COURSE GUIDE

CIT 206

DISCRETE STRUCTURES

Course Team

Theophilus Aniemeka Enem, PhD (Course Writer) –

Air Force Institute of Technology

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
University Village
Plot 91, Cadastral Zone Nnamdi Azikiwe Expressway
Jabi, Abuja

Lagos Office
14/16 Ahmadu Bello Way
Victoria Island, Lagos

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Printed 2022
ISBN: 978-058-851-5

CONTENTS **PAGE**

INTRODUCTION

The course, Discrete Structures, is a 3- credit unit course for students studying towards acquiring the Bachelor of Science in Computer Science. In this course we will study about discrete objects and the relationship between them and introduce the applications of discrete mathematics in the field of Computer Science. This course also covers sets, logic, proving techniques, combinatorics, functions, relations, graph theory and Boolean algebra.

The overall aims of this course are to introduce you to basic concepts of sets, logic, functions, matrices and graph theory.

In structuring this course, we commence with the introduction to discrete structures and move to the Boolean algebra and lattices.

What You Will Learn in This Course

The overall aims and objectives of this course is to provide guidance on what you should be achieving in the course of your studies. Each unit also has its own unit objectives which state specifically what you should be achieving in the corresponding unit. To evaluate you progress continuously, you are expected to refer to the overall course aims and objectives as well as the corresponding unit objectives upon completion of each.

Course Aims

The overall aims and objectives of this course will help you to:

1. Develop your knowledge and understanding of the basic concepts of sets
2. Build your capacity to evaluate logic and induction techniques
3. Develop your competence in sets operations
4. Build up your knowledge on graph to design complex network connections

Course Objectives

Upon completion of the course, you should be able to:

1. Prove basic set equalities;
2. Write an argument using logical notation and determine if the argument is valid or not;
3. Demonstrate the ability to write and evaluate a proof using mathematical induction;
4. Demonstrate an understanding of relations and functions and be able to determine their properties;
5. Recognize the use of Karnaugh map to construct and minimize the canonical sum of products of Boolean expressions and transform it into an equivalent Boolean expression;
6. Demonstrate different traversal methods for trees and graphs;
7. Discriminate between a Eulerian graph from a Hamiltonian graph for use in solving mathematical problems;
8. Model problems in Computer Science using graphs and trees;
9. Apply counting principles to determine probabilities.

Working through This Course

In order to have a thorough understanding of the course units, you will need to read and understand the contents, practice the steps and techniques involved. This course is designed to cover approximately thirteen weeks, and requires your devoted attention, answering the exercises in the tutor-marked assignments and gets them submitted to your tutors.

Course Materials

These include:

1. Course Guide
2. Study Units
3. Recommended Texts
4. A file for your assignments and for records to monitor your progress.

Study Units

There are three (3) Modules and eight (8) Units in this course:

Module 1: Introduction to Discrete Structures

Unit 1: Set Theory
Unit 2: Proofs and Induction
Unit 3: Logic

Module 2: Boolean Algebra and Graph Theory

Unit 1: Boolean Algebra and Lattices
Unit 2: Graph Theory

Module 3: Matrices, Applications to Counting and Discrete Probability

Unit 1: Matrices
Unit 2: Applications to Counting
Unit 3: Discrete Probability Generating Function

From the preceding, the content of the course can be divided into three major blocks:

1. Introduction to Discrete Structures
2. Boolean Algebra and Graph Theory
3. Matrices, Applications to Counting and Discrete Probability

Module one describes the Set Theory, a mathematical theory that underlies all of modern mathematics
Module two explain in details the Boolean algebra and graph theory
Module three discusses matrices, application to counting and discrete probability

Textbooks and References

- THEORY AND PROBLEMS OF DISCRETE MATHEMATICS- Seymour Lipschutz., 3rd Edition, Marc Lars Lipson. Schaum's Outline Series, McGraw-Hill. DOI: 10.1036/0071470387
- DISCRETE MATHEMATICS – An Open Introduction 3rd Edition, Oscar Levin, 2019. ISBN: 978-1792901690
- DISCRETE MATHEMATICS AND ITS APPLICATION, Kenneth H. Rosen, Tata McGraw-Hill Editions, 2003
- INTRODUCTION TO GRAPH THEORY – Richard J. Trudean, Dover publisher, Inc New York, 2013. ISBN: 13: 978-0-486-67870-2
- A TEXT BOOK OF GRAPH THEORY – Balakrishnan, R and Ranganathan, K, 2012. Department of Mathematics, University of Tiruchirappalli India. ISBN: 2191-6675 (electronic)
- PURE MATHEMATICS FOR ADVANCED LEVEL - Bunday, BD and Mulholland, H. (2014). Second edition. Published by Elsevier science. ISBN: 1483106136, 9781483106137
- DISCRETE STRUCTURES, LOGIC AND COMPUTABILITY. James, H. (2017). Published by Jones and Bartlett. Fourth Edition. ISBN:978-284-07040-8.
- A COURSE IN DISCRETE STRUCTURES - Pass, R., & Tseng, W. L. D (2019). Wei-Lung Dustin Tseng, Site Internet: www.freechbooks.com(2019)
- DISCRETE MATHEMATICS FOR COMPUTER SCIENCE - Haggard, G., Schlipf J., Whitesides, S., (2006). Thomson Brooks/Cole.

Presentation Schedule

The Presentation Schedule included in your course materials gives you the important dates for the completion of Tutor-Marked assignments and attending tutorials. Remember, you are required to submit all your assignments by the due date. You should guard against lagging behind in your work.

Assessment

There are two types of assessment for this course. The first one is the tutor-marked assignment and the second is a written examination. In tackling the assignments, you are expected to apply information and knowledge acquired during this course. The tutor-marked assignments must be submitted to your tutor, for formal assessment in accordance with the deadlines stated in the assignment file.

The work you submit to your tutor for assessment will count for 30% of your total course mark. At the end of the course, you will need to sit for a final three-hour examination. This also accounts for 70% of your total course mark.

Course Marking Scheme

This table shows how the actual course marking is broken down:

Assessment	**Marks**
Assignment 1-4	Four assignments, best three marks of the four count at 30% of course marks
Final Examination	70% of overall course marks
Total	100% of course marks

How to get the Most from the Course

In distance learning, the study units replace the university lecturer. This is one of the great advantages of distance learning; you can read and work through specially designed study materials, at your own pace, and at a time and place that suit you best. Think of it as reading the lecture instead of listening to a lecturer. In the same way that a lecturer might set you some reading to do, the study units tell you when to read your set books or other material. Just as a lecturer might give you an in-class exercise, your study units provides exercises for you to do at appropriate points.

Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit, and how a particular unit is integrated with the other units and the course as a whole. Next is a set of learning objectives. These objectives enable you know what you should be able to do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the units, you must go back and check whether you have achieved the objectives, in order to significantly improve your chances of passing the course.

Remember that your tutor's job is to assist you. When you need help, don't hesitate to call and ask your tutor to provide it.

1. Read this course guide thoroughly.
2. Organise a study schedule. Refer to the "course overview" for more details. Note the time you are expected to spend on each unit and how the assignments relate to the units. Whatever method you choose to use, you should decide on it and write in your own date, for working on each unit.
3. Once you have created your own study schedule, do everything you can, to stick to it. The major reason that students fail is that, they lag behind in their course work.
4. Turn to unit 1 and read the introduction and objectives for the unit.
5. Assemble the study materials. Information about what you need for a unit is given in the "overview" at the beginning of each unit. You will almost always need both the study unit you are working on and one of your set of books on your desk at the same time.
6. Work through the unit. The content of the unit itself has been arranged, to provide a sequence for you to follow. As you work through the unit, you will be instructed to read sections from your set of books or other articles. Use the unit to guide your reading.
7. Review the objectives for each study unit to confirm that you have achieved them. If you are not sure about any of the objectives, review the study material or consult your tutor.
8. When you are confident that you have achieved a unit's objectives, you can then start on the next unit. Proceed unit by unit through the course and try to pace your study, so that you can keep yourself on schedule.
9. When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to schedule. When the assignment is returned, pay particular attention to your tutor's comments, both on the tutor-marked assignment form and also on the assignment. Consult your tutor as soon as possible, if you have any question or problem.
10. After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this course guide).

Facilitation

There are 12 hours of tutorials provided in support of this course. You will be notified of dates, times and locations of these tutorials, together with the name and phone number of your tutor, as soon as you are allocated a tutorial group.

Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulty you might encounter, and provide assistance to you during the course. You must mail or submit your tutor-marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible.

Do not hesitate to contact your tutor by telephone, or e-mail if you need help. The following might be circumstances in which you would find help necessary. Contact your tutor if:

- you do not understand any part of the study units or assigned reading
- you have difficulty with the self-test or exercises
- you have a question or problem with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

You should try your best to attend the tutorials. This is the only chance to have face to face contact with your tutor and ask questions, which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefit from course tutorials, prepare a question list before attending them. You will learn a lot from participating in discussions actively.

Summary

The course, Discrete Structures is intended to get student acquainted with the basic principles of sets and operations in sets and to enable them prove basic set equalities. This course also provides you with knowledge on how to write an argument using logical notation and determine if the argument is valid or not.

We hope that you will find the course enlightening and that you will find it both interesting and useful. In the longer term, we hope you will get acquainted with the National Open University of Nigeria and we wish you every success in your future

CONTENTS **PAGE**

MODULE 1 INTRODUCTION TO DISCRETE STRUCTURES

UNIT 1: SET THEORY

CONTENTS

1.0 Introduction

This unit describes Set Theory, a mathematical theory that underlies all of modern mathematics. The best way to understand mathematics is to talk and write about mathematics. Mathematics is not all about finding solutions to given tasks. Therefore, as we tackle a more advanced and abstract mathematics in this unit, your basic understanding of it will be helped by how well you can read, write and talk about mathematical statements.

2.0 Objectives

By the end of this Unit, you will be able to:

- explain basic properties of sets and operations of sets
- work with sets precisely define the number of elements of a finite set
- discuss the essentials of mathematics
- describe what a declarative statement is.

3.0 Main Content

3.1 Introduction to Mathematical Statements

We will take a few examples of mathematical statements to illustrate what a proper communication in mathematics is all about.

3.1.1 Statement Definitions

A declarative sentence which is either true or false is called a **statement**. A statement is said to be an **Atomic Statement** if it cannot be divided into smaller statements, otherwise it is called a **Molecular Statement**.

Example 3.1.1.1

These statements are examples of atomic statements:

- Mobile numbers in Nigeria have 11 digits.
- 5 is larger than 7.
- 12 is a perfect square.
- Every even number greater than 2 can be expressed as the sum of two primes.

However, these are not statements:

- Would you like some ice cream?
- The product of two numbers.
- $1 + 3 + 5 + 7 + \cdot \cdot \cdot + 2n + 1$.
- Go to the lecture room!
- $4 + x = 12$

The sentence "$4 + x = 12$" is not a statement because it contains an unknown variable, x. Depending on the value of x, the sentence is either true or false, however, right now it is neither true nor false. We can also build a **complicated (molecular) sentence** by combining more than one or more simple atomic or molecular sentences by using **Logical Connectives**. An example of a molecular stamen is:

Mobile numbers in Nigeria have 11 digits **and** 5 is larger than 7.

This example of a molecular statement can also be broken down into smaller statements which were only connected by an "and". Obviously, molecular statements are still statements, therefore, they must be either true or false. The five connectives we can consider are "and", "or", "if… then", "if and only if", and "not.

"and" - I am a boy **and** my sister is a girl.

"or" - Delight is a boy **or** a girl.

"if… then" - **If** you register **then** you can write the exam.

"if and only if"- You can register **if and only if** you were admitted.

"not - You are **not** admitted.

The connectives, "and", "or", "if… then", "if and only if", connects two statements and are called binary connectives while the connective "not" applies to only a single sentence and is called a unary connective.

In order to determine the truth values of molecular statements, the key observation to make is to completely determined the truth values of the parts and the type of connective(s). We do not necessarily need to know what the individual parts actually say, we however, only need to know whether those parts are true or false. Therefore, in order to analyse logical connectives, we use **propositional variables** (also called **sentential** variables) which are the letters found in the middle of the English alphabet represented in capital: P, Q, R, S, … to represent each atomic statements in the molecular statement. These variables can only have two values, true or false. The logical connectives: "and", "or", "if… then", "if and only if", and "not" can be represented by these symbols $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, and $\neg$ respectively.

3.1.2 Logical Connectives

- $P \wedge Q$ is read as "P and Q," and it is called a **conjunction**.
- $P \vee Q$ is read as "P or Q," and it is called a **disjunction**.
- $P \rightarrow Q$ is read as "if P then Q," and it is called an **implication** or **conditional**.
- $P \leftrightarrow Q$ is read as "P if and only if Q," and it is called a **bi-conditional**.
- $\neg P$ is read as "not P," and it is called a **negation**.

The truth value of a statement is determined by the truth value(s) of its part(s), depending on the connectives:

Truth Conditions for Connectives.

• $P \wedge Q$ is true when both P and Q are true

• $P \vee Q$ is true when P or Q or both are true.

• $P \rightarrow Q$ is true when P is false or Q is true or both.

• $P \leftrightarrow Q$ is true when P and Q are both true, or both false.

• $\neg P$ is true when P is false and vice versa.

3.2 Sets

Sets are the most fundamental objects in all of mathematics.

3.2.1 Definition of Set: An informal definition of set is that a set is an unordered collections of objects. The objects that comprises of the set are called ***elements.*** The number of objects in a set can be finite or infinite.

3.2.2 Notations

A single set, ***A*** can be expressed with the following notations:

$A = \{1, 2\}$; $A = \{2, 1\}$; $A = \{1, 2, 1, 2\}$; $A = \{x \mid x \text{ is an integer}, 1 \leq x \leq 2\}$

The notation, $A = \{1, 2\}$ is read as, "***A*** is the set containing the elements 1 and 2."

The curly braces "{ }" is used to enclose the elements of a set and the comma "," is used to separate the elements inside the braces.

The symbol "|" (or ":" or "϶"), implies "such that". Therefore, the notation, $\{x \mid x \text{ is an integer}, 1 \leq x \leq 2\}$ is read as "the set of all x such that x is an integer between 1 and 2 (1 and 2 inclusive)".

Considering the notation:

$5 \in \{1, 2, 5\}$

The symbol "∈" implies "is in" or "is an element of." Therefore, the notation is read as 5 is an element of a set containing 1,2, and 5. This is a true statement. We can also write another true statement if we say that 3 "is not" an element of the set containing 1,2, and 5. This can be written as:

$3 \notin \{1, 2, 5\}$

Some other notations

⊆: $A \subseteq B$ asserts that A is a **subset** of B | every element of A is also an element of B.

If A is {2, 3, 4}, B is {2, 3, 4, 5}. Then $A \subseteq B$.

If A is {2, 3, 4}, B is {2, 3, 4}. Then $A \subseteq B$ and $B \subseteq A$.

If A is {2, 3, 4, 5}, B is {2, 3, 4, 6, 7}. Then B $\nsubseteq$ A.

$\subset$: A $\subset$ B asserts that A is a **proper subset** of B | every element of A is also an element of B, but every element of B is not an element of A.

Let A = {2, 3, 4} and B = {1, 2, 3, 4, 5}. Then, A $\subset$ B.

If A is {2, 3, 4}, B is {2, 3, 4}. Then A $\not\subset$ B (read as A is a **NOT** a proper subset of B).

U: A fixed set which contains all other sets under investigation is called **universal set.** In other words, all other sets under investigation are subsets of the universal set and it is denoted by **U**.

Example: Considering human population, the universal set consist of all people in the world.

3.2.3 Operations on Sets

$\cup$: A $\cup$ B is the **union** of A and B: is the set containing all elements which are elements of A or B or both.

If A is {1, 2, 4, 5}, B is {2, 3, 4}. Then A $\cup$ B = {1, 2, 3, 4, 5}

$\cap$: A $\cap$ B is the **intersection** of A and B: the set containing all elements which are elements of both A and B.

If A is {1, 2, 4, 5}, B is {2, 3, 4}. Then A $\cap$ B = {2, 4}

\: A \ B is A **minus** B: the set containing all elements of A which are not elements of B.

Let A = {1, 2, 4, 5, 6}, B = {2, 3, 4}. Then A \ B = {1, 5, 6}.

A^c or $\overline{A}$: The **complement** of A is the set of everything which is not an element of A.

Let the universal set, **U** be {1, 2, . . . , 9, 10}, A = {2, 3, 4}. Then A^c = {1, 5, 6, …, 9, 10}.

|A|: The **cardinality** (or size) of A is the number of elements in A.

|{1, 2, 3}| = |{a, b, c}| = |{1,{1, 2}, 5}| = |{1, 2, ∅}| = 3.

×: $A \times B$ is the **Cartesian product** of two non-empty sets A and B: the set of all ordered pairs (a, b) with $a \in A$ and $b \in B$.

Let A be a set. $A \times A$ is the set of ordered pairs (x, y) where $x, y \in A$.

The expression $A \times A \times \cdot \cdot \cdot \times A$ (n times) can also be denoted as A^n which is the set of all ordered subsets (with repetitions) of A of size n.

Examples

i. $\{0, 1\}^n$ the set of all "strings" of 0 and 1 of length n.

ii. Let A = {1, 2}, B = {3, 4, 5}. Then $A \times B$ = {(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)}.

Example 3.2.3.1

Prove that $A \times B = B \times A$, only if A = B.

Solution 3.2.3.1

Proof: Let $A \times B = B \times A$. then, $A \subseteq B$ and $B \subseteq A$. Therefore, A = B.

3.2.4 Rules of Set Theory

Let P, Q and R be sets.

i. **Commutative Law**: $(P \cup Q) = (Q \cup P)$ and $(P \cap Q) = (Q \cap P)$.

ii. **Associative Law**: $(P \cup (Q \cup R)) = ((P \cup Q) \cup R)$ and $(P \cap (Q \cap R)) = ((P \cap Q) \cap R)$.

iii. **Distributive Law**: $(P \cup (Q \cap R)) = (P \cup Q) \cap (P \cup R)$ and $(P \cap (Q \cup R)) = (P \cap Q) \cup (P \cap R)$.

iv. **De Morgan's Law**: $(P \cup Q)^C = (P^c \cap Q^c)$ and $(P \cap Q)^C = (P^c \cup Q^c)$

Some special sets we will consider in this unit:

- ∅ The empty set that contains no element (also denoted as { }).
- **U** The universe set is the set of all elements
- $\mathbb{N}$ {0, 1, 2, 3, . . . }, the non-negative integers
- $\mathbb{N}^+$ {1, 2, 3, . . . }, the positive integers
- $\mathbb{Z}$ {. . . −2, −1, 0, 1, 2 . . . }, the integers
- $\mathbb{Q}$ {q | q = a/b, a, b ∈ $\mathbb{Z}$, b 6= 0}, the rational numbers
- $\mathbb{Q}$+ {q | q ∈ Q, q > 0}, the positive rational
- $\mathbb{R}$ The real numbers

- $\mathbb{R}^+$ The positive reals
- $\mathcal{P}$(A) The power set of any set A is the set of all subsets of A.

3.2.5 Disjoint Set

Sets X and Y are said to be disjoint sets, if they have no element in common, that is, no element of X is in Y and no element of Y is in X.

Example 3.2.5.1:

i. Given $X = \{1,2,3\}$ and $Y = \{4,5,6\}$, then X and Y are disjoint sets.

ii. If $P = \{a, b, c, d\}$ and $Q = \{d, e, f, g\}$, then P and Q are not disjoint sets, since d is in both sets.

3.2.6 Power Set

We call the set of all subsets of A, the power set of A, and write it as $\mathcal{P}$(A)

Example 3.2.6.1 Let A = {1, 2, 3}. Find $\mathcal{P}$(A).

