SIE SPECIAL INDIAN EDITION

Elements of Discrete Mathematics

A Computer Oriented Approach

3e

ABOUT THE AUTHORS

Chung Laung Liu

Professor Chung Laung (Dave) Liu received his B.Sc. degree (1956) at the National Cheng Kung University in Taiwan, and his Science Master and Electrical Engineering degrees (1960), and his Science Doctor degree (1962) at the Massachusetts Institute of Technology. He was on the faculty of the Massachusetts Institute of Technology (1962–1972) and the University of Illinois at Urbana-Champaign (1972–1998), where he was Associate Provost from 1995 to 1998. Professor Liu has also worked as Visiting Professor at City University of Hong Kong, and Waseda University, Tokyo, Japan; Li K. T. Honorary Chair Professor at National Central University, Hsinchu, Taiwan; and Mei Yi Chi Honorary Chair Professor at National Tsing Hua University, Hsinchu, Taiwan.

He is the author and co-author of eight books and monographs, and over 200 technical papers.

He is a member of Academia Sinica, a Fellow of the Institute of Electrical and Electronics Engineers, and a Fellow of the Association for Computing Machinery.

Durga Prasad Mohapatra

Durga Prasad Mohapatra received his Ph. D. from Indian Institute of Technology Kharagpur and M.E. from Regional Engineering College (now NIT), Rourkela. He joined the faculty of the Department of Computer Science and Engineering at the National Institute of Technology, Rourkela in 1996, where he is now Assistant Professor. His research interests include discrete mathematics, software engineering, real-time systems and distributed computing. He has published more than thirty papers in these fields. Dr Mohapatra has been teaching discrete mathematics at NIT Rourkela for the past ten years. He has received Young Scientist Award for the year 2006 by Orissa Bigyan Academy. Currently, he is a member of IEEE.

Elements of Discrete Mathematics

A Computer Oriented Approach

3e

Chung Laung Liu
Department of Computer Science,
University of Illinois
Urbana Champaign

Durga Prasad Mohapatra
Department of Computer Science,
National Institute of Technology
Rourkela

Tata McGraw-Hill Publishing Company Limited
NEW DELHI

McGraw-Hill Offices

New Delhi New York St Louis San Francisco Auckland Bogotá Caracas
Kuala Lumpur Lisbon London Madrid Mexico City Milan Montreal
San Juan Santiago Singapore Sydney Tokyo Toronto

Tata McGraw-Hill

Special Indian Edition 2008

Adapted in India by arrangement with the McGraw-Hill Companies, Inc., New York

Sales Territories: India, Pakistan, Nepal Bangladesh, Sri Lanka and Bhutan

ISBN-13: 978-0-07-066913-0
ISBN-10: 0-07-066913-9

Managing Director: *Ajay Shukla*

General Manager: Publishing—SEM & Tech Ed: *Vibha Mahajan*
Sponsoring Editor: *Shalini Jha*
Junior Sponsoring Editor: *Nilanjan Chakravarty*
Senior Copy Editor: *Dipika Dey*
Junior Manager—Production: *Anjali Razdan*

General Manager: Marketing—Higher Education & School: *Michael J Cruz*
Product Manager: SEM & Tech Ed.: *Biju Ganesan*

Controller—Production: *Rajender P Ghansela*
Asst. General Manager—Production: *B L Dogra*

Typeset at Tej Composers, WZ-391, Madipur, New Delhi 110063, and printed at Rashtriya Printers, M-135, Panchsheel Garden, Naveen Shahdara, Delhi 110 032.
Cover Printer at: Rashtriya Printers
RYLLCRAXRCQAL

The McGraw-Hill Companies

To my parents, beloved wife Mami
and daughter Hara Priya
Your love, encouragement
and support are my greatest inspiration.

—Dr Durga Prasad Mohapatra

CONTENTS

PREFACE TO THE THIRD EDITION

This book containing a selection of topics from set theory, combinatorics, relations and functions, graph theory, finite state machines, analysis of algorithms, generating functions, recurrence relations and algebra is designed as a text on discrete mathematics for undergraduate students of engineering discipline, post graduate students of Mathematics and Statistics, and students of M.C.A.

This book, known for its mathematical emphasis and comprehensive coverage has become on the leading texts for this course. The third edition retains almost all the material in the second edition. The contents of the book do not require any background beyond higher secondary mathematics for understanding. It will be better, if students using this book know at least one high level programming language such as C. In the third edition, Chapter 2 (Computability and Formal Languages) and Chapter 7 (Finite State Machines) of the second edition, have been merged into a single chapter (Chapter 6), as both the chapters contain similar topics. The modified chapter (Chapter 6 of third edition) is renamed as "Modelling Computation". Besides this, in the third edition, all the chapters have been appropriately enhanced. In Chapter 1, propositions and predicate calculus have been discussed in more detail. In Chapter 2, conditional probability is extensively discussed by introducing Bayes' theorem. In chapter 3, the concepts on relations and functions have been presented more rigorously. The different types of functions including composite functions, inverse functions, hash functions, recursive functions, etc., have been introduced with several examples. Warshall's algorithm has been introduced with suitable example. Pigeonhole principle is explained in more detail with many examples and computer implementation. In Chapter 4, graph theory has been discussed with several examples. New sections on graph coloring and graph traversal techniques such as breadth first search and depth first search have been

introduced with their computer implementations. In Chapter 5, trees and cut-sets have been presented. Kruskal's algorithm and Prim's algorithm for constructing shortest spanning tree have been extensively illustrated with suitable examples. In Chapter 6, concepts of different types of grammars, finite state machine and turing machine have been introduced. Chapter 7 presents analysis of algorithms. Chapter 8 describes discrete numeric functions and generating functions. In Chapter 9, recurrence relations and recursive algorithms are presented. Also, divide and conquer algorithms have been introduced in Chapter 9 with several suitable examples. In Chapter 10, groups and rings are discussed. The concepts of sub-semi groups and sub-monoids are introduced. Also, the issues on error detection and correction are discussed in more detail. Chapter 11 presents Boolean algebra. Two new sections, namely, simplification of logic expressions using Karnaugh maps and simplification of logic expressions using Quine - McCluskey method are introduced.

Apart from the new sections, several programming examples, exercises and implementations have been provided. We have given emphasis on illustrating the basic concepts through several examples and programming implementations. The number of examples, exercises and programming implementations in each chapter has been significantly increased in the third edition. We hope that the new material will help the reader to easily understand the relevant topics in discrete mathematics and their applications to computer science. Also, we hope fervently that the students and teachers will find this text both stimulating and useful. We encourage the readers to take advantage of executing the programming implementations in order to clearly understand the underlying theoretical concepts.

This edition probably contains more material than one could cover in a one-semester course at an average pace. The topics on cut-sets, complexity of algorithms, homogeneous and partial solutions of recurrence relations, permutation groups and Burnside's theorem, Karnaugh maps and Quine - McCluskey method, etc., may be omitted from a basic study of the subject, if so desired by the instructor.

The layout of the chapters has been guided by the sequence of concepts such as moving from sets to relations, to graphs, to functions and to algebra. However, Chapter 8 (Discrete Numeric Functions and generating Functions), Chapter 9 (Recurrence Relations and Recursive Algorithms) and Chapter 10 (Groups and Rings) may be taught after Chapter3 (Relations and Functions).

Many people have contributed to make the third edition a reality. I would especially like to express my appreciation to Prof. Sunil K. Sarangi, Director, NIT Rourkela for his unstinted support and encouragement. I would also like to express my gratitude to Prof. Rajib Mall and Prof. Rajeev Kumar, CSE department, IIT Kharagpur for their encouragement. I would like to thank Prof. S. K. Rath, Prof. S. K. Jena, Prof. B. Majhi, Prof. R Baliarsingh, Prof. B. D. Sahu and other colleagues of CSE department, NIT Rourkela for their valuable guidance throughout the preparation of the manuscript. I acknowledge the help

and cooperation received from all the staff members of CSE department, NIT Rourkela. I would like to thank the editorial and production teams of Mc-Graw Hill Education India, for commissioning this edition and in particular Ms. Shalini Jha, Mr. Nilanjan Chakravarty, Ms. Dipika Dey and Ms. Anjali Razdan for their painstakingly and meticulous effort towards editing the manuscript.

Several students have contributed directly and indirectly to the contents of the third edition. In particular the UG and PG students of the CSE department of NIT Rourkela in the 2006-2007 batches have given me numerous ideas. The questions they posed in the classroom gave me the much required hints about the areas that required elaboration and the examples that should be included. Particularly I would like to thank Arindam, Pragyan, Baikuntha, Ganesh, Debashis, Siba Narayan, Chitta, Mahendra, Nilamadhab, Durga Prasad, Ravi Kiran, Sangram and Manish for their help in preparing the manuscript.

I also take this opportunity to thank my family members for their constant support. I thank my parents, my parents-in-law, my uncles and aunts, my brothers and sisters-in-law for their moral support. I also thank Pinki, Shiva and Bapi for their help. I must thank my daughter Harapriya for her patient wait when I was working on this revision. I sincerely express my gratitude to my wife Mami for her love and support and help in keying the manuscript. Without their constant encouragement and permission to spend extra hours at work, this revision would never have been complete.

I would welcome messages regarding typographical and other errors, comments and constructive suggestions to improve this edition, which can be sent to me at durga@nitrkl.ac.in or durgapm2004@yahoo.com.

D P Mohapatra

consideration. I hope that some of these personal views and tastes can be shared to some extent by the instructor using this book.

I would like to thank James N. Snyder, my department head, for his encouragement and support; Murray Edelberg, Jane W. S. Liu, and Andrew H. Sherman for their careful review of the manuscript; Donald K. Friesen for his contribution to the preparation of the Instructor's Manual; and Edward M. Reingold and F. Frances Yao for their many helpful suggestions. Several years ago, I had an opportunity to serve on a panel on the impact of computing on mathematics sponsored by the Committee on the Undergraduate Program in Mathematics of the Mathematical Association of America. I benefited greatly from the panel's discussion on the teaching of discrete mathematics, and I am much indebted to the members of the panel. I also thank Glenna Gochenour, Connie Nosbisch, Judy Watkins, and June Wingler for their typing and editorial assistance. Finally, thanks to Kathleen D. Liu for her assistance in the preparation of the index.

There is a certain amount of overlap between this book and the book *Introduction to Combinatorial Mamematics* I wrote a few years ago. In a number of instances, I follow quite closely the presentation in *Introduction to Combinatorial Mathematics*.

C. L. Liu

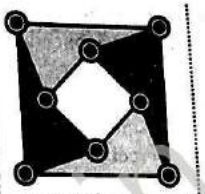
LIST OF SYMBOLS

Notations and Symbols used in this book

$\vee$ – or (disjunction/alternation)
$\wedge$ – and (conjuction)
$\oplus$ – Exclusive or, ring sum
$\in$ – belongs to
$\notin$ – does not belong to
$\subseteq$ – subset
$\subset$ – proper subset
$\cup$ – union (disjunction)
$\cap$ – intersection (conjunction)
$P(A)$ – power set of A
$p \rightarrow q$ – p implies q (conditional).
$p \leftrightarrow q$ – p if and only if q (biconditional)
$\overline{p}$, $\sim p$, p', $\neg p$ – negation of p
$\forall$ – for all (Universal quantifier)
$\exists$ – there exists (Existential quantifier)
Σ – summation
$\prod_{i_1 i_2}$ – projection
$\equiv$ – congruent modulo, equivalent
π – partition
∇ – backward difference
Δ – forward difference
ψ – number of elements those are invariant
N – set of all natural numbers
I – set of all integers
I^+ – set of all positive integers
I^- – set of all negative integers
R – set of all real numbers
R^+ – set of all positive real numbers
R^- – set of all negative real numbers
$A \times B$ – cartesian product of the sets A and B
A R b – a is related to b under the relation R
f^{-1} – inverse of the function f
gof – composition of the functions f and g

Objective

To discuss the concepts associated with set theory, propositions, predicate calculus and their applications.



CHAPTER

ONE

SETS AND PROPOSITIONS

1.1 INTRODUCTION

A major theme of this book is to study discrete objects and relationships among them. The term *discrete objects* is a rather general one. It includes a large variety of items such as people, books, computers, transistors, computer programs, and so on. In our daily lives as well as in our technical work we frequently deal with these items, making statements such as, "The people in this room are Computer Science majors in their second year of study," "All the books I bought are detective stories written by A. B. Charles," and "We want to select and buy a computer among those that are suitable for both scientific and business applications at a price not exceeding $200,000." We would like to abstract some of the basic concepts dealing with the many different kinds of discrete objects and establish certain common terminology for dealing with them.

A hint of the possibility of such an abstraction is quite evident when we observe that these three statements all have "something" in common. To be specific, in the first statement we are referring to people who possess the two attributes of being a Computer Science major and of being a sophomore; in the second statement we are referring to books that possess the two attributes of being a detective story and of being written by A. B. Charles; and in the third statement we are referring to computers that possess the three attributes of being suitable for scientific applications, of being suitable for business applications, and of being priced at no more than $200,000. To put it in another way, consider the group of all the Computer Science majors and the group of all the sophomores in the university. In our first statement we are then referring to those students who belong to both of these groups. Also, consider the collection of all detective stories and the collection of all books written by A. B. Charles. In our second statement we are then referring to those books that belong to both of these collections. Finally, in our third statement we are referring to all computers

that belong to the three categories of computers that are suitable for business applications, that are suitable for scientific applications, and that are priced at no more than $200,000.

Our example illustrates the many occasions on which we deal with several classes of objects and wish to refer to those objects that belong to all classes. Similarly, one would immediately perceive occasions on which we refer to objects that belong to one of several classes of objects, such as in the statement, "I want to interview all the students who speak either German or French," where we refer to those who belong either to the group of German-speaking students or to the group of French-speaking students.

We begin with the introduction of some basic terminology and concepts in elementary set theory. A *set* is a collection of *distinct* objects. Thus, the group of all sophomores in the university is a set. So is the group of all Computer Science majors in the university, and so is the group of all second-year Computer Science majors. We use the notation $\{a, b, c\}$ to denote the set which is the collection of the objects a, b, and c. The objects in a set are also called the *elements* or the *members* of the set. We usually also give names to sets. For example, we write $S = \{a, b, c\}$ to mean that the set named S is the collection of the objects a, b, and c. Consequently, we can refer to the set S as well as to the set $\{a, b, c\}$. As another example, we may have

Second-year-Computer-Science-majors
= {Smith, Jones, Wong, Yamamoto, Vögeli}

(The name of the set {Smith, Jones, Wong, Yamamoto, Vögeli} is Second-year-Computer-Science-majors, which is rather long. The reader probably would want to suggest alternative names such as S or CS. However, there is nothing wrong conceptually with having a "long" name.) We use the notation $a \in S$ to mean that a is an element in the set S. In that case, we also say that S *contains* the element a. We use the notation $d \notin S$ to mean that d is not an element in the set S. In that case, we also say that S does not contain the element d. Thus, in the example above, Jones $\in$ Second-year-Computer-Science-majors, while Kinkaid $\notin$ Second-year-Computer-Science-majors.

Note that a set contains only distinct elements. Thus, $\{a, a, b, c\}$ is a redundant representation of the set $\{a, b, c\}$. Similarly, {The-Midnight-Visitor, The-Midnight-Visitor, The-Missing-Witness, 114-Main-Street} is a redundant representation of the detective stories written by A. B. Charles. One might ask the question: What should we do if our collection of detective stories by A. B. Charles in the library indeed contains two copies of the book The-MidnightVisitor? In that case, the set {The-Midnight-Visitor, The-Missing-Witness, 114-Main-Street} is a set of distinct titles of detective stories by A. B. Charles in our library, while the set {The-Midnight-Visitor-1, The-Midnight-Visitor-2, TheMissing-Witness, 114-Main-Street} is the set of detective stories by A. B. Charles in our library where The-Midnight-Visitor-1 is copy 1 of the book The-Midnight. Visitor, and The-Midnight-Visitor-2 is copy 2 of the book. Note that The-Midnight-Visitor-1 and The-Midnight-Visitor-2 are two distinct elements in the latter set.

Note also that the elements in a set are not ordered in any fashion. Thus, $\{a, b, c\}$ and $\{b, a, c\}$ represent the same collection of elements.

As was introduced above, one way to describe the membership of a set is to list exhaustively all the elements in that set. In many cases, when the elements in a set share some common properties, we can describe the membership of the set by stating the properties that uniquely characterize the elements in the set. For example, let $S = \{2, 4, 6, 8, 10\}$. We can also specify the elements of S by saying that S is the set of all even positive integers that are not larger than 10. Indeed, we can use the notation

$$S = \{x \mid x \text{ is an even positive integer not larger than } 10\}$$

for the set $\{2, 4, 6, 8, 10\}$. In general, we use the notation

$$\{x \mid x \text{ possesses certain properties}\}$$

for a set of objects that share some common properties. Thus,

$$S = \{\text{Smith, Jones, Wong, Yamamoto, Vögeli}\}$$

and

$$S = \{x \mid x \text{ is a second-year Computer Science major}\}$$

are two different ways to describe the same set of elements.

It should be pointed out that our definition of a set does not preclude the possibility of having a set containing *no* elements. The set that contains no element is known as the *empty set*, and is denoted by $\{\ \}$. (We are consistent with the notation of using a pair of braces to enclose all the elements in the set. In this case, it just happens that there is no element in the enclosure.) In the literature, the empty set is also denoted by ϕ. So that the reader will be familiar with both notations, we shall use them interchangeably. For example, let S denote the set of all detective stories by A. B. Charles that were published in 1924. Clearly, S is the empty set if A. B. Charles was born in 1925. As another example, let S denote the set of all students who failed the course Discrete Mathematics. S might turn out to be the empty set if all students in the course studied hard for the final examination.

Let us note that we did not place any restriction on the elements in a set. Thus, S = {Smith, The-Midnight-Visitor, CDC-6600} is a well-defined set. That the elements, Smith (a person), The-Midnight-Visitor (the title of a book), and CDC-6600 (a computer) do not seem to share anything in common does not prohibit them from being elements of the same set. Indeed, we should point out that it is perfectly all right to have sets as members of a set. Thus, for example, the set $\{\{a, b, c\}, \{\{a, b, c\}, d\}$ contains the two elements $\{a, b, c\}$ and d, and the set $\{a, b, c\}$ contains the four elements $\{a, b, c\}$, a, b, and c. The set of all committees in the U.S. Senate could be represented by $\{\{a, b, c\}, \{a, d, e, f\}, \{b, e, g\}\}$, where each element of the set is a committee which, in turn, is a set with the senators in the committee as elements. Similarly, $\{a, \{a\}, \{\{a\}\}\}$ is a set with three *distinct* elements a, $\{a\}$, $\{\{a\}\}$. Also, the set $\{\{\ \}\}$, which can also be written as $\{\phi\}$, contains one element—the empty set. The set

$\{\{\ \}, \{\{\ \}\}\}$, which can also be written as $\{\phi, \{\phi\}\}$, contains two elements—the empty set and a set that contains the empty set as its only element. Perhaps an analogy will be helpful here. We can imagine that $\{a, b, c\}$ corresponds to a "box" in which there are three objects a, b, and c. Thus, $\{a, b, c, \{a, b\}\}$ corresponds to a box in which there are four objects a, b, c, and a box, in which there are two objects, a and b. Also, $\{\ \}$ corresponds to an empty box; $\{\{\ \}\}$ corresponds to a box in which there is an object that happens to be an empty box; and $\{\{\ \}, \{\{\ \}\}\}$ corresponds to a box in which there are two boxes—one empty and the other not. As another example, let

$$S_1 = \{John, Mary\}$$
$$S_2 = \{\{John, Mary\}\}$$
$$S_3 = \{\{\{John, Mary\}\}\}$$

We note that

$$John \in S_1$$
$$John \notin S_2$$
$$John \notin S_3$$
$$S_1 \in S_2$$
$$S_1 \notin S_3$$
$$S_2 \in S_3$$

Given two sets P and Q, we say that P is a *subset* of Q if every element in P is also an element in Q. We shall use the notation $P \subseteq Q$ to denote that P is a subset of Q. For example, the set $\{a, b\}$ is a subset of the set $\{y, x, b, c, a\}$, but it is not a subset of the set $\{a, c, d, e\}$. The set of all second-year Computer Science majors is a subset of the set of all sophomores. It is also a subset of the set of all Computer Science majors. On the other hand, the set of all Computer Science majors is not a subset of the set of all sophomores, nor is the set of all sophomores a subset of the set of all Computer Science majors. Let $A = \{a, b, c\}$ and $B = \{\{a, b, c\}, a, b, c\}$. We note that it is indeed possible to have both $A \in B$ and $A \subseteq B$. As further examples, we ask the reader to check the following statements:

1. For any set P, P is a subset of P.
2. The empty set is a subset of any set. However, the empty set is not always an element of any set.
3. The set $\{\phi\}$ is not a subset of the set $\{\{\phi\}\}$, although it is an element of the set $\{\{\phi\}\}$.

Two sets P and Q are said to be *equal* if they contain the same collection of elements. For example, the two sets

$$P = \{x \mid x \text{ is an even positive integer not larger than } 10\}$$
$$Q = \{x \mid x = y + z \text{ where } y \in \{1, 3, 5\}, z \in \{1, 3, 5\}\}$$

are equal. In a seemingly roundabout way, we can also say that two sets P and Q are equal if P is a subset of Q, and Q is a subset of P. We shall see later that on some occasions this is a convenient way to define the equality of two sets.

Let P be a subset of Q. We say that P is a *proper subset* of Q if P is not equal to Q, that is, there is at least one element in Q that is not in P. For example, the set $\{a, b\}$ is a proper subset of the set $\{y, x, b, c, a\}$. We use the notation $P \subset Q$ to denote that P is a proper subset of Q.

