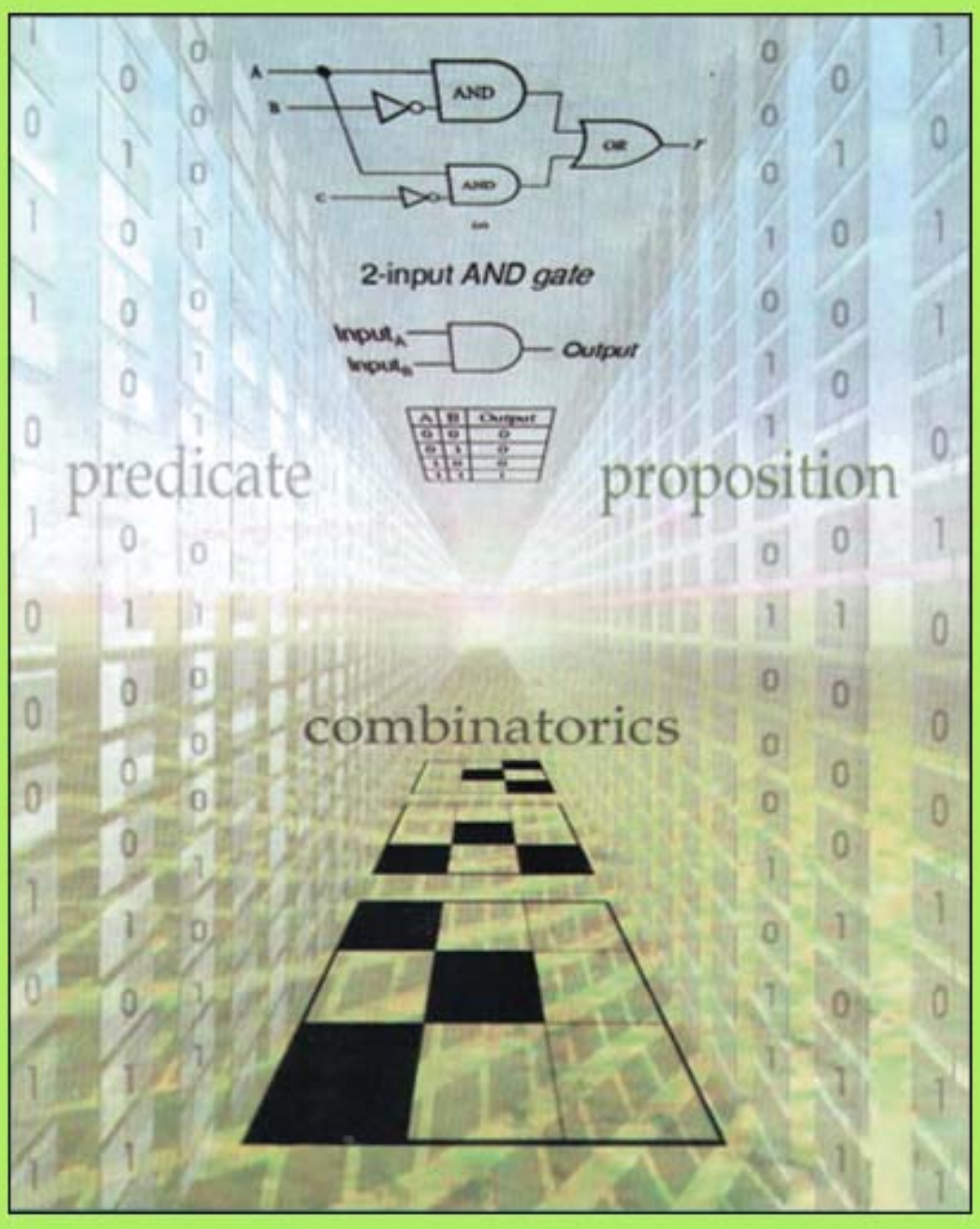
Indira Gandhi National Open University
School of Computer and Information Sciences

MCS-013
DISCRETE MATHEMATICS



Elementary Logic

1

Indira Gandhi
National Open University
School of Computer and
Information Sciences

MCS-013
DISCRETE MATHEMATICS

Block

1

ELEMENTARY LOGIC

Programme / Course Design Committee

Prof. Sanjeev K. Aggarwal, IIT, Kanpur
Prof. M. Balakrishnan, IIT , Delhi
Prof Harish Karnick, IIT, Kanpur
Prof. C. Pandurangan, IIT, Madras
Dr. Om Vikas, Sr. Director, MIT
Prof P. S. Grover, Sr. Consultant, SOCIS, IGNOU

Faculty of School of Computer and Information Sciences
Shri Shashi Bhushan
Shri Akshay Kumar
Prof Manohar Lal
Shri V.V. Subrahmanyam
Shri P.Venkata Suresh

Block Preparation Team

Modified from Block 5 , MESE-001 by Shri M.P.Mishra

Course Coordinator: Shri M.P.Mishra

Block Production Team

Shri H.K. Som, SOCIS

CRC prepared: by Shri Vikas Kumar.

Acknowledgements

To Prof. Parvin Sinclair for her valuable comments and suggestions.

April, 2004

ISBN

Printed and published on behalf on the Indira Gandhi National Open University, New Delhi by the Director, SOCIS.

BLOCK INTRODUCTION

"Contrariwise, "continued Tweedledee, "if it was so, it might be; and if it were so, it would be; but as it isn't, it ain't. That's logic."

From 'Alice in Wonderland'
By Lewis Carroll

Logic is the study and analysis of the nature of the valid argument, the reasoning tool by which valid inferences can be drawn from a given set of facts and premises. It is the basis on which all the sciences are built. Logic was extensively studied and developed in ancient Greece. But the mathematical theory of logic, called symbolic logic, only came into its own in the 19th century. This algebraic way of studying arguments was developed by the English mathematician George Boole (1815-1864).

In symbolic logic we study arguments. The basic building blocks of arguments are declarative sentences, called propositions or statements. In Unit 1 we introduce you to propositions and ways of combining them to form more complex propositions. We also introduce you to propositions that contain the quantifiers 'for every' and 'there exists'. In symbolic logic, the goal is to determine which propositions are true and which are false. Truth table a tool to find out all possible outcome of a propositions truth value will be discussed in Unit 1.

In Unit 2 we look at paths of reasoning by which we can show that certain statements are true. Such arguments are called 'proofs'. In this unit we try to give you an understanding of why a proof is written the way it is. We expose you to several patterns of reasoning that make up different proofs. In this unit we also discuss mathematical induction, a fundamental tool for proving many propositions involving natural numbers.

The last unit of the block, Unit 3, is closely linked with Unit 1. In this unit you will see that the set of propositions, along with certain operations, forms an algebraic structure called a Boolean algebra. You will also see the application of this theory for studying logic gates and circuits. Here we discuss how Boolean expressions can be represented with the help of gating diagrams. One important aspect of Boolean algebra that is, minimization of Boolean expression is discussed in detail in covered in Block 1 of the course MCS 012. Please try and tuch that discussion with what you study here.

Regarding the study of the block, and the course , the best way to absorb the material is to try all the exercises in the units as and when you get to them .Also after going through each unit, you must come back to the section 'Objectives', and check if you have achieved this. Doing this will help you confirm that you are ready to go further.

NOTATIONS AND SYMBOLS

N	the set of natural numbers
R	the set of real numbers
$p \vee q$	p or q (p, q being statements)
$p \oplus q$	either p or q, but not both.
$P \wedge q$	p and q
$\sim p$	not p
$p \rightarrow q$	p implies q p is sufficient for q p only if q
$p \leftrightarrow q$	p is necessary and sufficient for q p is necessary and sufficient for q p implies and is implied by q
$p \Rightarrow q$	If p is true, then q is true
$p \Leftrightarrow q$	p is true if and only if q is true.
$P \equiv q$	p is equivalent to q
$\therefore$	therefore
iff	if and only if
$\forall$	for all
$\exists$	there exists
$\exists!$	There exists one and only one
$P(X)$	set of all subsets of a set X
B	two-element Boolean algebra
B^n	B x B …. x B (n times)
$X(x_1, \ldots, x_k)$	Boolean expression in k-variables.
s.v.	state value
a par b	parallel connections of switches a and b
a set b	series connections of switches a and b
CNF	conjunctive normal form
DNF	disjunctive normal form

COURSE INTRODUCTION

Discrete mathematics, sometimes called finite mathematics, is the study of mathematical structure that are fundamentally discrete, in the sense of not supporting notion of continuity. Discrete mathematics deals with discrete objects, like the set of students in the IGNOU MCA course, the type of policies offered by an Insurance company, the number of blue-line buses in Delhi.

A study of discrete sets has become more and more necessary because of many application of Computer Science and various areas of engineering. Regarding computer science concept from discrete mathematics are useful to study or express objects or problems in computer algorithm and programming languages. For instance, to improve the efficiency of a computer programme, we need to study its logical structure, which involves a finite number of steps each requiring a certain amount of time. Using the theory of combinatorics and graph theory, major areas of discrete mathematics, we can do this. Therefore, a study of these areas would complement and improve your understanding of courses based on algorithm and problem solving . As you will find several of your courses will require the knowledge of basic concepts in discrete mathematics.

This is why we have included two courses of 2 credits each in your curriculum . The first course is this one of 2 blocks In this course we have chosen to introduce you to only a few topics involving discrete objects, to give you a flavor of this recently evolving area of mathematics.

In Block 1, we show you how to differentiate between a sentence and a statement (or proposition). Then we look at various ways of combining propositions, and of finding whether these statements are true or not. After this we talk about a theory first studied by Aristotle (384-322 B.C.), and later evolved mathematically by the 19^{th} century mathematicians Boole, De Morgan, Schroder and Frege. This is the theory of mathematical logic and the nature of mathematical proof. In this connection, it is necessary to mention the monumental work of A.N. Whitehead and Bertrand Russell, which they presented in their book 'Principia Mathematica' in 1913.

In the final unit of Block 1 we look at an important application of logic, namely, Boolean algebras and circuits.Boolean algebra we will use for representing logical logical expression.In this we can learn the use of logic gates to make gating diagram of given Boolean expressions.

In Blocks 2, we discuss combinatorics, or different ways of enumerating without actually counting. This theory was first developed by Pascal (1623-1662) and Jakob Bernoulli (1645-1705). We shall introduce you to various aspects of combinatorial reasoning, which underlies all analysis of computer systems, discrete operations research problems and finite probability. More specifically, you will study set, relations, functions, permutations, combinations, and partitions of numbers and there applications. Of course, all these would be presented from an application-oriented point of view. During this course you will find that everything that you learn here is having direct implication in your problem solving capabilities.

Now a word about our notation. Each unit is divided into sections, which may be further divided into sub-sections. These sections/sub-sections are numbered sequentially, in a unit as are the exercises. In each unit you, will find several exercises (numbered E1,E2….) and examples (also numbered sequentially). We show the end of an example by *** after it.

Another compulsory component of this course is its **assignment** – which is based on the whole course. Your academic counselor will evaluate them and return them to you

with detailed comments. Thus, the assignments are meant to be a teaching as well as an assessment aid.

We hope you enjoy studying this course. If you have a problem in understanding any portion of it, please ask your academic counselor for help. For your suggestions, comments, and problems related to this course write to the course coordinator at mpmishra@ignou.ac.in. Also, if you feel like studying any topic in greater detail, you may consult:

1 *Elements of Discrete Mathematics*, C.L. Liu, McGraw-Hill, 1985.

2 *Discrete Mathematics*, Richard Johnsonbaugh, Pearson Education,2003.

3 *Discrete Mathematical Structures*, Kolman, Busby and Ross , Prentice-Hall India, 2002.

UNIT 1 PROPOSITIONAL CALCULUS

Structure

1.0 INTRODUCTION

According to the theory of evolution, human beings have evolved from the lower species over many millennia. The chief asset that made humans "superior" to their ancestors was the ability to reason. How well this ability has been used for scientific and technological development is common knowledge. But no systematic study of logical reasoning seems to have been done for a long time. The first such study that has been found is by Greek philosopher Aristotle (384-322 BC). In a modified form, this type of logic seems to have been taught through the Middle Ages.

Then came a major development in the study of logic, its formalisation in terms of mathematics.It was mainly Leibniz (1646-1716) and George Boole (1815-1864) who seriously studied and development this theory, called **symbolic logic**. It is the basics of this theory that we aim to introduce you to in this unit and the next one.

In the introduction to the block you have read about what symbolic logic is. Using it we can formalise our arguments and logical reasoning in a manner that can easily show if the reasoning is valid, or is a fallacy. How we symbolise the reasoning is what is presented in this unit.

More precisely, in Section 1.2 (i.e., Sec. 1.2, in brief) we talk about what kind of sentences are acceptable in mathematical logic. We call such sentences statements or propositions. You will also see that a statement can either be true or false. Accordingly, as you will see, we will give the statement a truth value T or F.

In Sec. 1.3 we begin our study of the logical relationship between propositions. This is called prepositional calculus. In this we look at some ways of connecting simple propositions to obtain more complex ones. To do so, we use logical connectives like "and" and "or". We also introduce you to other connectives like "not", "implies" and "implies and is implied by". At the same time we construct tables that allow us to find the truth values of the compound statement that we get.

In Sec. 1.4 we consider the conditions under which two statements are "the same". In such a situation we can safely replace one by the other.

And finally, in Sec 1.5, we talk about some common terminology and notation which is useful for quantifying the objects we are dealing with in a statement.

It is important for you to study this unit carefully, because the other units in this block are based on it. Please be sure to do the exercises as you come to them. Only then will you be able to achieve the following objectives.

1.1 OBJECTIVES

After reading this unit, you should be able to:

- distinguish between propositions and non-propositions;
- construct the truth table of any compound proposition;
- identify and use logically equivalent statements;
- identify and use logical quantifiers.

Let us now begin our discussion on mathematical logic.

1.2 PROPOSITIONS

Consider the sentence 'In 2003, the President of India was a woman'. When you read this declarative sentence, you can immediately decide whether it is true or false. And so can anyone else. Also, it wouldn't happen that some people say that the statement is true and some others say that it is false. Everybody would have the same answer. So this sentence is either **universally true** or **universally false**.

Similarly, 'An elephant weighs more than a human being.' Is a declarative sentence which is either true or false, but not both. In mathematical logic we call such sentences **statements or propositions**.

On the other hand, consider the declarative sentence 'Women are more intelligent than men'. Some people may think it is true while others may disagree. So, it is neither universally true nor universally false. Such a sentence is not acceptable as a statement or proposition in mathematical logic.

Note that a **proposition should be either uniformly true or uniformly false**. For example, 'An egg has protein in it.', and 'The Prime Minister of India has to be a man.' are both propositions, the first one true and the second one false.

Would you say that the following are propositions?

'Watch the film.
'How wonderful!'
'What did you say?'

Actually, none of them are declarative sentences. (The first one is an order, the second an exclamation and the third is a question.) And therefore, none of them are propositions.

Now for some mathematical propositions! You must have studied and created many of them while doing mathematics. Some examples are

Two plus two equals four.
Two plus two equals five.
$x + y > 0$ for $x > 0$ and $y > 0$.
A set with n elements has 2^n subsets.

Of these statements, three are true and one false (which one?).
Now consider the algebraic sentence '$x + y > 0$'. Is this a proposition? Are we in a position to determine whether it is true or false? Not unless we know the values that x and y can take. For example, it is false for
$x = 1, y = -2$ and true if $x = 1, y = 0$. Therefore,
'$x + y > 0$' is not a proposition, while
'$x + y > 0$ for $x > 0, y > 0$' is a proposition.

Why don't you try this short exercise now?

E1) Which of the following sentences are statements? What are the reasons for your answer?

i) The sun rises in the West.
ii) How far is Delhi from here?
iii) Smoking is injurious to health.
iv) There is no rain without clouds.
v) What is a beautiful day!
vi) She is an engineering graduates.
vii) $2^n + n$ is an even number for infinitely many n.
viii) $x + y = y + x$ for all $x, y \in \mathbf{R}$.
ix) Mathematics is fun.
x) $2^n = n^2$.

Usually, when dealing with propositions, we shall denote them by lower case letters like p, q, etc. So, for example, we may denote

'Ice is always cold.' by p, or
'$\cos^2 \theta + \sin^2 \theta = 1$ for $\theta \in [0, 2\pi]$' by q.
We shall sometimes show this by saying
p: Ice is always cold., or
q: $\cos^2 \theta + \sin^2 \theta = 1$ for $\theta \in [0, 2\pi]$.

Now, given a proposition, we know that it is either true or false, but not both. If it is **true**, we will allot it the **truth value T.** If it is **false**, its **truth value will be F**. So, for example, the truth value of

Sometimes, as in the context of logic circuits (See unit 3), we will use 1 instead of T and 0 instead of F.

'Ice melts at 30^o C.' is F, while that of '$x^2 \geq 0$ for $x \in R$' is T.

Here are some exercises for you now.

E2) Give the truth values of the propositions in E1.

E3) Give two propositions each, the truth values of which are T and F, respectively. Also give two examples of sentences that are not propositions.

Let us now look at ways of connecting simple propositions to obtain compound statements.

1.3 LOGICAL CONNECTIVES

When you're talking to someone, do you use very simple sentences only? Don't you use more complicated ones which are joined by words like 'and', 'or', etc? In the same way, most statements in mathematical logic are combinations of simpler statements joined by words and phrases like 'and'. 'or', 'if … then'. 'if and only if', etc. These words and phrases are called **logical connectives**. There are 6 such connectives, which we shall discuss one by one.

1.3.1 Disjunction

Consider the sentence 'Alice or the mouse went to the market.'. This can be written as 'Alice went to the market or the mouse went to the market.' So, this statement is actually made up of two simple statements connected by 'or'. We have a term for such a compound statement.

Definition: The **disjunction** of two propositions p and q is the compound statement

p or q, denoted by **p ∨ q**.
For example, 'Zarina has written a book or Singh has written a book.' Is the disjunction of p and q, where
p : Zarina has written a book, and
q : Singh has written a book.

Similarly, if p denotes ' 2 > 0' and q denotes '2 < 5', then p ∨ q denotes the statement '2 is greater than 0 or 2 is less than 5.'.

Let us now look at how the truth value of p ∨ q depends upon the truth values of p and q. For doing so, let us look at the example of Zarina and Singh, given above. If even one of them has written a book, then the compound statement p ∨ q is true. Also, if both have written books, the compound statement p ∨ q is again true. Thus, if the truth value of even one out of p and q is T, then that of 'p ∨ q' is T. Otherwise, the truth value of p ∨ q is F. This holds for any pair of propositions p and q. To see the relation between the truth values of p, q and p ∨ q easily, we put this in the form of a table (Table 1), which we call a **truth table.**

Table 1: Truth table for disjunction

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

How do we form this table? We consider the truth values that p can take – T or F. Now, when p is true, q can be true or false. Similarly, when p is false q can be true or false. In this way there are 4 possibilities for the compound proposition p ∨ q. Given any of these possibilities, we can find the truth value of p ∨ q. For instance, consider the third possibility, i.e., p is false and q is true. Then, by definition, p ∨ q is true. In the same way, you can check that the other rows are consistent.

Let us consider an example.

Example 1: Obtain the truth value of the disjunction of 'The earth is flat'.
and '3 + 5 = 2'.

Solution: Let p denote 'The earth is flat,' and q denote '3 + 5 = 2'. Then we know that the truth values of both p and q are F. Therefore, the truth value of p ∨ q is F.

***

Try an exercise now.

E4) Write down the disjunction of the following propositions, and give its truth value.
   i) 2 + 3 = 7,
   ii) Radha is an engineer.

We also use the term 'inclusive or ' for the connective we have just discussed. This is because p ∨ q is true even when both p and q are true. But, what happens when we want to ensure that only one of them should be true? Then we have the following connective.

Definition: The **exclusive disjunction** of two propositions p and q is the statement **'Either p is true or q is true, but both are not true.'.** Either p is true or q is true, but both are not true.'. We denote this by **p ⊕ q .**

So, for example, if p is '2 + 3 = 5' and q the statement given in E4(ii), then p ⊕ q is the statement 'Either 2 + 3 = 5 or Radha is an engineer'. This will be true only if Radha is not an engineer.

In general, how is the truth value of p ⊕ q related to the truth values of p and q? This is what the following exercise is about.

E5) Write down the truth table for ⊕. Remember that p ⊕ q is not true if both p and q are true.

Now let us look at the logical analogue of the coordinating conjunction 'and'.

1.3.2 Conjunction

As in ordinary language, we use 'and' to combine simple propositions to make compound ones. For instance, ' 1 + 4 ≠ 5 and Prof. Rao teaches Chemistry.' is formed by joining '1 + 4 ≠ 5' and 'Prof. Rao teaches Chemistry' by 'and'. Let us define the formal terminology for such a compound statement.

Definition: We call the compound statement **'p and q'** the **conjunction** of the statements p and q. We denote this by **p ∧ q**.

For instance, '3 + 1 ≠ 7 ∧ 2 > 0' is the conjunction of '3 + 1 ≠ 7' and '2 > 0'.
Similarly, '2 + 1 = 3 ∧ 3 = 5' is the conjunction of '2 + 1 = 3' and '3 = 5'.

Now, when would p ∧ q be true? Do you agree that this could happen only when both p and q are true, and not otherwise? For instance, '2 + 1 = 3 ∧ 3 = 5' is not true because '3 = 5' is false.
So, the truth table for conjunction would be as in Table 2.

Table 2: Truth table for conjunction

P	q	p ∧ q
T	T	T
T	F	F
F	T	F
F	F	F

To see how we can use the truth table above, consider an example.

Example 2: Obtain the truth value of the conjunction of '2 ÷5 = 1' and 'Padma is in Bangalore.'.

Solution: Let p : 2 ÷5 = 1, and
q: Padma is in Bangalore.

Then the truth value of p is F. Therefore, from Table 3 you will find that the truth value of p ∧ q is F.

***

Why don't you try an exercise now?

E6) Give the set of those real numbers x for which the truth value of p ∧ q is T, where p : x > -2, and q : x + 3 ≠ 7

If you look at Tables 1 and 2, do you see a relationship between the truth values in their last columns? You would be able to formalize this relationship after studying the next connective.

1.3.3 Negation

You must have come across young children who, when asked to do something, go ahead and do exactly the opposite. Or, when asked if they would like to eat, say rice and curry, will say 'No', the 'negation' of yes! Now, if p denotes the statement 'I will eat rice.', how can we denote 'I will not eat rice.'? Let us define the connective that will help us do so.

Definition: The **negation** of a proposition p is **'not p'**, denoted by ~p.

For example, if p is 'Dolly is at the study center.', then ~ p is 'Dolly is not at the study center'. Similarly, if p is 'No person can live without oxygen.', ~ p is 'At least one person can live without oxygen.'.

Now, regarding the truth value of ~ p, you would agree that it would be T if that of p is F, and vice versa. Keeping this in mind you can try the following exercises.

E7) Write down ~ p, where p is
   i) $0 - 5 \neq 5$
   ii) $n > 2$ for every $n \in \mathbf{N}$.
   iii) Most Indian children study till class 5.

E8) Write down the truth table of negation.

Let us now discuss the conditional connectives, representing 'If …, then …' and 'if and only if'.

1.3.4 Conditional Connectives

Consider the proposition 'If Ayesha gets 75% or more in the examination, then she will get an A grade for the course.'. We can write this statement as 'If p, and q', where

p: Ayesha gets 75% or more in the examination, and
q: Ayesha will get an A grade for the course.

This compound statement is an example of the implication of q by p.

Definition: Given any two propositions p and q, we denote the statement **'If p, then q' by $p \rightarrow q$.** We also read this as 'p **implies** q'. or 'p is sufficient for q', or 'p **only if** q'. We also call p the **hypothesis** and q the conclusion. Further, a statement of the form $p \rightarrow q$ is called a **conditional statement** or a **conditional proposition**.

So, for example, in the conditional proposition 'If m is in **Z**, then m belongs to **Q**.' the hypothesis is '$m \in \mathbf{Z}$' and the conclusion is '$m \in \mathbf{Q}$'.

Mathematically, we can write this statement as

$$m \in \mathbf{Z} \rightarrow m \in \mathbf{Q}.$$

Let us analyse the statement $p \rightarrow q$ for its truth value. Do you agree with the truth table we've given below (Table 3)? You may like to check it out while keeping an example from your surroundings in mind.

Table 3: Truth table for implication

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

You may wonder about the third row in Table 3. But, consider the example '$3 < 0 \rightarrow 5 > 0$'. Here the conclusion is true regardless of what the hypothesis is. And therefore, the conditional statement remains true. In such a situation we say that the **conclusion is vacuously true.**

Why don't you try this exercise now?

E9) Write down the proposition corresponding to $p \rightarrow q$, and determine the values of x for which it is false, where
$p : x + y = xy$ where $x, y \in \mathbf{R}$
$q : x \not< 0$ for every $x \in \mathbf{Z}$.

Now, consider the implication 'If Jahanara goes to Baroda, then the she doesn't participate in the conference at Delhi.'. What would its converse be? To find it, the following definition may be useful.

Definition: The **converse** of $p \rightarrow q$ is $q \rightarrow p$. In this case we also say 'p is necessary for q', or 'p **if** q'.

So, in the example above, the converse of the statement would be 'If Jahanara doesn't participate in the conference at Delhi, then she goes to Baroda.'. This means that Jahanara's non-participation in the conference at Delhi is necessary for her going to Baroda.

Now, what happens when we combine an implication and its converse?

To show '$p \rightarrow q$ and $q \rightarrow p$', we introduce a shorter notation.

Definition: Let p and q be two propositions. The compound statement $(p \rightarrow q) \wedge (q \rightarrow p)$ is the **biconditional** of p and q. We denote it by $\mathbf{p \leftrightarrow q}$, and read it as 'p **if and only** q'.

The two connectives $\rightarrow$ and $\leftrightarrow$ are called **conditional connectives.**

We usually shorten 'if and only 'if' to **iff**.

We also say that 'p **implies and is implied** by q'. or 'p is **necessary and sufficient for** q'.

For example, 'Sudha will gain weight if and only if she eats regularly.' Means that 'Sudha will gain weight if she eats regularly **and** Sudha will eat regularly if she gains weight.'

One point that may come to your mind here is whether there's any difference in the two statements $p \leftrightarrow q$ and $q \leftrightarrow p$. When you study Sec. 1.4 you will realize why they are inter-changeable.

Let us now consider the truth table of the biconditional, i.e., of the **two-way** implication.

To obtain its truth values, we need to use Tables 2 and 3, as you will see in Table 4. This is because, to find the value of $(p \rightarrow q) \wedge (q \rightarrow p)$ we need to know the values of each of the simpler statements involved.

Table 4: Truth table for two-way implication.

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

As you can see from the last column of the table (and from your own experience), $p \leftrightarrow q$ is true only when both p and q are true or both p and q are false. In other words, $p \leftrightarrow q$ is true only when p and q have the same truth values. Thus, for example,'Parimala is in America iff 2 + 3 = 5' is true only if 'Parimala is in America,' is true.

Here are some related exercises.

E10) For each of the following compound statements, first identify the simple propositions p, q, r, etc., that are combined to make it. Then write it in symbols, using the connectives, and give its truth value.

i) If triangle ABC is equilateral, then it is isosceles.
ii) a and b are integers if and only if ab is a rational number.
iii) If Raza has five glasses of water and Sudha has four cups of tea, then Shyam will not pass the math examination.
iv) Mariam is in Class 1 or in Class 2.

E11) Write down two propositions p and q for which $q \rightarrow p$ is true but $p \leftrightarrow q$ is false.

Now, how would you determine the truth value of a proposition which has more than one connective in it? For instance, does $\sim p \vee q$ mean $(\sim p) \vee q$ or $\sim (p \vee q)$? We discuss some rules for this below.

1.3.5 Precedence Rule

While dealing with operations on numbers, you would have realized the need for applying the BODMAS rule. According to this rule, when calculating the value of an arithmetic expression, we first calculate the value of the Bracketed portion, then apply **Of, Division, Multiplication, Addition and Subtraction, in this order.** While calculating the truth value of compound propositions involving more than one connective, we have a similar **convention** which tells us which connective to apply first.

Why do we need such a convention? Suppose we didn't have an order of preference, and want to find the truth of, say $\sim p \vee q$. Some of us may consider **the value of $(\sim p) \vee q$, and some may consider $\sim (p \vee q)$. The truth values can be different in these cases. For instance, if p and q are both true, then $(\sim p) \vee q$ is true, but $\sim (p \vee q)$ is false. So, for the purpose of unambiguity, we agree to such an order or rule. Let us see what it is.**

The rule of precedence: The order of preference in which the connectives are applied in a formula of propositions that has no brackets is

i) $\sim$
ii) $\wedge$
iii) $\vee$ and $\oplus$
iv) $\rightarrow$ and $\leftrightarrow$

Note that the 'inclusive or' and 'exclusive or' are both third in the order of preference. However, if both these appear in a statement, we first apply the left most one. So, for instance, in $p \vee q \oplus \sim p$, we first apply $\vee$ and then $\oplus$. The same applies to the 'implication' and the 'biconditional', which are both fourth in the order of preference.

To clearly understand how this rule works, let us consider an example.

Example 3: Write down the truth table of $p \rightarrow q \wedge \sim r \leftrightarrow r \oplus q$

Solution: We want to find the required truth value when we are given the truth values of p, q and r. According to the rule of precedence given above, we need to first find the truth value of ~ r, then that of ($q \wedge \sim r$), then that of ($r \oplus q$), and then that of $p \rightarrow (q \wedge \sim r)$, and finally the truth value of $[p \rightarrow (q \wedge \sim r)] \leftrightarrow r \oplus q$.

So, for instance, suppose p and q are true, and r is false. Then ~ r will have value T, $q \wedge \sim r$ will be T, $r \oplus q$ will be T, $p \rightarrow (q \wedge \sim r)$ will be T, and hence, $p \rightarrow q \wedge \sim r \leftrightarrow r \oplus q$ will be T.

You can check that the rest of the values are as given in Table 5. Note that we have 8 possibilities ($=2^3$) because there are 3 simple propositions involved here.

Table 5: Truth table for $p \rightarrow q \wedge \sim r \leftrightarrow r \oplus q$

p	q	r	~ r	$q \wedge \sim r$	$r \oplus q$	$p \rightarrow q \wedge \sim r$	$p \rightarrow q \wedge \sim r \leftrightarrow r \oplus q$
T	T	T	F	F	F	F	T
T	T	F	T	T	T	T	T
T	F	T	F	F	T	F	F
T	F	F	T	F	F	F	T
F	T	T	F	F	F	T	F
F	T	F	T	T	T	T	T
F	F	T	F	F	T	T	T
F	F	F	T	F	F	T	F

***

You may now like to try some exercises on the same lines.

E12) In Example 3, how will the truth values of the compound statement change if you first apply $\leftrightarrow$ and then $\rightarrow$?

E13) In Example 3, if we replace $\oplus$ by $\wedge$, what is the new truth table?

E14) From the truth table of $p \wedge q \vee \sim r$ and $(p \wedge q) \vee (\sim r)$ and see where they differ.

E15) How would you bracket the following formulae to correctly interpret them? [For instance, $p \vee \sim q \wedge r$ would be bracketed as $p \vee ((\sim q) \wedge r)$.]

i) $p \vee q$,

ii) $\sim q \rightarrow \sim p$,

iii) $p \rightarrow q \leftrightarrow \sim p \vee q$,

iv) $p \oplus q \wedge r \rightarrow \sim p \vee q \leftrightarrow p \wedge r$.

So far we have considered different ways of making new statements from old ones. But, are all these new ones distinct? Or are some of them the same? And "same" in what way? This is what we shall now consider.

1.4 LOGICAL EQUIVALENCE

'Then you should say what you mean', the March Have went on. 'I do,' Alice hastily replied, 'at least … at least I mean what I say – that's the same thing you know.'
'Not the same thing a bit!' said the Hatter. 'Why you might just as well say that "I see what I eat" is the same thing as "I eat what I see"!'

-from 'Alice in Wonderland'
by Lewis Carroll

In Mathematics, as in ordinary language, there can be several ways of saying the same thing. In this section we shall discuss what this means in the context of logical statements.

Consider the statements 'If Lala is rich, then he must own a car.'. and 'if Lala doesn't own a car, then he is not rich.'. Do these statements mean the same thing? If we write the first one as $p \to q$, then the second one will be $(\sim q) \to (\sim p)$. How do the truth values of both these statements compare?

We find out in the following table.

Table 6

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

Consider the last two columns of Table 6. You will find that '$p \to q$' and '$q \to \sim p$' have the same truth value for every choice of truth values of p and q. When this happens, we call them equivalent statements.

Definition: We call two propositions r and s **logically equivalent** provided they have the same truth value for every choice of truth values of simple propositions involved in them. We denote this fact by $r \equiv s$.

So, from Table 6 we find that $(p \to q) \equiv (\sim q \to \sim p)$.

You can also check that $(p \leftrightarrow q) \equiv (q \leftrightarrow p)$ for any pair of propositions p and q.

As another example, consider the following equivalence that is often used in mathematics. You could also apply it to obtain statements equivalent to 'Neither a borrower, nor a lender be.'!

Example 4: For any two propositions p and q, show that $\sim (p \vee q) \equiv \sim p \wedge \sim q$.

Solution: Consider the following truth table.

Table 7

p	q	~ p	~ 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

Fig. 1: Augustus De Morgan (1806-1871) was born in Madurai

You can see that the last two columns of Table 7 are identical. Thus, the truth values of $\sim (p \vee q)$ and $\sim p \wedge \sim q$ agree for every choice of truth values of p and q. Therefore, $\sim (p \vee q) \equiv \sim p \wedge \sim q$.

***

The equivalence you have just seen is one of **De Morgan's laws.** You might have already come across these laws in your previous studies of basic Mathematics.

The other law due to De Morgan is similar : $\sim (p \wedge q) \equiv \sim p \vee \sim q$.

In fact, there are several such laws about equivalent propositions. Some of them are the following, where, as usual, p, q and r denote propositions.

a) **Double negation law** : $\sim (\sim p) \equiv p$
b) **Idempotent laws:** $p \wedge p \equiv p$, $p \vee p \equiv p$
c) **Commutativity:** $p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$
d) **Associativity:** $(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
e) **Distributivity:** $\vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

We ask you to prove these laws now.

E16) Show that the laws given in (a)-(e) above hold true.
E17) Prove that the relation of 'logical equivalence' is an equivalence relation.
E18) Check whether ($\sim p \vee q$) and ($p \rightarrow q$) are logically equivalent.

The laws given above and the equivalence you have checked in E18 are commonly used, and therefore, **useful to remember.** You will also be applying them in Unit 3 of this Block in the context of switching circuits.

Let us now consider some prepositional formulae which are always true or always false. Take, for instance, the statement 'If Bano is sleeping and Pappu likes ice-cream, then Beno is sleeping'. You can draw up the truth table of this compound proposition and see that it is always true. This leads us to the following definition.

Definition: A compound proposition that is true for all possible truth values of the simple propositions involved in it is called a **tautology.** Similarly, a proposition that is false for all possible truth values of the simple propositions that constitute it is called a **contradiction.**

Let us look at some example of such propositions.

Example 5: Verify that $p \wedge q \wedge \sim p$ is a contradiction and $p \rightarrow q \leftrightarrow \sim p \vee q$ is a tautology.

Solution: Let us simultaneously draw up the truth tables of these two propositions below.

Table 8

p	q	~ p	p ∧ q	p ∧ q ∧ ~ p	p → q	~ p ∨ q	p → q ↔ ~ p ∨ q
T	T	F	T	F	T	T	T
T	F	F	F	F	F	F	T
F	T	T	F	F	T	T	T
F	F	T	F	F	T	T	T

Looking at the fifth column of the table, you can see that $p \wedge q \wedge \sim p$ is a contradiction. This should not be surprising since $p \wedge q \wedge \sim p \equiv (p \wedge \sim p) \wedge q$ (check this by using the various laws given above).

And what does the last column of the table show? Precisely that $p \rightarrow q \leftrightarrow \sim p \vee q$ is a tautology.

***

Why don't you try an exercise now?

E19) Let T denote a tautology (i.e., a statement whose truth value is always T) and F a contradiction. Then, for any statement p, show that

i) $p \vee T \equiv T$
ii) $p \wedge T \equiv p$
iii) $p \vee F \equiv p$
iv) $p \wedge F \equiv F$

Another way of proving that a proposition is a tautology is to use the properties of logical equivalence. Let us look at the following example.

Example 6: Show that $[(p \rightarrow q) \wedge \sim q] \rightarrow \sim p$ is a tautology.

Solution: $[(p \rightarrow q) \wedge \sim q] \rightarrow \sim p$
$\equiv [(\sim p \vee q) \wedge \sim q] \rightarrow \sim p$, using E18, and symmetricity of $\equiv$.
$\equiv [(\sim p \wedge \sim q) \vee (q \wedge \sim q)] \rightarrow \sim p$, by De Morgan's laws.
$\equiv [(\sim p \wedge \sim q) \vee F] \rightarrow \sim p$, since $q \wedge \sim q$ is always false.
$\equiv (\sim p \wedge \sim q) \rightarrow \sim p$, using E18.

Complementation law:
$q \wedge \sim q$ is a contradiction.

Which is tautology.

And therefore the proposition we started with is a tautology.

***

The laws of logical equivalence can also be used to prove some other logical equivalences, without using truth tables. Let us consider an example.

Example 7: Show that $(p \rightarrow \sim q) \wedge (p \rightarrow \sim r) \equiv \sim [p \wedge (q \vee r)]$.

Solution: We shall start with the statement on the left hand side of the equivalence that we have to prove. Then, we shall apply the laws we have listed above, or the equivalence in E 18, to obtain logically equivalent statements. We shall continue this process till we obtain the statement on the right hand side of the equivalence given above. Now

$(p \rightarrow \sim q) \wedge (p \rightarrow \sim r)$
$\equiv (\sim p \vee q) \wedge (\sim p \vee \sim r)$, by E18
$\equiv \sim p \vee (\sim q \wedge \sim r)$, by distributivity
$\equiv \sim p \vee [\sim (q \vee r)]$, by De Morgan's laws
$\equiv \sim [p \wedge (q \vee r)]$, by De Morgan's laws

So we have proved the equivalence that we wanted to.

***

You may now like to try the following exercises on the same lines.

E20) Use the laws given in this section to show that
$\sim (\sim p \wedge q) \wedge (p \vee q) \equiv p$.

E21) Write down the statement 'If it is raining and if rain implies that no one can go to see a film, then no one can go to see a film.' As a compound proposition. Show that this proposition is a tautology, by using the properties of logical equivalence.

E22) Give an example, with justification, of a compound proposition that is neither a tautology nor a contradiction.

Let us now consider proposition-valued functions.

1.5 LOGICAL QUANTIFIERS

In Sec. 1.2, you read that a sentence like 'She has gone to Patna.' Is not a proposition, unless who 'she' is clearly specified.
Similarly, 'x > 5' is not a proposition unless we know the values of x that we are considering. Such sentences are examples of 'propositional functions'.

Definition: A propositional function, or a **predicate,** in a variable x is a sentence p(x) involving x that becomes a proposition when we give x a definite value from the set of values it can take. We usually denote such functions by p(x), q(x), etc. The set of values x can take is called the universe of discourse.

So, if p(x) is 'x > 5', then p(x) is not a proposition. But when we give x particular values, say x = 6 or x = 0, then we get propositions. Here, p(6) is a true proposition and p(0) is a false proposition.

Similarly, if q(x) is 'x has gone to Patna.', then replacing x by 'Taj Mahal' gives us a false proposition.

Note that a predicate is usually not a proposition. But, of course, every proposition is a prepositional function in the same way that every real number is a real-valued function, namely, the constant function.

Now, can all sentences be written in symbolic from by using only the logical connectives? What about sentences like 'x is prime and x + 1 is prime for some x.'? How would you symbolize the phrase 'for some x', which we can rephrase as 'there exists an x'? You must have come across this term often while studying mathematics. **We use the symbol '∃' to denote this quantifier, 'there exists'.** The way we use it is, for instance, to rewrite 'There is at least one child in the class.' as'(∃ x in U)p(x)', where p(x) is the sentence 'x is in the class.' and U is the set of all children.

∃ is called the **existential quantifier.**

Now suppose we take the negative of the proposition we have just stated. Wouldn't it be 'There is no child in the class.'? We could symbolize this as 'for all x in U, q(x)' where x ranges over all children and q(x) denotes the sentence 'x is not in the class.', i.e., $q(x) \equiv \sim p(x)$.

We have a **mathematical symbol for the quantifier 'for all', which is '∀'.** So the proposition above can be written as

∀ is called the **universal quantifier**.

'$(\forall x \in U)q(x)$', or '$q(x), \forall x \in U$'.

An example of the use of the existential quantifier is the true statement.

$(\exists x \in \mathbf{R})\ (x + 1 > 0)$, which is read as 'There exists an x in **R** for which x + 1 > 0.'.

Another example is the false statement

$(\exists x \in \mathbf{N})\ (x - \frac{1}{2} = 0)$, which is read as 'There exists an x in **N** for which $x - \frac{1}{2} = 0$.'.

An example of the use of the universal quantifier is $(\forall x \notin \mathbf{N})\ (x^2 > x)$, which is read as 'for every x not in **N**, $x^2 > x$.'. Of course, this is a false statement, because there is at least one $x \notin \mathbf{N}$, $x \in \mathbf{R}$, for which it is false.

We often use both quantifiers together, as in the statement called **Bertrand's postulate:**

$(\forall n \in \mathbf{N} \setminus \{1\})\ (\exists x \in \mathbf{N})$ (x is a prime number and $n < x < 2n$).

In words, this is 'for every integer n > 1 there is a prime number lying strictly between n and 2n.'

As you have already read in the example of a child in the class,
$(\forall x \in U)p(x)$ is logically equivalent to $\sim (\exists x \in U)(\sim p(x))$. Therefore,
$\sim(\forall x \in U)p(x) \equiv \sim\sim (\exists x \in U)(\sim p(x)) \equiv (\exists x \in U)(\sim p(x))$.

This is one of the rules for negation that relate $\forall$ and $\exists$. The two rules are

$\sim (\forall \mathbf{x} \in \mathbf{U})\mathbf{p(x)} \equiv (\exists x \in \mathbf{U})$ **(~ p(x)),** and

$\sim (\exists \mathbf{x} \in \mathbf{U})\mathbf{p(x)} \equiv (\forall x \in \mathbf{U})$ **(~ p(x))**

Where U is the set of values that x can take.