Solution 3.2.6.1 $\mathcal{P}$(A) is a set of sets, all of which are subsets of A.

So, $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

Note: The power set of a set A is normally, 2^n, where n is the cardinality of the set A. Therefore, since |A| = 3, the cardinality of the power set of A, $|\mathcal{P}(A)| = 2^3 = 8$.

Note: Although 2 ∈ A, it will be wrong to say that 2 ∈ $\mathcal{P}$(A) because none of the elements in $\mathcal{P}$(A) are numbers. However, we can say that {2} ∈ $\mathcal{P}$(A) because {2} ⊆ A.

We can relate the symbols of union and intersect to resemble the logic symbols of “or” and “and”. Remember that the statement x ∈ A ∪ B is read as x is an element of A or x is an element of B. Therefore,

$x \in A \cup B \leftrightarrow x \in A \vee x \in B$.

Similarly,

$x \in A \cap B \leftrightarrow x \in A \wedge x \in B$.

Also,

$x \notin A \leftrightarrow \neg(x \in A)$

Example 3.2.6.2

Let A = {2, 4, 6}, B = {1, 2, 3, 4, 5, 6}, C = {1, 2, 3}, D = {1, 3, {4, 5}, x}, and E = {7, 8, 9}.

Determine each statement to be either true, false, or meaningless.

1. $A \subset B$. 2. $B \subset A$. 3. $A \in C$. 4. $\emptyset \in B$. 5. $\emptyset \subset A$.

6. $A < E$. 7. $3 \in C$. 8. $x \subset D$. 9. $\{9\} \subset E$.

Solution 3.2.6.2

1. True. Every element in A is an element in B.
2. False. For example, $1 \in B$ but $1 \notin A$.
3. False. The elements in C are 1, 2, and 3. The set A is not equal to 1, 2, or 3.
4. False. The set B has exactly 6 elements, and none of them is an empty set.
5. True. Everything in the empty set (nothing) is also an element of A. Notice that the empty set is a subset of every set.
6. Meaningless. A set cannot be less than another set.
7. True. 3 is one of the elements of the set C.
8. Meaningless. x is not a set, so it cannot be a subset of another set.
9. True. 9 is the only element of the set {9}, and is an element of E, so every element in {9} is an element of E.

3.2.7 Venn Diagrams

A Venn Diagram is a great tool used to visualize and represent operations on sets. It is used to display sets as intersecting circles. We can highlight a region under consideration when we carry out an operation. The cardinality of a set can be represented by putting numbers in the corresponding area.

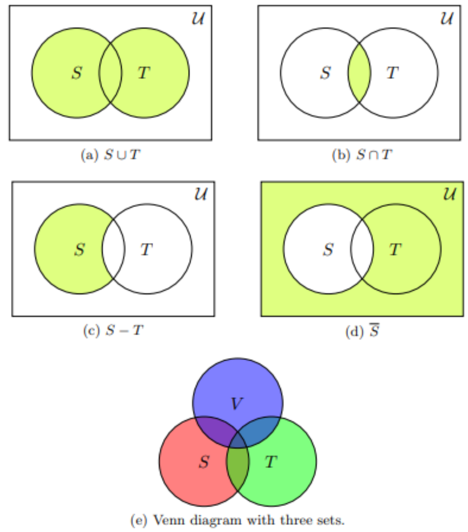


Figure 1.1: Venn diagrams of sets S, T, and V under universe $\mathcal{U}$.

3.3 Relations

3.3.1 Definition 3.3.1: A relation on a single set S is a subset of S × S. A relation on sets S and T is a subset of S × T. Now, let's consider relationships among sets. For example, we can say that X is married to Y and they both have a child, Z. In our daily lives, we deal a lot with talks about relationships. For example, if we consider two human beings (A, B), "taller-than", "smarter-than" are relations between them. That is (A, B) ∈ "taller-than" if person A is taller than person B. "≥" is a relation on R; "≥" = {(x, y) | x, y ∈ R, x ≥ y}.

3.3.2 Definition: A relation R on a set S is:

i. **Reflexive** if for all x ∈ S, (x, x) ∈ R.

ii. **Symmetric** if for all x, y ∈ S, whenever (x, y) ∈ R, (y, x) ∈ R.

iii. **Transitive** if for all x, y, z ∈ S, whenever (x, y) ∈ R and (y, z) ∈ R, then (x, z) ∈ R.

Example 3.3.1.1

i. "≤" is reflexive, but "<" is not.

ii. "sibling-of" is symmetric, but "≤" and "sister-of" is not.

iii. "sibling-of", "≤", and "<" are all transitive, but "parent-of" is not (however, "ancestor-of" is transitive).

A relation that is reflexive, symmetric and transitive is called an **Equivalence** relation and is denoted by the symbol "≡".

Let "≡" be an equivalence relation on the set S. An equivalence class is a maximal subset E of the set S such that any two elements in the set E is related. There can be multiple equivalence class corresponding to the relation ≡.

4.0 Conclusion

The bulk of work in this unit is on how set theory (a branch of mathematical logic gives insight into how Discrete Structure are viable in Computer Science. Emphasis were made on a set being a collection of objects or groups of objects. The unit further highlighted on the rules of set theory and its power set.

5.0 Summary

In this unit we learnt that Sets are the most fundamental objects in all of mathematics. That, a set is a collection of objects or groups of objects. A statement can be an Atomic Statement if it cannot be divided into smaller statements, otherwise it is called a Molecular Statement. There are rules governing the set and Venn diagram is a great tool used to visualize and represent operations on sets.

6.0 Tutor-Marked Assignments

1. Describe each of the following sets both in words and by listing out enough elements to see the pattern.
   a. $\{x : x + 2 \in \mathbb{N}\}$.
   b. $\{x : x + 2 \in \mathbb{N}^+\}$.
   c. $\{x \in \mathbb{N} : x + 2 \in \mathbb{N}\}$.
   d. $\{x : x \in \mathbb{N} \vee -x \in \mathbb{N}\}$.
   e. $\{x : x \in \mathbb{N} \wedge -x \in \mathbb{N}\}$.
2. Let A = {7, 1, 2, 3, 6}, B = {2, 3, 4}, C = {1, 6, 7} and D = {5, 8, 4, 9} be subsets of **U** = $\{n \in \mathbb{N} : 1 \leq n \leq 10\}$.
   a. Find the following;
   i. $A \cup C$ ii. $(A \cap D^c) \cup (A \cap B)^c$ iii. $\emptyset \cup B$ iv. $(A \cup B)^c$
   b. Represent the sets in 2a above by the use of a Venn Diagram.

3. Using a Venn Diagram, determine if the representation $A \cap \bar{B}$ is equivalent to $A \setminus B$.
4. Using the sets W = {2, a, {u, v, w}, ∅}, X = {∅, a}, Y = {1, 2, 4} and Z = {2, 4, 8}. Determine if the following statements are true, false or meaningless. State your reasons for each.

   i. $w \in A$ ii. $B \in A$ iii. $D > C$ iv. $\{2, a\} \in A$

5. Find the cardinality of each set below (show cardinality check):

   i. A = {23, 24, . . . , 37, 38}

   ii. B = {1, {2, 3, 4}, 5, ∅}

   iii. $\mathcal{P}(K \cap L) \ni K = \{n \in \mathbb{N} : n \leq 19\}$ and $L = \{ n \in \mathbb{N} : n \text{ is prime}\}$

   iv. $\mathcal{P}(C) \ni C = \{a, b, c, d\}$

6. Let A = {1, 2, 3}, B = {4, 5, 6, 7}. Find $B \times A$.
7. If $|A| = 5$ and $|B| = 8$ and $|A \cup B| = 11$ what is the size of $A \cap B$?
8. If $|A^c \cap B| = 10$ and $|A \cap B^c| = 8$ and $|A \cap B| = 5$ then how many elements are there is $A \cup B$?

7.0 References/Further Reading

Bunday, BD and Mulholland, H. (2014). Pure Mathematics for Advanced Level. Second edition. Published by Elsevier science. ISBN: 1483106136, 9781483106137

James, H. (2017). Discrete Structures, Logic and Computability. Published by Jones and Bartlett. Fourth Edition. ISBN:978-284-07040-8.

Seymour, L. S. (1964). Outline Series: Theory and Problems of Set Theory and Related Topics, pp. 1-133.

Stroud, KA. (2013) Engineering Mathematics. 7th edition. www.pdffiller.com/448950026--ENGINEERING-MATHEMATICS-7TH-EDITION-by-KA-Stroud.

UNIT 2 PROOFS AND INDUCTION

CONTENTS

1.0 Introduction

Mathematical Induction is an elegant and powerful technique that is used to prove certain types of mathematical statements and propositions which assert that for all positive integers something is true or that for all positive integers from some point on. There are many forms of mathematical proofs. In this unit, we will introduce several basic types of proofs, with special emphasis on a technique called induction that is invaluable to the study of discrete mathematics.

2.0 Objectives

By the end of this unit, you will be able to:

- explain the basic types of proofs
- prove certain mathematical statement
- mention types of induction techniques.

3.0 Main Content

3.1 Basic Proof Techniques

Proof techniques can either be direct, indirect or by induction. The choice of a proof technique depends on the problem or task at hand. Therefore, it is important to realize that there is no single method applicable to solving all tasks. This implies that your level of ingenuity, skills and implementation of common sense must be applied to every task. In this Unit, we will discuss the direct, proof by induction and indirect proofs (proof by contrapositive and proof by contradiction).

3.2 Direct Proof (Proof by Construction)

In order to prove a mathematical statement, we have to show that for a given premise, the conclusion given can be derived. Considering any given task: such that we are given a premise X, how do we show that a conclusion Y holds? One way to achieve this is by giving a Direct Proof. In this form of proof, we start with a premise X, and directly deduce the conclusion Y through a series of logical steps.

The two steps to directly prove that $X \rightarrow Y$ is true.

a. Demonstrate that Y must follow from X.

Example 3.2.1. Let n be an integer. If n is even, then n^2 is even. If n is odd, then n^2 is odd.

Solution 3.2.1

Using **direct proof**: For an integer k;

If n is even, then $n = 2k$, and

$$n^2 = (2k)^2 = 4k^2 = 2\,(2k^2), \text{ which is even.}$$

If n is odd, then $n = 2k + 1$, and

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2\,(2k^2 + 2k) + 1, \text{ which is odd.}$$

3.3 Proof by Induction

The initial step

Firstly, prove that the proposition is true for $n = 1$. If the claim is that the proposition is true for $n \geq a$, first prove it for $n = a$.

Inductive step

Prove that if the proposition is true for n = k, then it must also be true for n = k + 1. This is the difficult step and we will break it down into steps.

Step 1: Here we perform **Inductive Hypothesis** by writing down what the proposition asserts for the case n = k.

Step 2: Now, write down what the proposition asserts for the case n = k + 1. Clearly remember that this is what you have to prove.

Step 3: By using the assumption made in Step 1, try and prove the statement in Step 2. Have in mind that this stage varies from problem to problem depending on the mathematical contents, therefore, there is no single way to solve all problems. The main aim here is to apply your skills and determine how you get from Step1 to Step2.

After the initial and inductive steps have been successfully performed, we then conclude immediately that the proposition is true for all $n \geq 1$.

Example 3.3.1. The sum of the first n positive integers is $\frac{1}{2}n(n + 1)$.

Initial step: If n = 1, the sum is simply 1.

Now, for n = 1, $\frac{1}{2}n\ (n + 1) = \frac{1}{2} \times 1 \times 2 = 1$. So, the result is true for n = 1.

Inductive step:

Stage 1: Our assumption (the inductive hypothesis) asserts that

$$1+2+3+ \cdots + k = \frac{1}{2}k(k + 1).$$

Stage 2: We want to prove that

$$1+2+3+ \cdots + (k + 1) = \frac{1}{2}(k + 1)[(k + 1) + 1] = \frac{1}{2}(k + 1)(k + 2).$$

Stage 3: How can we get to stage 2 from stage 1?

The answer here is that we get the left-hand side of stage 2 from the left-hand side of stage 1 by adding (k + 1). So, $1+2+3+ \cdots + (k + 1) = 1 + 2 + 3 + \cdots + k + (k + 1)$

$= \frac{1}{2}$ k(k + 1) + (k + 1) *using the inductive hypothesis*

= (k + 1)($\frac{1}{2}$k + 1) *factorising*

$= \frac{1}{2}$ (k + 1)(k + 2) *which is what we wanted to prove*.

This completes the inductive step. Hence, the result is true for all n ≥ 1.

Example 3.3.2. If a and b are consecutive integers, then the sum a + b is odd.

Solution 3.3.2

Proof. We have to define the propositional form F(x) to be true when the sum of x and its successor is odd.

Step 1: Let's consider the proposition F(1). The sum 1 + 2 = 3 is odd because we can demonstrate there exists an integer k such that 2k + 1 = 3. That is, 2(1) + 1 = 3. Thus, F(x) is true when x = 1.

Step 2: Assume that F(x) is true for some x. Thus, for some x we have that x + (x + 1) is odd. We add one to both x and x + 1 which gives the sum (x+1) + (x+2). We can make claim to two things: firstly, the sum (x+1) + (x+2) = F(x+1). Secondly, we claim that the addition of two (2) to any integer does not change the evenness or oddness of that integer (e.g., 1 + 2 = 3, 2 + 2 = 4). With these two observations we claim that F(x) is odd implies F(x + 1) is odd.

Step 3: By the principle of mathematical induction, we thus claim that F(x) is odd for all integers x. Thus, the sum of any two consecutive numbers is odd.

3.4 Indirect Proofs

3.4.1 Proof by Contrapositive

This proof starts by assuming that the conclusion Y is false, and through a series of logical steps deduce that the premise X must also be false.

Based on first-order logic we can make a statement such as P → Q is equivalent to ¬Q → ¬P. Steps to proving a theorem by contrapositive:

b. Assume ¬Q is true.
c. Show that ¬P must be true.
d. Observe that P → Q by contraposition

Example 3.4.1.1 Let n be an integer. If n is even, then n^2 is even.

Solution 3.4.1.1

Proof by contrapositive**:** Suppose that n is not even. Then by solution 3.2.1, n^2 is not even as well. Yes, that all!

3.4.2 Proof by Contradiction.

This form of proof assumes both that the premise X is true and the conclusion Y is false, and reach a logical fallacy.

Steps to proving a theorem by contradiction:

a. Assume P is true.
b. Assume ¬Q is true.
c. Demonstrate a contradiction.

Example 3.4.2.1 Let's apply this form of proof to example 3.4.1.1

Solution 3.4.2.1

Proof by contradiction: Suppose that n^2 is even, but n is odd. Applying solution 3.2.1, we see that n^2 must be odd. But n^2 cannot be both odd and even at the same time.

4.0 Conclusion

You have learnt from this unit that proof techniques can either be direct, indirect or by induction. That the choice of a proof technique depends on the problem or task at hand. You should note that there is no single method applicable to solving all tasks. This means that your level of ingenuity, skills and implementation of common sense must be applied to every task.

5.0 Summary

In this Unit, we have discussed the direct, indirect proofs, and proof by induction (proof by contrapositive and proof by contradiction). We also performed Inductive Hypothesis and applied necessary skills.

6.0 Tutor-Marked Assignment

1. Prove the following:
   a. $\sqrt{2}$ is irrational.
   b. Let x and y be non-negative reals. Then, $\frac{x + y}{2} \geq \sqrt{xy}$.
2. Use induction to prove for all $n \in \mathbb{N}$ that $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.
3. Prove that $7^n - 1$ is a multiple of 6 for all $n \in \mathbb{N}$.
4. Prove that $1 + 3 + 5 + \cdot \cdot \cdot + (2n - 1) = n^2$ for all $n \geq 1$.
5. Prove that $F_0 + F_2 + F_4 + \cdot \cdot \cdot + F_{2n} = F_{2n+1} - 1$ where F_n is the nth Fibonacci number.

7.0 References/Further Reading

Bunday, BD and Mulholland, H. (2014). Pure Mathematics for Advanced Level. Second edition. Published by Elsevier science. ISBN: 1483106136, 9781483106137

James, H. (2017). Discrete Structures, Logic and Computability. Published by Jones and Bartlett. Fourth Edition. ISBN:978-284-07040-8.

Seymour, L. S. (1964). Outline Series: Theory and Problems of Set Theory and Related Topics, pp. 1-133.

Stroud, KA. (2013) Engineering Mathematics. 7th edition. www.pdffiller.com/448950026--ENGINEERING-MATHEMATICS-7TH-EDITION-by-KA-Stroud.

UNIT 3 LOGIC

CONTENTS

1.0 Introduction

Logic is a formal study of mathematics; it is the study of mathematic reasoning and proofs itself. In this unit we cover some basic forms of logic. The propositional logic, where we will consider the logical connectives such as "and", "or", and "not". In the first-order logic, we will additionally include tools to reason. It contains predicates, quantifiers and variables.

2.0 Objectives

By the end of this Unit, you will be able to:

- discuss some mathematical reasoning and proofs
- explain some basic forms of logic
- use logical connectives
- apply some tools to reason.

3.0 Main Content

3.1 Propositional Logic

Logic is the study of consequences. Given a few mathematical statements or facts, we would like to be able to draw some conclusions. For example, we can say the statement: "Abuja is the capital of Nigeria" is True and that the statement: "The month of December is fall in the summer" is False. This kind of statements are called propositions because they are either true or false. The truth or falsehood of a proposition is called its truth value.

As stated earlier, propositional variables (also called **sentential** variables) which are the letters found in the middle of the English alphabet represented in capital: P, Q, R, S, … to represent each atomic statements in the molecular statement. These variables can only have two values, true or false. The logical connectives: “and”, “or”, “if… then”, “if and only if (or if)”, and “not” represented by these symbols $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, and $\neg$ respectively. The atomic statements: “It is raining” and “I need an umbrella” can be represented by the letters P and Q respectively.

P	**Q**	**¬P**	**¬Q**	**P ∧ Q**	**P ∨ Q**	**P → Q**	**P ↔ Q**
T	T	F	F	T	T	T	T
T	F	F	T	F	T	F	F
F	T	T	F	F	T	T	F
F	F	T	T	F	F	T	T

Example 3.1.1. Make a truth table for the statement $\neg P \vee Q$.

Solution 3.1.1. I solving such exercises, you will have to be careful as to knowing the exact position of the ¬. Note that this statement is not $\neg(P \vee Q)$, the negation belongs only to P (i.e. $\neg P$). Here is the truth table:

P	**Q**	**¬P**	**¬P ∨ Q**
T	T	F	T
T	F	F	F
F	T	T	T
F	F	T	T

Example 3.1.2. Analyze the statement, “if you get more doubles than any other player you will lose, or that if you lose you must have bought the most properties,” using truth tables.

Solution 3.1.2. Let’s start by breaking down the molecular statement into atomic statements. Let P be the statement “you get more doubles than any other player,”; Q be the statement “you will lose,” and R be the statement “you must have bought the most properties.” Now let’s construct a truth table to represent the statement as this symbol $(P \rightarrow Q) \vee (Q \rightarrow R)$.

The truth table needs to contain 8 rows in order to account for every possible combination of truth and falsity among the three statements. Here is the full truth table:

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

This is a true statement about monopoly, such that it is regardless of how many properties you own, how many doubles you roll, or whether you win or lose, the outcome is true for all 8 possible combinations.

The statement about monopoly in example 3.1.2 is an example of a **tautology**. Tautology is a statement which is true on the basis of its logical form alone. Tautologies are always true but they don't tell us much about the world. No knowledge about monopoly was required to determine that the statement was true.

3.1.1 Logical Equivalence

Two molecular statements P and Q are logically equivalent provided P is true precisely when Q is true. That is, P and Q have the same truth value under any assignment of truth values to their individual atomic parts. Then we symbolize it as $P \equiv Q$. In order to verify that two or more statements are logically equivalent, you may have to make a truth table for each and check whether the columns for the statements are identical.