1.2 COMBINATIONS OF SETS

Now we shall show how sets can be *combined* in various ways to yield new sets. For example, let P be the set of students taking the course. Theory of Computation and Q be the set of students taking the course Music Appreciation. If a certain announcement was made in both the Theory of Computation and the Music Appreciation classes, what is the set of students who know about the news announced? Clearly, it is the set of students who are taking either Theory of Computation or Music Appreciation, or both. If both these courses have their final examinations scheduled in the same hours, what is the set of students who will have conflicting final examinations? Clearly, it is the set of students who are taking both Theory of Computation and Music Appreciation. To formalize these notions, we define the union and the intersection of sets. The *union* of two sets P and Q, denoted $P \cup Q$, is the set whose elements are exactly the elements in either P or Q (or both).* For example,

$$\{a, b\} \cup \{c, d\} = \{a, b, c, d\}$$
$$\{a, b\} \cup \{a, c\} = \{a, b, c\}$$
$$\{a, b\} \cup \phi = \{a, b\}$$
$$\{a, b\} \cup \{(a, h)\} = \{a, b, \{a, b\}\}$$

The *intersection* of two sets P and Q, denoted $P \cap Q$, is the set whose elements are exactly those elements that are in both P and Q. For example,

$$\{a, b\} \cap \{a, c\} = \{a\}$$
$$\{a, b\} \cap \{c, d\} = \phi^{\dagger}$$
$$\{a, b\} \cap \phi = \phi$$

If the elements in P are characterized by a common property and the elements in Q are characterized by another common property, then the union of P and Q is the set of elements possessing at least one of these properties, and the intersection of P and Q is the set of elements possessing both of these properties. According to the definitions, $P \cup Q$ and $Q \cup P$ denote the same set, as do $P \cap Q$ and $Q \cap P$.

It follows that the union of the set $P \cup Q$ and the set R, denoted $(P \cup Q) \cup R$ where the parentheses are used as delimiters to avoid confusion, contains exactly the elements in P, the elements in Q, and the elements in R. We shall use the notation $P \cup Q \cup R$ for $(P \cup Q) \cup R$, and shall refer to the set $P \cup Q \cup R$ as the

* We do not wish to introduce the notion of algebraic operations until Chapter 10. Thus, at this, moment. $P \cup Q$ is simply a name we have chosen for a set.

† Two sets are said to be *disjoint* if their intersection is the empty set.

union of the three sets P, Q, R. In general, the union of the set $(\ldots((P_1 \cup P_2) \cup P_3)\ldots) \cup P_{k-1}$ and the set P_k, denoted $(\ldots((P_1 \cup P_2) \cup P_3)\ldots \cup P_{k-1}) \cup P_k$, contains exactly the elements in P_1 the elements in P_2, ..., the elements in P_{k-1}, and the elements in P_k. We shall use the notation $P_1 \cup P_2 \cup P_3 \ldots \cup P_{k-1} \cup P_k$ for $(\ldots((P_1 \cup P_2) \cup P_3) \ldots \cup P_{k-1}) \cup P_k$ and shall refer to the set $P_1 \cup P_2 \cup P_3 \ldots \cup P_{k-1} \cup P_k$ as the union of the k sets $P_1, P_2, P_3, \ldots, P_{k-1}, P_k$. Similarly, the intersection of the set $P \cap Q$ and the set R, denoted $(P \cap Q) \cap R$, contains exactly the elements that are in P, Q, and R. Also, the intersection of the set $(\ldots((P_1 \cap P_2) \cap P_3)\ldots) \cap P_{k-1}$ and the set P_k, denoted $(\ldots((P_1 \cap P_2) \cap P_3)\ldots \cap P_{k-1}) \cap P_k$, contains exactly the elements that are in P_1 and P_2, ..., and P_{k-1}, and P_k. We shall use the notation $P_1 \cap P_2 \cap P_3 \ldots \cap P_{k-1} \cap P_k$ for $(\ldots((P_1 \cap P_2) \cap P_3)\ldots \cap P_{k-1}) \cap P_k$ and shall refer to the set $P_1 \cap P_2 \cap P_3 \ldots \cap P_{k-1} \cap P_k$ as the intersection of the k sets $P_1, P_2, P_3, \ldots, P_{k-1}, P_k$. For example, the set of all undergraduate students in a university is the union of the sets of freshmen, sophomores, juniors, and seniors, and the set of graduating seniors is the intersection of the set of seniors, the set of students who have accumulated 144 or more credit hours, and the set of students who have a C or better grade-point average.

Let P denote the set of students taking Theory of Computation, Q denote the set of students taking Music Appreciation, and R denote the set of students having type AB blood. Suppose an emergency announcement was made in the classes of Theory of Computation and Music Appreciation calling for type AB blood donors. We want to determine the members of the set of potential donors who heard about the emergency call. Since $S = P \cup Q$ is the set of students who heard about the emergency call, $R \cap S$ is the set of potential donors who heard about the emergency call. Instead of using a new name S for the set $P \cup Q$, we can simply write $R \cap (P \cup Q)$. Note that the set of potential donors who heard about the emergency call is also the set of students with type AB blood in the Theory of Computation class together with the set of students with type AB blood in the Music Appreciation class—that is, the set $(R \cap P) \cup (R \cap Q)$. This example suggests very strongly that for any sets P, Q, R, the two sets $R \cap (P \cup Q)$ and $(R \cap P) \cup (R \cap Q)$ are equal. Indeed, this is the case, as we now show.

We show first that $R \cap (P \cup Q)$ is a subset of $(R \cap P) \cup (R \cap Q)$ by showing that every element in $R \cap (P \cup Q)$ is also in $(R \cap P) \cup (R \cap Q)$. Let x be an element in $R \cap (P \cup Q)$. The element x must be in R and must be either in P or Q. If x is in P, x is in $R \cap P$. If x is in Q, x is in $R \cap Q$. Consequently, x is in $(R \cap P) \cup (R \cap Q)$, and we conclude that $R \cap (P \cup Q)$ is a subset of $(R \cap P) \cup (R \cap Q)$. Second, we show that $(R \cap P) \cup (R \cap Q)$ is a subset of $R \cap (P \cup Q)$. Let x be an element in $(R \cap P) \cup (R \cap Q)$. Thus, x must either be in $R \cap P$ or be in $R \cap Q$. That is, x must either be in both R and P or be in both R and Q. In other words, x must be in R and must be either in P or in Q. Consequently, x is in $R \cap (P \cup Q)$, and we can conclude that $(R \cap P) \cup (P \cap Q)$ is a subset of $R \cap (P \cup Q)$. It follows that the two sets $R \cap (P \cup Q)$ and $(R \cap P) \cup (R \cap Q)$ are equal.

In a similar manner we can show that for any sets P, Q, R, the two sets $R \cup (P \cap Q)$ and $(R \cup P) \cap (R \cup Q)$ are equal. Furthermore, we have

$$R \cap (P_1 \cup P_2 \cup \ldots \cup P_k) = (R \cap P_1) \cup (R \cap P_2) \cup \ldots \cup (R \cap P_k)$$
$$R \cup (P_1 \cap P_2 \cap \ldots \cap P_k) = (R \cup P_1) \cap (R \cup P_2) \cap \ldots \cap (R \cup P_k)$$

We leave the details to the reader.*

The *difference* of two sets P and Q, denoted $P - Q$, is the set containing exactly those elements in P that are not in Q. For example,

$$\{a, b, c\} - \{a\} = \{b, c\}$$
$$\{a, b, c\} - \{a, d\} = \{b, c\}$$
$$\{a, b, c\} - \{d, e\} = \{a, b, c\}$$

If P is the set of people who have tickets to a ball game and Q is the set of people who are ill on the day of the game, then $P - Q$ is the set of people who will go to the game. Note that Q might contain some or none of the elements of the set P. However, these elements will not appear in $P - Q$ in any case, just as in the example, those people who are ill but do not have tickets to the ball game will not go to the game anyway. Indeed, if the elements in Q are characterized by some common property, then $P - Q$ is the set of elements in P that do not possess this property. If Q is a subset of P, the set $P - Q$ is also called the *complement of Q with respect to P*. For example, let P be the set of all students in the course Theory of Computation and Q be the set of those students who have passed the course. Then $P - Q$ is the set of students who failed the course. On many occasions, when the set P is clear from the context, we shall abbreviate the *complement of Q with respect to P as the complement of Q*, which will be denoted $\overline{Q}$. For example, let P be the set of all students in the course Theory of Computation. Let Q be the set of Computer Science majors in the course, and R be the set of sophomores in the course. Then the complement of Q refers to the set of students in the course who are not Computer Science majors, and the complement of R refers to the set of those students who are not sophomores, if it is understood that in our discussion we always restrict ourselves to students in the course Theory of Computation. Indeed, when our discussion is always restricted to the subsets of a set P, P is referred to as the *universe*.

The *symmetric difference* of two sets P and Q, denoted $P \oplus Q$, is the set containing exactly all the elements that are in P or in Q but not in both. In other words, $P \oplus Q$ is the set $(P \cup Q) - (P \cap Q)$. For example,

$$\{a, b\} \oplus \{a, c\} = \{b, c\}$$
$$\{a, b\} \oplus \phi = \{a, b\}$$
$$\{a, b\} \oplus \{a, b\} = \phi$$

* Again, we do not wish to introduce the notions of algebraic operations, associativity, and distributivity until Chap. 11. Note, however, these notions are not needed here because $P \cap Q$, $P_1 \cap P_2 \cap \ldots \cap P_k$, $P \cup Q$, $P_1 \cup P_2 \cup \ldots \cup P_k$ are simply names for sets obtained according to our definitions.

If we let P denote the set of cars that have defective steering mechanisms and Q denote the set of cars that have defective transmission systems, then $P \oplus Q$ is the set of cars that have one but not both of these defects. Suppose that a student will get an A in a course if she did well in both quizzes, will get a B if she did well in one of the two quizzes, and will get a C if she did poorly in both quizzes. Let P be the set of students who did well in the first quiz and Q be the set of students who did well in the second quiz. Then $P \cap Q$ is the set of students who will get A's, $P \oplus Q$ is the set of students who will get B's, and $S - (P \cup Q)$ is the set of students who will get C's, where S is the set of all students in the course. We define $P_1 \oplus P_2 \oplus \ldots \oplus P_k$ to be the set of elements that are in an odd number of the sets $P_1, P_2, \ldots, P_k$.

The *power set* of a set A, denoted $\mathcal{P}(A)$, is the set that contains exactly all the subsets of A. Thus $\mathcal{P}(\{a, b\}) = \{\{\ \}, \{a\}, \{b\}, \{a, b\}\}$, and $\mathcal{P}(\{\ \}) = \{\{\ \}\}$. Note that for any set A, $\{\ \} \in \mathcal{P}(A)$ as well as $\{\ \} \subseteq \mathcal{P}(A)$. For example, let A = {novel, published-in-1975, paperback} be the three attributes concerning the books in the library in which we are interested. Then $\mathcal{P}(A)$ is the set of all possible combinations of these attributes the books might possess, ranging from books that have none of these attributes [the empty set in $\mathcal{P}(A)$] to books that have all three of these attributes [the set A in $\mathcal{P}(A)$].

Sets obtained from combinations of given sets can be represented pictorially. If we let P and Q be the sets represented by the cross-hatched areas in Fig. 1.1*a*, then the cross-hatched areas in Fig. 1.1*b* represent the sets $P \cup Q$, $P \cap Q$, $P - Q$, and $P \oplus Q$, respectively. These diagrams are known as *Venn diagrams*.

1.3 FINITE AND INFINITE SETS

Intuitively, it is quite clear that by the size of a set we mean the number of distinct elements in the set. Thus, there is little doubt when we say the size of the set $\{a, b, c\}$ is 3, the size of the set $\{a, \phi, d\}$ is also 3, the size of the set $\{\{a, b\}\}$ is 1, and the size of the set ϕ is 0. Indeed, we could stop our discussion on the size of sets at this point if we were only interested in the size of "finite" sets. However, a much more intriguing topic is the size of "infinite" sets. At this point, a

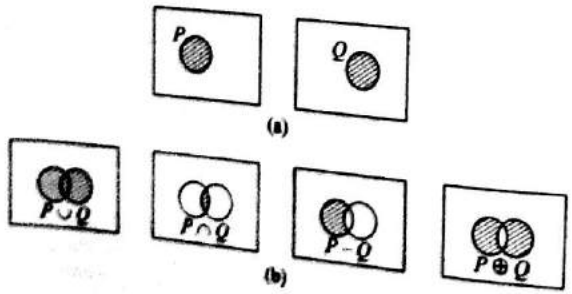


Fig. 1.1

perceptive reader will probably ask the question, "What is an infinite set in the first place?" An evasive answer such as, "An infinite set is not a finite set," is no answer at all, because if we start to think about it, we should also ask the question, "What is a finite set anyway?"

Let us begin be declaring that we have not yet committed ourselves to the precise definitions of finite sets and infinite sets. As the basis of our discussion, we want to construct an example of an infinite set. For a given set A, we define the *successor* of A, denoted A^+, to be the set $A \cup \{A\}$. Note that $\{A\}$ is a set that contains A as the only element. In other words, A^+ is a set that consists of all the elements of A together with an additional element which is the set A. For example, if $A = \{a, b\}$, then $A^+ = \{a, b\} \cup \{\{a, b\}\} = \{a, b, \{a, b\}\}$; and if $A = \{\{a\}, b\}$, then $A^+ = \{\{a\}, b, \{\{a\}, b\}\}$. Let us now construct a sequence of sets starting with the empty set ϕ. The successor of the empty set is $\{\phi\}$, whose successor is $\{\phi, \{\phi\}\}$, and whose successor, in turn, is $\{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$. It is clear that we can go on to construct more and more successors. Let us also assign names to these sets. In particular, we use 0, 1, 2, 3, ... as the names of the sets.*

Let

$$0 = \phi$$
$$1 = \{\phi\}$$
$$2 = \{\phi, \{\phi\}\}$$
$$3 = \{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

We have, clearly, $1 = 0^+$, $2 = 1^+$, $3 = 2^+$, and so on. Let us now, define a set N such that

1. N contains the set 0.
2. If the set n is an element in N, so is the set n^+.
3. N contains no other sets.

Since for every set in N its successor is also in N, the reader probably would agree that N is indeed an "infinite set." However, let us proceed in a more precise way.

We shall talk about the sizes of sets in a comparative manner. To this end, let us introduce a definition: Given two sets P and Q, we say that there is a *one-to-one correspondence* between the elements in P and the elements in Q if it is possible to pair off the elements in P and Q such that every element in P is paired off with a distinct element in Q.† Thus, there is a one-to-one correspondence between the elements in the set $\{a, b\}$ and the elements in the set $\{c, d\}$, because we can pair a with c and b with d, or we can pair a with d and b with c. There is also a one-to-one correspondence between the elements in the set $\{a, b, c\}$ and the elements in the set $\{\phi, a, d\}$. On the other hand, there is no one-to-one correspondence between the elements in the sets $\{a, b, c\}$ and $\{a, d\}$. The intention of introducing the notion of one-to-one correspondence between the

* Using 0, 1, 2, 3, ... as names of sets is just as good as using $A, B, C, D, \ldots$. As will be seen, it is intentional that we choose 0, 1, 2, 3, ... as names.

† Such an intuitive definition will be made more formal in Chapter 3.

elements of two sets is quite obvious, because we can now compare two sets and say that they are of the same size or that they are of different sizes. The basis of our comparison is indeed the sets we constructed above, namely, 0, 1, 2, 3, ..., and N. We are now ready to introduce some formal definitions. A set is said to be *finite* if there is a one-to-one correspondence between the elements in the set and the elements in some set n, where $n \in N$; n is said to be the *cardinality* of the set. Thus, for example, the cardinalities of the sets $\{a, b, c\}$, $\{a, \phi, d\}$, $\{\phi, \{\phi\}, \{\phi, \{\phi\}\}\}$ are all equal to 3. Note that it is now precise for us to say that a set is an infinite set if it is not a finite one. We can, however, be more precise about the "size" of infinite sets: A set is said to be *countably infinite* (or the cardinality of the set is countably infinite)* if there is a one-to-one correspondence between the elements in the set and the elements in N. We observe first of all that the set of all natural numbers $\{0, 1, 2, 3, \ldots\}$† is a countably infinite set. It follows that the set of all nonnegative even integers $\{0, 2, 4, 6, 8, \ldots\}$ is a countably infinite set because there is an obvious one-to-one correspondence between all nonnegative even integers and all natural numbers, namely, the even integer $2i$ corresponds to the natural number i for $i = 0, 1, 2, \ldots$. Similarly, the set of all nonnegative multiples of 7 $\{0, 7, 14, 21, \ldots\}$ is also a countably infinite set. So is the set of all positive integers $\{1, 2, 3, \ldots\}$. We note that a set is a countably infinite set if starting from a certain element we can sequentially list all the elements in the set one after another, because such a listing will yield a one-to-one correspondence between the elements in the set and the natural numbers. For example, the set of all integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is a countably infinite set, since its elements can be listed sequentially as $\{0, 1, -1, 2, -2, 3, -3, \ldots\}$. This example suggests that the union of two countably infinite sets is also a countably infinite set. It indeed is the case. As a matter of fact, the union of a finite number of countably infinite sets is a countably infinite set and, furthermore, so is the union of a countably infinite number of countably infinite sets (see Prob. 1.26).

1.4 UNCOUNTABLY INFINITE SETS

We show in this section that there are infinite sets with cardinalities that are not countably infinite. We now introduce a "proof technique" that probably is new to the reader.‡

* In the literature, the cardinality of a countably infinite set is also referred to as $\aleph_0$. ($\aleph$ is the first letter in the Hebrew alphabet.)

† The notation is perhaps confusing. However, it is intentional, because the set N is *indeed* a precise definition of the set of natural numbers.

‡ Indeed, throughout this book, we will need to show on many occasions that something cannot possibly exist, or some task can never be done. We are all familiar with how to demonstrate the existence of something or how to describe a procedure for performing a certain task. But, how does one demonstrate something that cannot possibly exist under any circumstances? How does one prove that some task cannot be done by anybody however intelligent, or any machine however powerful?

Three boys—James, Joe, and John—were asked to taste ice cream of three different flavors—chocolate, vanilla, and strawberry. The following table summarizes the flavors they each like and dislike:

	Chrocolate	Vanilla	Strawberry
James	Yes	No	Yes
Joe	No	No	Yes
John	Yes	Yes	Yes

We make a trivial observation: Suppose we were told that there is a boy who disagrees with James on whether chocolate ice cream is delicious (that is, James likes chocolate ice cream, but the boy dislikes it), who disagrees with Joe on whether vanilla ice cream is delicious (that is, Joe dislikes vanilla ice cream, but the boy likes it), and who also disagrees with John on whether strawberry ice cream is delicious (that is, John likes strawberry ice cream, but the boy dislikes it). Clearly, this boy cannot be James, Joe, or John, but must be a *different* boy, since he disagrees with each of their tastes on at least one of the flavors as illustrated in the following table:

	Chocolate	Vanilla	Strawberry
James	(Yes)	No	Yes
Joe	No	(No)	Yes
John	Yes	Yes	(Yes)
New boy	No	Yes	No

We may have a more general situation. Suppose that there are n boys and ice cream of n different flavors. If we were told that there is a boy who disagrees with the first boy on whether the first flavor is delicious, who disagrees with the second boy on whether the second flavor is delicious, and who disagrees with the nth boy on whether the nth flavor is delicious, then we can be certain that this boy is not one of the n boys, because he disagrees with each of them in at least one way. This seemingly frivolous example illustrates a *diagonal argument* in which we assert that a certain object (a new boy) is not one of the given objects (the n boys we know), using the fact that this object is different from each of the given objects in at least one way.

As an example of infinite sets with cardinalities that are not countably infinite, we now show that the set of real numbers between 0 and 1 is not a countably infinite set. Our proof procedure is to assume that the set is countably infinite and then show the existence of a contradiction. If the cardinality of the set of real numbers between 0 and 1 is countably infinite, there is a one-to-one correspondence between these real numbers and the natural numbers. Consequently, we can exhaustively list them one after another in decimal form as in the following:*

*A number such as 0.34 can be written in two different forms, namely, 0.34000... or 0.339999 .... We follow an arbitrarily chosen convention of writing it in the latter form.

$$0{\cdot}a_{11}\,a_{12}\,a_{13}\,a_{14}\ \ldots$$
$$0{\cdot}a_{21}\,a_{22}\,a_{23}\,a_{24}\ \ldots$$
$$0{\cdot}a_{31}\,a_{32}\,a_{33}\,a_{34}\ \ldots$$
$$\ldots\ldots\ldots\ldots$$
$$0{\cdot}a_{i1}\,a_{i2}\,a_{i3}\,a_{i4}\ \ldots$$
$$\ldots\ldots\ldots\ldots$$

where a_{ij} denotes the jth digit of the ith number in the list. Consider the number

$$0{\cdot}b_1\,b_2\,b_3\,b_4\ \cdots$$

where

$$b_i=\begin{cases}1 & \text{if } a_{ii}=9\\ 9-a_{ii} & \text{if } a_{ii}=0,1,2,\ldots,8\end{cases}$$

for all i. Clearly, the number $0{\cdot}b_1\,b_2\,b_3\,b_4\ \ldots$ is a real number between 0 and 1 that does not have an infinite string of trailing 0s (for example, 0.34000 ...). Moreover, it is different from each of the numbers in the list above because it differs from the first number in the first digit, the second number in the second digit, the ith number in the ith digit, and so on. Consequently, we conclude that the list above is not an exhaustive listing of the set of all real numbers between 0 and 1, contradicting the assumption that this set is countably infinite.

