i > 5$ or equivalently $x_i < 6$. Then number of solutions with

$0 \leq x_i \leq 5$will be $|A_1' \cap A_2' \cap A_3' \cap A_4'|$

Now $|S| = {}^{13+4-1}C_{13} = {}^{16}C_{13} = 560$

$$|A_i| = {}^{(13-6)+4-1}C_{13-6} = {}^{10}C_7 = 120$$

$$|A_i \cap A_j| = {}^{(13-6-6)+4-1}C_{13-6-6} = {}^{4}C_1 = 4$$

Since each $x_i \leq 6$, therefore sum of three x_i' would exceed 13. Therefore,

$|A_i \cap A_j \cap A_k| = 0$.

Similalry, $|A_1 \cap A_2 \cap A_3 \cap A_4|$ is also zero.

Now from theorem 3, we have

$$|A_1' \cap A_2' \cap A_3' \cap A_4'| = |S| - \sum_{i=1}^{4} |A_i| + \sum_{1 \leq i < j \leq 4} |A_i \cap A_j| = 560 - 4 \times 120 + {}^4C_2 \times 4 = 104$$

Note: This questions can also be done with the help of generating function.

4.5 Onto Functions

We know that the total number of functions from a set A having n elements to a set B having m elements is m^n, If m □n then number of one-one functions is m!/m – n)!. With the help of the inclusion-exclusion principle we obtain the number of onto functions in the following theorem.

Theorem 4: Let A and B be two sets having n and m elements respectively. Then the number of onto functions from A to B is

$$m^n - {}^mC_1(m-1)^n + {}^mC_2(m-2)^n - \ldots\ldots + (-1)^{m-1}\, {}^mC_{m-1}$$

Proof : Let S be the set of all functions from A to B them $|S|=m^n$. Let$B = (b_1,b_2,\ldots, b_m)$. For each $i=1,2,\ldots m$, let S_i be the set of all functions from A to B – (b_i). That is, S_i contains all functions $fb_i: A \to B - \{b_i\}$. Since $|B - \{b_i\}| = m - 1$,

$|S_i| = (m - 1)^n$.

For I = j, $S_i \cap S_j$ is the set of functions which takes values in the set $B - \{b_i, b_j\}$. Again $|B - \{b_i, b_j\}| = m - 2$, therefore , $|S_i \cap S_j| = (m - 2)^n$.In general, for any k-tuple $\{t_i, i_2, \ldots, i_k\}$ with $1 \le i_i < i_2 < i_3 \ldots < i_k \le m$, we have $|S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}| = (m - k)^n$

We observe that a function from A to B is onto iff it does not belong to any S_1' S, I = 1, 2,….,m. Applying the principle of inclusion-exclusion, we get $|S_1' \cap S_2' \cap \ldots S_m'|$

$$= |S| - \sum_{i=1}^{m} |S_i| + {}^mC_2 |S_i \cap S_j| - {}^mC_3 | S_i \cap S_j \cap S_k| + \ldots + (-1)^m |S_1 \cap S_2 \ldots \cap S_m|$$

$$= m^n - {}^mC_1(m - 1)^n + {}^mC_2 (m - 2)^n \ldots + (-1)^{m-1}\, {}^mC_{m-1}.1^m + 0$$

$$= mn - {}^mC_1(m - 1)^n + {}^mC_2(m - 2)^n\ 0 \ldots + (-1)^{m-1}\, {}^mC_{m-1}.$$

Example : In how many ways six different jobs can be assigned to four different persons if each person is assigned at least one job.

Solution : In how the set of six jobs and B be the set of five persons. Now we have to assign jobs to person such that each person gets at least one job. This is equivalent to finding onto functions from the set A to the set B. Here $|A| = 6$ and $\backslash B| = 5$. Therefore, there are $5^6 - {}^5C_1(5 - 1)^6 + {}^5C_2(5 - 2)^6 - {}^5C_3(5 - 3)^6 + {}^5C_4(5 - 4)^6 = 1800$

Ways to assign the jobs to the persons in the desired manner.

Suggested Further Readings

(1) Felix. H. (1978) Set theory, Chelsea publishing Co. New York.

(2) P. T. Johnstone, (1987) Notes on Logic and set theory, Cambridge University Press.

(3) I. N. Herstein. (1983), Topic in Algebra, Vikas publishing house Pvt. Ltd.

(4) John B, Fraleigh, A first course in Abstract Algebra, Narosa publishing house Pvt. Ltd.

(5) S. Ganguly and M. N. Mukherjee, A Treatise on basic Algebra, Academic Publishers- Kolkata.

Rough Work

ROUGH WORK

ROUGH WORK