Example 3.1.3. Check if the statement $\neg P \vee Q$ is logically equivalent to $P \to Q$.

Solution 3.1.3. let us start by making the truth table for these statements. Check example 3.1.1 and our first truth table.

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

Since the statements ¬P ∨ Q and P → Q either both true or both false for whatever values of P and Q. We therefore say these statements ¬P ∨ Q and P → Q are logically equivalent.

Exercise 3.1.4. Make a truth table to determine whether the statement ¬(P∨Q) is logically equivalent to ¬P ∧ ¬Q.

Solution 3.1.4.

Try it yourself.

The solution to exercise 3.1.4 will show that both statements are logically equivalent. It also shows that we can distribute a negation over a disjunction ("or"). Likewise, the distribution of negation over a conjunction ("and") is also possible.

De Morgan's Laws

1. ¬(P ∧ Q) is logically equivalent to ¬P ∨ ¬Q
2. ¬(P ∨ Q) is logically equivalent to ¬P ∧ ¬Q

Example 3.1.5. Without using truth tables prove that the statements ¬(P → Q) and P ∧ ¬Q are logically equivalent.

Solution 3.1.5. Let's start with one of the statements, and transform it into the other through a sequence of logically equivalent statements.

Start with ¬(P → Q).

We can rewrite the implication as a disjunction this is logically equivalent to

¬(¬P ∨ Q). (Solution 3.1.3 shows that P → Q is logically equivalent to ¬P ∨ Q)

By applying DE Morgan's law we get

$\neg\neg P \wedge \neg Q$. (the double negation $\neg\neg P$ is logically equivalent to P)

Finally, use double negation to arrive at

$P \wedge \neg Q$.

Deduction Rule

An argument is valid provided the conclusion must be true given that the premises are true. This means that for all times the premises are found to be true, the conclusion must be true for the argument to be a valid deduction rule, else it is invalid.

Example 3.1.6. Determine if the argument $\frac{\begin{array}{c}P \to Q\\ P\end{array}}{\therefore Q}$ is a valid deduction rule.

Solution 3.1.6. Considering solution 3.1.2, we can see that:

P	**Q**	**P → Q**
T	T	T
T	F	F
F	T	T
F	F	T

Our premises are P → Q and P. From the truth table we can see that row 1 where both of the premises are true, our condition Q is also true. Therefore, if P → Q and P are both true, we see that Q must be true as well. This implies that the argument is a valid deduction rule.

Exercise 3.1.6. Decide whether $\frac{\begin{array}{c}P \to Q\\ \neg P \vee Q\end{array}}{\therefore Q}$ is a valid deduction rule.

Solution 3.1.6.

Try it yourself.

Example 3.1.7. Decide whether $\frac{\begin{array}{c}P \to Q\\ Q \to R\\ R\end{array}}{\therefore P \vee Q}$ is a valid deduction rule.

Solution 3.1.7.

P	**Q**	**R**	**P → Q**	**Q → R**	**P ∨ Q**
T	T	T	T	T	T
T	T	F	T	F	T

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

The premises $P \rightarrow Q$, $Q \rightarrow R$ and R are all true in rows 1, 5, and 7. However, the conclusion $P \vee Q$ is not always true when the premises are all true as seen in row 7. Hence this is not a valid deduction rule.

3.2 First Order Logic

First order logic is an extension of propositional logic. Propositional logic only deals with “facts”, statements that may be true or false e.g. “It is raining”. However, one cannot have variables that stand for books or tables. First order logic operates over a set of objects (e.g., real numbers, people, etc.). It allows us to express properties of individual objects, to define relationships between objects, and, most important of all, to quantify over the entire set of objects.

Let’s give a classic argument in first order logic:

All men are mortal.

Adam is a man.

Therefore, Adam is a mortal.

In first order logic, the argument might be translated as follows:

$$\frac{\forall x\, \mathrm{Man}(x) \rightarrow \mathrm{Mortal}(x) \quad \mathrm{Man}\ (\mathrm{Adam})}{\mathrm{Mortal}\ (\mathrm{Adam})}$$

Let’s give some statements in first order logic:

i. “When you paint a with blue paint, it becomes blue.” cannot be made in propositional logic but can be made in first order logic. In propositional logic, we would need a statement about every single wall, one cannot make the general statement about all walls.

ii. "When you take the vaccine, all the chances of contracting the disease dies." In first order logic, we can talk about all the bacteria without naming them explicitly.

4.0 Conclusion

With the overview of proposition logic and, given a few mathematical statements, we were able to draw some conclusions that logic is the study of consequences. We were also able to apply De Morgan's law and logical equivalence.

5.0 Summary

At the end of this unit you have learnt some mathematical reasoning and proofs. Some basic forms of logic were highlighted using logical connectives. There was some applications of reasoning tools.

6.0 Tutor-Marked Assignment

1. Consider the statement about a party, "If it's your birthday or there will be cake, then there will be cake."

   a. Translate the above statement into symbols. Clearly state which statement is P and which is Q.

   b. Make a truth table for the statement.

   c. Assuming the statement is true, what (if anything) can you conclude if there will be cake?

   d. Assuming the statement is true, what (if anything) can you conclude if there will not be cake?

   e. Suppose you found out that the statement was a lie. What can you conclude?

2. Make a truth table for the statement $(P \vee Q) \rightarrow (P \wedge Q)$.

3. Using a truth table, determine if the following statements are logically equivalent.

   i. $(P \vee Q) \rightarrow R$ and $(P \rightarrow R) \vee (Q \rightarrow R)$.

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

iii. "I will not eat or drink" and "I will not eat and I will not drink". **Hint:** First translate to statement into a logical expression.

4. Simplify the following statements (so that negation only appears right before variables).
   a. $\neg(P \rightarrow \neg Q)$.
   b. $(\neg P \vee \neg Q) \rightarrow \neg(\neg Q \wedge R)$.
   c. $\neg((P \rightarrow \neg Q) \vee \neg(R \wedge \neg R))$.
   d. It is false that if Sam is not a man then Chris is a woman, and that Chris is not a woman.
5. Show that $\dfrac{\begin{matrix} P \rightarrow Q \\ Q \rightarrow R \end{matrix}}{\therefore P \rightarrow R}$ is a valid deduction rule.

7.0 References/Further Reading

James, H. (2017). Discrete Structures, Logic and Computability. Published by Jones and Bartlett. Fourth Edition. ISBN:978-284-07040-8.

Stroud, K. (2013) Engineering Mathematics. 7th edition. www.pdffiller.com/448950026-ENGINEERING-MATHEMATICS-7TH-EDITION-by-KA-Stroud.

Bunday, B and Mulholland, H. (2014). Pure Mathematics for Advanced Level. Second edition. Published by Elsevier science. ISBN: 1483106136, 9781483106137

Pass, R., & Tseng, W. L. D (2019). A Course in Discrete Structures. Wei-Lung Dustin Tseng, Site Internet: www.freechbooks.com(2019)

Haggard, G., Schlipf J., Whitesides, S., (2006). Discrete Mathematics for Computer Science. Thomson Brooks/Cole.

MODULE 2 BOOLEAN ALGEBRA AND GRAPH THEORY

UNIT 1 BOOLEAN ALGEBRA AND LATTICES

CONTENTS

1.0 Introduction

In this unit, you will acquire the skills to distinguish a partially ordered set, in which a pair of elements has both a least upper bound and greatest lower bound. To achieve this, you will learn from this unit, the types of relations and Boolean algebra.

2.0 Objectives

By the end of this unit, you will be able to:

- manipulate symbolic logic
- distinguish a partially ordered set
- explain operations that have logical significance.

3.0 Main Content

3.1 LATTICES

3.1.1 Partially Ordered Sets

We begin the study of lattices and Boolean algebras by generalizing the idea of inequality. Recall that a ***relation*** on a set X is a subset of X×X. A relation P on X is called a ***partial order*** of X if it satisfies the following axioms:

i. The relation is ***reflexive***: (a, a) ∈ P for all a ∈ X.

ii. The relation is ***antisymmetric***: if (a, b) ∈ P and (b, a) ∈ P, then a = b.

iii. The relation is ***transitive***: if (a, b) ∈ P and (b, c) ∈ P, then (a, c) ∈ P.

We usually write $a \preccurlyeq b$ to mean (a, b) ∈ P unless some symbol is naturally associated with a particular partial order, such as $a \preccurlyeq b$ with integers a and b, or $A \subset B$ with sets A and B. A set X together with a partial order $\preccurlyeq$ is called a **partially ordered set**, or **poset**.

A **partially ordered set** $(L, \preccurlyeq)$ is called a lattice if every pair of elements a and b in L has both a **Least Upper Bound** (LUB) or **Supremum** and a **Greatest Lower Bound** (GLB) or **Infimum**.

Let Y be a subset of a poset X. An element *u* in X is an **upper bound** of Y if $a \preccurlyeq u$ for every element $a \in Y$. If *u* is an upper bound of Y such that $u \preccurlyeq v$ for every other upper bound *v* of Y, then u is called an LUB of Y. An element *l* in X is said to be a **lower bound** of Y if $l \preccurlyeq a$ for all $a \in Y$. If *l* is a lower bound of Y such that $k \preccurlyeq l$ for every other lower bound *k* of Y, then l is called a GLB of Y.

The least upper bound is also called the **join** of a and b, denoted by $a \vee b$. The greatest lower bound is called the **meet** of a and b, and is denoted by $a \wedge b$.

If $(L, \preccurlyeq)$ is a lattice and a, b, c, d ∈ L, then the meet and join have the following order properties:

i. $a \wedge b \preccurlyeq \{a, b\} \preccurlyeq a \vee b$,

ii. $a \preccurlyeq b$ if and only if $a \wedge b = a$,

iii. $a \preccurlyeq b$ if and only if $a \vee b = a$,

iv. if $a \preccurlyeq b$, then $a \wedge c \preccurlyeq b \wedge c$ and $a \vee c \preccurlyeq b \vee\wedge c$

v. if $a \preccurlyeq b$ and $c \preccurlyeq d$, then $a \wedge c \preccurlyeq b \wedge d$ and $a \vee c \preccurlyeq b \vee d$

Therefore, by the definitions of LUB and GLB, this implies that if the join and meet exist, they are unique.

Example 3.1.1 The set of integers (or rationals or reals) is a poset where $a \leq b$ has the usual meaning for two integers a and b in $\mathbb{Z}$.

Example 3.1.2 Let X be any set. We will define the **power set** of X to be the set of all subsets of X. We denote the power set of X by $\mathcal{P}(X)$. For example, let X = {a, b, c}. Then $\mathcal{P}(X)$ is the set of all subsets of the set {a, b, c}:

$\emptyset$, {a}, {b}, {c}, {a, b}, {a, c}, {b, c}, {a, b, c}.

On any power set of a set X, set inclusion, ⊂, is a partial order. We can represent the order on {a, b, c} schematically by a diagram such as the one in Figure 3.1.

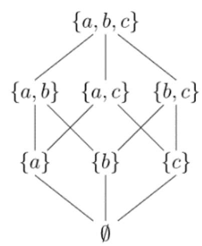


Figure 3.1 Partial Order of ({a, b, c})

Example 3.3 Let G be a group. The set of subgroups of G is a poset, where the partial order is set inclusion.

Example 3.4 There can be more than one partial order on a particular set. We can form a partial order on $\mathbb{N}$ by a ≼ b if a | b. The relation is certainly reflexive since a | a for all a ∈ N. If m | n and n | m, then m = n; hence, the relation is also antisymmetric. The relation is transitive, because if m | n and n | p, then m | p.

Example 3.5 Let X = {1, 2, 3, 4, 6, 8, 12, 24} be the set of divisors of 24 with the partial order defined in Example 3.4. Figure 3.2 shows the partial order on X.

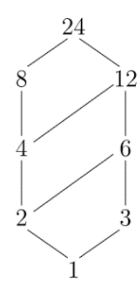


Figure 3.2 A partial order on the divisors of 24

Example 3.6 Let Y = {2, 3, 4, 6} be contained in the set X of Example 3.5. Then Y has upper bounds 12 and ,24, with 12 as a least upper bound. The only lower bound is 1; hence, it must be a greatest lower bound.

Theorem 3.1 Let Y be a nonempty subset of a poset X. If Y has a least upper bound, then Y has a unique least upper bound. If Y has a greatest lower bound, then Y has a unique greatest lower bound.

Proof: It is possible to define binary operations on many posets by using the greatest lower bound and the least upper bound of two elements. A lattice is a poset L such that every pair of elements in L has a least upper bound and a greatest lower bound.

Example 3.7 Let X be a set. Then the power set of X, $\mathcal{P}(X)$, is a lattice. For two sets A and B in $\mathcal{P}(X)$, the least upper bound of A and B is A ∪ B. Certainly A ∪ B is an upper bound of A and B, since A ⊂ A ∪ B and B ⊂ A ∪ B. If C is some other set containing both A and B, then C must contain A ∪ B; hence, A ∪ B is the least upper bound of A and B. Similarly, the greatest lower bound of A and B is A ∩ B.

Axiom 3.1 Principle of Duality: Any statement that is true for all lattices remains true when $\preccurlyeq$ is replaced by $\succcurlyeq$ and ∨ and ∧ are interchanged throughout the statement.

Theorem 3.2 If L is a lattice, then the binary operations ∨ and ∧ satisfy the following properties for a, b, c ∈ L.

i. Commutative laws: $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$
ii. Associative laws: $a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.
iii. Idempotent laws: $a \vee a = a$ and $a \wedge a = a$.
iv. Absorption laws: $a \vee (a \wedge b) = a$ and $a \wedge (a \vee b) = a$.

Proof

By the Principle of Duality, we need only prove the first statement in each part.

i. By definition $a \vee b$ is the least upper bound of {a, b}, and $b \vee a$ is the least upper bound of {b, a}; however, {a, b} = {b, a}.
ii. We will show that $a \vee (b \vee c)$ and $(a \vee b) \vee c$ are both least upper bounds of {a, b, c}. Let $d = a \vee b$. Then $c \preccurlyeq d \vee c = (a \vee b) \vee c$.
We also know that
$a \preccurlyeq a \vee b = d \preccurlyeq d \vee c = (a \vee b) \vee c$.

A similar argument demonstrates that $b \preccurlyeq (a \vee b) \vee c$. Therefore, $(a \vee b) \vee c$ is an upper bound of {a, b, c}. We now need to show that $(a \vee b) \vee c$ is the least upper bound of {a, b, c}. Let u be some other upper bound of {a, b, c}. Then $a \preccurlyeq u$ and $b \preccurlyeq u$ hence, $d = a \vee b \preccurlyeq u$. Since $c \preccurlyeq u$, it follows that $(a \vee b) \vee c = d \vee c \preccurlyeq u$. Therefore, $(a \vee b) \vee c$ must be the least upper bound of {a, b, c}. The argument that shows $a \vee (b \vee c)$ is the least upper bound of {a, b, c} is the same. Consequently, $a \vee (b \vee c) = (a \vee b) \vee c$.

iii. The join of a and a is the least upper bound of {a}; hence, $a \vee a = a$.

iv. Let $d = a \wedge b$. Then $a \preccurlyeq a \vee d$. On the other hand, $d = a \wedge b \preccurlyeq a$, and so $a \vee d \preccurlyeq a$. Therefore, $a \vee (a \wedge b) = a$.

Given any arbitrary set L with operations $\vee$ and $\wedge$, satisfying the conditions of the previous theorem, it is natural to ask whether or not this set comes from some lattice. The following theorem says that this is always the case.

Theorem 3.3 Let L be a nonempty set with two binary operations $\vee$ and $\wedge$ satisfying the commutative, associative, idempotent, and absorption laws. We can define a partial order on L by $a \preccurlyeq b$ if $a \vee b = b$. Furthermore, L is a lattice with respect to $\preccurlyeq$ if for all $a, b \in L$, we define the least upper bound and greatest lower bound of a and b by $a \vee b$ and $a \wedge b$, respectively.

Proof

Firstly, let's show that L is a poset under $\preccurlyeq$. Since $a \vee a = a$, $a \preccurlyeq a$ and $\preccurlyeq$ is reflexive. To show that $\preccurlyeq$ is antisymmetric, let $a \preccurlyeq b$ and $b \preccurlyeq a$. Then $a \vee b = b$ and $b \vee a = a$. By the commutative law, $b = a \vee b = b \vee a = a$. Finally, we must show that $\preccurlyeq$ is transitive. Let $a \preccurlyeq b$ and $b \preccurlyeq c$. Then $a \vee b = b$ and $b \vee c = c$. Thus,

$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$,

or $a \preccurlyeq c$.

Now, to show that L is a lattice, we need to prove that $a \vee b$ and $a \wedge b$ are, respectively, the least upper and greatest lower bounds of a and b. Since $a = (a \vee b) \wedge a = a \wedge (a \vee b)$, it follows that $a \preccurlyeq a \vee b$. Similarly, $b \preccurlyeq a \vee b$. Therefore, $a \vee b$ is an upper bound for a and b. Let u be any other upper bound of both a and b. Then $a \preccurlyeq u$ and $b \preccurlyeq u$. But $a \vee b \preccurlyeq u$ since

$$(a \vee b) \vee u = a \vee (b \vee u) = a \vee u = u.$$

Exercise 3.1: Prove that $a \wedge b$ is the greatest lower bound of a and b.

3.2 Boolean Algebras

Let us investigate the example of the power set, $\mathcal{P}(X)$, of a set X more closely. The power set is a lattice that is ordered by inclusion. By the definition of the power set, the largest element in $\mathcal{P}(X)$ is X itself and the smallest element is $\emptyset$, the empty set. For any set A in $\mathcal{P}(X)$, we know that $A \cap X = A$ and $A \cup \emptyset = A$. This suggests the following definition for lattices. An element I in a poset X is a **largest element** if $a \preccurlyeq I$ for all $a \in X$. An element O is a **smallest element** of X if $O \preccurlyeq a$ for all $a \in X$.

Let A be in $\mathcal{P}(X)$. Recall that the complement of A is

$$A' = X \backslash A = \{x : x \in X \text{ and } x \notin A\}.$$

We know that $A \cup A' = X$ and $A \cap A' = \emptyset$. We can generalize this example for lattices. A lattice L with a largest element I and a smallest element O is ***complemented*** if for each $a \in L$, there exists an a' such that $a \vee a' = I$ and $a \wedge a' = O$.

In a lattice, L, the binary operations $\vee$ and $\wedge$ satisfy commutative and associative laws; however, they need not satisfy the distributive law

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c);$$

however, in $\mathcal{P}(X)$ the distributive law is satisfied since

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

for $A, B, C \in \mathcal{P}(X)$. We will say that a lattice L is ***distributive*** if the following distributive law holds:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

for all $a, b, c \in L$.

Theorem 3.4 A lattice L is distributive if and only if

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

for all $a, b, c \in L$.

Proof

Let us assume that L is a distributive lattice.

$$\begin{aligned} a \vee (b \wedge c) &= [a \vee (a \wedge c)] \vee (b \wedge c) \\ &= a \vee [(a \wedge c) \vee (b \wedge c)] \end{aligned}$$

$= a \vee [(c \wedge a) \vee (c \wedge b)]$

$= a \vee [c \wedge (a \vee b)]$

$= a \vee [(a \vee b) \wedge c]$

$= [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c]$

$= (a \vee b) \wedge (a \vee c).$

The converse follows directly from the Duality Principle.

A ***Boolean algebra*** is a lattice B with a greatest element I and a smallest element O such that B is both distributive and complemented. The power set of X, $\mathcal{P}(X)$, is our prototype for a Boolean algebra. As it turns out, it is also one of the most important Boolean algebras. The following theorem allows us to characterize Boolean algebras in terms of the binary relations $\vee$ and $\wedge$ without mention of the fact that a Boolean algebra is a poset.