Now, consider the proposition

'There is a criminal who has committed every crime.'

We could write this in symbols as

$(\exists c \in A)(\forall x \in B)$ (c has committed x)

Where, of course, A is the set of criminals and B is the set of crimes (determined by law).

What would its negation be? It would be

$\sim (\exists c \in A)(\forall x \in B)$ (c has committed x)

Where, of course, A is the set of criminals and B is the set of crimes (determined by law).

What would its negation be? It would be

$\sim (\exists c \in A)(\forall x \in B)$ (c has committed x)

$\equiv (\forall c \in A)[\sim (\forall x \in B)$ (c has committed x)

$\equiv (\forall c \in A)(\exists x \in B)$ (c has not committed x).

We can interpret this as 'For every criminal, there is a crime that this person has not committed.'.

A predicate can be a function in two **or more** variables.

These are only some examples in which the quantifiers occur singly, or together. Sometimes you may come across situations (as in E23) where you would use $\exists$ or $\forall$ twice or more in a statement. It is in situations like this or worse [say, $(\forall x_i \in U_1)(\exists x_2 \in U_2)(\exists x_3 \in U_2)(\exists x_3 \in U_3)(\forall x_4 \in U_4) \ldots (\exists x_n \in U_n)p$]
where our rule for negation comes in useful. In fact, applying it, in a trice we can say that the negation of this seemingly complicated example is

$(\exists x_1 \in U_1)(\forall x_2 \in U_2)(\forall x_3 \in U_3)(\exists x_4 \in U_4) \ldots (\forall x_n \in U_n)(\sim p)$.

Why don't you try some exercise now?

E23) How would you present the following propositions and their negations using logical quantifiers? Also interpret the negations in words.

i) The politician can fool all the people all the time.

ii) Every real number is the square of some real number.

iii) There is lawyer who never tell lies.

E24) Write down suitable mathematical statements that can be represented by the following symbolic propostions. Also write down their negations. What is the truth value of your propositions?

i) $(\forall x)(\exists y)p$

ii) $(\exists x)(\exists y)(\forall z)p$.

And finally, let us look at a very useful quantifier, which is very closely linked to ∃. You would need it for writing, for example, 'There is one and only one key that fits the desk's lock.' In symbols. The symbol is ∃! X which stands for **'there is one and only one x'** (which is the same as **'there is a unique** x' or **'there is exactly one** x').

So, the statement above would be (∃! X ∈ A) (x fits the desk's lock), where A is the set of keys.

For other examples, try and recall the statements of uniqueness in the mathematics that you've studied so far. What about 'There is a unique circle that passes through three non-collinear points in a plane.'? How would you represent this in symbols? If x denotes a circle, and y denotes a set of 3 non-collinear points in a plane, then the proposition is

(∀ y ∈ P) (∃! X ∈ C) (x passes through y).

Here C denotes the set of circles, and P the set of sets of 3 non-collinear points.
And now, some short exercises for you!

E25) Which of the following propositions are true (where x, y are in R)?
i) $(x \geq 0) \rightarrow (\exists\, y)\ (y^2 = x)$
ii) $(\forall\, x)\ (\exists!\, y)\ (y^2 = x^3)$
iii) $(\exists x)\ (\exists!\, y)\ (xy = 0)$

Before ending the unit, let us take quick look at what e have covered in it.

1.6 SUMMARY

In this unit, we have considered the following points.

1. What a mathematically acceptable statement (or proposition) is.
2. The definition and use of logical connectives:
   Give propositions p and q,
   i) their disjunction is 'p and q', denoted by $p \vee q$;
   ii) their exclusive disjunction is 'either p or q', denoted by $p \oplus q$;
   iii) their conjunction is 'p and q', denoted by $p \wedge q$;
   iv) the negation of p is 'not p', denoted by $\sim p$;
   v) 'if p, then q' is denoted by $p \rightarrow q$;
   vi) 'p if and only if q' is denoted by $p \leftrightarrow q$;
3. The truth tables corresponding to the 6 logical connectives.
4. Rule of precedence : In any compound statement involving more than one connective, we first apply '$\sim$', then '$\wedge$', then '$\vee$' and '$\oplus$', and last of all '$\rightarrow$' and '$\leftrightarrow$'.
5. The meaning and use of logical equivalence, denoted by '$\equiv$'.
6. The following laws about equivalent propositions:
   i) **De Morgan's laws:** $\sim (p \wedge q) \equiv \sim p \vee \sim q$
   $\sim (p \vee q) \equiv \sim p \wedge \sim q$
   ii) **Double negation law:** $\sim (\sim p) \equiv p$
   iii) **Idempotent laws:** $p \wedge p \equiv p$,
   $p \vee p \equiv p$
   iv) **Commutativity:** $p \vee q \equiv q \vee p$
   $p \wedge q \equiv q \wedge p$
   v) **Associativity:** $(p \vee q) \vee r \equiv p \vee (q \vee r)$
   $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
   vi) **Distributivity:** $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
   $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

vii) $(\sim p \vee q) \equiv p \rightarrow q$ (ref. E18).

7. Logical quantifiers: 'For every' denoted by '$\forall$', 'there exist' denoted by '$\exists$', and 'there is one and only one' denoted by '$\exists!$'.
8. The rule of negation related to the quantifiers:
   $\sim (\forall x \in U) p(x) \equiv (\exists x \in U) (\sim p(x))$
   $\sim (\exists x \in U) p(x) \equiv (\forall x \in U) (\sim p(x))$

Now we have come to the end of this unit. You should have tried all the exercises as you came to them. You may like to check your solutions with the ones we have given below.

1.7 SOLUTIONS/ ANSWERS

E1) (i), (iii), (iv), (vii), (viii) are statements because each of them is universally true or universally false.
(ii) is a question.
(v) is an exclamation.
The truth or falsity of (vi) depends upon who 'she' is.
(ix) is a subjective sentence.
(x) will only be a statement if the value(s) n takes is/are given.
Therefore, (ii), (v), (vi), (ix) and (x) are not statements.

E2) The truth value of (i) is F, and of all the others is T.

E3) The disjunction is
'2+3 = 7 or Radha is an engineer.'.
Since '2+3 = 7' is always false, the truth value of this disjunction depends on the truth value of 'Radha is an engineer.'. If this is T, them we use the third row of Table 1 to get the required truth value as T. If Radha is not an engineer, then we get the required truth value as F.

Table 9: Truth table for 'exclusive or'

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

E4) p will be a true proposition for $x \in]-2, \infty[$ and $x \neq 4$, i.e., for $x \in]-2, 4[\cup]4, \infty[$.

E5) i) $0 - 5 = 5$
ii) 'n is not greater than 2 for every $n \in \mathbf{N}$.', or 'There is at least one n $n \in \mathbf{N}$ for which $n \leq 2$.'
iii) There are some Indian children who do not study till Class 5.

E6)

Table 10: Truth table for negation

p	~ p
T	F
F	T

E7) $p \rightarrow q$ is the statement 'If $x + y = xy$ for $x, y \in R$, then $x \not\subset 0$ for every $\in \mathbf{Z}$'.

In this case, q is false. Therefore, the conditional statement will be true if p is false also, and it will be false for those values of x and y that make p true.

So, $p \to q$ is false for all those real numbers x of the form $\frac{y}{y-1}$, where

$y \in \mathbf{R} \setminus \{1\}$. This is because if $x = \frac{y}{y-1}$ for some $y \in \mathbf{R} \setminus \{1\}$, then $x + y = xy$,

i.e., p will be true.

E8) i) $p \to q$, where p : ΔABC is isosceles. If q is true, then $p \to q$ is true. If q is false, then $p \to q$ is true only when p is false. So, if ΔABC is an isosceles triangle, the given statement is always true. Also, if ΔABC is not isosceles, then it can't be equilateral either. So the given statement is again true.

ii) p : a is an integer.
q : b is an integer.
r : ab is a rational number
The given statement is $(p \wedge q) \leftrightarrow r$.
Now, if p is true and q is true, then r is still true.

So, $(p \wedge q) \leftrightarrow r$ will be true if $p \wedge q$ is true, or when $p \wedge q$ is false and r is false.
In all the other cases $(p \wedge q) \leftrightarrow r$ will be false.

iii) p : Raza has 5 glasses of water.
q : Sudha has 4 cups of tea.
r : Shyam will pass the math exam.

The given statement is $(p \wedge q) \to \sim r$.
This is true when $\sim r$ is true, or when r is true and $p \wedge q$ is false.
In all the other cases it is false.

iv) p : Mariam is in Class 1.
q : Mariam is in Class 2.

The given statement is $p \oplus q$.
This is true only when p is true or when q is true.

E9) There are infinitely many such examples. You need to give one in which p is true but q is false.

E10) Obtain the truth table. The last column will now have entries TTFTTTTT.

E11) According to the rule of precedence, given the truth values of p, q, r you should first find those of $\sim r$, then of $q \wedge \sim r$, and $r \wedge q$, and $p \to q \wedge \sim r$, and finally of $(p \to q \wedge \sim r) \leftrightarrow r \wedge q$.

Referring to Table 5, the values in the sixth and eighth columns will be replaced by

$r \wedge q$
T
F
F
F
T
F
F
F

$p \to q \wedge \sim r \leftrightarrow r \wedge q$
F
F
T
T
T
F
F
F

E12) They should both be the same, viz.,

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

E13) i) $(\sim p) \vee q$
ii) $(\sim q) \rightarrow (\sim p)$
iii) $(p \rightarrow q) \leftrightarrow [(\sim p) \vee q]$
iv) $[(p \oplus (q \wedge r) \rightarrow [(\sim p) \vee q]] \leftrightarrow (p \wedge r)$

E14) a)

p	~ p	~ (~ p)
T	F	T
F	T	F

The first and third columns prove the double negation law.

b)

p	q	p ∨ q	q ∨ p
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

The third and fourth columns prove the commutativity of ∨.

E15) For any three propositions p, q, r:
i) $p \equiv p$ is trivially true.
ii) if $p \equiv q$, then $q \equiv p$ (if p has the same truth value as q for all choices of truth values of p and q, then clearly q has the same truth values as p in all the cases.
iii) if $p \equiv q$ and $q \equiv r$, then $p \equiv r$ (reason as in (ii) above).

Thus, ≡ is reflexive, symmetric and transitive.

E16)

p	q	~ p	~ p ∨ q	p → q
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

The last two columns show that $[(\sim p) \vee q] \equiv (p \rightarrow q)$.

E17) i)

p	$\mathcal{T}$	$p \vee \mathcal{T}$
T	T	T
F	T	T

The second and third columns of this table show that $p \vee \mathcal{T} = T$.

ii)

p	$\mathcal{F}$	$p \wedge \mathcal{F}$
T	F	F
F	F	F

The second and third columns of this table show that $p \wedge \mathcal{F} = F$.
You can similarly check (ii) and (iii).

E18) $\sim (\sim p \wedge q) \wedge (p \vee q)$
$\equiv (\sim(\sim p) \vee \sim q) \wedge (p \wedge q)$, by De Morgan's laws.
$\equiv (p \vee \sim q) \wedge (p \vee q)$, by the double negation law.
$\equiv p \vee (\sim q \wedge q)$, by distributivity
$\equiv p \vee \mathcal{F}$, where $\mathcal{F}$ denotes a contradiction
$\equiv p$, using E 19.

E19) p: It is raining.
q: Nobody can go to see a film.
Then the given proposition is
$[p \wedge (p \rightarrow q)] \rightarrow q$
$\equiv p \wedge (\sim p \vee q) \rightarrow q$, since $(p \rightarrow q) \equiv (\sim p \vee q)$
$\equiv (p \wedge \sim p) \vee (p \wedge q) \rightarrow q$, by De Morgan's law
$\equiv \mathcal{F} \vee (p \wedge q) \rightarrow q$, since $p \wedge \sim p$ is a contradiction
$\equiv (\mathcal{F} \vee p) \wedge (F \vee q) \rightarrow q$, by De Morgan's law
$\equiv p \wedge q \rightarrow q$, since $\mathcal{F} \vee p \equiv p$.
which is a tautology.

E20) There are infinitely many examples. One such is:
'If Venkat is on leave, then Shabnam will work on the computer'.This is of the form $p \rightarrow q$. Its truth values will be T or F, depending on those of p and q.

E21) i) $(\forall\, t \in [0, \infty[)\ (\forall\, x \in H)p(x,t)$ is the given statement where p(x, t) is the predicate 'The politician can fool x at time t second.', and H is the set of human beings.
Its negation is $(\exists\, t \in [0, \infty[)\ (\exists\, x \in \mathbf{H})\ (\sim p(x, t))$, i.e., there is somebody who is not fooled by the politician at least for one moment.

ii) The given statement is
$(\forall\, x \in \mathbf{R})\ (\exists\, y \in \mathbf{R})\ (x = y^2)$. Its negation is
$(\exists\, x \in \mathbf{R})\ (\forall\, y \in \mathbf{R})\ (x \neq y^2)$, i.e.,
there is a real number which is not the square of any real number.

iii) The given statement is
$(\exists\, x \in L)\ (\forall\, t \in [0, \infty[)p(x, t)$, where L is the set of lawyers and p(x, t) : x does not lie at time t. The negation is
$(\forall\, x \in L)\ (\exists\, t \in [0, \infty[)\ (\sim p)$, i.e., every lawyer tells a lie at some time.

E22) i) For example,

$(\forall\, \mathbf{x} \in \mathbf{N})\ (\exists\, y \in \mathbf{Z})\ (\frac{x}{y} \in \mathbf{Q})$ is a true statement. Its negation is

$\exists\, \mathbf{x} \in \mathbf{N})\ (\forall\, y \in \mathbf{Z})\ (\frac{x}{y} \notin \mathbf{Q})$

You can try (ii) similarly.

E23) (i), (iii) are true.
(ii) is false (e.g., for x = -1 there is no y such that $y^2 = x^3$).

(iv) is equivalent to ($\forall$ x $\in$ **R**) [~ ($\exists!$ y $\in$ **R**) (x + y = 0)], i.e., for every x there is no unique y such that x + y = 0. This is clearly false, because for every x **there is** a unique y(= - x) such that x + y = 0.

UNIT 2 METHODS OF PROOF

Structure

2.0 INTRODUCTION

In the previous unit you studied about statements and their truth values. In this unit, we shall discuss ways in which statements can be linked to form a logically valid argument. Throughout your mathematical studies you would have come across the terms 'theorem' and 'proof'. In sec. 2.2, we shall talk about what a theorem is and what constitutes a mathematically acceptable proof.

Fig. 1: George Boole (1815-1864)

In Sec 2.3, we shall discuss some ideas formalised by the English mathematician Boole and the German logician Frege (1848-1925). These are the different methods used for proving or disproving a statement. As you go through the different types of **valid arguments,** please try and find connections with what we discussed in Block 1.

The principle of mathematical induction has a very special place in mathematics because of its simplicity and vast applicability. You will revisit this tool for proving statements in sec. 2.4.

Please go through this unit carefully. You need to be able to convince your learners that its contents are part of the foundation on which all mathematical knowledge is built.

2.1 OBJECTIVES

After reading this unit, you should be able to develop in your learners the ability to:

- explain the terms 'theorem', 'proof' and 'disproof';
- describe the direct method and some indirect methods of proof;
- state and apply both forms of the principle of induction

2.2 WHAT IS A PROOF?

Suppose I tell somebody, "I am stronger than you." The person is quite likely to turn around, look menacingly at me, and say, "Prove it!" What she or he really wants is to be convinced of my statement by some evidence. (In this case it would probably be a big physical push!)

Convincing evidence is also what the world asks for before accepting a scientist's predictions, or a historian's claims.

In the same way, if you want a mathematical statement to be accepted as true, you would need to provide **mathematically acceptable** evidence to support it. This means

that you would need to show that the statement is **universally** true. And this would be done in the form of a logically valid argument.

Definition: An **argument** (in mathematics or logic) is a finite sequence of statements $p_1 , \cdots , p_n , p$ such that $(p_1 \wedge p_2 \wedge \cdots \wedge p) \rightarrow p$.

Each statement in the sequence, $p_1 , p_2 , \ldots , p_n$ is called a **premise** (or an **assumption,** or a **hypothesis**). The final statement p is called the **conclusion.**

Let's consider an example of an argument that shows that a given statement is true.

Example 1: Give an argument to show that the mathematical statement 'For any two sets A and B, $A \cap B \subseteq A$' is true.

Solution: One argument could be the following.
Let x be an arbitrary element of $A \cap B$.
Then $x \in A$ and $x \in B$, by definition of '$\cap$'.
Therefore, $x \in A$.
This is true for every x in $A \cap B$.
Therefore, $A \cap B \subseteq A$, by definition of `$\subseteq$'.

***

The argument in Example 1 has a peculiar nature. The truth of each of the 4 premises and of its conclusion follows from the truth of the earlier premises in it. Of course, we start by assuming that the first statement is true. Then, assuming the definition of `intersection', the second statement is true. The third one is true, whenever the second one is true because of the properties of logical implication. The fourth statement is true whenever the first three are true, because of the definition and properties of the term `for all'. And finally, the last statement is true whenever all the earlier ones are. In this way we have shown that the given statement is true. In other words, we have proved the given statement, as the following definition show.

Definitions: We say that a proposition p **follows logically from** propositions $p_1 , p_2 , \cdots , p_n$ if p must be true whenever $p_1 , p_2 , \cdots , p_n$ are true, i.e., $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \Rightarrow p$.
[Here, **note** the use of the implication arrow `$\Rightarrow$'. For any two propositions r and s, `$r \Rightarrow s$' **denotes 's is true whenever r is true.'** Note that, using the contrapositive, this also denotes `r is false whenever s is false'. Thus `$r \rightarrow s$' and `$r \Rightarrow s$' are different except when both r and s are true or both are false.]

A **proof** of a proposition p is a mathematical argument consisting of a sequence of statements $p_1 , p_2 , \cdots , p_n$ from which p logically follows. So, p is the conclusion of this argument.

The statement that is proved to be true is called a **theorem.**

Sometimes, as you will see in Sec.2.3.3, instead of showing that a statement p is true, we try to prove that it is false, i.e., that ~ p is true. Such a proof is called a **disproof** of p. In the next section you will read about some ways of disproving a statement.

Sometimes it happens that we feel a certain statement is true, but we don't succeed in proving it. It may also happen that we can't disprove it. Such statements are called **conjectures.** If and when a conjecture is proved, it would be called a theorem. If it is disproved, then its negative will be a theorem!

In this context, there's a very famous conjecture which was made by a mathematician **Goldbach** in 1742. He stated that :

For every $n \in N$. If n is even and $n > 2$, then n is the sum of two primes.
To this day, no one has been able to prove it or disprove it. To disprove it several people have hunting for an example for which the statement is not true, i.e., an even number n>2 such that n cannot be written as the sum of two prime numbers.

Now, as you have seen, a mathematical proof of a statement consists of one or more premises. These premises could be of four types:

i) a proposition that has been proved earlier (e.g., to prove that the complex roots of a polynomial in **R**[x] occur in pairs, we use the division algorithm); or
ii) a proposition that follows logically from the earlier propositions given in the proof (as you have seen in Example 1); or
iii) a mathematical fact that has never been proved, but is universally accepted as true (e.g., two points determine a line). Such a fact is called an **axiom** (or a **postulate**);
iv) the definition of a mathematical term (e.g., assuming the definition of '$\subseteq$' in the proof of $A \cap B \subseteq A$).

You will come across more examples of each type while doing the following exercises, and while going through proofs in this course and other course.

E1) Write down an example of a theorem, and its proof (of at least 4 steps), taken from school-level algebra. At each step, indicate which of the four types of premise it is.
E2) Is every statement a theorem? Why?

So far we have spoken about valid, or acceptable, arguments. Now let us see an example of a sequence of statements that will not form a valid argument. Consider the following sequence.

If Maya sees the movie, she won't finish her homework.
Maya won't finish her homework.
Therefore, Maya sees the movie.

Looking at the argument, can you say whether it is valid or not? Intuitively you may feel that the argument isn't valid. But, is there a formal logical tool that you can apply check if your intuition is correct? What about truth tables? Let's see.

The given argument is of the form
$[(p \rightarrow q) \wedge q] \Rightarrow p$, where
p: Maya sees the movie, and
q: Maya won't finish here homework.

Let us look at the truth table related to this argument (see Table 1).

Table 1.

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

This last column gives the truth values of the premises. The first column given corresponding truth values of the conclusion. **Now, the argument will only be valid if whenever both the premises are true, the conclusion is true.** This happens in the first row, but not in the third row. **Therefore, the argument is** not valid.

Why don't you check an argument for validity now?

E3) Check whether the following argument is valid
$(p \rightarrow q \vee \sim r) \wedge (q \rightarrow p) \Rightarrow (p \rightarrow r)$

You have seen that a proof is a logical argument that verifies the truth of a theorem. There are several ways of proving a theorem, as you will see in the next section. All of them are based on one or more **rules of inference**, which are different forms of arguments. We shall now present four of the most commonly used rules.

i) Law of detachment (or modus ponens)
Consider the following argument:

'Modus ponens' is a Latin term which means 'method of affirmation'.

If Kali can draw, she will get a job.
Kali can draw.
Therefore, she will get a job.

To study the form of the argument, let us take p to be the proposition 'Kali can draw'. And q to be the proposition 'Kali will get a job.' Then the premises are $(p \rightarrow q)$ and p. The conclusion is q.

So, the form of the argument is
$p \rightarrow q$
$\frac{p}{\therefore q}$, i.e., $[(p \rightarrow q) \wedge p] \Rightarrow q$.

$\therefore$ denotes 'therefore'.

Is this argument valid? To find out, let's construct its truth table (see Table 2).

Table 2: Truth table for $[(p \rightarrow q) \wedge p] \Rightarrow q$

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

In the table, look at the second column (the conclusion) and the fourth column (the premises). Whenever the premises are true, i.e., in Row 1, the conclusion is true. Therefore, the argument is valid.

This form of valid argument is called the law of detachment because the conclusion q is detached from a premise (namely, $p \rightarrow q$). It is also called the **law of direct inference**.

ii) Law of contraposition (or modus tollens)
To understand this law, consider the following argument:

'Modus tollens' means 'method of denial'.

If Kali can draw, then she will get a job.
Kali will not get a job.
Therefore, Kali can't draw.

Taking p and q as in (i) above, you can see that the premises are $p \rightarrow q$ and $\sim q$. The conclusion is $\sim p$

So the argument is
$p \rightarrow q$
$\sim q$, i.e., $[(p \rightarrow q) \wedge \sim] \Rightarrow \sim p$.

If you check, you'll find that this is a valid form of argument. There are two more rules of inference that most commonly form the basis of several proofs. The following exercise is about them.

E4) You will find three arguments below. Convert each of them into the language of symbols, and check if they are valid.

i) Either the eraser is white or oxygen is a metal.
The eraser is black.
Therefore, oxygen is a metal.

ii) If madhu is a 'sarpanch', she will head the 'panchayat'.
If Madhu heads the 'panchayat', she will decide on property disputes.
Therefore, if Madhu is a 'sarpanch', she will decide on property disputes.

iii) Either Munna will cook or Munni will practise Karate.
If Munni practices Karate, then Munna studies.
Munna does not study.
Therefore, Munni will practise Karate.

E5) Write down one example each of modus ponens and modus tollens.

As you must have discovered, the arguments in E4(i) and (ii) are valid. The first one is an example of a **disjunctive syllogism**. The second one is an example of a **hypothetical syllogism.**

Thus, a disjunctive syllogism is of the form

$p \vee q$

$\sim \dfrac{p}{q}$ i.e., $[(p \vee q) \wedge \sim p] \Rightarrow q$.

And, a hypothetical syllogism is of the form

$p \rightarrow q$

$q \rightarrow r$, i.e., $[(p \rightarrow q) \wedge (q \rightarrow r)] \Rightarrow (p \rightarrow r)$.

$\overline{p \rightarrow r}$

Let us now see how different forms of arguments can be put together to prove or disprove a statement.

2.3 DIFFERENT METHODS OF PROOF

In this section we shall consider three different strategies for proving a statement. We will also discuss a method that is used only for disproving a statement.

Let us start with a proof strategy based on the first rule of inference that we discussed in the previous section.

2.3.1 Direct Proof

This form of proof is based entirely on modus ponens. Let us formally spell out the strategy.

Definition: A direct proof of $p \Rightarrow q$ is a logically valid argument that begins with the assumptions that p is true and, in one or more applications of the law of detachment, concludes that q must be true.

So, to construct a direct proof of $p \Rightarrow q$, we start by assuming that p is true. Then, in one or more steps of the form $p \Rightarrow q_1$, $q_1 \Rightarrow q_2$, ……., $q_n \Rightarrow q$, we conclude that q is true. Consider the following examples.

Example 2: Give a direct proof of the statement 'The product of two odd integers is odd'.

Solution: Let us clearly analyse what our hypotheses are, and what we have to prove. We start by considering any two odd integers x and y. So our hypothesis is p: x and y are odd.

The conclusion we want to reach is
q : xy is odd.
Let us first prove that $p \Rightarrow q$.
Since x is odd, $x = 2m + 1$ for some integer m.
Similarly, $y = 2n + 1$ for some integer n.
Then $xy = (2m + 1)(2n + 1) = 2(2mn + m + n) + 1$
Therefore, xy is odd.
So we have shown that $p \Rightarrow q$.

Now we can apply modus ponens to $p \wedge (p \Rightarrow q)$ to get the required conclusion.

Note that the essence of this direct proof lies in showing $p \Rightarrow q$.

***

Example 3: Give a direct proof of the theorem 'The square of an even integer is an even integer.'

Solution: First of all, let us write the given statement symbolically, as
$(\forall x \in \mathbf{Z})(p(x) \Rightarrow q(x))$
where p(x) : x is even, and
q(x) : x^2 is even, i.e., q(x) is the same as p (x^2).

The direct proof, then goes as follows.

Let x be an even number (i.e., we assume p(x) is true).
Then $x = 2n$, for some integer n (we apply the definition of an even number).
Then $x^2 = (2n)^2 = 4n^2 = 2(2n^2)$.
x^2 is even (i.e., q (x) is true).

***

Why don't you try an exercise now?

E6) Give a direct proof of the statement 'If x is a real number such that $x^2 = 9$, then either x=3 or x = -3. '.

Let us now consider another proof strategy.

2.3.2 Indirect Proofs

In this sub-section we shall consider two roundabout methods for proving $p \Rightarrow q$.

Proof by contrapositive: In the first method, we use the fact that the proposition $p \Rightarrow q$ is logically equivalent to its contrapositive ($\sim q \Rightarrow \sim p$),
i.e.,

$$(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p).$$

For instance, 'If Ammu does not agree with communalists, then she is not orthodox.' is the same as 'If Ammu is orthodox, then she agrees with communalists.'.

Because of this equivalence, to prove $p \Rightarrow q$, we can, instead, prove $\sim q \Rightarrow \sim p$. This means that we can assume that $\sim q$ is true, and then try to prove that $\sim p$ is true. In other words, **what we do to prove $p \Rightarrow q$ in this method is to assume that q is false and then show that p is false.** Let us consider an example.

Example 4: Prove that 'If $x, y \in \mathbf{Z}$ such that xy is odd, then both x and y are odd.', by proving its contrapositive.

Solution: Let us name the statements involved as below.
p : xy is odd
q : both x and y are odd.
So,
$\sim p$: xy is even, and
$\sim q$: x is even or y is even, or both are even.

We want to prove $p \Rightarrow q$, by proving that $\sim q \Rightarrow \sim p$. So we start by assuming that $\sim q$ is true, i.e., we suppose that x is even.

The $x = 2n$ for some $n \in \mathbf{N}$.
Therefore, $xy = 2ny$.
Therefore xy is even, by definition.
That is, $\sim p$ is true.

So, we have shown that $\sim q \Rightarrow \sim p$. Therefore, $p \Rightarrow q$.

Why don't you ask your students to try some related exercises now?

E7) Write down the contrapositive of the statement 'If f is a 1-1 function from a finite set X into itself, then f must be subjective.'.

E8) Prove the statement 'If x is an integer and x^2 is even, then x is also even.' By proving its contrapositive.

And now let us consider the other way of proving a statement indirectly.

Proof by contradiction: In this method, to prove q is true, we start by assuming that q is false (i.e., $\sim q$ is true). Then, by a logical argument we arrive at a situation where a statement is true as well as false, i.e., we reach a contradiction $r \wedge \sim r$ for some statement that is always false. This can only happen when $\sim q$ is false also. Therefore, q must be true.

This method is called **proof by contradiction**. It is also called reductio ad absurdum (a Latin phrase) because it relies on reducing a given assumption to an absurdity.

Let us consider an example of the use of this method.

Example 5: Show that $\sqrt{5}$ is irrational.

Solution: Let us try and prove the given statement by contradiction. For this, we begin by assuming that $\sqrt{5}$ is rational. This means that there exist positive integers a and b such that $\sqrt{5} = \frac{a}{b}$, where a and b have no common factors.

This implies $a = \sqrt{5}\, b \Rightarrow a^2 = 5b^2 \Rightarrow 5 | a^2 \Rightarrow 5 | a$.

Therefore, by definition, $a = 5c$ for some $c \in \mathbf{Z}$.
Therefore, $a^2 = 25c^2$.

But $a^2 = 5b^2$ also.

So $25c^2 = 5b^2 \Rightarrow 5c^2 = b^2 \Rightarrow 5 \mid b^2 \Rightarrow 5 \mid b$.

But now we find that 5 divides both a and b, which contradicts our earlier assumption that a and b have no common factor.

Therefore, we conclude that our assumption that $\sqrt{5}$ is rational is false, i.e, $\sqrt{5}$ is irrational.

***

We can also use the method of contradiction to prove an implication $r \Rightarrow s$. Here we can use the equivalence $\sim (r \rightarrow s) \equiv r \wedge \sim s$. So, to prove $r \Rightarrow s$, we can begin by assuming that $r \Rightarrow s$ is false, i.e., r is true and s is false. Then we can present a valid argument to arrive at a contradiction.

Consider the following example from plane geometry.

Example 6: Prove the following:
If two distinct lines L_1 and L_2 intersect, then their intersection consists of exactly one point.

Solution: To prove the given implication by contradiction, let us begin by assuming that the two distinct lines L_1 and L_2 intersect in more than one point. Let us call two of these distinct points A and B. Then, both L_1 and L_2 contain A and B. This contradicts the axiom from geometry that says 'Given two distinct points, there is exactly one line containing them.'.

Therefore, if L_1 and L_2 intersect, then they must intersect in only one point.

***

The contradiction rule is also used for solving many logical puzzles by discarding all solutions that educe to contradictions. Consider the following example.

Example 7: There is a village that consists of two types of people – those who always tell the truth, and those who always lie. Suppose that you visit the village and two villagers A and B come up to you. Further, suppose
A says, "B always tells the truth," and
B says, "A and I are of opposite types".
What types are A and B ?

Solution: Let us start by assuming A is a truth-teller.
∴ What A says is true.
∴ B is a truth-teller.
∴ What B says is true.
∴ A and B are of opposite types.

This is a contradiction, because our premises say that A and B are both truth-tellers.
∴ The assumption we started with is false.
∴ A always tells lies.
∴ What A has told you is lie.
∴ B always tells lies.
∴ A and B are of the same type, i.e., both of them always lie.

***

Here are a few exercises for you now. While doing them you would realize that there are situations in which all the three methods of proof we have discussed so far can be used.

E9) Use the method of proof by contradiction to show that
ii) For $x \in \mathbf{R}$, if $x^3 + 4x = 0$, then $x = 0$

E10) Prove E 9(ii) directly as well as by the method of contrapositive.

E11) Suppose you are visiting the village described in Example 7 above. Another two villagers C and D approach you. C tells you, "Both of us always tell the truth," and D says, "C always lies." What types are C and D?

There can be several ways of proving a statement.

Let us now consider the problem of showing that a statement is false.

2.3.3 Counterexamples

Suppose I make the statement 'All human beings are 5 feet tall.'. You are quite likely to show me an example of a human being standing nearby for whom the statement is not true. And, as you know, the moment we have even one example for which the statement $(\forall x)p(x)$ is false [i.e.,$(\exists x)\ (\sim p(x))$ is true], then the statement is false.

An example that shows that a statement is false is a **counterexample** to such a statement. The name itself suggests that it is an example to counter a given statement.

A common situation in which we look for counterexamples is to disprove statements of the form $p \rightarrow q$ needs to be an example where $p \wedge \sim q$. Therefore, a counterexample to $p \rightarrow q$ needs to be an example where $p \wedge \sim q$ is true, i.e., p is true and $\sim q$ is true, i.e., the hypothesis p holds but the conclusion q does not hold.

For instance, to disprove the statement 'If n is an odd integer, then n is prime.', we need to look for an odd integer which is not a prime number. 15 is one such integer. So, n = 15 is a counterexample to the given statement.

Notice that a **counterexample to a statement p proves that** p is false, i.e., $\sim$ **p is true**.

Let us consider another example.

Example 8: Disprove the following statement:

$(\forall\ a \in \mathbf{R})\ (\forall\ b \in \mathbf{R})\ [(a^2 = b^2) \Rightarrow (a = b)]$.

Solution: A good way of disproving it is to look for a counterexample, that is, a pair of real numbers a and b for which $a^2 = b^2$ but $a \neq b$. Can you think of such a pair? What about a = 1 and b = -1? They serve the purpose.

In fact, there are infinitely many counterexamples. (Why?)

***

Now, an exercise!

E12) Disprove the following statements by providing a suitable counterexample.
i) $\forall\ x \in \mathbf{Z},\ x \in \mathbf{Q} \setminus \mathbf{N}$.
ii) $(x+y)^n = x^n + y^n\ \forall\ n \in \mathbf{N},\ x, y \in \mathbf{Z}$.
iii) $f : \mathbf{N} \rightarrow \mathbf{N}$ is 1-1 iff f is onto.
(**Hint:** To disprove $p \Leftrightarrow q$ it is enough to prove that $p \Leftrightarrow q$ is false or $q \Rightarrow p$ is false.)

There are some other strategies of proof, like a constructive proof, which you must have come across in other mathematics courses. We shall not discuss this method here.

Other proof-related adjectives that you will come across are **vacuous** and **trivial**.

A **vacuous proof** make use of the fact that if p is false, the $p \rightarrow q$ is true, regardless of the truth value of q. So, to vacuously prove $p \rightarrow q$, all we need to do is to show that p is false. For instance, suppose we want to prove that 'If $n > n + 1$ for $n \in \mathbf{Z}$, then $n^2 = 0$.'.

Since 'n . n + 1' is false for every $n \in \mathbf{Z}$, the given statement is vacuously true, or true by default.

Similarly, a **trivial proof** of $p \rightarrow q$ is one based on the fact that if q is true, then $p \rightarrow q$ is true, regardless of the truth value of p. So, for example, 'If $n > n + 1$ for $n \in \mathbf{Z}$, then $n + 1 > n$' is trivially true since $n + 1 > n \; \forall \; n \in \mathbf{Z}$. The truth value of the hypothesis (which is false in this example) does not come into the picture at all.

Here's a chance for you to think up such proofs now!

E13) Give one example each of a vacuous proof and trivial proof.

And now let us study a very important technique of proof for statements that are of the form p(n), $n \in \mathbf{N}$.

2.4 PRINCIPLE OF INDUCTION

In a discussion with some students the other day, of them told me very cynically that all Indian politicians are corrupt. I asked him how he had reached such a conclusion. As an argument he gave me instances of several politicians, all of whom were known to be corrupt. What he had done was to formulate his general opinion of politicians on the basis of several particular instances. This is an example of **inductive logic**, a process of reasoning by which general rules are discovered by the observation of several individual cases. Inductive reasoning is used in all the sciences, including mathematics. But in mathematics we use a more precise form.

Precision is required in mathematical induction because, as you know, a statement of the form $(\forall \; n \in \mathbf{N})p(n)$ is true only if it can be shown to be true for each n in **N**. (In the example above, even if the student is given an example of one clean politician, he is not likely to change his general opinion.)

How can we make sure that our statement p(n) is true for each n that we are interested in? To answer this, let us consider an example.

Suppose we want to prove that $1+2+3+\ldots\ldots+n = \frac{n(n+1)}{2}$ for each $n \in \mathbf{N}$. Let us call p(n) the predicate '$1+2+\ldots+n = \frac{n(n+1)}{2}$'. Now, we can verify that it is true for a few values, say, n = 1, n = 5, n = 10, n = 100, and so on. But we still can't be sure that it will be true for some value of n that we haven't tried.

But now, suppose we can show that if p(n) is true for some n,n = k say, then it will be true for n = k + 1. Then we are in a very good position because we already know that p(1) is true. And, since p(1) is true, so is p(1+1), i.e., p(2), and so on. In this way we can show that p(n) is true for every n ε **N**. So, our proof boils down to two steps, namely,

i) Checking that p(1) is true;

ii) Proving that whenever p(k) is true, then p(k+1) is true, where k ∈ **N**.

This is the principle that we will now state formally, in a more general form.

Principle of Mathematical Induction (PMI): Let p(n) be a predicate involving a natural number n. Suppose the following two conditions hold:

i) p(m) is true for some m ε **N**;
ii) If p(k) is true, then p(k+1) is true, where k(≥m) is any natural number.

Then p(n) is true for every n ≥ m.

Looking at the two conditions in the principle, can you make out why it works? (As a hint, put m = 1 in our example above.)

Well, (i) tells us that p(m) is true. Then putting k = m in (ii), we find that p(m + 1) is true. Again, since p(m+1) is true, p(m+2) is true, and so on.

Going back to the example above, let us complete the second step. We know that p(k) is true, i.e.,$1 + 2+\ldots+k = \frac{k(k+1)}{2}$. We want to check if p(k + 1) is true. So let us find

$$\begin{aligned} 1 + 2+\ldots + (k + 1) &= (1+2+\ldots+k) + (k+1) \\ &= \frac{k(k+1)}{2} + (k + 1), \text{ since p(k) is true} \\ &= \frac{(k+1)(k+2)}{2} \end{aligned}$$

So, p(k + 1) is true.

And so, by the principle of mathematical induction, we know that p(n) is true for every n ∈ **N**.

What does this principle really say? It says that if you can walk a few steps, say m steps, and if at each stage you can walk one more step, then you can walk and distance. It sounds very simple, but you may be surprised to know that the technique in this principle was first used by Europeans only as late as the 16th century by the Venetian F. Maurocylus (1494-1573). He used it to show that $1+3+ \ldots +(2n – 1) = n^2$. Pierre de Fermat (1601 – 1665) improved on the technique and proved that this principle is equivalent to the following often-used principle of mathematics.

The Well-ordering Principle: Any non-empty subset of N contains a smallest element.

You may be able to see the relationship between the two principles if we reword the PMI in the following form.

Principle of Mathematical Induction (Equivalent form): Let **S** ⊆ **N** be such that

i) m ∈ **S**
ii) For each k ∈ **N**, k ≥ m, the following implication is true: K ∈ **S** ⇒ k 1 ∈ S. Then **S** = {m,m + 1, m + 2, …}.

The term ‘mathematical induction’ was first used by De Morgan.

Can you see the equivalence of the two forms of the PMI? If you take S = { n ∈ **N** | p(n) is true } then you can see that the way we have written the principle above is a mere rewrite of the earlier form.

Now, let us consider an example of proof using PMI.

Example 9: Use mathematical induction to prove that

Note that p(n) is a predicate, not a statement, unless we know the value of n.

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n}{6}\ (n + 1)\ (2n + 1)\ \forall\ n \in \mathbf{N}.$$

Solution: We call p(n) the predicate

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n}{6}\ (n + 1)\ (2n + 1).$$

Since we want to prove it for every $n \in \mathbf{N}$, we take m = 1.

Step 1: p(1) is $1^2 = \frac{1}{6}\ (1 + 1)\ (2 + 1)$, which is true

Step 2: Suppose for an arbitrary $k \in \mathbf{N}$, p(k) is true, i.e.,

$$1^2 + 2^2 + \ldots + k^2 = \frac{k}{6}(k + 1)\ (2k + 1) \text{ is true.}$$

Step 3: To check if the assumption in step 2 implies that p(k + 1) is true. Let's see.

$$P(k + 1) \text{ is } 1^2 + 2^2 + \ldots + k^2 + (k + 1)^2 = \frac{k+1}{6}\ (k + 2)\ (2k + 3)$$

$$\Leftrightarrow (1^2 + 2^2 + \ldots + k^2) + (k + 1)^2 \quad \frac{k+1}{6}(k + 2)\ (2k + 3)$$

$$\Leftrightarrow \frac{k}{6}(k + 1)\ (2k + 1) + (k + 1)^2 = \frac{k+1}{6}\ (k + 2)\ (2k + 3),$$

since p(k) is true.

$$\Leftrightarrow \frac{k+1}{6}[k(2k + 1) + 6(k + 1)] = \frac{k+1}{6}\ (k + 2)\ (2k + 3)$$

$$\Leftrightarrow 2k^2 + 7k + 6 = (k + 2)\ (2k + 3), \text{ dividing throughout by } \frac{k+1}{6},$$

which is true.

So, p(k) is true implies that p(k + 1) is true.

So, both the conditions of the principle of mathematical induction hold. Therefore, its conclusion must hold, i.e., p(n) is true for every n ε **N**.

***

Have you gone through Example 9 carefully? If so, you would have noticed that the proof consists of three steps:

Step 1: (called the **basis of induction**): Checking if p(m) is true for some $m \in \mathbf{N}$.
Step 2: (called the **induction hypothesis**): Assuming that p(k) is true for an arbitrary $k \in \mathbf{N}$, $k \geq m$.
Step 3: (called the **induction step**): Showing that p(k + 1) is true, by a direct or an indirect proof.

Now let us consider an example in which $m \neq 1$.

Example 10: Show that $2^n > n^3$ for ≥ 10.

Solution: We write p(n) for the predicate '$2^n > n^3$'.

Step 1: For n = 10, 2^{10} =1024, which is greater that 10^3. Therefore, p(10) is true.
Step 2: We assume that p(k) is true for an arbitrary $k \geq 10$. Thus, $2^k > k^3$.
Step 3: Now, we want to prove that $2^{k+1} > (k + 1)^3$.