It is possible to continue in this direction to classify infinite sets so that notions such as some infinite sets are "more infinite" than other infinite sets can be made precise. This, however, will be beyond our scope of discussion.

1.5 MATHEMATICAL INDUCTION

Let us consider some illustrative examples:

Example 1.1 Suppose we have stamps of two different denominations, 3 cents and 5 cents. We want to show that it is possible to make up exactly any postage of 8 cents or more using stamps of these two denominations. Clearly, the approach of showing case by case how to make up postage of 8 cents, 9 cents, 10 cents, and so on, using 3-cent and 5-cent stamps will not be a fruitful one, because there is an infinite number of cases to be examined* Let us consider an alternative approach. We want to show that if it is possible to make up exactly a postage of k cents using 3-cent and 5-cent stamps, then it is also possible to make up exactly a postage of $k+1$ cents using 3-cent and 5-cent stamps. We examine two cases: Suppose we make up a postage of k cents using at least one 5-cent stamp. Replacing a 5-cent stamp by two 3-cent stamps will yield a way to make up a postage of $k+1$ cents. On the other hand, suppose we make up a postage of k cents using 3-cent stamps only. Since $k \geq 8$, there must be at least three 3-cent stamps. Replacing three 3-cent stamps by two 5-cent stamps will

* See, however, Prob. 1.30.

yield a way to make up a postage of $k+1$ cents. Since it is obvious how we can make up a postage of 8 cents, we conclude that we can make up a postage of 9 cents, which, in turn, leads us to conclude that we can make up a postage of 10 cents, which, in turn, leads us to conclude that we can make up a postage of 11 cents, and so on. ■

Example 1.2 Suppose we remove a square from a standard 8×8 chessboard as shown in Fig. 1.2*a*. Given 21 L-shaped triominoes* as shown in Fig. 1.2*b*, we want to know whether it is possible to *tile* the 63 remaining squares of the chessboard with the triominoes. (By tiling the remaining squares of the chessboard, we mean covering each of them exactly once without parts of the triominoes extending over the removed square or the edges of the board.) The answer to our question is affirmative, as Fig. 1.3 shows. We can actually prove a more general result, which we shall proceed to do.

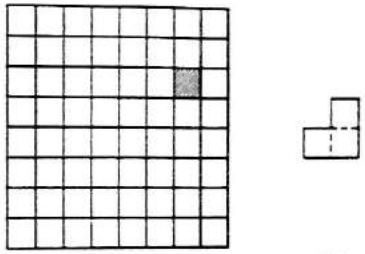


Fig. 1.2

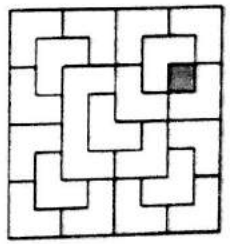


Fig. 1.3

A chessboard with one of its squares removed will be referred to as a *defective* chessboard. We want to show that any defective $2^n \times 2^n$ chessboard can be tiled with L-shaped triominoes.† It is trivially obvious that a defective 2×2 chessboard can be tiled with an L-shaped tromino. Let us now assume that any defective $2^k \times 2^k$ chessboard can be tiled with L-shaped triominoes and proceed to show that any defective $2^{k+1} \times 2^{k+1}$ chessboard can also be tiled with L-shaped triominoes. Consider a defective $2^{k+1} \times 2^{k+1}$ chessboard as shown in Fig. 1.4*a*. Let us divide the chessboard into four quadrants, each of which is a $2^k \times 2^k$ chessboard, as shown in Fig. 1.4*b*.

* The word *trio*mino is derived from the word domino. Also, there are tetrominoes, *penta*minoes, *hexa*minoes and, in general, *poly*minoes.

† One would immediately question whether $2^n \times 2^n - 1$ is always divisible by 3. The answer is affirmative. (See Prob. 1.36.)

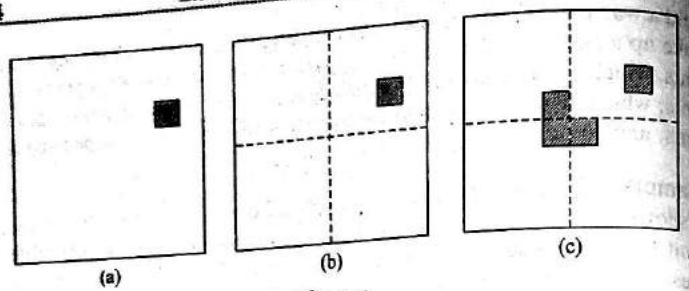


Fig. 1.4

One of these $2^k \times 2^k$ chessboards is a defective one. Furthermore, by placing an L-shaped triomino at the center of the $2^{k+1} \times 2^{k+1}$ chessboard, as shown in Fig. 1.4c, we can imagine that the other three quadrants are also defective $2^k \times 2^k$ chessboards. Since we assume that any defective $2^k \times 2^k$ chessboard can be tiled with L-shaped triominoes, we can tile each of the quadrants with L-shaped triominoes, and conclude that any defective $2^{k+1} \times 2^{k+1}$ chessboard can be tiled with L-shaped triominoes. Thus, starting with the tiling of any defective 2×2 chessboard, we have proved that we can tile any $2^n \times 2^n$ defective chessboard. ■

These two examples illustrate a very powerful proof technique in mathematics known as the principle of *mathematical induction*. For a given statement involving a natural number n, if we can show that:

1. The statement is true for $n = n_0$; and
2. The statement is true for $n = k + 1$, assuming that the statement is true for $n = k$, $(k \geqq n_0)$,

then we can conclude that the statement is true for all natural numbers $n \geqq n_0$. (1) is usually referred to as the *basis of induction*, and (2) is usually referred to as the *induction step*. Also, the assumption that the statement is true for $n = k$ in (2) is usually referred to as the *induction hypothesis*. For example, in the postage-stamp problem, we want to prove the statement, "It is possible to make up exactly any postage of n cents using 3-cent stamps and 5-cent stamps for $n \geqq 8$." In order to prove the statement we show that:

1. *Basis of induction*. It is possible to make up exactly a postage of 8 cents.
2. *Induction step*. It is possible to make up exactly a postage of $k + 1$ cents, assuming it is possible to make up exactly a postage of k cents, $(k \geqq 8)$.

We note that the principle of mathematical induction is a direct consequence of the definition of natural numbers. Consider a set S such that

1. The natural number n_0 is in S.
2. If the natural number k is in S, then the natural number $k + 1$ is also in S, $(k \geqq n_0)$.

According to the definition of the set of natural numbers, we can conclude that S contains all the natural numbers larger than or equal to n_0. However, this is exactly the statement of the principle of mathematical induction when we consider S to be the set of natural numbers for which a given statement is true.

We consider now more examples:

Example 1.3 The king summoned the best mathematicians in the kingdom to the palace to find out how smart they were. The king told them: "I have placed white hats on some of you and black hats on the others. You may look at, but not talk to, one another. I will leave now and will come back every hour on the hour. Every time I return, I want those of you who have determined that you are wearing white hats to come up and tell me immediately." As it turned out, at the nth hour everyone of the n mathematicians who were given white hats informed the king that she knew that she was wearing a white hat. Why?

We shall prove by induction that if there are n mathematicians wearing white hats, then they will all figure that out on the nth hour.

1. *Basis of induction*. For $n = 1$, there is only one mathematician wearing a white hat. Since the king said that white hats were placed on some of the mathematicians (kings never lie), the mathematician who saw that all other mathematicians had on black hats would realize immediately that she was wearing a white hat. Consequently, she would inform the king on the first hour (when the king returned for the first time) that she was wearing a white hat.
2. *Induction step*.* Assume that if there were k mathematicians wearing white hats, then they would have figured out that they were wearing white hats and informed the king so on the kth hour. Now, suppose that there were $k + 1$ mathematicians wearing white hats. Every mathematician wearing a white hat saw that k of her colleagues were wearing white hats. However, that her k colleagues did not inform the king of their findings on the kth hour can only imply that there were more than k people wearing white hats. Consequently, she knew that she must be wearing a white hat also. On the $(k + 1)$st hour, she (together with all other mathematicians wearing white hats) would tell the king their conclusion. ■

Example 1.4 Consider the following solitaire game: for every integer i, there is an unlimited supply of balls marked with the number i. Initially, we are given a tray of balls, and we throw away the balls in the tray one at a time. If we throw away a ball that is marked with i, we can replace it by any finite number of balls

* To help you understand the argument better, we will explore the reasoning for the case that there were two mathematicians wearing white hats. Consider one of these two mathematicians. She saw that one of her colleagues was wearing a white hat. She reasoned that if she were wearing a black hat, her colleague would be the only one wearing a white hat. In that case, her colleague would have figured out the situation and informed the king on the first hour. (All mathematicians are smart.) That this did not happen implies that she was also wearing a white hat. Consequently, she told the king on the second hour (and so did the other mathematician with a white hat, since, again, all mathematicians are smart).

marked 1, 2, ..., $i-1$. (Thus, no replacement will be made if we throw away a ball marked with 1.) The game ends when the tray is empty. We want to know whether the game always terminates for any tray of balls given initially.

We shall prove that the game always terminates by induction on n, the largest number that appears on the balls in the tray.

1. *Basis of induction.* For $n = 1$, there is a finite number of balls marked with 1 in the tray initially. Since there is no replacement after a ball marked 1 is thrown away, the game terminates after a finite number of moves.
2. *Induction step.* We assume that the game terminates if the largest number that appears on the balls is k. Consider the case when the largest number that appears on the ball is $k+1$. According to the induction hypothesis, we eventually have to throw away a ball marked $k+1$. (If we throw away only balls marked 1, 2, ..., k, they will be exhausted in a finite number of moves.) Repeating this argument, we would have thrown away all balls marked with $k+1$ in a finite number of moves. Again, by the induction hypothesis, the game terminates after a finite number of moves from then on. ■

Example 1.5 Show that

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad n \geqq 1$$

by mathematical induction.

1. *Basis of induction.* For $n = 1$, we have
$$1^2 = \frac{1(1+1)(2+1)}{6}$$
2. *Induction step.* Assume that
$$1^2 + 2^2 + \ldots + k^2 = \frac{k(k+1)(2k+1)}{6}$$
We have
$$\begin{aligned} 1^2 + 2^2 + \ldots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\ &= \frac{(k+1)[k(2k+1)+6(k+1)]}{6} \\ &= \frac{(k+1)(2k^2+7k+6)}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \\ &= \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} \end{aligned}$$
■

Example 1.6 Show that any integer composed of 3^n identical digits is divisible by 3^n. (For example, 222 and 777 are divisible by 3; 222,222,222 and 555,555,555 are divisible by 9.) We shall prove the result by induction on n.

1. *Basis of induction.* For $n = 1$, we note that any 3-digit integer with three identical digits is divisible by 3.*
2. *Induction step.* Let x be an integer composed of 3^{k+1} identical digits. We note that x can be written as
$$x = y \times z$$
where y is an integer composed of 3^k identical digits and
$$z = 10^{2\cdot 3^k} + 10^{3^k} + 1 = \underbrace{1000000\ldots01}_{3^k-1\text{ 0s}}\underbrace{000000\ldots01}_{3^k-1\text{ 0s}}$$
Since we assume that y is divisible by 3^k and z is clearly divisible by 3, we conclude that x is divisible by 3^{k+1}. ■

Example 1.7 Show that $2^n > n^3$ for $n \geq 10$.

1. *Basis of induction.* For $n = 10$, $2^{10} = 1024$ which is larger than 10^3.
2. *Induction step.* Assume that $2^k > k^3$. Note that
$$2^{k+1} = 2 \cdot 2^k > \left(1+\frac{1}{10}\right)^3 \cdot 2^k \geqq \left(1+\frac{1}{k}\right)^3 \cdot 2^k > \left(1+\frac{1}{k}\right)^3 \cdot k^3 = (k+1)^3$$
■

A more "powerful" form of the principle of mathematical induction, which is referred to as the *principle of strong mathematical induction*, can be stated as follows: For a given statement involving a natural number n, if we can show that

1′. The statement is true for $n = n_0$; and
2′. The statement is true for $n = k+1$, assuming that the statement is true for $n_0 \leqq n \leqq k$,

then we can conclude that the statement is true for all natural numbers $n \geqq n_0$.

We note that this is indeed a more powerful form of the principle of mathematical induction presented at the beginning of this section. Specifically, in the induction step, in order to prove that the statement is true for $n = k+1$, we are *allowed* to make a stronger assumption in 2′ (namely, the statement is true for $n_0 \leqq n \leqq k$) than in 2 above (namely, the statement is true for $n = k$.) In other words, the principle of strong mathematical induction enables us to make the same conclusion while assuming more. We leave the proof of the principle of strong mathematical induction to Prob. 1.53. We present now some examples:

Example 1.8 A jigsaw puzzle consists of a number of pieces. Two or more pieces with matched boundaries can be put together to form a "big" piece. To be

* We remind the reader of the elementary result that an integer is divisible by 3 if the sum of its digits is divisible by 3.

more precise, we use the term *block* to refer to either a single piece or a number of pieces with matched boundaries that are put together to form a "big" piece. Thus, we can simply say that blocks with matched boundaries can be put together to form another block. Finally, when all pieces are put together as one single block, the jigsaw puzzle is said to be solved. Putting two blocks with matched boundaries together is counted as one move. We shall use the principle of strong mathematical induction to prove that for a jigsaw puzzle with n pieces, it will always take $n - 1$ moves to solve the puzzle.

1. *Basis of induction*. For a jigsaw puzzle with one piece, it does not take any moves to solve the puzzle.
2. *Induction step*. Assume that for any jigsaw puzzle with n pieces, $1 \leq n \leq k$, it takes $n - 1$ moves to solve the puzzle. Now, consider a jigsaw puzzle with $k + 1$ pieces. For the last move that produces the solution of the puzzle, two blocks—one with n_1 pieces and the other with n_2, where $n_1 + n_2 = k + 1$—are put together to form a single block. According to the induction hypothesis, it takes $n_1 - 1$ moves to put together one block, and $n_2 - 1$ moves to put the other block together. Including the last move to unite the two blocks, the total number of moves is equal to

$$(n_1 - 1) + (n_2 - 1) + 1 = k + 1 - 1 = k$$

■

Example 1.9 We want to show that any positive integer n greater than or equal to 2 is either a prime or a product of primes.

1. *Basis of induction*. For $n = 2$, since 2 is a prime, the statement is true.
2. *Induction step*. Assume that the statement is true for any integer n, $2 \leqq n \leqq k$. For the integer $k + 1$, if $k + 1$ is a prime, then the statement is true. If $k + 1$ is not a prime, then $k + 1$ can be written as pq, where $p \leqq k$ and $q \leqq k$. According to the induction hypothesis, p is either a prime or a product of primes. Also, q is either a prime or a product of primes. Consequently, pq is a product of primes. ■

Example 1.10 Suppose we wish to trace our family tree to identify our ancestors. Quite often, incomplete family records prohibit us from going back beyond a few generations. Figure 1.5*a* and *b* show two examples of family trees. We make a simplifying assumption that for any of our ancestors, either we can trace both of his or her parents or we can trace neither of them. In a family tree, a person is referred as a "leaf" if we have no record to go on to trace his or her parents, and a person is referred to as an "internal node" if his or her parents have been traced.*

We want to show that in any family tree, the number of leaves is always one more than the number of internal nodes. We shall prove the statement by

* We introduce these terms simply for the convenience of our presentation. They will be presented again formally in Chapter 5 when we study trees as a special class of graphs.

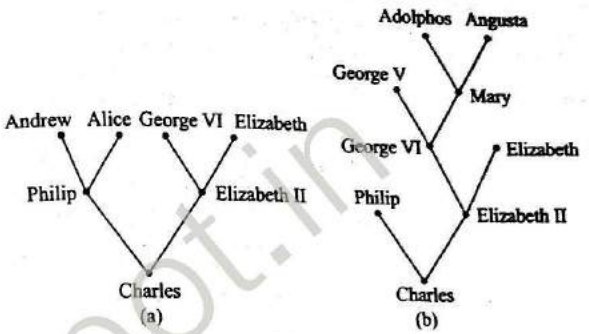


Fig. 1.5

induction on n, the number of people in the family tree, using the principle of strong mathematical induction.

1. *Basis of induction*. We note that the statement is true when $n = 1$. When there is only one person in a family tree, this person is a leaf, and there is no internal node.
2. *Induction step*. We assume that the statement is true for all family trees with n people, for $1 \leqq n \leqq k$. We want to show the statement is true for any family tree with $k + 1$ people. Consider the family tree of a man that has $k + 1$ people. Let p denote the number of leaves in the tree, and q denote the number of internal nodes in the tree. Since there are at least three people in the tree, both parents of this man are in the tree. Now, consider the family tree of each of his parents, as illustrated in Fig. 1.6. Let n_1 denote the number of people in his father's family tree, with p_1 of them being leaves and q_1 of them being internal nodes. Let n_2 denote the number of people in his mother's family tree, with p_2 of them being leaves and q_2 of them being internal nodes. Since $n_1 \leqq k$ and $n_2 \leqq k$, according to the induction hypothesis

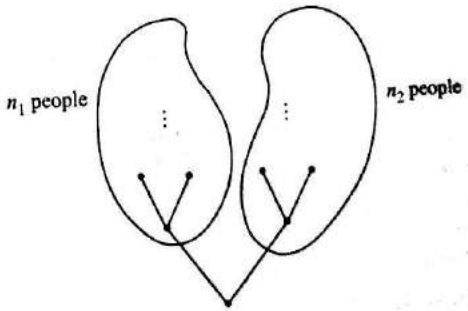


Fig. 1.6

$$p_1 = q_1 + 1$$
$$p_2 = q_2 + 1$$

Since

$$p = p_1 + p_2$$
$$q = q_1 + q_2 + 1$$

we have

$$p = q_1 + q_2 + 2 = q + 1$$ ■

1.6 PRINCIPLE OF INCLUSION AND EXCLUSION

We present in this section some results related to the cardinality of finite sets. We shall use the notation $|P|$ to denote the cardinality of the set P. Some simple results, the derivation of which is left to the reader, are:

$$|P \cup Q| \leqq |P| + |Q|$$
$$|P \cap Q| \leqq \min(|P|, |Q|)$$
$$|P \oplus Q| = |P| + |Q| - 2|P \cap Q|$$
$$|P - Q| \geqq |P| - |Q|$$

We show in the following a less obvious result. Let A_1 and A_2 be two sets. We want to show that

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| \qquad (1.1)$$

Note that the sets A_1 and A_2 might have some common elements. To be specific, the number of common elements between A_1 and A_2 is $|A_1 \cap A_2|$. Each of these elements is counted twice in $|A_1| + |A_2|$ (once in $|A_1|$ and once in $|A_2|$), although it should be counted as one element in $|A_1 \cup A_2|$. Therefore, the *double count* of these elements in $|A_1| + |A_2|$ should be adjusted by the subtraction of the term $|A_1 \cap A_2|$ in the right-hand side of (1.1). As an example, suppose that among a set of 12 books, 6 are novels, 7 were published in the year 1984, and 3 are novels published in 1984. Let A_1 denote the set of books that are novels, and A_2 denote the set of books published in 1984. We have

$$|A_1| = 6 \quad |A_2| = 7 \quad |A_1 \cap A_2| = 3$$

Consequently, according to (1.1),

$$|A_1 \cup A_2| = 6 + 7 - 3 = 10$$

That is, there are 10 books which are either novels or 1984 publications, or both. Consequently, among the 12 books there are 2 nonnovels that were not published in 1984.

Extending the result in (1.1), we have, for three sets A_1, A_2, and A_3,

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \qquad (1.2)$$

As we shall prove a more general result in the following, we shall not prove the result in (1.2) here. On the other hand, we suggest that a reader check the result in (1.2) by examining the Venn diagram in Fig. 1.7.