Theorem 3.5 A set B is a Boolean algebra if and only if there exist binary operations $\vee$ and $\wedge$ on B satisfying the following axioms.

i. $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$ for $a, b \in B$.
ii. $a \vee (b \vee c) = (a \vee b) \vee c$ and $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ for $a, b, c \in B$.
iii. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ for $a, b, c \in B$.
iv. There exist elements I and O such that $a \vee O = a$ and $a \wedge I = a$ for all $a \in B$.
v. For every $a \in B$ there exists an $a' \in B$ such that $a \vee a' = I$ and $a \wedge a' = O$.

Proof

Let B be a set satisfying (i) – (v) in the theorem. One of the idempotent laws is satisfied since

$$\begin{aligned} a &= a \vee O \\ &= a \vee (a \wedge a') \\ &= (a \vee a) \wedge (a \vee a') \\ &= (a \vee a) \wedge I \\ &= a \vee a. \end{aligned}$$

Notice that

$$I \vee b = (b \vee b') \vee b = (b' \vee b) \vee b = b' \vee (b \vee b) = b' \vee b = I.$$

Consequently, the first of the two absorption laws holds, since

$$a \vee (a \wedge b) = (a \wedge I) \vee (a \wedge b)$$
$$= a \wedge (I \vee b)$$
$$= a \wedge I$$
$$= a.$$

The other idempotent and absorption laws are proven similarly. Since B also satisfies (i)–(iii), the conditions of Theorem 3.3 are met; therefore, B must be a lattice. Condition (iv) tells us that B is a distributive lattice.

For, $a \in B$, $O \vee a = a$; hence, $O \preccurlyeq a$ and O is the smallest element in B. To show that I is the largest element in B, we will first show that $a \vee b = b$ is equivalent to $a \wedge b = a$. Since $a \vee I = a$ for all $a \in B$, using the absorption laws we can determine that

$$a \vee I = (a \wedge I) \vee I = I \vee (I \wedge a) = I \text{ or } a \preccurlyeq I$$

for all a in B. Finally, since we know that B is complemented by (v), B must be a Boolean algebra.

Conversely, suppose that B is a Boolean algebra. Let I and O be the greatest and least elements in B, respectively. If we define $a \vee b$ and $a \wedge b$ as least upper and greatest lower bounds of $\{a, b\}$, then B is a Boolean algebra by Theorem 3.3 and Theorem 3.4.

Some of these identities in Boolean algebras are listed in the following theorem.

Theorem 3.6 Let B be a Boolean algebra. Then,

i. $a \vee I = I$ and $a \wedge O = O$ for all $a \in B$.
ii. If $a \vee b = a \vee c$ and $a \wedge b = a \wedge c$ for $a, b, c \in B$ then, $b = c$.
iii. If $a \vee b = I$ and $a \wedge b = O$, then $b = a'$.
iv. $(a')' = a$ for all $a \in B$.
v. $I' = O$ and $O' = I$.
vi. $(a \vee b)' = a' \wedge b'$ and $(a \wedge b)' = a' \vee b'$ (De Morgan's Laws).

Proof

We will prove only (ii). The rest of the identities are left as your exercises.

For $a \vee b = a \vee c$ and $a \wedge b = a \wedge c$, we have

$$b = b \vee (b \wedge a)$$
$$= b \vee (a \wedge b)$$
$$= b \vee (a \wedge c)$$

$= (b \vee a) \wedge (b \vee c)$

$= (a \vee b) \wedge (b \vee c)$

$= (a \vee c) \wedge (b \vee c)$

$= (c \vee a) \wedge (c \vee b)$

$= c \vee (a \wedge b)$

$= c \vee (a \wedge c)$

$= c \vee (c \wedge a)$

$= c.$

Finite Boolean Algebras

A Boolean algebra is a ***finite Boolean algebra*** if it contains a finite number of elements as a set. Finite Boolean algebras are particularly nice since we can classify them up to isomorphism.

Let B and C, be Boolean algebras. A bijective map ϕ: $B \rightarrow C$ is an ***isomorphism*** of Boolean algebras if

$$\phi(a \vee b) = \phi(a) \vee \phi(b)$$

$$\phi(a \wedge b) = \phi(a) \wedge \phi(b)$$

for all a and b in B.

We will show that any finite Boolean algebra is isomorphic to the Boolean algebra obtained by taking the power set of some finite set X. We will need a few lemmas and definitions before we prove this result. Let B be a finite Boolean algebra. An element $a \in B$ is an ***atom*** of B if $a \neq O$ and $a \wedge b = a$ for all $b \in B$ with $b \neq O$. Equivalently, a is an atom of B if there is no $b \in B$ with $b \neq O$ distinct from a such that $O \preccurlyeq b \preccurlyeq a$.

Lemma 3.1 Let B be a finite Boolean algebra. If b is an element of B with $b \neq O$, then there is an atom a in B such that $a \preccurlyeq b$.

Proof

If b is an atom, let a = b. Otherwise, choose an element b_1, not equal to O or b, such that $b_1 \preccurlyeq b$. We are guaranteed that this is possible since b is not an atom. If b_1 is an atom, then we are done. If not, choose, b_2, not equal to O or b_1, such that $b_2 \preccurlyeq b_1$. Again, if b_2 is an atom, let $a = b_2$. Continuing this process, we can obtain a chain

$$O \preccurlyeq \ldots \preccurlyeq b_3 \preccurlyeq b_2 \preccurlyeq b_1 \preccurlyeq b.$$

Since B is a finite Boolean algebra, this chain must be finite. That is, for some k, b_k is an atom. Let $a=b_k$.

Lemma 3.2 Let a and b be atoms in a finite Boolean algebra B such that $a \neq b$. Then $a \wedge b = O$.

Proof

Since $a \wedge b$ is the greatest lower bound of a and b, we know that $a \wedge b \preccurlyeq a$. Hence, either $a \wedge b = a$ or $a \wedge b = O$. However, if $a \wedge b = a$, then either $a \preccurlyeq b$ or $a = O$. In either case we have a contradiction because a and b are both atoms; therefore, $a \wedge b = O$.

Lemma 3.3 Let B be a Boolean algebra and $a, b \in B$. The following statements are equivalent.

i. $a \preccurlyeq b$,
ii. $a \wedge b' = O$,
iii. $a' \vee b = I$.

Proof

(i) ⇒ (ii). If $a \preccurlyeq b$, then $a \vee b = b$. Therefore,

$$
\begin{aligned}
a \wedge b' &= a \wedge (a \vee b)' \\
&= a \wedge (a' \wedge b') \\
&= (a \wedge a') \wedge b' \\
&= O \wedge b' \\
&= O.
\end{aligned}
$$

(ii) ⇒ (iii). If $a \wedge b' = O$, then $a' \vee b = (a \wedge b')' = O' = I$.

(iii) ⇒ (i). If $a' \vee b = I$, then

$$
\begin{aligned}
a &= a \wedge (a' \vee b) \\
&= (a \wedge a') \vee (a \wedge b) \\
&= O \vee (a \wedge b) \\
&= a \wedge b.
\end{aligned}
$$

Thus, $a \preccurlyeq b$.

Lemma 3.4 Let B be a Boolean algebra and b and c be elements in B such that $b \not\preccurlyeq c$. Then there exists an atom $a \in B$ such that $a \preceq b$ and $a \not\preccurlyeq c$.

Proof

By Lemma 3.3, $b \wedge c' \neq O$. Hence, there exists an atom a such that $a \preccurlyeq b \wedge c'$. Consequently, $a \preccurlyeq b$ and $a \not\preccurlyeq c$.

Lemma 3.5 Let $b \in B$ and $a_1,\ldots,a_n$ be the atoms of B such that $a_i \preceq b$. Then $b = a_1 \vee\cdots\vee a_n$. Furthermore, if $a, a_1,\ldots,a_n$ are atoms of B such that, $a \preccurlyeq b$, $a_i \preccurlyeq b$, and $b = a \vee a1 \vee\cdots\vee an$, then $a = a_i$ for some $i = 1,\ldots,n$.

Proof

Let $b1 = a_1 \vee\cdots\vee a_n$. Since $a_i \preccurlyeq b$ for each i, we know that $b_1 \preccurlyeq b$. If we can show that $b \preccurlyeq b_1$, then the lemma is true by antisymmetry. Assume $b \preccurlyeq b_1$. Then there exists an atom a such that $a \preccurlyeq b$ and $a \not\preccurlyeq b_1$. Since a is an atom and $a \preccurlyeq b$, we can deduce that $a = a_i$ for some a_i. However, this is impossible since $a \preccurlyeq b_1$. Therefore, $b \preccurlyeq b_1$.

Now suppose that $b = a1\vee\cdots\vee an$. If a is an atom less than b,

$$a = a \wedge b = a \wedge (a_1 \vee\cdots\vee a_n) = (a \wedge a_1) \vee\cdots\vee (a \wedge a_n).$$

But each term is O or a with $a \wedge ai$ occurring for only one .ai. Hence, by Lemma 3.2, $a = a_i$ for some i.

Theorem 3.6 Let B be a finite Boolean algebra. Then there exists a set X such that B is isomorphic to $\mathcal{P}(X)$.

Proof

We will show that B is isomorphic to $\mathcal{P}(X)$, where X is the set of atoms of B. Let $a \in B$. By Lemma 3.5, we can write a uniquely as $a = a_1 \vee\cdots\vee a_n$ for $a_1, \ldots, a_n \in X$. Consequently, we can define a map $\phi: B \to \mathcal{P}(X)$ by

$$\phi(a) = \phi(a_1 \vee\cdots\vee a_n) = \{a_1, \ldots, a_n\}.$$

Clearly, ϕ is onto.

Now let $a = a_1 \vee\cdots\vee a_n$ and $b = b_1 \vee\cdots\vee b_m$ be elements in B, where each ai and each bi is an atom. If $\phi(a) = \phi(b)$, then $\{a_1,\cdots, a_n\} = \{b_1,\cdots,b_m\}$ and $a = b$.

Consequently, ϕ is injective.

The join of a and b is preserved by ϕ since

$$\phi(a \vee b) = \phi(a_1 \vee\cdots\vee a_n \vee b_1 \vee\cdots\vee b_m)$$

$$= \{ a_1,\cdots, a_n, b_1,\cdots,b_m\}$$

$$= \{ a_1,\cdots, a_n\} \cup \{ b_1,\cdots,b_m\}$$

$= \phi(a_1 \vee \cdots \vee a_n) \cup \phi(b_1 \vee \cdots \vee b_m)$

$= \phi(a) \cup \phi(b)$.

Similarly, $\phi(a \wedge b) = \phi(a) \cap \phi(b)$.

Exercise 3.2 Prove

Corollary 3.1. *The order of any finite Boolean algebra must be 2n for some positive integer n.*

Study Questions

1. Describe succinctly what a poset is. Do not just list the defining properties, but give a description that another student of algebra who has never seen a poset might understand. For example, part of your answer might include what type of common algebraic topics a poset generalizes, and your answer should be short on symbols.
2. How does a lattice differ from a poset? Answer this in the spirit of the previous question.
3. How does a Boolean algebra differ from a lattice? Again, answer this in the spirit of the previous two questions.
4. Give two (perhaps related) reasons why any discussion of finite Boolean algebras might center on the example of the power set of a finite set.
5. Describe a major innovation of the middle twentieth century made possible by Boolean algebra.

4.0 Conclusion

In conclusion, the unit dwelt extensively on partially ordered sets, principle of duality and Boolean algebra. A poset is short for partially ordered set which is a set whose elements are ordered but not all pairs of elements are required to comparable in the order. A Boolean algebra is a finite Boolean algebra if it contains a finite number of elements as a set. Finite Boolean algebras are particularly nice since we can classify them up to isomorphism The power set is a lattice that is ordered by inclusion.

5.0 Summary

In the unit you have learnt that:

- A relation P on X is called a partial order of X if it satisfies the axioms of reflective, antisymmetric and transitive.

- lattices and Boolean algebras are generalizing by the idea of inequality
- A Boolean algebra is a finite Boolean algebra if it contains a finite number of elements as a set.
- power set is a lattice that is ordered by inclusion.
- Finite Boolean algebras are particularly nice since we can classify them up to isomorphism.

6.0 Tutor-Marked Assignment

1. Draw the lattice diagram for the power set of X = {a, b, c, d} with the set inclusion relation, $\subset$.
2. Draw the diagram for the set of positive integers that are divisors of 30. Is this poset a Boolean algebra?
3. Let B be the set of positive integers that are divisors of .210. Define an order on B by $a \preccurlyeq b$ if $a \mid b$. Prove that B is a Boolean algebra. Find a set X such that B is isomorphic to $\mathcal{P}(X)$.
4. Prove or disprove: $\mathbb{Z}$ is a poset under the relation $a \preccurlyeq b$ if $a \mid b$.
5. Draw the switching circuit for each of the following Boolean expressions.
   i. $(a \vee b \vee a') \wedge a$
   ii. $(a \vee b)' \wedge (a \vee b)$
   iii. $a \vee (a \wedge b)$
   iv. $(c \vee a \vee b) \wedge c' \wedge (a \vee b)'$
6. Draw a circuit that will be closed exactly when only one of three switches a, b, and c are closed.
7. Prove or disprove: The set of all nonzero integers is a lattice, where $a \preccurlyeq b$ is defined by $a \mid b$.

7.0 References/Further Reading

Donnellan, T. (1968). Lattice Theory. Pergamon Press.

Halmos, P.(1956). The Basic Concepts of Algebraic Logic, American Mathematical Monthly vol., 53, 363–87.

Hohn, F. (1955). Some Mathematical Aspects of Switching, American Mathematical Monthly, vol., 62, 75–90.

Hohn, F. (1966). Applied Boolean Algebra. 2nd ed. Macmillan, New York.

Lidl, R. and Pilz, G. (1998). Applied Abstract Algebra. 2nd ed. Springer, New York,

Whitesitt, J. (2010). Boolean Algebra and Its Applications. Dover, Mineola, NY.

UNIT 2 GRAPH THEORY

CONTENTS

1.0 Introduction

Graphs are simple, however, they are extremely useful mathematical objects. They are universal in the practical applications of Computer Science. For example:

i. In a computer network, we can use graphs to represent how computers are connected to each other. We use the nodes to represent the individual computers and the edges to represent the network connections. Such a graph can then be used to route messages as quickly as possible.
ii. In a digitalized map, nodes represent intersections (or cities), and edges represent roads (or highways). We may use directed edges to capture one-way traffic on streets, and weighted edges to capture distance. Such a graph can be used for generation directions (e.g., in GPS units).
iii. On the internet, nodes represent web pages, and (directed) edges represent links from one web page to another. Such a graph can be used to rank each web page in the order of importance when displaying search results (e.g., the importance of a web page can be determined by the

amount of other web pages that are referencing it or pointing to it, and recursively how important those web pages are).

iv. In a social network, nodes represent people, and edges represent friendships. One hot research topic currently is the understanding social networks. For example, how does a network achieve “x-degrees of separation”, where everyone is approximately x number of friendships away from anyway else?

2.0 Objectives

By the end of this Unit, you will be able to:

- design complex network connections
- analyse traffic routes and determine the shortest path to any location
- discuss more on rating of web sites through referencing or site visits.

3.0 Main Content

3.1 Graphs

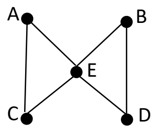
Graphs are made up of a collection of dots that are called **vertices** and lines connecting those dots that are called **edges**. When two vertices are connected by an edge, we say that they are **adjacent**.

Definition 3.1.1 A graph is an ordered pair G = (V, E) consisting of a nonempty set V (**vertices**) and a set E (**edges**) of two-element subsets of V.

- **Definition 3.1.2.** A **directed graph** G is a pair (V, E) where V is a set of vertices (or nodes), and $E \subseteq V \times V$ is a set of edges. The **order** of the two connected vertices is important.
- **Definition 3.1.3.** An **undirected graph** additionally has the property that $(u, v) \in E$ if and only if $(v, u) \in E$.

Example 3.1.1.1 In a school social gathering, Abel, Bill, Clair, Dan, and Eve were assigned to a group. In that group, all members are allowed to “discuss” with each other. However, it turns out that the discussions were between Abel and Clair, Bill and Dan. While Eve discussed with everyone. Represent this situation with a graph.

Solution 3.1.1.1 Each person will be represented by a vertex and each discussion will be represented by an edge. That is, two vertices will be adjacent (there will be an edge between them) if and only if the people represented by those vertices discussed.



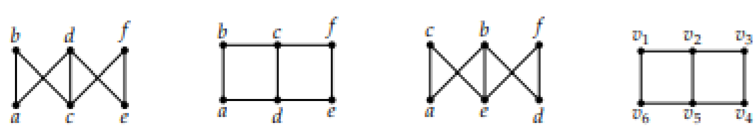
From definition 3.1.1, a graph could be G = (V, E) = ({a, b, c, d}, {{a, b}, {a, c}, {b, c}, {b, d}, {c, d}}). This graph has four vertices (a, b, c, d) and five edges (the pairs {a, b}, {a, c}, {b, c}, {b, d}, {c, d}).

Exercise 3.1.1.2 Draw the graph ({a, b, c, d}, {{a, b}, {a, c}, {b, c}, {b, d}, {c, d}}).

In **directed graphs**, edge (u, v) (starting from node u, ending at node v) is not the same as edge (v, u). We also allow “self-loops” or “recursive-loops”, i.e., edges of the form (v, v). Since the edge (u, v) and (v, u) must both be present or missing, we often treat a non-self-loop edge as an unordered set of two nodes (e.g., {u, v}). A common extension is a weighted graph, where each edge additionally carries a weight (a real number). The weight can have a variety of meanings in practice: distance, importance and capacity, to name a few.

Example 3.1.1.3 Before we proceed further, try to determine:

i. Which (if any) of the graphs below are the same?



ii. Are the graphs below the same or different?

Graph 1:

V = {a, b, c, d, e},

E = {{a, b}, {a, c}, {a, d}, {a, e}, {b, c}, {d, e}}.

Graph 2:

V = {v1, v2, v3, v4, v5},

E = {{v1, v3}, {v1, v5}, {v2, v4}, {v2, v5}, {v3, v5}, {v4, v5}}

iii. Are the graphs below equal?

G1 = ({a, b, c}, {{a, b}, {b, c}}); G2 = ({a, b, c}, {{a, c}, {c, b}}).

Solution 3.1.1.3 (iii). No. Here the vertex sets of each graph are equal, which is a good start. Also, both graphs have two edges. In the first graph, we have edges {a, b} and {b, c}, while in the second graph we have edges {a, c} and {c, b}. Now we do have {b, c} = {c, b}, so that is not the problem. The issue is that {a, b}, {a, c}. Since the edge sets of the two graphs are not equal (as sets), the graphs are not equal (as graphs).

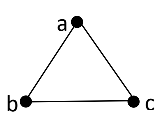
Example 3.1.1.4 Consider the graphs:

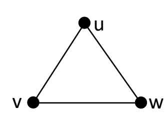
G1 = {V1, E1} where V1 = {a, b, c} and E1 = {{a, b}, {a, c}, {b, c}};

G2 = {V2, E2} where V2 = {u, v, w} and E2 = {{u, v}, {u, w}, {v, w}}.

Are these graphs the same?

Solution 3.1.1.4 The two graphs are NOT equal. It is enough to notice that V1, V2 since a ∈ V1 but a ∉ V2. However, both of these graphs consist of three vertices with edges connecting every pair of vertices. By drawing the graph as follows:





We can clearly see that these graphs are basically the same, so while they are not equal, they will be isomorphic. This means the renaming of the vertices of one of the graphs and results in the second graph.

3.1.4 Isomorphic Graphs

An **isomorphism** between two graphs G1 and G2 is a bijection, f: V1 → V2 between the vertices of the graphs such that {a, b} is an edge in G1 if and only if {f(a), f(b)} is an edge in G2. Two graphs are isomorphic if there is an isomorphism between them. In this case we write G1 ≅ G2.