$2^{k+1} = 2.2^k > 2.k^3$, by our assumption

$> (1 + \frac{1}{10})^3 .k^3$, since $2 > (1 + \frac{1}{10})^3$

$\geq (1 + \frac{1}{k})^3 \ .k^3$, since ≥ 10

$= (k + 1)^3$.

Thus, p(k + 1) is true if p(k) is true for k≥ 10.

Therefore by the principle of mathematical induction, p(n) is true ∀ n ≥ 10.

***

Why don't you try to apply the principle now?

E14) Use mathematical induction to prove that

$1 + \frac{1}{4} + \frac{1}{9} + \ldots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$ ∀ n ∈ **N**.

E15) Show that for any integer n > 1, $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{n}} > \sqrt{n}$.

(**Hint**: The basis of induction is p(2).).

Before going further a **note of warning!** To prove that p(n) is true ∀ n ≥ m, both the basis of induction **as well as** the induction step must hold. If even one of these conditions does not hold, we cannot arrive at the conclusion that p(n) is true ∀ n ≥ m.

For example, suppose p(n) is $(x + y)^n \leq x^n + y^n$ ∀ x,y ∈ **R**. Then p(1) is true. But Steps 2 and 3 do not hold. Therefore, p(n) is not true for every n ∈ **N**. (Can you find a value of n for which p(n) is false?)

As another example, take p(n) to be the statement ' 1 + 2 + … +n < n'. Then, if p(k) is true, so is p(k + 1) (prove it!). But the basis step does not hold for any m ∈ **N**. And, as you can see, p(n) is false.

Now let us look at a situation in which we may expect the principle of induction to work, but it doesn't. Consider the sequence of numbers 1,1,2,3,5,8,…. These are the **Fibonacci numbers**, named after the Italian mathematician Fibonacci. Each term in the sequence, from the third on, is obtained by Fibonacci. Each term in the sequence, from the third term on, is obtained by adding the previous 2 terms. So, if a_n is the nth term, then $a_1 = 1$, $a_2 = 1$, and $a_n = a_{n-1} + a_{n-2}$ ∀ n≥ 3.

Suppose we want to show that $a_n < 2^n$ ∀ n ∈ **N** using the PMI. Then, if p(n) is the predicate $a_n < 2^n$, we know that p(1) is true.

Now suppose we know that p(k) is true for an arbitrary k ∈ **N**, i.e., $a_k < 2^k$. We want to show that $a_{k+1} < 2^{k+1}$, i.e., $a_k + a_{k-1} < 2^{k+1}$. But we don't know anything about a_{k-1} . So how can we apply the principle of induction in the form that we have stated it? In such a situation, a stronger, more powerful, version of the principle of induction comes in handy. Let's see what this is.

Principle of Strong Mathematical Induction: Let p(n) be a predicate that involves a natural number n. Suppose we can show that

i) p(m) is true for some m ∈ **N**, and
ii) Whenever p(m), p(m +1), …, p(k) are true, then p(k + 1) is true, where k ≥ m.

Then we can conclude that p(n) is true for all natural numbers n ≥ m.

In using the strong form we often need to check Step 1 for more than one value of n.

Why do we call this principle stronger than the earlier one? This is because, in the induction step we are making more assumptions, i.e., that p(n) is true for every n lying between m and k, not just that p(k) is true.

Let us now go back to the fibonacci sequence. To use the strong form of the PMI, we take m = 1. We have seen that p(1) is true. We also need to see if p(2) is true. This is because we have to use the relation $a_n = a_{n-1} + a_{n-2,}$ which is valid for $n \geq 3$.

Now that we know that both p(1) and p(2) are true, let us go the next step. In step 2, for an arbitrary $k \geq 2$, we assume that p(n) is true for every n such that $1 \leq n \leq k$, i.e., $a_n < 2^n$ for $1 \leq n \leq k$.

Finally, in Step 3, we must show that p(K + 1) is true, i.e., $a_{k+1} < 2^{k+1}$. Now

$a_{k+1} = a_k$
$< 2^k + 2^{k-1}$, by our assumption in Step 2.
$= 2^{k-1} (2 + 1)$
$< 2^{k-1} .2^2$
$= 2^{k+1}$
P(k + 1) is true.
P(n) is true $\forall$ n $\in$ **N**.

Though the "strong" form of the PMI appears to be different from the "weak" from, the **two are actually equivalent**. This is because each can be obtained from the other. So, we can use either form of mathematical induction. In a given problem we use the form that is more suitable. For instance, in the following example, as in the case of the one above, you would agree that it is better to use the strong form of the PMI.

Example 11: Use induction to prove that any integer $n \geq 2$ is either a prime or a product of primes.

Solution: Here p(n) is the predicate 'n is a prime or n is a product of primes.'.

Step 1: (**basis of induction**) : since 2 is a prime, p(2) is true.
Step 2: (**induction hypothesis**): Assume that p(n) is true for any integer n such that $2 \leq n \leq k$, i.e., p(3), p(4),…, p(k) are true.
Step 3: (**induction step**): Now consider p(k +1). If k + 1 is a prime, then p(k + 1) is true. If k + 1 is not a prime, then k + 1 = rs, where $2 \leq r \leq k$ and $2 \leq s \leq k$. But, by our induction hypothesis, p(r) is true and p(s) is true. Therefore, r and s are either primes or products of primes. And therefore, k + 1 is a product of primes. So, p(k + 1) is true.

Therefore, p(n) is true $\forall$ $n \geq 2$.

***

Why don't you try some exercises now?

E16) If $a_1, a_2, \ldots$ are the terms in the Fibonacci sequence, use the weak as well as the strong forms of the principle of mathematical induction to show that $a_n > \frac{3}{2} \forall n \geq 3$. Which form did you find more convenient?

E17) Consider the following "proof" by induction of the statement. 'Any n marbles are of the same size.', and say why it is wrong.
Basis of induction : For n = 1, the statement is clearly true.
Induction hypothesis: Assume that the statement is true for n = k.
Induction step: Now consider any k + 1 marbles 1,2, …, k + 1. By the induction hypothesis the k marbles 2,3,…,k + 1 are of the same size. Therefore, all the k + 1 marbles are of the same size.Therefore, the given

statement is true for every n.

E18) Prove that the following result is equivalent to the principle of mathematical induction (strong form):
Let $S \subseteq \mathbf{N}$ such that
i) $m \in \mathbf{S}$
ii) If m, m + 1, m + 2, …, k are in S, then $k + 1 \in S$.
Then $S = \{n \in \mathbf{N} \mid n \geq m\}$.

E19) To prove that $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n} - 1 \ \forall\ n \in \mathbf{N}$, which form of the principle of mathematical induction would you use, and why? Also, prove the inequality.

With this we come the end of our discussion on various techniques of proving of disproving mathematical statements. Let us take a brief look at what you have read in this unit.

2.5 SUMMARY

In this unit, you have studied the following points.

1. What constitutes a proof of a mathematical statement, including 4 commonly used rules of inference, namely,
   i) law of detachment (or modus ponen) : $[(p \rightarrow q) \wedge p] \Rightarrow q$
   ii) law of contraposition (or modus tollens) : $[(p \rightarrow q) \wedge \sim q] \Rightarrow \sim p$
   iii) disjunctive syllogism : $[(p \rightarrow q) \wedge (q \rightarrow r)] \Rightarrow (p \rightarrow r)$
2. The description and examples of a direct proof, which is based on modus ponens.
3. Two types of indirect proofs : proof by contrapositive and proof by contradiction.
4. The use of counterexamples for disproving a statement.
5. The "strong" and "weak" forms of the principle of mathematical induction, and their equivalence with the well-ordering principle.

2.6 SOLUTIONS/ ANSWERS

E1) For example,

Theorem: $(x + y)^2 = x^2 + 2xy + y^2$ for $x, y \in \mathbf{R}$.

Proof: for $x, y \in \mathbf{R}$, $(x + y)^2 = (x + y)(x + y)$ (by definition of 'square')
$(x + y)(x + y) = x(x + y) + y(x + y)$ (by distributivity, and by definition of addition and multiplication of algebraic terms).

Therefore, $(x + y)^2 = x^2 + 2xy + y^2$ (using an earlier proved statement that a =b and b = c implies that a = c).

E2) No, not unless it has been proved to be true

E3)

premises ↓ conclusion ↓

p	q	r	~ r	q ∨ ~ r	p → q ∨ ~ r	q → p	p → r
T	T	T	F	T	T	T	T
T	T	F	T	T	T	T	F
T	F	T	F	F	F	T	T
T	F	F	T	T	T	T	F
F	T	T	F	T	T	F	T
F	T	F	T	T	T	F	T
F	F	T	F	F	T	T	T
F	F	F	T	T	T	T	T

The premises are true in Rows 1, 2, 4, 7, 8. So, the argument will be valid if the conclusion is also true in these rows. But this does not happen in Row 2, for instance. Therefore, the argument is invalid.

E4) i) Let p : The eraser is white,
q : Oxygen is a metal.
Then the argument is
$p \vee q$
$\sim \frac{p}{q}$
Its truth table is given below.

conclusion ↓ premises ↓

p	q	~ p	p∨ q
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

All the premises are true only in the third row. Since the conclusion in this row is also true, the argument is valid.

ii) The argument is $(p \rightarrow q) \wedge (q \rightarrow r) \Rightarrow (p \rightarrow r)$
where p: Madhu is a 'sarpanch',
q : Madhu heads the 'Panchayat'.
r : Madhu decides on property disputes.
This is valid because, whenever both the premises are true, so is the conclusion (see the following table.)

premises ↓ ↓ conclusion ↓

P	q	r	p → q	q → r	p → r
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	T
T	F	F	F	T	F
F	T	T	T	T	T
F	T	F	T	F	T
F	F	T	T	T	T
F	F	F	T	T	T

iii) The argument is $[(p \vee q) \wedge (q \rightarrow r) \wedge \sim r] \Rightarrow q$
Where p: Munna will cook.
q: Munni will practise Karate.
r: Munna studies.

This is **not valid**, as you can see from Row 4 of the following truth table.

conclusion ↓ premises ↓ ↓

p	Q	r	~ r	p ∨ q	Q → r
T	T	T	F	T	T
T	T	F	T	T	F
T	F	T	F	T	T
T	F	F	T	T	T
F	T	T	F	T	T
F	T	F	T	T	F
F	F	T	F	F	T
F	F	F	T	F	T

E5) We need to prove $p \Rightarrow q$, where
p: $x \in \mathbf{R}$ such that $x^2 = 9$, and
q: x = 3 or x = -3.
Now, $x^2 = 9 \Rightarrow \sqrt{x^2} = \pm\sqrt{9} \Rightarrow x = \pm 3$.

Therefore, p is true and $(p \Rightarrow q)$ is true, allows us to conclude that q is True.

E6) If f is not surjective, then f is not a 1-1 function from X into itself.

E7) We want to prove $\sim q \Rightarrow \sim p$, where
p: $x \in \mathbf{Z}$ such that x^2 is even,
q: x is even.
Now, we start by assuming that q is false, i.e., x is odd.
Then $x = 2m + 1$ for some $m \in Z$.
Therefore, $x^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$
Therefore, x^2 is odd, i.e., p is false.
Thus, $\sim q \Rightarrow \sim p$, and hence, $p \Rightarrow q$.

E8) i) This is on the lines of Example 5.
ii) Let us assume that $x^3 + 4x = 0$ and $x \neq 0$. Then $x(x^2 + 4) = 0$ and $x \neq 0$. Therefore, $x^2 + 4 = 0$, i.e., $x^2 = -4$. But $x \in \mathbf{R}$ and $x^2 = -4$ is a contradiction. Therefore, our assumption is false. Therefore, the given statement is true.

E9) Direct proof: $x^3 + 4x = 0 \Rightarrow x(x^2 + 4) = 0$
$\Rightarrow x = 0$ or $x^2 + 4 = 0$
$\Rightarrow x = 0$, since $x^2 \neq -4 \; \forall \; x \in R$.
Proof by contrapositive: Suppose $x \neq 0$. Then $x(x^2 + 4) \neq 0$ for any $x \in \mathbf{R}$.
$x^3 + 4x \neq 0$ for every $x \in \mathbf{R}$.
So we have proved that 'For $x \in \mathbf{R}$, $x \neq 0 \Rightarrow x^3 + 4x \neq 0$.'.
That is, 'For $x \in \mathbf{R}$, x^3 4x = 0 $\Rightarrow$ x =0.'.

E10) Suppose C tells the truth. Therefore, D always tells the truth. Therefore, C always lies, which is a contradiction. Therefore, C can't be a truth-teller, i.e., C is a liar. Therefore, D is a truth-teller.

E11) i) What about x = 1?

ii) Take n= 2, x = 1 and y = -1, for instance.

iii) Here we can find an example f such that f is 1-1 but not onto, or such that f is onto but not 1-1.
Consider f: $\mathbf{N} \rightarrow \mathbf{N}$: (f(x) = x + 10. Show that this is 1-1, but not surjective.

E12) i) **Theorem:** The area of every equilateral triangle of side a and perimeter 2a is divisible by 3.

Proof: Since there is no equilateral triangle that satisfies the hypothesis, the proposition is vacuously true.

ii) **Theorem:** If a natural number c is divisible by 5, then the perimeter of the equilateral triangle of side c is 3c.

Proof: Since the conclusion is always true, the proposition is trivially true.

E13) Let p(n) be the given predicate.

Step 1: p(1) : $1 \leq 2 - 1$, which is true.

Step 2: Assume that p(k) is true for some $k \geq 1$, i.e., assume that $1 + \frac{1}{4} + \ldots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$.

Step 3: To show that p(k + 1) is true, consider

$$1 + \frac{1}{4} + \ldots + \frac{1}{k^2} + \frac{1}{(k+1)^2} = (1 + \frac{1}{4} + \ldots + \frac{1}{k^2}) + \frac{1}{(k+1)^2}$$

$$\leq (2 - \frac{1}{k}) + \frac{1}{(k+1)^2}, \text{ by step 2.}$$

Now, $(2 - \frac{1}{k}) + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{(k+1)}$

iff $\frac{1}{(k+1)^2} \leq \frac{1}{k} - \frac{1}{(k+1)}$

iff $k \leq k + 1$, which is true.
Therefore, $(2 - \frac{1}{k}) + \frac{1}{(k+1)^2} \leq 2 - \frac{1}{(k+1)}$

Therefore, p(k + 1) is true.
Thus, by the PMI, p(n) is true $\forall$ n $\in$ **N**.

E14) p(2) : $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} > \sqrt{2}$, which is true.
Now, assume that p(k) is true for some $k \geq 2$. Then

$$\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\ldots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}} > \sqrt{k}+\frac{1}{\sqrt{k+1}},$$ since p(k) is true.

$$= \frac{\sqrt{k(k+1)}}{\sqrt{k+1}}+1$$

$$> \sqrt{k+1},$$ since $\sqrt{k+1} > \sqrt{k}$.

Hence p(k + 1) is true.
P(n) is true $\forall$ n $\geq$ 2.

E15) We shall apply the strong form of the PMI here.
Let p(n) : $a_n > \frac{3}{2}$.

Step 1: p(3) and p(4) are true.

Step 2: Assume now that for k $\in$ **N**, $\geq$ 3, p(n) is true for every n such that 3 $\leq$ n $\leq$ k.

Step 3: We want to show that p(k + 1) is true. Now

$$a_{k+1} = a_k + a_{k-1} > \frac{3}{2}+\frac{3}{2},$$ by step 2

$$> \frac{3}{2}.$$

p(k + 1) is true.
Thus, p(n) is true $\forall$ n $\geq$ 3.

In this case, you will be able to use the weak form conveniently too since $a_k > \frac{3}{2}$ is enough for showing that p(k + 1) is true.

Thus, **in this case the weak form is more appropriate** since fewer assumptions give you the same result.

E16) The problem is at the induction step. The first marble may be a different size from the other k marbles. So, we have not shown that p(k+1) is true whenever p(k) is true.

E17) With reference to the statement of the strong form of the PMI, let
S = { n $\in$ **N** $\mid$ p(n) is true }.
Then you can show how the form in this problem is the same as the statement of the strong form of the PMI.

E18) Let p(n) : $\sum_{i=i}^{n} \frac{1}{\sqrt{i}} \leq 2\sqrt{n}-1.$

The weak form suffices here, since the assumption that p(k) is true is enough to prove that p(k + 1) is true. We don't need to assume that p(1), p(2),…,p(k – 1) are also true to show that p(k + 1) is true. Let's prove that p(n) is true $\forall$ n $\in$ **N**.

Now, p(1) : 1 $\leq$ 2 – 1, which is true.
Next, assume that p(k) is true for some k $\in$ **N**.

Then $\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+...+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}} \le (2\sqrt{k}-1)+\frac{1}{\sqrt{k+1}}$, since p(k) is true.

Now $2\sqrt{k}-1+\frac{1}{\sqrt{k+1}} \le 2\sqrt{k+1}-1$

$\Leftrightarrow 2(\sqrt{k+1}-\sqrt{k}) \ge \frac{1}{\sqrt{k+1}}$

$\Leftrightarrow 2(k+1-\sqrt{k(k+1)} \ge 1$

$\Leftrightarrow 1 \ge 0$, which is true.

p(k + 1) is true.

p(n) is true $\forall$ n $\in$ **N**.

UNIT 3 BOOLEAN ALGEBRA AND CIRCUITS

Structure

3.0 INTRODUCTION

Fig. 1: Claude Shannon

This unit is very closely linked with Unit 1. It was C.E.Shannon, the founder of information theory, who observed an analogy between the functioning of switching circuits and certain operations of logical connectives. In 1938 he gave a technique based on this analogy to **express and manipulate** simple switching circuits algebraically. Later, the discovery of some new solid state devices (called **electronic switches** or **logic gates**) helped to modify these algebraic techniques and, thereby, paved a way to solve numerous problems related to digital systems algebraically.

In this unit, we shall discuss the symbolic logic techniques which are required for the algebraic understanding of circuits and computer logic. In Sec. 3.2, we shall introduce you to **Boolean algebras** with the help of certain examples based on objects you are already familiar with. You will see that such algebras are apt for describing operations of logical circuits used in computers.

In Sec. 3.3, we have discussed the linkages between **Boolean expressions** and logic circuits.

In Sec. 3.4, you will read about how to express the overall functioning of a circuit mathematically in terms of certain suitably defined functions called **Boolean functions**. In this section we shall also consider a simple **circuit design problem** to illustrate the applications of the relationship between Boolean functions and circuits.

Let us now consider the objectives of this unit.

3.1 OBJECTIVES

After reading this unit, you should be able to:

- define and give examples of Boolean algebras, expressions and functions;
- give algebraic representations of the functioning of logic gates;
- obtain and simplify the Boolean expression representing a circuit;
- construct a circuit for a Boolean expression;
- design and simplify some simple circuits using Boolean algebra techniques.

3.2 BOOLEAN ALGEBRAS

Let us start with some questions: Is it possible to design an electric/electronic circuit without actually using switches(or logic gates) and wires? Can a circuit be redesigned, to get a simpler circuit with the help of pen and paper only?

The answer to both these questions is `Yes'. What allows us to give this reply is the concept of **Boolean algebras**. Before we start a formal discussion on these types of algebras, let us take another look at the objects treated in Unit 1.

As before, let the letters p, q, r,. . . denote statements (or propositions). We write $\mathcal{S}$ for the set of all propositions. As you may recall, a tautology $\mathcal{T}$ (or a contradiction $\mathcal{F}$) is any proposition which is always true (or always false, respectively). By abuse of notation, we shall **let $\mathcal{T}$ denote the set of all tautologies and $\mathcal{F}$ denote the set of all contradictions.** Thus,

$$\mathcal{T} \leq \mathsf{S}, \mathcal{F} \leq \mathsf{S}.$$

You already know from Unit 1 that, given two propositions p and q, both p ^ q and p v q are again propositions. And so, by the definition of a binary operation, you can see that both $\wedge$ (**conjunction**) and $\vee$ (**disjunction**) are binary operations on the set S, where we are writing $\wedge$ (p, q) as $p \wedge q$ and v (p, q) as $p \vee q \; \forall \; p, q \in S$.

Again, since ~ p is also a proposition, the operation ~ **(negation)** defines a unary function $\sim: \mathsf{S} \to \mathsf{S}$. Thus, the set of propositions S, with these operations, acquires an algebraic structure.

As is clear from Sec.1.3, under these three operations, the elements of S satisfy **associative laws, commutative laws, distributive laws** and **complementation laws.**

Also, by E19 of Unit 1, you know that $p \vee \mathcal{F} = p$ and $p \wedge \mathcal{T} = p$, for any proposition p. These are called the **identity laws**. The set S with the three operations and properties listed above is a particular case of an algebraic structure which we shall now define.

In the NCERT textbook, '+' and '.' are used instead of '$\vee$' and '$\wedge$', respectively.

Definition: A Boolean algebra B is an algebraic structure which consists of a set X ($\neq \varnothing$) having two binary operations (denoted by $\vee$ and $\wedge$), one unary operation (denoted by ') and two specially defined elements **O** and **I** (say), which satisfy the following five laws for all x, y, z $\in$ **X**.

B1. Associative Laws: $x \vee (y \vee z) = (x \vee y) \vee z$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$

B2. Commutative Laws: $x \vee y = y \vee x$, $x \wedge y = y \wedge x$

B3. Distributive Laws: $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

B4. Identity Laws: $x \vee \mathbf{O} = x$, $x \wedge \mathbf{I} = x$

B5. Complementation Laws: $x \wedge x' = \mathbf{O}$, $x \vee x' = \mathbf{I}$.

We write this algebraic structure as **B** = (**X**, $\vee$, $\wedge$, ' , **O, I**), or simply **B**, if the context makes the meaning of the other terms clear. The two operations $\vee$ and $\wedge$ are called the **join operation** and **meet operation**, respectively. The unary operation ' is called the **complementation**.

From our discussion preceding the definition above, you would agree that the set S of propositions is a Boolean algebra, where $\mathcal{T}$ and $\mathcal{F}$ will do the job of **I** and **O**, respectively. Thus, (S, $\wedge$, $\vee$, ~, $\mathcal{F}$, $\mathcal{T}$) is an example of a Boolean algebra.

We give another example of a Boolean algebra below.

Example 1: Let X be a non-empty set, and $\mathcal{P}$(**X**) denote its power set, i.e., $\mathcal{P}$(**X**) is the set consisting of all the subsets of the set X. Show that $\mathcal{P}$(**X**) is a Boolean algebra.

Solution: We take the usual set-theoretic operations of intersection ($\cap$), union ($\cup$), and complementation (^{c}) in $\mathcal{P}(X)$ as the three required operations. Let ø and X play the roles of **O** and **I**, respectively. Then you can verify that all the conditions for ($\mathcal{P}$ **(X)**, $\cup$, $\cap$, ^{c}, **Φ**, **X**) to be a Boolean algebra hold good.

For instance, the identity laws (B4) follow from two set-theoretic facts, namely, `the intersection of any subset with the whole set is the set itself' and `the union of any set with the empty set is the set itself'. On the other hand, the complementation laws (B5) follow from another set of facts from set theory, namely, `the intersection of any subset with its complement is the empty set' and `the union of any set with its complement is the whole set'.

***

Yet another example of a Boolean algebra is based on **switching circuits**. For this, we first need to elaborate on the functioning of ordinary switches in a mathematical way. In fact, we will present the basic idea which helped the American, C.E.Shannon, to detect the connection between the functioning of switches and Boole's symbolic logic.

You may be aware of the functioning of a simple on-off switch which is commonly used as an essential component in the electric (or electronic) networking systems. A switch is a device which allows the current to flow only when it is placed in the **ON** position, i.e., when the gap is **closed** by a conducting rod. Thus, the **ON** position of a switch is one state of a switch, called a **closed state**. The other state of a switch is the open state, when it is placed in the **OFF** position. So, a switch has two stable states.

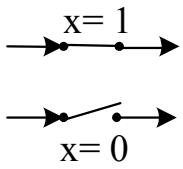


Fig. 2: OFF-ON position

There is another way to talk about the functioning of a switch. We can denote a switch by x, and use the values 0 and 1 to depict its two states, i.e., to convey that x is open we write x = 0, and to convey that x is closed we write x = 1 (see Fig.2).

These values which denote the state of a switch x are called the **state-values** (**s.v.,** in short) of that switch.

We shall also write x′ for a switch which is always in a state opposite to x. So that,

x **is open** $\rightarrow$ x' **is closed** and x **is closed** $\rightarrow$ x' **is open**.

The switch x' is called the invert of the switch x. For example, the switch a' shown in Fig.3 is an invert of the switch a.

Table 1: s.v. of x'

x	x'
0	1
1	0

Table 1 alongside gives the state value of x' for a given state value of the switch x. These values are derived from the definition of x' and our preceding discussion.

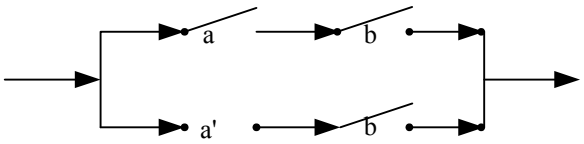
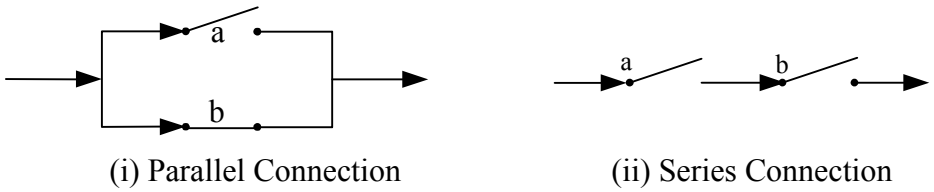


Fig. 3: a` is the invert of a.

Note that the variable x that denotes a switch can only take on 2 values, 0 and 1. Such a variable (which can only take on two values) is called a **Boolean variable**. Thus, if x is a Boolean variable, so is x'. Now, in order to design a circuit consisting of several switches, there are two ways in which two switches can be connected: **parallel connections** and **series connections** (see Fig.4).

Do you see a connection between Table 1 above and Table 10, Unit 1 ?



(i) Parallel Connection (ii) Series Connection

Fig. 4: Two ways of connecting switches

From Fig.4(i) above, you can see that in case of a parallel connection of switches a and b (say), current will flow from the left to the right extreme if **at** least one of the two switches is closed. Note that 'parallel' **does not** mean that both the switches are in the same state.

On the other hand, current can flow in a series connection of switches only when **both** the switches a and b are closed (see Fig.4 (ii)).

Given two switches a and b, we write a **par** b and a **ser** b for these two types of connections, respectively.

In view of these definitions and the preceding discussion, you can see that the state values of the connections a **par** b and a **ser** b, for different pairs of state values of switches a and b, are as given in the tables below.

Table 2: State values of a par b and a ser b.

s.v. of a	**s.v.** of b	**s.v.** of a **par** b
0	0	0
0	1	1
1	0	1
1	1	1

s.v. of a	**s.v.** of b	**s.v.** of a **ser** b
0	0	0
0	1	0
1	0	0
1	1	1

We have now developed a sufficient background to give you the example of a Boolean algebra which is based on switching circuits.

Example 2: The set S = {0, 1} is a Boolean algebra.

Solution: Take **ser** and **par** in place of $\wedge$and $\vee$, respectively, and inversion(') instead of ~ as the three required operations in the definition of a Boolean algebra,. Also take 0 for the element **O** and 1 for the element **I** in this definition.
Now, using Tables 1 and 2, you can check that the five laws B1-B5 hold good. Thus, (**S, par, ser,**', 0, 1) is a Boolean algebra.

***

A Boolean algebra whose underlying set has only two elements is very important in the study of circuits. We call such an algebra a **two-element Boolean algebra**, and denote it by $\mathcal{B}$. From this Boolean algebra we can build many more, as in the following example.

Example 3: Let $\mathcal{B}^n = \mathcal{B} \times \mathcal{B} \times \cdots \times \mathcal{B} = \{(e_1, e_2, \ldots, e_n) \mid \text{each } e_i = 0 \text{ or } 1\}$, for $n \geq 1$, be the Cartesian product of n copies of $\mathcal{B}$. For $i_k, j_k \in \{0, 1\}$ $(1 \leq k \leq n)$, define

$$(i_1, i_2, \ldots, i_n) \wedge (j_1, j_2, \ldots, j_n) = (i_1 \wedge j_1, i_2 \wedge j_2, \ldots, i_n \wedge j_n),$$
$$(i_1, i_2, \ldots, i_n) \vee (j_1, j_2, \ldots, j_n) = (i_1 \vee j_1, i_2 \vee j_2, \ldots, i_n \vee j_n), \text{ and}$$
$$(i_1, i_2, \ldots, i_n)' = (i'_1, i'_2, \ldots, i'_n).$$

Then B^n is a Boolean algebra, for all $n \geq 1$.

Solution: Firstly, observe that the case n = 1 is the Boolean algebra $\mathcal{B}$.
Now, let us write 0 = (0, 0, . . . , 0) and **I** = (1, 1, . . . , 1), for the two elements of $\mathcal{B}^n$ consisting of n-tuples of 0's and 1's, respectively. Using the fact that $\mathcal{B}$ is a Boolean algebra, you can check that $\mathcal{B}^n$, with operations as defined above, is a Boolean algebra for every $n \geq 1$.

***

The Boolean algebras $\mathcal{B}^n$, $n \geq 1$, (called **switching algebras**) are very useful for the study of the hardware and software of digital computers.

We shall now state, without proof, some other properties of Boolean algebras, which can be deduced from the five laws (B1-B5).

Theorem 1: Let $\mathcal{B} = (\mathbf{S}, \vee, \wedge, ', \mathbf{O}, \mathbf{I})$ be a Boolean algebra. Then the following laws hold $\forall x, y \in S$.

a) **Idempotent laws** : $x \vee x = x$, $x \wedge x = x$.
b) **Absorption laws :** $x \vee (x \wedge y) = x$, $x \wedge (x \vee y) = x$.
c) **Involution law :** $(x')' = x$.
d) **De Morgan's laws :** $(x \vee y)' = x' \wedge y'$, $(x \wedge y)' = x' \vee y'$.

In fact, you have already come across some of these properties for the Boolean algebras of propositions in Unit 1. In the following exercise we ask you to verify them.

E1) a) Verify the identity laws and absorption laws for the Boolean algebra $(\mathbf{S}, \wedge, \vee, \sim, \mathcal{T}, \mathcal{F})$ of propositions.
b) Verify the absorption laws for the Boolean algebra $(\mathcal{P}(\mathbf{X}), \cup, \cap, ^c, \Phi, \mathbf{X})$.

In Theorem 1, you may have noticed that for each statement involving $\vee$ and $\wedge$, there is an analogous statement with $\wedge$ (instead of $\vee$) and $\vee$ (instead of $\wedge$). This is not a coincidence, as the following definition and result shows.

Definition : If p is a proposition involving $\sim$, $\wedge$ and $\vee$, the **dual** of p, denoted by p^d, is the proposition obtained by replacing each occurrence of $\wedge$ (and/or $\vee$) in p by $\vee$ (and/or $\wedge$, respectively) in p^d .
For example, $x \vee (x \wedge y) = x$ is the **dual** of $x \wedge (x \vee y) = x$.

Now, the following principle tells us that if a statement is proved true, then we have simultaneously proved that its dual is true.

Theorem 2 (The principle of duality): If s is a theorem about a Boolean algebra, then so is its dual s^d .
It is because of this principle that the statements in Theorem 1 look so similar.

Let us now see **how to apply Boolean algebra methods to circuit design.**

While expressing circuits mathematically, we identify each circuit in terms of some Boolean variables. Each of these variables represents either a simple switch or an input to some electronic switch.

Definition: Let $\mathcal{B} = (S, \vee, \wedge, ', \mathbf{O}, \mathbf{I})$ be a Boolean algebra. **A Boolean expression** in variables $x_1, x_2, \ldots, x_k$ (say), each taking their values in the set **S** is defined recursively as follows:

i) Each of the variables $x_1, x_2, \ldots, x_k$, as well as the elements **O** and **I** of the Boolean algebra $\mathcal{B}$ are Boolean expressions.

ii) If $\mathbf{X_1}$ and $\mathbf{X_2}$ are previously defined Boolean expressions, then $\mathbf{X_1 \wedge X_2}$, $\mathbf{X_1 \vee X_2}$ and $\mathbf{X'_1}$ are also Boolean expressions.

For instance, $x_1 \wedge x'_3$ is a Boolean expression because so are x_1 and x'_3 , Similarly, because $x_1 \wedge x_2$ is a Boolean expression, so is $(x_1 \wedge x_2) \wedge (x_1 \wedge x'_3)$.

If **X** is a Boolean expression in n variables $x_1, x_2, \ldots, x_n$ (say), we write this as $\mathbf{X = X(x_1, \ldots, x_n)}$.
In the context of simplifying circuits, we need to reduce Boolean expressions to

simpler ones. `Simple' means that the expression has fewer connectives, and all the literals involved are distinct. We illustrate this technique now.

Example 4: Reduce the following Boolean expressions to a simpler form.

(a) $X(x_1, x_2) = (x_1 \wedge x_2) \wedge (x_1 \wedge x'_2)$;
(b) $X(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_3)$.

Solution: (a) Here we can write

$(x_1 \wedge x_2) \wedge (x_1 \wedge x'_2) = ((x_1 \wedge x_2) \wedge x_1) \wedge x'_2$	(Associative law)
$= (x_1 \wedge x_2) \wedge x'_2$	(Absorption law)
$= x_1 \wedge (x_2 \wedge x'_2)$	(Associative law)
$= x_1 \wedge \mathbf{O}$	(Complementation law)
$= \mathbf{O}$.	(Identity law)

Thus, in its simplified form, the expression given in (a) above is **O**, i.e., a **null expression.**

(b) We can write

$(x_1 \wedge x_2) \vee (x_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x_3)$	
$= [x_1 \wedge \{x_2 \vee (x'_2 \wedge x_3\}] \wedge (x_1 \wedge x_3)$	(Distributive law)
$= [x_1 \wedge \{(x_2 \vee x'_2) \wedge (x_2 \vee x_3)\}] \wedge (x_1 \wedge x_3)$	(Distributive law)
$= [x_1 \wedge \{\mathbf{I} \wedge (x_2 \vee x_3)\}] \wedge (x_1 \wedge x_3)$	(Complementation law)
$= [x_1 \wedge (x_2 \vee x_3)] \wedge (x_1 \wedge x_3)$	(Identity law)
$= [(x_1 \wedge x_2) \vee (x_1 \wedge x_3)] \wedge (x_1 \wedge x_3)$	(Distributive law)
$= [(x_1 \wedge x_2) \wedge (x_1 \wedge x_3)] \vee [(x_1 \wedge x_3) \wedge (x_1 \wedge x_3)]$	(Distributive law)
$= (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_3)$	(Idemp.,& assoc. laws)
$= x_1 \wedge [(x_2 \wedge x_3) \vee x_3]$	(Distributive law)
$= x_1 \wedge x_3$	(Absorption law)

Thus, the simplified form of the expression given in (b) is $(x_1 \wedge x_3)$.

***

Now you should find it easy to solve the following exercise.

E2) Simplify the Boolean expression
$\mathbf{X}(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee ((x_1 \wedge x_2) \wedge x_3) \vee (x_2 \wedge x_3)$.

With this we conclude this section. In the next section we shall give an important application of the concepts discussed here.

3.3 LOGIC CIRCUITS

If you look around, you would notice many electric or electronic appliances of daily use. Some of them need a simple switching circuit to control the auto-stop (such as in a stereo system). Some would use an auto-power off system used in transformers to control voltage fluctuations. Each circuit is usually a combination of on-off switches, wired together in some specific configuration. Nowadays certain types of **electronic blocks** (i.e., solid state devices such as transistors, resistors and capacitors) are more in use. We call these electronic blocks **logic gates,** or simply, **gates.** In Fig. 5 we have shown a box which consists of some electronic switches (or logic gates), wired together in a specific manner. Each line which is entering the box from the left represents an independent power source (called **input**), where all of them need not supply voltage to the box at a given moment. A single line coming out of the box gives the **final output** of the circuit box. The output depends on the type of input.

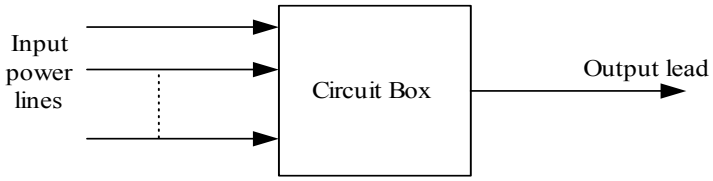


Fig. 5: A Logic circuit

This sort of arrangement of **input power lines, a circuit box** and **output lead** is basic to all electronic circuits. Throughout the unit, any such interconnected assemblage of logic gates is referred to as a **logic circuit.**

As you may know, computer hardwares are designed to handle only two levels of voltage, both as inputs as well as outputs. These two levels, denoted by 0 and 1, are called **bits** (an acronym for **binary digits**). When the bits are applied to the logic gates by means of **one** or **two** wires (input leads), the output is again in the form of voltages 0 and 1. Roughly speaking, **you may think of a gate to be on or off according to whether the output voltage is at level 1 or 0, respectively.**

Three basic types of logic gates are an **AND-gate,** an **OR-gate** and a **NOT-gate.** We shall now define them one by one.

Definition : Let the Boolean variables x_1 and x_2 represent any two bits. An **AND-gate** receives inputs x_1 and x_2 and produces the output, denoted by $x_1 \wedge x_2$, as given in Table 3 alongside.

Table 3:Outputs of AND-gate

x_1	x_2	$x_1 \wedge x_2$
0	0	0
1	1	0
0	1	0
1	1	1

The standard pictorial representation of an **AND**-gate is shown in Fig.6 below.

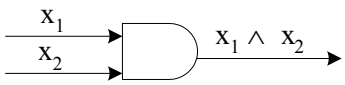


Fig. 6: Diagrammatic representation of an AND -gate

From the first three rows of Table 3, you can see that whenever the voltage in any one of the input wires of the **AND**-gate is at level 0, then the output voltage of the gate is also at level 0. You have already encountered such a situation in Unit 1. In the following exercise we ask you to draw an analogy between the two situations.

E3) Compare Table 3 with Table 2 of Unit 1. How would you relate $x_1 \wedge x_2$ with $p \wedge q$, where p and q denote propositions?

Let us now consider another elementary logic gate.

Table 4: Output of an OR-gate.

x_1	x_2	$x_1 \vee x_2$
0	0	0
0	1	1
1	0	1
1	1	1

Definition : An **OR-gate** receives inputs x_1 and x_2 and produces the output, denoted by $x_1 \vee x_2$, as given in Table 4. The standard pictorial representation used for the **OR**-gate is as shown in Fig.7.

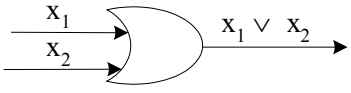


Fig. 7: Diagrammatic representation of an OR-gate

From Table 4 you can see that the situation is the other way around from that in Table 3, i.e., the output voltage of an **OR**-gate is at level 1 whenever the level of voltage in even one of the input wires is 1. What is the analogous situation in the context of propositions? The following exercise is about this.

E4) Compare Table 4 with Table 1 of Unit 1. How would you relate $x_1 \vee x_2$ with $p \vee q$, where p and q are propositions?

And now we will discuss an electronic realization of the invert of a simple switch about which you read in Sec. 3.2.

Definition : A NOT-gate receives bit x as input, and produces an output denoted by x', as given in Table 5. The standard pictorial representation of a **NOT-**gate is shown in Fig. 8 below.

Table 5: Output of a NOT-gate

x	x'
0	1
1	0

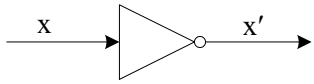


Fig. 8: Diagrammatic representation of NOT-gate

If you have solved E5 and E6, you would have noticed that Tables 3 and 4 are the same as the truth tables for the logic connectives $\wedge$ (conjunction) and $\vee$(disjunction). Also Table 3 of Unit 1, after replacing T by 1 and F by 0, gives Table 5. This is why the output tables for the three elementary gates are called **logic tables.** You may find it useful to remember these logic tables because they are needed very often for computing the logic tables of logic circuits.

Another important fact that these logic tables will help you prove is given in the following exercise.

E5) Let $\mathcal{B} = \{0, 1\}$ consist of the bits 0 and 1. Show that $\mathcal{B}$ is a Boolean algebra, i.e., that the bits 0 and 1 form a two-element Boolean algebra.

As said before, a logic circuit can be designed using elementary gates, where the output from an **AND-**gate, or an **OR**-gate, or a **NOT**-gate is used as an input to other such gates in the circuitry. The different levels of voltage in these circuits, starting from the input lines, move only in the direction of the arrows as shown in all the figures given below. For instance, one combination of the three elementary gates is shown in Fig.9.

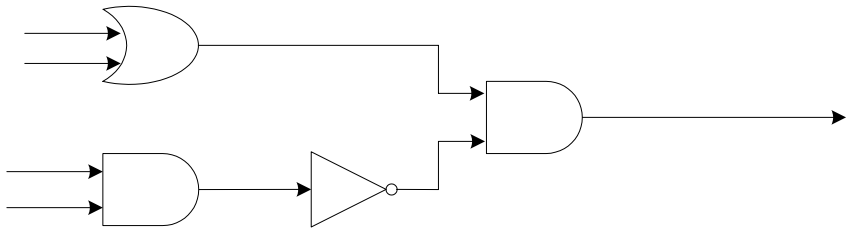


Fig. 9: A logic circuit of elementary gates.

Now let us try to see the connection between logic circuits and Boolean expressions. We first consider the elementary gates. For a given pair of inputs x_1 and x_2 , the output in the case of each of these gates is an expression of the form $x_1 \wedge x_2$ or $x_1 \vee x_2$ or x' .

Next, let us look at larger circuits. Is it possible to find an expression associated with a logic circuit, using the symbols $\wedge$, $\vee$ and ' ? Yes, it is. We will illustrate the technique of finding a Boolean expression for a given logic circuit with the help of some examples. But first, note that the output of a gate in a circuit may serve as an input to some other gate in the circuit, as in Fig. 9. So, to get an expression for a logic circuit the process always moves in the direction of the arrows in the circuitry. With this in mind, let us consider some circuits.