Let us consider some illustrative examples:

Example 1.11 Suppose we have six computers with the following specifications:

Computer	Floating-point arithmetic unit	Magnetic disk memory	Graphic display terminal
I	Yes	Yes	No
II	Yes	Yes	Yes
III	No	No	No
IV	No	Yes	Yes
V	No	Yes	No
VI	No	Yes	Yes

Let A_1, A_2, and A_3 be the sets of computers with a floating-point arithmetic unit, magnetic-disk storage, and graphic display terminal, respectively. We have

$$|A_1| = 2 \quad |A_2| = 5 \quad |A_3| = 3$$
$$|A_1 \cap A_2| = 2 \quad |A_1 \cap A_3| = 1 \quad |A_2 \cap A_3| = 3$$
$$|A_1 \cap A_2 \cap A_3| = 1$$

Consequently,

$$|A_1 \cup A_2 \cup A_3| = 2 + 5 + 3 - 2 - 1 - 3 + 1 = 5$$

That is, five of the six computers have one or more of the three kinds of hardware considered. ■

Example 1.12 Out of 200 students, 50 of them take the course Discrete Mathematics, 140 of them take the course Economics, and 24 of them take both courses. Since both courses have scheduled examinations for the following day, only students who are not in either one of these courses will be able to go to the party the night before. We want to know how many students will be at the party. Examining the Venn diagram in Fig. 1.8*a*, where A_1 is the set of students in the course Discrete Mathematics and A_2 is the set of students in the course Economics, we note that the number of students who take either one or both courses is equal to

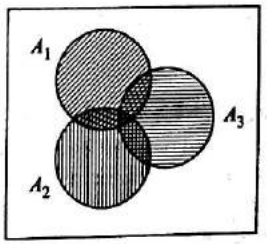
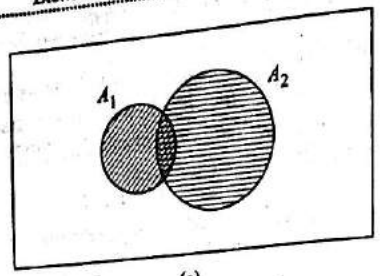
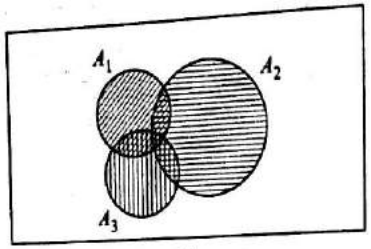


Fig. 1.7

$$50 + 140 - 24 = 166$$



(a)



(b)

Fig. 1.8

Consequently, the number of students who will be at the party is

$$200 - 166 = 34$$

Suppose that 60 of the 200 are underclass students. Among the underclass students, 20 of them take Discrete Mathematics, 45 of them take Economics, and 16 of them take both. We want to know how many upperclass students will be at the party. According to the Venn diagram in Fig. 1.8*b*, where A_3 is the set of underclass students, we have

$$|A_1 \cup A_2 \cup A_3| = 50 + 140 + 60 - 24 - 20 - 45 + 16 = 177$$

Thus, the number of upperclass students who will go to the party is

$$200 - 177 = 23$$

■

Example 1.13 Thirty cars were assembled in a factory. The options available were a radio, an air conditioner, and white-wall tires. It is known that 15 of the cars have radios, 8 of them have air conditioners, and 6 of them have white-wall tires. Moreover, 3 of them have all three options. We want to know at *least* how many cars do not have any options at all. Let A_1, A_2, and A_3 be the sets of cars with a radio, an air conditioner, and white-wall tires, respectively. Since

$$|A_1| = 15 \qquad |A_2| = 8 \qquad |A_3| = 6$$

and

$$|A_1 \cap A_2 \cap A_3| = 3$$

according to (1.2)

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= 15 + 8 + 6 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + 3 \\ &= 32 - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \end{aligned}$$

Since

$$\begin{aligned} |A_1 \cap A_2| &\geqq |A_1 \cap A_2 \cap A_3| \\ |A_1 \cap A_3| &\geqq |A_1 \cap A_2 \cap A_3| \\ |A_2 \cap A_3| &\geqq |A_1 \cap A_2 \cap A_3| \end{aligned}$$

we have

$$|A_1 \cup A_2 \cup A_3| \leqq 32 - 3 - 3 - 3 = 23$$

That is, there are *at most* 23 cars that have one or more options. Consequently, there are *at least* 7 cars that do not have any options. ■

In the general case, for the sets $A_1, A_2, \ldots, A_r$, we have

$$|A_1 \cup A_2 \cup \ldots \cup A_r| = \sum_i |A_i| - \sum_{1 \leqq i < j \leqq r} |A_i \cap A_j| + \sum_{1 \leqq i < j < k \leqq r} |A_i \cap A_j \cap A_k| + \ldots + (-1)^{r-1} |A_1 \cap A_2 \cap \ldots \cap A_r| \quad (1.3)$$

Although the result in (1.2) is not difficult to visualize, the result in (1.3) is not as obvious. We now prove (1.3) by induction on the number of sets r. Clearly, (1.1) can serve as the basis of induction. As the induction step, we assume that (1.3) is valid for any $r-1$ sets. We note first that, viewing $(A_1 \cup A_2 \cup \ldots \cup A_{r-1})$ and A_r as two sets, according to (1.1) we have

$$\begin{aligned} |A_1 \cup A_2 \cup \ldots \cup A_r| = |A_1 \cup A_2 \cup \ldots \cup A_{r-1}| + |A_r| \\ - |A_r \cap (A_1 \cup A_2 \cup \ldots \cup A_{r-1})| \end{aligned} \quad (1.4)$$

Now

$$|A_r \cap (A_1 \cup A_2 \cup \ldots \cup A_{r-1})| = |(A_r \cap A_1) \cup (A_r \cap A_2) \cup \ldots \cup (A_r \cap A_{r-1})|$$

According to the induction hypothesis, for the $r-1$ sets $A_r \cap A_1, A_r \cap A_2, \ldots, A_r \cap A_{r-1}$, we have

$$\begin{aligned} &|(A_r \cap A_1) \cup (A_r \cap A_2) \cup \ldots \cup (A_r \cap A_{r-1})| \\ &= |A_r \cap A_1| + |A_r \cap A_2| + \ldots + |A_r \cap A_{r-1}| \\ &\quad - |(A_r \cap A_1) \cap (A_r \cap A_2)| - |(A_r \cap A_1) \cap (A_r \cap A_3)| \\ &\quad - \ldots \\ &\quad - |(A_r \cap A_1) \cap (A_r \cap A_2) \cap (A_r \cap A_3)| + \ldots \\ &\quad - \ldots \\ &\quad + (-1)^{r-2} |(A_r \cap A_1) \cap (A_r \cap A_2) \cap \ldots \cap (A_r \cap A_{r-1})| \\ &= |A_r \cap A_1| + |A_r \cap A_2| + \ldots + |A_r \cap A_{r-1}| \\ &\quad - |A_r \cap A_1 \cap A_2| - |A_r \cap A_1 \cap A_3| - \ldots \\ &\quad + |A_r \cap A_1 \cap A_2 \cap A_3| + \ldots \\ &\quad - \ldots \\ &\quad + (-1)^{r-2} |A_r \cap A_1 \cap A_2 \cap \ldots \cap A_{r-1}| \end{aligned} \quad (1.5)$$

Also, according to the induction hypothesis, for the $r-1$ sets $A_1, A_2, \ldots, A_{r-1}$ we have

$$|A_1 \cup A_2 \cup \ldots \cup A_{r-1}| = |A_1| + |A_2| + \ldots - |A_1 \cap A_2| - |A_1 \cap A_3| - \ldots + \ldots + (-1)^{r-2}|A_1 \cap A_2 \cap \ldots \cap A_{r-1}| \quad (1.6)$$

Substituting (1.5) and (1.6) into (1.4), we obtain (1.3).

Example 1.14 Let us determine the number of integers between 1 and 250 that are divisible by any of the integers 2, 3, 5, and 7. Let A_1 denote the set of integers between 1 and 250 that are divisible by 2, A_2 denote the set of integers that are divisible by 3, A_3 denote the set of integers that are divisible by 5, and A_4 denote the set of integers that are divisible by 7. Since

$$|A_1| = \left\lfloor \frac{250}{2} \right\rfloor^* = 125 \qquad |A_2| = \left\lfloor \frac{250}{3} \right\rfloor = 83$$

$$|A_3| = \left\lfloor \frac{250}{5} \right\rfloor = 50 \qquad |A_4| = \left\lfloor \frac{250}{7} \right\rfloor = 35$$

$$|A_1 \cap A_2| = \left\lfloor \frac{250}{2\times 3} \right\rfloor = 41 \qquad |A_1 \cap A_3| = \left\lfloor \frac{250}{2\times 5} \right\rfloor = 25$$

$$|A_1 \cap A_4| = \left\lfloor \frac{250}{2\times 7} \right\rfloor = 17 \qquad |A_2 \cap A_3| = \left\lfloor \frac{250}{3\times 5} \right\rfloor = 16$$

$$|A_2 \cap A_4| = \left\lfloor \frac{250}{3\times 7} \right\rfloor = 11 \qquad |A_3 \cap A_4| = \left\lfloor \frac{250}{5\times 7} \right\rfloor = 7$$

$$|A_1 \cap A_2 \cap A_3| = \left\lfloor \frac{250}{2\times 3\times 5} \right\rfloor = 8 \qquad |A_1 \cap A_2 \cap A_4| = \left\lfloor \frac{250}{2\times 3\times 7} \right\rfloor = 5$$

$$|A_1 \cap A_3 \cap A_4| = \left\lfloor \frac{250}{2\times 5\times 7} \right\rfloor = 3 \qquad |A_1 \cap A_3 \cap A_4| = \left\lfloor \frac{250}{3\times 5\times 7} \right\rfloor = 2$$

$$|A_1 \cap A_2 \cap A_3 \cap A_4| = \left\lfloor \frac{250}{2\times 3\times 5\times 7} \right\rfloor = 1$$

we have

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = 125 + 83 + 50 + 35 - 41 - 25 - 17 - 16 - 11 - 7 + 8 + 5 + 3 + 2 - 1 = 193$$

We shall present more examples on the application of the formula (1.3), which is called the *principle of inclusion and exclusion*, in later chapters. ■

* We use $\lfloor x \rfloor$ to denote the largest integer that is smaller than or equal to x.

*1.7 MULTISETS

We recall that a set is a collection of distinct objects. There are many occasions, however, when we encounter collections of nondistinct objects. For example, consider the names of the students in a class. We might have two or more students who have the same name, and we might wish to talk about the collection of the names of the students. We define a *multiset* to be a collection of objects that are not necessarily distinct. Thus, $\{a, a, a, b, b, c\}$, $\{a, a, a, a\}$, $\{a, b, c\}$, and $\{\ \}$ are all examples of multisets. The *multiplicity* of an element in a multiset is defined to be the number of times the element appears in the multiset. Thus, the multiplicity of the element a in the multiset $\{a, a, a, c, d, d\}$ is 3. The multiplicity of the element b is 0, the multiplicity of the element c is 1, and the multiplicity of the element d is 2. Note that sets are merely special instances of multisets in which the multiplicity of an element is either 0 or 1. The cardinality of a multiset is defined to be the cardinality of the set it corresponds to, *assuming* that the elements in the multiset are all distinct.

Let P and Q be two multisets. The union of P and Q, denoted $P \cup Q$, is a multiset such that the multiplicity of an element in $P \cup Q$ is equal to the maximum of the multiplicities of the element in P and in Q. Thus, for $P = \{a, a, a, c, d, d\}$ and $Q = \{a, a, b, c, c\}$

$$P \cup Q = \{a, a, a, b, c, c, d, d\}$$

For example, let the multiset R = {electrical engineer, electrical engineer, electrical engineer, mechanical engineer, mathematician, mathematician, physicist} be the personnel needed in the first phase of an engineering project, and the multiset S = {electrical engineer, mechanical engineer, mechanical engineer, mathematician, computer scientist, computer scientist} be the personnel needed in the second phase of the project. The multiset $R \cup S$ is the personnel we should hire for the project.

The intersection of P and Q, denoted $P \cap Q$, is a multiset such that the multiplicity of an element in $P \cap Q$ is equal to the minimum of the multiplicities of the element in P and in Q. Thus, for $P = \{a, a, a, c, d, d\}$ and $Q = \{a, a, b, c, c\}$

$$P \cap Q = \{a, a, c\}$$

For the example above on the engineering project, the multiset $R \cap S$ is the personnel that will be involved in both phases of the project.

The difference of P and Q, denoted $P - Q$, is a multiset such that the multiplicity of an element in $P - Q$ is equal to the multiplicity of the element in P minus the multiplicity of the element in Q if the difference is positive, and is equal to 0 if the difference is 0 or is negative. For example, let $P = \{a, a, a, b, b, c, d, d, e\}$ and $Q = \{a, a, b, b, b, c, c, d, d, f\}$. We have

$$P - Q = \{a, e\}$$

For the engineering project example, the multiset $R - S$ is the personnel to be reassigned after the first phase of the project.

Note that the definitions of union, intersection, and difference of multisets are so chosen that they are consistent with that of sets. We did not define the symmetric difference of two multisets here; the interested reader might want to see Prob. 1.64.

Finally, we define the sum of two multisets P and Q, denoted $P + Q$, to be a multiset such that the multiplicity of an element in $P + Q$ is equal to the sum of the multiplicities of the element in P and in Q. Note that there is no corresponding definition of the sum of two sets. For example, let $P = \{a, a, b, c, c\}$ and $Q = \{a, b, b, d\}$. We have $P + Q = \{a, a, a, b, b, b, c, c, d\}$. As another example, let R be a multiset containing the account numbers of all the transactions in a bank on a certain day, and S be a multiset containing the account numbers of all the transactions on the next day. R and S are multisets because an account might have more than one transaction in a day. Thus, $R + S$ is a combined record of the account numbers of the transactions in these two days.

1.8 PROPOSITIONS

A *proposition* is a declarative sentence that is either true or false. "It rained yesterday," "The pressure inside of the reactor chamber exceeds the safety threshold," and "We shall have chicken for dinner" are all examples of propositions. On the other hand, "What time is it?" and "Please submit your report as soon as possible" are not propositions because they are not declarative sentences, and, consequently, it is not meaningful to speak of them being true or false. Note that we do not rule out the possibility that a proposition is definitely true such as "15 is divisible by 3," and the possibility that a proposition is definitely false such as "Champaign is the state capital of Illinois." A proposition that is true under all circumstances is referred to as a *tautology*, and a proposition that is false under all circumstances is referred to as a *contradiction*.

We shall frequently refer to propositions by symbolic names. For example, if we let p denote the proposition, "Every student in the class passed the final examination," we can conveniently say that p is true or p is false depending on the outcome of the final examination. The two possibilities of a proposition being true or false are also referred to as the two possible values a proposition might assume. It is customary to use T to denote the value *true* and to use F to denote the value *false*. Consequently, instead of saying that the proposition, "Every student in the class passed the final examination" is true, we can simply say that the value of p is T.

The area of logic which deals with propositions is called the *propositional calculus*. It was developed by the great Greek philosopher Aristotle before 2300 years.

1.9 LOGICAL CONNECTIVES

Two or more existing propositions can be combined to yield new propositions by using logical operators. These logical operators are also known as *logical*

connectives. For example, the two propositions, "Water froze this morning" and "Temperature was below 0°C this morning" are equivalent. Also the two propositions, "He was born in 1934" and "He will be 60 years old in 1994" are equivalent. The two propositions, "I will go to the ball game tonight" and "There is no class tomorrow" might or might not be equivalent. On the other hand, the two propositions, "x is a prime number" and "x is not divisible by 2" are not equivalent because that x is not divisible by 2 does not necessarily mean that x is a prime number.

Propositions can be combined to yield new propositions. For example, in connection with the operation of a company, let p denote the proposition that the volume of the monthly sales is less than \$200,000 and let q denote the proposition that the monthly expenditure exceeds \$200,000. We might want to have a proposition to describe the situation where the volume of the monthly sales is less than \$200,000 and the monthly expenditure exceeds \$200,000. We might also want to have a proposition to describe the situation where either the volume of the monthly sales is less than \$200,000 or the monthly expenditure exceeds \$200,000. Clearly, these propositions are examples of "combinations" of the propositions p and q.

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

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

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

p	$\bar{p}$
F	T
T	F

Fig. 1.9

Let p and q be two propositions. We define the *disjunction* of p and q, denoted $p \vee q$, to be a proposition which is true when either one or both of p and q are true, and which is false when both p and q are false. In the above example on the operation of a company, the disjunction of the proposition that the monthly volume of sales is less than \$200,000 and the proposition that the monthly expenditure is more than \$200,000 is the proposition that either the monthly volume of sales is less than \$200,000 or the monthly expenditure exceeds \$200,000 or both.

Let us consider another example. Suppose p denotes the proposition, "He must be reading" and q represents the proposition, "He must be writing", then $p \vee q$ represents the proposition, "He must be reading or writing". We can denote disjunction by other symbols such as +, and *or*.

Very often, we use *or* in an exclusive sense. When the exclusive *or* is used to combine the propositions p and q, then the proposition "p or q (but not both)" is resulted. This resulting proposition is true when p is true and q is false, and when p is false and q is true. It is false when both p and q are true and when both p and q are false.

Let p and q be two propositions. We define the *exclusive or* of p and q, denoted by $p \oplus q$, to be a proposition which is true when exactly one of p and q is true and is false otherwise. Suppose p represents the proposition, "I shall complete my homework" and q represents the proposition, "I shall go to the school". Then, $p \oplus q$ represents the proposition, "I shall complete my homework or go to the school (but not both)".

Let p and q be two propositions. We define the *conjunction* of p and q, denoted by $p \wedge q$, to be a proposition which is true when both p and q are true, and is false when either one or both of p and q are false. In the foregoing example concerning the operation of a company, the conjunction of the proposition that the monthly volume of sales is less than \$200,000 and the proposition that the monthly expenditure is more than \$200,000 is the proposition that both the monthly volume of sales is less than \$200,000 and the monthly expenditure exceeds \$200,000.

Let us consider another example. Suppose p represents the proposition, "Ram is a boy" and q represents the proposition, "Sita is a girl". So, the solution for $p \wedge q$ is "Ram is a boy and Sita is a girl". According to the truth table, $p \wedge q$ and $q \wedge p$ have the same truth values. Therefore, the statement which contains a conjunction has different meanings for specific purpose. For example, let us consider the proposition, "Sun is red and sky is blue". We can also write the same proposition as, "Sky is blue and sun is red". But, if the proposition is, "He bought a chair and sat on it", then we cannot write, "He sat on it and bought a chair". Here, the meaning of 'and' is of '*and then*'. So, the conjunction '$\wedge$' has different meanings for different situations. We can denote conjunction by other symbols such as '&', a dot (.) or 'AND'.

Let p be a proposition. We define the *negation* of p, denoted $\overline{p}$,* to be a proposition which is true when p is false, and is false when p is true. $\overline{p}$ is read as "not p" and interpreted as "It is not the case that p". Thus, the negation of the proposition that the monthly volume of sales is less than \$200,000 is the proposition that the monthly volume of sales exceeds or equals \$200,000.

Let us consider another example. Suppose p represents, "Hari is a batsman". Then, $\overline{p}$ represents, "Hari is not a batsman".

A proposition obtained from the combination of other propositions is referred to as a *compound* proposition. A proposition that is not a combination of other propositions is referred to as an *atomic* proposition. In other words, a compound proposition is made up of atomic propositions. For example, if p and q are two atomic propositions, then $p \wedge q$, $\overline{p}$, $(p \wedge q) \vee (\overline{p} \wedge q)$, $p \vee (\overline{q})$ are compound propositions. The compound propositions mentioned above are statement formulas derived from the statement variables p and q. So, p and q are called as the components of the statement formulas. It may be noticed that, we have used parentheses in some cases to avoid ambiguity. The use of parenthesis is strongly recommended as $\neg(p \wedge q)$ means negation of the conjunction of p and q

* In the literature, the notation $-p$ or $\neg p$ or $\sim p$ is also used.

whereas $(\neg p) \wedge q$ means negation of p and then conjunction with q. Similarly $\neg(p \vee q) \wedge (p \wedge q)$ means that conjunction of $\neg(p \vee q)$ and $(p \wedge q)$. But for simplicity, we can reduce the number of parenthesis in some cases. For example, we can assume that $\neg p \vee q$ is equivalent to $(\neg p) \vee q$. A convenient and precise way to describe the definition of a compound proposition is a table such as those shown in Fig. 1.9 where the values of a compound proposition are specified for all possible choices of the values of the atomic propositions of the compound proposition. Specifically, the tables in Fig. 1.9 show the definitions of the disjunction, exclusive or and conjunction of two propositions and that of the negation of a proposition. Such tables are called *truth tables* for the compound propositions.

Truth tables help to determine the truth values of compound propositions. There are various combinations of the components of compound proposition in the truth table. Compound propositions have many components. If there are n distinct components in a compound proposition, then we require 2^n possible combinations of truth values in order to construct the truth table. For example, to construct the truth table for $p \vee q$, we require $2^2 = 4$ combinations of truth values as there are 2 components (p and q) involved in $p \vee q$.

Example 1.15 Construct the truth table for $(p \wedge q) \wedge \overline{p}$.

p	q	$p \wedge q$	$\overline{p}$	$(p \wedge q) \wedge \overline{p}$
T	T	T	F	F
T	F	F	F	F
F	T	F	T	F
F	F	F	T	F

■

1.10 CONDITIONALS AND BICONDITIONALS

There are two other important ways to construct compound propositions that we want to present: Consider the propositions, "The temperature exceeds 70°C" and "The alarm will be sounded," which we shall denote p and q, respectively. Also, consider the proposition, "If the temperature exceeds 70°C, then the alarm will be sounded," which we shall denote r. It is easy to see that r is true if the alarm is sounded when the temperature exceeds 70°C (both p and q are true), and r is false if the alarm is not sounded when the temperature exceeds 70°C (p is true and q is false). On the other hand, when the temperature is equal to or less than 70°C (p is false), the proposition r *cannot possibly be false*, no matter whether the alarm is sounded or not. Consequently, we say that r is also true when the temperature is equal to or less than 70°C.

Let us now formalize the notion of combining two propositions p and q to form one that reads "If p then q" introduced in the example above. Let p and q be two propositions. We define a proposition "If p then q," denoted $p \rightarrow q$, which is true if both p and q are true or if p is false, and is false if p is true and q is false,

as specified in the truth table in Fig. 1.10. The compound proposition "If p then q" also reads "p implies q and is called a *conditional statement*. A conditional statement is also called as an *implication*. Here, the statement p is known as the antecedent and q the consequent. According to the definition, it is not mandatory that there should be any kind of relation between p and q in order to construct $p \to q$.

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

Fig. 1.10

Example 1.16 Write the following statement in symbolic form: The hut will be destroyed if there is a cyclone.

Solution: Let the statements be denoted as follows:

p: The hut will be destroyed.

q: There is a cyclone.