Example 3.1.4.1 Decide whether the graphs G1 = {V1, E1} and G2 = {V2, E2} are equal or isomorphic. V1 = {a, b, c, d}, E1 = {{a, b}, {a, c}, {a, d}, {c, d}} and V2 = {a, b, c, d}, E2 = {{a, b}, {a, c}, {b, c}, {c, d}}.

Solution 3.1.4.1 The graphs are NOT equal, since {a, d} ∈ E1 but {a, d} ∉ E2. However, we can confirm that both graphs contain the exact same number of vertices and edges. By this, they might be isomorphic (this is a good start but in most cases, it is not enough).
Let's try to build an isomorphism. From the definition, let's try to build a bijection f: V1 → V2, such that f(a) = b, f(b) = c, f(c) = d and f(d) = a. This is a bijection, but to make sure that the function is an isomorphism, we must make sure it respects the edge relation.
In G1, the vertices a and b are connected by an edge. In G2, f(a) = b and f(b) = c are connected by an edge. We are on the right track, however, we have to check the other three edges. The edge {a, c} in G1 corresponds to {f(a), f(c)} = {b, d}, now we have a problem here. There is no edge between b and d in G2. Thus f is **NOT an isomorphism**.
If f is not an isomorphism, it does not mean that there is no isomorphism between G1 and G2. Let's draw the graphs and then try to create some match ups (if possible).
It is noticeable in G1 that the vertex a is adjacent to every other vertex. In G2, there is also a vertex with such property and that is c. Therefore, we can build the bijection g: V1 → V2 by defining g(a) = c to start with. Next, which vertex should we match with b? In G1, the vertex b is only adjacent to vertex a. There is exactly one vertex like this in G2, that is d. Therefore, let g(b) = d. By looking at the last two, we can see that we are free to choose the matches. Therefore, let go with g(c) = b and g(d) = a (switching these would still work fine).
Finally, let's check that there is really is an isomorphism between G1 and G2 using g. We have seen that g is definitely a bijection. Now we have to make sure that the edges are respected. The four edges in G1 are

{a, b}, {a, c}, {a, d}, {c, d}.

Under the proposed isomorphism these become

{g(a), g(b)}, {g(a), g(c)}, {g(a), g(d)}, {g(c), g(d)}

The bijection results in the edges:

{c, d}, {c, b}, {c, a}, {b, a}.

These edges are precisely the edges in G2. Thus g is an isomorphism, hence G1 ≅ G2.

3.1.5 Subgraphs

3.1.5.1 Definition. We say that G′ = (V′, E′) is a subgraph of G = (V, E), and write G′ ⊆ G, provided V′ ⊆ V and E′ ⊆ E.

3.1.5.2 Definition. We say that G′ = (V′, E′) is an induced subgraph of G = (V, E) provided V′ ⊆ V and every edge in E whose vertices are still in V′ is also an edge in E′.

Example 3.1.5. Considering the graph G1. Which of the graphs G2, G3 and G4 are subgraphs or induced subgraphs of G1?

Solution 3.1.5. By carefully applying the definitions of a subgraph and an induced subgraph, we can see that:

i. The graphs G2 and G3 are both **subgraphs** of G1.

ii. Only the graph G2 is an **induced subgraph**. This is because every edge in G1 that connects vertices in G2 is also an edge in G2. However, in G3, the edge {a, b} is in E1 but not E3, even though vertices a and b are in V3.

iii. The graph G4 is **NOT a subgraph** of G1. It might seem like it is, however, if you look closely, you will realize that vertex e does not exist in G4. Therefore, it is enough to say that G4 is NOT a subgraph of G1, since {c, f} ∈ E4 but {c, f} ∉ E1 and that we don't have the required E4 ⊆ E1.

3.1.6 Bipartite Graphs

A graph is **bipartite** if the vertices can be divided into two sets, A and B, with no two vertices in adjacent in A and B. The vertices in A can be adjacent to some or all of the vertices in B. If each vertex in A is adjacent to all the vertices in B, then the graph is a **complete bipartite** graph, and gets a special name: $K_{m,n}$, where |A| = m and |B| = n.

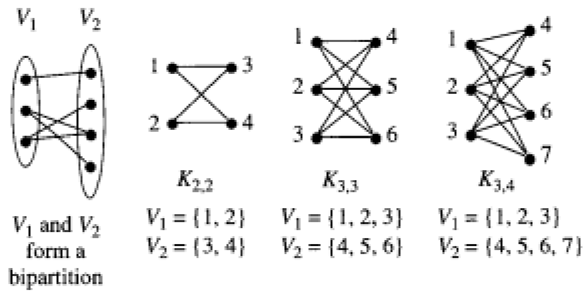
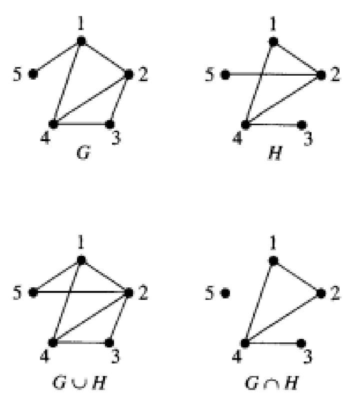


Figure 3: Bipartition and complete bipartite graphs.

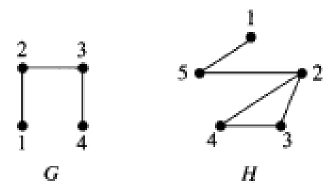
3.1.7 Union and Intersection of a Graph: These are two useful operations for combining graphs. Let G1 = (V1, E1) and G2 = (V2, E2) be graphs.

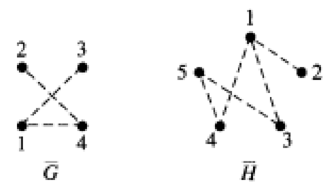
i. The union of G1 and G2, denoted by G1 ⋃ G2, is the graph G3 defined as G3 = (V1 ⋃ V2, E1 ⋃ E2).

ii. The intersection of G 1 and G2, denoted by G1 ∩ G2, is the graph G4 defined as G4 = (V1 ∩ V2, EI ∩ E2).



3.1.8 Complement of a Graph: This operation that is used with a single graph. To define this, we need an analogue of a universal set. In this case, we use the complete graph on the vertex set of the graph for which we would like to find the complement. Let G = (V, E) be a subgraph of $K_{|V|}$, the complete graph on |V| vertices. The complement of $G^{¯}$ in $K_{|V|}$, denoted as G = (V1, El), is the subgraph of $K_{|V|}$ with V1 = V and E1 = $K_{|V|}$ (E) - E.





3.2 The Handshaking Problem

Theorem 1. **(Handshaking Theorem)** Let G be a graph with at least two vertices. At least two vertices of G have the same degree.

Proof. The proof is by induction on the number of vertices n in a graph. Let $n_o = 2$ and T = {n ∈ N: any graph with n vertices has at least two vertices of the same degree}.

(Base step) For n_o, the only graphs to consider are the graph consisting of two isolated vertices and the graph having a single edge. Clearly, the result holds for each of these graphs. Therefore, the base case $n_o = 2$ is true and $n_o \in T$.

(Inductive step) Let n ≥ no. Show that if n ∈ T, then n + 1 ∈ T.

Assuming that any graph on n vertices with n ≥ 2 has two vertices of the same degree, we must prove that any graph on n + 1 vertices has two vertices of the same degree.

Let G = (V, E) be a graph with n + 1 vertices where n + 1 ≥ 3. Clearly, $0 \leq deg(v) \leq n$ for any v ∈ V.

If there is an isolated vertex in G, then by the induction hypothesis, the subgraph of G consisting of all the vertices but one isolated vertex must have two vertices with the same degree. Adding an isolated vertex to the subgraph with at least two vertices having the same degree gives the result for G.

If there is no isolated vertex in G, then all the degrees of vertices v ∈ V satisfy $1 \leq deg(v) \leq n$. In this case, we have at most n different values for the degrees of vertices in G. Since G has n + 1 vertices, then by the Pigeon-Hole Principle (see reference material for more explanation), at least two vertices of G have the same degree.

Therefore, n + 1 ∈ T. By the Principle of Mathematical Induction, T = {n ∈ N: n ≥ 2}.

The handshake theorem is sometimes called the degree sum formula, and can be written symbolically as

$\sum_{v \in V} d(v) = 2e.$

Here we are using the notation d(v) for the degree of the vertex v. One use for the theorem is to actually find the number of edges in a graph. To do this, you must be given the degree sequence for the graph (or be able to find it from other information). This is a list of every degree of every vertex in the graph, generally written in non-increasing order.

Example 3.2.1. How many vertices and edges must a graph have if its degree sequence is (4, 4, 3, 3, 3, 2, 1)?

Solution 3.2.1. The number of vertices is easy to find: it is the number of degrees in the sequence: 7. To find the number of edges, we compute the sum of the degrees:

$4 + 4 + 3 + 3 + 3 + 2 + 1 = 20.$

Therefore, the number of edges is half of 20 (20/2) = 10.

Example 3.2.2. At a recent mathematics competition, 9 mathematicians greeted each other by shaking hands. Is it possible that each mathematician shook hands with exactly 7 people at the competition?

Solution 3.2.2. It looks like this should be possible. Each mathematician chooses one person to not shake hands with. But this cannot happen. We are asking whether a graph with 9 vertices can have degree 7 for each vertex. If such a graph existed, the sum of the degrees of the vertices would be 9 x 7 = 63. This would be twice the number of edges (handshakes) resulting in a graph with 31.5 edges. That is impossible. Thus at least one (in fact an odd number) of the mathematicians must have shaken hands with an even number of people at the competition.

3.3 Euler Paths and Circuits

An Euler path, in a graph or multigraph can be defined as a walk through the graph which uses every edge exactly once. While an Euler circuit is an Euler path which starts and stops at the same vertex. The main goal here is to find a quick way to determine if a graph has an Euler path or an Euler circuit.

In summary, we can conclude the followings:

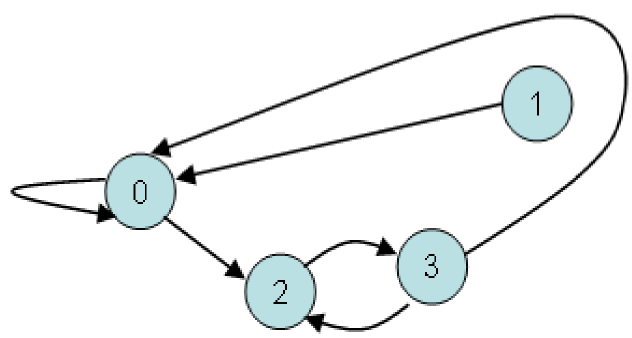
i. A graph has an Euler circuit if and only if the degree of every vertex is even.

ii. A graph has an Euler path if and only if there are at most two vertices with odd degree.

3.4 Adjacency Matrices

A graph can be represented in several different ways in a computer. It can be shown diagrammatically when the number of vertices and edges are reasonably small. Though, graphs can also be represented in the form of matrices. Thus, adjacency matrix is a square matrix used to represent a finite graph in graph theory and computer science. The element of the matrix shows whether pairs of vertices are adjacent or not in the graph. Also, directed and undirected graphs can be represented using adjacency matrices. Let $G = (V, E)$ be a graph with "n" vertices, then the $n \times n$ matrix A, in which $V = \{v_1, v_2, . . . , v_n\}$ is the vertex set, E is the edge set, $a_{ij} = 1$ is the number of edges between the vertices v_i and v_j (if there exists a path from v_i to v_j) and $a_{ij} = 0$ otherwise is called adjacency matrix.

Example 3.4.1: The adjacency matrix A_{G_1} of the directed graph G_1 is given in Figure 1.



	0	1	2	3
0	true	false	true	false
1	true	false	false	false
2	false	false	false	true
3	true	false	true	false

4.0 Conclusion

Graphs are very simple and are extremely useful mathematical objects. They are universal in the practical applications. They are made up of a collection of dots that are called vertices and lines connecting those dots that are called edges. There are directed or undirected graph.

5.0 Summary

In this unit, you have learnt that:

- Graphs useful mathematical objects
- You can use your knowledge on graph to design complex network connections

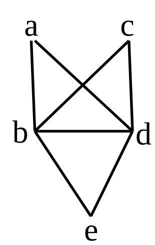
- Analyse traffic routes and determine the shortest path to any location
- Graphs are used on rating of web sites through referencing or site visits
- Two graphs are isomorphic if there is an isomorphism between them
- A graph is bipartite if the vertices can be divided into two sets

6.0 Tutor-Marked Assignment

1. Are the graphs below equal? Are they isomorphic? If they are isomorphic, give the isomorphism else state why they are not.

   $G_1 = V_1 = \{a, b, c, d, e\}$, $E_1 = \{\{a, c\}, \{a, d\}, \{a, e\}, \{b, d\}, \{b, e\}, \{c, e\}, \{d, e\}\}$

   $G_2 =$



2. Consider the following two graphs:

   G1 V1 = {a, b, c, d, e, f, g} E1 = {{a, b}, {a, d}, {b, c}, {b, d}, {b, e}, {b, f}, {c, g}, {d, e}, {e, f}, {f, g}}.

   G2 V2 = {v1, v2, v3, v4, v5, v6, v7}, E2 = {{v1, v4}, {v1, v5}, {v1, v7}, {v2, v3}, {v2, v6}, {v3, v5}, {v3, v7}, {v4, v5}, {v5, v6}, {v5, v7}}

   i. Let f: G1 → G2 be a function that takes the vertices of Graph 1 to vertices of Graph 2. The function is given by the following table:

x	a	b	c	d	e	f	g
f(x)	v4	v5	v1	v6	v2	v3	v7

   Does f define an isomorphism between Graph 1 and Graph 2?

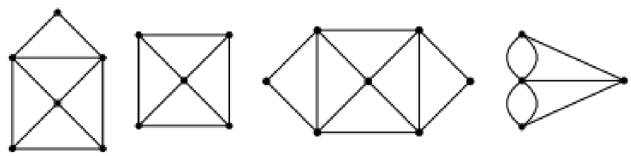
   ii. Define a new function g (with g, f) that defines an isomorphism between Graph 1 and Graph 2.

3. If 10 people each shake hands with each other, how many handshakes took place? What does this question have to do with graph theory?
4. Decide whether the statements below about subgraphs are **true** or **false**. If true in 1 or 2 sentences, explain why, else, give a counterexample if false.

i. Any subgraph of a complete graph is also complete.
ii. Any induced subgraph of a complete graph is also complete.
iii. Any subgraph of a bipartite graph is bipartite.

5.

i. Which of the graphs below have Euler paths or Euler circuits?



ii. List the degrees of each vertex of the graphs 5 i above. Is there a connection between degrees and the existence of Euler paths and circuits?
iii. Is it possible for a graph with a degree 1 vertex to have an Euler circuit? If so, draw one. If not, explain why not. What about an Euler path?
iv. What if every vertex of the graph has degree 2? Is there an Euler path or an Euler circuit? Draw some graphs.

7.0 References/Further Reading

Chiranjib, M and Gyan, M (2014). Role of Adjacency Matrix in Graph Theory, IOSR Journal Computer Engineering, 16(2): 58- 63.

Donnellan, T. (1968). Lattice Theory. Pergamon Press.

Halmos, P.(1956). The Basic Concepts of Algebraic Logic, American Mathematical Monthly vol., 53, 363–87.

Hohn, F. (1955). Some Mathematical Aspects of Switching, American Mathematical Monthly, vol., 62, 75–90.

Hohn, F. (1966). Applied Boolean Algebra. 2nd ed. Macmillan, New York.

Lidl, R. and Pilz, G. (1998). Applied Abstract Algebra. 2nd ed. Springer, New York,

Whitesitt, J. (2010). Boolean Algebra and Its Applications. Dover, Mineola, NY.

MODULE 3 MATRICES, APPLICATIONS TO COUNTING AND DISCRETE PROBABILITY

UNIT 1 MATRICES AND DETERMINANTS

CONTENTS

1.0 Introduction

In many analysis, variables are assumed to be related by sets of linear equations. Matrix algebra provides a clear and concise notation for the formulation and solution of such problems, many of which would be complicated in conventional algebraic notation. The concept of determinant is based on that of matrix.

2.0 Objectives

By the end of this Unit, you will be able to:

- compactly write and work with multiple linear equations
- discuss the concept of matrices

- explain how to perform some simple operations addition, subtraction, multiplication, determinant and transpose
- explain how to find the inverse of a matrix
- explain the business application aspect of matrices.

3.0 Main Content

3.1 MATRIX

Definition 3.1.1. A matrix is a rectangular array of numbers. A matrix with m rows and n columns is said to have dimension m × n.

Definition 3.1.2. A set of mn numbers (real or complex), arranged in a rectangular formation (array or table) having m rows and n columns and enclosed by a square bracket [ ] is called m × n matrix (read "m by n matrix") .

A matrix may be represented as follows

$$A = \begin{bmatrix} a_{11} \ a_{12} \dots a_{1n} \\ a_{21} \ a_{22} \dots a_{2n} \\ \dots \quad \dots \quad \dots \\ a_{m1} \ a_{m2} \dots a_{mn} \end{bmatrix}$$

The letters a_{ij} stand for real numbers. Note that a_{ij} is the element in the ith row and jth column of the matrix. Thus, the matrix A is sometimes denoted by simplified form as (a_{ij}) or by $\{a_{ij}\}$ i.e., $A = (a_{ij})$. Matrices are usually denoted by capital letters A, B, C etc. and its elements by corresponding small letters a, b, c etc.

Order of a Matrix: The order or dimension of a matrix is the ordered pair having as first component the number of rows and as second component the number of columns in the matrix. If there are 3 rows and 2 columns in a matrix, then its order is written as (3 × 2) or (3, 2) which is read as three by two. In general, if m are rows and n are columns of a matrix, then its order is (m × n).

Example 3.1.1.

$A = \begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}$, $B = \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}$ and $C = \begin{bmatrix} 4 & 2 & 6 \\ 2 & 1 & 3 \end{bmatrix}$.

The order of the matrices, A, B and C are (2 × 2), (3 × 1) and (2 × 3) respectively.

Definition 3.1.3. Matrices A and B are equal, A = B, if A and B have the same dimensions and each entry of A is equal to the corresponding entry of B.

3.1.1 Types of Matrices

1. **Row Matrix and Column Matrix**: A matrix consisting of a single row is called a row matrix or a row vector, whereas a matrix having single column is called a column matrix or a column vector.

2. **Null or Zero Matrix:** A matrix in which each element is „0‟ is called a Null or Zero matrix. Zero matrices are generally denoted by the symbol O. This distinguishes zero matrix from the real number 0.

For example O = $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$is a zero matrix of order 2 × 3.

The matrix O_{mxn} has the property that for every matrix A_{mxn}, A + O = O + A = A

3. **Square matrix:** A matrix A having same numbers of rows and columns is called a square matrix. A matrix A of order m × n can be written as $A_{m\times n}$. If m = n, then the matrix is said to be a square matrix. A square matrix of order n × n, is simply written as An. A = and C =.

Thus $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$ are square matrix of order 2 and 3.

3.1.2. Main or Principal Diagonal: The principal (leading) diagonal of a square matrix is the ordered set of elements a_{ij}, where i = j, extending from the upper left-hand corner to the lower right-hand corner of the matrix. Thus, the principal diagonal contains elements a_{11}, a_{22}, a_{33} etc. For example, the principal diagonal of

$$\begin{bmatrix} a & d & g \\ b & e & h \\ c & f & i \end{bmatrix}$$

consists of **a**, **e** and **i**, in that order.