Example 5: Find the Boolean expression for the logic circuit given in Fig.9 above.

Solution: In Fig.9, there are four input terminals. Let us call them x_1 , x_2 , x_3 and x_4 . So, x_1 and x_2 are inputs to an **OR**-gate, which gives $x_1 \vee x_2$ as an output expression (see Fig. 9(a)).

Similarly, the other two inputs x_3 and x_4 , are inputs to an **AND-**gate. They will give $x_3 \wedge x_4$ as an output expression. This is, in turn, an input for a **NOT**-gate in the circuit. So, this yields $(x_3 \wedge x_4)'$ as the output expression. Now, both the expressions $x_1 \vee x_2$ and $(x_3 \wedge x_4)'$ are inputs to the extreme right **AND**-gate in the circuit. So, they give $(x_1 \vee x_2) \wedge (x_3 \wedge x_4)'$ as the final output expression, which represents the logic circuit.

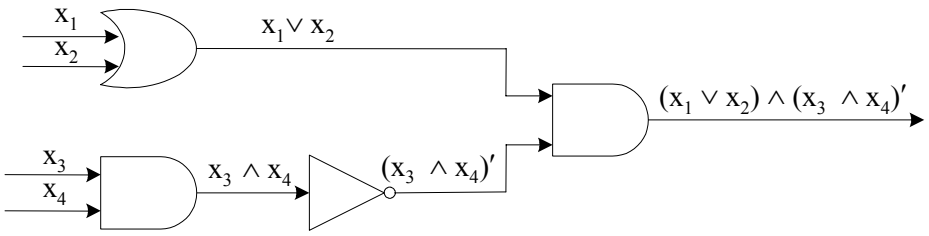


Fig. 9 (a)

***

You have just seen how to find a Boolean expression for a logic circuit. For more practice, let us find it for another logic circuit.

Example 6: Find the Boolean expression C for the logic circuit given in Fig. 10.

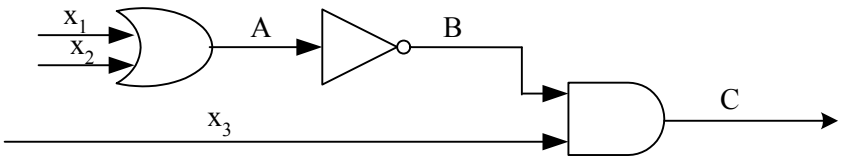


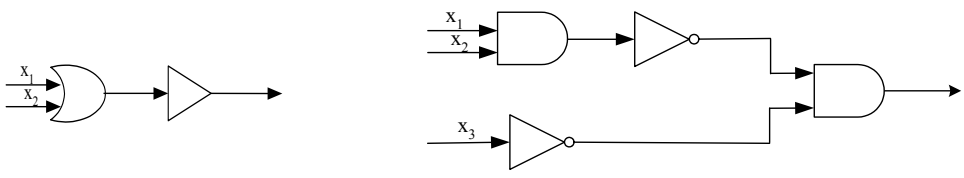
Fig. 10

Solution: Here the first output is from an **OR**-gate, i.e., A is $x_1 \vee x_2$. This, in turn, serves as the input to a **NOT-**gate attached to it from the right. The resulting bit B is $(x_1 \vee x_2)'$. This, and x_3 , serve as inputs to the extreme right **AND**-gate in the circuit given above. This yields an output expression $(x_1 \vee x_2)' \wedge x_3$, which is C, the required expression for the circuit given in Fig.10.

***

Why don't you try to find the Boolean expressions for some more logic circuits now?

E6) Find the Boolean expression for the output of the logic circuits given below.



(a) **(b)**

So far, you have seen how to obtain a Boolean expression that represents a given circuit. Can you do the converse? That is, can you construct a logic circuit corresponding to a given Boolean expression? In fact, this is done when a circuit

designing problem has to be solved. The procedure is quite simple. We illustrate it with the help of some examples.

Example 7: Construct the logic circuit represented by the Boolean expression $(x'_1 \wedge x_2) \vee (x_1 \vee x_3)$, where $x_i (1 \leq i \leq 3)$ are assumed to be inputs to that circuitry.
Solution: Let us first see what the portion $(x'_1 \wedge x_2)$ of the given expression contributes to the complete circuit. In this expression the literals x'_1 and x_2 are connected by the connective $\wedge$ (**AND**). Thus the circuit corresponding to it is as shown in Fig.11(a) below, by the definitions of **NOT**-gate and **AND**-gate.

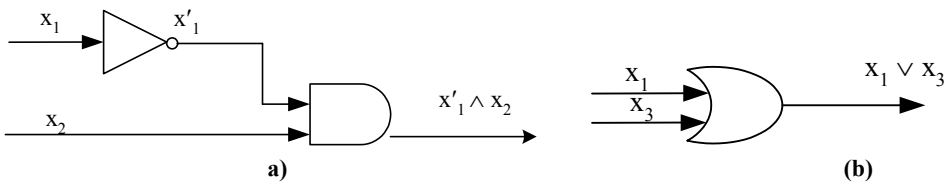


Fig. 11: Logic circuits for the expressions $x'_1 \wedge x_2$ and $x_1 \vee x_3$.

Similarly, the gate corresponding to the expression $x_1 \vee x_3$ is as shown in Fig.11(b) above. Finally, note that the given expression has two parts, namely, $x'_1 \wedge x_2$ and $x_1 \vee x_3$, which are connected by the connective $\vee$ (**OR**). So, the two logic circuits given in Fig.11 above, when connected by an **OR**-gate, will give us the circuit shown in Fig. 12 below.

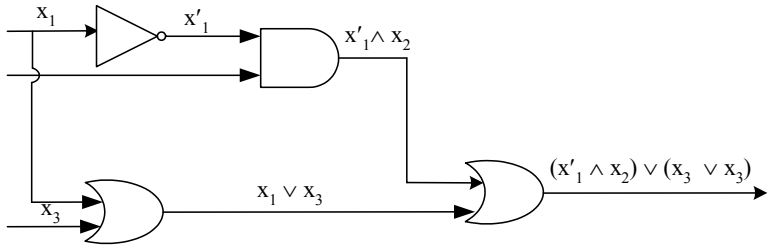


Fig.12: Circuitry for the expression $(x'_1 \wedge x_2) \vee (x_1 \vee x_3)$

This is the required logic circuit which is represented by the given expression.

***

Example 8: Given the expression $(x'_1 \vee (x_2 \wedge x'_3)) \wedge (x_2 \vee x'_4)$, find the corresponding circuit, where $x_i (1 \leq i \leq 4)$ are assumed to be inputs to the circuitry.

Solution: We first consider the circuits representing the expressions $x_2 \wedge x'_3$ and $x_2 \vee x'_4$. They are as shown in Fig.13(a).

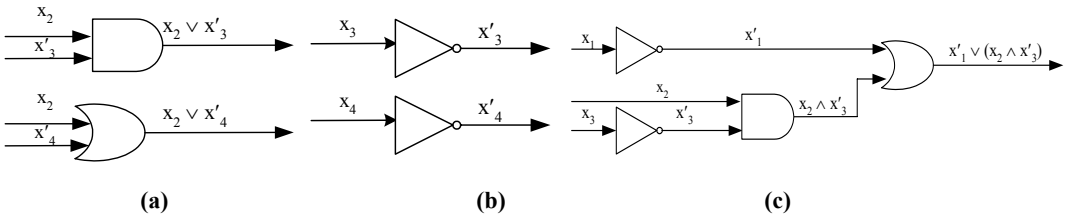


Fig. 13: Construction of a logic circuitry.

Also you know that the literals x'_3 and x'_4 are outputs of the **NOT**-gate. So, these can be represented by logic gates as shown in Fig.13(b). Then the circuit for the part $x'_1 \vee (x_2 \wedge x'_3)$ of the given expression is as shown in Fig.13(c). You already know how to construct a logic circuit for the expression $x_2 \vee x'_4$.

Finally, the two expressions $(x'_1 \vee (x_2 \wedge x'_3))$ and $(x_2 \vee x'_4)$ being connected by the connective $\wedge$ (**AND**), give the required circuit for the given expression as shown in Fig.14.

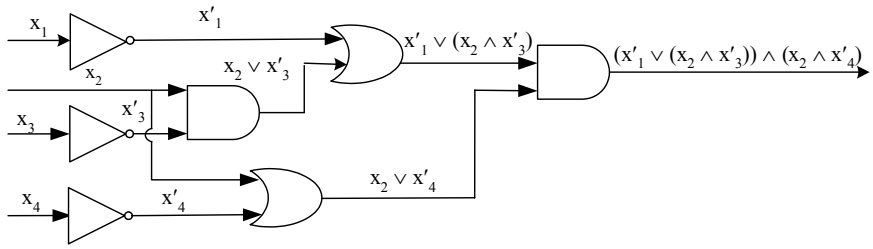


Fig. 14: Circuitry for the expression $(x'_1 \vee (x_2 \wedge x'_3)) \wedge (x_2 \vee x'_4)$.

***

Why don't you try to solve some exercises now?

E7) Find the logic circuit corresponding to the expression $x'_1 \wedge (x_2 \vee x'_3)$.

E8) Construct the logic circuit and obtain the logic table for the expression $x_1 \vee (x'_2 \wedge x_3)$.

So far we have established a one-to-one correspondence between logic circuits and Boolean expressions. You may wonder about the utility of this. The mathematical view of a circuit can help us understand the **overall functioning** of the circuit. To understand how, consider the circuit given in Fig.10 earlier.

You may think of the inputs bits x_1 , x_2 , and x_3 as three variables, each one of which is known to have two values only, namely, 0 or 1, depending upon the level of voltage these inputs have at any moment of time. Then the idea is to evaluate the expression $(x_1 \vee x_2)' \wedge x_3$, which corresponds to this circuit, for different values of the 3-tuple (x_1 , x_2 , x_3).

How does this evaluation help us to understand the functioning of the circuit? To see this, consider a situation in which the settings of x_1 , x_2 and x_3 at a certain stage of the process are $x_1 = x_3 = 0$ and $x_2 = 1$. Then we know that $x_1 \vee x_2 = 0 \vee 1 = 1$ (see the second row of Table 3 given earlier). Further, using the logic table of a **NOT**-gate, we get $(x_1 \vee x_2)' = 1' = 0$. Finally, from Table 3, we get $(x_1 \vee x_2)' \wedge x_3 = 0 \wedge 1 = 0$. Thus, the expression $(x_1 \vee x_2)' \wedge x_3$ has value 0 for the set of values (0, 1, 0) of input bits (x_1 , x_2 , x_3). **Thus, if x 1 and x 3 are closed, while x_2 is open, the circuit remains closed.**

Using similar arguments, you can very easily calculate the other values of the expression $(x_1 \vee x_2)' \wedge x_3$ in the set

$$\{0,1\}^3 = \{(x_1 , x_2 , x_3) \mid x_i = 0 \text{ or } 1,\ 1 \leq i \leq 3\}$$

of values of input bits. We have recorded them in Table 6.

Observe that the row entries in the first three columns of Table 6 represent the different values which the input bits (x_1 , x_2 , x_3) may take. Each entry in the last column of the table gives the output of the circuit represented by the expression $(x_1 \vee x_2)' \wedge x_3$ for the corresponding set of values of (x_1 , x_2 , x_3). For example, if (x_1 , x_2 , x_3) is (0,1,0), then the level of voltage in the output lead is at a level 0 (see the third row of Table 6).

You should verify that the values in the other rows are correct.

Table 6: Logic table for the expression $(x_1 \vee x_2)' \wedge x_3$.

Table 6 is the **logic table** for the circuit given in Fig. 10.

x_1	x_2	x_3	$x_1 \vee x_2$	$(x_1 \vee x_2)$	$(x_1 \vee x_2)' \wedge x_3$
0	0	0	0	1	0
0	0	1	0	1	1
0	1	0	1	0	0
1	0	0	1	0	0
0	1	1	1	0	0
1	1	0	1	0	0
1	0	1	1	0	0
1	1	1	1	0	0

Why don't you try an exercise now?

E9) Compute the logic table for the circuit given in E6(b) above.

You have seen how the logic table of an expression representing a circuit provides a functional relationship between the state (or level) of voltage in the input terminals and that in the output lead of that logic circuitry. This leads us the concept of Boolean functions, which we will now discuss.

3.4 BOOLEAN FUNCTIONS

In the last section you studied that an output expression is not merely a device for representing an interconnection of gates. It also defines output values as a function of input bits. This provides information about the overall functioning of the corresponding logic circuit. So, this function gives us a relation between **the inputs to the circuit** and its **final output** .

This is what helps us to understand control over the functioning of logic circuits from a mathematical point of view. To explain what this means, let us reformulate the logic tables in terms of functions of the input bits.

Let us first consider the Boolean expression

$$X(x_1 , x_2) = x_1 \wedge x'_2,$$

where x_1 and x_2 take values in $\mathcal{B} = \{0, 1\}$. You know that all the values of this expression, for different pairs of values of the variables x_1 and x_2 , can be calculated by using properties of the Boolean algebra $\mathcal{B}$. For example,

$$0 \wedge 1' = 0 \wedge 0 = 0 \Rightarrow X(0, 1) = 0.$$

Similarly, you can calculate the other values of $X(x_1, x_2) = x_1 \wedge x'_2$ over $\mathcal{B}$.

In this way we have obtained a function $f : \mathcal{B}_2 \to B$, defined as follows:

$$f(e_1 , e_2) = X(e_1 , e_2) = e_1 \wedge e'_2 , \text{ where } e_1 , e_2 \in \{0, 1\}.$$

So f is obtained by replacing x_i with e_i in the expression $X(x_1 , x_2)$. For example, when $e_1 = 1$, $e_2 = 0$, we get $f(1, 0) = 1 \wedge 0' = 1$.

More generally, each Boolean expression $X(x_1 , x_2 , \ldots , x_k)$ in k variables, where

each variable can take values from the two-element Boolean algebra $\mathcal{B}$, defines a function $f : B^k \to B : f(e_1 , \ldots , e_k) = X(e_1 , \ldots , e_k)$.

Any such function is called a **Boolean function.**
Thus, each Boolean expression over $\mathcal{B} = \{0, 1\}$ gives rise to a Boolean function.
In particular, corresponding to each circuit, we get a Boolean function.
Therefore, the logic table of a circuit is just another way of representing the Boolean function corresponding to it.

For example, the logic table of an **AND**-gate can be obtained using the function $\wedge : \mathcal{B}^2 \to B : \wedge (e_1 , e_2) = e_1 \wedge e_2$.

To make matters more clear, let us work out an example.

Example 9: Let $f : \mathcal{B}^2 \to \mathcal{B}$ denote the function which is defined by the Boolean expression $X(x_1 , x_2) = x'_1 \wedge x'_2$. Write the values of f in tabular form.

Solution: f is defined by $f(e_1 , e_2) = e'_1 \wedge e'_2$ for $e_1 , e_2 \in \{0, 1\}$. Using Tables 3, 4 and 5, we have

$f(0, 0) = 0' \wedge 0' = 1 \wedge 1 = 1$, $f(0, 1) = 0' \wedge 1' = 1 \wedge 0 = 0$,
$f(1, 0) = 1' \wedge 0' = 0 \wedge 1 = 0$, $f(1, 1) = 1' \wedge 1' = 0 \wedge 0 = 0$.

We write this information in Table 7.

Table 7: Boolean function for the expression $x'_1 \wedge x'_2$.

e_1	e_2	e'_1	e'_2	$f(e_1, e_) = e'_1 \wedge e'_2$
0	0	1	1	$1 \wedge 1 = 1$
0	1	1	0	$1 \wedge 0 = 0$
1	0	0	1	$0 \wedge 1 = 0$
1	1	0	0	$0 \wedge 0 = 0$

***

Why don't you try an exercise now?

E10) Find all the values of the Boolean function $f : \mathcal{B}_2 \to \mathcal{B}$ defined by the Boolean expression $(x_1 \wedge x_2) \vee (x_1 \wedge x'_3)$.

Let us now consider the Boolean function $g : \mathcal{B}_2 \to \mathcal{B}$, defined by the expression $X(x_1 , x_2) = (x_1 \vee x_2)'$.
Then $g(e_1 , e_2) = (e_1 \vee e_2)' , e_1 , e_2 \varepsilon \mathcal{B}$.

So, the different values that g will take are

$g(0, 0) = (0 \vee 0)' = 0' = 1$, $g(0, 1) = (0 \vee 1)' = 1' = 0$,
$g(1, 0) = (1 \vee 0)' = 1' = 0$, $g(1, 1) = (1 \vee 1)' = 1' = 0$.

In tabular form, the values of g can be presented as in Table 8.

Table 8: Boolean function of the expression $(x_1 \vee x_2)'$.

e_1	e_2	$e_1 \vee e_2$	$g(e_1, e_2) = (e_1 \vee e_2)'$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

By comparing Tables 7 and 8, you can see that $f(e_1 , e_2) = g(e_1 , e_2)$ for all

$(e_1 , e_2) \in \mathcal{B}^2$. So f and g are the same function.

What you have just seen is that **two (seemingly) different Boolean expressions can have the same Boolean function specifying them.** Note that if we replace the input bits by propositions in the two expressions involved, then we get logically equivalent statements. This may give you some idea of how the two Boolean expressions are related. We give a formal definition below.

Definition : Let $X = X(x_1 , x_2 , \ldots , x_k)$ and $Y = Y(x_1 , x_2 , \ldots , x_k)$ be two Boolean expressions in the k variables $x_1 , \ldots , x_k$. We say **X is equivalent to Y** over the Boolean algebra $\mathcal{B}$, and write **$X \equiv Y$,** if both the expressions X and Y define the same Boolean function over $\mathcal{B}$, i.e.,

$$X(e_1 , e_2 , \ldots , e_k) = Y(e_1 , e_2 , \ldots , e_k), \text{ for all } e_i \in \{0, 1\}.$$

So, the expressions to which f and g (given by Tables 7 and 8) correspond are equivalent.

Why don't you try an exercise now?

E11) Show that the Boolean expressions
$X = (x_1 \wedge x_2) \vee (x_1 \wedge x_3)$ and $Y = x_1 \wedge (x_2 \vee x'_3)$
are equivalent over the two-element Boolean algebra $\mathcal{B} = \{0, 1\}$.

So far you have seen that given a circuit, we can define a Boolean function corresponding to it. You also know that given a Boolean expression over $\mathcal{B}$, there is a circuit corresponding to it. Now, you may ask:

Given a Boolean function $f : \mathcal{B}^n \to \mathcal{B}$, is it always possible to get a Boolean expression which will specify f over B? The answer is `yes', i.e., for every function $f : \mathcal{B}^n \to \mathcal{B}$ ($n \geq 2$) there is a Boolean expression (in n variables) whose Boolean function is f itself.

To help you understand the underlying procedure, consider the following examples.

Example 10: Let $f : \mathcal{B}^2 \to \mathcal{B}$ be a function which is defined by
$f(0, 0) = 1, f(1, 0) = 0, f(0, 1) = 1, f(1, 1) = 1.$

Find the Boolean expression specifying the function f.

Solution: f can be represented by the following table.

Input		Output
x_1	x_2	$f(x_1, x_2)$
0	0	1
1	0	0
0	1	1
1	1	1

We find the Boolean expression according to the following algorithm:

In Boolean algebra terminology this is known as the 'disjunctive normal form' (DNF) of the expression.

Step 1: Identify all rows of the table where the output is 1: these are the 1st, 3rd and 4th rows.

Step 2: Combine the variables in each of the rows identified in Step 1 with `and'. Simultaneously, apply `not' to the variables with value zero in these rows. So, for the
1st row: $x'_1 \wedge x'_2$,

3rd row: $x'_1 \wedge x_2$,
4th row: $x_1 \wedge x_2$.

Step 3: Combine the Boolean expressions obtained in Step 2 with `or' to get the compound expression representing f:
So, $f(x_1 , x_2) = (x'_1 \wedge x'_2) \vee (x'_1 \wedge x_2) \vee (x_1 \wedge x_2)$.

***

You can complete Example 10, by doing the following exercise.

E12) In the previous example, show that $X(e_1 , e_2) = f(e_1 , e_2) \; \forall e_1 , e_2 \in \mathcal{B}$.

E13) By Theorem 2, we could also have obtained the expression of f in Example 10 in `conjunctive normal form' (CNF). Please do so.

An important remark: To get a Boolean expression for a Boolean function h (say), we should first see how many points v_i there are at which $h(v_i) = 0$, and how many points v_i there are at which $h(v_i) = 1$. **If the number of values for which the function h is 0 is less than the number of values at which h is 1, then we shall choose to obtain the expression in CNF, and not in DNF.** This will give us a shorter Boolean expression, and hence, a simpler circuit. For similar reasons, we will prefer DNF if the number of values at which h is 0 is more.

Why don't you apply this remark now?

E14) Find the Boolean expressions, in DNF or in CNF (keeping in mind the remark made above), for the functions defined in tabular form below.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

(a)

x_1	x_2	x_3	$g(x_1, x_2, x_3)$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

(b)

Boolean functions tell us about the functioning of the corresponding circuit. Therefore, circuits represented by two equivalent expressions should essentially do the same job. We use this fact while redesigning a circuit to create a simpler one. In fact, in such a simplification process of a circuit, we write an expression for the circuit and then evaluate the same (over two-element Boolean algebra $\mathcal{B}$) to get the Boolean function. Next, we proceed to get an equivalent, simpler expression. Finally, the process terminates with the construction of the circuit for this simpler expression. Note that, **as the two expressions are equivalent, the circuit represented by the simpler expression will do exactly the same job as the circuit represented by the original expression.**

Let us illustrate this process by an example in some detail.

Example 11: Design a logic circuit capable of operating a central light bulb in a hall by three switches x_1 , x_2 , x_3 (say) placed at the three entrances to that hall.

Solution: Let us consider the procedure stepwise.
Step 1: To obtain the function corresponding to the unspecified circuit.

To start with, we may assume that the bulb is off when all the switches are off. Mathematically, this demands a situation where $x_1 = x_2 = x_3 = 0$ implies $f(0, 0, 0) = 0$, where f is the function which depicts the functional utility of the circuit to be designed.
Let us now see how to obtain the other values of f. Note that every change in the state of a switch should alternately put the light bulb on or off. Using this fact repeatedly, we obtain the other values of the function f.

Now, if we assign the value (1,0,0) to (x_1 , x_2 , x_3), it brings a single change in the state of the switch x_1 only. So, the light bulb must be on. This can be written mathematically in the form $f(1, 0, 0) = 1$. Here the value 1 of f stands for the on state of the light bulb.
Then, we must have $f(1, 1, 0) = 0$, because there is yet another change, now in the state of switch x_2 .

You can verify that the other values of $f(x_1 , x_2 , x_3)$ are given as in Table 9.

Table 9: Function of a circuitry for a three-point functional bulb.

x_1	x_2	X_3	$f(x_1, x_2, x_3)$
0	0	0	0
1	0	0	1
1	1	0	0
1	1	1	1
0	1	0	1
0	1	1	0
0	0	1	1
1	0	1	0

Step 2: To obtain a Boolean expression which will specify the function f. Firstly, note that the number of 1's in the last column of Table 9 are fewer than the number of 0's. So we shall obtain the expression in DNF (instead of CNF).

By following the stepwise procedure of Example 10, you can see that the required Boolean expression is given by

$$X(x_1 , x_2 , x_3) = (x_1 \wedge x'_2 \wedge x_3) \vee (x'_1 \wedge x_2 \wedge x'_3) \vee (x'_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$$

At this stage we can directly jump into the construction of the circuit for this expression (using methods discussed in Sec.3.3). But why not try to get a simpler circuit?

Step 3 : To simplify the expression $X(x_1 , x_2 , x_3)$ given above. Firstly, observe that

$$\begin{aligned}(x_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3) &= x_1 \wedge [(x'_2 \wedge x_3) \vee (x_2 \wedge x_3)] \\ &= x_1 \wedge [(x'_2 \vee x_2) \wedge x_3] \\ &= x_1 \wedge (1 \wedge x_3) \\ &= x_1 \wedge x_3 ,\end{aligned}$$

by using distributive, complementation and identity laws (in that order).
Similarly, you can see that

$$(x'_1 \wedge x'_2 \wedge x_3) \vee (x_1 \wedge x_3) = (x'_2 \vee x_1) \wedge x_3 .$$

We thus have obtained a simpler (and equivalent) expression, namely,

$$X(x_1 , x_2 , x_3) = (x'_1 \wedge x_2 \wedge x'_3) \vee [(x'_2 \vee x_1) \wedge x_3] ,$$

whose Boolean function is same as the function f. (Verify this!)

Step 4: To design a circuit for the expression obtained in Step 3.

Now, the logic circuit corresponding to the simpler (and equivalent) expression

obtained in Step 3 is as shown in Fig.15.

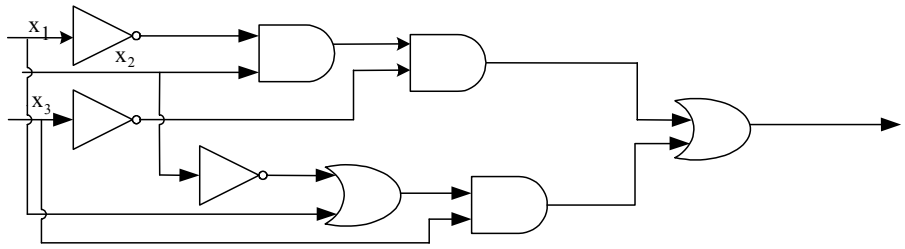


Fig. 15: A circuit for the expression $(x'_1 \wedge x_2 \wedge x'_3) \vee ((x'_2 \vee x_1) \wedge x_3)$

So, in 4 steps we have designed a 3-switch circuit for the hall.

***

We can't claim that the circuit designed in the example above is the simplest circuit. How to get that is a different story and is beyond the scope of the present course.

Why don't you try an exercise now?

E15) Design a logic circuit to operate a light bulb by two switches, x_1 and x_2 (say).

We have now come to the end of our discussion on applications of logic. Let us briefly recapitulate what we have discussed here.

3.5 SUMMARY

In this unit, we have considered the following points.

1. The definition and examples of a Boolean algebra. In particular, we have discussed the two-element Boolean algebra $\mathcal{B} = \{0, 1\}$, and the switching algebras B_n, $n \geq 2$.
2. The definition and examples of a Boolean expression.
3. The three elementary logic gates, namely, **AND**-gate, **OR**-gate and **NOT**-gate; and the analogy between their functioning and operations of logical connectives.
4. The method of construction of a logic circuit corresponding to a given Boolean expression, and vice-versa.
5. How to obtain the logic table of a Boolean expression, and its utility in the understanding of the overall functioning of a circuit.
6. The method of simplifying a Boolean expression.
7. The method of construction of a Boolean function $f : \mathcal{B}^n \rightarrow B$, corresponding to a Boolean expression, and the concept of **equivalent** Boolean expressions.
8. Examples of the use of Boolean algebra techniques for constructing a logic circuit which can function in a specified manner.

3.6 SOLUTIONS/ ANSWERS

E1) a) In E19 of Unit 1, you have already verified the Identity laws. Let us proceed to show that the propositions $p \vee (p \wedge q)$ and p are logically equivalent. It suffices to show that the truth tables of both these propositions are the same. This follows from the first and last columns of the following table.

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

Similarly, you can see that the propositions $p \wedge (p \vee q)$ and p are equivalent propositions. This establishes the absorption laws for the Boolean algebra $(S, \wedge, \vee', \mathcal{T}, \mathcal{F})$.

b) Let A and B be two subsets of the set X. Since $A \cap B \subseteq A$, $(A \cap B) \cup A = A$. Similarly, as $A \subseteq A \cup B$, we have $(A \cup B) \cap A = A$. Thus, both the forms of the absorption laws hold good for the Boolean algebra $(\mathcal{P}(X), \cup, \cap, ^c, X,)$.

E2) We can write

$$X(x_1, x_2, x_3) = ((x_1 \wedge x_2) \vee ((x_1 \wedge x_2) \wedge x_3)) \vee (x_2 \wedge x_3)$$
$$= (x_1 \wedge x_2) \vee (x_2 \wedge x_3) \quad \text{(by Absorption law)}$$
$$= x_2 \wedge (x_1 \vee x_3) \quad \text{(by Distributive law)}$$

This is the simplest form of the given expression.

E3) Take the propositions p and q in place of the bits x_1 and x_2, respectively. Then, when 1 and 0 are replaced by T and F in Table 3 here, we get the truth table for the proposition $p \wedge q$ (see Table 2 of Unit 1).
This establishes the analogy between the functioning of the **AND**-gate and the conjunction operation on the set of propositions.

E4) Take the propositions p and q in place of the bits x_1 and x_2, respectively. Then, when 1 and 0 are replaced by T and F in Table 4 here, we get the truth table for the proposition $p \vee q$ (see Table 1 of Unit 1).
This establishes the analogy between the functioning of the **OR**-gate and the disjunction operation on the set of propositions.

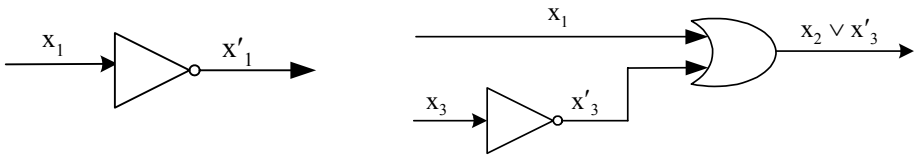
E5) Firstly, observe that the information about the outputs of the three elementary gates, for different values of inputs, can also be written as follows:

$0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0$, $1 \wedge 1 = 1$; (see Table 3)
$0 \vee 0 = 0$, $0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$; and (see Table 4)
$0' = 1$, $1' = 0$. (see Table 5)

Clearly, then both the operations # and # are the binary operations on $\mathcal{B}$ and $' : \mathcal{B} \to \mathcal{B}$ is a unary operation. Also, we may take 0 for **O** and 1 for **I** in the definition of a Boolean algebra.
Now, by looking at the logic tables of the three elementary gates, you can see that all the five laws B1-B5 are satisfied. Thus, $\mathcal{B}$ is a Boolean algebra.

E6) a) Here x_1 and x_2 are inputs to an **OR**-gate, and so, we take $x_1 \vee x_2$ as input to the **NOT**-gate next in the chain which, in turn, yields $(x_1 \vee x_2)'$ as the required output expression for the circuit given in (a).
b) Here x_1 and x_2 are the inputs to an **AND**-gate. So, the expression $x_1 \wedge x_2$ serves as an input to the **NOT**-gate, being next in the chain.
This gives the expression $(x_1 \wedge x_2)'$ which serves as one input to the extreme right **AND**-gate. Also, since x'_3 is another input to this **AND**-gate (coming out of a **NOT**-gate), we get the expression $(x_1 \wedge x_2)' \wedge x'_3$ as the final output expression which represents the circuit given in (b).

E7) You know that the circuit representing expressions x_1 and $x_2 \vee x'_3$ are as shown in Fig.16 (a) and (b) below.



(a) **(b)**

Fig. 16

Thus, the expression $x'_1 \vee (x_2 \vee x'_3)$, being connected by the symbol $\wedge$, gives the circuit corresponding to it as given in Fig.17 below.

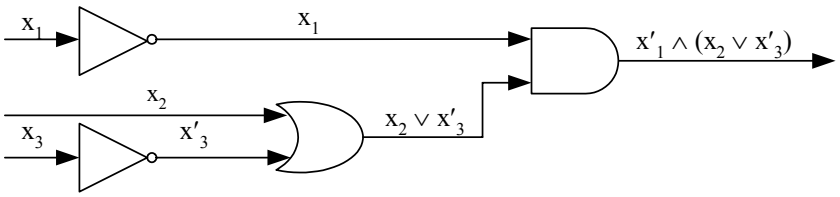


Fig. 17: A logic circuit for the expression $x'_1 \wedge (x_2 \vee x'_3)$

E8) You can easily see, by following the arguments given in E9, that the circuit represented by the expression $x_1 \vee (x'_2 \wedge x_3)$ is as given in Fig.18.

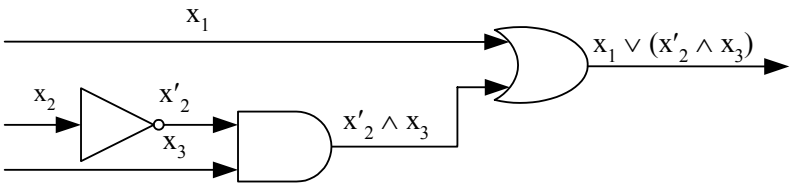


Fig. 18

The logic table of this expression is as given below.

x_1	x_2	x_3	x'_2	$x'_2 \wedge x_3$	$X_1 \vee (x'_2 \wedge x_3)$
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	0	0	0
1	0	0	1	0	1
0	1	1	0	0	0
1	1	0	0	0	1
1	0	1	1	1	1
1	1	1	0	0	1

E9) Since the output expression representing the circuit given in E8(b) is found to be $(x_1 \wedge x_2)' \wedge x'_3$, the logic table for this circuit is as given below.

x_1	x_2	x_3	$x_1 \wedge x_2$	$(x_1 \wedge x_2)'$	x'_3	$(x_1 \wedge x_2)' \wedge x'_3$
0	0	0	0	1	1	1
0	0	1	0	1	0	0
0	1	0	0	1	1	1
1	0	0	0	1	1	1
0	1	1	0	1	0	0
1	1	0	1	0	1	0
1	0	1	0	1	0	0
1	1	1	1	0	0	0

E10) Because the expression $(x_1 \wedge x_2) \vee (x_1 \wedge x'_3)$ involves three variables, the

corresponding Boolean function, f (say) is a three variable function, i.e. f : $B_3 \to B$. It is defined by

$f(e_1, e_2, e_3) = (e_1 \wedge e_2) \vee (e_1 \wedge e'_3)$, e_1, e_2 and $e_3 \in B$.

Now, you can verify that the values of f in tabular form are as given in the following table.

e_1	e_2	E_3	$e_1 \wedge e_2$	e'_3	$e_1 \wedge e'_3$	$f(e_1, e_2, e_3) = (e_1 \wedge e_2) \vee (e_1 \wedge e'_3)$
0	0	0	0	1	0	0
0	0	1	0	0	0	0
0	1	0	0	1	0	0
1	0	0	0	1	1	1
0	1	1	0	0	0	0
1	1	0	1	1	1	1
1	0	1	0	0	0	0
1	1	1	1	0	0	1

E11) To show that the Boolean expressions X and Y are equivalent over the two-element Boolean algebra $B = \{0, 1\}$, it suffices to show that the Boolean functions f and g (say) corresponding to the expressions X and Y, respectively, are the same. As you can see, the function f for the expression X is calculated in E10 above.
Similarly, you can see that the Boolean function g for the expression Y in tabular form is as given below.

x_1	x_2	x_3	x'_3	$x_2 \vee x'_3$	$G(x_1, x_2, x_3) = X_1 \wedge (x_2 \vee x'_3)$
0	0	0	1	1	0
0	0	1	0	0	0
0	1	0	1	1	0
1	0	0	1	1	1
0	1	1	0	1	0
1	1	0	1	1	1
1	0	1	0	0	0
1	1	1	0	1	1

Comparing the last columns of this table and the one given in E10 above, you can see that $f(e_1, e_2, e_3) = g(e_1, e_2, e_3) \; \forall \; e_1, e_2, e_3 \in B = \{0, 1\}$. Thus, **X** and **Y** are equivalent.

E12) Firstly, let us evaluate the given expression $X(x_1, x_2)$ over the two-element Boolean algebra $B = \{0, 1\}$ as follows:

$X(0, 0) = (0' \wedge 0') \vee (0' \wedge 0) \vee (0 \wedge 0)$
$= (1 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 0)$
$= 1 \vee 0 \vee 0 = 1 = f(0, 0);$

$X(1, 0) = (1' \wedge 0') \vee (1' \wedge 0) \vee (1 \wedge 0)$
$= (0 \wedge 1) \vee (0 \wedge 0) \vee (1 \wedge 0)$
$= 0 \vee 0 \vee 0 = 0 = f(1, 0);$

$X(0, 1) = (0' \wedge 1') \vee (0' \wedge 1) \vee (0 \wedge 1)$
$= (1 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 1)$
$= 0 \vee 1 \vee 0 = 1 = f(0, 1);$

$X(1, 1) = (1' \wedge 1') \vee (1' \wedge 1) \vee (1 \wedge 1)$
$= (0 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 1)$

$= \quad 0 \vee 0 \vee 1 = 1 = f(1, 1).$

It thus follows that $\mathbf{X}(e_1, e_2) = f(e_1, e_2) \; \forall \; e_1, e_2 \in \boldsymbol{B} = \{0, 1\}$.

E13) **Step 1:** Identify all rows of the table where output is 0: This is the 2nd row.
Step 2: Combine x_1 and x_2 with `or' in these rows, simultaneously applying `not' to x_i if its value is 0 in the row: So, for the 2nd row the expression we have is $x_1 \vee x_2$.
Step 3: Combine all the expressions obtained in Step 2 with `and' to get the **CNF** form representing f: In this case there is only 1 expression.
So f is represented by $x_1 \vee x_2$ in CNF.

E14) a) Observe from the given table that, among the two values 0 and 1 of the function $f(x_1, x_2, x_3)$, the value 1 occurs the least number of times. Therefore, by the remark made after **E 13**, we would prefer to obtain the Boolean expression in **DNF**. To get this we will use the stepwise procedure adopted in Example 10.
Accordingly, the required Boolean expression in DNF is given by

$$X(x_1, x_2, x_3) = (x_1 \wedge x_2 \wedge x_3) \wedge (x_1 \wedge x'_2 \wedge x'_3) \vee (x'_1 \wedge x'_2 \wedge x'_3).$$

b) By the given table, among the two values 0 and 1 of the function the points v i at which $g(v_i) = 0$ are fewer than the points v_i at which $g(v_i) = 1$. So we would prefer to obtain the corresponding Boolean expression in CNF.
Applying the stepwise procedure in the solution to E13, the required Boolean expression (in CNF) is given by

$$X(x_1, x_2, x_3) = (x'_1 \vee x_2 \vee x'_3) \wedge (x_1 \vee x'_2 \vee x'_3) \wedge (x_1 \vee x'_2 \vee x_3).$$

E15) Let g denote the function which depicts the functional utility of the circuit to be designed. We may assume that the light bulb is off when both the switches x_1 and x_2 are off, i.e., we write $g(0, 0) = 0$.
Now, by arguments used while calculating the entries of Table 9, you can easily see that all the values of the function g are as given below:

$$g(0, 0) = 0, \; g(0, 1) = 1, \; g(1, 0) = 1, \; g(1, 1) = 0.$$

Thus, proceeding as in the previous exercise, it can be seen that the Boolean expression (in DNF), which yields g as its Boolean function, is given by the expression

$$X(x_1, x_2) = (x'_1 \wedge x_2) \vee (x_1 \wedge x'_2),$$

because $g(0, 1) = 1$ and $g(1, 0) = 1$.

Finally, the logic circuit corresponding to this Boolean expression is shown in Fig. 19.

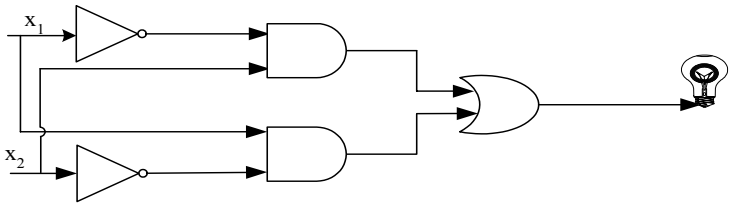


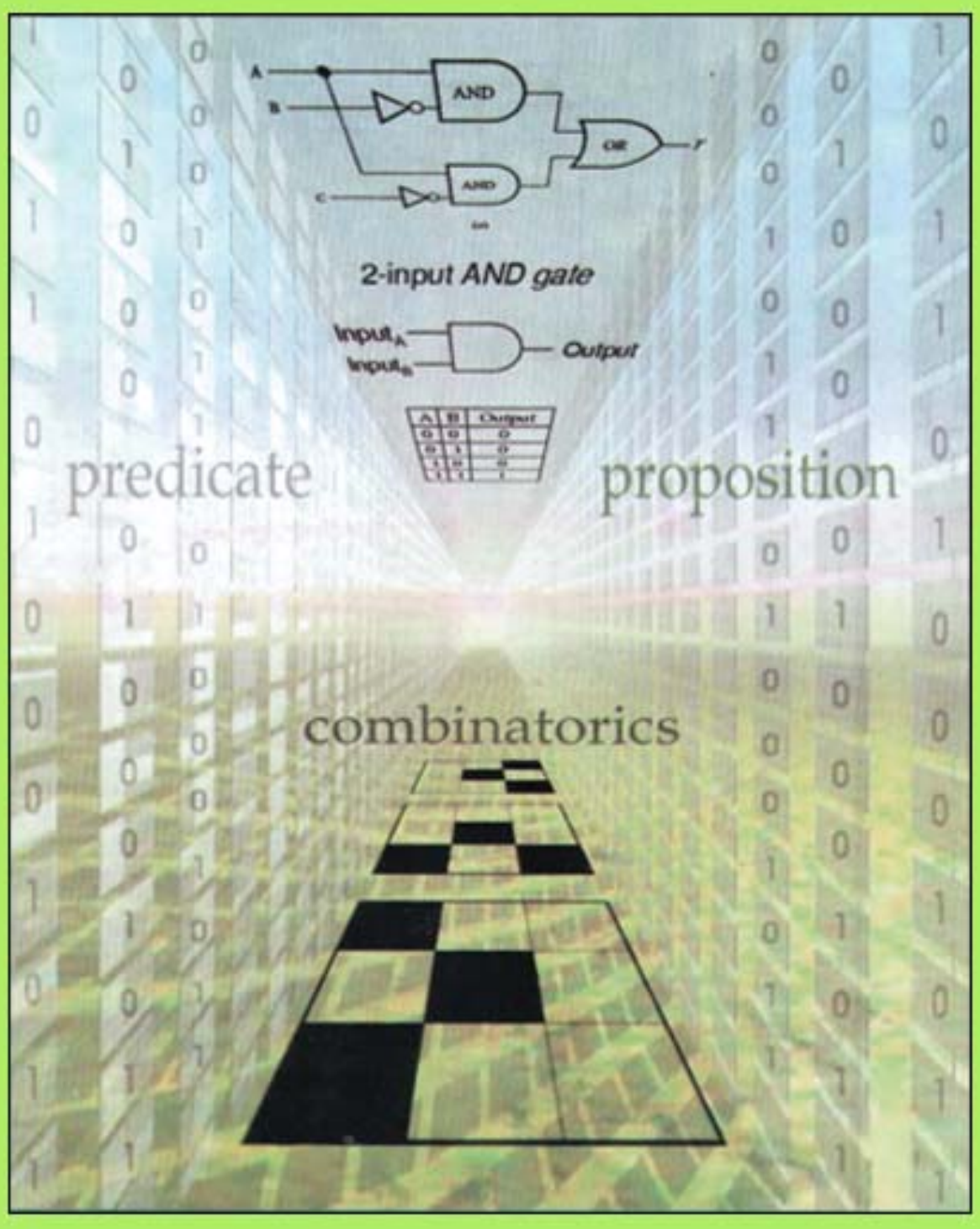
Fig. 19

SOCIAS-IGNOU/P.O.10.5T/MAY, 2004

Indira Gandhi National Open University
School of Computer and Information Sciences

MCS-013

DISCRETE MATHEMATICS



Basic Combinatorics 2

Indira Gandhi
National Open University
School of Computer and
Information Sciences

MCS-013
DISCRETE MATHEMATICS

Block

2

BASIC COMBINATORICS

Programme / Course Design Committee

Prof. Sanjeev K. Aggarwal, IIT, Kanpur
Prof. M. Balakrishnan, IIT , Delhi
Prof Harish Karnick, IIT, Kanpur
Prof. C. Pandurangan, IIT, Madras
Dr. Om Vikas, Sr. Director, MIT
Prof P. S. Grover, Sr. Consultant, SOCIS, IGNOU

Faculty of School of Computer and Information Sciences
Shri Shashi Bhushan
Shri Akshay Kumar
Prof Manohar Lal
Shri V.V. Subrahmanyam
Shri P.Venkata Suresh

Block Preparation Team

Prof. Parvin Sinclair (Editor)
SOS, IGNOU

Shri M.P. Mishra
SOCIS, IGNOU

Partially based on Block-2, MTE-13.