It may be observed that the given statement uses "if" in the sense of "If ... then ...". So, the given statement may be rewritten as "If there is a cyclone, then the hut will be destroyed. Now, this statement can be symbolized as $q \to p$. ■

A reader who sees the compound proposition "If p then q" for the first time would probably feel a bit uncertain about the fact that the compound statement is true whenever p is false, no matter whether q is true or not. Let us examine a few more examples. Consider the statement "If you try, then you will succeed." Clearly, if you try and succeed, the statement is true. If you try and fail, the statement is false. However, if you did not try, then there is no way for you to argue that the statement is false. Since not being false means being true, we can conclude that if you did not try, then the statement is true. As another example, consider the order from the security officer of a company that every visitor must wear a badge. Note that the order can be rephrased as a proposition "If one is a visitor, then one wears a badge." To check whether the order has been enforced (whether the proposition is true), we shall stop each person in the plant one by one. If she is a visitor, we can determine whether the order has been enforced by observing whether she is wearing a badge. On the other hand, if she is not a visitor, then there is no way we can possibly conclude that the order has not been enforced, and hence the statement is true. As another example, we recall that in Sec. 1.1 we make a statement that the empty set is a subset of any set. According to the definition of a set being a subset of another set, this statement can be rephrased as "If x is an element of the empty set then x is an element of any set". Clearly, the statement is true.

Example 1.17 John made the following statements:

1. I love Lucy.
2. If I love Lucy, then I also love Vivian.

Given that John either told the truth or lied in both cases, determine whether John really loves Lucy. Suppose John lied. Then according to statement 1, he does not love Lucy. It follows that statement 2 must be true, which is a contradiction. Consequently, John must have told the truth, and we can confirm that he really loves Lucy.

One can also be a bit more formal by letting p denote the statement, "John loves Lucy," and q denote the statement, "John loves Vivian." The truth table in Fig. 1.10 shows that it is possible for both p and $p \to q$ to be true but not possible for both of them to be false. ■

There are some related *implications* which can be constructed from $p \to q$. For the proposition $p \to q$, the proposition $q \to p$ is called its *converse*. The proposition $\overline{q} \to \overline{p}$ is called the *contrapositive* of $p \to q$. The proposition $\overline{p} \to \overline{q}$ is called the *inverse* of $p \to q$. It may be observed that, only the contrapositive, $\overline{q} \to \overline{p}$, of an implication $p \to q$ has the same truth value as $p \to q$. The converse, $q \to p$, and the inverse, $\overline{p} \to \overline{q}$ do not have the same truth value as $p \to q$.

Example 1.18 Give the converse, contrapositive and inverse of the following implication: "If it rains today, I will go to college tomorrow."

Solution: The converse, contrapositive and inverse of the above implication can be written as follows:

Converse: I will go to college tomorrow only if it rains today.

Contrapositive: If I do not go to college tomorrow, then it will not have rained today.

Inverse: If it does not rain today, then I will not go to college tomorrow. ■

Let p denote the proposition, "A new computer will be acquired" and q denote the proposition, "Additional funding is available." Consider the proposition, "A new computer will be acquired if and only if additional funding is available," which we shall denote r. Clearly, r is true if a new computer is indeed acquired when additional funding is available. (Both p and q are true.) The proposition r is also true if no new computer is acquired when additional funding is not available. (Both p and q are false.) On the other hand, r is false if a new computer is acquired although no additional funding is available (p is true and q is false), or if no new computer is acquired although additional funding is available (p is false and q is true).

Let p and q be two propositions. We define a proposition, "p if and only if q," denoted $p \leftrightarrow q$, which is true if both p and q are true or if both p and q are false, and which is false if p is true while q is false and if p is false while q is true. The compound proposition $p \leftrightarrow q$ is also interpreted as "p is necessary and sufficient for q" and is called a *biconditional statement*. The truth table in Fig. 1.11 shows the definition of $p \leftrightarrow q$.

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

Fig. 1.11

Example 1.19 An island has two tribes of natives. Any native from the first tribe always tells the truth, while any native from the other tribe always lies. You arrive at the island and ask a native if there is gold on the island. He answers, "There is gold on the island if and only if I always tell the truth." Which tribe is he from? Is there gold on the island? As it turns out, we cannot determine which tribe he is from. However, we can determine if there is gold on the island. Let p denote the proposition that he always tells the truth, and q denote the proposition that there is gold on the island. Thus, his answer is the proposition $p \leftrightarrow q$. Suppose that he always tells the truth; that is, the proposition p is true. Furthermore, his answer to our question must be true; that is, $p \leftrightarrow q$ is true. Consequently, q must be true. Suppose he always lies; that is, the proposition p is false. Also, his answer to our question is a lie, which means that $p \leftrightarrow q$ is false. Consequently, q must be true. Thus, in both cases we can conclude that there is gold on the island, although the native could have been from either tribe. ■

We can combine compound propositions to yield new propositions. For example, let p and q be propositions. We have $p \wedge q$, $\bar{p} \wedge \bar{q}$ and, consequently,

$$((p \wedge q) \vee (\bar{p} \wedge \bar{q})) \rightarrow p \qquad (1.7)$$

as compound propositions where parentheses are used as delimiters. The value of a compound proposition can always be determined by constructing its truth table in a step-by-step manner. As the table in Fig. 1.12 shows, the entries for the columns corresponding to the compound propositions can be constructed column by column from left to right.

p	q	$p \wedge q$	$\bar{p} \wedge \bar{q}$	$(p \wedge q) \vee (\bar{p} \wedge \bar{q})$	$((p \wedge q) \vee (\bar{p} \wedge \bar{q})) \rightarrow p$
F	F	F	T	T	F
F	T	F	F	F	T
T	F	F	F	F	T
T	T	T	F	T	T

Fig. 1.12

1.11 WELL-FORMED FORMULAS

We have already introduced the notion of a statement formula in earlier sections. A statement formula is an expression which consists of variables, parentheses, and connective symbols. All such expressions are not statement formulas. Now, we shall present a formal definition of a statement formula. This is also called as a *well-formed formula (wff)*. A well-formed formula can be produced by using the following rules:

Rule 1: A statement variable itself is a well-formed formula.

Rule 2: If p is a well-formed formula, then $\bar{p}$ is also a well-formed formula.

Rule 3: If p and q are two well-formed formulas, then $(p \vee q)$, $(p \wedge q)$, $(p \rightarrow q)$, and $(p \leftrightarrow q)$ are also well-formed formulas.

Rule 4: A string of symbols consisting of the statement variables, connectives, and parentheses is said to be a well-formed formula, if and only if it can be produced by applying *rules 1, 2 and 3* finitely many times.

Example 1.20 The following, are some well-formed formulas according to this definition:

$$\overline{(p \wedge q)},\ (p \rightarrow (q \rightarrow r)),\ (p \rightarrow (p \wedge q)),\ ((p \rightarrow q) \leftrightarrow (\bar{p} \vee q))$$

To reduce the number of parentheses in the well-formed formulas, some conventions may be introduced. For example, we shall omit the outmost parentheses for our convenience. So, we shall write $\overline{p \wedge q}$ instead of $\overline{(p \wedge q)}$, $p \rightarrow (q \rightarrow r)$ instead of $(p \rightarrow (q \rightarrow r))$, $p \rightarrow (p \rightarrow q)$ instead of $(p \rightarrow (p \wedge q))$ and $(p \rightarrow q) \leftrightarrow (\bar{p} \vee q)$ instead of $((p \rightarrow q) \leftrightarrow (\bar{p} \vee q))$. Since, the only formulas we shall discuss in this chapter are well-formed formulas, we shall simply use the term 'formula' for well-formed formulas. ■

1.12 TAUTOLOGIES

A truth table which is constructed for a given formula represents the truth value which results when the variables are replaced by statement formulas. It is the final column of the truth table which decides the truth value for the whole statement formula. The truth values in the last column of the truth table generally depend upon the truth values of the statement variables rather than on the formulas themselves. But, for the sake of easiness, we use the term "the truth value of a formula" to mean the values of the entries in the last column of the truth table. It is possible to have a case where all the truth values in the last column can be True (T) or can be False (F).

Example 1.21 Let us consider the truth tables for $p \wedge \bar{p}$ and $p \vee \bar{p}$.

Case 1: $p \wedge \bar{p}$, here, all the entries in the last column are false.

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

Truth table for $p \wedge \bar{p}$

Case 2: $p \wedge \bar{p}$, here, all the entries in the last column are true.

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

Truth table for $p \vee \bar{p}$ ■

Such a statement formula whose truth value is always true regardless of the truth values of the variables concerned is called a *universally valid formula* or a *tautology* and the statement formula whose all truth values are false, is called a *contradiction*.

It may be observed that the conjunction of two tautologies is also a tautology. If p and q be two statement formulas which are tautologies, then $p \wedge q$ is also a tautology. The negation of a tautology is also a tautology.

A formula p is called a *substitution instance* of another formula q, if p can be generated from q by substituting formulas for some variables of q. Here, the condition required is that the same formula is substituted for the same variable each time it occurs.

Example 1.22 Let $(p \wedge q) \rightarrow p$ be a formula.

If we replace p by $p \leftrightarrow q$,

Then

$((p \leftrightarrow q) \wedge q \rightarrow (p \leftrightarrow q))$ is a substitution instance of the given formula.

It should be remembered that the substitutions are performed only for the atomic formulas, but not for the compound formulas. So, $p \rightarrow q$ is not a substitution instance of $p \rightarrow \bar{r}$ because, in this case r should be replaced and not $\bar{r}$. It may be observed that, the substitution instance of a tautology is also a tautology. ■

1.13 LOGICAL EQUIVALENCES

Let p and q be two statement formulas and $a_1, a_2, \ldots a_n$ represent all the variables contained in both p and q. If there exists an assignment of truth values to the statement variables $a_1, a_2, \ldots a_n$ and the resulting truth values of p and q, such that the truth value of p is equal to the truth value of q for each of the 2^n possible sets of truth values, then p and q are said to be *logically equivalent* or simply *equivalent*. In other words, we can say that, the compound propositions which have the same truth values in all possible cases are called *logically equivalent*. Let us assume that the variables and the assignment of truth values to the variables appear in the same order in both the truth tables of p and q. It may be observed that, if p and q are equivalent, then the final columns in both the truth tables of p and q are identical.

For example:

i. $p \vee p$ is equivalent to p.

ii. $p \vee \bar{q}$ is equivalent to $\bar{q} \vee p$.

iii. $\bar{q} \vee q$ is equivalent to $p \vee \bar{p}$.

From the definition of *bi-conditional*, it can be observed that $p \leftrightarrow q$ is true whenever p and q have the same truth values. So, we can say that p and q are *logically equivalent* if $p \leftrightarrow q$ is a *tautology*. Conversely, if $p \leftrightarrow q$ is a *tautology*, then p and q are *equivalent*. We represent the equivalence of two statement formulas, say p and q, by writing $p \equiv q$, which may be read, as "p is equivalent to q". It can be proved that equivalence of two statement formulas is a symmetric relation, i.e. if $p \equiv q$ then $q \equiv p$. Also, this relationship is transitive, i.e. if $p \equiv q$, and $q \equiv r$, then $p \equiv r$.

We can determine whether two propositions are equivalent by examining their truth tables. For example, according to the truth tables in Figs. 1.9 and 1.12, the proposition in (1. 7) is equivalent to the proposition $p \vee q$. As another example, we note that the two propositions $p \leftrightarrow q$ and $(p \rightarrow q) \wedge (q \rightarrow p)$ are equivalent by comparing the truth tables in Figs. 1.11 and 1.13. Indeed, we realize that the choice of the notation $p \leftrightarrow q$ is not accidental.

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

Fig. 1.13

Example 1.23 There are two restaurants next to each other. One has a sign that says, "Good food is not cheap," and the other has a sign that says, "Cheap food is not good." Are the signs saying the same thing? Let g denote the proposition that the food is good, and c denote the proposition that the food is cheap. The first sign can then be written as $g \rightarrow \bar{c}$, and the second sign be written as $c \rightarrow \bar{g}$. The truth table in Fig. 1.14 shows that indeed the two signs say the same thing. ■

g	c	$\bar{g}$	$\bar{c}$	$g \rightarrow \bar{c}$	$c \rightarrow \bar{g}$
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	T	T
T	T	F	F	F	F

Fig. 1.14

Example 1.24 As a final example, we ask the reader to verify that the two propositions

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

and

$$((\bar{p} \vee (\bar{q} \wedge \bar{r})) \vee s$$

are equivalent. ■

We shall discuss the subject of constructing, manipulating, and simplifying compound propositions in Chapter 11, after we have developed the concept of boolean algebras.

A reader probably will recognize that the combination of propositions to yield new propositions bears a strong similarity to the combination of sets to yield new sets. To be specific, we note the similarity between the notions of the union of two sets and of the disjunction of two propositions, between the notions of the

intersection of two sets and of the conjunction of two propositions, and between the notions of the complement of a set and of the negation of a proposition. Such similarities are not accidental, as we shall see in Chapter 11.

1.14 THEORY OF INFERENCE FOR STATEMENT CALCULUS

One of the important functions of logic is to provide principles of reasoning or rules of inference. The theory associated with these rules is known as *inference theory* since it deals with the inferring of a conclusion from some premises or facts or axioms. The process of deriving a conclusion from a set of premises by using the standard rules of inference, is called a *formal proof* or *deduction*. In a formal proof, each rule of inference which is used at any step of the derivation is explicitly mentioned.

Let us see what we mean by the rules and theory of inference. The rules of inference mean the criteria for finding the validity of an argument. The rules are expressed in the forms of statements involved.

In any argument, a conclusion is said to be true if the premises are considered to be true, and the reasoning used in derivation of the conclusion follows some standard rules of inference. This type of argument is called *sound*. In logic, we give importance on the discussion of the rules of inference by using which conclusions are derived. Any conclusion which is derived by using these rules is called a *valid conclusion* and the corresponding argument is called a *valid argument*. In other words, we can say that in logic, our important concern is the *validity* but not necessarily the *soundness* of an argument.

1.14.1 Validity Using Truth Tables

Let p and q be two statement formulas. We define "q is a valid conclusion of the premise p" or "q logically follows from p" if and only if $p \rightarrow q$ is a tautology. We can extend this definition to include a set of formulas. We say that C is a valid conclusion of the set of premises $\{A_1, A_2, \ldots, A_n\}$ if and only if $A_1 \wedge A_2 \wedge \ldots \wedge A_n \rightarrow C$ is a tautology. Suppose a set of premises and a conclusion is given to us. Then, we can determine whether the conclusion is a valid conclusion of the given premises by constructing truth tables.

Theoretically, it may be possible to determine in a finite number of steps whether a conclusion is a valid conclusion of the given set of premises by constructing truth tables. But, when the number of variables present in all the statement formulas is large, then this method seems to be very much tedious. This limitation suggests investigating some other possible techniques. We shall discuss some more possible techniques in the next section.

1.14.2 Rules of Inference

Now, we present the derivation process by which one can justify that a particular formula is a valid conclusion of a given set of premises. Before describing the

derivation process, we present three rules of inference which we call *Rule P*, *Rule T* and *Rule CP*.

Rule P: A premise can be inserted at any point in the derivation.

Rule T: If the formula q is tautologically implied by any one or more of the previous formulas in a derivation, then q can be inserted in the derivation.

Rule CP: *Rule CP* stands for rule of conditional proof. It is also known as *deduction theorem*. It states that, if we can derive a formula q from p and a set of premises, then we can derive $p \rightarrow q$ from the set of premises alone.

Rule CP, is used in the cases, where the conclusion is of the form $p \rightarrow q$. In these cases, p is taken as an extra premise and q is derived from the given premises and from p.

The tautology $(p \wedge (p \rightarrow q)) \rightarrow q$ is the basis for the rule of inference, called *modus ponens* or *law of detachment*.

Before describing the actual process of derivation, we present some important implications and equivalences in Tables 1.1 and 1.2 that will be used very often. The implications and equivalences which will be used more often than the others are given special names.

Now, we present some examples to explain the use of some of the important implications and equivalences in the process of derivation.

Example 1.25 Let the implication, "If it rains today, then I shall carry an umbrella" and its hypothesis, "It is raining today", are true. Then, by modus

Table 1.1 Some Important Implications

Rule No.	*Tautology*
IM_1	$p \wedge q \rightarrow p$ (simplification)
IM_2	$p \wedge q \rightarrow q$ (simplification)
IM_3	$p \rightarrow (p \vee q)$ (addition)
IM_4	$q \rightarrow (p \vee q)$ (addition)
IM_5	$\overline{p} \rightarrow (p \rightarrow q)$
IM_6	$q \rightarrow (p \rightarrow q)$
IM_7	$\overline{(p \rightarrow q)} \rightarrow p$
IM_8	$\overline{(p \rightarrow q)} \rightarrow \overline{q}$
IM_9	$p, q \rightarrow p \wedge q$ (conjunction)
IM_{10}	$[\overline{p}, (p \vee q)] \rightarrow q$ (disjunctive syllogism)
IM_{11}	$[p, (p \rightarrow q)] \rightarrow q$ (modus ponens)
IM_{12}	$[\overline{q}, (p \rightarrow q)] \rightarrow \overline{p}$ (modus tollens)
IM_{13}	$[p \rightarrow q, q \rightarrow r] \rightarrow (p \rightarrow r)$ (hypothetical syllogism)
IM_{14}	$[p \vee q, p \rightarrow r, q \rightarrow r] \rightarrow r$ (dilemma)
IM_{15}	$[p \vee q, \overline{p} \vee r] \rightarrow (q \vee r)$ (resolution)

Table 1.2 Some Important Equivalences

EQ_1	$\overline{\overline{p}} \equiv p$ (double negation law)
EQ_2	$p \vee q \equiv q \vee p$ (commutative law)
EQ_3	$p \wedge q \equiv q \wedge p$ (commutative law)
EQ_4	$(p \vee q) \vee r \equiv p \vee (q \vee r)$ (associative law)
EQ_5	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ (associative law)
EQ_6	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ (distributive law)
EQ_7	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ (distributive law)
EQ_8	$\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$ (De Morgan's law)
EQ_9	$\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$ (De Morgan's law)
EQ_{10}	$p \vee p \equiv p$ (idempotent law)
EQ_{11}	$p \wedge p \equiv p$ (idempotent law)
EQ_{12}	$r \vee (p \wedge \overline{p}) \equiv r$
EQ_{13}	$r \wedge (p \vee \overline{p}) \equiv r$
EQ_{14}	$r \vee (p \vee \overline{p}) \equiv T$
EQ_{15}	$r \wedge (p \wedge \overline{p}) \equiv F$
EQ_{16}	$p \rightarrow q \equiv \overline{p} \vee q$
EQ_{17}	$\overline{p \rightarrow q} \equiv p \wedge \overline{q}$
EQ_{18}	$p \rightarrow q \equiv \overline{q} \rightarrow \overline{p}$
EQ_{19}	$p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$
EQ_{20}	$\overline{p \leftrightarrow q} \equiv p \leftrightarrow \overline{q}$
EQ_{21}	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
EQ_{22}	$(p \leftrightarrow q) \equiv (p \wedge q) \vee (\overline{p} \wedge \overline{q})$
EQ_{23}	$p \vee (p \wedge q) \equiv p$ (absorption law)
EQ_{24}	$p \wedge (p \vee q) \equiv p$ (absorption law)
EQ_{25}	$p \vee \overline{p} \equiv T$ (negation law)
EQ_{26}	$p \wedge \overline{p} \equiv F$ (negation law)

ponens, it is clear that the conclusion of the implication, "I shall carry umbrella" is true. ■

Example 1.26 Show that q is a valid inference from the premises $p \rightarrow q$, $p \vee q$, and $\overline{q}$.

Solution:

{1}	(1) $p \rightarrow q$	*Rule P*
{2}	(2) $\overline{q}$	*Rule P*
{1, 2}	(3) $\overline{p}$	*Rule T*, (1), (2), and modus tollens
{4}	(4) $p \vee q$	*Rule P*
{1, 2, 4}	(5) q	*Rule T*, (3), (4) and disjunctive syllogism.

Here, the first column of numbers for each row represents the premises on which the formula in the row depends. The second column of numbers shows the formula as well as the row of derivation in which it occurs. In the last column, P or T represents the rule of inference followed by a comment describing from which formulas and tautology that particular formula has been derived. For example, the fifth row represents that the formula in this row is numbered as (5) and has been derived from the premises in (1), (2) and (4). In this row, the formula q has been derived by applying *Rule T* on formulas present in (3) and (4) and by using the implication *disjunctive syllogism.* ■

Example 1.27 Show that $\overline{p}$ is tautologically implied by $\overline{(p \wedge \overline{q})}$, $\overline{q} \vee r$, $\overline{r}$.

Solution:

{1}	(1) $\overline{(p \wedge \overline{q})}$	*Rule P*
{1}	(2) $\overline{p} \vee q$	*Rule T*, (1) and De Morgan's law
{1}	(3) $p \rightarrow q$	*Rule T*, (2) and EQ_{16} $(p \rightarrow q \equiv \overline{p} \vee q)$
{4}	(4) $\overline{q} \vee r$	*Rule P*
{4}	(5) $q \rightarrow r$	*Rule T*, (4) and EQ_{16} $(p \rightarrow q \equiv \overline{p} \vee q)$
{1, 4}	(6) $p \rightarrow r$	*Rule T*, (3), (5) and hypothetical syllogism
{7}	(7) $\overline{r}$	*Rule P*
{1, 4, 7}	(8) $\overline{p}$	*Rule T*, (6), (7) and modus tollens. ■

Example 1.28 Derive the following using the *CP* rule:

$$(\overline{p} \vee q, \overline{q} \vee r, r \rightarrow s) \rightarrow (p \rightarrow s)$$

Solution: According to the *CP* rule, here, we will include p as an additional premise and show s first.