3.1.3. Particular cases of a square matrix

1. **Diagonal matrix**: A square matrix in which all elements are zero except those in the main or principal diagonal is called a diagonal matrix. Some elements of the principal diagonal may be zero but not all.

For example, $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ are diagonal matrices.

In general, $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} = (a_{ij})_{nxn}$

is a diagonal matrix if and only if

$a_{ij} = 0$ for $i \neq j$, and

$a_{ij} \neq 0$ for at least one $i = j$

2. **Scalar Matrix**

A diagonal matrix in which all the diagonal elements are same, is called a scalar matrix i.e.

Thus, $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$ and $\begin{bmatrix} k & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & k \end{bmatrix}$ are scalar matrices.

3. **Identity Matrix or Unit Matrix**

A scalar matrix in which each diagonal element is 1 (unity) is called a unit matrix. An identity matrix of order n is denoted by I_n.

Thus, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ are identity matrices of the order 2 and 3 respectively.

In general, $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = (a_{ij})_{mxn}$

Is an identity matrix if and only if

$a_{ij} = 0$ for $i \neq j$, and

$a_{ij} \neq 1$ for $i = j$.

Note: If a matrix A and identity matrix I are conformable for multiplication, then I has the property that AI = IA = A i.e., I is the identity matrix for multiplication.

4. Equal Matrices

Two matrices A and B are said to be equal if and only if they have the same order and each element of matrix A is equal to the corresponding element of matrix B. this implies that for each i, j, $a_{ij} = b_{ij}$.

Thus, $I_2 = \begin{bmatrix} 2 & 1 \\ 3 & 0 \end{bmatrix}$ and $I_3 = \begin{bmatrix} \frac{4}{2} & 2-1 \\ \sqrt{9} & 0 \end{bmatrix}$

Then A = B because the order of matrices A and B is same and $a_{ij} = b_{ij}$ for every i, j.

Example 3.1.1. Find the values of x, y, z and a which satisfy the matrix equation

$$\begin{bmatrix} x+3 & 2y+x \\ z-1 & 4a-6 \end{bmatrix} = \begin{bmatrix} 0 & -7 \\ 3 & 2a \end{bmatrix}$$

Solution 3.1.1. By the definition of equality of matrices, we have:

x + 3 = 0 ……………………………(1)
2y + x = -7 ………………………….(2)
z – 1 = 3 …………………………….(3)
4a – 6 = 2a ………………………….(4)

i. From (1) x = -3,
ii. Put the value of x in (2), we get y = -2,
iii. From (3) z = 4,
iv. From (4) a = 3

5. The Negative of a Matrix

The negative of the matrix A_{mxn}, denoted by $-A_{mxn}$, is the matrix formed by replacing each element in the matrix A_{mxn} with its additive inverse. For example,

If $A_{3x2} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$

Then $A_{3x2} = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}$

for every matrix A_{mxn}, the matrix $-A_{mxn}$ has the property that

A + (-A) = (-A) + A = 0

i.e., (-A) is the additive inverse of A.

The sum $B_{m-n} + (-A_{mxn})$ is called the difference of B_{mxn} and A_{mxn} and is denoted by $B_{mxn} – A_{mxn}$.

3.1.4. Operations on Matrices

1. Multiplication of a Matrix by a Scalar: If A is a matrix and k is a scalar (constant), then kA is a matrix whose elements are the elements of A, each multiplied by k.

For example, if , $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix}$ then for a scalar k,

$$\text{k}A = \begin{bmatrix} k & 2k & 3k \\ 2k & 4k & 6k \\ 3k & 6k & 9k \end{bmatrix}$$

Example 3.3.1. From A given, determine 3A.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix}$$

$$3A = 3\begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 3 & 6 & 9 \end{bmatrix} = \begin{bmatrix} 3 & 6 & 9 \\ 6 & 12 & 16 \\ 9 & 18 & 27 \end{bmatrix}$$

2. Addition and subtraction of Matrices: If A and B are two matrices of same order m × n then their sum A + B is defined as C, m × n matrix such that each element of C is the sum of the corresponding elements of A and B. For example,

Let $A = \begin{bmatrix} 2 & 9 \\ 5 & 6 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 5 \\ 3 & 2 \end{bmatrix}$.

Then, C = A + B = $\begin{bmatrix} 2+1 & 9+(\ 5) \\ 5+3 & 6+2 \end{bmatrix}$ = $\begin{bmatrix} 3 & 4 \\ 8 & 4 \end{bmatrix}$

Similarly, the difference A – B of the two matrices A and B is a matrix each element of which is obtained by subtracting the elements of B from the corresponding elements of A.

Then, D = A - B = $\begin{bmatrix} 2-1 & 9-(\ 5) \\ 5-3 & 6-2 \end{bmatrix}$ = $\begin{bmatrix} 1 & 14 \\ 3 & 8 \end{bmatrix}$

If A, B and C are the matrices of the same order m × n then,

A + B = B + A and (A + B) + C = A + (B + C) i.e., the addition of matrices is commutative and associative respectively.

Note: The sum or difference of two matrices of different order is not defined. For example, the sum or difference of a matrices with orders (3×2) and (2×2) is not defined.

3. Product of Matrices: Two matrices A and B are said to be conformable for the product AB if the number of columns of A is equal to the number of rows of B. Then the product matrix AB has the same number of rows as A and the same number of columns as B.

Thus the product of the matrices A_{mxp} and B_{pxn} is the matrix $(AB)_{mxn}$. The elements of AB are determined as follows:

The element C_{ij} in the ith row and jth column of $(AB)_{mxn}$ is found by

$c_{ij} = a_{i1}b_{1j} + ai_{2b2j} + a_{i3}b_{3j} + \ldots\ldots\ldots + a_{in}b_{nj}$

For example, let's consider the matrices:

$$A_{2x2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \text{ and } B_{2x2} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

Since the number of columns of A is equal to the number of rows of B, the product AB is defined and is given as

$$AB = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{12}\,b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}$$

Thus c_{11} is obtained by multiplying the elements of the first row of A i.e., a_{11}, a_{12} by the corresponding elements of the first column of B i.e., b_{11}, b_{21} and adding the product. Similarly, c_{12} is obtained by multiplying the elements of the first row of A i.e., a_{11}, a_{12} by the corresponding elements of the second column of B i.e., b_{12}, b_{22} and adding the product. Similarly, for c_{21}, c_{22}. Note:

i. Multiplication of matrices is not commutative i.e., $AB \neq BA$ in general. 2.

ii. For matrices A and B if $AB = BA$ then A and B commute to each other.

iii. A matrix A can be multiplied by itself if and only if it is a square matrix. The product A × A, in such cases is written as A^2. Similarly, we may define higher powers of a square matrix i.e., $A \times A^2 = A^3$, $A^2 \times A^2 = A^4$.

iv. In the product AB, A is said to be pre multiple of B and B is said to be post multiple of A.

Example 3.1.2. If $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, find AB and BA.

Solution 3.1.2.

$$AB = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1.2 + 2.1 & 1.1 + 2.1 \\ 1.2 + 3.1 & 1.1 + 3.1 \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$

$$BA = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 2.1 + 1.\ 1 & 2.2 + 1.3 \\ 1.1 + 1.\ 1 & 1.2 + 1.3 \end{bmatrix}$$

$$= \begin{bmatrix} 2 - 1 & 4 + 3 \\ 1 - 1 & 2 + 3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 7 \\ 0 & 5 \end{bmatrix}$$

Exercise 3.1.2 clearly shows that multiplication of matrices in general, is not commutative i.e., AB ≠ BA.

Example 3.1.3. If $A = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 2 & 1 \\ 3 & 1 \end{bmatrix}$, find AB

Solution 3.1.3. Since A is a (2 × 3) matrix and B is a (3 × 2) matrix, they are conformable for multiplication. We have

$$AB = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 2 & 1 \\ 3 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 3.1 + 1.2 + 2.3 & 3.\ 1 + 1.1 + 2.1 \\ 1.1 + 0.2 + 1.3 & 1.\ 1 + 0.1 + 1.1 \end{bmatrix}$$

$$= \begin{bmatrix} 3 + 3 + 6 & 3 + 1 + 2 \\ 1 + 0 + 3 & 1 + 0 + 1 \end{bmatrix}$$

$$= \begin{bmatrix} 11 & 0 \\ 4 & 0 \end{bmatrix}$$

Remarks:

If A, B and C are the matrices of order (m × p), (p × q) and (q × n) respectively, then,

i. Associative law: (AB)C = A(BC).

ii. Distributive law: C (A + B) = CA + CB and (A + B) C = AC + BC.

3.2 Determinant

The determinant of a matrix is a scalar (number), obtained from the elements of a matrix by specified, operations, which is characteristic of the matrix. The determinants are defined only for square matrices. Determinant is denoted by det (A) or |A| for a square matrix A.

Determinant of a 2 × 2 matrix: Given the matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, then

$$|A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

$$= |\ a_{11}a_{22} - a_{21}a_{12}|$$

Example 3.2.1. If $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$, find |A|.

Solution 3.2.1.

$$|A| = \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix} = |1.3 - (\ 1.2)| = |3 + 2| = 5$$

Determinant of a 3 × 3 matrix: Given the matrix $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, then

$$|A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

$$= a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{12}\ (a_{21}a_{33} - a_{31}a_{23}) + a_{13}\ (a_{21}a_{32} - a_{31}a_{22})$$

These determinants are called minors. We take the sign + or – , according to $(-1)^{i+j}\ a_{ij}$ Where i and j represent row and column.

3.2.1. Minor and Cofactor of Element

The minor M_{ij} of the element a_{ij} in a given determinant is the determinant of order (n – 1 × n – 1) obtained by deleting the ith row and jth column of A_{nxn}. For example, in the determinant

$$|A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

i. The minor of the element a_{11} is $M_{11} = \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}$

ii. The minor of the element a_{12} is $M_{12} = \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix}$

iii. The minor of the element a_{13} is $M_{13} = \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$ and so on.

The scalars $C_{ij} = (-1)^{i+j} M_{ij}$ are called the cofactor of the element a_{ij} of the matrix A.

The value of the determinant in equation (1) can also be found by its minor elements or cofactors, as

$a_{11}M_{11} – a_{12}M_{12} + a_{13}M_{13}$

Or

$a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13}$.

Hence, the |A| is the sum of the elements of any row or column multiplied by their corresponding cofactors. The value of the determinant can be found by expanding it from any row or column.

Example 3.2.3. If $A = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 3 & 4 \end{bmatrix}$ find |A| by expansion about (a) the first row (b) the first column. **Solution 3.2.3. (a)** Using the first row

$$|A| = \begin{vmatrix} 3 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 3 & 4 \end{vmatrix}$$

$$= 3\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} - 2\begin{vmatrix} 0 & 2 \\ 1 & 4 \end{vmatrix} + 1\begin{vmatrix} 0 & 1 \\ 1 & 3 \end{vmatrix}$$

= 3(1.4 – (-2).3) -2(0.4 – 1. -2) +1(0.3 – 1.1)

= 3(4+6) -2(0+2) +1(0-1)

= 30 – 4 – 1

= 25

Solution 3.2.3. (b) Using the first column

$$|A| = \begin{vmatrix} 3 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 3 & 4 \end{vmatrix}$$

$$= 3\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} - 0\begin{vmatrix} 2 & 1 \\ 3 & 4 \end{vmatrix} + 1\begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix}$$

= 3(1.4 – (-2).3) - 0(2.4 – 3.1) +1(2.-2 – 1.1)

= 3(4+6) - 0(8 - 2) +1(-4 - 1)

= 30 – 0 – 5

= 25

3.3. Special Matrices

1. Transpose of a Matrix

If A = $[a_{ij}]$ is m × n matrix, then the matrix of order n × m obtained by interchanging the rows and columns of A is called the transpose of A. It is denoted A^t or A′. For example,

if $A = \begin{bmatrix} 3 & 2 & 1 \\ 0 & 1 & 2 \\ 1 & 3 & 4 \end{bmatrix}$ then, $A^t = \begin{bmatrix} 3 & 0 & 1 \\ 2 & 1 & 3 \\ 1 & 2 & 4 \end{bmatrix}$

2. Symmetric Matrix

A square matrix A is called symmetric if A = A^t. For example,

if $C = \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 3 \\ 1 & 3 & 0 \end{bmatrix}$ then, $C^t = \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 3 \\ 1 & 3 & 0 \end{bmatrix} = C$

3. Skew Symmetric

A square matrix A is called skew symmetric if A = $-A^t$. For example,

If $C = \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 3 \\ 1 & 3 & 0 \end{bmatrix}$ then,

$C^t = \begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 3 \\ 1 & 3 & 0 \end{bmatrix} = (\ 1)\begin{bmatrix} 0 & 4 & 1 \\ 4 & 0 & 3 \\ 1 & 3 & 0 \end{bmatrix}$

$C^t = -C$. Thus matrix C is skew symmetric.

4. Singular and Non-singular Matrices

A square matrix A is called singular if |A| = 0 and is non-singular if |A| ≠ 0, for example if t

$A = \begin{bmatrix} 1 & 3 \\ 1 & 3 \end{bmatrix}$ then,

$|A| = \begin{vmatrix} 1 & 3 \\ 1 & 3 \end{vmatrix} = |1.3 - (1.3)| = |3 - 3| = 0$

Then, |A| = 0, Hence A is singular.

5. Adjoint of a Matrix

Let A = (a_{ij}) be a square matrix of order n × n and (c_{ij}) is a matrix obtained by replacing each element a_{ij} by its corresponding cofactor c_{ij} then $(c_{ij})^t$ is called the adjoint of A. It is written as Adj (A).

Example 3.1.4. If $A = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 3 & 1 \\ 0 & 1 & 2 \end{bmatrix}$, find the cofactor matrix of A

Solution 3.1.4. The cofactors of A are:

$C_{11} = (-1)^{1+1} \begin{vmatrix} 3 & 1 \\ 1 & 2 \end{vmatrix} = 5$; $C_{12} = (-1)^{1+2} \begin{vmatrix} 1 & 1 \\ 0 & 2 \end{vmatrix} = -2$; $C_{13} = (-1)^{1+3} \begin{vmatrix} 1 & 3 \\ 0 & 1 \end{vmatrix} = 1$

$C_{21} = (-1)^{2+1} \begin{vmatrix} 0 & -1 \\ 1 & 2 \end{vmatrix} = -1$; $C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & -1 \\ 0 & 2 \end{vmatrix} = 2$; $C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = -1$

$C_{31} = (-1)^{3+1} \begin{vmatrix} 0 & -1 \\ 3 & 1 \end{vmatrix} = 3$; $C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = -2$; $C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 0 \\ 1 & 3 \end{vmatrix} = 3$

The matrix of cofactors of A will be, C:

$$C = \begin{bmatrix} 5 & -2 & 1 \\ -1 & 2 & -1 \\ 3 & -2 & 3 \end{bmatrix}$$

$$C^t = \begin{bmatrix} 5 & -1 & 3 \\ -2 & 2 & -2 \\ 1 & -1 & 3 \end{bmatrix}$$

Therefore, Adj (A) = C^t

Adjoint of a 2×2 Matrix

The adjoint of matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is denoted by Adj (A) and is defined as:

$$Adj\ (A) = \begin{bmatrix} d & -a \\ -c & b \end{bmatrix}$$

6. Inverse of a Matrix

If A is a non-singular square matrix then, $A^{-1} = \frac{adj\ (A)}{|A|}$

2×2 Matrix

Example 3.1.5. If $A = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$, find A^{-1}.

Solution 3.1.5.

$$|A| = \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix} = |1.3 - (1.2)| = |3 - 2| = 1$$

$$\text{Adj (A)} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$$

$$A^{-1} = \frac{adj\ (A)}{|A|} = \frac{1}{1}\begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$$

Alternately: For a non-singular matrix A of order (n × n) if there exist another matrix B of order (n × n) such that their product is the identity matrix I of order (n × n) i.e., AB = BA = I.

Then B is said to be the inverse (or reciprocal) of A and is written as $B = A^{-1}$.

Example 3.1.6. If $A = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix}$ and $B = \begin{bmatrix} 7 & 3 \\ 2 & 1 \end{bmatrix}$. Show that AB = BA = I then, $B = A^{-1}$.

Solution 3.1.6.

$$AB = \begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix}\begin{bmatrix} 7 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$BA = \begin{bmatrix} 7 & 3 \\ 2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 2 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Example 3.1.7. If $A = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 3 & 3 \\ 1 & 2 & 2 \end{bmatrix}$

Solution 3.1.7.

|A| = 0 +2 (–2 +3) – 3(–2 + 3) = 2 – 3

|A| = –1, Hence solution exists.

Cofactor of A are:

$C_{11} = 0$; $C_{12} = -1$; $C_{13} = 1$

$C_{21} = 2$; $C_{22} = -3$; $C_{23} = 2$

$C_{31} = 3$; $C_{32} = -3$; $C_{33} = 2$

The matrix of cofactors of A is:

$$C = \begin{bmatrix} 0 & 1 & 1 \\ 2 & 3 & 2 \\ 3 & 3 & 2 \end{bmatrix}$$

The transpose of C is:

$$C^t = \begin{bmatrix} 0 & 2 & 1 \\ -1 & 3 & 3 \\ 1 & 2 & 2 \end{bmatrix} = Adj\ (A)$$

So,

$$A^{-1} = \frac{1}{|A|} adj\ (A) = \frac{1}{-1} \begin{bmatrix} 0 & 2 & 1 \\ 1 & 3 & 3 \\ 1 & 2 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 2 & 1 \\ 1 & 3 & 3 \\ 1 & 2 & 2 \end{bmatrix}$$

7. Solution of Linear Equations by Matrices

For a linear system:

$a_{11}x_1 + a_{12}x_2 +$ ------ $+ a_{1n}x_n = b_1$

$a_{21}x_1 + a_{22}x_2 +$ ------ $+ a_{2n}x_n = b_2$………………………….. (1)

| | | |

$a_{n1}x_1 + a_{n2}x_2 +$ ------ $+ a_{nn}x_n = b_n$

It can be written as the matrix equation:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Let $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}, X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$ and $B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$.

The equation can be written as, AX = B.

If $B \neq 0$, then (1) is called **non-homogenous** system of linear equations and if $B = 0$, it is called a system of **homogenous linear equations**.

If now $B \neq 0$ and A is non-singular then A^{-1} exists.

Multiply both sides of $AX = B$ on the left by A^{-1}, we get

$$A^{-1}(AX) = A^{-1}B$$

$$(A^{-1}A)\, X = A^{-1}B$$

$$1X = A^{-1}B$$

$$\text{Or} \qquad X = A^{-1}B$$

Where $A^{-1}B$ is an $n \times 1$ column matrix. Since X and $A^{-1}B$ are equal, each element in X is equal to the corresponding element in $A^{-1}B$. These elements of X constitute the solution of the given linear equations.

If A is a singular matrix, then of course it has no inverse, and either the system has no solution or the solution is not unique.

Example 3.1.8. Use matrices to find the solution set of

$$x + y - 2z = 3$$
$$3x - y + z = 5$$
$$3x + 3y - 6z = 9$$

Solution 3.1.8.

$$A = \begin{bmatrix} 1 & 1 & 2 \\ 3 & 1 & 1 \\ 3 & 3 & 6 \end{bmatrix}$$

$$|A| = 3 + 21 - 24 = 0$$

Since $|A| = 0$, the solution of the given linear equations does not exist.