Course Coordinator : Shri M.P.Mishra

Block Production

Shri H.K. Som, SOCIS

May, 2004

ISBN – 81- 266-1232-0

Printed and published on behalf on the Indira Gandhi National Open University, New Delhi by the Director, SOCIS.

BLOCK 2 BASIC COMBINATORICS

Have you ever thought about how you can decide whether a given element belongs to a collection or not? Or, how a communication engineer can find the total number of distinct ways in which a fixed number of dots and dashes can be used for telegraphic communication? Or, how we can count the number of primes less than or equal to a given number? Problems such as these are what we discuss in this block. The focus of this block is a variety of techniques used for counting, that is, combinatorial techniques. We use them to study the problem of determining the size, and in some cases also the structure, of various sets that arise in such diverse applications as games theory, probability, and algorithm analysis.

This block consists of four units. The first unit deals with sets, relations and functions. In this we discuss the basic concepts moreover we also expose you to different representations of sets, including the Venn diagram invented by the English Priest and logician John Venn (1834-1923). Then we consider operations on sets, different types of relations, functions and operations and functions.

In second unit we deal with permutations and combinations, the binomial and multinomial theorems, and combinatorial probability. In this context, you might find it interesting to note that the notion of permutation can be found in the Hebrew work "Sefer Yetzirah" (i.e., The Book of Creation). This is a manuscript written by a mystic some time between 200 and 600 A.D. Also, the 'binomial theorem', which everybody is so familiar with, first appeared in the work of Euclid (300 B.C.) What is of further historical interest is that Blaise Pascal (1623-1662), published in the 1650s a treatise dealing with the relationships among binomial coefficients, combinations, and polynomials. These results were used by Jakob Bernoulli (1645-1705) to prove the general form of the binomial theorem.

The third unit of this block deals with the pigeonhole principle and the principles of inclusion and exclusion. The latter principle has an interesting history, being found in different manuscripts under such names as the "Sieve Method" or the "Principle of Cross Classification". A set-theoretic version of this principle, which concerned itself with set unions and intersection, is found in "Doctrine of Chances" (1718), a text on probability theory by Abraham De Moivre (1667-1754). Somewhat earlier, in 1713, Pierre Remond de Montmort (1678-1719) used the idea behind the principle in his solution of the problem of derangements.

On the other hand, the pigeonhole principle has no clear-cut mathematical origin. This is also known as the Dirichlet-drawer principle, after the famous German mathematician Dirichlet (1805-1859).

In the fourth, and last, unit of this block, we discuss partitions of natural numbers. We consider efficient techniques for counting the number of ways of distributing a finite number of objects into a finite number of containers, usually called boxes. It was Leonard Euler (1707-1783) who advanced the study of partitions of integers in his 1740 volume opus, "Introduction in Analysin Infinitorum".

Before we end, a note of advice! If you really want to get to grips with the content of this block, you must attempt the Miscellaneous Exercises given at the end of the block. Doing this, will help you understand the underlying reasoning better, and hence appreciate the theory of combinatorics.

NOTATIONS AND SYMBOLS

$\cap$	Intersection of two Sets
$\cup$	Union of two Sets
$\subseteq$	Subsets
$\supseteq$	Contains
$\sim$	Set difference
$\forall$	For all
$\exists$	There exists
ϕ	Empty Set
N	Set of natural numbers
R	Set of real numbers
Z	Set of integers
n!	n(n −1)...2.1
P(n,r)	$\frac{n!}{(n-r)!}$
C(n,r)	$\frac{n!}{(n-r)!r!}$
$P(n;r_1,r_2,\ldots r_k)$	$\frac{n!}{r_1!r_2!\ldots_k!}$
n(A),|A|	The cardinality of the set A
P(X)	The power set of the set X
P(A)	The probability of the event A
P_n	The number of partitions of the natural number n
P_n^k	The number of partitions of n with exactly k parts
$P_n(k)$	The number of partitions of n with no part larger than k
$S_n^m (n \geq m)$	The Stirling number of the second kind
$[x]_n$	x(x-1)(x-2)….(x-n+1), i.e., falling factorial
D_n	The number of derangements of n objects.

UNIT 1 SETS, RELATIONS AND FUNCTIONS

Structure **Page No.**

1.0 INTRODUCTION

In common parlance, we find people using the words given in the title of this unit. Do they have the same meaning in mathematics? You'll find this out by studying this unit. You will also see how basic the concept of 'set' and 'function' or to any area of mathematics and subjects depend on mathematics.

In this unit we will begin by introducing you to various kinds of sets. You will also study operations like, 'union' and 'intersection'. While doing so you will see in what way Venn diagrams are a useful tool for understanding and working with sets.

Next we will discuss what a relation is, and expose you to some important types of relations. You will come across while studying banking, engineering, information technology and computer science, of course mathematics. As you will see in your study of computer science, an extensive use of functions is made in problem-solving.

Finally, we lead you detailed discussion of functions. Over here we particularly focus on various points of functions and fundamental operations on functions.

1.1 OBJECTIVES

After studying this unit, you should be able to:

- explain what a set , a relation or a function is
- give examples and non-examples of sets, relations and functions
- perform different operations on sets
- establish relationships between operations on sets and those on statements in logic
- use Venn diagrams
- explain the difference between a relation and a function.
- describe different types of relations and functions.
- define and perform the four basic operations on functions

1.2 INTRODUCING SETS

In our daily life we encounter collections, like the collection of coins of various countries, a collection of good students in a class, a collection of faculty members of

IGNOU, etc. In the first of these examples, it is easy for anybody anywhere to tell whether an object belongs to this collection or not. If we take the collection of coins of a country, then a coin will be in the collection if it is a coin of that country, not otherwise. The criterion for being a member of the collection is objective and clear. However, if we take the collection of all good students, it is very difficult to say whether a person belongs to this collection or not because the characteristic *good* is not very clearly defined. In this case the collection is not 'well-defined', while the previous collection is 'well-defined'. Similarly, the collection of all the IGNOU students is well-defined.

Definition: A **set** is a well-defined collection. The objects belonging to a set are called **elements** or **members** of that set.

We write the elements of a set within curly brackets. For instance, consider the set A of stationary items used by Nazia. We write this as

A = {pen, pencil, eraser, sharpener, paper}

Another example is the set

B = {Lucknow, Patna, Bhopal, Itanagar, Shillong}

of the capitals of 5 states of India.

Note that A and B are well-defined collections. However, the collection of short people is not well-defined, and therefore, it is not a set.

Also note that **the elements of a set don't have to appear 'similar'**. For example, **{pen,Lucknow,4} is a set** consisting of 3 clearly defined elements.

As you have seen, we usually, denote sets by capital letters of the English alphabet. We usually denote the elements by small letters a,b,x,y …. If x is an element of a set A, we write this as $\mathbf{x \in A}$ (read as 'x belongs to A'). If x is not an element of A, we write this as $\mathbf{x \notin A}$ (read as 'x does not belong to A').

There are three ways of representing sets: 'Set-builder form', 'Tabular form' and the pictorial representation through Venn diagrams.

In the **'Set-builder form',** or **'property method'** of representation of sets, we write between brackets { } a variable x, which stands for each of the elements of the set which have the properties p(x), and separate x and p(x) by a symbol ':' or '|' (read as 'such that'). So the set looks like {x: p(x)} or {x | p(x)}.

For instance, the set {x | x is a white flower} is the set of all white flowers, or {x: x is a natural number and $2<x<11$} is the set of natural numbers lying between 2 and 11.

In **'Tabular form'**, or the **'listing method'**, the elements of a set are listed one by one within the brackets { }, each separated from the other by a comma, as in the examples A and B given above.

The accepted convention for writing a set by the listing method is that elements will not be repeated. For example, in the set A= {4,2,8,2,6}, 2 is repeated, which is not necessary.So we will write A ={4,2,8,6}.

We shall introduce you to Venn diagrams a little later. For now, let us consider a few more sets.

Definition: A set with no element is called the **empty(**or **null**, or **void) set**, and is denoted by ϕ or{}.

For example A = {x:x is an integer between 13 and 17 which is divisible by 6}, has no element, i.e., A is the **empty set.**

Definition: A set having a finite number of elements is called a **finite set**.

For example, {1,2,4,6} is a finite set because it has four elements, ϕ, the null set, is also a finite set because it has zero number of elements; the set of stars in the sky is also a finite set.

Definition: A set having infinitely many elements is called an **infinite set**.

For example, the set **N** of natural numbers is infinite. Similarly, **Q , Z, R** and **C**, the set of rational numbers and complex numbers, respectively, are infinite set.

B= The set of all strengthness in a given plane.

Now try the following exercises.

E1) How would you represent the set of all students who have offered the IGNOU course?

E2) Explain, with reason, whether or not

i) the collection of all good teachers is a set

ii) the set of points on a line is finite.

E3) Represent the set of all integers by the listing method.

When we deal with several sets, we need to understand the nature of the elements of those sets, whether the elements of two given sets have some elements in common or not, and so on. These questions involve concepts, which we now define.

Definition: A set A is said to be a **subset** of a set B if each element of A is also an element of B. In this case B is called a **superset** of A. If A is a subset of B, we represent this by $\mathbf{A \subseteq B}$.

As a statement in logic we represent this situation as,

$A \subseteq B \Leftrightarrow [x \in A \Rightarrow x \in B]$

'B contains A' or 'B is a superset of A' is represented by $B \supseteq \mathbf{A}$.
If A is not a subset of B, we represent this by $\mathbf{A \not\subseteq B}$.

For example, if A ={4,5,6} and B ={4,5,7,8,6}, then $A \subseteq B$. But if C = {3,4} then $C \not\subseteq B$.

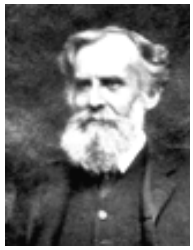
Remark: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Definition: Two sets A and B are **equal** if every element of A belongs to B and every element of B belongs to A. We represent this by **A=B**.

For example, if A= {1,2,3}, B ={2,3,1}, then $A \subseteq B$ and $B \subseteq A$, so that A = B.

Definition: A set A is said to be a **proper subset** of a set B if A is a subset of B and A and B are not equal. We represent this by $\mathbf{A \subset B}$.

For example, if A ={4,5,6} and B = {4,5,7,8,6}, then $A \subset B$; and if A={Java, C, C++, Cobol} and B={Java, C++}, then $A \supset B$.



(1834 -1923)
Fig 1: John Venn

Note: A set can have many subsets and many supersets. For example A={1,2,3,4,5}, B= {2,3,4,5,6,7}, and C= {2,3}, then for C, A and B can be used as supersets.

Similarly, if X= {Ram, Rani, Sita, Gita}, Y= {Rani}, and Z= {Sita}, then Y and Z both are subsets of X.

Definition: The **power set** of a set A is the set of all the subsets of A, and is denoted by **P(A)**.

Mathematically, $P(A) = \{ x : x \subseteq A \}$.

Note that $\phi \in P(A)$ and $A \in P(A)$ for all sets A.

For example, if A={1}, then P(A)= $\{\phi, \{1\}\}$ and

if A= {1,2}, then P(A)=$\{\phi$, {1}, {2}, {1,2}$\}$

Similarly, if A = {1,2,3}, then P(A) = $\{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Definition: Any set which is a **superset** of all the sets **under consideration** is known as the **universal set**. This is usually denoted by Ω**, S** or **U.**

For example, if A = {1,2,3}, B = {3,4,6,9} and C = {0,1}, then we can take U = {0,1,2,3,4,5,6,7,8,9} or U= **N**, or U=**Z** as the universal set.

Note that the universal set can be chosen arbitrarily for a given problem. But once chosen, it is fixed for the discussion of that problem.

Theorem 1: If A is a set with n elements, then $|P(A)| = 2^n$.

Proof: We shall prove this by mathematical induction.
For this, we first check if it is true for n= 1.Then assuming that it is true for n = m, we prove it for the case n = m +1. It will, then, follow that the result will be true $\forall\, n \in \mathbf{N}$.

Step I: If $|A| = 1$, then $P(A) = 2 = 2^1$.

Step II: Assume that the theorem holds for all sets A of cardinality k, i.e. if $|A| = k$, then A has 2^k subsets.

Step III: Now consider any set $A = \{x_1, x_2, x_3, \ldots, x_k, x_{k+1}\}$, with k+1 elements. Consider its subset $B= \{x_1, x_2, x_3, \ldots, x_k\}$. Now B has 2^k subsets, each being a subset of A. Now, take any such subset $\{x_{i_1}, x_{i_2}, \ldots, x_{i_r}\}$ of B. Then $\{x_{i_1}, x_{i_2}, \ldots, x_{i_r}, x_{k+1}\}$ is a subset of A that is not a subset of B. So, for each of the 2^k subsets of B, we attach x_{k+1} to it to get 2^k more subsets of A.

You can see that this covers all the subsets of A.

So the number of subsets of A=$2^k + 2^k = 2.2^k = 2^{k+1}$.
Hence the theorem.

Now try these exercises.

E4) Give two proper subsets and two supersets of the set of vowels of the English alphabet.

E5) Find the power set of the set A ={a,e,i,o,u}.

E6) For which set A, is P(A) = 1 ?

E7) If $A \subseteq B$, is $P(A) \subseteq P(B)$? Why?

E8) $P(A) = P(B) \Rightarrow A = B$. True or false? Why?

Let us conclude this section with the **pictorial** representation of sets. You know that the pictorial representation of any object helps in understanding the object. This is why a pictorial representation of sets, known as a **Venn diagram,** helps in understanding and dealing with sets.

The English priest and logician John Venn invented the Venn diagram. Through Venn diagrams we can easily visualize the abstract concept of a set and operations on sets. In this diagram, the universal set is usually represented by a rectangle and its subsets are shown as circles or other closed geometrical figures inside this rectangle.

For example, A = {Lucknow, Patna, Bhopal, Itanagar, Shillong} can be represented using a Venn diagram as in Fig. 2. Here U could be any superset of A.

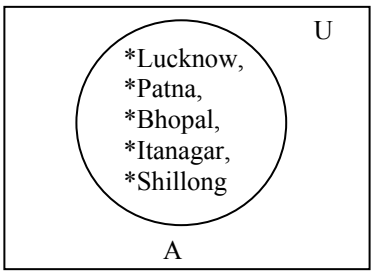


Fig. 2: A Venn diagram

Now that you are familiar with basic definitions related to sets, let us discuss some basic operations that can be performed on sets. This is when we shall appeal to Venn diagrams very often, as you will see.

1.3 OPERATIONS ON SETS

Let us now study sets obtained by applying operations on sets. We will cover four operations here, namely, union of sets, intersection of sets, complement of sets and symmetric difference. While studying them you will see how useful a Venn diagram can be for proving results related to these operations. In this section we will also look at some rules that are common to operations on sets and operations on statements, which you studied in Block 1.

1.3.1 Basic Operations

In this sub-section we shall define each of the operations one by one.

Definition: The **union** of two sets A and B is the set of all those elements which are either in A or in B or in both A and B. This set is denoted by $\mathbf{A \cup B}$, and read as 'A union B'.

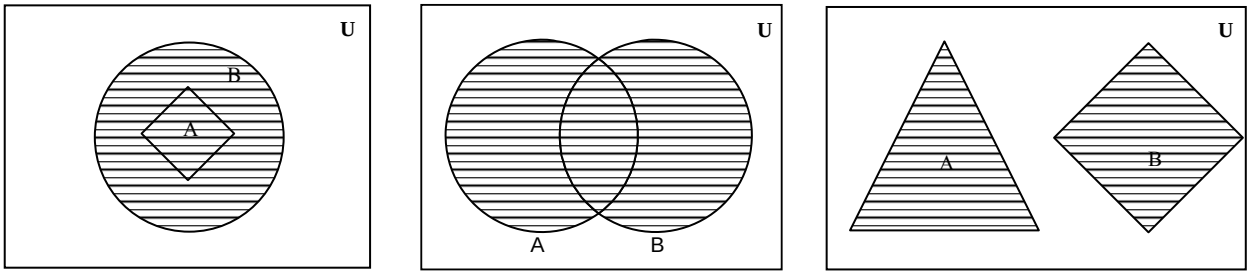
Symbolically, $A \cup B = \{x : x \in A \text{ or } x \in B\}$

For example, if A = {x: x is a stamp} and B = {4,5}, then

$A \cup B$= {x:x is a stamp or a natural number lying between 3 and 6}.

And A={Ram, Mohan, Ravi} and B={Ravi, Rita, Neetu},
then $A \cup B$={Ram, Mohan, Ravi, Rita, Neetu}.

If $A \subseteq B$, then $A \cup B = B$, and vice versa. This can be shown immediately using a Venn diagram, as in Fig.3.(a), where A is shown as the square contained in the circle representing B. In Fig.3(b), $A \cup B$ is shown when A and B have some elements in common, and in Fig.3(c), we depict $A \cup B$ when A and B have no element in common.



(a) (b) (c)

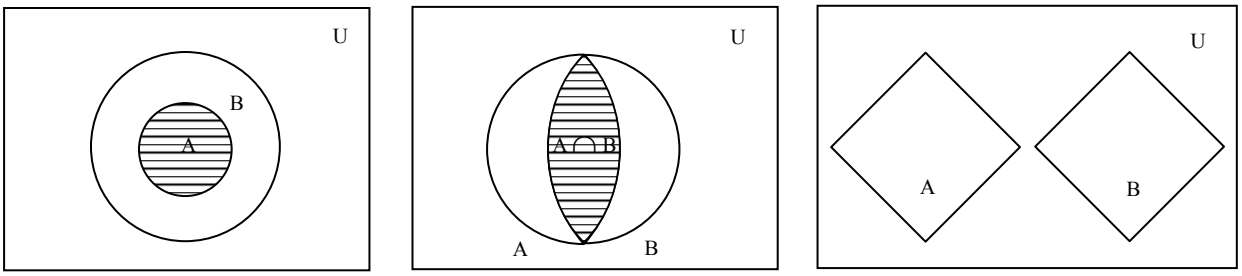
Fig. 3: Venn diagram for union

Definition: The **intersection** of sets A and B is the set of all the elements which are common to both A and B. This set is denoted by **A ∩ B**, and read as 'A intersection B'.

Symbolically, $A \cap B = \{x : x \in A \text{ and } x \in B\}$;
For example $A = \{1,2,3\}$ and $B = \{2,1,5,6\}$, then $A \cap B = \{1,2\}$.
Again if $A = \{1\}$ and $B = \{5\}$ then $A \cap B = \{\ \}$ or ϕ.

Remark: For any two sets A and B, $A \cap B \subseteq A \subseteq A \cup B$ and $A \cap B \subseteq B \subseteq A \cup B$.

What is $A \cap B$ if $A \subseteq B$? Do you agree that it is A? Let us use a Venn diagram to check this (see Fig.4(a)). If A and B have some elements in common, then the Venn diagram for $A \cap B$ looks like Fig 4.(b), and if A and B have no element in common, then the Venn diagram will be as in Fig.4(c).



(a) (b) (c)

Fig. 4: Venn diagram for intersection of sets

Definition: The **difference of two sets** A and B is the set of all those elements of A which are not elements of B. Sometimes, we call this set the **relative component** of B in A. It is denoted by **A~B** or **A\B**, and is read as 'A complement B'.

Symbolically, $A \sim B = \{x : x \in A \text{ and } x \notin B\}$ and
$B \sim A = \{x : x \in B \text{ and } x \notin A\}$

For example, if $A = \{4,5,6,7,8,9\}$ and $B = \{3,5,2,7\}$, then $A \sim B = \{4,6,8,9\}$ and $B \sim A = \{3,2\}$. From this example it is clear that $A \sim B \neq B \sim A$. In fact, this is usually the case. So, **the difference of sets is not a commutative operation**.

In Fig.5(a), $A \subseteq B$, so that $A \sim B = \phi$.

In Fig.5(b) we show $A \sim B$ when $A \supseteq B$, and in Fig.5(c) we show $A \sim B$ when neither $A \subseteq B$ nor $B \subseteq A$.

In Fig. 5(d), we show $A \sim B$ when A and B are disjoint.

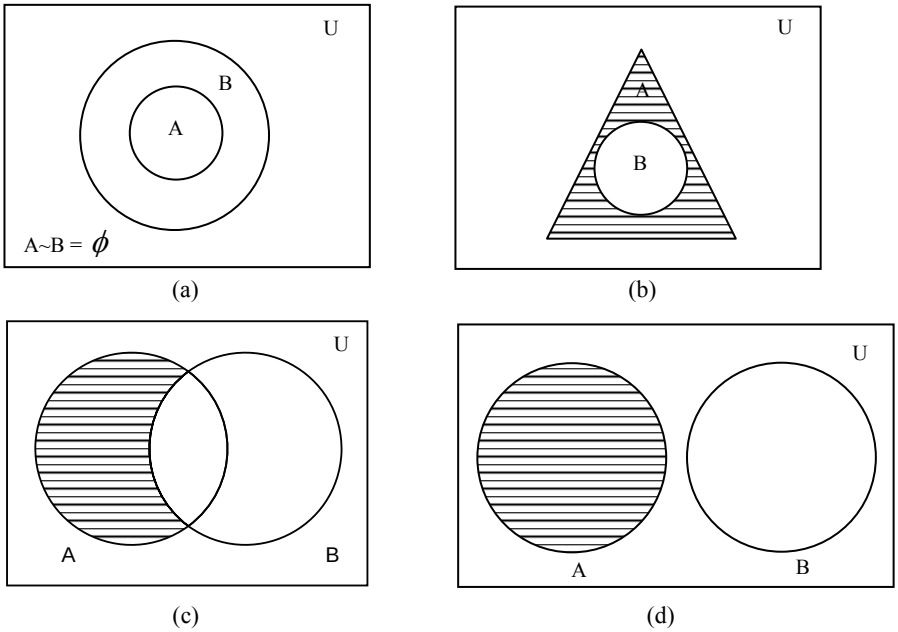


Fig. 5: A ~ B in different situation is the shaded portion.

There is one particular 'difference' that shows up very often, which we now define.

Definition: The **complement of a set** A, is the set U \ A, and is denoted by A′ or A^c. For example, U={Physics, Chemistry, Mathematics} and A={Mathematics}, then the complement of A is A′= {Physics, Chemistry}.

The Venn diagram showing the complement of Á is the set of those elements of the universal set U which are outside A (see Fig.6).

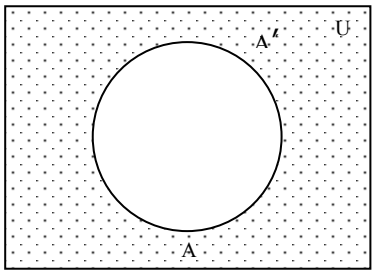


Fig. 6: Venn diagram for A′.

Definition: The **symmetric difference** of two sets A and B is the set of all those elements which are in A or in B, but not in both. It is denoted by A Δ B.

i.e., A Δ B =(A~B) ∪ (B~A).

Note that A Δ B = B Δ A, i.e. the symmetric difference is commutative.

For example A= {1,2,3,4,5} and B= {3,5,6,7}, then A~ B= {1,2,4},and B~A = {6,7}
∴ A Δ B={A~B) ∪ (B~A) = {1,2,4,6,7}

Now you may try these exercises.

E 9) Make a Venn diagram for A Δ B for each of the situations i) A $\subseteq$ B, ii) A $\not\subseteq$ B, iii) B $\not\subseteq$ A and A ∩ B ≠ ϕ ; iv) A ∩ B= ϕ .

E10) Let A= {Math, Physics, Science}, B={Computer,Math,Chemistry}, C={Math}. Find A ∪ (B ∩ C).

E11) If A = {1,2,3,4,5,6}, B={4,5,6,7,8,9},find i) A~ B, ii) B~ A, iii) A Δ B.

E12) For which sets A and B would A~B = B~A ?

E13) Write a program in C to perform E 10.

E14) Under what conditions can $A \cap B = A \cup B$?

While discussing these operations, you may be wondering that they seem to satisfy properties very similar to those of propositional logic covered in Block 1 of this course.You are right! Let us look at this aspects now.

1.3.2 Properties Common to Logic and Sets

Before looking into the properties we shall first present a very useful principle to you. This will allow you to see how one property can be proved in several situations simultaneously.

Duality Principle: The 'duality principle' is very convenient for dealing with theorems about sets. Basically if any theorem is given to you, by applying the duality principle you can get another theorem (the dual of the previous one). In any statement involving the union and intersection of sets, we can get from one of the statements to the other by interchanging $\cap$ with $\cup$ and ϕ with U.

For example, the dual of $A \cup (B \cap C)$ is $A \cap (B \cup C)$ and the dual of $U \cup \phi = U$ is $U \cap \phi = \phi$. So, for example what is true for $A \cup (B \cap C)$ will be true for $A \cap (B \cup C)$ too. This is why if the first property in each of the pairs below is proved the second one follows immediately.

For any universal set U and subsets A, B and C of U, **the following properties hold**.

i) Associative properties:
Union: $A \cup (B \cup C) = (A \cup B) \cup C$
Intersection: $A \cap (B \cap C) = (A \cap B) \cap C$

ii) Commutative properties:
Union: $A \cup B = B \cup A$
Intersection: $A \cap B = B \cap A$.

iii) Identity:
Union: $A \cup \phi = A$
Intersection: $A \cap U = A$.

iv) Complement:
Union: $A \cup A' = U$
Intersection: $A \cap A' = \phi$

Fig. 7: Augustus De Morgan (1806–1871)

v) Distributive properties:
Union: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Intersection: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan's Laws:

For any two sets A and B the following laws known as De Morgan's laws, hold

1. $(A \cup B)' = A' \cap B'$, and
2. $(A \cap B)' = A' \cup B'$

De Morgan's laws can also be expressed as

1. $A \sim (B \cup C) = (A \sim B) \cap (A \sim C)$
2. $A \sim (B \cap C) = (A \sim B) \cup (A \sim C)$

Each of the properties above corresponds to a related property for mathematical statements in logic (which we have covered in Unit 2 and Unit 3 of Block 1 of this course).

Now try these exercises.

E15) Find the dual of

i) $A \cap (B \cap C) = (A \cap B) \cap C$, and ii) $(A \cup B) \cap (A \cup C)$.

E16) Draw a Venn diagram to represent $A \cup (B \cap C)$.

E17) Check whether $(A \cup B) \cap C = A \cup (B \cap C)$ or not using a Venn diagram.

Let us now focus on subsets of a particular kind of product of sets.

1.4 RELATIONS

Sometimes we need to establish relations between two or more sets. For example, a software development company has a set of specialists in different technology domains, or a company gets some projects to develop. Here the company needs to establish a relation between professionals and the project in which they will participate. To solve this type of problem the following concepts are required.

1.4.1 Cartesian product

Very often we deal with several sets at a time, and we need to study their combined action. For instance, combinations of a set of teachers and a set of students. In such a situation we can take a product of these sets to handle them simultaneously. To understand this product let us first consider the following definitions.

iff is short for 'if and only if'.

Definition: An **ordered pair**, usually denoted by (x,y), is a pair of elements x and y of some sets. This is ordered in the sense that $(x,y) \neq (y,x)$ whenever $x \neq y$,that is , the order of placing of the element in the pair matters.

Any two ordered pairs (x,y) and (a,b) are equal iff x = a and y = b.

For example if, A= {a,b,c}and B= {x,y,z},then

$A \times B = \{a,b,c\} \times \{x,y,z\} = \{(a,x), (a,y),(a,z),(b,x),(b,y),(b,z),(c,x),(c,y), (c,z)\}$,and

$B \times A = \{x,y,z\} \times \{a,b,c\} = \{(x,a),(x,b),(x,c),(y,a),(y,b),(y,c),(z,a),(z,b),(z,c)\}$.

Now let us think about how $B \times A$ can be represented geometrically? For instance what is the geometric view of $\{2\} \times \mathbf{R}$? This is the line x =2 given in Fig.8(a).

Now, after seeing geometric representation of $\{2\} \times \mathbf{R}$, can you tell what $\{1,3\} \times \{2,3\}$ = {(1,2),(3,2),(1,3),(3,3) }looks like? You will get four points in the first quadrant, as shown in Fig.8(b).

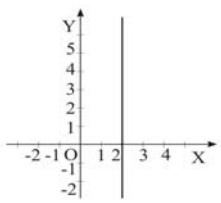


Fig. 8(a): {2} × R, i.e., x = 2.

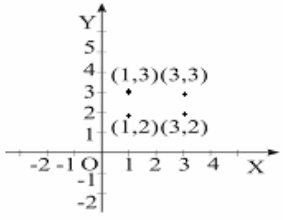


Fig.8(b): {1,3}×{2,3}

Now, you know that the multiplication of numbers is commutative. Is the Cartesian product of sets also commutative? For instance, is $\{1\}\times\{2\}=\{2\}\times\{1\}$? No, because $(1,2) \neq (2,1)$. So, $\mathbf{A\times B \neq B\times A}$ **usually**.

We can extend the definition of $A \times B$ to define the Cartesian product of n sets A_1, A_2, ….,A_n as follows.

$A_1 \times A_2 \times A_3 \times \ldots \times, A_n = \{(x_1,x_2,x_3,\ldots,x_n)\}: x_1 \in A_1, \wedge x_2 \in A_2 \wedge x_3 \in A_3 \wedge \ldots, \wedge x_n \in A_n\}$.

The element $(x_1,x_2,\ldots,x_n)$ is called an **n-tuple.** For instance, the 3–tuple $(1,1,3) \in \{1\} \times \{1,2\} \times \{2,3\}$.

Now you may try some exercises.

E18) If X= {a,b,c} and Y={1,2,3},find

i) $X \times X$, ii) $X \times Y$, and iii) $X \times \phi$.

E19) Under what conditions on A and B is $A\times B = B\times A$?

E20) Give the geometric representation of $\mathbf{R} \times \{2\}$.

With what you studied in this sub-section, you now have the background to discuss relations.

1.4.2 Relations and their Types

We often speak of relations which hold between two or more objects, e.g., discrete mathematics is one of the courses in the IGNOU MCA Ist semester, Nehru wrote Freedom of India, Chennai is the capital of Tamil Nadu. These are the relations in everyday situations. In these examples some sort of connections between pairs of objects are shown, and hence they express a relation between the pairs of objects.

Definition: A **relation between two sets A and B** is a subset of $A \times B$. Any subset of $A \times A$ is **a relation on the set A**.

For instance, if A ={1,2,3} and B = {p,q}, then the subset {(1,p),(2,q),(2,p)} is a relation on $A \times B$. And {(1,1), (2,3)} is a relation on A.

Also, $R= \{(x,y) \in \mathbf{N} \times \mathbf{N} : x > y\}$ is a relation on **N,** the set of natural numbers, since $R \subseteq \mathbf{N} \times \mathbf{N}$.

If $R \subseteq A \times B,$. we write $_x\mathbf{R}_y$ if and only if $(x,y) \in R$($_xR_y$ is read as 'x is related to y').

Theorem 2: The total number of distinct relations between a finite set A and a finite set B is 2^{mn}, where m and n are the number of elements in A and B, respectively.

For example, $R_1 = \mathbf{N} \times L$, where L is set of straight lines, in this relation we can give different ordering of the straight lines.
If the relation $R_2 = \{1,2,3\} \times \{l_1,l_2\}$, then line l_1 and l_2 can get three different ordering.

Proof: The number of elements of $A \times B$ is mn. Therefore, the number of elements of the power set of $A\times B$ is 2^{mn} (See Theorem 1). Thus, $A \times B$ has 2^{mn} different subsets. Now every subset of $A\times B$ is a relation from A to B, by definition. Hence the number of different relations from A to B is 2^{mn}.

As you have seen, any and every subset of $A \times A$ is a relation on A. However, some relations have special properties. Let us consider these types one by one.

1.4.3 Properties of Relations

Reflexive Relations: A relation R on a set A is called a **reflexive relation** if $(a,a) \in R \; \forall \; \mathbf{a} \in \mathbf{A}$.

In other words, R is reflexive if every element in A is related to itself.
Thus, R is **not reflexive** if there is at least one element $a \in A$ such that $(a,a) \notin R$.

For example, if A= {1,2,3,4}, then the relation R_1= {(1,1), (2,2), (3,3), (4,4)} in A is reflexive because for $x \in A, (x,x) \in R_1$. However, R_2= {(1,1), (2,1), (4,4)} is not reflexive since $2 \in A$, but $(2,2) \notin R_2$.

Symmetric Relations: A relation R on a set A is called a **symmetric relation** if $(a,b) \in R \Rightarrow (b,a) \in R$.Thus, R is symmetric if bRa holds whenever aRb holds.

A relation R in a set A is **not symmetric** if there exist two distinct elements $a, b \in A$, such that aRb, but not bRa.

For example, if L is the set of all straight lines in a plane, then the relation R in L, defined by 'x is parallel to y', is symmetric, since if a straight line a is parallel to a straight line b, then b is also parallel to a. Thus, $(a,b) \in R \Rightarrow (b,a) \in R$.

However, if R is the relation on **N** defined by 'xRy iff x–y>0', then R is not symmetric, since, $4-2>0$ but $2-4 \ngtr 0$.Thus, $(4,2) \in R$ but $(2,4) \notin R$.

Transitive Relations: A relation R on a set A is called a **transitive relation** if whenever $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$ for $a,b,c \in A$.
Thus, $[(a,b), \in R, (b,c) \in R \Rightarrow (a,c) \in R]$, $\forall$ $a,b,c \in A \Rightarrow$ R is transitive.

A relation R in a set A is **not transitive** if there exist elements $a,b,c \in A$, not necessarily distinct, such that $(a,b) \in R$, $(b,c) \in R$ but $(a,c) \notin R$.

For example, if L is the set of all straight lines in a plane and R is the relation on L defined by ' x is parallel to y' then if a is parallel to b and b is parallel to c, then a is parallel to c. Hence R is transitive. However, the relation 'xSy'on L defined by 'iff x intersects y' is not transitive.

Also, the relation R on A, the set of all Indians, defined by 'xRy iff x loves y', is not a transitive relation.

Equivalence Relations: A relation R on a set A is called an **equivalence relation** if and only if

(i) R is reflexive, i.e., for all $a \in R$, $(a, a) \in R$,

(ii) R is symmetric, i.e., $(a, b) \in R \Rightarrow (b, a) \in R$, for all $a, b \in A$, and

(iii) R is transitive, i.e., $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$, for all $a, b, c \in A$.

One of the most trivial examples of an equivalence relation is that of **'equality'.**
For any elements a,b,c in a set A,

(i) a = a, i.e., reflexivity

(ii) $a = b \Rightarrow b = a$, i.e., symmetricity

(iii) a = b and $b = c \Rightarrow a = c$, i.e., transitivity.

Now let us see if 'xRy iff ' 'x ≤ y' gives an equivalence relation on **R**.

(i) $x \leq x$, i.e., $(x,x) \in \mathbf{R}$, i.e., R is reflexive.

(ii) However, $2 \leq 3$ but $3 \not\leq 2$. So, R is not symmetric.

Thus, R is not an equivalence relation.

Now you may try these exercises.

E 21) Let A be the set of all people on Earth. A relation R is defined on the set A by 'aRb if and only if a loves b' for a,b ∈ A.

Examine if R is i) reflexive, ii) symmetric, iii) transitive.

Now we shall study a particular kind of relation, which is very useful in mathematics, as well as in computer science, as you will soon see.

1.5 FUNCTIONS

A function is a special kind of relation. If we take the example of the set A of students of IGNOU, and the set B of their enrolment numbers. Now consider R = {(a,b)∈ A×B | b is enrollment number of a },this is a relation between A and B. It is a 'special' relation, 'special' because to each a ∈ A ∃ ! b such that aRb. We call such a relation a function from A to B.

Let us define this term formally.

Definition: A **function from a non-empty set A to a non-empty set B** is a subset R of A×B such that for each a ∈ A ∃ a unique b ∈ B such that (a,b) ∈ R. So, this relation satisfies the following two conditions:

(i) for each a ∈ A, there is some b ∈ B such that (a,b) ∈ R

(ii) if (a,b) ∈ R and (a,b′) ∈ R then b = b′.

We usually present functions as a rule associating elements of one set with another. So, let us present the definition again, with this view.

Definition: Let A and B be non-empty sets. A **function** (or a **mapping**) f from A to B is a rule that assigns to each element x in A **exactly one** element y in B. We write this as f: A → B, read it as 'f is a function from A to B'.

Note that

(i) to each a ∈ A, f assigns an element of B; and

(ii) to each a ∈ A, f assigns only **one element** of B.

So, for example, suppose A ={1,2,3}, B= {1,4,9,11} and f assigns to each member in A its square values. Then f is a function from A to B. But if A={1,2,3,4}, B={1,4,9,10} and f is the same rule, then f is not a function from A to B since no member of B is assigned to the element 4 in A.

Note that the former example, 11 ∈ B, but there is no element in A which is assigned to 11. This does not matter. It is not necessary that every element of B be related to some element of A.

Functions are not restricted to sets of numbers only. For instance, let A be the set of mothers and B be the set of human beings. Then the rule that assigns to every mother her eldest child is a **function**. But the rule that assigns to each mother her children is **not** a **function** because it does not relate a unique element of B to each element of A.

Now, given a function, we have certain sets and terms that are associated with it. Let us give them some names.

Definitions: Let f be a function from A to B. The set A is called the **domain** of the function f and B is called the **co-domain** of f. The set $\{f(x)| x \in A\}$ is called the **range** of f, and is also denoted by f(A).

Given an element $x \in A$, the unique element of B to which the function f associates, it is denoted by f (x) and is called the **f-image** (or **image**) of x or the value of the function f for x. We also say that f **maps** x to f(x). The element x is referred to as the **pre-image** of f (x).

For example, if A = {1,2,3,4}, B = {1,8,27,64,125}, and the rule f assigns to each member in A its cube, then f is a function from A to B. The domain of f is A, its codomain is B and its range is {1,8,27,64}.

Can you tell what will be the domain and codomain for rule f : $f(x) = \frac{x}{1-x}$?

You can see that 1–x = 0, if x = 1, in this case f(x) will be undefined.
Domain of f can be taken as R~{1}and codomain can be **R**.

Remark: Each element of A has a **unique image,** and each element of B need not appear as the image of an element in A. Further, more than one element of A can have the same image in B.

Let us look at some examples of functions, and non-functions now.

i) If b is be a fixed element of B, then f: A→B : f(x)= b $\forall$ x $\in$ A is called a **constant function**.

Note that if b=0, then f is called the **zero map**, and is denoted by **0**.

ii) f : A→ A : f(x) = x $\forall$ x $\in$ A is called the **identity function** , and is denoted by **I**.

iii) Consider A= {1,2,3,4}, B= {1,4,5} and the rule f which associates 1→1, 2→ 4, 3→5, 4→5. Then f is a function from A to B.

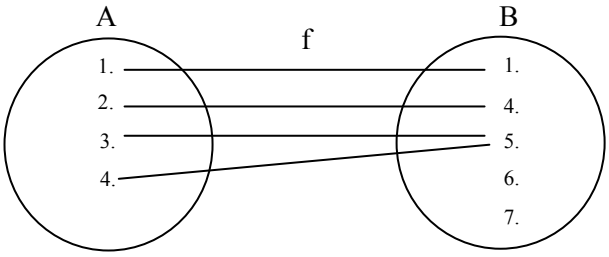


Fig.11: The rule f is a function

iv) The function f from **R** to **Z**, defined by the rule that f maps any real number x to the greatest integer less than or equal to x. is known as the **greatest integer** function or the **floor function**. We denote this function's action by f(x)=[x], where [x] is the greatest integer $\leq$x.

For example, if x = 0.6 then f(x) =[x]=0, if x= 2.3 then f(x)=[x]=2, and if x = –5, then [x]′= –5 .

v) Function f: **R→R**: f(x)=|x| is known as the modulus (or absolute value) function, where |x| is the absolute value of x.

For example, if x=10 then f(x)=|x|=10 and if x= –10, then f(x)=|x|=10.

vi) Now take, A={a,b,c} and B={1,2,3,4,5}. Consider the rule f which associates a→1, a→ 3, b→2, c→3. This is not a function from A to B because, elements 1 and 3 ∈ B are assigned to the same element a ∈ A.