{1}	(1) $\overline{p} \vee q$	*Rule P*
{1}	(2) $p \rightarrow q$	*Rule T*, (1) and EQ_{16} $(p \rightarrow q \equiv \overline{p} \vee q)$
{3}	(3) p	P (assumed premise)
{1, 3}	(4) q	*Rule T*, (2),(3) modus ponens
{5}	(5) $\overline{q} \vee r$	*Rule P*
{1, 3, 5}	(6) r	*Rule T*, (4), (5) and disjunctive syllogism
{7}	(7) $r \rightarrow s$	*Rule P*
{1, 3, 5, 7}	(8) s	*Rule T*, (6), (7) and modus ponens.
{1, 5, 7}	(9) $p \rightarrow s$	*Rule CP.* ■

Example 1.29 Show that the following system is inconsistent:

$$p \rightarrow q, p \rightarrow r, q \rightarrow \overline{r}, p$$

Solution:

{1}	(1) $p \rightarrow q$	*Rule P*

		Rule P
{2}	(2) p	*Rule T*, (1), (2) and modus ponens
{1, 2}	(3) q	*Rule P*
{4}	(4) $p \to r$	*Rule T*, (2), (4) and modus ponnes
{2, 4}	(5) r	*Rule T*, (3), (5) and conjunction
{3, 5}	(6) $q \wedge r$	*Rule P*
{7}	(7) $q \to \bar{r}$	*Rule T*, (7) and EQ_{16} $(p \to q \equiv \bar{p} \vee q)$
{7}	(8) $\bar{q} \vee \bar{r}$	*Rule T*, (8) and De Morgan's law
{7}	(9) $\overline{q \wedge r}$	*Rule T*, (6), (9) and conjunction.
{1, 2, 5, 7}	(10) $(q \wedge r) \wedge \overline{q \wedge r}$	

Since, we obtain $(q \wedge r) \wedge \overline{q \wedge r}$, which is a contradiction, so we conclude that the given system is inconsistent. ■

1.14.3 Consistency of Premises

A set of formulas $A_1, A_2, \ldots A_m$ is said to be consistent if their conjunction has the truth value T for some assignment of the truth values to the atomic variables appearing in $A_1, A_2, \ldots A_m$.

If for every assignment of the truth values to the atomic variables at least one of the formulas $A_1, A_2, \ldots A_m$ is false, so that their conjunction is identically false, then the formulas $A_1, A_2, \ldots A_m$ are called inconsistent.

Alternatively, a set of formulas $A_1, A_2, \ldots A_m$ is inconsistent if their conjunction implies a contradiction, that is,

$A_1 \wedge A_2 \wedge \ldots \wedge A_m \to B \wedge \bar{B}$, where B is any formula. It may be noted that $B \wedge \bar{B}$ is a contradiction and it is necessary and sufficient for the implication that $A_1 \wedge A_2 \wedge \ldots \wedge A_m$ is a contradiction.

This notion of inconsistency is used in a procedure called *proof by contradiction* or *reduction* and *absurd* or *indirect method of proof.*

Example 1.30 Using indirect method show that

$$(r \to \bar{q}, r \vee s, s \to \bar{q}, p \to q) \to \bar{p}.$$

Solution: Following the indirect method, we introduce p as an additional premise and show that this additional premise leads to a contradiction.

{1}	(1) $p \to q$	*Rule P*
{2}	(2) p	*Rule P* (assumed)
{1, 2}	(3) q	*Rule T*, (1), (2) and modus ponens
{4}	(4) $s \to \bar{q}$	*Rule P*
{1, 2, 4}	(5) $\bar{s}$	*Rule T*, (3), (4) and modus tollens
{6}	(6) $r \vee s$	*Rule P*
{1, 2, 4, 6}	(7) r	*Rule T*, (5), (6) disjunctive syllogism
{8}	(8) $r \to \bar{q}$	*Rule P*

{8}	(9) $\bar{r} \vee \bar{q}$	*Rule T*, (8) and EQ_{16} $(p \to q \equiv \bar{p} \vee q)$
{8}	(10) $\overline{r \wedge q}$	*Rule T*, (8) and De Morgan's law
{1, 2, 4, 6}	(11) $r \wedge q$	*Rule T*, (7), (3) and conjunction
{1, 2, 4, 6, 8}	(12) $r \wedge q \wedge \overline{r \wedge q}$	*Rule T*, (10), (11) and conjunction.

Hence it leads to a contradiction. ■

1.15 PREDICATE CALCULUS

After getting some idea about statements and statement formulas, now let us pay attention to the concept of a predicate in an atomic statement. The logic associated with the predicates in any statement is called *predicate logic*. In this section, we shall discuss the predicates and predicate calculus. Let us first know what these predicates are?

Consider the two statements:

1. Dog is an animal.
2. Cat is an animal.

Since, both the statements are about two individuals which are animals, so expressing these statements by symbols will require two different symbols to denote them.

But, if a new symbol is introduced to denote the phrase, "is an animal" and if by some method we join it with symbols denoting the name of individuals, we are done. The part, "is an animal" is called a *predicate*. Writing the two statements in this form will reveal the common feature also.

We shall use capital letters to represent predicates and lower case letters to represent the names of individuals or objects in general. So, a statement can be written symbolically in terms of the predicate letter followed by the name(s) of the object(s) to which the predicate is applied. Let us again consider the above two statements. Suppose, the predicate, "is an animal" is represented by the predicate letter A, "Dog' by d and "Cat" by c. Then the statements (1) and (2) can be written as $A(d)$ and $A(c)$. In general, any statement of the type "r is S", where S is a predicate and r is the subject, can be written as $S(r)$. A statement which is expressed by using a predicate letter must have at least one name of an object associated with the predicate.

A predicate may require more than one name to express a statement. A predicate that requires $n (n > 0)$ names is known as an n-place predicate. Let us understand it with some examples:

3. The predicate A in (1) and (2) is a one place predicate
4. Consider the statement: x is greater than y.

Suppose predicate G represents "greater than". Then, G is a 2-place predicate since two names are required to express the statement as $G(x, y)$.

In general, if P is an n-place predicate letter and $x_1, x_2, \ldots, x_n$ are the names of objects, then, $P(x_1, x_2, \ldots, x_n)$ denotes a statement.

1.16 THE STATEMENT FUNCTION, VARIABLE AND QUANTIFIERS

Consider the phrase, "y is a man". Let this be expressed as $M(y)$. It may be noted that $M(y)$ is not a statement. However, if y is replaced by a name an such as a and a, b, s etc. then it will result in a statement. For example, $M(a)$, $M(b)$, and $M(s)$ represent statements.

We define a *simple statement function* of one variable as an expression which consists of a predicate symbol and an individual variable. Here, $M(y)$ is a simple statement function of one variable. The statement function turns to be a statement when the variable is replaced by the name of an object. The statement which is obtained from the statement function by a replacement is called a *substitution instance* of the statement function.

We can form *compound statement functions* by combining one or more simple statement functions and the logical connectives. Suppose $M(x)$ represents "x is a man" and $V(x)$ represents "x is a vegetarian". Then, we can compose many compound statements such as

$$M(x) \wedge V(x),\ \sim M(x) \vee V(x),\ \sim V(x) \text{ etc.}$$

It is possible to form statement functions of two variables by using statement function of one variable.

For example, let $M(x)$: x is a man

$V(y)$: y is a vegetarian,

Then, $M(x) \wedge V(y)$: x is a man and y is a vegetarian.

But, always it is not possible to express statement functions of two variables using statement functions of one variable.

So far, we have known that statements can be obtained from statement functions by replacing the variables with names of objects. There is another method to obtain the statements. In order to understand this alternative method, let us first consider the following statements:

5. All dogs are animals.
6. Every rose is red.

Clearly, each one is a statement about all individuals or objects belonging to a particular set.

We can also write the above statements in the following way:

(5′) For all x, if x is a dog, then x is an animal.

(6′) For all x, if x is a rose, then x is red.

Now, if a symbol is introduced which denote the phrase "For all x" then the statements (5′) and (6′) can be symbolized.

We use the symbol $(\forall x)$ or (x) to represent the phrase "For all x". Now, using the following:

$D(x)$: x is a dog

$A(x)$: x is an animal

$R(x)$: x is red

$C(x)$: x is rose

(5′) and (6′) can be written as:

5″. $\forall x(D(x) \rightarrow A(x))$

6″. $\forall x(C(x) \rightarrow R(x))$.

The symbols (x) or $\forall x$ are called *universal quantifiers* and represent "for all x", "Every x", "for any x". It may be noted that statements remain unchanged if the quantifying variable, say x, is changed or replaced by another variable, say y, throughout. For example, the statements $(x)\,(D(x) \rightarrow A(x))$ and $(y)\,(D(y) \rightarrow A(y))$ are equivalent.

Now let us introduce another quantifier which symbolizes the expression such as "there exists some" or "there is at least one". This quantifier is called *existential quantifier* and symbolized as $(\exists x)$. The area of logic that deals with predicates and quantifiers is called *predicate calculus*.

Example 1.31

(a) Symbolize the expression "Some roses are red".

Solution: $(\exists x)\,(C(x) \wedge R(x))$

(b) Symbolize the expression "Some numbers are irrational".

Solution:

Let I: x is irrational.

N: x is a number.

Then, the above statement can be symbolized as

$$(\exists x)\,(N(x) \wedge I(x))$$

It may be observed that a conjunction is used with the existential quantifier and an implication is used with the universal quantifier. ■

1.16.1 Predicate Formulas

From the earlier discussions, we know that $P(x_1, x_2, \ldots, x_n)$ denotes an n-place predicate formula in which P is the predicate and $(x_1, x_2, \ldots, x_n)$ are n individual variables or objects. Normally, the expression $P(x_1, x_2, \ldots, x_n)$ is called an *atomic formula* of predicate calculus. Now, we present some examples of atomic formulas.

Example 1.32 S $M(y)$, $P(b, a, x)$, $M(x, y, z)$

Some rules should be kept in mind while obtaining a well-formed formula (wff) of a predicate calculus. The rules are:

1. An atomic formula is a well formed formula.
2. If A and B are well formed formulas (well-formed formulas), then $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ and $(A \equiv B)$ are also well-formed formulas.

3. If M is a well formed formula, then $\overline{M}$ is also a well-formed formula.
4. If M is a well formed formula, then $(x)M$ and $(\exists x)M$ are also well-formed formulas, where x is any variable.
5. Only the formulas which are obtained by applying rules (1) to (4) are well formed formulas.

Note: As mentioned earlier, we shall use the term "formula" for "well-formed formula" in rest of the chapter.

1.17 FREE AND BOUND VARIABLE

If any formula contains a part like $(\exists x)\ M(x)$ or $(\forall x)\ M(x)$, then that part is called *x-bound* part of the formula. Any occurrence of x in an x-bound part, is known as a *bound occurrence* of x. Any occurrence of x which is not a bound occurrence is known as *free occurrence*. The formula that immediately follows the quantifier is known as the *scope of the quantifier*. In other words, the *scope of a quantifier* is the part of a logical expression to which the quantifier is applied. So, a variable is free if it lies outside the scope of all quantifiers in the formula which specifies this variable. For example, the formula $M(x)$ in $(\exists x)$ $M(x)$ or $(\forall x)\ M(x)$ is known as the *scope of the quantifier*.

Example 1.33

(i) $(x)\ M(x)$
Here, $M(x)$ is the scope of the quantifier

(ii) $(\exists x)\ (M(x) \wedge N(x))$
Here, $[M(x) \wedge N(x)]$ is the scope of quantifier and all occurrences of x are bound.

(iii) $M(x) \wedge \exists(x)\ N(x)$

Here, scope of $(\exists x)$ is $N(x)$ and it contains bound occurrence of x while occurrence of x in M is free. ■

It should be kept in mind that bound variable can be replaced by any other variable but not by a constant. Hence, the formulas $(x)\ M(y, x)$ and $(z)\ M(y, z)$ are same.

It may be observed that, if there is a free variable in the formula, then we have a statement function and in the case when every occurrence of a variable is bound and no variable has free occurrence, then we get a statement.

Example 1.34 Write the following predicate in symbolic form: "Someone in your school has visited Agra".

Solution: Let $S(x)$: x is in your school.
$A(x)$: x has visited Agra.

We symbolize the predicate as

$$(\exists x)\ (S(x) \wedge A(x)).$$

■

Example 1.35 Symbolize the expression "Everyone has exactly one favorite language".

Solution: Let $M(y, x)$: y is the favorite language of x.
Then, we can symbolize the statement as

$$(\forall x)\ (\exists y)\ (M(y, x) \wedge ((\forall z)\ (z \neq y) \rightarrow \overline{M}(z, x))).$$ ■

1.17.1 The Universe of Discourse

Example 1.35 indicates that symbolizing a statement in predicate calculus could be very much complex. The complexity can be reduced to some extent by restricting the class of individuals or objects under consideration. According to this restriction, the quantified variables represent only those objects which belong to a specific domain or class. This restricted class is known as the *universe of discourse* or simply *universe*. For example, if the present discussion is on integers only, then the universe of discourse could be the set of integers. If the discussion is based on fruits only, then the universe of discourse is the class of fruits. Now, we explain the concept of the universe of discourse with some examples.

Example 1.36 Symbolize the statement "All dogs are animal".

Solution: Let $D(x)$: x is a dog.
$A(x)$: x is an animal.

Then the given statement can be symbolized as

$$(x)\ (D(x) \rightarrow A(x))$$

If the universe of discourse is taken into account and the universe is the set of all dogs, then the above statement can be symbolized as $(x)\ A(x)$. ■

Example 1.37 Symbolize the statement "Everyone in final year class has a cellular phone".

Solution: Let $C(x)$: x is in final year class.
$P(x)$: x has a cellular phone.

Then the given statement can be symbolized as

$$(x)\ (C(x) \rightarrow P(x)) \text{ (without using universe)}$$

Let the universe be the set of all students in final year class. Then the above statement can be symbolized as $(x)\ P(x)$.

The universe of discourse must be defined clearly as the truth value of a statement depends on it. In order to illustrate this, let us consider the following example. ■

Example 1.38 Consider the predicate

$P(x)$: x is greater than 2.

and the statements $(x)\,P(x)$ and $(\exists x)\,P(x)$. Suppose, the universe of discourse is stated as:

(a) $\{-5, -3, 0, 1, 2\}$
(b) $\{3, 5, 7, 10\}$
(c) $\{-1, 0, 2, 6\}$

Then, the statement $(x)\,P(x)$ is true only for the universe of discourse (b) and false for (a) and (c). Similarly, the statement $(\exists x)\,P(x)$ is true for both (b) and (c) and false for (a). ■

1.18 INFERENCE THEORY OF PREDICATE CALCULUS

In this section, we discuss the inference theory of predicate calculus. We will use the same terminologies and notations as that used for statement calculus.

1.18.1 Valid Formulas and Equivalences

A formula P is said to be a valid formula in the universe of discourse S if, for every assignment of object names from S to the corresponding variable names in P and for every assignment of statement to statement variables, the resulting statements have truth value T.

Let P and Q be two predicate formulas defined over the universe S. We define the equivalence of P and Q as follows:

If, for every assignment of object names from the universe of discourse S to every variable of P and Q, the resulting statements have identical truth values, then the predicate formulas P and Q are said to be equivalent over the universe S. We denote this as $P \equiv Q$.

All possible substitutions of the object variables can be enumerated, if the universe of discourse is a finite set. But this is not possible in the case of infinite universe of discourse.

Let the universe of discourse be denoted by the finite set S such that $S = \{q_1, q_2, \ldots, q_n\}$.

From the concepts of quantifiers and by the process of enumeration of all the objects in S, it can be observed that,

$$(x)\,P(x) \equiv P(q_1) \wedge P(q_2) \wedge \ldots \wedge P(q_n)$$
$$(\exists x)\,P(x) \equiv P(q_1) \vee P(q_2) \vee \ldots \vee P(q_n)$$

Now, we will prove the following two important equivalences by using the above two expressions and De Morgan's law.

(i) $\sim((x)\,P(x)) \equiv (\exists x) \sim P(x)$
(ii) $\sim((\exists x)\,P(x)) \equiv (x) \sim P(x)$

Proof

(i) $\sim((x)\,P(x)) \equiv \sim[[P(q_1) \wedge P(q_2) \wedge \ldots \wedge P(q_n)]$

$$\equiv \sim P(q_1) \vee \sim P(q_2) \vee \ldots \vee \sim P(q_n)$$
(by using De Morgan's law)
$$\equiv (\exists x) \sim P(x)$$

(ii) $\sim((\exists x)\,P(x)) \equiv \sim[P(q_1) \vee P(q_2) \vee \ldots \vee P(q_n)]$
$$\equiv \sim P(q_1) \wedge \sim P(q_2) \wedge \ldots \wedge \sim P(q_n)$$
(by using De Morgan's law)
$$\equiv (x) \sim P(x).$$ ■

Assuming that the negation symbol appearing before the quantifier negates not the quantifier but the entire quantified statement, we may omit some parentheses in (i) and (ii) and rewrite them as

(i) $\sim(x)\,P(x) \equiv (\exists x) \sim P(x)$
(ii) $\sim(\exists x)\,P(x) \equiv (x) \sim P(x)$

If the universal and existential quantifiers are said to be *duals* of each other, then, from (i) and (ii), we can state that the negation of the quantified formula is equivalent to a formula in which the quantifier is replaced by its *dual* and the scope of the quantifier by its *negation*.

Example 1.39 Express the negation of following statements in English.

(a) Some drivers do not obey the speed limit.

Solution: Not every driver obeys the speed limit.

(b) All Swedish movies are serious.

Solution: Some Swedish movies are not serious.

(c) There is someone in the class who does not have good attitude.

Solution: Not everyone in the class has good attitude. ■

Example 1.40 Express the following statements using quantifiers. Then construct the negation of the statement. Express the negation in simple English.

(a) Every bird can fly.
(b) Some birds can talk.

Solution:

(a) Let $P(x)$: x can fly.
Let the universe of discourse be birds.
Then, the above statement can be expressed as, $\forall x\,P(x)$. The negation is, $\exists x \sim P(x)$. This can be expressed as, "There is a bird that cannot fly".

(b) Let $Q(x)$: x can talk.
Let the universe of discourse be birds.
Then, the above statement can be expressed as, $\exists x\,Q(x)$. The negation is, $\forall x \sim Q(x)$. This can be expressed as, "No bird can talk". ■

1.18.2 Theory of Inference for Predicate Calculus

We have already discussed the rules of inference for statement calculus. While deriving the conclusion in predicate calculus, the rules of inference given for the statement calculus along with some additional rules for handling quantifiers can be used. We shall now present some rules of inference for predicate calculus involving quantifiers.

Rule US (Universal Specification): This rule of inference is used to conclude that $P(a)$ is true, where a is a particular member of the universe of discourse, given the premise $\forall x\, P(x)$. For example, this rule can be used when we conclude from the statement "All students are brilliant" that "Ram is brilliant", where Ram is a member of the universe of discourse of all students. This rule of inference is also known as *universal instantiation*.

Rule UG (Universal Generalization): This rule of inference states that $\forall x\, P(x)$ is true when the given premise $P(a)$ is true for all elements a belonging to the universe of discourse. This rule can be used when we want to prove that $\forall x\, P(x)$ is true by taking an arbitrary element a from the universe of discourse and using $P(a)$ is true. The selected element a must be an arbitrary element, and not a specific element of the universe of discourse.

Rule ES (Existential Specification): This rule of inference permits us to conclude that there exists an element a in the universe of discourse for which $P(a)$ is true, if the premise $\exists x\, P(x)$ is true. Here, the selected element a cannot be arbitrary, but it should be an element, for which $P(a)$ is true. This rule of inference is also known as *existential instantiation*.

Rule EG (Existential Generalization): This rule of inference is used to conclude that the premise $\exists x\, P(x)$ is true when a particular element a with $P(a)$ true is given. In other words, if we know one element a in the universe of discourse for which $P(a)$ is true, then we can say that $\exists x\, P(x)$ is true.

We have summarized these rules of inference in Table 1.3.

Table 1.3 Rules of Inference for Predicate Calculus Involving Quantifiers

Tautology	*Name of Rule of Inference*
$\forall x\, P(x) \to P(a)$	Universal Specification (*US*)
$P(a) \to \forall x\, P(x)$, for an arbitrary a	Universal Generalization (*UG*)
$\exists x\, P(x) \to P(a)$, for some element a	Existential Specification (*ES*)
$P(c) \to \exists x\, P(x)$, for some element a	Existential Generalization (*EG*)

The restrictions on *UG* and *ES* if not imposed may lead to invalid conclusion. Let us understand this through an example.

Example 1.41 Let $S(a, b)$: a is divisible by b. Let the universe of discourse be $\{3, 5, 9, 13\}$, so that the statement $(\exists a)\, S(a, 3)$ is true. However, $(\forall a)\, S(a, 3)$ is false.

Now, consider the following derivation.

{1}	(1)	$(\exists a)\, S(a, 3)$	*P*
{1}	(2)	$S(y, 3)$	*ES*, (1)
{1}	(3)	$\forall x\, S(x, 3)$	*UG*, (2)

In the third step the restriction on UG is neglected. Since 'y' is not free in the premise (in first step), so the restriction on ES is satisfied. But 'y' is free in step 2 and resulted from the use of ES, hence it cannot be generalized and so we get an invalid conclusion. ■

Example 1.42 Prove that

$$(\forall x\, (P(x) \to Q(x)) \wedge \forall x\, (Q(x) \to S(x))) \to \forall x\, (P(x) \to S(x))$$

Solution:

{1}	(1) $\forall x$	$(P(x) \to Q(x))$	*P*
{1}	(2)	$P(a) \to Q(a)$	*T*, *US*, (1)
{3}	(3)	$\forall x\, (Q(x) \to S(x))$	*P*
{3}	(4)	$Q(a) \to S(a)$	*T*, *US*, (3)
{1, 3}	(5)	$P(a) \to S(a)$	*T*, (2), (4), hypothetical syllogism.
{1, 3}	(6)	$\forall x\, (P(x) \to S(x))$	*UG*, (5)

■

Example 1.43 Show that the premises "Every one in this college has purchased a computer" and "Hari is a student in this college" imply the conclusion "Hari has purchased a computer".