Example 3.1.9. Use matrices to find the solution set of

$$4x + 8y + z = -6$$
$$2x - 3y + 2z = 0$$
$$x + 7y - 3z = -8$$

Solution 3.1.9.

$$A = \begin{bmatrix} 4 & 8 & 1 \\ 2 & 3 & 2 \\ 1 & 7 & 3 \end{bmatrix}$$

$$|A| = -32 + 48 + 17 = 61$$

Since $|A| \neq 0$ then, A^{-1} exists.

$$A^{-1} = \frac{1}{|A|} adj\,(A) = \frac{1}{61}\begin{bmatrix} 5 & 31 & 19 \\ 8 & 13 & 16 \\ 17 & 20 & 28 \end{bmatrix}$$

Now since,

X = A^{-1}B, we have

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{61}\begin{bmatrix} 5 & 31 & 19 \\ 8 & 13 & 16 \\ 17 & 20 & 28 \end{bmatrix}\begin{bmatrix} 6 \\ 0 \\ 8 \end{bmatrix}$$

$$= \frac{1}{61}\begin{bmatrix} 30 + 152 \\ 48 + 48 \\ 102 + 224 \end{bmatrix}\begin{bmatrix} 2 \\ 0 \\ 2 \end{bmatrix}$$

Hence solution set: {(x, y, z)} = {$(\ 2, 0, 2)$}.

4.0 Conclusion

A matrix is a rectangular array of numbers with m rows and n columns. Matrix algebra provides a clear and concise notation for the formulation and solution of some problems. There are different types of matrices: row, column, null, square, diagonal, upper triangular, lower triangular, symmetric and antisymmetric matrix. Different operations are carried out on matrices which include: addition, subtraction, multiplication, determinant and inverse.

5.0 Summary

In this unit, you are have learnt how to write and work with multiple linear equations.

- Understand the concept of matrices
- Know how to perform some simple operations addition, subtraction, multiplication, determinant and transpose
- Know how to find the inverse of a matrix

6.0 Tutor-Marked Assignment

1. Write the following matrices in tabular form:
   a. A = [a_{ij}], where i = 1, 2, 3 and j = 1, 2, 3, 4
   b. B = [b_{ij}], where i = 1 and j = 1, 2, 3, 4
   c. C = [c_{jk}], where j = 1, 2, 3 and k = 1
2. Show that if $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$ then,

a. $(A + B)(A + B) \neq A^2 + 2AB + B^2$

b. $(A + B)(A - B) \neq A^2 - B^2$

3. Write each product as a single matrix

a. $\begin{bmatrix} 3 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 0 & 2 \\ 1 & 1 \end{bmatrix}$

b. $\begin{bmatrix} 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}$

c. $\begin{bmatrix} 3 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 2 & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

4. If $A = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 3 & 0 \\ 1 & 2 \end{bmatrix}$ and $= \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}$, find

a. $CB + A^2$

b. $B^2 + AC$

c. kABC, where k = 2.

5. Find K such that the following matrices are singular

a. $\begin{bmatrix} K & 6 \\ 4 & 3 \end{bmatrix}$

b. $\begin{bmatrix} 1 & 2 & -1 \\ -3 & 4 & K \\ -4 & 2 & 6 \end{bmatrix}$

c. $\begin{bmatrix} 1 & 1 & -2 \\ 3 & -1 & 1 \\ K & 3 & -6 \end{bmatrix}$

6. Find the solution set of the following system by means of matrices:

a. $2x - 3y = -1$
$x + 4y = 5$

b. $x + y = 2$
$2x - z = 1$
$2y - 3z = -1$

c. $x - 2y + z = -1$
$3x + y - 2z = 4$
$y - z = 1$

d. $-4x + 2y - 9z = 2$
$3x + 4y + z = 5$
$x - 3y + 2z = 8$

e. $x + y - 2z = 3$
$3x - y + z = 0$
$3x + 3y - 6z = 8$

7.0 References/Further Reading

Deitel, H. M. and Deitel, P. J. (1998). C++ How to Programme (2nd Edition), New Jersey: Prentice Hall.

French, C. S. (1992). Computer Science, DP Publications. (4th Edition), 199-217.

Shaffer, Clifford A. A. (1998). Practical Introduction to Data Structures and Algorithm Analysis, Prentice Hall, pp. 77-102.

UNIT 2 APPLICATIONS TO COUNTING

CONTENTS

1.0 Introduction

Counting is a basic mathematical tool that has uses in many diverse circumstances. How much RAM can a 32-bit register address? How many poker hands form full houses compared to flushes? How many ways can ten-coin tosses end up with four heads? To count, we can always take the time to enumerate all the possibilities; but even just enumerating all poker hands is already daunting, let alone all 32-bit addresses. This unit discusses some techniques that serve as useful shortcuts for counting.

2.0 Objectives

By the end of this unit, you will be able to:

- apply product and sum rules
- discuss permutation and combination
- use Pascal's triangle to expand a binomial expression
- identify and apply inclusion-exclusion and pigeonhole principle.

3.0 Main Content

3.1 The Product and Sum Rules

The product and sum rules represent the most intuitive notions of counting. Suppose there are n(A) ways to perform task A, and regardless of how task A is performed, there are n(B) ways to perform task B.

Then, there are $n(A) \times n(B)$ ways to perform both task A and task B; this is the **product rule**. This can generalize to multiple tasks, e.g., $n(A) \times n(B) \times n(C)$ ways to perform task A, B, and C, as long as the independence condition holds, e.g., the number of ways to perform task C does not depend on how task A and B are done.

Example 3.1.1. On an 8×8 chess board, how many ways can I place a pawn and a rook?

Example 3.1.1. 1. First I can place the pawn anywhere on the board; there are 64 ways. Then I can place the rook anywhere except where the pawn is; there are 63 ways. In total, there are $64 \times 63 = 4032$ ways.

Example 3.1.2. On an 8×8 chess board, how many ways can I place a pawn and a rook so that the rook does not threaten the pawn?

Solution 3.1.2. Firstly, I can place the rook anywhere on the board; there are 64 ways. At the point, the rook takes up on square, and threatens 14 others (7 in its row and 7 in its column). Therefore, I can then place the pawn on any of the $64 - 14 - 1 = 49$ remaining squares. In total, there are $64 \times 49 = 3136$ ways.

Example 3.1.3. If a finite set A has n elements, then $|P(A)| = 2^n$.

Solution 3.1.3. We can proof this by using the product rule. P(A) is the set of all subsets of A. To form a subset of A, each of the n elements can either be in the subset or not (2 ways). Therefore, there are 2^n possible ways to form unique subsets, therefore, $|P(A)| = 2^n$.

Example 3.1.4. How many legal configurations are there in the towers of Hanoi?

Solution 3.1.4. Each of the n rings can be on one of three poles, giving us 3^n configurations. Normally we would also need to count the height of a ring relative to other rings on the same pole, but in the case of the towers of Hanoi, the rings sharing the same pole must be ordered in a unique fashion: from small at the top to large at the bottom.

The **sum rule** is probably even more intuitive than the product rule. Suppose there are n(A) ways to perform task A, and distinct from these, there are n(B) ways to perform task B. Then, there are $n(A) + n(B)$ ways to perform task A or task B. This can generalize to multiple tasks, e.g., $n(A) + n(B) + n(C)$ ways to perform task A, B, or C, as long as the distinct condition holds, e.g., the ways to perform task C are different from the ways to perform task A or B.

Example 3.1.5. To fly from Lagos to Brisbane you must fly through Istanbul or Dubai.

Solution 3.1.5. There are 5 such flights a day through Istanbul, and 3 such flights a day through Dubai. How many different flights are there in a day that can take you from Lagos to get to Brisbane? The answer is 5 + 3 = 8.

Example 3.1.6. How many 4- to 6-digit pin codes are there?

Solution 3.1.6. By the product rule, the number of distinct n digit pin codes is 10^n (each digit has 10 possibilities). By the sum rule, we have 104 + 105 + 106 number of 4- to 6-digit pin codes (to state the obvious, we have implicitly used the fact that every 4-digit pin code is different from every 5-digit pin code).

3.2 Permutations and Combinations

Permutations and combinations are also tools for counting. Given n distinct objects, how many ways are there to "choose" r of them? Well, it depends on whether the r chosen objects are ordered or not. For example, suppose we deal three cards out of a standard 52-card deck. If we are dealing one card each to Alice, Bob and Cathy, then the order of the cards being dealt matters; this is called a **permutation** of 3 cards. On the other hand, if we are dealing all three cards to Alice, then the order of the cards being dealt does not matter; this is called a **combination** of 3 cards.

3.2.1. Permutations

Definition 3.2.1.1. A permutation of a set A is an ordered arrangement of the elements in A. An ordered arrangement of just r elements from A is called an r-permutation of A. For non-negative integers $r \leq n$, P(n, r) denotes the number of r-permutations of a set with n elements.

What is P(n, r)? To form an r-permutation from a set A of n elements, we can start by choosing any element of A to be the first in our permutation; there are n possibilities. The next element in the permutation can be any element of A except the one that is already taken; there are n−1 possibilities. Continuing the argument, the final element of the permutation will have n − (r − 1) possibilities. Applying the product-rule, we have:

Theorem 3.2.1. $P(n, r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$ ……………. (1)

Note that 0! = 1.

Example 3.2.1.1. How many one-to-one functions are there from a set A with m elements to a set B with n elements?

Solution 3.2.1.1. If m > n we know there are no such one-to-one functions. If m ≤ n, then each one-to-one function f from A to B is a m-permutation of the elements of B: we choose m elements from B in an ordered manner (e.g., first chosen element is the value of f on the first element in A). Therefore there are P(n, m) such functions.

3.2.2. Combinations

Considering unordered selections.

Definition 4.10. An unordered arrangement of r elements from a set A is called an r-combination of A. For non-negative integers r ≤ n, C(n, r) or $\binom{n}{r}$ denotes the number of r-combinations of a set with n elements. C(n, r) is also called the binomial coefficients (we will soon see why).

For example, how many ways are there to put two pawns on a 8 × 8 chess board? We can select 64 possible squares for the first pawn, and 63 possible remaining squares for the second pawn. But now we are over counting, e.g., choosing squares (b5, c8) is the same as choosing (c8, b5) since the two pawns are identical. Therefore, we divide by 2 to get the correct count: 64 × 63/2 = 2016. More generally,

Theorem 3.2.2.

$$C(n, r) = \frac{n!}{(n-r)!r!}$$

Proof. Let us express P(n, r) in turns of C(n, r). It must be that P(n, r) = C(n, r)P(r, r), because to select an r-permutation from n elements, we can first selected an unordered set of r elements, and then select an ordering of the r elements. Rearranging the expression gives:

$$C(n, r) = \frac{P(n,r)}{P(r,r)} = \frac{n!/(n-r)!}{r!} = \frac{n!}{(n-r)!r!}$$

Example 3.2.2.1. How many poker hands (i.e., sets of 5 cards) can be dealt from a standard deck of 52 cards?

Solution 3.2.2.1. Exactly C(52, 5) = 52!/(47!5!).

Example 3.2.2.2. How many full houses (3 of a kind and 2 of another) can be dealt from a standard deck of 52 cards?

Solution 3.2.2.2. We have 13 denominations (ace to king), and 4 suites (spades, hearts, diamonds and clubs). To count the number of full houses, we may

i. First pick a denomination for the "3 of a kind": there are 13 choices.
ii. Pick 3 cards from this denomination (out of 4 suites): there are C(4, 3) = 4 choices.
iii. Next pick a denomination for the "2 of a kind": there are 12 choices left (different from the "3 of a kind").
iv. Pick 2 cards from this denomination: there are C(4, 2) = 6 choices.

So in total there are $13 * 4 * 12 * 6 = 3744$ possible full houses.

3.3 Combinatorial Identities

There are many identities involving combinations. These identities are fun to learn because they often represent different ways of counting the same thing; 66 counting one can also prove these identities by churning out the algebra, but that is boring. We start with a few simple identities.

Lemma 3.1. If $0 \leq k \leq n$, then C(n, k) = C(n, n − k).

Proof. Each unordered selection of k elements has a unique complement: an unordered selection of n − k elements. So instead of counting the number of selections of k elements from n, we can count the number of selections of n−k elements from n (e.g., to deal 5 cards from a 52 card deck is the same as to throw away 52 − 5 = 47 cards).

An algebraic proof of the same fact (without much insight) goes as follows:

$$C(n, r) = \frac{n!}{(n-k)!k!} = \frac{n!}{(n-(n-k))!(n-k)!} = C(n, n-k)$$

Lemma 3.2. (Pascal's Identity). If $0 < k \leq n$, then $C(n + 1, k) = C(n, k - 1) + C(n, k)$.

Proof. Here is another way to choose k elements from n + 1 total element. Either the n + 1st element is chosen or not:

i. If it is, then it remains to choose $k-1$ elements from the first n elements.

ii. If it isn't, then we need to choose all k elements from the first n elements.

By the sum rule, we have $C(n + 1, k) = C(n, k - 1) + C(n, k)$.

Pascal's identity, along with the initial conditions $C(n, 0) = C(n, n) = 1$, gives a recursive way of computing the binomial coefficients $C(n, k)$. The recursion table is often written as a triangle, called Pascal's Triangle; as shown in Figure 3.1.

Lemma 3.3. $\sum_{k=0}^{n} C(n, k) = 2^n$.

Proof. Let us once again count the number of possible subsets of a set of n elements. We have already seen by induction and by the product rule that there are 2n such subsets; this is the RHS.

Another way to count is to use the sum rule:

No of subsets = $\sum_{k=0}^{n}$ No of subsets of size k $= \sum_{k=0}^{n} C(n, k)$ This is the LHS.

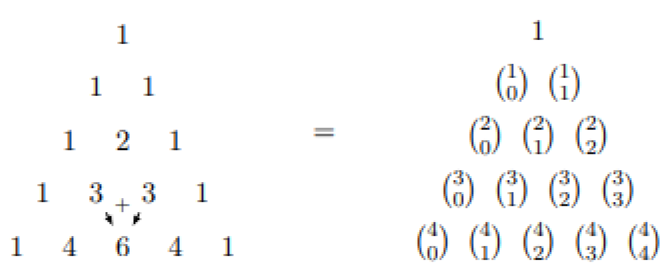


Figure 3.1. Pascal's triangle contains the binomial coefficients C(n, k) ordered as shown in the figure. Each entry in the figure is the sum of the two entries on top of it (except the entries on the side which are always 1).

Theorem 3.3.1. (The Binomial Theorem). For $n \in \mathbb{N}$,

$$(x + y)^n \sum_{k=0}^{n} C(n,k)x^{n-k}y^k$$

Proof. If we manually expand $(x + y)^n$, we would get 2^n terms with coefficient 1 (each term corresponds to choosing x or y from each of the n factors). If we then collect these terms, how many of them have the form $x^{n-k} y^k$? Terms of that form must chooses n−k many x's, and k many y's. Because just choosing the k many y's specifies the rest to be x's, there are C(n, k) such terms.

Exercise 3.3.1. What is the coefficient of $x^{13}y^7$ in the expansion of $(x-3y)^{20}$? We write $(x - 3y)^{20}$ as $(x + (-3y))^{20}$ and apply the binomial theorem, which gives us the term: $C(20, 7)x^{13}(-3y)^7 = -3\ 7C(20, 7)x^{13}y^7$.

If we substitute specific values for x and y, the binomial theorem gives us more combinatorial identities as corollaries.

Corollary 3.1. $\sum_{k=0}^{n} C(n,k) = 2^n$, again.

Proof. Simply write $2n = (1+1)^n$ and expand using the binomial theorem.

Corollary 3.2. $\sum_{k=1}^{n}(-1)^{k+1} C(n,k) = 1$.

Proof. Expand $0 = 0^n = (1 - 1)^n$ using the binomial theorem:

$$0 = \sum_{k=0}^{n} C(n,k)1^{n-k} (-1)^k$$
$$= C(n,0) + \sum_{k=1}^{n}(-1)^k\ C(n,k)$$

Rearranging terms gives us:

$$C(n,0) = -\sum_{k=1}^{n}(-1)^k\ C(n,k) = \sum_{k=1}^{n}(-1)^{k+1}C(n,k)$$

This proves the corollary since C(n, 0) = 1.

3.3.1 Using Pascal's triangle to expand a binomial expression

Let's now see how useful the triangle can be when we want to expand a binomial expression. Consider the binomial expression a + b, and suppose we wish to find $(a + b)^2$. We know that

$$(a + b)^2 = (a + b)(a + b)$$
$$= a^2 + ab + ba + b^2$$

$$= a^2 + 2ab + b^2$$

That is,

$$(a + b)^2 = 1a^2 + 2ab + 1b^2$$

Observe the following in the final result:

1. As we move through each term from left to right, the power of a decreases from 2 down to zero.
2. The power of b increases from zero up to 2.
3. The coefficients of each term, (1, 2, 1), are the numbers which appear in the row of Pascal's triangle beginning 1,2.
4. The term 2ab arises from contributions of 1ab and 1ba, i.e. 1ab + 1ba = 2ab. This is the link with the way the 2 in Pascal's triangle is generated; i.e. by adding 1 and 1 in the previous row.

If we want to expand $(a + b)^3$ we select the coefficients from the row of the triangle beginning 1,3: these are 1,3,3,1. We can immediately write down the expansion by remembering that for each new term we decrease the power of a, this time starting with 3, and increase the power of b. So,

$$(a + b)^3 = 1a^3 + 3a^2b + 3ab^2 + 1b^3$$

which we would normally write as just

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Thinking of $(a + b)^3$ as

$$(a + b)(a^2 + 2ab + b^2) = a^3 + 2a^2b + ab^2 + ba^2 + 2ab^2 + b^3$$

$$= a^3 + 3a^2b + 3ab^2 + b^3$$

we note that the term $3ab^2$, for example, arises from the two terms ab^2 and $2ab^2$; again this is the link with the way 3 is generated in Pascal's triangle - by adding the 1 and 2 in the previous row.

Example 3.3.2. Suppose we wish to find $(a + b)^4$.

Solution 3.3.2. To find this we use the row beginning 1,4, and can immediately write down the expansion. $(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab3 + b^4$.

Example 3.3.3. Suppose we want to expand $(2x + y)^3$.

Solution 3.3.3. We pick the coefficients in the expansion from the relevant row of Pascal's triangle: (1,3,3,1). As we move through the terms in the expansion from left to right we remember to decrease the power of 2x and increase the power of y. So,

$$(2x + y)^3 = 1(2x)^3 + 3(2x)^2y + 3(2x)^1y^2 + 1y^3$$

$$= 8x^3 + 12x^2y + 6xy^2 + y^3$$

Example 3.3.4. Let's expand $\left(1 + \frac{2}{x}\right)^3$.

Solution 3.3.4. We pick the coefficients in the expansion from the row of Pascal's triangle (1,3,3,1). Powers of 2 x increase as we move left to right. Any power of 1 is still 1.

$$\left(1 + \frac{2}{x}\right)^3 = 1(1)^3 + 3(1)^2\left(\frac{2}{x}\right) + 3(1)^1\left(\frac{2}{x}\right)^2 + 1\left(\frac{2}{x}\right)^3$$

$$= 1 + \frac{6}{x} + \frac{12}{x^2} + \frac{8}{x^3}$$

3.4 Inclusion-Exclusion Principle

Some counting problems simply do not have a closed form solution. In this section we discuss a counting tool that also does not give a closed form solution. The inclusion-exclusion principle can be seen as a generalization of the sum rule.

Suppose there are n(A) ways to perform task A and n(B) ways to perform task B, how many ways are there to perform task A or B, if the methods to perform these tasks are not distinct? We can cast this as a set cardinality problem. Let X be the set of ways to perform A, and Y be the set of ways to perform B. Then:

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

This can be observed using the Venn Diagram. The counting argument goes as follows: To count the number of ways to perform A or B ($|X \cup Y|$) we start by adding the number of ways to perform A (i.e., $|X|$) and the number of ways to perform B (i.e., $|Y|$). But if some of the ways to perform A and B are the same ($|X \cap Y|$), they have been counted twice, so we need to subtract those.

Example 3.4.1. How many positive integers ≤ 100 are multiples of either 2 or 5?