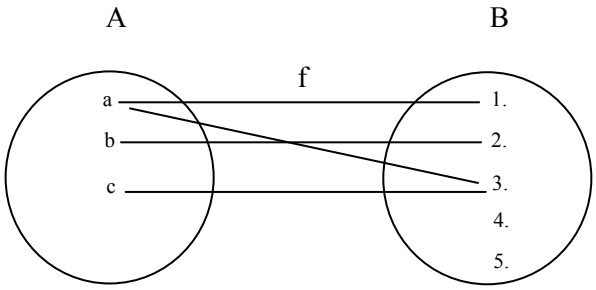


Fig.9: The rule f is not a function

vii) Consider A= {1,2,3}, B= {1,4,5,6,7} and the rule f which associates 1→1, 2→ 1, 2→4. Here f is not a function from A to B since no member of B is assigned to the element 3 ∈ A.

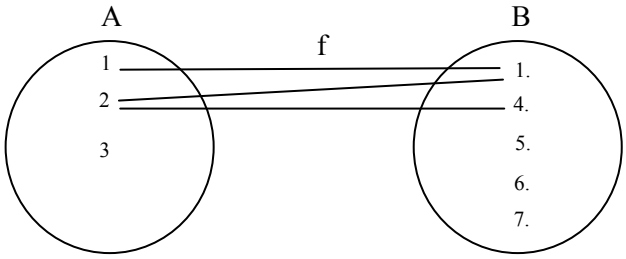


Fig.10: The rule is not a function

Now you may try these exercises.

E22) Let A= {a,b,c,d}, B= {1,2,3} and R= {(a,2), (b,1), (c,2), (d,1)}. Is R a function? Why.

E23) Every function is a relation. Is every relation a function? Why?

E24) Consider the following pseudocode.

1. read(n)
2. while n >1 do
3. begin
4. if n is even then n := n div 2
5. else n := 2n + 1;
6. end

Write a function of n that describes the operations performed.

E25) If A= {1,2,3,4}, B = {2,3,4,5,6,7} and the rule f assigned to each member in A is f(x)= x + 1, then find the domain and range of f.

Now let us discuss some types of functions.

1.5.1 Types of Functions

Here we shall look at different types of mappings.

'Surjective' comes from the French word 'sur', meaning 'on top of '.

Onto Mapping: A mapping f: A→ B is said to an **onto** (or **surjective**) **mapping** if f(A)= B, that is, the range and co-domain coincide. In this case we say that **f maps A onto B**.

For example, *f*: **Z**→ **Z** : f(x) = x+1, x∈**Z**, then every element y in the co-domain **Z** has a pre-image y–1 in the domain **Z**. Therefore, f(**Z**) = **Z** ,and f is an onto mapping.

Injective Mapping: A mapping *f*: A→ B is said to be **injective** (or **one-one**) if the images of distinct elements of A under f are distinct, i.e., if $x_1 \neq x_2$ in A, then $f(x_1) \neq f(x_2)$ in B. This is briefly denoted by saying f is **1–1**.

For example f: **R**→ **R** be defined by f(x) = 2x+1, x∈**R**, then for $x_1, x_2 \in \mathbf{R}$ ($x_1 \neq x_2$) we have $f(x_1) \neq f(x_2)$. So, f is **1–1**.

Bijective Mapping: A mapping f: A→ B is said to be **bijective** (or **one-one onto,**) if f is both injective and surjective, i.e., one-one as well as onto.

For example, f: **Z**→ **Z** : f(x) = x+2, x∈**Z** is both injective and surjective. So, f is bijective.
There is a particular kind of bijective function that we use very often. Let us define this.

Definition: A bijective mapping f : A→ A is said to be a **permutation** on the set A. Let A = $\{a_1, a_2, \ldots, a_n\}$, and f be a bijection from A onto A that maps a_i to $f(a_i)$, then we write f as

$f = \begin{pmatrix} a_1 & a_2 \ldots a_n \\ f(a_1) & f(a_2) \ldots f(a_n) \end{pmatrix}$. So, the identity mapping $I = \begin{pmatrix} a_1 & a_2 \ldots a_n \\ a_1 & a_2 \ldots a_n \end{pmatrix}$.

Now, associated with a bijective function, we get another function very naturally, which we now define.

Definition: Let f: A→ B be a bijective mapping. Then the mapping g : B→ A which associates to each element b ∈ B the unique element a ∈ A, such that f(a) = b, is called the inverse mapping of the mapping f: A→ B. We denote this function g by f^{-1}.

Note that a function f is invertible iff f^{-1} exists iff f is bijective.
Hence, if f: A→B is a one-one onto mapping, then f^{-1} : B→A exists, and is also 1-to-1.

Note the inverse of the permutation $f = \begin{pmatrix} a_1 & a_2 \ldots a_n \\ b_1 & b_2 \ldots b_n \end{pmatrix}$ is the permutation $\begin{pmatrix} b_1 & b_2 \ldots b_n \\ a_1 & a_2 \ldots a_n \end{pmatrix}$.

For example, A= **R**~{3} and B= **R**~(1}, and the function f: A→ B is defined by $f(x) = \frac{x-2}{x-3}$.

We can see that f is a one–to–one function.
∴ f inverse exists.

To get $f^{-1}(x)$ the following steps are required;

1. Replace f(x) by y in the equation describing the function. You will get

   $y = \frac{x-2}{x-3}$.

2. Interchange x and y. In other words, replace every x by y, and vice versa. You will get $x = \frac{y-2}{y-3}$.

3. Solve for y.

4. Replace y by $f^{-1}(x)$.

By applying these steps we get $f^{-1}(x) = \frac{3x-2}{x-1}$.

Now try these exercises.

E26) Explain why $f : \mathbf{Z} \rightarrow \mathbf{Z}$: $f(x) = x^2$ is onto? Domain and range of f is **Z**.

E27) Which of the following kind of function would you use to provide photo identity numbers? Why?

i) Constant function, ii) one-to-one function, and iii) identity function.

E28) Find f inverse of rule $f : f(x) = x^3 - 3$.

Now we can see how different operations like addition, subtraction, multiplication and division can be applied on functions.

1.5.2 Operations on Functions

If given whose domains ranges are subsets of the **real numbers**, we define the function f+g by (f + g)(x) to be the function whose value at x is the sum of f(x) and g(x). Symbolically,

(f + g)(x) = f(x) + g(x). This is called pointwise addition of f and g.

The domain of **f+g** is the **intersection** of the domains of f and g since to compute (f + g)(x) it is necessary and sufficient to compute both f(x) and g(x).

Other operations on functions are defined similarly:

- (fg)(x) = f(x)g(x) (pointwise multiplication)
- $f^p(x) = (f(x))^p$ for any real exponent p with the domain of f^p consisting of those points for which the p-th power of f(x) makes sense.
- (f/g)(x) = f(x)/g(x), for $g(x) \neq 0$ (pointwise multiplication)

For example, if f(x) = 3 sin (x) and $g(x) = x^2$, then

$(f+g)(x) = 3\sin(x) + x^2$
$(fg)(x) = 3\sin(x)*x2$
$(f-g)(x) = 3\sin(x) - x^2$
$(f/g)(x) = 3\sin(x) / x^2$

The domains of both f and g are all **real numbers**, but the domain of f/g is $\{ x \mid x \neq 0\}$.

Now let us consider two functions f and g from A= {1,2} to, B= {1,2,3,4}, where f={(1,1),(2,4)}. Let g be defined by the rule $g(x)= x^2$ where the domain of g is the set {1,2}. Here both have the same domain. Since f and g assign the same image to each element in the domain, they have the same effect throughout. This is why we treat them as the same, or equal.

Definition: If f and g are two functions defined on the same domain A and if **f(a)= g(a)** for every $a \in A$, then the functions **f** and **g** are **equal**, i.e., f = g.

For example $f(x) = x^2+5$, where x is a real number, and $g(x) = x^2+5$, where x is a complex number. Then the function f is not equal to the function g since they have different domains although $f(x)= x^2+5= g(x \forall x \in \mathbf{R})$. By this example we can conclude that even if f(a)= g(a), f and g may not be the same.

So far, the operations you have seen are the same as those for member systems. However, there is yet another operation on functions which we now define.

Definition: Let f and g be the operation of combining two functions by applying them one after the other. That is, the composition of f(x) and g(x), denoted by, fog .

For example, consider f : $\mathbf{R} \to \mathbf{R}$: $f(x) = (x^3 + 2x)^3$. We can write it as the composition of g and h, where the value of f(x) can be obtained by first calculating $x^3 + 2x$ and then taking its third power . We can write g for first or inside function $g(x) = x^3 + 2x$. We write h for the second function : $h(x) = x^3$. The use of the variable x is irrelevant, we could as well write $h(y) = y^3$ for $y \in \mathbf{R}$. We can see that $goh(x) = g(x^3 + 2x) = (x^3 + 2x)^3 = f(x)$.

In general $(f \circ g) \neq (g \circ f)$.

For example, if, $f(x) = x^2$ and $g(x) = x+1$, then $(f \circ g)(x) = (x + 1)^2$ and $(g \circ f)(x) = x^2+1$.
Here we can see that $f \circ g \neq g \circ f$.

Let us see another example, where $f(x) = x^2$, $g(x) = x +1$, $h(x) = x^3$
Then, $f \circ (g \circ h)(x) = (x^3 +1)^2$ and $(f \circ g) \circ h(x) = (x^3+1)^2$. Here we can see $f \circ (g \circ h) = (f \circ g) \circ h$.

Now let us see how you can get **product** of two permutations f and g of the same set,

Let $f=\begin{pmatrix} a_1 & a_2 \dots & a_n \\ f(a_1) & f(a_2) \dots f(a_n) \end{pmatrix}$ and

$g=\begin{pmatrix} a_1 & a_2 \dots a_n \\ g(a_1) & g(a_2) \dots g(a_n) \end{pmatrix}$. Then $fg=\begin{pmatrix} a_1 & a_2 \dots & a_n \\ f[g(a_1)] & f[g(a_2)] \dots & f[g(a_n)] \end{pmatrix}$ is itself a permutation.

For example if, $f=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ then

$fg=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $gf=\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Note that $f \circ g \neq g \circ f$. Thus the **multiplication of permutations is not commutative** in general.

However, the multiplication of permutations is associative. For example, if $f=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, $g=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $h=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ be the permutations on A = {1,2,3,4}, then

$fg=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, $gf=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$, $gh=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$,

$f(gh)=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $(fg)h=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

Here we can see the multiplication of permutation is commutative.

Now try these exercises.

E 29) Let $f(x) = 1/x$ and $g(x) = x^3 + 2$. Find the following functions, where $x \in \mathbf{R}$.

i) (f + g)(x)

ii) (f - g)(x)

iii) (fg)(x)

iv) (f/g)(x)

E30) Let f(x) = $\sqrt{x+1}$ $\forall x \geq -1$ and g(x) = x^3 $\forall x \in \mathbf{R}$. Define the following functions. Also give their domains.

i) (f + g)

ii) (f – g)

iii) (fg)

iv) (f/g)

v) ($f \circ g$)

With this we have come to the end of this unit. Let us now summaries what we have covered in this unit.

1.6 SUMMARY

In this unit we have covered the following points:

1. We introduced basic concepts related to sets and different ways of representing them.
2. We worked at different operations on sets and there Venn diagram representations.
3. We explored some properties common to operations on sets and logical statements.
4. In the process we also documented the duality principle.
5. We defined relations as a Cartesian product of sets and looked at several examples and type of relations.
6. We defined a function as a particular kind of relation. Then we studied different types of functions as well as basic operations on functions. In the process we considered permutations and their product.

1.7 SOLUTIONS / ANSWERS

E1) A={x:x is a student of IGNOU.}

E2) i) The collection of all good teachers is **not** a set because this collection is not well-defined. The characteristic 'good' cannot be measured objectively.

ii) The set of points on a line is **not** finite because infinitely many points make a straight line.

E3) {…, –3, –2, –1,0,1,2,3,…}.

E4) Set of vowels of English alphabet V={a,e,i,o,u}. Two subsets of set V are V1={a,e}, and V2={i,o}. Two supersets of V are V3={a,b,c,…,z}, and V4={a,c,d,e,i,o,u,…,z}.

E5) Powerset of A={a,e,i,o,u} is

$\{\phi,\{a\},\{e\},\{i\},\{o\},\{u\},\{a,e\},\{a,i\},\{a,o\},\{a,u\},\{e,i\},\{e,o\},\{e,u\},\{i,o\},\{i,u\},$
$\{o,u\},\{a,e,i\},\{a,i,o\},\{a,o,u\},\{e,i,o\},\{i,o,u\},\{i,o,u\},\{a,e,i,o\},\{e,i,o,u\},\{a,e,i,o,u\}.$

E6) For empty set A={ } or ϕ, P(A)=1

E7) If $A \subseteq B$, then $P(A) \subseteq P(B)$ because every subset of A is a subset of B.

E8) If P(A) =P(B) then $A \in P(A) = P(B) = A \subseteq B$. Similarly, $B \subseteq A$. Therefore A = B.

E9)

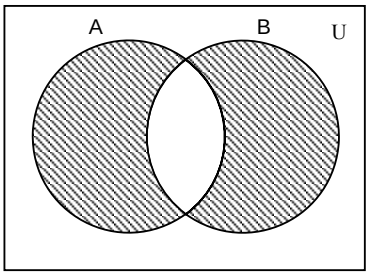


Fig.12: The Shaded portion is $A \Delta B$

You can try them for the other situations. We are showing in Fig. 12 for the second situation.

E10) $A \cup (B \cap C)$ = {Math, Physics, Science}= A.

E11) i) $A \sim B = \{1,2,3\}$

ii) $B \sim A = \{7,8,9\}$

iii) $A \Delta B = \{1,2,3,7,8,9\}$

E12) Only if A and B are ϕ.

E13) Write separate functions to find A~B, B~A and $A \Delta B$ with passing sets A and B as argument, return the resultant set.

E14) $A \cap B$ can be equal to $A \cup B$ if either $A \subseteq B$ or $B \subseteq A$.

E15) i) Dual of $A \cap (B \cap C) = (A \cap B) \cap C$ is $A \cup (B \cup C) = (A \cup B) \cup C$.

ii) Dual of $(A \cup B) \cap (A \cup C)$ is $(A \cap B) \cup (A \cap C)$.

E16)

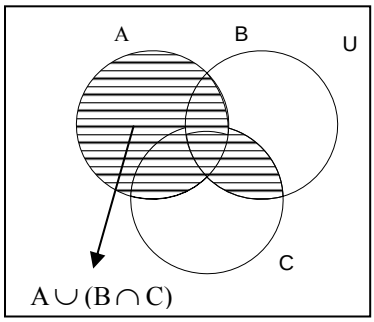


Fig.13: The lined portion represents $A \cup (B \cap C)$

E17)

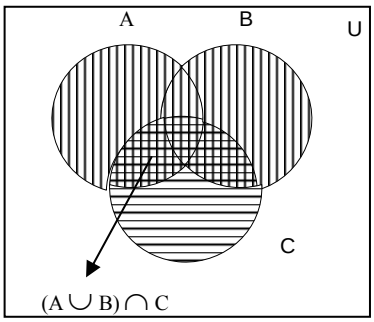


Fig.14(a)

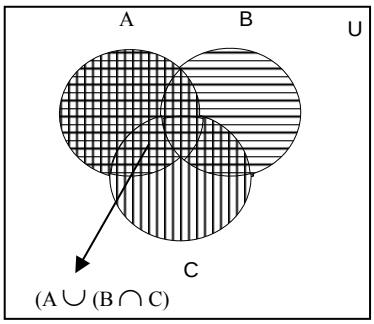


Fig.14(b)

Shaded area in Fig.14 (a) and Fig.14(b) are not same so $(A \cup B) \cap C$ is not equal to $(A \cup (B \cap C)$.

E18) i) $X \times X = \{(a,a),(a,b),(a,c),(b,b),(b,c),(c,c)\}$.

ii) $X \times Y = \{(a,1), (b,1), (c,1), (a,2), (b,2), (c,2), (a,3), (b,3), (c,3)\}$.

iii) $X \times \phi = \phi$.

E19) $A \times B = B \times A$ iff $A = B$.

E20) The geometric diagram for $R \times \{2\}$ will be the line parallel to Y axis.

See Fig.15.

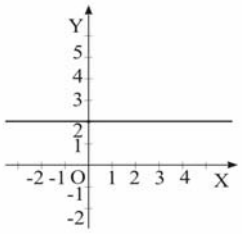


Fig.15: y=2

E21) i) For $a \in A$, aRa is reflexive because every one loves herself or himself.

ii) R is not symmetric because if a loves b then b need not love a, 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 need not love c; i.e., if aRb and bRc, aRc need not be. Thus, R is not transitive.

Hence, R is reflexive but is neither symmetric nor transitive.

E22) R is a function because each element of A is assigned to a unique element of B.

E23) Not every relation is a function. For example, this relation does not satisfy the property that,

a) Each element of A must have assigned one element in B.

b) If $a \in A$ is assigned $b \in B$ and $a \in A$ is assigned $b' \in B$ then $b = b'$.

That is why relations those who don't satisfy above properties are not a function

E24) We can see that the code has no effect on the value of $n \leq 0$.In the While loop, the value of n is halved whenever it is even. If n becomes odd before reaching 1, the second part of the while loop is invoked, and n remains odd and increases forever.

This shows that f : N→N is the function defined by $f(n) = \begin{cases} 0 \text{ if } n = 0. \\ 1, \text{if } n \text{ is a power of } 2, \\ \text{undefined otherwise} \end{cases}$

E25) The domain of f is {1,2,3,4} and range of f is {2,3,4,5}.

E26) Function $f(x) = x^2$ is one-to-one because for every value of x, x^2 will be a number that is different for different x. Hence, $f(x) = x^2$ is one-one mapping.

E27) One-to-one function will be used for providing identity card number, because each person must have unique identity numbers.

E28) Step 1: $y = x^3 - 3$

Step 2: $x = y^3 - 3$

Step 3: $y = \sqrt[3]{x+3}$

Step 4: $f^{-1}(x) = \sqrt[3]{x+3}$.

E29) i) $(f+g)(x) = \frac{1}{x} + x^3 + 2$

ii) $(f-g)(x) = \frac{1}{x} - (x^3 + 2)$

iii) $(f.g)(x) = \left(\frac{1}{x}\right)(x^3 + 2)$

iv) $(f/g)(x) = \frac{1}{x(x^3+2)}$ $\forall x \in R$.

E30) i) $(f+g)(x) = \sqrt{x+1} + x^3 \quad \forall x \geq -1$

ii) $(f-g)(x) = \sqrt{x+1} - x^3 \quad \forall x \geq -1$

iii) $(f.g)(x) = \sqrt{x+1}\ x^3 \quad \forall x \geq -1$

iv) $(f/g)(x) = \sqrt{x+1}\ / x^3 \quad \forall x \geq -1, x \neq 0$

v) $(f \circ g)(x) = f(x^3) = \sqrt{x^3+1} \quad \forall x \geq -1$.

UNIT 2 COMBINATORICS — AN INTRODUCTION

Structure **Page No.**

2.0 INTRODUCTION

Let us start with thinking about how to assess the efficiency of a computer programme. For this we would need to estimate the number of times each procedure is called during the execution of the programme. How would we do this? The theory of combinatorics helps us in this matter, as you will see while studying this unit.

Combinatorics deals with counting the number of ways in which objects can be arranged according to some pattern (listing). Mostly, it deals with a finite number of objects and a finite number of ways of arranging them. Sometimes an infinite number of objects and infinite number of ways in which they can be arranged are also considered. However, in this unit and block, we shall restrict our discussion to a finite number of objects.

We start our discussion in Sec. 2.2, with two counting principles. These principles help us in counting the number of ways in which a task can be done when it consists of several subtasks, and there are many possible ways of doing the subtasks.

In Sec. 2.3 we look at arrangements of objects in which the order matters. Such arrangements are called permutations. Here we look at various linear and circular permutations, and how to count their number in a given situation.

In Sec. 2.4, we consider arrangements of objects in which the order does not matter. Such arrangements are called combinations. We will consider situations that require us to count combinations. You will see that most of these situations require us to apply the multiplication principle also.

In the next section, Sec. 2.5, we consider binomial and multinomial coefficients. We see how they are related to the objects studied in Sec. 2.4.

Finally, in Sec. 2.6, we consider the applications of what we have presented in the rest of the unit, for finding the probability of the occurrence of an event. As you will see, this application is natural, since we use similar counting arguments for obtaining discrete probabilities. This discussion will be useful for you, for instance, in coding theory as well as in designing **reliable** computer systems.

We continue our study of combinatorics in the next unit. We also have a section of miscellaneous exercises at the end of the block of which several are based on this unit. Doing these exercises, and every exercise given in the unit, will help you achieve the following objectives of this unit.

2.1 OBJECTIVES

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

- explain the multiplication and addition principles, and apply them;
- differentiate between situations involving permutations and those involving combinations;
- perform calculations involving permutations and combinations;
- prove and use formulae involving binomial and multinomial coefficients;
- apply the concepts presented so far for calculating combinatorial probabilities.

2.2 MULTIPLICATION AND ADDITION PRINCIPLES

Let us start with considering the following situation: Suppose a shop sells six styles of pants. Each style is available in 8 lengths, six waist sizes, and four colours. How many different kinds of pants does the shop need to stock?

There are 6 possible types of pants; then for each type, there are 8 possible length sizes; for each of these, there are 6 possible waist sizes; and each of these is available in 4 different colours. So, if you sit down to count all the possibilities, you will find a huge number, and may even miss some out! However, if you apply the multiplication principle, you will have the answer in a jiffy!

So, what is the multiplication principle? There are various ways of explaining this principle. One way is the following:

Suppose that a task/procedure consists of a sequence of subtasks or steps, say, Subtask 1, Subtask 2,…, Subtask k. Furthermore, suppose that Subtask 1 can be performed in n_1, ways, Subtask 2 can be performed in n_2 ways after Subtask 1 has been performed, Subtask 3 can be performed in n_3 ways after Subtask 1 and Subtask 2 have been performed, and so on. Then **the multiplication principle** says that the number of ways in which the whole task can be performed is $n_1.n_2….n_k$.

Let us consider this principle in the context of boxes and objects filling them. Suppose there are m boxes. Suppose the first box can be filled up in k(1) ways. For every way of filling the first box, suppose there are k(2) ways of filling the second box. Then the two boxes can be filled up in k(1).k(2) ways. In general, if for every way of filling the first (r – 1) boxes, the rth box can be filled up in k(r) ways, for r = 2,3,…, m, then the total number of ways of filling all the boxes is k(1).k(2)… k(m).

So let us see how the multiplication principle can be applied to the situation above (the shop selling pants). Here k(1) = 6, k(2) = 8, k(3) = 6 and k(4) = 4. So, the different kinds of pants are $6 \times 8 \times 6 \times 4 = 1152$ in number.

Let’s consider one more example.

Example 1: Suppose we want to choose two persons from a party consisting of 35 members as president and vice-president. In how many ways can this be done?

Solution: Here, Subtask 1 is ‘choosing a president’. This can be done in 35 ways. Subtask 2 is ‘choosing a vice-president’. For each choice of president, we can choose the vice-president in 34 ways. Therefore, the total number of ways in which Subtasks 1 and 2 can be done is $35 \times 34 = 1190$.

* * *

There is another fundamental principle called the **addition principle**. This is applied in situations like the following one:

Suppose that a task consists of performing exactly one subtask from among a collection of disjoint (mutually exclusive) subtasks, say, Subtask 1, Subtask 2,…., Subtask k. (i.e., the task is performed if **either** Subtask 1 is performed, **or** Subtask 2,…, or Subtask k is performed.) Further, suppose that Subtask i can be performed in n_i ways, i = 1,2,…, k. Then, the number of ways in which the task can be performed is the sum $n_1+n_2+\ldots+n_k$.

Let us consider an example of its application.

Example 2: There are three political parties, P_1, P_2 and P_3. The party P_1 has 4 members, P_2 has 5 members and P_3 has 6 members in an assembly. Suppose we want to select two persons, both from the same party, to become president and vice-president. In how many ways can this be done?

Solution: From P_1, we can do the task in $4 \times 3 = 12$ ways, using the multiplication principle. From P_2, it can be done in $5 \times 4 = 20$ ways. From P_3 it can be done in $6 \times 5 = 30$ ways. So, by the addition principle, the number of ways of doing the task is $12 + 20 + 30 = 62$.

* * *

Though both these principles seem simple, quite a number of combinatorial enumerations can be done with them. For instance, what we see from Example 2 is that the addition principle helps us to count all possible arrangements grouped into mutually exclusive and exhaustive classes.

Why don't you try a few exercises that involve the use of these principles now?

E1) Give a situation related to computing in which the addition principle is used, and one in which the multiplication principle is used.

E2) Find the number of words of length 4, meaningful or not, made with the letters a,b,…, j.

E3) If n couples are at a dance, in how many ways can the men and women be paired for a single dance?

E4) How many integers between 100 and 999 consist of distinct even digits?

E5) Consider all the numbers between 100 and 999 that have distinct digits. How many of them are odd?

Let us now consider certain arrangements of objects, in which the order in which they are arranged matters.

2.3 PERMUTATIONS

Suppose we have 15 books that we want to arrange on a shelf. How many ways are there of doing it? Using the multiplication principle, you would say —-

$15 \times 14 \times 13 \times \ldots\ldots 2 \times 1 = 15!$

n! denotes '**n factorial**', which means $n \times (n-1) \times . \times 2 \times 1$ for any $n \in \mathbf{N}$.)

Each of these arrangements of the books is a permutation of the books. Let us define this term formally.

Definition: An arrangement of a set of n objects **in a given order** is called a **permutation** of the objects (taken altogether at a time).

An **ordered** arrangement of the n objects, taking r at a time, (where $r \leq n$) is called **a permutation of the n objects taking r at a time**. The total number of such permutations is denoted by **P(n,r)**.

As an example, let us consider picking out books, three at a time, from the shelf of 15 books. The first book can be chosen in 15 ways, the next in 14 ways, and the third in 13 ways. So the multiplication principle tells us that the total number of permutations of the 15 books taken 3 at a time is $P(15,3) = 15 \times 14 \times 13$.

Other notations used for P(n,r) are ${}^{n}P_{r}$, P_{r}^{n} , ${}_{n}P_{r}$.

Again, consider the permutations of a,b,c,d, taken 2 at a time. These are ab, ba, ac, ca, ad, da, bc, cb, bd, db, cd, dc. (Note that ab and ba are considered different even though they consist of the same two objects.) Or, we can argue combinatorically as above: The first letter can be chosen in 4 ways, and then the next letter can be chosen. We can list out all the cases in 3 ways. So, the total number of permutations are $P(4,2) = 4 \times 3 = 12$.

Now, is there a formula for finding the value of P(n,r)? This is what the following theorem tells us.

Theorem 1: The number of permutations of n objects, taken r at a time, where $0 \leq r \leq n$, is given by $P(n,r) = \dfrac{n!}{(n-r)!}$

Consider r boxes arranged in a line. Choose one object out of n and place it in the first box. This can be done in n ways. Then from the remaining (n–1) objects choose one and place it in the second box. The first two boxes can be filled in n(n – 1) ways. We continue this operation till the rth box is filled. So, by the multiplication principle, the total number of ways of doing this is n(n – 1) (n – 2) …(n – r+1).

$$\begin{aligned} P(n,r) &= n(n-1)\ldots(n-r+1). \\ &= n(n-1)\ldots((n-r+1)((n-r)((n-r-1)\ldots3.2.1 \\ &= (n-r)\ldots((n-r-1)\ldots3.2.1 \\ &= n!/(n-r)! \end{aligned}$$

Proof: In particular, Theorem 1 tells us that the number of permutation of n objects, taken all at a time, is given by

We define 0! = 1

$P(n,n) = n!$

and $P(n, 0) = 1 \qquad \forall n \in \mathbf{N}$.

So, for example, by Theorem 1 we can find

$P(6,4) = 6.5.4.3 = 6!/(6-4)!$ And $P(6,0) = 1$.

Why don't you try some exercises now?

E6) If m and n are positive integers, show that $(m+n)! \geq m! + n!$.

E7) How many 3-digit numbers can be formed from the 6 digits 2,3,5,7,8,9 if repetitions are not allowed? How many of these numbers are less than 400? How many are even?

E8) How many ways are there to rank n candidates for the job of chief engineer? In how many rankings will Ms. Sheela be in the second place.

In defining the concept of permutation we assumed that the objects were distinguishable. What does this mean, and what happens if we remove this assumption? Let's see.

2.3.1 Permutation of Objects Not Necessarily Distinct

We have shown that there are P(n,r) ways to choose r objects from a set of n distinct objects and arrange them in linear order. Here we consider the same problem with the relaxed condition that some of the objects in the collection may not be distinguishable.

For example, we consider permutations of the letters of the word DISTINCT. Here there are 8 letters of which 2 are I, 2 are T, and three are 4 other different letters. To count the permutations in such a situation, we have the following result.

Theorem 2: Suppose there are n objects classified into k distinct types, with m_1 identical objects of the first type, m_2 identical objects of the second type,…, and m_k identical objects of the kth type, where $m_1+m_2+...+m_k = n$. Then the number of distinct arrangements of these n objects, denoted by $P(n; m_1, m_2,..m_k)$ is $\frac{n!}{m_1!m_2!...m_k!}$.

Proof: Let x be the number of such permutations. If the objects of Type i are considered distinct, then they can be arranged amongst themselves in $m_1!$ ways, where i = 1,2,…, k. Therefore, by the multiplication principle, the total number of permutations of these n distinct objects, taken all at a time, is $xm_1!m_2!…m_k!$.

But this is precisely n! when there are n distinct objects.

Hence, $xm_1!m_2!…m_k! = n!$, that is, $x = n!/m_1!m_2!…m_k!$

So for example, this result tells us that the number of distinct 8 letter words, not necessarily meaningful, that we can make from the letter of the word "DISTINCT" is $\frac{8!}{2!2!1!1!1!1!} = 14$.

Here are some related exercises.

E9) How many permutations are there of the letters, taken all at a time, of the words
(i) ASSESSES, (ii) PATTIVEERANPATTI?

E10) How many licence plates can be made if each should have 3 letters of the English alphabet with no letter repeated? What will be the answer if the letters can be repeated?

So far, we have considered permutations of objects as linear arrangements of objects; this means that we visualize arrangements of objects in a **line**. But there is a variant in which the objects are arranged along the circumference of a circle. Let us consider that now.

2.3.2 Circular Permutation

Consider an arrangement of 4 objects, a,b,c,d as in Fig. 1. We observe the objects in the clockwise direction. On the circumference there is no preferred origin, and hence the permutations abcd, bcda, cdab, dabc will look exactly alike. So, each linear

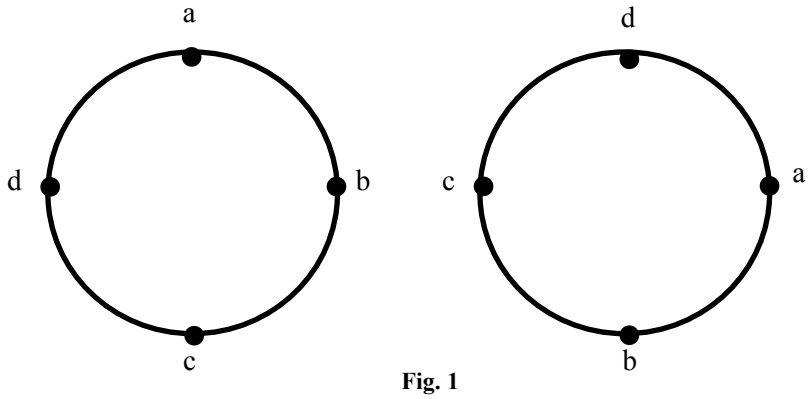


Fig. 1

permutation, when treated as a circular permutation, is repeated 4 times. Similarly, if n objects are placed in a circular arrangement, each linear arrangement is repeated n times. So, if we consider all the n! permutations of n things, each circular permutation will be indistinguishable from the (n–1) others obtained by the process of rotating the objects in the same order. So the number of distinct circular permutations will be n!/n = (n–1)!. Thus, we have shown that **the number of circular permutations of n things, taken all at a time, is (n–1)!.**

Let us consider some examples.

Example 3: In how many distinct ways is it possible to seat eight persons at a round table?

Solution: Clearly we need the number of circular permutations of 8 things. Hence the answer is 7! = 5040.

* * *

Example 4: In the preceding question, what would be the answer if a certain pair among the eight persons

(i) must not sit in adjacent seats?

(ii) must sit in adjacent seats

Solution: To answer (i), let us first solve (ii) from 7! we have to subtract the number of cases in which the pair of persons sit together. If we consider the pair as forming one unit, then we have the circular permutations of 7 objects, which is (7–1)! (Note that this is the answer for (ii).) But even as a unit they can be arranged in two ways. Hence the required answer is 2(6!). Now to answer (i), we must subtract these possibilities from the total number of ways of seating all the people. This is 7!–2(6!) = 3600.

* * *

Example 5: Suppose there are five married couples and they (10 people) are made to sit about a round table so that neither two men nor two women sit together. Find the number of such circular arrangements.

Solution: Five females can be made to sit about a round table in (5–1)! = 4! ways. One male can be seated in between two females. There are five positions, and hence they can be made to sit in 5! ways. By the multiplication principle, the total number of ways of such seating arrangements is 4! × 5! = 2880.

* * *

Example 6: Consider seven people seated about a round table. How many circular arrangements are possible if at least one of them will not have the same neighbours in any two arrangements?

Solution: The two distinct arrangements in Fig. 2 show that each has the same neighbours.

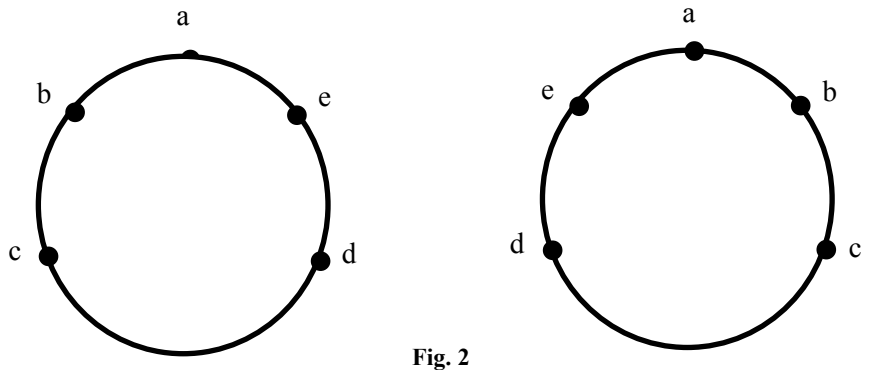


Fig. 2

Hence, the total number of circular arrangements = $(7-1)! \times \frac{1}{2} = 360$.

* * *

You may try the following exercise.

E11) If there are 7 men and 5 women, how many circular arrangements are possible in which women do not sit adjacent to each other?

Permutations apply to ordered arrangement of objects. What happens if order does not matter? Let's see.

2.4 COMBINATIONS

Let's begin by considering a situation where we want to choose a committee of 3 faculty members from a group of seven faculty members. In how many distinct ways can this be done? Here order doesn't matter, because choosing F_1, F_2, F_3 is the same as choosing F_2, F_1, F_3, and so on. (Here F_i denotes the ith faculty member.) So, for every choice of members, to avoid repetition, we have to divide by 3!. Thus, the number would be $\frac{7 \times 6 \times 5}{3!} = \frac{7!}{3!4!}$.

More generally, suppose there are n distinct objects and we want to select r objects, where $r \leq n$, where the order of **the objects in the selection does not matter**. This is called **a combination** of n things taken r at a time. The number of ways of doing this is represented by ${}_nC_r$, ${}^nC_r$, C_r^n, $\binom{n}{r}$ or C (n, r). We will use the notation C(n, r), in conformity with the notation P(n, r) for permutations. We read C(n, r) as 'n choose r' to emphasize the fact that only **choice** is involved but **not ordering**.

In the example that we started the section with, you saw that the number of combinations was 7!/3!4!, i.e., $\frac{P(7,3)}{3!}$. In fact, this relationship between C(n, r) and P(n, r) is true in general. We have the following result.

Theorem 3: The number of combinations of n objects, taken r at a time, where $0 \leq r \leq n$ is given by

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

Proof: C(n, r) counts the number of ways of choosing r out of n distinct objects without regard to the order. Any one of these choices is simply a subset of r objects of the set of n objects we have. Such a set can be ordered in r! ways. Thus, to each combination, there corresponds r! permutations. Hence there are r! times as many permutations as there are combinations. Hence, by the multiplication principle, we get

$P(n, r) = r!\, C(n,r)$

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

Using Theorem 3, we can very quickly find out, for instance, how many ways there are of choosing 2 rooms out of 20 rooms offered. This is $C(20,2) = \frac{20!}{18!2!} = 190$.

Now, to find C(20,2), I took a short cut. I cancelled 18! From the number and denominator. In practice, I only needed to calculate $\frac{20 \times 19}{2 \times 1}$. This practice is useful, in general, i.e., we use the identity $C(n, r) = \frac{n(n-1)...\text{r factors}}{r(r-1)...\text{r factors}}$ for calculations. In fact, sometimes r is much larger than n – r, in which case we cancel r!. This is also what the following result suggests.

Theorem 4: C(n, r) = C(n, n – r), for $0 \le r \le n$, $n \in \mathbf{N}$.

Proof 1: For every choice of r things from n things, there uniquely corresponds a choice of n – r things from those n objects, which are the unchosen objects. This one-to-one correspondence shows that these numbers must be the same. This proves the theorem.

Proof 2: $C(n, r) = \frac{n!}{(n-r)!r!} = \frac{n!}{(n-r)!(n-n-r)!} = C(n, n-r)$.

Because of these two theorems we have, for instance,

C(n, n) = C(n, 0) = P(n, 0) = 1. C(n, 1), and = C(n, n–1) = P(n, 1) = n.

The numbers C(n, r) are also called the binomial coefficients as they occur as the coefficients of x^r in the expansion of $(1+x)^n$ in ascending powers of x, as you will see in Sec. 1.5. At this stage, let us consider some examples involving C(n, r).

Example 7: Evaluate C(6, 2), C(7, 4) and C(9, 3).

Solution: $C(6, 2) = \frac{6.5}{2.1} = 15, C(7, 4) = \frac{7.6.5}{3.2.1} = 35, \text{and } C(9,3) = \frac{9.8.7}{3.2.1} = 84.$

Example 8: Find the number of distinct sets of 5 cards that can be dealt from a deck of 52 cards.

Solution: The order in which the cards are dealt is not important. So, the required number is $C(52, 5) = \frac{52!}{5!47!} = \frac{52 \times 51 \times 50 \times 49 \times 48}{5 \times 4 \times 3 \times 2 \times 1} = 2{,}598{,}960.$

Example 9: Suppose a valid computer password consists of 8 characters, the first of which is the digit 1, 3 or 5. The rest of the 7 characters are either English alphabets or a digit. How many different passwords are possible?

Solution: Firstly, the initial character can be chosen in C(3, 1) ways. Now, there are 26 alphabets and 10 digits to choose the rest of the characters from, and repetition is allowed. So, the total number of possibilities for these characters is $(26+10)^7$.

Therefore, by the multiplication principle, the number of passwords possible are $C(3, 1).36^7$.

Here are some exercises now.

E12) At a certain office, a committee consisting of one male and one female worker is to be constituted from among 12 men and 15 women workers. In how many distinct ways can this be done?

E13) In how many ways can a prize winner choose any 3 CDs from the 'Ten Best' list?

E14) How many different 7-person committees can be formed, each containing 3 women and 4 men, from a set of 20 women and 30 men?

So far we have been considering combinations of distinct objects. Let us now look at combinations in which repetitions are allowed. We start with considering the following situations.

Suppose five friends stop at a sweet shop where each of them has one of the following: a samosa, a dosa, and a vada. The order of consumption does not matter. How many different purchases are possible?

Let s, t, and d represent samosa, dosa, vada, respectively. In the following table we have listed some possible ways of purchasing these. For instance, the second row represents the possibility that all 5 friends order only dosas.

s	d	**v**
x	x	xxx
xxx	xxxx	xx

These orders can also be represented by x's and | 's. For instance, the first row can be written as x|x|xxx. So, any order will consist of five x's and two |'s.

Conversely, any sequence of five x's and two |'s represents an order. So, there is a 1-to-1 correspondence between the orders placed and sequences of five x's and two |'s. But the number of such sequences is just the number of distinct ways of placing 2 |'s in 7 possible places. This is C(7,2).

More generally, if we wish to select with repetition, r out of n distinct objects, we are considering all arrangements of r of one kind (say x's) and n – 1 of the other kind (say |'s) (because (n – 1) |'s are needed to separate n types).

The following result gives us the total number of such possibilities.

Theorem 5: Let n and r be natural numbers. Then the number of solutions in natural numbers, to the equation $x_1 + x_2 + \ldots + x_n = r$, is C(n + r – 1,r). Equivalently, the

number of ways to choose r objects from a collection of n objects, with repetition allowed, is C(n + r – 1,r).

Proof: Any string will consist of r objects and n – 1 bars, to denote the n different categories in which these objects can fall. So, it will be a string of length n + r – 1, containing exactly r stars and n – 1 bars. The total number of such strings is the number of ways we can position (n – 1) bars in r different places. This is C(n + r – 1,r).

Now we demonstrate how such strings correspond to solution of the equation $x_1 + \ldots + x_n = r$.

n – 1 bars in the string divide the string into n substrings of stars. The number of stars in these n substrings are the values of $x_1, x_2, \ldots, x_n$. Since there are r stars altogether, the sum is r. Therefore, is a one-to-one correspondence between the strings and the solutions, and the theorem is proved.

Let us consider examples of the use of this result.

Example 10: In how many ways can a prize winner choose three books from a list of 10 best sellers, if repeats are allowed?

Solution: Here, note that a person can choose all three books to be the same title. Applying Theorem 5, the solution is C(10 + 3 – 1, 3) = C(12, 3) = 220.

* * *

Example 11: Determine the number of integer solutions to the equation $x_1 + x_2 + x_3 + x_4 = 7$, where $x_i \geq 0$ for all i = 1,2,3,4.