Solution: Let $P(x)$ denote "x is in this college" and let $Q(x)$ denote "x has purchased a computer". Then the premises can be written as $\forall x(P(x) \to Q(x))$ and P(Hari). The conclusion is Q(Hari).

In the following, we present the steps which are used to establish the conclusion from the given premises.

		Induction Step	Basis of Induction
{1}	(1)	$\forall x\, (P(x) \to Q(x))$	*P*
{1}	(2)	P(Hari) $\to Q$(Hari)	*US*, (1)
{3}	(3)	P(Hari)	*P*
{1, 3}	(4)	Q(Hari)	(2), (3), modus ponens

■

1.18.3 Formulas Involving More Than One Quantifier

Till now, we have written only those formulas in which the universal and existential quantifiers occur singly. Now, we shall consider some cases where

the quantifiers occur multiple times. Many such cases are possible when the quantifier occurs in combination. In the case of 2-place predicate, they become specifically more important. If $A(x, y)$ is a 2-place predicate formula then the following possibilities exist:

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

We can also construct some formulas involving multiple quantifiers. Following are some examples of formulas containing more than one quantifier.

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

Using De Morgan's Law, negation of any of the above formulas can be done. For example,

$$\sim[(x)\,(y)\,A(x, y)]$$
$$\Leftrightarrow (\exists x)\,(\sim(y)\,A(x, y))$$
$$\Leftrightarrow (\exists x)\,(\exists y) \sim A(x, y)$$

The following implication of rules should be carefully:

(1) $(x)\,(\exists y)\,A(x, y)$
Applying *US*, we can write, $(\exists y)\,A(x, y)$ or $(\exists y)\,A(w, y)$.
But we should not write $(\exists y)\,A(y, y)$ since y is a bound variable i.e. $(\exists y)\,A(x, y)$ is not free.

(2) Now consider the statement $(x)\,A(x, y)$
Using *EG*, it can be generalized as

$$(\exists y)\,(x)\,A(x, y) \text{ or } (\exists z)\,(x)\,A(x, z).$$

But we should not generalize it as

$$(\exists x)\,(x)\,A(x, x)$$

Similar care should be taken while using *UG* and *ES* rules.

1.19 METHODS OF PROOF

In this section, we shall discuss some important methods for proving theorems. A theorem is a statement which can be shown to be true. Theorems are also known as *propositions*, *facts* or *results*.

1. *Trivial Proof:* In an implication $p \rightarrow q$, if we can establish that q is true, then regardless of the truth-value of p, the implication $p \rightarrow q$ will be true. So, the

construction of a trivial proof of $p \rightarrow q$ needs to show that the truth-value of q is true.

2. *Vacous Proof:* If the hypothesis p of an implication $p \rightarrow q$ is false, then $p \rightarrow q$ is true for any proposition q.

Example 1.44 Prove the proposition $P(0)$ where $P(n)$ is the proposition "If n is a positive integer greater than 1, then $n^2 > n$".

Solution: The proposition $P(0)$ is the implication "If 0 is a positive integer greater than 1, then $0^2 > 0$". Since 0 is not a positive integer, so the proposition is true. ■

3. *Direct Proof:* Suppose, the hypothesis p is true. Then, the implication $p \rightarrow q$ can be proved if we can prove that q is true by using the rules of inference and some other theorems. This represents that the combination p true and q false never occurs.

Example 1.45 Let $P(n)$ be the proposition "If a and b are positive real numbers, then $(a + b)^n \geq a^n + b^n$." Prove that $P(1)$ is true.

Solution: Suppose the hypothesis of this implication is true, i.e. a and b are positive real numbers. Then, $P(1)$ is true, since $(a + b)^1 = a + b \geq a^1 + b^1 = a + b$. ■

Example 1.46 Prove that the sum of two odd integers is even.

Solution: Let us assume that n and m are two odd integers. So, we can express them as $n = 2k + 1$ and $m = 2l + 1$, where k and l are any integers. So, $n + m = 2(k + l + 1)$, which is even. Thus, the sum of two odd integers is even. ■

Example 1.47 Prove the statement: "If x is a number such that $x^2 + 7x + 12 = 0$, then $x = -4$ or $x = -3$".

Solution: A direct proof of the statement proceeds as follows:
Assume $x^2 + 7x + 12 = 0$. Using the rules of algebra, we have $x^2 + 7x + 12 = (x + 3)\,(x + 4) = 0$. It is known that if the product of two numbers is zero, then one or the other of the two factors must be zero. Hence, $x + 3 = 0$, and $x + 4 = 0$ implies $x = -3$ or $x = -4$. ■

4. *Indirect Proof:* This method is also known as *direct proof of contra positive*. We know that the implication $p \rightarrow q$ is equivalent to its contrapositive $\sim q \rightarrow \sim p$. So, we can prove the implication by showing that its contrapositive $\sim q \rightarrow \sim p$ is true. So, an indirect proof of $p \rightarrow q$ proceeds as follows:

(a) First assume q is false.
(b) Then, prove on the basis of this assumption and other available information from the frame of reference that p is false.

Example 1.48 Prove that if n is an integer and $n^3 + 5$ is odd, then n is even.

Solution: Let us assume that n is odd, so $n = 2k + 1$, for some integer k. Then, $n^3 + 5 = 2(4k^3 + 6k^2 + 3k + 3)$. Since $n^3 + 5$ is two times some integer, so it is even and therefore not odd. Since the negation of the conclusion of the implication implies that the hypothesis is false, the original implication is true. ■

Example 1.49 Prove that if x is irrational then $1/x$ is irrational.

Solution: If $1/x$ were rational, then by definition $1/x = p/q$ for some integers p and q with $q \neq 0$. Since $1/x$ cannot be 0 (if it were, then we would have the contradiction $1 = x$. 0 by multiplying both sides by x), so $p \neq 0$. Now $x = 1/(1/x)$ $= 1/(p/q) = q/p$, by the usual rules of algebra and arithmetic. Hence x can be written as the quotient of two integers with the denominator nonzero. Thus by definition, x is rational. ■

5. *Proof by Contradiction:* There are some other methods which can be used when neither a direct proof nor an indirect proof is successful. Now, we discuss some additional methods of proof.

If a contradiction q can be found so that $\sim p \rightarrow q$ is true, then the proposition $\sim p$ must be false. So, p must be true. This method can be used when a contradiction, such as $r \wedge \sim r$, can be found so that it is possible to show that the implication $\sim p \rightarrow (r \wedge \sim r)$ is true. This type of argument is known as *proof by contradiction.*

The proof by contradiction proceeds as follows:

(a) First assume $p \wedge (\sim q)$ is true.
(b) Then find some conclusion (on the basis of this assumption) that is patently false or violates some other fact already established.
(c) Then the contradiction found out in step (b) leads us to conclude that $p \wedge (\sim q)$ is false. Hence, $p \rightarrow q$ is true.

Very often, one obtains the proposition $p \wedge (\sim p)$ in a proof by contradiction. So, in this case, one should give a proof by contra positive.

Example 1.50 Prove that the sum of an irrational number and a rational number is irrational.

Solution: Suppose that r is a rational number and i is an irrational number and $s = r + i$ is rational. We know that the sum of two rational numbers is rational. So, $s + (-r) = i$ is rational, which is a contradiction. Hence the proof. ■

Example 1.51 Show that at least 10 of any 64 days chosen must fall on the same day of the week.

Solution: If there were 9 or fewer days on each day of the week, this would account for at most $9.7 = 63$ days. But we choose 64 days. This contradiction shows that at least 10 of the days must be on the same day of the week. ■

6. *Proof by Cases:* We can use the tautology $[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \wedge q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$ as a rule of inference to proof an implication of the form $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$.

This implies that the original implication with a hypothesis made up of the disjunction of the propositions $p_1, p_2, \ldots, p_n$, can be proved by proving each of the n implications $p_i \rightarrow q$, $i = 1, 2, \ldots n$, separately. Such an argument is called a *proof by cases*. It may be noted that the method of proof by cases is valid when $n = 2$. For example, the statements $(p_1 \vee p_2) \rightarrow q$ and $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q)$ may be considered which are equivalent.

Example 1.52 Prove that if x and y are real numbers, then $\max(x, y) + \min(x, y) = x + y$.

Solution: There are two possible cases, i.e. $x \leq y$ and $x \geq y$. If $x \leq y$, then $\max(x, y) + \min(x, y) = y + x = x + y$. If $x \geq y$, then $\max(x, y) + \min(x, y) = x + y$. Since these are the only two cases, the equality always holds. Hence the proof. ■

Example 1.53 Prove the triangle inequality, which states that if x and y are real numbers then $|x| + |y| \geq |x + y|$ (where $|x|$ represents the absolute value of x, which equals x if $x \geq 0$ and equals $-x$ if $x < 0$).

Solution: There are four cases:

Case 1: $x \geq 0$ and $y \geq 0$. Then $|x| + |y| = x + y = |x + y|$.

Case 2: $x < 0$ and $y < 0$. Then $|x| + |y| = -x + (-y) = -(x + y) = |x + y|$ since $x + y < 0$.

Case 3: $x \geq 0$ and $y < 0$. Then $|x| + |y| = x + (-y)$. If $x \geq -y$ then $|x + y| = x + y$. But since $y < 0$, $-y > y$ so that $|x| + |y| = x + (-y) > x + y = |x + y|$. If $x < -y$ then $|x + y| = -(x + y) = -x + (-y)$. But, since $x \geq 0$, $x \geq -x$, so that $|x| + |y| = x + (-y) \geq -x + (-y) = |x + y|$.

Case 4: $x < 0$ and $y \geq 0$. This is identical to case 3 with the roles of x and y reversed. ■

Hence the proof.

7. *Proof by Elimination of Cases:* Very often, while solving a problem or in constructing a proof, we are confronted with two alternatives: either p has to be true or q has to be true. If we verify that p is false, then obviously we must conclude that q is true.

This method of proof is identical to the rule of inference *disjunctive syllogism*, i.e. $[(p \vee q) \wedge (\sim p)] \rightarrow q$, and, it can be extended to any finite number of cases:

$$[\{(p_1 \vee p_2 \vee p_3 \vee \ldots \vee p_n) \vee q\} \wedge (\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3) \wedge \ldots (\sim p_n)] \rightarrow q$$

Similarly, a proof by elimination of cases can take another form based on the following tautology:

$$\{[p \rightarrow (q \vee r)] \wedge (\sim q)\} \rightarrow (p \rightarrow r)$$

In other words, if we are given that p implies two possible conclusions q or r, and if one of the conclusions q is definitely false, then, we may conclude that p implies the other conclusion r.

Finally, there is a third form of a proof by elimination of cases. In this situation, a statement of the form $p \rightarrow (q \vee r)$ is proved by proving instead the equivalent statement $(p \wedge \sim q) \rightarrow r$.

Suppose, for example, that we wish to prove the following statement for a real number X: if $x^2 + 7x + 12 = 0$ and $x \neq 3$ and then demonstrating $x = 4$.

We might observe that this method of proof of $p \rightarrow (q \vee r)$ by elimination of cases is quite similar in form to proof by contradiction; however, a proof by contradiction of $p \rightarrow (q \vee r)$ would go one step further and assume $p \wedge (\sim q) \wedge (\sim r)$ (since $\sim(q \vee r) = (\sim q) \vee (\sim r)$ by De Morgan's law), and then attempt to find a contradiction.

8. *Conditional Proof:* This method of proof is actually just another form of elimination of cases.

We know that the two propositions $p \rightarrow (q \rightarrow r)$ and $(p \wedge q) \rightarrow r$ are equivalent. So, a proof of the conditional $p \rightarrow (q \rightarrow r)$ can proceed as follows:

(a) First, join the two antecedents p and q.
(b) Then prove r on the basis of these assumptions and other available information.

9. *Proof of Equivalence:* We can use the tautology

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$$

to prove a theorem which is a biconditional, i.e. a statement of the form $p \leftrightarrow q$, where p and q are propositions.

In other words, the proposition "p iff q" can be proved if both the implications "if p, then q" and "if q, then p" are proved.

To do this, we break the proof into two halves: first we prove $p \rightarrow q$, and then we prove $q \rightarrow p$. However, one may prove $q \rightarrow p$ first.

Example 1.54 Prove that if n is a positive integer, then n is odd if and only if $5n + 6$ is odd.

Solution: This theorem has the form "p iff q" where p is "n is odd" and q is "$5n + 6$ is odd". To prove this theorem we need to show that $p \rightarrow q$ and $q \rightarrow p$ are true.

First, assume that n is odd, so that $n = 2k + 1$ for some integer k. Then, $5n + 6 = 5(2k + 1) + 6 = 10k + 11 = 2(5k + 5) + 1$. Hence $5n + 6$ is odd. To prove the converse, suppose that n is even, so that $n = 2k$ for some integer k. Then $5n + 6 = 10k + 6 = 2(5k + 3)$, so that $5n + 6$ is even. Hence n is odd, if and only if $5n + 6$ is odd. ■

1.20 EUCLIDEAN ALGORITHM

Possibly, the oldest recorded nontrivial algorithm is the *Euclidean algorithm*. Euclid devised an algorithm for computing the Greatest Common Divisor (GCD) of two non-negative integers. If the two integers M and N are non-negative, i.e. $M \geq 0$ and $N \geq 0$, then the Greatest Common Divisor is the largest integer P(say) ≥ 0 such that M and N both are divisible by P.

The Euclidean algorithm to compute the Greatest Common Divisor (GCD) of two integers M and N is a recursive definition and is as follows:

$$GCD\ (M, N) = \begin{cases} GCD(N, M) & \text{If } N > M \\ M, & \text{If } N = 0 \\ GCD(N, R), & \text{otherwise} \end{cases}$$

where, R is the remainder when M is divided by N, or $M = aN + R$, a is some constant.

Example 1.55 By applying the Euclidean algorithm, compute $GCD(25, 6)$.

Solution:

$= GCD(25, 6)$ here $M = 25, N = 6$
$= GCD(6, 1),$ since $6 < 25, N < M$
$= GCD(1, 0),$ since $1 < 6, N < M$
$= 1,$ since $N = 0$

So, $GCD(25, 6) = 1$. ■

Example 1.56 By applying the Euclidean algorithm, compute

(a) $GCD(18, 4)$
(b) $GCD(26, 2)$
(c) $GCD(28, 8)$

Solution:

(a) $GCD(18, 4) = GCD(4, 2) = GCD(2, 0) = 2$
(b) $GCD(26, 2) = GCD(2, 0) = 2$
(c) $GCD(28, 8) = GCD(8, 4) = GCD(4, 0) = 4$ ■

Figure 1.15 shows the code for computing GCD of two numbers using Euclidean algorithm.

1.20.1 Euclidean Prime

Let n be a prime number. Let $P(n)$ be 1 added to the product of all prime numbers up to and including P, i.e $P(n) = \{2*3*5* \ldots *n\} + 1$. We call n, a *Euclidean prime*, if $P(n)$ is a prime number. For example, it may be verified that 13 is not a Euclidean prime.

less than or equal to 21, 33, 43.

```
/* Program to compute Greatest Common Divisor* /

# include<stdio.h>
# include<conio.h>

int GCD(int , int);

/* Definition of the Greatest Common Divisor Function */

int GCD( int n, int m)
{
        if(( n >= m) && (( n % m) == 0))
                return(m);
        else
                GCD(m,(n % m));
}


void main()
{
        int n, m;
        int result;
        printf("\n Input the first integer number: ");
        scanf("%d", &n);

        printf("\n Input the second integer number: ");
        scanf("%d", &m);

        result = GCD(n, m);
        printf("\n Greatest Common Divisor of : %d and %d is = %d", n, m, result);
      getch();
}
```

Fig. 1.15 The code for computing GCD of two numbers using Euclidean algorithm

Problems

1.1 Determine whether each of the following statements is true or false. Briefly explain your answer.

(a) $\phi \subseteq \phi$
(b) $\phi \in \phi$
(c) $\phi \subseteq \{\phi\}$
(d) $\phi \in \{\phi\}$
(e) $\{\phi\} \subseteq \phi$
(f) $\{\phi\} \in \phi$
(g) $\{\phi\} \subseteq \{\phi\}$
(h) $\{\phi\} \in \{\phi\}$
(i) $\{a, b\} \subseteq \{a, b, c, \{a, b, c\}\}$
(j) $\{a, b\} \in \{a, b, c, \{a, b, c\}\}$
(k) $\{a, b\} \subseteq \{a, b, \{\{a, b\}\}\}$
(l) $\{a, b\} \in \{a, b, \{\{a, b\}\}\}$
(m) $\{a, \phi\} \subseteq \{a, \{a, \phi\}\}$
(n) $\{a, \phi\} \in \{a, \{a, \phi\}\}$

1.2 Determine the following sets:

(a) $\phi \cup \{\phi\}$
(b) $\phi \cap \{\phi\}$
(c) $\{\phi\} \cup \{a, \phi, \{\phi\}\}$
(d) $\{\phi\} \cap \{a, \phi, \{\phi\}\}$
(e) $\phi \oplus \{a, \phi, \{\phi\}\}$
(f) $\{\phi\} \oplus \{a, \phi, \{\phi\}\}$

1.3 (a) Let A and B be sets such that $(A \cup B) \subseteq B$ and $B \not\subseteq A$. Draw the corresponding Venn diagram.

(b) Let A, B, and C be sets such that $A \subseteq B$, $A \subseteq C$, $(B \cap C) \subseteq A$, and $A \subseteq (B \cap C)$. Draw the corresponding Venn diagram.

(c) Let A, B, and C be sets such that $(A \cap B \cap C) = \phi$, $(A \cap B) \neq \phi$, $(A \cap C) \neq \phi$, and $(B \cap C) \neq \phi$. Draw the corresponding Venn diagram.

1.4 Give an example of sets A, B, and C such that $A \in B$, $B \in C$, and $A \notin C$.

1.5 Determine whether each of the following statements is true for arbitrary sets A, B, C. Justify your answer.

(a) If $A \in B$ and $B \subseteq C$, then $A \in C$.
(b) If $A \in B$ and $B \subseteq C$, then $A \subseteq C$.
(c) If $A \subseteq B$ and $B \in C$, then $A \in C$.
(d) If $A \subseteq B$ and $B \in C$, then $A \subseteq C$.

1.6 Let A, B, C be subsets of U. Given that

$$A \cap B = A \cap C$$
$$\bar{A} \cap B = \bar{A} \cap C$$

Is it necessary that $B = C$? Justify your answer.

1.7 Given that

$$(A \cap C) \subseteq (B \cap C)$$
$$(A \cap \bar{C}) \subseteq (B \cap \bar{C})$$

show that $A \subseteq B$.

1.8 What can you say about the sets P and Q if

(a) $P \cap Q = P$?
(b) $P \cup Q = P$?
(c) $P \oplus Q = P$?
(d) $P \cap Q = P \cup Q$?

1.9 (a) Let $A \subseteq B$ and $C \subseteq D$. Is it always the case that $(A \cup C) \subseteq (B \cup D)$? Is it always the case that $(A \cap C) \subseteq (B \cap D)$?

(b) Let $W \subset X$ and $Y \subset Z$. Is it always the case that $(W \cup Y) \subset (X \cup Z)$? Is it always the case that $(W \cap Y) \subset (X \cap Z)$?

1.10 (a) Given that $A \cup B = A \cup C$, is it necessary that $B = C$?
(b) Given that $A \cap B = A \cap C$, is it necessary that $B = C$?
(c) Given that $A \oplus B = A \oplus C$, is it necessary that $B = C$?
Justify your answers.

1.11 For $A = \{a, b, \{a, c\}, \phi\}$, determine the following sets:

(a) $A - \{a\}$
(b) $A - \phi$
(c) $A - \{\phi\}$
(d) $A - \{a, b\}$
(e) $A - \{a, c\}$
(f) $A - \{\{a, b\}\}$
(g) $A - \{\{a, c\}\}$
(h) $\{a\} - A$
(i) $\phi - A$
(j) $\{\phi\} - A$
(k) $\{a, c\} - A$
(l) $\{\{a, c\}\} - A$
(m) $\{a\} - \{A\}$

1.12 Let A, B, C be arbitrary sets.

(a) Show that $(A - B) - C = A - (B \cup C)$
(b) Show that $(A - B) - C = (A - C) - B$
(c) Show that $(A - B) - C = (A - C) - (B - C)$

1.13 Let A, B, C be sets. Under what condition is each of the following statements true?

(a) $(A - B) \cup (A - C) = A$
(b) $(A - B) \cup (A - C) = \phi$
(c) $(A - B) \cap (A - C) = \phi$
(d) $(A - B) \oplus (A - C) = \phi$

1.14 Let A, B be two sets.

(a) Given that $A - B = B$, what can be said about A and B?
(b) Given that $A - B = B - A$, what can be said about A and B?

1.15 Let A denote the set of all automobiles that are manufactured domestically. Let B denote the set of all imported automobiles. Let C denote the set of all automobiles manufactured before 1977. Let D denote the set of all automobiles with a current market value of less than \$2000. Let E denote the set of all automobiles owned by students at the university. Express the following statements in set-theoretic notation:

(a) The automobiles owned by students at the university are either domestically manufactured or imported.