Solution 3.4.1. Let A be the set of multiples of 2 and B be the set of multiples of 5. Then $|A| = 50$, $|B| = 20$, and $|A \cap B| = 10$ (since this is the number of multiples of 10). By the inclusion-exclusion principle, we have 50 + 20 − 10 = 60 multiples of either 2 or 5.

What if there are more tasks? For three sets, we can still gleam from the Venn diagram that

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$$

More generally,

Theorem 3.4.1. Let $A_1, \ldots, A_n$ be finite sets. Then,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{I, I \subseteq \{1,\ldots,n\}, |I|=k} \left|\bigcap_{i \in I} A_i\right| = \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{k+1} \left|\bigcap_{i \in I} A_i\right|$$

Proof. Consider some $x \in \bigcup_i A_i$. We need to show that it gets counted exactly one in the RHS. Suppose that x is contained in exactly m of the starting sets (A_1 to A_n), $1 \leq m \leq n$. Then for each $k \leq m$, x appears in C(m, k) many k-way intersections (that is, if we look at $|\bigcap_{i \in I} A_i|$ for all $|I| = k$, x appears in C(m, k) many terms). Therefore, the number of times x gets counted by the inclusion-exclusion formula is exactly

$$\sum_{k=1}^{m} (-1)^{k+1} C(m, k)$$

and this is 1 by Corollary 3.2.

3.5 Pigeonhole Principle

In this section, we will discuss the pigeonhole principle: a proof technique that relies on counting. The principle says that if we place k + 1 or more pigeons into k pigeon holes, then at least one pigeon hole contains 2 or more pigeons. For example, in a group of 367 people, at least two people must have the same birthday (since there are a total of 366 possible birthdays). More generally, we have

Lemma 3.4. (Pigeonhole Principle). If we place n (or more) pigeons into k pigeon holes, then at least one box contains $\lceil n/k \rceil$ or more pigeons.

Proof. Assume the contrary that every pigeon hole contains $\leq \lceil n/k \rceil - 1 < n/k$ many pigeons. Then the total number of pigeons among the pigeon holes would be strictly less than $k(n/k) = n$, a contradiction.

Example 3.5.1. In a group of 800 people, how many people are likely to share the same birthday?

Solution 3.5.1. There are at least $\lceil 800/366 \rceil = 3$ people with the same birthday.

4.0 Conclusion

Specially, you have learned about counting. You have also learned how to carry out counting using some special techniques and principles.

5.0 Summary

In this unit, you have learnt how to use Pascal's triangle to expand a binominal expression. You have also been taught how to identify and apply inclusion-exclusion and pigeonhole principle.

6.0 Tutor-Marked Assignment

1. How many positive divisors does $2000 = 2^4 5^3$ have?
2. Six friends Adam, Brian, Chris, Dan, Elvis and Frank want to go see a movie. If there are only six seats available, how many ways can we seat these friends
3. Expand the following:
   a. $(1 + p)^4$
   b. $(3a - 2b)^5$
   c. $\left(1 + \frac{3}{a}\right)^4$
   d. $\left(x - \frac{1}{x}\right)^6$
4. Find the minimum number of students in a class such that three of them are born in the same month.

5. Show that from any three integers, one can always choose two, so that $a^3b - ab^3$ is divisible by 10.

7.0 References/Further Reading

Asimow, L and Maxwell, M (2010). Probability and Statistics with Applications. A problem solving text. ACTEX publications Inc. Winsted, Conecticut. ISBN: 978-1-56698-721-9

Coolman, R. (2015). Properties of Pascal's triangle. Published 17 June 2015.

Fraleigh, J. B. (1982). A First Course in Abstract Algebra, 3rd ed., Addison-Wesley.

Gallian, J. A. (1998. Contemporary Abstract Algebra, 4th edition, Houghton-Mifflin.

Kiltinen, J.O. (2004). Parity Theorem for Permutations - Convergence (December 2004)

UNIT 3 DISCRETE PROBABILITY GENERATING FUNCTION

CONTENTS

1.0 Introduction

Discrete probability generating functions are important and useful tools for dealing with sums and limits of random variables. The exact strength of Probability Generating Function (PGF), is that, it gives an easy way of characterizing the distribution of $A + B$ when A and B are independent. To find the distribution of a sum using the common probability function we know is quite difficult, hence, the use of PGF which transform a sum into a product makes it much easier to handle. The PGF gives us details of everything we need to know about the distribution.

2.0 Objectives

By the end of this unit, you will be able to:

- obtain the sum of Geometric, Binomial and Exponential series
- define Probability Generating Functions (PGFs) and use it to calculate the mean, variance and probability
- identify and calculate the PGF for Geometric, Binomial and Exponential distributions.

3.0 Main Content

3.1 Common Sums

3.1.1 Geometric Series

$1 + z + z^2 + z^3 + z^4 + \ldots = \sum_{x=0}^{\infty} z^x = \frac{1}{1-z}$, when $|z| < 1$.

This formular proves that $\sum_{x=0}^{\infty} P(X = x) = 1$ when $X \sim$ Geometric(p):

$$P(X = x) = p(1-p)^x \quad \Longrightarrow \quad \sum_{x=0}^{\infty} P(X = x) = \sum_{x-0}^{\infty} p(1-p)^x$$

$$= \boldsymbol{p} \sum_{x=0}^{\infty} (1-p)^x$$

$$= \frac{p}{1-(1-p)} \quad (because\ |1-p| < 1)$$

$$= 1 \quad (which\ is\ the\ sum\ of\ geometric\ series)$$

3.1.2 Binomial Theorem

Binomial theorem states that for any $p, q \in \mathbb{R}$ and integer n, then

$(p+q)^n = \sum_{x=0}^{n} \binom{n}{x} p^x q^{n-x}$, where $\binom{n}{x} = \frac{n!}{(n-x)!x!}$.

The Binomial Theorem proves that $\sum_{x=0}^{n} P(X = x) = 1$ when $X \sim$ Binomial(n, p):

$$P(X = x) = \binom{n}{x} p^x (1-p)^{n-x} \ for \ x = 0, 1, 2, 3, \ldots, n,$$

$$\therefore \quad \sum_{x=0}^{n} P(X = x) = \sum_{x=0}^{n} \binom{n}{x} p^x (1-p)^{n-x} = [p + (1-p)]^n = 1^n = 1$$

Hence the prove.

3.1.3 Exponential Series

Exponential series state that for any $\lambda \in \mathbb{R}, then \ \sum_{x=0}^{\infty} \frac{\lambda^x}{x!} = e^{\lambda}$.

The Exponential Series proves that $\sum_{x=0}^{\infty} P(X = x) = 1$ when $X \sim$ Poisson(λ):

$$P(X = x) = \frac{\lambda^x}{x!} e^{-\lambda} \ for \ \ x = 0, 1, 2, 3, \cdots,$$

$$\therefore \quad \sum_{x=0}^{\infty} P(X = x) = \sum_{x=0}^{\infty} \frac{\lambda^x}{x!} e^{-\lambda} = e^{-\lambda} \sum_{x=0}^{\infty} \frac{\lambda^x}{x!} = e^{-\lambda} e^{\lambda} = 1$$

But we know that $e^{\lambda} = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n \ \ for \ \lambda \in \mathbb{R}$.

3.2 Probability Generating Function (PGF)

Let be a random variable defined over the negative integers $\{0, 1, 2, 3, \cdots\}$. The probability generating function of X is given by

$G_X(z) = p_0 + p_1 z + p_2 z^2 + \ldots = \sum_{j=0}^{\infty} p_j z^j = \mathbb{E}(z^X),\ for\ all\ z \in \mathbb{R}$ for which the sum converges. Therefore, to calculate the probability generating function, we that

$G_X(z) = \mathbb{E}(z^X) = \sum_{x=0}^{\infty} z^x\, P(X = x).$

3.2.1 Properties of the PGF

(1) $G_X(0) = P(X = 0)$:

$G_X(0) = 0^0 \times P(X = 0) + 0^1 \times P(X = 1) + 0^2 \times P(X = 2) + \ldots$

$G_X(0) = P(X = 0).$

(2) $G_X(1) = 1$: $G_X(1) = \sum_{x=0}^{\infty} 1^x\, P(X = x) = \sum_{x=0}^{\infty} P(X = x) = 1.$

Example 3.2.2: Let X have a binomial distribution function with parameters $n\ and\ p$ (or $X \sim B(n, p)$, so $P(X = x) = \binom{n}{x} p^x q^{n-x}$ for $x = 0, 1, 2, 3, \ldots, n$. The probability generating function is given by

$$G_X(z) = \sum_{x=0}^{n} z^x \binom{n}{x} p^x q^{n-x} = \sum_{x=0}^{\infty} \binom{n}{x} (pz)^x\, q^{n-x}$$

$$= (pz + q)^n \quad \text{by Binomial Theorem.}$$

Hence, $G_X(z) = (pz + q)^n\ \ for\ all\ s \in \mathbb{R}$.

Example 3.2.3: Let X have a Geometric distribution function with parameter p (or $X \sim P(\lambda)$, so $P(X = x) = p(1 - p)^x = pq^x$ for $x = 0, 1, 2, 3, \ldots,$ where $q = 1 - p$. The probability generating function is given by

$$G_X(z) = \sum_{x=0}^{\infty} z^x\, pq^x = p \sum_{x=0}^{\infty} (qz)^x = \frac{p}{1 - qz} \quad for\ all\ z\ such\ that\ |qz| < 1.$$

Hence, $G_X(z) = \frac{p}{1-qz}\ \ for\ |z| < \frac{1}{q}$.

Example 3.2.4: Let X have a Poisson distribution function with parameter λ (or $X \sim P(\lambda)$, so $P(X = x) = \frac{\lambda^x}{x!} e^{-\lambda}$ for $x = 0, 1, 2, 3, \ldots$. The probability generating function is given by

$$G_X(z) = \sum_{x=0}^{\infty} z^x \frac{\lambda^x}{x!} e^{-\lambda} = e^{-\lambda} \sum_{x=0}^{\infty} \frac{(\lambda z)^x}{x!} = e^{-\lambda} e^{(\lambda z)} = e^{\lambda(z-1)}$$

Hence, $G_X(z) = e^{\lambda(z-1)}\ for\ all\ \ z \in \mathbb{R}$.

3.3 Using the PGF to calculate the mean (expectation) and variance

Here, we will use the PGF to calculate the moments of the distribution of X. The moments of a distribution include the mean, variance, etc.

3.3.1 Mean (Expected value)

Let X be a discrete random variable with PGF $G_X(z)$. Then, the expectation value can be expressed by

$E[X] = \sum_{x=1}^{\infty} x\, P(X = x) = G'_X(1)$, where $G'_X(z)$ denotes the derivative of $G_X(z)$.

Hence, $G'_X(z) = \sum_{x=0}^{\infty} x\, P(X = x)\, z^{x-1} = \sum_{x=1}^{\infty} x\, P(X = x) z^{x-1}$.

Also, the **second moment** is

$$E[X^2] = G''_X(1) + G'_X(1)$$

But we know that, $G'_X(z) = \sum_{x=1}^{\infty} x\, P(X = x)\, z^{x-1}$, then

$$G''_X(z) = \sum_{x=2}^{\infty} x(x-1)\, P(X = x)\, z^{x-2} = \sum_{x=0}^{\infty} (x^2 - x)\, P(X = x)\, z^{x-2}$$

3.3.2 Variance

Similarly, let X be a random variable with PGF $G_X(z)$. Then, the variance is given by

$$Var[X] = E[X^2] - E[X]^2 = G''_X(1) + G'_X(1) + G'_X(1)^2.$$

Example 3.3.3: Let X have a Poisson distribution function with parameter λ. The PGF of X is $G_X(z) = e^{\lambda(z-1)}$. Find (i) Mean, $E[X]$ (ii) Variance, $Var[X]$.

Solution: Given $G_X(z) = e^{\lambda(z-1)}$, then

(i) $G'_X(z) = \lambda e^{\lambda(z-1)}$, *which implies that* $E[X] = G'_X(1) = \lambda$

(ii) Thus, $G''_X(1) = \lambda^2 e^{\lambda(z-1)}|_{z=1} = \lambda^2$

and

$$E[X^2] = G''_X(1) + G'_X(1) = \lambda^2 + \lambda$$

$$\therefore \quad Var[X] = E[X^2] - E[X]^2 = \lambda^2 + \lambda - \lambda^2 = \lambda$$

Example 3.3.4: Let X be a random variable that has Bernoulli distribution with parameter p. The PGF is defined by $G_X(z) = (1-p) + pz$. Calculate $E[X]$ and $Var[X]$.

Solution: This implies that $G'_X(z) = p$ *and* $G''_X(z) = 0$

Hence, $E[X] = G'_X(1) = p$

and

$$Var[X] = G''_X(1) + G'_X(1) + G'_X(1)^2 = 0 + p - p^2 = p(1-p).$$

3.4 Using the PGF to calculate the probabilities

As well as calculating the moments of distribution of X, we can also calculate the probabilities using the PGF. Given the PGF $G_X(z) = E(z^X)$ of any probability function, we can recover all the possible probabilities $P(X = x)$ $(or \ \ sometimes \ written \ as \ p_x)$.

$$\therefore \qquad G_X(z) = E(z^X) = p_0 + p_1 z + p_2 z^2 + \ldots = \sum_{j=0}^{\infty} p_j z^j$$

Hence, $p_0 = P(X = 0) = G_X(0)$.

Also, the **first derivative** of the PGF is

$$G'_X(z) = p_1 + 2p_2 z + 3p_3 z^2 + 4p_4 z^3 + \ldots$$

Which implies that

$$p_1 = P(X = 1) = G'_X(0).$$

The **second derivative** of the PGF is

$$G''_X(z) = 2p_2 + 6p_3 z + 12p_4 c + \ldots$$

Which implies that

$$p_2 = P(X = 2) = \frac{1}{2!} G''_X(0).$$

For the **third derivative** of the PGF, we have

$$G'''_X(z) = 6p_3 + 24p_4 z + \ldots$$

Which implies that

$$p_3 = P(X = 3) = \frac{1}{3!} G'''_X(0).$$

Therefore, the $\boldsymbol{n^{th}}$ **derivative** or the **general form** is given by

$$p_n = P(X = n) = \left(\frac{1}{n!}\right) G^{(n)}{}_X(0) = \left(\frac{1}{n!}\right) \frac{d^n}{dz^n} (G_X(z))|_{z=0}.$$

Example 3.4.1: Let X be a discrete random variable with PGF $G_X(z) = \frac{z}{5}(2 + 3z^2)$. Obtain the distribution of X.

Solution: Given $G_X(z) = \frac{z}{5}(2 + 3z^2) = \frac{2}{5} z + \frac{3}{5} z^3$

$$\therefore \qquad G_X(z) = \frac{2}{5}z + \frac{3}{5}z^3 \qquad \Longrightarrow \qquad G_X(0) = P(X = 0) = 0.$$

$$G'_X(z) = \frac{2}{5} + \frac{9}{5}z^2 \qquad \Longrightarrow \qquad G'_X(0) = P(X = 1) = \frac{2}{5}$$

$$G''_X(z) = \frac{18}{5}z \qquad \Longrightarrow \qquad \frac{1}{2!}G''_X(0) = P(X = 2) = 0.$$

$$G'''_X(z) = \frac{18}{5} \qquad \Longrightarrow \qquad \frac{1}{3!}G'''_X(0) = P(X = 3) = \frac{3}{5}$$

$$G^{(k)}{}_X(z) = 0, for\ all\ k \geq 4 \quad \Longrightarrow \quad \frac{1}{k!}G^{(k)}{}_X(0) = P(X = k) = 0\ for\ all\ k \geq 4$$

Therefore, the distribution of $X, is\ X = \begin{cases} 1\ with\ probability\ \frac{2}{5} \\ 3\ with\ probability\ \frac{3}{5} \end{cases}$

3.5 Geometric Random Variables

The PGF of a geometrically distributed random variable X is

$$G(z) = \sum_{j=1}^{\infty} p(1-p)^{j-1}z^j = \quad pz\sum_{j=0}^{\infty}(1-p)^j z^j \quad = \frac{pz}{1-(1-p)z}$$

$$G(z) = \sum_{j=1}^{\infty} p(1-p)^{j-1}z^j = \qquad G'(z) = \frac{p}{(1-(1-p)z)^2}, \qquad G''(z)$$

$$= \frac{2p(1-p)}{(1-(1-p)z)^3}$$

$$\therefore \qquad E[X] = G'_X(1) = \frac{1}{P}$$

and

$$Var[X] = G''_X(1) + G'_X(1) + G'_X(1)^2 \quad = \quad \frac{2(1-P)}{P^2} + \frac{1}{p} + \frac{1}{p^2} \quad = \quad \frac{1-p}{p^2}$$

3.6 Binomial Distribution

Let X have a binomial distribution function with parameters $n\ and\ p$. Then, the PGF is

$$G_X(z) = ((1-p)+pz)^n = \sum_{j=0}^{n}\binom{n}{j}(1-p)^{n-j}p^j z^j.$$

$$\Longrightarrow \qquad G'_X(z) = np\big((1-p)+pz\big)^{n-1} \quad and \quad E[X] = G'_X(1) = np.$$

$$\Longrightarrow \qquad G''_X(z) = n(n-1)p^2\big((1-p)+pz\big)^{n-2}$$

$$\therefore \qquad Var[X] = G''_X(z) + G'_X(1) + G'_X(1)^2 = (n^2-n)p^2 + np - n^2p^2$$

$$-np^2 + np = np(1 - p).$$

4.0 Conclusion

PGFs are very useful tool for dealing with sums of random variables, which are difficult to tackle using the standard probability function.

5.0 Summary

In this unit, you have learnt how to

- Compute the sums Geometric, Binomial and Exponential series.
- Know the properties of PGF.
- Use PGF TO calculate the mean, variance and probability.
- Identify and calculate the PGF for Geometric and Binomial distributions.

6.0 Tutor-Marked Assignment

1. Find the sequence generated by the following generating functions:

   a. $\frac{4x}{1-x}$

   b. $\frac{1}{1-4x}$

   c. $\frac{x}{1+x}$

   d. $\frac{3x}{(1+x)^2}$

   e. $\frac{1+x+x^2}{(1-x)^2}$ (Hint: multiplication).

2. Show how you can get the generating function for the triangular numbers in three different ways:

   a. Take two derivatives of the generating function for 1, 1, 1, 1, 1, . . .

   b. Multiply two known generating functions.

3. Find a generating function for the sequence with recurrence relation $a_n = 3a_{n-1} - a_{n-2}$ with initial terms $a_0 = 1$ and $a_1 = 5$.

4. Starting with the generating function for 1, 2, 3, 4, . . ., find a generating function for each of the following sequences.

   a. 1, 0, 2, 0, 3, 0, 4, ...

   b. 1, −2, 3, −4, 5, −6, ...

   c. 0, 3, 6, 9, 12, 15, 18, ...

   d. 0, 3, 9, 18, 30, 45, 63, ... (Hint: relate this sequence to the previous one.)

5. Let X be a discrete random variable with PGF $G_X(z) = \frac{w}{3}(2 + 5w^3)$. Calculate the distribution of X.

7.0 References/Further Reading

Abramowitz, M. and Stegun, I. A. (1964). Handbook of Mathematical Functions, National Bureau of Standards, Applied Mathematics Series Nr.55, Washington, D.C.

Casella, G and Berger, R. L. (2002). Statistical Inference (2nd Edition). Pacific Grove: Duxbury.

Clive, M., John, B., Tim, W., Wait, K. and Dan, B. (2011). Electrical Engineering: Know It All. Newnes. Pp. 884.

Levin, O., (2021). Discrete Mathematics: An Open Introduction 3rd Edition, Oscar Levin, 2019. ISBN: 978-1792901690.

Spanos, Aris (1999). Probability Theory and Statistical Inference. New York: Cambridge musiUniversity, pp. 109-130.