Solution: The solution of the equation corresponds to a selection, with repetition, of size 7 from a collection of size 4. Hence, there are C(4 + 7 – 1, 7) = 120 solutions. (n = 4, r = 7 in Theorem 5.)

* * *

So, from this sub-section, we see the equivalence of the following:

(a) The number of integer solutions of the equation $x_1 + x_2 + \ldots + x_n = r$, $x_i \geq 0$, $1 \leq i \leq n$.

(b) The number of selections, with repetition, of size r from a collection of size n.

(c) The number of ways r identical objects can be distributed among n distinct containers.

Why don't you try some exercises now?

E15) A student in a college hostel is allowed four fruits per day. There are 6 different types of fruits from which she can choose what she wants. For how many days can a student make a different selection?

E16) An urn contains 15 balls, 8 of which are red and 7 are black. In how many ways can:

i) 5 balls be chosen so that all 5 are red?

ii) 7 balls be chosen so that at least 5 are red?

In this section we have considered choosing r objects, with repetition, out of n objects, regardless of order. What happens when order comes into the picture? Let's consider an example.

Example 12: A box contains 3 red, 3 blue and 4 white socks. In how many ways can 8 socks be pulled out of the box, one at a time, if order is important?

Solution: Let us first see what happens if order isn't important. In this case we count the number of solutions of r+b+w = 8, $0 \le r, b \le 3$, $0 \le w \le 4$. To apply Theorem 5, we write x = 3 – r, y = 3 – b, z = 4 – 10.

Then we have x+y+z = 10 – 8 = 2, and the number of solutions this has is C(3+2–1,2) = 6.

These 6 solutions are (1, 0, 1) (0, 1, 1), (1, 1, 0), (2, 0, 0), (0, 2, 0), (0, 0, 2). So, the corresponding solutions for (r, b, w) are

(3, 3, 2), (2, 3, 3), (3, 2, 3), (3, 1, 4), (2, 2, 4), (1, 3, 4).

Now, we consider order. From Theorem 2 we know that the number of ways of pulling out 3 red, 3 blue and 2 white socks in some order is $\frac{8!}{3!3!2!}$. This number would be the same if you had 2 red, 3 blue and 3 white socks, etc. By this reasoning and considering all different orderings, the number of possibilities is

$$3\left(\frac{8!}{3!3!2!}\right)+2\left(\frac{8!}{3!1!4!}\right)+\frac{8!}{2!2!4!}=3220.$$

* * *

What we see, via Example 13, is that if we want to find the number of possibilities wherein order matters and repetition is allowed them:

Step 1: Find the possibilities when order doesn't matter, using Theorem 5;

Step 2: Use Theorem 2, to find the possibilities for each solution obtained in Step 1.

Why don't you try and exercise now?

E17) How many 6-letter words, not necessarily meaningful can be formed from the letters of CARACAS?

Let us now consider why C(n,r) shows up as the coefficients in the binomial expansions.

2.5 BINOMIAL COEFFICIENTS

You must be familiar with expressions like a+b, p+q, x+y, all consisting of two terms. This is why they are called binomials. You also know that a **binomial expansion** refers to the expansion of a positive integral power of such a binomial. For instance, $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$ is a binomial expansion. Consider coefficients 1, 5, 10, 10, 5, 1 of this expansion. In particular, let us consider the coefficient 10, of a^3b^2 in this expansion. We can get this term by selecting a from 3 of the binomials and b from the remaining 2 binomials in the product (a+b) (a+b) (a+b) (a+b) (a+b). Now, a can be chosen in C(5, 3) ways, i.e., 10 ways. This is the way each coefficient arises in the expansion.

The same argument can be extended to get the coefficients of $a^r b^{n-r}$ in the expansion of $(a+b)^n$. From the n factors in $(a+b)^n$, we have to select r for a and the remaining (n – r) for b. This can be done in C(n, r) ways. Thus, the coefficient of $a^r b^{n-r}$ in the expansion of $(a+b)^n$ is C(n, r).

In view of the fact that C(n, r) = C(n, n – r), the coefficients of $a^r b^{n-r}$ and $a^{n-r} b^r$ will be the same. r can only take the values 0, 1, 2, …, n. We also see that C(n, 0) = C(n, n) = 1 are the coefficients of a^n and b^n. Hence we have established the binomial expansion.

$(a+b)^n = a^n + C(n, 1)\, a^{n-1}b + C(n, 2)a^{n-2}b^2 + \ldots + C(n, r)\, a^{n-r}b^r + \ldots + b^n$.

In analogy with 'binomial', which is a sum of two symbols, we have 'multinomial' which is a sum of two or more (though finite) distinct symbols. Multinomial expansion refers to the expansion of a positive integral power of a multinomial. Specifically we will consider the expansion of $(a_1 + a_2 + \ldots + a_m)^n$. For the expansion we can use the same technique as we use for the binomial expansion. We consider the nth power of the multinomial as the product of n factors, each of which is the same multinomial. Every term in the expansion can be obtained by picking one symbol from each factor and multiplying them. Clearly, any term will be of the form $a_1^{r_1} a_2^{r_2} \ldots a_m^{r_m}$ where $r_1, r_2, \ldots$, are non-negative integers such that $r_1 + r_2 + \ldots + r_m = n$. Such a term is obtained by selecting a_1 from r_1 factors, a_2 from r_2 factors **from among the remaining $(n - r_1)$ factors**, and so on. This can be done in

$C(n, r_1).\ C(n - r_1, r_2).C(n - r_1 - r_2, r_3) \ldots C(n - r_1 - r_2 - \ldots - r_{m-1}, r_m)$ ways.

If you simplify this expression, it will reduce to $\dfrac{n!}{r_1! r_2! \ldots r_m!}$.

So, we see that the **multinomial expansion** is

$$(a_1 + a_2 + \ldots + a_m)^n = \Sigma \frac{n!}{r_1! r_2! \ldots r_m!} a_1^{r_1} a_2^{r_2} \ldots a_m^{r_m}$$

where the summation is over all non-negative integers $r_1, r_2, \ldots, r_m$ adding to n.

The coefficient of $a_1^{r_1} a_2^{r_2} \ldots a_m^{r_m}$ in the expansion of $(a_1 + a_2 + \ldots + a_m)^n$ is $\dfrac{n!}{r_1! r_2! \ldots r_m!}$, and is called a **multinomial coefficient**, in analogy with the binomial coefficient. We represent this by $C(n; r_1, r_2, \ldots, r_m)$. This is also represented by many authors as $\left[\dfrac{n}{r_1, r_2, \ldots . r_m}\right]$.

For instance, the coefficient of $x^2y^2z^2t^2u^2$ in the expansion of $(x + y + z + t + u)^{10}$ is $C(10; 2, 2, 2, 2, 2) = 10!/(2!)^5$.

Let us see an example involving such coefficients.

Example 13: What is the sum of the coefficients of all the terms in the expansion of $(a+b+c)^7$?

Solution: The required answer is $\Sigma \dfrac{7!}{r!s!t!}$, where the summation is over all non-negative integers r, s, t adding to n. But it is also the value of $\Sigma \dfrac{7!}{r!s!t!} a^r b^s c^t$ for a = b = c = 1.

So the answer is $(1 + 1 + 1)^7 = 3^7$.

* * *

This short detour was just to give you an idea of the way in which the Cs and Ps can be extended. Let us now consider some identities involving the binomial coefficients. We first consider Pascal's formula.

Theorem 6 (Pascal's formula): For all positive integers n and all r such that $1 \le r \le n$, $C(n + 1, r) = C(n, r) + C(n, r - 1)$.

Proof 1: The left hand side of the identity represents the number of ways of choosing r things out of (n+1) distinct things. Suppose we select an object from the (n+1) things and mark it. Then the number of combinations in which the marked thing is absent is C(n, r), as we then choose r things out of the unmarked n things. The number of combinations in which the marked thing is present is C(n, r–1), as we have to choose (r – 1), things out of the unmarked things, and attach the marked thing to it to make r things. Pascal's formula now follows from the fact that the sum of the last two numbers mentioned must be equal to C(n+1, r).

Proof 2: $C(n, r) + C(n, r - 1) = \dfrac{n!}{(n-r)!r!} + \dfrac{n!}{(n-r+1)!(r-1)!}$

$$= \frac{n!}{r!(n+1-r)!}(n - r + 1 + r) = C(n + 1, r).$$

Pascal's formula gives us a recursive way to calculate the binomial coefficients, since it tells us the value of C(n, r) in terms of binomial coefficients with a smaller value of n. Note that we use the fact that $C(n, 0) = 1$ for all $n \ge 0$ to start the recursion, since Theorem 6 only applies for $1 \le r \le n$. This recursive approach allows us to form Pascal's triangle, the display of the binomial coefficients shown in Fig.4.

The nth row of Pascal's triangle gives the binomial coefficients C(n, r) as r goes from 0 (at the left) to n (at the right); the top row is Row D. This consists of just the number 1, for the case n = 0. The left and right borders are all 1's, reflecting the fact that C(n, 0) = C(n, n) = 1 for all n. Each entry in the interior of the Pascal's triangle is the sum of the two entries immediately above it to the left and right. We call this property the **Pascal property**. For example, each 15 in Row 6 (remember that we are starting the count of rows with 0) is the sum of the 10 and the 5 immediately above it.

```
                                    1
                                  1   1
                                1   2   1
                              1   3   3   1
                            1   4   6   4   1
                          1   5   10  10  5   1
                        1   6   15  20  15  6   1
                      1   7   21  35  35  21  7   1
                    1   8   28  56  70  56  28  8   1
                  1   9   36  84  126 126 84  36  9   1
                1   10  45  120 210 252 210 120 45  10  1
              1   11  55  165 330 462 462 330 165 55  11  1
```

Fig. 3: Pascal's triangle

The diagonals of Pascal's triangle are also interesting. The diagonal parallel to the left edge but moved one unit to the right reads (from the top down) 1, 2, 3, 4, 5,…, reflecting the fact that $C(n, 1) = n$ for $n \ge 1$. The next diagonal to the right, reading 1,

3, 6, 10, 15,…, reflects the fact that differences increase by 1 as we move down the diagonal.

Let us now consider some identities involving binomial coefficients.

Identity 1: $C(n, 0) + C(n, 1) + C(n, 2) + \ldots + C(n, n-1) + C(n, n) = 2^n$

By setting $a = b = 1$ in the binomial expansion of $(a+b)^n$, we get this identity. In the context of sets, it tells us the number of distinct subset that can be formed from a set with n elements. Note that the number of subsets containing precisely r elements is $C(n, r)$. Hence the total number of subsets is $\sum_{r=0}^{n} C(n,r) = 2^n$, by the identity. So, this identity tells us that **the number of distinct subsets of a set with n elements is 2^n.**

Identity 2: $C(n, 0) - C(n, 1) + C(n, 2) - \ldots + (-1)^n C(n, n) = 0$.

We get this by setting $a = 1$, $b = -1$ in the expansion of $(a+b)^n$.

Now, adding the two identities, we get

$$2 \sum_{r \text{ even}} C(n, r) = 2^n, \text{ i.e., } \sum_{r \text{ even}} C(n, r) = 2^{n-1}$$

Similarly subtracting the second identity from the first leads us to the equation

$$\sum_{r \text{ odd}} C(n, r) = 2^{n-1}.$$

These two equations tell us that the number of subsets of a set of n elements with an even number of elements is equal to the number of subsets with an odd number of elements, both being 2^{n-1}.

Why don't you try to prove some identities now?

E18) Show that $C(n, m)\, C(m, k) = C(n, k)\, C(n-k, m-k)$, $1 \le k \le m \le n$.

E19) Prove that $C(k, k) + C(k + 1, k) + C(k + 2, k) + \ldots + C(n, k) = C(n+1, k+1)$ for all natural numbers $k \le n$.

Before ending this section, we just mention another extension of the definition of binomial coefficients. So far, we have defined $C(n, r)$ for $n \ge r \ge 0$. We can extend this definition for any real number x, and any non-negative integer k, by

$$C(x, k) = \frac{x(x-1)\ldots(x-k+1)}{k!}.$$

This definition coincides with that of $C(n, k)$, when n is a non-negative integer.

So far, in this unit, we have considered various ways of counting different kinds of arrangements. These methods are, not surprisingly, helpful in finding the probability of an event. We shall now discuss this.

2.6 COMBINATORIAL PROBABILITY

Historically, counting problems have been closely associated with probability. The probability of getting at least 6 heads on 10 flips of a fair coin, the probability of finding a defective bulb in a sample of 25 bulbs if 5 percent of the bulbs from which the sample was drawn are defective — all these probabilities are essentially counting problems. In fact, Pascal's triangle (Fig. 4) was developed by Pascal around 1650 while analysing some gambling probabilities.

Let us start by recalling some basic facts about probability. An **experiment** is a clearly defined procedure that produces one of a given set of outcomes. The set of all outcomes is called **the sample space** of the experiment.

For example, the experiment could be checking the weather to see if it is raining or not on a particular day. The sample space here would be {raining, not raining}.

Given an experiment, we can often associate more than one sample space with it. For instance, suppose the experiment is the tossing of two coins.

i) If the observer wants to record the number of tails observed as the outcomes, the sample space is {0, 1, 2}.

ii) If the outcomes are the sequence of heads and tails observed, then the sample space is {HH, HT, TH, TT}.

A subset of the sample space of an experiment is called an **event**. For example, for an experiment consisting of tossing 2 coins, with sample space {HH, HT, TH, TT}, the event that two heads do **not** show up is the subset {HT, TH, TT}.

Suppose X is a sample space of an experiment with N out comes. Then, the events are all the 2^N subsets of X. The empty set ϕ is called the **impossible event**, and the set X itself is called the **sure event**.

Now, for the purpose of this course, we will assume that all the outcomes of an experiment are **equally likely**, that is, there is nothing to prefer one case over the other. For example, in the experiment of coin tossing, we assume that the coin is unbiased. This means that 'head' and 'tail' are equally likely in a toss. The toss itself is considered a random mechanism ensuring 'equally likely' outcomes. Of course, there are coins that are 'loaded', which means that one side of the coin may be heavier than the other. But such coins are excluded from our discussion. Also, in our discussions we shall always assume that our **sample space is finite**.

Given this background, we have the following definition.

Definition: Then the **probability of the event A**, represented by **P(A)**, is $\frac{n(A)}{n(X)}$.

We represent the number of elements of a finite set A, i.e., the **cardinality** of A, by n(A) or $|A|$.

For instance, the probability that a card selected from a desk of 52 cards is a spade is $\frac{13}{52}$, because A is the set of 13 spades in the deck.

From the definition, we get the following statements:

i) As $n(\phi) = 0$, it follows that $P(\phi) = 0$.

ii) By definition, $P(X) = \frac{n(X)}{n(X)} = 1$.

iii) If A and B are two events, then $n(A \cup B) = n(A) + n(B) - n(A \cap B)$. Therefore, $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

iv) (**Addition Theorem in Probability**) : If A and B are two mutually exclusive events, then the probability of their union is the sum of the probabilities of A and B. i.e., if $A \cap B = \phi$, then $\mathbf{P(A \cup B) = P(A) + P(B).}$

[This is a consequence of (i) and (iii) above.]

v) Suppose A is an event. Then the probability of A^c (also denoted by A′), the event complementary to A, or the event 'not A' is 1 – P(A), i.e.,

$\mathbf{P(A^c) = 1 - P(A)}$.

The reason is that the events A and A^c are mutually exclusive and exhaustive, i.e., $A \cup A^c = X$ and $P(A) + P(A^c) = 1$.

vi) (The generalised addition theorem) : If the events $A_1, A_2, \ldots, A_m$ are pairwise disjoint (i.e., mutually exclusive), then $\mathbf{P(\bigcup_i A_i) = \sum_i P(A_i).}$

Let us consider some examples from combinatorial probability.

Example 14: A die is rolled once. What are the probabilities of the following events?

(i) getting an even number,

(ii) getting at least 2,

(iii) getting at most 2,

(iv) getting at least 10.

Solution: If we call the events A, B, C and D, then we have X = {1, 2, 3, 4, 5, 6}, A = {2,4,6}, B = {2,3,4,5,6}, C = {1,2}, and D = ϕ.

Hence, P(A) = 3/6, P(B) = 5/6, P(C) = 2/6, P(D) = 0.

* * *

Example 15: A coin is tossed n times. What is the probability of getting exactly r heads?

Solution: If H and T represent head and tail, respectively, then X consists of sequences of length n that can be formed using only the letters H and T. Therefore, $n(X) = 2^n$. The event A consists of those sequences in which there are precisely r Hs. So, n(A) = C(n, r). Hence, the required probability is $C(n, r)/2^n$.

* * *

Example 16: Two dice, one red and one white, are rolled. What is the probability that the white die turns up a smaller number than the red die?

Solution: If the number on the red die is x and that on the white die is y, then X consists of the 36 pairs (x, y), where x and y can be any integer from {1, 2, 3, 4, 5, 6}.

For the event A, we need x < y. For x = 1, 2, 3, 4, 5, y can be x + 1, x+2,…, 6, i.e., 6 – x in number. Thus, by the addition principle,

$n(A) = \sum_{x=1}^{5} (6 - x) = 5 + 4 + 3 + 2 + 1 = 15.$

Hence, P(A) = 15/36 = 5/12.

* * *

Example 17: If a five-digit number is chosen at random, what is the probability that the product of the digits is 20?

Solution: If X is the collection of all 5-digit numbers, then $n(X) = 9.10^4 = 90000$. Now, 20 can be factored in only two ways, viz., 1.1.1.4.5 and 1.1.2.2.5, as the product of five factors. Of course, these factors can be permuted to give all possible cases for A. The numbers 5, 4, 1, 1, 1 can be permuted in 5!/1!1!3! = 20 ways, and the numbers 5, 2, 2, 1, 1 can be permuted in 5!/1!2!2! = 30 ways.

So, n(A) = 20 + 30 = 50.

Hence, P(A) = 50/90000 = 1/1800.

* * *

Example 18: Suppose A and B are mutually exclusive events such that P(A) = 0.3 and P(B) = 0.4. What is the probability that

i) A does not occur?

ii) A or B occurs?

iii) Either A or B does not occur?

Solution:

i) This is $P(A^c) = 0.7$.

ii) This is $P(A \cup B) = 0.7$.

iii) This is $P(A^c \cup B^c) = P[(A \cap B)^c] = P(\phi^c) = P(X) = 1$

* * *

Try some exercises now.

E20) A,B,C and D are four candidates for a chairperson's post. Suppose that A is twice as likely to be elected as B, B is thrice as likely as C, and C and D are equally likely to be elected. What is the probability of election of each candidate?

E21) In a ten-question true-false exam, a student must achieve six correct answers to pass. If she selects her answers randomly, what is the probability that she will pass?

There are several other methods for solving combinatorial problems. These will be taken up in the next two units. Let us now summarise what we have covered in this unit.

2.7 SUMMARY

In this unit we have discussed some counting techniques. Specifically, we have covered the following points.

1. The multiplication and addition principles for counting the number of ways in which a task can be completed.
2. What a permutation is, the derivation of the formula $P(n,r) = \frac{n!}{(n-r)!}$, and its application for solving problems.
3. The number of distinct arrangement of n objects of which m_1 are of Type 1, m_2 are of Type 2,…, m_k are of Type k, where $m_1, m_2 + \ldots, m_k = n$, is $P(n; m_1, m_2, \ldots, m_k) = \frac{n!}{m_1! m_2! \ldots m_k!}$.
4. What a circular permutation is, and that the number of such permutations of n objects, taken all at a time, is (n−1)!
5. What a combination is, the derivation of the formula

$C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{(n-r)!r!}$, and its application for solving problems.

6. The proof and applications of the fact that the number of ways of choosing r objects from a collection of n objects, with repetition allowed, is C(n+r–1,r).

7. Why C(n,r) is called a binomial coefficients, and its analogue for multinomials.

8. Some identities involving C(n,r), including Pascal's formula C(n+1,r) = C(n,r) + C(n,r–1).

9. The use of counting techniques for finding some discrete probabilities.

2.8 SOLUTIONS/ ANSWERS

E1) For instance, both principles are used to find the number of ways in which 17 files are stored if there are 3 storage locations of 1000 K each and 10 files are of 100 K, 5 of 200 K 2 of 500 K.

E2) Here we apply the multiplication principle. Each letter has 10 possibilities. Therefore, the total number of words is 10^4.

E3) Suppose we number the men as 1, 2, 3,…, n. Then the first man can be paired with any of the n women, the second can be paired with any from the remaining (n – 1) women, and so on. Hence, the number of ways of pairing is n(n – 1)… 1 = n!.

E4) By the multiplication principle, the number of integers between 100 and 999 with all digits even is 4.5.5 = 100 (Note that the first digit cannot be zero, but the second and third digits can be 0.)

E5) For a number to be odd the last digit should be odd. So, the last position can be filled up in 5 ways. If the middle position is filled up by 0, then the first position can be filled up in 8 ways. Thus the number of odd numbers with 0 in the middle position and all digits distinct is 40, by the multiplication principle.

If the middle position is filled up by a digit other than 0, then this can be done in 8 ways. Then the first position can be filled up in 7 ways. So, the number of odd numbers with all digits distinct with the middle digit not zero is 5.8.7 = 280.

Thus, by the addition principle the answer is 40 + 280 = 320.

E6) $(m + n)! = (m + n)(m + n - 1) \ldots (m + 1) m!$.
$\Rightarrow (m + n)! - m! = \geq m^n + n! \geq m! [n! + m^n - 1]$
$\Rightarrow (m + n)! - m! - n! \geq n! (m! - 1) + m! (m^n - 1) \geq 0$.

E7) Without repetitions, the number is P(6, 3). For the number to be less than 400, the leftmost digit can only be 2 or 3. The rest of the digits can be filled in P(5, 2) ways. So, the total number of numbers less than 400 will be 2P(5, 2). Similarly, the total number of even numbers is 3P(5, 2).

Note: That the addition principle has been used in both cases.

E8) A ranking is an ordering of the n candidates. This can be done in P(n,n) = n! ways. The total number of rankings in which Sheela is in 2nd place in P(n – 1, n – 1) = (n – 1)!

E9) In the word 'ASSESSES', we have A once, E twice, and S five times. Thus the number of permutations is 8!/1!2!5! = 168.
In the word 'PATTIVEERANPATTI', R, N and V occur once, P, E and I occur twice, A thrice and T four times. Thus the required number of permutations is 16!/1!1!1!2!2!2!3!4! = 9.10.

E10) By the multiplication principle, the answer is 26.25.24 if the letters cannot be repeated, and 26.26.26 if the letters can be repeated.

E11) The seven men can be seated first. This can be done in 6! ways. The women can sit in between two men. There are seven such places. So, the women can sit in P(7,5) ways. Hence the answer is 6! × P(7,5).

E12) This can be done in C(12, 1).C(15,1) ways, i.e., 180 ways.

E13) This can be done in C(10, 3) ways, i.e., 120 ways.

E14) The total number of possibilities is C(20,3).C(30,4) = 31,241,700.

E15) Applying Theorem 5, we get C(9, 4) = 126 days.

E16) i) Be careful! This is not an application of Theorem 5. This is only the number of ways of choosing 5 balls out of 8 balls, i.e. C(8, 5).

ii) First pick 5 red balls, in C(8,5) ways. Then pick the remaining 2 arbitrarily. These 2 can be chosen in C(2+2–1, 2) = 3 ways. So, the total number of ways is C(8, 5) × 3.

E17) We have 2Cs, 3As, 1R and 1S. If order is not a concern, we consider the solutions of

$c+a+r+s = 6,\ 0 \le c \le 2,\ 0 \le a \le 3,\ 0 \le r, s \le 1.$

We convert this to the equivalent problem

$x+y+z+t = 1$, where $x = 2 - c$, $y = 3 - a$, $r = 1 - z$, $s = 1 - t$,

The number of solutions of this is $C(4 + 1 - 1, 1) = 4$.

There are (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0) and (0, 0, 0, 1).

The corresponding solutions in (c, a, r, s) are (1, 3, 1, 1), (2, 2, 1, 1), (2, 3, 0, 1), (2, 3, 1, 0).

Now order becomes important to us. Applying Theorem 2, the required number is

$$\frac{6!}{1!3!1!1!} + \frac{6!}{2!2!1!1!} + 2\left(\frac{6!}{2!3!1!0!}\right) = 420.$$

E18) The left side counts the ways to select a group of m people chosen from a set of n people and then select a subset of k leaders, say, of this group of m. This can also be done by selecting the subset of k leaders from the set of n people first, and then selecting the remaining m – k members of the group from the remaining n – k people. The number of ways in which this can be done is given on the right hand side. Therefore, the identity.

You can also prove this algebraically.

E19) One can prove this by induction on the variable n. The base case is trivial, since if n = 0, then k = 0 as well, and the equation reduces to C(0, 0) = C(1, 1), which is true. The induction step is proved by Pascal's formula and the induction hypothesis.

E20) The relative weightages of A, B, C and D are 6.3, 1, 1, respectively. So, P(A) = $\frac{6}{11}, P(B) = \frac{3}{11}, P(C) = \frac{1}{11} = P(D)$.

E21) The answer is same as the probability of getting at least 6 heads in 10 tosses of a true coin. Hence, the answer is

$C(10, 6)/2^{10} + C(10, 7)/2^{10} + C(10, 8)/2^{10} + C(10, 9)/2^{10} + C(10, 10)/2^{10}$

$= (210 + 120 + 45 + 10 + 1)/1024 = 193/512.$

UNIT 3 SOME MORE COUNTING PRINCIPLES

Structure **Page No.**

3.0 INTRODUCTION

In this unit, we continue our discussion of the previous unit on combinatorial techniques. We particularly focus on two principles of counting – the pigeonhole principle and the principle of inclusion-exclusion.

In Sec. 3.2 you will see how obvious the pigeonhole principle is. Its proof is very simple, and amazingly, it has several useful applications. We shall also include some of these in this section.

In Sec. 3.3, we focus on the principle (or formula) of inclusion-exclusion. As you will see, this principle tells us how many elements do not fit into any of n categories. We prove this result and also give a generalisation. Following this, in Sec. 3.4 we give several important applications of inclusion-exclusion.

We shall continue our discussion on combinatorial techniques in the next unit.

3.1 OBJECTIVES

After studying this unit, you should be able to:

- prove the pigeonhole principle, and state the generalised pigeonhole principle;
- identify situations in which these principles apply, and solve related problems;
- prove the principle of inclusion-exclusion;
- apply inclusion-exclusion for counting the number of surjective functions, derangements and for finding discrete probability.

3.2 PIGEONHOLE PRINCIPLE

Let us start with considering a situation where we have 10 boxes and 11 objects to be placed in them. Wouldn't you agree that regardless of the way the objects are placed in the two boxes at least one box will have more than one object in it? On the face of it, this seems obvious. This is actually an application of the pigeonhole principle, which we now state.

Theorem 1 (The Pigeonhole Principle): Let there be n boxes and (n+1) objects. Then, under any assignment of objects to the boxes, there will always be a box with more than one object in it.

This can be reworded as: if m pigeons occupy n pigeonholes, where m > n, then there is at least one pigeonhole with two or more pigeons in it.

Proof: Let us label the n pigeonholes 1, 2, …, n, and the m pigeons p_1, p_2, …, p_m. Now, beginning with p_1, we assign one each of these pigeons the holes numbered 1, …, n, respectively. Under this assignment, each hole has one pigeon, but there are still (m–n) pigeons left. So, in whichever way we place these pigeons, at least one hole will have more than one pigeon in it. This completes the proof!

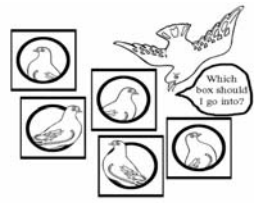


Fig. 1 The pigeonhole principle

This result appears very trivial, but has many applications. For example, using it you can show that:

- if 8 people are picked in any way from a group, at least 2 of them will have been born on the same weekday.
- in any group of 13 people, at least two are born in the same month.

Let us consider some examples of its application, in detail.

Example 1: Assuming that friendship is mutual, show that in any group of people we can always find two persons with the same number of friends in the group.

Solution: If there are n persons in the group, then let the number of friends the ith person has be f(i), i = 1,…, n. Clearly, f(i) can take values only between 0 and (n – 1).

If some f(i) is 0, it means that the ith person does not have any friends in the group. In this case, no person can be friends with all the other (n – 1) people. So, no f(i) can be (n – 1). So, only one of the values 0 or (n – 1) can be present among the f(i)'s. So, the n f(i)'s can take only (n – 1) distinct values. Therefore, by the pigeonhole principle, two f(i)'s must be equal. Then the corresponding i's have the same number of friends in the group.

* * *

Example 2: Suppose 5 points are chosen at random within or on the boundary of an equilateral triangle of side 1 metre. Show that we can find two points at a distance of at most ½ metre.

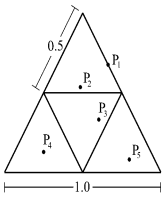


Fig. 2

Solution: Divide the triangle into four equilateral triangles of side ½ m by joining the midpoints of the sides by three line segments (see Fig. 2). These four triangles may now be considered as boxes and the five points as objects. By the pigeonhole principle, at least one of these smaller triangles will have two points in or on it. Clearly, the distance between these two points is at most ½ metre.

* * *

Example 3: Given any ten different positive integers less than 107, show that there will be two disjoint subsets with the same sum.

Solution: The highest numbers we could be given would be 97, 98, …, 106, which add up to 1015. So, consider pigeonholes marked 0, 1, 2,…, 1015. The set of 10 positive integers have 2^{10} = 1024 subsets. Put a subset in the pigeonhole marked with the sum of the numbers in the set. The 1024 subsets have to be put in 1016 pigeonholes. So, some pigeonhole will have more than one subset with the same sum.

Now, note that two subsets that we get with the same sum, may not be disjoint. But, by dropping the common elements in them, we are left with disjoint subsets with the same sum.

* * *

Here are some related exercises for you to do.

E1) If 10 points are chosen in an equilateral triangle of side 3 cms., show that we can find two points at a distance of at most 1 cm.

E2) On 11 occasions a pair of persons from a group of 5 was called for a function. Show that some pair of persons must have attended the function at least twice.

E3) Four persons were found in a queue, independently, on 25 occasions. Show that at least on two occasions they must have been in the queue in the same order.

As you know, **mathematics develops through a process of generalisation**. You know that the principle is valid for n+1 objects and n boxes. It is natural to ask: what if we have, say, 4n+1 objects and 4 boxes? Can we prove a similar principle? In fact, we can, as given below.

Theorem 2 (The Generalized Pigeonhole Principle): If nm + 1 objects are distributed among m boxes, then at least one box will contain more than n objects.

This can be reworded as: Let k and n be positive integers. If k balls are put into n boxes, then some box contains at least [k/n] + 1 balls, where [x] denotes the greatest integer less than x.

Proof: We prove this by contradiction (see Unit 2, Block 1). Suppose all the m boxes have at most n objects in them. Then the total number of objects is at most nm, a contradiction. Hence, the theorem.

Applying this result, we see, for example, that suppose 479 students are enrolled in the course Discrete Mathematics, consisting of 6 units. Then, at least $\left[\frac{479}{6}\right]+1=80$ students are studying the same unit at a given point of time.

Let us consider a few more examples of the application of this principle.

Example 4: Show that in any group of 30 people, we can always find 5 people who were born on the same day of the week.

Solution: 30 people can be assigned to 7 days of the week. Then at least $\left[\frac{30}{7}\right]+1=5$ of them must have been born on the same day.

* * *

Example 5: 20 cards, numbered from 1 to 20, are placed face down on a table. 12 cards are selected one at a time and turned over. If two of the cards add up to 21, the player loses. Is it possible to win this game?

Solution: The pairs that can add up to 21 are (1, 20), (2, 19),…, (10,11). So, there are 10 such pairs. In turning 12 cards, at least one of these pairs will be included. Therefore, the player will lose.

* * *

Example 6: Show that every sequence of $n^2 + 1$ distinct integers includes either an increasing subsequence of n + 1 numbers or a decreasing subsequence of n + 1 numbers.

Solution: Let the sequence be $a_1, a_2,\ldots, a_{n^2+1}$. Suppose there is no increasing subsequence of n + 1 numbers. For each of these a_ks, let s(k) be the length of the longest increasing subsequence beginning at a_k. Since all n^2+1 of the s(k)'s are between 1 and n, at least $\left[\frac{n^2+1}{n}\right]+1 = n+1$ of these numbers are the same. (The s(k)'s are the objects and the numbers from 1 to n are the boxes.)

Now, if i < j and s(i) = s(j), then $a_i > a_j$. Otherwise a_i followed by the longest increasing subsequence starting at a_j would be an increasing subsequence of length s(j) + 1 starting at a_i. This is a contradiction, since s(i) = s(j).

Therefore, all the n + 1 integers a_k, for which s(k) = m, must form a decreasing subsequence of length at least n + 1.

* * *

Example 7: Take n integers, not necessarily distinct. Show that the sum of some of these numbers is a multiple of n.

Solution: Let S(m) be the sum of the first m of these numbers. If for some r and m, r < m, S(m) – S(r) is divisible by n, then $a_{r+1} + a_{r+2} + \ldots + a_m$ is a multiple of n. This also means that S(r) and S(m) leave the same remainder when divided by n. So, if we cannot find such pairs m and r, then it means that the n numbers S(1), S(2),…, S(n) leave different remainders when divided by n. But there are only n possible remainders, viz., 0, 1, 2,…, (n – 1). So, one of these numbers must leave a remainder of 0. This means that one of the S(i) s is divisible by n. This completes the proof.

In fact, in this example we have proved that one of the sums of consecutive terms is divisible by n.

* * *

You may like to try some exercises now.

E4) If any set of 11 integers is chosen from 1, …,20, show that we can find among them two numbers such that one divides the other.

E5) If 100 balls are placed in 15 boxes, show that two of the boxes must have the same number of balls.

E6) If $a_1, a_2,\ldots, a_n$ is a permutation of 1, 2,…, n and n is odd, show that the product $(a_1 – 1)(a_2 – 2)\ldots(a_n – n)$ must be even.

There are several corollaries to Theorem 2. We shall present one of them here.

Theorem 3: If a finite set S is partitioned into s subsets, then at least one of the subsets has $\frac{|S|}{k}$ or more elements.

Proof: Let $A_1, \ldots, A_k$ be a partition of S. (This means that $A_i \cap A_j = \phi$ for $i \neq j$ and $S = A_1 \cup A_2 \cup \ldots \cup A_k$.) Then the average value of $|A_i|$ is $\frac{1}{k}[\,|A_1| + \ldots + |A_k|\,] = \frac{|S|}{k}$.

So the largest A_i has at least $\frac{|S|}{k}$ elements.

A consequence of this result is the following theorem.

Theorem 4: Consider a function f: S → T, where S and T are finite sets satisfying $|S| > r|T|$. Then at least one of the sets $f^{-1}(t)$, t∈T, has more than r elements. ($f^{-1}(t)$ denotes the inverse image of the set {t}, i.e., $f^{-1}(t) = \{x \in S : f(x) = t\}$.)

Proof: The family $\{f^{-1}(t): t \in T\}$ partitions S into k sets with $k \leq |T|$. By Theorem 3, some set in this family, say $f^{-1}(t')$, has at least $\frac{|S|}{k}$ members. Since $\frac{|S|}{k} \geq \frac{|S|}{T} > r$ by our hypothesis, $f^{-1}(t')$ has more than r elements.

Corollary: If f: S → T and $|S| > |T|$, then **f is not injective.**

Proof: Putting r = 1 in Theorem 4, we see that at least one of the sets $f^{-1}(t)$ has more than one element.

We conclude this section with some more extensions of the pigeonhole principle.

Theorem 5: Suppose we put an infinity of objects in a finite number of boxes. Then at least one box must have an infinity of objects.

Proof: If every box contains only a finite number of objects, then the total number of objects must be finite. Hence the theorem.

Theorem 6 (A generalisation of Theorem 3): Let $A_1, A_2, \ldots, A_k$ be subsets of a finite set S such that each element of S is in at least t of the sets A_i. Then the average number of elements in the A_is is at least $t.\frac{|S|}{k}$. (Note that, in this statement, the sets A_i may overlap.)

We leave the proof to you to do, and give you some related exercises now.

E7) Every positive integer is given one of the seven colours in VIBGYOR. Show that at least one of the colours must have been used infinitely many times.

E8) Let A be a fixed 10-element subset of {1, 2,…, 50}. Show that A possesses two different 5-element subsets, the sum of whose elements are equal.

E9) The positive integers are grouped into 100 sets. Show that at least one of the sets has an infinity of even numbers. Is it necessary that at least one set should have an infinity of even numbers and an infinity of odd numbers?

Let us now consider another very important counting principle.

3.3 INCLUSION-EXCLUSION PRINCIPLE

Let us begin with considering the following situation: In a sports club with 54 members, 34 play tennis, 22 play golf, and 10 play both. There are 11 members who play handball, of whom 6 play tennis also, 4 play golf also, and 2 play both tennis and golf. How many play none of the three sports?

To answer this, let S represent the set of all members of the club. Let T represent the set of tennis playing members, G represent the set of golf playing members, and H

represent the set of handball playing members. Let us represent the number of elements in A by $|A|$. Consider the number $|S|-|T|-|G|-|H|$. Is this the answer to the problem? No, because those who are in T as well as G have been subtracted twice. To compensate for this double subtraction, we may now consider the number $|S|-|T|-|G|-|H|+|T\cap G|+|G\cap H|+|H\cap T|$. Is this the answer? No, because those playing all the three games have been subtracted thrice and then added thrice. But those members have to be totally excluded also. Hence, we now consider the number $|S|-|T|-|G|-|H|+|T\cap G|+|G\cap H|+|H\cap T|-|T\cap G\cap H|$. This is the correct answer. This reduces to 54 – 34 – 22 – 11 + 10 + 6 + 4 – 2 = 5.

To solve this problem we have made inclusions and exclusions alternately to arrive at the correct answer. This is a simple case of **the principle of inclusion and exclusion**. It is also known as the **sieve principle** because we subject the objects to sieves of a progressively finer mesh to arrive at a certain grading.

Let us state and prove this principle now.

A^c, or $\bar{A}$, denotes the complement of the set A

Theorem 7 (The inclusion-exclusion formula): Let $A_1, A_2,\ldots, A_n$ be n sets in a universal set U consisting of N elements. Let S_k denote the sum of the sizes of all the sets formed by intersecting k of the A_is at a time. Then the number of elements in none of the sets $A_1, A_2,\ldots, A_n$ is given by

$$\left|\bar{A}_1\cap\bar{A}_2\cap\ldots\cap\bar{A}_n\right| = N - S_1 + S_2 - S_3 + \ldots + (-1)^k S_k + \ldots + (-1)^n S_n .$$

RHS is short for 'right-hand side'.

Proof: The proof is on the same lines of the counting argument given in the 'sports club' example at the beginning of this section. If an element is in none of the A_is, then it should be counted only once, as part of 'N' in the RHS of the formula above. It is not counted in any of the S_ks since it is in none of the A_is.

Next, an element in exactly one A_i, say A_r, is counted once in N, and once in S_1, and in none of the other S_ks. So the net count is 1–1 = 0.

Finally, take an element x in exactly m of the A_is. This is counted once in N, m times in S_1, C(m, 2) times in S_2 (since x is in C(m, 2) intersections $A_i\cap A_j$),…, C(m, k) times in S_k for $k \le m$. x is not counted in any S_k for k > m. So the net count of x in the RHS of the formula is

1– C(m,1) + C(m,2) – … + $(-1)^k$ C(m, k) + … + $(-1)^m$ C(m, m) = 0, by Identity 2 in Sec. 2.5.

So the only elements that have a net count of 1 in the RHS are those in $\bigcap_{i=1}^{n}\bar{A}_i$. The rest have a net count of 0. Hence the formula.

From this result, we immediately get the following one.

Corollary: Given the situation of Theorem 7,

$$\left|A_1\cup A_2\cup\ldots\cup A_n\right| = S_1 - S_2 + \ldots + (-1)^{k-1}S_k + \ldots + (-1)^{n-1}S_n .$$

Why don't you try and prove this result? (see E 10.)

What the inclusion-exclusion principle tells us is that to calculate the size of $A_1\cup A_2\cup\ldots\cup A_n$, calculate the size of all possible intersections of the sets $A_1, A_2,\ldots,A_n$. Add the results obtained by intersecting an odd number of the sets, and then subtract the results obtained by intersecting an even number of the sets. Therefore, this principle is ideally suited to situations in which

i) we just want the size of $A_1 \cup A_2 \cup \ldots \cup A_n$, not a listing of its elements, and

ii) multiple intersections are fairly easy to count.

Now let us consider some examples in which Theorem 7 is applied.

Example 8: How many ways are there to distribute r distinct objects into five (distinct) boxes with

i) at least one empty box?

ii) no empty box ($r \geq 5$)?

Solution: Let U be all possible distributions of r distinct objects into five boxes. Let A_i denote the set of possible distributions with the ith box being empty.

i) Then the required number of distributions with at least one empty box is $|A_1 \cup A_2 \cup \ldots \cup A_5|$. We have $N = 5^r$. Also, $|A_i| = (5-1)^r$, the number of distributions in which the objects are put into one of the remaining four boxes. Similarly, $|A_i \cap A_j| = (5-2)^r$, and so forth. Thus, by the corollary above, we have

$$|A_1 \cup \ldots \cup A_5| = S_1 - S_2 + S_3 - S_4 + S_5$$
$$= C(5,1)4^r - C(5,2)3^r + C(5,3)2^r - C(5,4)1^r + 0$$

ii) $\left|\bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_5\right| = 5^r - C(5,1)4^r + C(5,2)3^r - C(5,3)2^r + C(5,4)1^r$, by Theorem 7.

* * *

Example 9: How many solutions are there to the equation $x + y + z + w = 20$, where x, y, z, w are positive integers such that $x \leq 6$, $y \leq 7$, $z \leq 8$, $w \leq 9$?

Solution: To use inclusion-exclusion, we let the objects be the solutions (in positive integers) of the given equation. A solution is in A_1 if $x > 6$, in A_2 if $y > 7$, in A_3 if $z > 8$, and in A_4 if $w > 9$. Then what we need is $\left|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4\right|$.

Now, to find the total number of **positive** solutions to the given equation, we rewrite it as $x_1+y_1+z_1+w_1 = 16$, where $x_1 = x+1$, $y_1 = y+1$, $z_1 = z+1$, $w_1 = w+1$. Any non-negative solution of this equation will be a positive solution of the given equation. So, the number of positive solutions is

N = C(16+4–1, 16) (see Example 11 of Unit 2)
= C(19, 3).

Similarly, $|A_1| = C(13,3), |A_2| = C(12,3), |A_3| = C(11,3),$

$|A_4| = C(10,3)$, $|A_1 \cap A_2| = C(6,3), |A_2 \cap A_3| = C(5,3)$, and so on. **Note** that for a solution to be in 3 or more A_i s, the sum of the respective variables would exceed 20, which is not possible. By inclusion- exclusion, we obtain

$$\left|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4\right| = C(19, 3) - C(13, 3) - C(12, 3) - C(11, 3) - C(10, 3)$$

+ C(6, 3) + C(5, 3) + C(4, 3) + C(4, 3) + C(3, 3) = 217.

* * *

Now you may try the following exercises.

E10) Prove the corollary to Theorem 7.

E11) How many numbers from 0 to 999 are not divisible by either 5 or 7?

Let us now consider applications of the inclusion-exclusion principle to some specific problem types.

3.4 APPLICATIONS OF INCLUSION-EXCLUSION

In this section we shall consider three broad kinds of applications — for counting the number of surjective functions, finding probability and finding the number of derangements.

3.4.1 Application to Surjective Functions

Let us first recall that a function $f : S \to T$ is called **surjective** (or **onto**) if $f(S) = T$, that is, if for every $t \in T \; \exists \; s \in S$ such that $f(s) = t$. Now let us prove a very useful result regarding the number of such functions.

Theorem 8: The number of functions from an m-element set **onto** a k-element set is $\sum_{i=0}^{k} (-1)^i C(k,i)(k-i)^m$, where $1 \le k \le m$.

Proof: We will use the inclusion-exclusion principle to prove this. For this, we define the objects to be all the functions (not just the onto functions) from M, an m-element set, to K, a k-element set. For these objects, we will define A_i to be the set of all $f: M \to K$ for which the ith element of K is not in f(M). Then what we want is $\left|\bar{A}_1 \cap .... \cap \bar{A}_k\right|$.

Now, the total number of functions from M to K is k^m. Also, the number of mappings that exclude a specific set of i elements in K is $(k-i)^m$, and there are C(k, i) such sets. Therefore, $|A_i| = (k-1)^m$, $|A_i \cap A_j| = (k-2)^m$, and so on.

Now, applying Theorem 7, we get

$$\left|\bar{A}_1 \cap ... \cap \bar{A}_k\right| = k^m - C(k,1)(k-1)^m + C(k,2)(k-2)^m - ... + (-1)^{k-1} C(k,k-1)1^m$$

Hence the result.

For example, the number of functions from a five-element set onto a three-element set are $\sum_{i=0}^{k} (-1)^i C(k,i)(k-i)^m$ for m = 5 and k = 3, that is, $3^5 - 3.2^5 + 3.1^5 = 150$.

Why don't you try some exercises now?

E12) Eight people enter an elevator. At each of four floors it stops, and at least one person leaves the elevator. After four floors the elevator is empty. In how many ways can this happen?

E13) How many six-digit numbers contain exactly three different digits?

Now we look at another application.

3.4.2 Application to Probability

An important application of the principle of inclusion-exclusion is used in probability. We have the following theorem.

Theorem 9: Suppose $A_1, A_2, \ldots, A_n$ are n events in a probability space. Then

$$P(A_1 \cup A_2 \cup \ldots \cup A_n) = \sum_{r=1}^{n} (-1)^{r+1} \sum_{1 \le i_1 < i_2 < \ldots < i_r \le n} P(A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r})$$

Proof: Let us begin by observing that $A_1 \cup A_2 \cup \ldots \cup A_n$ means that at least one of the events $A_1, A_2, \ldots, A_n$ occurs. Now, let the ith property be that an outcome belongs to the event A_i. By De Morgan's law, $\bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_n$ is the complement of $A_1 \cup A_2 \cup \ldots \cup A_n$. But the principle of inclusion-exclusion gives

$$\left| \bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_n \right| = N - \sum (-1)^r \sum_{1 \le i_1 < i_2 < \ldots < i_r \le n} \left| A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r} \right|$$, where N is the total number of outcomes.

Now, we divide throughout by N and note that

$P(A_1 \cup A_2 \cup \ldots \cup A_n) = 1 - P(\bar{A}_1 \cap \bar{A}_2 \cap \ldots \cap \bar{A}_n)$, to get the result.

Let us consider an example of the use of this result.

Example 12: Find the probability of a student in a college studying Japanese, given the following data:

All students have to study at least one language out of Hindi, Spanish and Japanese. 65 study Hindi, 45 study Spanish and 42 study Japanese. Further, 20 study Hindi and Spanish, 25 study Hindi and Japanese, 15 study Spanish and Japanese, and 8 study all 3 languages.

Solution: The total number of students is $|H \cup S \cup J|$, where H, S and J denote the number of students studying Hindi, Spanish and Japanese, respectively. By the inclusion-exclusion principle,

$$|H \cup S \cup J| = |H| + |S| + |J| - |H \cap S| - |H \cap J| - |S \cap J| + |H \cap S \cap J|$$
$$= 65 + 45 + 42 - 20 - 25 - 15 + 8 = 100$$

Therefore, the required probability is $\frac{|J|}{100} = 0.42$.

* * *

You could do the following exercises now.

E14) What is the probability that a 13-card hand has at least one card in each suit?

E15) What is the probability that a number between 1 and 10,000 is divisible by neither 2, 3, 5 nor 7?

Let us now come to the use of inclusion-exclusion for counting the number of a particular kind of permutation.

3.4.3 Application to Derangements

As you know, a permutation of a set is an arrangement of the elements of a set.

So, for example, a rearrangement $1 \to 1, 2 \to 2, 4 \to 3, 3 \to 4$ is a permutation of the 4-element set {1, 2, 3, 4}. In this permutation, the position of the elements 1 and 2 are **fixed**, but the positions of 3 and 4 have been interchanged. Now consider the permutation $1 \to 4, 2 \to 1, 3 \to 2, 4 \to 3$, of {1, 2, 3, 4}, in which the position of **every element** has been changed. This is an example of a derangement, a term we shall now define.

Definition: A **derangement** of a set S is a permutation of the elements of S which does not fix any element of S, i.e., it is a rearrangement of the elements of S in which the position of every element is altered.

So, if we treat a permutation as a 1-to-1 function from S to S, then a derangement is a function $f:S \to S$ such that $f(s) \neq s \ \forall \ s \in S$.

We have the following theorem regarding the number of derangements.

Theorem 10: The number of derangements of an n-element set is $D_n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$.

Proof: Let A_i be the set of all permutations of the n-element set that fix i $\forall$ i = 1, …, n. Then

$$D_n = \left| \bigcap_{i=1}^{n} \bar{A}_i \right| = n! - \sum_i \left| A_i \right| + \sum_{i<j} \left| A_i \cap A_j \right| - \ldots + (-1)^n \left| A_1 \cap \ldots \cap A_n \right|$$

$$= n! - C(n, 1)\,(n-1)! + C(n, 2)\,(n-2)! - \ldots + (-1)^n C(n, n)0!$$

$$= n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}\right), \text{ which is the expression we wanted.}$$

Remark: The expression $\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}\right)$ is the beginning of the expansion for e^{-1}. Even for moderately large values of n, D_n is very close to $n!e^{-1}$=0.36788 n!.

As an extension of Theorem 10, we have the following results.

Theorem 11: For a set of n objects, the number of permutations in which

(i) only r of these n objects are deranged is

$$n! - C(r, 1)\,(n-1)! + C(r, 2)\,(n-2)! - \ldots + (-1)^r C(r, r)\,(n-r)!;$$

(ii) exactly r elements are fixed is $C(n, r)\, D_{n-r}$.

We will not prove these formulae here, but shall consider some examples of their applications.

Example 12: Let n books be distributed to n children. The books are returned and distributed to the children again later on. In how many ways can the books be distributed so that no child will get the same book twice?

Solution: The required number is $(n!)^2e^{-1}$, since corresponding to each first distribution, there are $(n!)e^{-1}$ ways of distributing again.

* * *

Example 13: Suppose 10 people have exactly the same briefcases, which they leave at a counter. The cases are handed back to the people randomly. What is the probability that no one gets the right case?

Solution: The number of possibilities favourable to the event is D_{10}. The total number of possibilities is 10!. Thus, the probability that none will get the right briefcase is $D_{10}/10! = 0.36788$.

* * *

Note that, since $D_n \approx n!e^{-1}$, the possibility in all such examples is essentially e^{-1}, which is independent of n.

You may now try the following exercises.

E16) Each of the n guests at a party puts on a coat when s/he leaves. None of them gets the correct coat. In how many ways can this happen? In how many ways can just one of the guests get the right coat?

E17) In how many ways can the integers 1, 2, 3,…,9 be permuted such that no odd integer will be in its natural position.

E18) Find the number of permutations in which exactly four of the nine integers 1, 2,…,9 are fixed.

With this we come to the end of this unit. In the next unit we shall continue our discussion on 'counting' from a slightly different perspective. Let us now summarise what we have covered in this unit.

3.6 SUMMARY

In this unit, you have studied the following points.

1. The pigeonhole principle, stated in several forms, its proof, and its applications.
2. The generalized pigeonhole principle, its proof, and applications.
3. The inclusion-exclusion principle, and its proof.
4. Finding the number of surjective functions, the discrete probability and the number of derangements, by using the inclusion-exclusion principle.

3.7 SOLUTIONS /ANSWERS

E1) By drawing lines parallel to the sides and through the points trisecting each side, we can divide the equilateral triangle into 9 equilateral triangles of side 1 cm. Thus, if 10 points are chosen, at least two of them must lie in one of the 9 triangles.

E2) 5 persons can be paired in C(5, 2) =10 ways. Hence, if pairs are invited 11 times, at least one pair must have been invited twice or more times, by the pigeonhole principle.

E3) Four persons can be arranged in a line in 4! = 24 ways. Hence, if we consider 25 occasions, at least on two occasions the same ordering in the queue must have been found, by the pigeonhole principle.

E4) Consider the following grouping of numbers:

{1, 2, 4, 8, 16}, {3, 9, 18}, {5, 15}, {6, 12}, {7, 14}, {10, 20}, {11}, {13}, {17}, {19}.

There are 10 groupings, exhausting all the 20 integers from 1 to 20. If 11 numbers are chosen it is impossible to select at most one from each group. So two numbers have to be selected from some group. Obviously one of them will divide the other.

E5) Suppose $x_1, x_2, \ldots, x_{15}$ are the number of balls in the 15 boxes, listed in increasing order, assuming that all these numbers are different. Then, clearly, $x_i \geq i - 1$ for i = 1, 2,…,15. But then, $\sum_{i=1}^{15} x_i \geq 14.15/2 = 105$.

But the total number of balls is only 100, a contradiction. Thus, the x_is cannot all be different.

E6) In the sequence $a_1, a_2, \ldots, a_n$, there are (n+1)/2 odd numbers and (n–1)/2 even numbers because n is odd. Hence, it is impossible to pair all the a_is with numbers from 1, 2,…, n with opposite parity (evenness and oddness). Hence, in at least one pair (i, a_i), both the numbers will be of the same parity. This means that the factor $(a_i - i)$ will be even, and hence the product will be even.

E7) Consider the seven colours as containers, and the integers getting the respective colour as their contents. Then we have a distribution of an infinite number of objects among 7 containers. Hence, by Theorem 5, at least one container must have an infinity of objects, that is, the colour of that container must have been used an infinite number of times.

E8) Let H be the family of 5-element subsets B of A. For each B in H, let f(B) be the sum of the numbers in B. Obviously, we must have

$f(B) \geq 1 + 2 + 3 + 4 + 5 = 15$, and $f(B) \leq 46 + 47 + 48 + 49 + 50 = 240$.

Hence, $f: H \to T$ where T = {15, 16,…, 240}.

Since $|T| = 226$ and $|H| = C(10,5) = 252$, by Theorem 4, H contains different sets with the same image under f, that is different sets, the sums of whose elements are equal.

E9) The 100 collections can be considered as containers. There are an infinity of even numbers. When these even numbers are distributed into 100 containers, at least one container must have an infinity of them, by Theorem 5.

E10) The inclusion-exclusion formula can be rewritten as

$$\left|\bar{A}_1 \cap \ldots \cap \bar{A}_n\right| = N - (S_1 - S_2 + \ldots + (-1)^{n-1} S_n.$$

Also, we know that $\left|\bar{A}_1 \cap \ldots \cap \bar{A}_n\right| = N - |A_1 \cup \ldots \cup A_n|$.

Hence the result.

E11) Let the objects be the integers 0, 1,…, 999. Let A_1 be the set of numbers divisible by 5, and A_2 the set of numbers divisible by 7. Now, N = 1000, $|A_1|$ = 200, $|A_2|$ =143 and $|A_1 \cap A_2| = 29$. So, by Theorem 7, the answer is 1000 – 200 – 143 + 29 = 686.

E12) The answer to this problem is clearly the number of functions from an 8-element set (the set of people) onto a set of 4-elements (the set of floors). This number is

$$\sum_{i-0}^{4} C(4,i)(4-i)^8 = 4^8 - 4.3^8 + 6.2^8 - 4.1^8.$$

E13) We can choose three digits in C(10,3) = 120 ways.
The number of 6-digit numbers, using all the three digits, is the same as the number of functions from a 6-set onto a 3-set. This number is

$3^6 – 3.2^6 + 3.1^6 = 540$.

Hence, the answer is 120.540 = 64800. This will include numbers starting with 0 also.

E14) The total number of ways in which 13 cards can be chosen from a deck of 52 cards is C(52, 13).

If A_i is a choice of cards, none of which are from the ith suit, for i = 1,2,3,4, then $|A_i| = C(39,13), |A_i \cap A_j| = C(26,13)$, and $C(A_i \cap A_j \cap A_k) = C(13,13)$.

So, $\left|\cap \bar{A}_i\right| = C(52,13) - 4C(39,13) + C(4,2)C(26,13) - C(4,3)\,C(13, 13)$

Hence, the required probability is $\dfrac{\left|\cap \bar{A}_i\right|}{C(52,13)}$.

E15) If A,B,C,D are the integers divisible by 2, 3, 5, 7, respectively, then

$$\left|\bar{A} \cap \ldots \cap \bar{D}\right| = 10{,}000 - \left[\frac{10000}{2}\right] - \left[\frac{10000}{3}\right] - \left[\frac{10000}{5}\right] - \left[\frac{10000}{7}\right]$$

$$+ \left[\frac{10000}{6}\right] + \left[\frac{10000}{15}\right] + \left[\frac{10000}{35}\right] + \left[\frac{10000}{14}\right] + \left[\frac{10000}{21}\right] + \left[\frac{10000}{10}\right]$$

$$- \left[\frac{10000}{30}\right] - \left[\frac{10000}{42}\right] - \left[\frac{10000}{105}\right] - \left[\frac{10000}{70}\right] + \left[\frac{10000}{210}\right]$$

= 2285, where [x] denotes the greatest integer ≤ x.

Hence, the required probability is $\dfrac{2285}{10000} = 0.23$.

E16) If A_r is the event that the rth person gets the right coat, then by Theorem 7,

$$\left|\cap \bar{A}_i\right| = n! - \sum_r |A_r| + \sum_{r,s} |A_r \cap A_s| - \ldots$$

$$= n! - n(n-1)! + C(n,2)(n-2)! - C(n,3)(n-3)! + \ldots$$

$= C(n,2)(n-2)! - C(n,3)(n-3)!+\ldots$

$= n!\left(\sum_{r=0}^{n}(-1)^r\frac{1}{r!}\right)$

The number of ways in which only one person receives the correct coat is the sum of all possible intersections of $(n-1)$ $\bar{A}_i$ s. This is

$n!\ n(n-1)!\left(\sum_{r=0}^{n-1}(-1)^r\frac{1}{r!}\right) = n!\left(\sum_{r=0}^{n-1}(-1)^r\frac{1}{r!}\right)$.

E17) 1, 3, 5, 7, 9 are the odd integers.
By Theorem 11(i), the required number of ways is
$9! - C(5,1)8! + C(5,2)7! - C(5,3)6! + C(5,4)5! - C(5,5)4!$

E18) By Theorem 11(ii), the required number of permutations is
$C(9,4)D_{9-4}=C(9,4)D_5$.

UNIT 4 PARTITIONS AND DISTRIBUTIONS

Structure **Page No.**

4.0 INTRODUCTION

In the last two units we have exposed you to a variety of combinatorial techniques. In this unit we look at a few more ways of counting arrangements of objects when order matters, and when it doesn't.

In Sec. 4.2, we focus on the ways in which a natural number can be written as a sum of natural numbers. In the process you will be introduced to a useful 'recurrence relation'.

We link this, in Sec. 4.3, with the different ways in which n objects can be distributed among m containers. As you will see, there are four broad possible kinds of distributions. In each case, we consider ways of counting all the distributions. In the process you will also be introduced to Stirling numbers.

With this unit we come to the end of our discussion on counting techniques. Some of the problems you have studied here will be looked at from different approaches in our later course MCS-033.

You should attempt the assignment based on the course after studying this unit, and this block.

4.1 OBJECTIVES

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

- define an integer partition, and count the number of partitions of an integer;
- count the number of ways of distributing distinguishable and indistinguishable objects, respectively, into distinguishable containers;
- count the number of ways of distributing distinguishable and indistinguishable objects, respectively, into indistinguishable containers.

4.2 INTEGER PARTITIONS

Suppose a detergent manufacturer wants to promote her product by giving a gift token with 100 bars out of the whole stock. The lucky persons among her customers will get the gift. Some of them may buy more than one bar at a time with the hope of getting gifts. In how many ways can the 100 gift tokens get distributed? One possible way is that all the 100 bars with gifts are bought by 100 different customers. We can indicate this situation by $100 = \underbrace{1+1+...+1}_{100 \text{ times}}$. Another possibility is that somebody buys 2 bars,

somebody else buys 3 bars, and the remaining 95 bars are distributed amongst 95 different people. We are not interested in the order in which the bars are bought. For example, here we are not interested in whether the person who bought 2 bars bought them before the person who bought the 3 bars. So, we can indicate this situation by $100 = \underbrace{1+1+...+1}_{95 \text{ times}} + 2 + 3$. More generally, we can indicate each way of distributing the 100 bars with gifts by $100 = p_1 + p_2 + p_2 + \ldots + p_k$, where the p_i are natural numbers, and $p_1 \leq p_2 \leq \ldots \leq p_k$. Each way of writing 100 in this form is called an **integer partition** of 100. More generally, we have the following definition.

Definition: Any representation of $n \in \mathbf{N}$ as a sum of positive integers in non-increasing order is called a **partition** (or **integer partition**) of n. Each such partition can be written in the form $n = p_1 + p_2 + \ldots + p_k$, where $p_1 \leq p_2 \leq \ldots \leq p_k$.

Here, $p_1, p_2, \ldots, p_k$ are called the **parts** of the partition, and the **number of parts** of the partition is k.

While we chose 100 in the example above, it is really a huge number in the context of integer partitions. Let us consider a smaller number, say 5. How many partitions of 5 can you think of? There are 7 altogether, namely, 5, 1+4, 2+3, 1+1+3, 1+2+2, 1+1+1+2 and 1+1+1+1+1.

In books, you will often come across the notation p(n) for the number of partitions of n.

If **we represent the number of partitions of the integer n by P_n,** we have shown that $P_5 = 7$. These partitions have 1, 2, 2, 3, 3, 4 and 5 parts, respectively.

If **we represent the number of partitions of n with exactly k parts by** P_n^k, then we have $P_5^1 = 1, P_5^2 = 2, P_5^3 = 2, P_5^4 = 1, P_5^5 = 1$.

To check your understanding of the material so far, try the following exercises.

E1) Write down all the partitions of 7. Also find P_7^4 and P_7^5.

E2) Let us consider the situation of the detergent manufacturer again. Suppose she only wants to distribute 10 gift tokens in 5 specific sales districts, where the sales are low. What is the number of ways of doing this?

You may wonder if you've found all the partitions in E2. One way to check is by finding out the required number in terms of partitions of smaller numbers, which may be easier to find. One such relation between partitions of n and n+1, n+2, etc. is given in the following theorem.

Theorem 1: $P_n^1 + P_n^2 + \ldots + P_n^k = P_{n+k}^k, P_n^1 = P_n^n = 1,$ for $1 \leq k \leq n$, that is, the number of **partitions of n with at most k parts** is the same as the number of **partitions of n+k with exactly k parts**.

Before we begin the proof of this theorem, let us consider an example. Let us take n = 4, k = 3. According to Theorem 1, we must have $P_4^1 + P_4^2 + P_4^3 = P_7^3$. Note that $P_4^1 + P_4^2 + P_4^3$ is the total number of partitions of 4 with 1, 2 or 3 parts, i.e., the number of partitions with **at most** 3 parts. There is one partition of 4 with one part, 4 = 4. Let us write this as a 3-tuple, (4, 0, 0), adding two more zeroes since we are considering partitions with at most **3** parts. If we add 1 to all the entries of this 3-tuple, we get (4+1,0+1,0+1) = (5,1,1) and (1+1+5 is a partition of 7 with three parts. Similarly, consider the partition 4 = 1+3 of 4 into two parts. Again, we can write this as (1, 3, 0).

Now, if we add 1 to each of the entries, we get (2, 4, 1) and 1+2+4 is a partition of 7 into three parts. Conversely, if we take the partition 7 = 1 + 3 +3 of 7 into three parts, write it as (1, 3, 3) and **subtract** 1 from all the entries, we get (0, 2, 2) which corresponds to the partition 4 = 2+2 of 4 into 2 parts. In this way, we can match every partition of 4 with **at most 3** parts with a partition of 7 with **exactly 3** parts, and vice versa. This is the basic idea behind our proof of Theorem 1, which we now give.

Proof of Theorem 1: The cases $P_n^1 = 1 = P_n^n$ follow from the definition.

We will prove the general formula now. Let M be the set of partitions of n having k or less parts. We can consider each partition belonging to M as a k-tuple after adding as many zeroes as necessary. Define the mapping

$$(p_1, p_2, \ldots, p_m, \underbrace{0,0,\ldots,0}_{\substack{(k-m)\\ \text{times}}}) \mapsto (p_1+1, p_2+1, \ldots, p_m+1, \underbrace{1,1,\ldots,1}_{\substack{(k-m)\\ \text{times}}}),\ m \le k$$

from M into the set M′ of partitions of n+k into exactly k parts. This mapping is bijective, since

i) two distinct k-tuples in M are mapped onto two distinct k-tuples in M′;

ii) every k-tuple in M′ is the image of a k-tuple of M. This is because, if

$(p_1, p_2, \ldots, p_k)$ is a partition of n+k with k parts, then it is the image of

$(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$ under the mapping above.

Therefore, $|M| = P_n^1 + \ldots + P_n^k = |M'| = P_{n+k}^k$, and the theorem is proved.

Note that $P_n^k = 0$ **if n < k**, since there is no partition of n with k parts if n < k. Also, $\mathbf{P_n^n = P_n^1 = 1}$.

The formula in Theorem 1 is an identity which allows us to find P_n^r from values of P_m^k, where m < n, k ≤ r. This is why it is also called a **recurrence relation** for P_n^k.

Theorem 1 is every useful. For instance, to verify your count in E2, you can use it because $P_{10}^5 = P_5^1 + P_5^2 + \ldots + P_5^5 = 7$.

From Theorem 1, the P_n^ks may be calculated recursively as shown in Table 1.

Table 1 : P_n^k for 1 ≤ n, k ≤ 6

n \ k	1	2	3	4	5	6
1	1	0	0	0	0	0
2	1	1	0	0	0	0
3	1	1	1	0	0	0
4	1	2	1	1	0	0
5	1	2	2	1	1	0
6	1	3	3	2	1	1

In this table, the second entry in the row corresponding to n = 4 is P_4^2. By Theorem 1, $P_4^2 = P_2^1 + P_2^2$, which is the sum of the entries in the row corresponding to n = 2.

Similarly, P_6^3 is the sum of the entries in the row corresponding to n = 3.

Now, here is an exercise for you.

E3) Use Table 1 to find the values of $P_7^k, 1 \leq k \leq 6$.

The partition of a number n into k parts also tells us how n objects can be distributed among k boxes. We will now consider all possibilities of such distributions.

4.3 DISTRIBUTIONS

By a distribution we mean a way of placing several objects into a number of containers. For example, consider the distribution of 6 balls among 3 boxes. We may have all 6 balls of different shapes, sizes and colours, i.e., they are all distinguishable. Or, all the balls could be exactly the same, i.e., they are all indistinguishable.

Similarly, all 3 boxes may look different, or all 3 could be exactly the same. So, we see that there are 4 possibilities here.

In fact, we have the following possibilities for any set of n objects and m boxes.

Case 1: The objects are distinguishable, and so are the boxes;

Case 2: The objects are distinguishable and the boxes are indistinguishable;

Case 3: The objects are indistinguishable and the boxes are distinguishable;

Case 4: The objects are indistinguishable, and so are the boxes.

You may be surprised to know that in each of the cases the number of such distributions is different. In fact, the distribution problem is to count all possible distributions in any of these situations, or in a combination of these cases.

A general guideline for modelling a 'distribution problem' is that a distribution of distinct objects corresponds to an arrangement, and a distribution of identical objects corresponds to a selection. Let us consider examples of each of the four cases given above.

(a) There are twenty students and four colleges. In how many ways can the students be accommodated in the four colleges?

In this example the students, as well as the colleges, are clearly distinguishable. This comes under Case (1).

(b) Suppose we want to group 100 students into 10 groups of 10 each for the purpose of a medical examination. In how many ways can this be done?

Here the groups are indistinguishable, though the students in them are distinguishable. Hence, this falls under Case (2).

(c) An employer wants to distribute 100 one-rupee notes among 6 employees. What is the number of ways of doing this?

Though the one-rupee notes can be distinguished by their distinct numbers, we don't consider them to be distinguishable as far as their use is concerned. The employees, of course, are distinguishable. Hence, this is an example of Case (3).

(d) There are 1000 one-rupee notes. In how many ways can they be bundled into 20 bundles?

As before, the rupee notes are treated as indistinguishable. Clearly, the bundles are, by themselves, not distinguishable. Only the quantity in each may vary. Hence, this falls under Case (4).

Let us consider each case in some detail now.

4.3.1 Distinguishable Objects into Distinguishable Containers

Let us consider the example (A) above. Since any number of students can be put in a college, there are $20 \times 20 \times 20 \times 20$ possibilities, by the multiplication principle.

More generally, suppose we are distributing n objects into m containers, both being distinguishable. Then the total number of such distributions is n^m.

Let us look at an example.

Example 1: Show that the number of words of length n on an alphabet of m letters is m^n.

Solution: The m letters of the alphabet can be used any number of times in a word of n letters. The word can be considered as n ordered boxes, each holding a letter from the alphabet. The boxes become distinguishable because they are 'ordered'. The letters of the alphabet are clearly distinguishable. So, the number of ways of doing this is m^n.

* * *

Several people are confused while solving the problem above. They tend to take the m letters as the containers instead! Let's consider another example.

Example 2: Suppose we have a set S with n objects. An m-sample from this set S is an ordered arrangement of m letters taken from S, with replacement at every draw, in m draws. Find the number of m-samples from an n-element set.

Solution: Every m-sample is a word of length m from the 'alphabet' S containing n letters. Hence, the required number is n^m.

* * *

Now here are some exercises for you to solve.

E4) Find the number of three-letter words that can be formed using the letters of the English alphabet. How many of them end in x? How many of them have a vowel in the middle position?

E5) How many five-digit numbers are even? How many five-digit numbers are composed of only odd digits?

E6) There are 4 women and 5 men. A committee of three, a president, a vice-president, and a secretary, has to be formed from them. In how many ways can this be done if

i) the vice-president should be a woman?

ii) exactly one out of the vice-president and the secretary should be a woman?

iii) there is at least one woman in the committee?

Now suppose, we want to find the number of distributions of n distinguishable objects into m distinguishable containers, with **the extra condition** that no container should

contain more than one object. It is clear that this requires m ≥ n. Then we can get all these arrangements by first choosing n containers to contain exactly one object, and then permuting the n objects among the chosen containers. This can be done in C(m, n). n! = P(m, n) ways.
So, we have proved the following result.

Theorem 2: The number of ways of distributing n distinguishable objects into m distinguishable containers such that no container contains more than one object is P(m, n).

For example, the cardinality of the set of 5-digit numbers with all digits being distinct odd numbers is P (5,5). This is because the possible digits are 1, 3, 5, 7, 9.

Why don't you try an exercise now?

E7) Find the number of m-letter words with distinct letters, all taken from an alphabet with n letters, where n ≥ m. Is this different from the number of injective mappings from an m-element set into an n-element set, where n ≥ m? Give reasons for your answer.

Let us now consider the second type of distribution.

4.3.2 Distinguishable Objects into Indistinguishable Containers

Here we shall find the number of ways of distributing n distinguishable objects into m indistinguishable containers. For this, we first find the number when exactly k of the containers are occupied. This brings us to Stirling numbers of the second kind, named after James Stirling (1692-1770).

Suppose n ≥ m. The number of distributions of n distinguishable objects into m indistinguishable containers **such that no container is empty** is represented by $\mathbf{S_n^m}$. This number is called the Stirling number of the second kind. As you can see, this is also the number of partitions of a set of n objects into m classes.

Definition: For natural numbers n and m, the **Stirling number of the second kind**, S_n^m, is the number of partitions of an n-element set into exactly m parts.

Note that:

i) $S_n^m = 0$ if n < m, for, if the number of containers exceeds the number of objects, then it is impossible to have all the containers non-empty.

ii) $S_n^n = 1$, since there is only one way of putting n distinguishable objects in n indistinguishable boxes so that no box is empty.

iii) $S_n^1 = 1$.

Now, we shall use the inclusion exclusion principle to find the value of S_n^m.

Theorem 3: $S_n^m = \frac{1}{m!}\sum_{k=0}^{m}(-1)^k C(m, m-k)(m-k)^n$, $n \geq m$.

Proof: If the m classes are distinguishable, the number of partitions is the same as the number of functions from an n-element set onto an m-element set. As the classes are distinguishable here, we have to divide this number by m!. The result follows from Theorem 8, Unit 3.

For example, to obtain the Stirling number, S_5^3, we know that the number of functions from a 5-element set onto a three-element set is 150. So, by Theorem 3, $S_5^3 = 150/3! = 25$.

Remark: You may be wondering how we have jumped straightaway to the Stirling numbers of the second kind. What about the first kind? We won't be using them in any way here. However, for a the sake of completeness, we define **Stirling numbers of the first kind, s(n, k),** as follows.

For a positive integer n, and $0 \le k \le n$, s(n, k) is the coefficient of x^k in the expansion of the multinomial $x(x-1)(x-2)\ldots(x-n+1)$.

Getting back to S_n^m, you may feel that the formula in Theorem 3 is a little cumbersome. Sometimes, the following recurrence relation for S_n^m may be more useful.

Theorem 4: If $1 < m \le n$, then $S_{n+1}^m = S_n^{m-1} + mS_n^m$.

Proof: Let us take n+1 objects, mark one of them, and consider the distribution of these n+1 objects into m indistinguishable containers. Then we have 2 situations.

Case (1) (The marked object is placed in one container without any other objects.): In this case, the remaining n objects can be placed in (m – 1) containers in S_n^{m-1} ways.

Case (2) (The marked object is placed with at least one more object in a container.): In this case, we can first distribute the n unmarked objects into m containers, and then put the marked objects m to one of these m containers. So, the number of such partitions is mS_n^m.

Therefore, by the addition principle, we get $S_{n+1}^m = S_n^{m-1} + mS_n^m$.

There is a generalisation of Theorem 4 that is of independent interest, which we now state.

Theorem 5: $S_{n+1}^m = \sum_{k=0}^{n} C(n,k).S_k^{m-1}$

Proof: Let us mark one object in a set of (n+1) objects. Suppose the marked object is present in a box with (n – k + 1) elements, where $m - 1 \le k \le n$. Then we can choose n – k more objects to go with the marked object in C(n, n – k) ways. The remaining k objects can be distributed into $(m-1)^n$ boxes in S_k^{m-1} ways. So the number of ways of distributing the n – k objects is $C(n, n-k)\ S_k^{m-1}$. The result now follows from the addition principle by allowing k to vary from 0 to n.

Let us see some examples of the use of these recurrences.

Example 3: Calculate S_3^2 and S_4^2.

Solution: Using Theorem 4, we get $S_3^2 = S_2^1 + 2 \times S_2^2 = 1 + 2 \times 1 = 3$, and $S_4^2 = S_3^1 + 2S_3^2 = 1 + 2 \times 3 = 7$.

* * *

Now let us find what we had started with in this sub-section.

Theorem 6: The number of ways of distributing n distinguishable objects into m indistinguishable containers is $S_n^1 + S_n^2 + \ldots + S_n^m$, where n ≥ m. (Note that here we do not insist that no container is empty.)

Proof: When we distribute n distinguishable objects into m indistinguishable containers there are m cases. Case (k) is that exactly k containers are non-empty. Here k varies from 1 to m. The number of distributions in Case (k) is S_n^k. The result now follows from the addition principle.

Let us consider an example.

Example 4: In how many ways can 20 students be grouped into 3 groups?

Solution: Theorem 6 says that this can be done in $S_{20}^1 + S_{20}^2 + S_{20}^3$ ways.

Now, using Theorem 3, we get this number to be

$$1 + \frac{1}{2}\sum_{k=0}^{2}(-1)^k C(2,2-k)(2-k)^{20} + \frac{1}{6}\sum_{k=0}^{3}(-1)^k C(3,3-k)(3-k)^{20}$$

= 581,130,734.

* * *

Try some exercises now.

E8) Find the number of surjective functions from an n-element set onto an m-element set.

E9) Find the number of ways of placing n people in n – 1 rooms, no room being empty.

Let us now consider the third possibility for distributing objects into containers.

4.3.3 Indistinguishable Objects into Distinguishable Containers

Suppose there are n indistinguishable objects and m distinguishable containers. As the objects are indistinguishable, the distributions depend only on the number of objects in each container. As the containers are distinguishable, they can be assumed to be arranged in a line. Hence, the number of distributions is the number of ways of writing the number n as the sum $x_1+x_2+\ldots+x_m$, where the x_i's are non-negative integers.

We have covered this situation in Theorem 5 of Unit 2. Over there we have shown that **the number of distributions of n indistinguishable objects into m distinguishable containers is C (m+n–1, n)**. In particular, the number of non-negative integral solutions of the equation $x_1+x_2+\ldots+x_m = n$ is C (m+n–1, n).

Incidentally, we note that the number of distributions of n indistinguishable objects into m distinguishable containers **with at most one object per container** is C (m, n).

Let us consider an example.

Example 5: How many distinct solutions are there of x + y + z + w = 10

i) in non-negative integers?

ii) in positive integers?

Solution:

i) From the result quoted above, the answer is C(4 + 10 – 1, 10) = 286.

ii) We want x, y, z, w to be positive. Hence, we can write them respectively as X+1, Y+1, Z+1, W+1, where X, Y, Z, W are non-negative. Hence we want the number of non-negative solutions of the equation X+1+Y+1+Z+1+W+1=10, i.e., X+Y+Z+W= 6. The answer, now, is C (4 + 6 – 1, 6) = 84.
Try some exercises now.

E10) Show that the number of positive solutions of the equation $x_1+x_2+\ldots+ x_n = m$ is $C(m – 1, m – n)$.

E11) In how many ways can an employer distribute 100 one-rupee notes among 6 employees so that each gets at least one note?

Let us now consider the fourth case.

4.3.4 Indistinguishable Objects into Indistinguishable Containers

Suppose there are n indistinguishable objects and m indistinguishable containers. Any distribution is determined purely by an **unordered** m-tuple of non-negative integers with sum n. This is equivalent to the number of increasing sequences of length m of non-negative integers with sum n. But this is precisely the number of partitions of the integer n with at most m parts, viz., $P_n^1 + P_n^2 + ... + P_n^m = P_{n+m}^m$, from Theorem 1 of this unit.

Let us consider an example of this case.

Example 6: In how many ways can 20 identical books be placed in 4 identical boxes?

Solution: The answer is $P_{20}^1 + P_{20}^2 + P_{20}^3 + P_{20}^4 = P_{24}^4$

Why don't you try some exercises now?

E12) In how many ways can 1000 one-rupee notes be bundled into a maximum of 20 bundles?

E13) A car manufacture has 5 service centres in a city. 10 identical cars were served in these centres for a particular mechanical defect. In how many ways could the cars have been distributed at the various centres?

With this we have come to the end of this unit. Let us take a quick look at what we have studied in this unit.

4.4 SUMMARY

1. A partition of $n \in \mathbf{N}$ into k parts is $x_1+x_2+\ldots+x_k = n$, where $x_1 \le x_2 \le \ldots \le x_k$. P_n is the set of all partitions of n, and P_n^k is the set of all partitions into exactly k parts.

2. The proof and applications of the recurrence relation,
$P_n^1 + P_n^2 + ... + P_n^k = P_{n+k}^k, P_n^1 = P_n^n = 1, 1 \le k \le n.$

3. The number of ways of distributing n objects into m containers is :

i) n^m, if the objects and containers are distinguishable.

ii) $\sum_{i=1}^{m} S_n^i$, if the objects are distinguishable but the containers are not.

(Here S_j^i is a Stirling number of the second kind).

iii) C(m+n−1, n) if the objects are not distinguishable but the containers are distinguishable.

iv) P_{n+m}^m, if neither the objects nor the containers are distinguishable.

Further, in (i) above, if there is an extra requirement that each container contain at most one object, then the number of distributions is P(m, n). Again, in (iii) above, with the same extra requirement, the number of distributions is C(m, n).

4.5 SOLUTIONS /ANSWERS

E1) In the table below we give all possible partitions of 7.

Table 2

Number of parts	Partitions
1	7
2	1+6, 2+5, 3+4
3	1+1+5, 1+2+4, 1+3+3, 2+2+3
4	1+1+1+4, 1+1+2+3, 1+2+2+2
5	1+1+1+1+3, 1+1+1+2+2
6	1+1+1+1+1+2
7	1+1+1+1+1+1+1

From the table, we see that $P_7^4 = 3,\ P_7^5 = 2.$

E2) The required number is $P_{10}^5 = 7.$

E3) $P_7^1 = 1 = P_7^7.$

$P_7^2 = P_5^1 + P_5^2 = 1 + 2 = 3$, from Table 1.

$P_7^3 = P_4^1 + P_4^2 + P_4^3 = 1 + 2 + 1 = 4$, from Table 1.

Similarly, $P_7^4 = P_3^1 + P_3^2 + P_3^3 + P_3^4 = 3,\ P_7^5 = P_2^1 + P_2^2 = 2$ and $P_7^6 = P_1^1 = 1.$

E4) The 26 letters are distinguishable objects. We have to fill then in three distinguishable containers, viz., the first, second, and third positions of a three-lettered word. The solution is 26^3.

If the last letter is to be x, the number is only $26^2 \times 1$.

If the middle letter is a vowel, then by the multiplication principle, the answer is $26 \times 5 \times 26$.

E5) The total number of even numbers is $9 \times 10 \times 10 \times 10 \times 5 = 45{,}000$, since the last digit can only by 0, 2, 4, 6 or 8.

The number of 5-digit numbers composed of only odd digits (i.e., 1, 3, 5, 7, 9) is clearly $5^5 = 3125$.

E6) i) We can choose a woman for vice-president in 4 ways. To fill the remaining 2 positions we can select 2 from the remaining 8 persons in $8 \times 7 = 56$ ways. Hence, the required number is $4 \times 56 = 224$.

ii) If the vice-president is a woman (chosen in 4 ways), others can be selected in $5 \times 4 = 20$ ways. Similarly, if the woman is a secretary, the others can be chosen in 20 ways. Hence, by the addition and multiplication principles, the answer is $20 \times 4 + 20 \times 4 = 160$.

iii) Without any restriction, three can be selected in $9 \times 8 \times 7 = 504$ ways. If no woman is to be selected, then it can be done in $5 \times 4 \times 3 = 60$ ways. What we need is the complement of this. Thus, the required answer is $504 - 60 = 444$.

E7) If the alphabet has n letters, the m-letter words with distinct letters can be formed in $n\,(n-1)(n-2)\ldots(n-m+1) = P(n, m)$ ways.

Now, in an injective mapping, images of distinct elements should be distinct (see Unit 1). There are n possible images for the first element of the m-set, n–1 possible images for the second, and so on. Hence, the number of such mappings is also P(n, m).

E8) Suppose $N = \{1, 2, \ldots, n\}$ and $M = \{1, 2, \ldots, m\}$. If f is an onto function from N to M, then the inverse images, $f^{-1}(1), f^{-1}(2), \ldots, f^{-1}(k)$ constitute a partition of N into m classes. The number of ways in which this can be done is S_n^m, where the order of partition is immaterial. But, in functions, the order cannot be ignored. So, the distribution can be done in $m!.S_n^m$ ways.

E9) This is S_n^{n-1}. This can be done by putting one person each in n – 2 rooms and 2 persons in 1 room. This can be done in C(n, 2) ways. So $S_n^{n-1} = C(n,2)$.

E10) If a positive solution is $x_1, x_2, \ldots, x_n$, then it can be written as $X_1+1, X_2+1, \ldots, X_n + 1$, where the X_i's are non-negative. Thus, the required number is the number of non-negative solutions of $X_1+X_2+\ldots+X_n+n = m$, which is $C(n + m – n – 1, m – n) = C(m – 1, m – n)$.

E11) This is the number of positive solutions of $x_1+\ldots+x_6 = 100$.
So, the required number is $C(100 – 1, 100 – 6) = C(99, 94) = 71{,}523{,}144$.

E12) $P_{1000}^1 + P_{1000}^{20} + P_{1020}^{20}$.

Had the requirement been that there be exactly 20 bundles, then the number would have been P_{1000}^{20}.

E13) $P_{10}^1 + P_{10}^2 + P_{10}^3 + P_{10}^4 + P_{10}^5 = P_{15}^5$.

SOCIAS-IGNOU/P.O.10.5T/MAY, 2004