(b) All domestic automobiles manufactured before 1977 have a market value of less than \$2000.

(c) All imported automobiles manufactured after 1977 have a market value of more than \$2000.

1.16 Let A denote the set of all freshmen. B denote the set of all sophomores, C denote the set of all mathematics majors, D denote the set of all computer science majors, E denote the set of all students in the course Elements of Discrete Mathematics, F denote the set of all students who went to a rock concert on Monday night, G denote the set of all students who stayed up late Monday night. Express the following statements in set-theoretic notation:

(a) All sophomores in computer science are in the course Elements of Discrete Mathematics.

(b) Those and only those who are in the course Elements of Discrete Mathematics or who went to the rock concert stayed up late Monday night.

(c) No student in the course Elements of Discrete Mathematics went to the rock concert Monday night. (The obvious reason is the long problem sets in the course Elements of Discrete Mathematics.)

(d) The rock concert was only for freshmen and sophomores.

(e) All sophomores who are neither mathematics nor computer science majors went to the rock concert.

1.17 Determine the power sets of the following sets.

(a) $\{a\}$ (b) $\{\{a\}\}$

(c) $\{\phi, \{\phi\}\}$

1.18 Let $A = \{\phi, b\}$. Construct the following sets:

(a) $A - \phi$ (b) $\{\phi\} - A$

(c) $A \cup \mathcal{P}(A)$ (d) $A \cap \mathcal{P}(A)$

1.19 Let $A = \{\phi\}$. Let $B = \mathcal{P}(\mathcal{P}(A))$.

(a) Is $\phi \in B$? $\phi \subseteq B$?

(b) Is $\{\phi\} \in B$? $\{\phi\} \subseteq B$?

(c) Is $\{\{\phi\}\} \in B$? $\{\{\phi\}\} \subseteq B$?

1.20 Let $A = \{\phi, \{\phi\}\}$. Determine whether each of the following statements is true or false.

(a) $\phi \in \mathcal{P}(A)$ (b) $\phi \subseteq \mathcal{P}(A)$

(c) $\{\phi\} \subseteq \mathcal{P}(A)$ (d) $\{\phi\} \subseteq A$

(e) $\{\phi\} \in \mathcal{P}(A)$ (f) $\{\phi\} \in A$

(g) $\{\{\phi\}\} \subseteq \mathcal{P}(A)$ (h) $\{\{\phi\}\} \subseteq A$

(i) $\{\{\phi\}\} \in \mathcal{P}(A)$ (j) $\{\{\phi\}\} \in A$

1.21 Let $A = \{a, \{a\}\}$. Determine whether each of the following statements is true or false.

(a) $\phi \in \mathcal{P}(A)$ (b) $\phi \subseteq \mathcal{P}(A)$

(c) $\{a\} \in \mathcal{P}(A)$ (d) $\{a\} \subseteq \mathcal{P}(A)$

(e) $\{\{a\}\} \in \mathcal{P}(A)$ (f) $\{\{a\}\} \subseteq \mathcal{P}(A)$

(g) $\{a, \{a\}\} \in \mathcal{P}(A)$ (h) $(a, \{a\}) \subseteq \mathcal{P}(A)$

(i) $\{\{\{a\}\}\} \in \mathcal{P}(A)$ (j) $\{\{\{a\}\}\} \subseteq \mathcal{P}(A)$

1.22 Determine whether each of the following statements is true or false. Briefly explain your answer.

(a) $A \cup \mathcal{P}(A) = \mathcal{P}(A)$ (b) $A \cap \mathcal{P}(A) = A$

(c) $\{A\} \cup \mathcal{P}(A) = \mathcal{P}(A)$ (d) $\{A\} \cap \mathcal{P}(A) = A$

(e) $A - \mathcal{P}(A) = A$ (f) $\mathcal{P}(A) - \{A\} = \mathcal{P}(A)$

1.23 Let A and B be two arbitrary sets.

(a) Show that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$ or give a counter example.

(b) Show that $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$ or give a counter example.

1.24 Determine the cardinalities of the sets:

(a) $A = \{n^7 | n \text{ is a positive integer}\}$ (b) $B = \{n^{109} | n \text{ is a positive integer}\}$

(c) $A \cup B$ (d) $A \cap B$

Justify your answers.

1.25 Show that at most a countably infinite number of books can ever be written in English. (We define a book to be a finite sequence of words, divided into sentences, paragraphs, and chapters.)

1.26 (a) Show that the set of all positive rational numbers is a countably infinite set. (*Hint*: Consider all the points in the first quadrant of the plane whose x coordinate and y coordinate are integral values.)

(b) Show that the union of a countably infinite number of countably infinite sets is a countably infinite set.

1.27 Let N denote the set of all natural numbers. Let S denote the set of all *finite* subsets of N. What is the cardinality of the set S? Justify your answer.

1.28 (a) Give an example to show that the cardinality of a set that is the intersection of two countably infinite sets may also be countably infinite.

(b) Give an example to show that the cardinality of a set that is the intersection of two countably infinite sets may be finite.

1.29 Mr. Kantor built a machine that tells "lucky" numbers from "unlucky" numbers. That is, given a natural number, the machine will respond with the answer "lucky" or "unlucky." Two such machines are considered different if there is at least one number which one machine considers lucky but the other considers unlucky. Prove that there are more than a countably infinite number of such machines.

1.30 Solve the postage stamp problem in Example 1.1 by showing how postages of $3k$, $3k + 1$, $3k + 2$ cents can be made up with 3-cent and 5-cent stamps.

1.31 Mr. J. E. Roberts claims that he is a one-third Indian. When asked how this is possible, his answer was, "My father was a one-third Indian and my mother was a one-third Indian." Is this a correct proof by induction?

1.32 We present a proof of the statement "Any n billiard balls are of the same color" by induction.

Basis of induction. For $n = 1$, the statement is trivially true.

Induction step. Suppose we are given $k + 1$ billiard balls which we number $1, 2, \ldots, (k + 1)$. According to the induction hypothesis, balls $1, 2, \ldots, k$ are of the same color. Also, balls $2, 3, \ldots, (k + 1)$ are of the same color. Consequently, balls $1, 2, \ldots, k, (k + 1)$ are all of the same color.

What is wrong with the proof?

1.33 Prove by induction that for $n \geq 0$ and $a \neq 1$

$$1 + a + a^2 + \ldots + a^n = \frac{1 - a^{n+1}}{1 - a}$$

1.34 Show that $n^3 + 2n$ is divisible by 3 for all $n \geq 1$ by induction.

1.35 Show that $n^4 - 4n^2$ is divisible by 3 for all $n \geq 2$ by induction.

1.36 Show that $2^n \times 2^n - 1$ is divisible by 3 for all $n \geq 1$ by induction.

1.37 Show that

$$1 + 2 + 2^2 + 2^3 + \ldots + 2^n = 2^{n+1} - 1$$

by induction.

1.38 Determine the sum

$$1 + 3 + 5 + \ldots + (2n - 1)$$

by (a) guessing a general formula on the basis of the values of the sum for $n = 1, 2, 3, 4, 5$; (b) proving that the general formula is valid by induction.

1.39 Prove by induction that for $n \geq 1$

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \ldots + n \cdot n! = (n + 1)! - 1$$

where $n!$ stands for the product $1 \cdot 2 \cdot 3 \ldots n$.

1.40 Prove by induction that for $n \geq 1$

$$1 \cdot 2 + 2 \cdot 3 + \ldots + n(n + 1) = \frac{n(n + 1)(n + 2)}{3}$$

1.41 Show that

$$1^2 - 2^2 + 3^2 - 4^2 + \ldots (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n + 1)}{2}$$

(a) By induction.

(b) By using the result in Example 1.5.

1.42 Show that

$$1^2 + 3^2 + 5^2 + \ldots + (2n - 1)^2 = \frac{n(2n - 1)(2n + 1)}{3}$$

1.43 Show that

$$1^3 + 2^3 + \ldots + n^3 = (1 + 2 + 3 + \ldots + n)^2$$

1.44 Show that

$$\frac{1^2}{1 \cdot 3} + \frac{2^2}{3 \cdot 5} + \ldots + \frac{n^2}{(2n - 1)(2n + 1)} = \frac{n(n + 1)}{2(2n + 1)}$$

1.45 (a) Show that

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \ldots + \frac{1}{n(n + 1)} = \frac{n}{n + 1}$$

(b) Show that

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \ldots + \frac{n^2}{(2n - 1)(2n + 1)} = \frac{n}{2n + 1}$$

(c) Show that

$$\frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \frac{1}{7 \cdot 10} + \ldots + \frac{1}{(3n - 2)(3n + 1)} = \frac{n}{3n + 1}$$

(d) Determine and prove a general formula that includes the results in (a), (b), and (c) as special cases.

1.46 Show that

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + 3 \cdot 4 \cdot 5 + \ldots + n(n + 1)(n + 2) = \frac{n(n + 1)(n + 2)(n + 3)}{4}$$

1.47 Formulate and prove by induction a general formula stemming from the observations that

$$1^3 = 1$$
$$2^3 = 3 + 5$$
$$3^3 = 7 + 9 + 11$$
$$4^3 = 13 + 15 + 17 + 19$$

1.48 Prove by induction that the sum of the cubes of three consecutive integers is divisible by 9.

1.49 Show that for any integer n

$$(11)^{n+2} + (12)^{2n+1}$$

is divisible by 133.

1.50 It is known that for any positive integer $n \geq 2$

$$\frac{1}{n + 1} + \frac{1}{n + 2} + \ldots + \frac{1}{2n} - A > 0$$

where A is a constant. How large can A be?

1.51 Show that for any positive integer $n > 1$

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{n}} > \sqrt{n}$$

1.52 When n couples arrived at a party, they were greeted by the host and hostess at the door. After rounds of handshaking, the host asked the guests as well as his wife (the hostess) to indicate the number of hands each of them had shaken. He got $2n + 1$ different answers. Given that no one shook hands with his or her spouse, how many hands had the hostess shaken? Prove your result by induction.

1.53 (a) Let S be a set of natural numbers such that: (1) The natural number n_0 is in S. (2) If the natural numbers $n_0, n_0 + 1, n_0 + 2, \ldots, k$ are in S, then the natural number $k + 1$ is also in S.

Show that S is the set of all natural numbers larger than or equal to n_0.

Hint: Assume that n_1 is the smallest natural number not in S.

(b) Use the result in part (a) to show that the principle of strong mathematical induction is indeed valid.

1.54 Among the integers 1–300, how many of them are not divisible by 3, nor by 5, nor by 7? How many of them are divisible by 3, but not by 5 nor by 7?

1.55 N toys are to be distributed randomly among N children. There is an interesting way for the children to choose the toys so that no two of them will choose the same toy. A graph such as that shown in Fig. 1P.1(*a*) is drawn where there are N vertical lines and an arbitrary number of random horizontal segments between adjacent vertical lines with the stipulation that no two horizontal segments meet at the same point. The N toys are

assigned to the bottoms of the vertical lines, and each child chooses as a starting point the top of a vertical line. From this starting point, the child will trace a path downward. However, whenever the child runs into a horizontal segment, he or she must turn horizontally, and then turn downward again when the adjacent vertical line is reached. For example, Fig. 1P.1(*b*) shows the path that John follows. It is claimed that no matter how many horizontal segments are drawn, in whatever possible way, no two children will reach the same toy. Prove this claim by induction on the number of horizontal segments drawn.

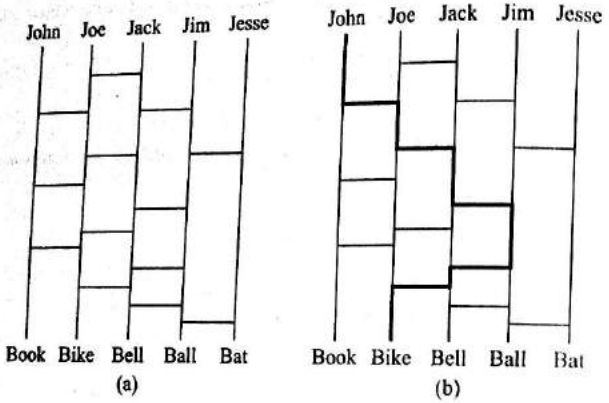


Fig. 1P.1

1.56 A survey was conducted among 1000 people. Of these 595 are Democrats, 595 wear glasses, and 550 like ice cream; 395 of them are Democrats who wear glasses, 350 of them are Democrats who like ice cream, and 400 of them wear glasses and like ice cream; 250 of them are Democrats who wear glasses and like ice cream. How many of them who are not Democrats, do not wear glasses, and do not like ice cream? How many of them are Democrats who do not wear glasses, and do not like ice cream?

1.57 It is known that at the university 60 percent of the professors play tennis, 50 percent of them play bridge, 70 percent jog, 20 percent play tennis and bridge, 30 percent play tennis and jog, and 40 percent play bridge and jog. If someone claimed that 20 percent of the professors jog and play bridge and tennis, would you believe this claim? Why?

1.58 The 60,000 fans who attended the homecoming football game bought up all the paraphernalia for their cars. Altogether, 20,000 bumper stickers, 36,000 window decals, and 12,000 key rings were sold. We know that 52,000 fans bought at least one item and no one bought more than one of a given item. Also, 6000 fans bought both decals and key rings, 9000 bought both decals and bumper stickers, and 5000 bought both key rings and bumper stickers.

(a) How many fans bought all three items?
(b) How many fans bought exactly one item?
(c) Someone questioned the accuracy of the total number of purchasers; 52,000 (given that all the other numbers have been confirmed to be correct). This person claimed the total number of purchasers to be either 60,000 or 44,000. How do you dispel the claim?

1.59 Out of a total of 130 students, 60 are wearing hats to class, 51 are wearing scarves, and 30 are wearing both hats and scarves. Of the 54 students who are wearing sweaters, 26 are wearing hats, 21 are wearing scarves, and 12 are wearing both hats and scarves. Everyone wearing neither a hat nor a scarf is wearing gloves.

(a) How many students are wearing gloves?
(b) How many students not wearing a sweater are wearing hats but not scarves?
(c) How many students not wearing a sweater are wearing neither a hat nor a scarf?

1.60 Among 100 students, 32 study mathematics, 20 study physics, 45 study biology, 15 study mathematics and biology, 7 study mathematics and physics, 10 study physics and biology, and 30 do not study any of the three subjects.

(a) Find the number of students studying all three subjects.
(b) Find the number of students studying exactly one of the three subjects.

1.61 At a DAR (Daughters of the American Revolution) meeting of 30 women, 17 are descended from George Washington, 16 are descended from John Adams, and 5 are not descended from Washington or Adams. How many of the 30 women are descended from both Washington and Adams?

1.62 Seventy-five children went to an amusement park where they can ride on the merry-go-round, roller coaster, and ferris wheel. It is known that 20 of them have taken all three rides, and 55 of them have taken at least two of the three rides. Each ride costs \$0.50, and the total receipt of the amusement park was \$70. Determine the number of children who did not try any of the rides.

1.63 (a) Among 50 students in a class, 26 got an A in the first examination and 21 got an A in the second examination. If 17 students did not get an A in either examination, how many students got an A in both examinations?

(b) If the number of students who got an A in the first examination is equal to that in the second examination, if the total number of students who got an A in exactly one examination is 40, and if 4 students did not get an A in either examination, determine the number of students who got an A in the first examination only, who got an A in the second examination only, and who got an A in both examinations.

1.64 A possible way to define the symmetric difference of two multisets P and Q, denoted $P \oplus Q$, is to let the multiplicity of an element in $P \oplus Q$ be equal to the absolute value of the difference between the multiplicities of the element in P and Q. What is a possible inconsistency with such a definition?
Hint: Consider the multisets $(P \oplus Q) \oplus R$ and $P \oplus (Q \oplus R)$.

1.65 To describe the various restaurants in the city, we let p denote the statement, "The food is good," q denote the statement, "The service is good," and r denote the statement, "The rating is three-star." Write the following statements in symbolic form.

(a) Either the food is good, or the service is good, or both.
(b) Either the food is good or the service is good, but not both.
(c) The food is good while the service is poor.
(d) It is not the case that both the food is good and the rating is three-star.
(e) If both the food and services are good, then the rating will be three-star.
(f) It is not true that a three-star rating always means good food and good service.

1.66 Let p denote the statement, "The material is interesting," and q denote the statement, "The exercises are challenging," and r denote the statement, "The course is enjoyable." Write the following statements in symbolic form:

(a) The material is interesting and the exercises are challenging.

(b) The material is uninteresting, the exercises are not challenging, and the course is not enjoyable.
(c) If the material is not interesting and the exercises are not challenging, then the course is not enjoyable.
(d) The material is interesting means the exercises are challenging, and conversely.
(e) Either the material is interesting or the exercises are not challenging, but not both.

1.67 Write the following statements in symbolic form:

(a) The sun is bright and the humidity is not high.
(b) If I finish my homework before dinner and it does not rain, then I will go to the ball game.
(c) If you do not see me tomorrow, it means I have gone to Chicago.
(d) If the utility cost goes up or the request for additional funding is denied, then a new computer will be purchased if and only if we can show that the current computing facilities are indeed not adequate.

1.68 Let p denote the statement, "The weather is nice" and q denote the statement, "We have a picnic." Translate the following in English and simplify if possible:

(a) $p \wedge \bar{q}$ (b) $p \leftrightarrow q$
(c) $\bar{q} \leftrightarrow \bar{p}$ (d) $\overline{(\bar{p} \vee q)} \vee \overline{(p \wedge \bar{q})}$

1.69 (a) Write a compound statement that is true when exactly two of the three statements p, q, r are true.
(b) Write a compound statement that is true when none, or one, or two of the three statements p, q, r are true.

1.70 Construct the truth tables for the folllowing statements:

(a) $p \to p$ (b) $(p \to p) \vee (p \to \bar{p})$
(c) $(p \to p) \to (p \to \bar{p})$ (d) $(p \vee \bar{q}) \vee \bar{p}$
(e) $(p \vee \bar{q}) \to \bar{p}$ (f) $p \leftrightarrow (\bar{p} \vee \bar{q})$
(g) $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$
(h) $(\bar{q} \to \bar{p}) \to (p \to q)$

1.71 (a) Given that the value of $p \to q$ is false, determine the value of $(\bar{p} \vee \bar{q}) \to q$.
(b) Given that the value of $p \to q$ is true, can you determine the value of $\bar{p} \vee (p \leftrightarrow q)$?

1.72 Consider the following advertisement for a game:

(a) There are three statements in this advertisement.
(b) Two of them are not true.
(c) The average increase in IQ scores of people who learn this game is more than 20 points. Is statement (c) true?

1.73 A certain country is inhabited only by people who either always tell the truth or always tell lies, and who will respond to questions only with a "yes" or a "no." A tourist comes to a fork in the road, where one branch leads to the capital and the other does not. There is no sign indicating which branch to take, but there is an inhabitant, Mr. Z, standing at the fork. What single question should the tourist ask him to determine which branch to take?
Hint: Let p stand for "Mr. Z always tells the truth" and let q stand for "The left-hand branch leads to the capital." Formulate a proposition A involving p and q such that Mr. Z's answer to the question "Is A true?" will be "yes" when and only when q is true.

1.74 Tony, Mike, and John belong to the Alpine Club. Every club member is either a skier or a mountain climber or both. No mountain climber likes rain, and all skiers like snow. Mike dislikes whatever Tony likes and likes whatever Tony dislikes. Tony likes rain and snow. Is there a member of the Alpine Club who is a mountain climber but not a skier?

1.75 What is the truth value of the quantification $\forall x\, Q(x)$, if the statement $Q(x)$ and universe of discourse given as follows:

(a) $Q(x)$: $x + 1 > x$, U = {all real numbers}
(b) $Q(x)$: $x < 5$, U = {all real numbers}
(c) $Q(x)$: $x^2 < 12$, U = {positive integer not exceeding 3}

1.76 What is the truth value of the quantification $(\exists x)\, Q(x)$, if the statement $Q(x)$ and universe of discourse is given as follows:

(a) $Q(x)$: $x > 32$, U = {all real number}
(b) $Q(x)$: $x = x + 2$ U = {all real number}
(c) $Q(x)$: $x^2 < 12$, U = {positive integer not exceeding 3}

1.77 Translate these statements into English
(x): x is a cat
$A(x)$: x is an animal

(a) $\forall x((x) \to A(x))$ (b) $\forall x((x) \wedge A(x))$
(c) $\exists x((x) \to A(x))$ (d) $(\forall x)((x) \wedge \sim A(x))$

1.78 Translate each of these statements into logical expression using predicates, quantifiers and logical connections.

(a) Someone in your class can speak Oriya.
(b) Everyone in your class is honest.
(c) There is a person in the class who was not born in India.
(d) A student in your class has been in NCC.

1.79 Express the negation of these propositions using quantifier and then express the negation in English.

(a) Some people do not follow the rules.
(b) Some people are very serious.
(c) No one can keep a secret.
(d) There is someone in this class who is very intelligent.

1.80 Establish these logical equivalences, where P is a proposition not involving any quantifier.

(a) $(\forall x\, Q(x)) \vee P \equiv \forall x(Q(x) \vee P)$ (b) $(\exists x\, Q(x)) \vee P \equiv \exists x(Q(x) \vee P)$
(c) $(\forall x\, Q(x)) \wedge P \equiv \forall x(Q(x) \wedge P)$ (d) $(\exists x\, Q(x)) \wedge P \equiv \exists x(Q(x) \wedge P)$

1.81 Translate these statements into English.
Let $P(x, y)$ = 'x has sent a letter to y', where universe of discourse for both x and y consist of all students in your class.

(a) $\exists x\, \exists y\, Q(x, y)$ (b) $\exists x\, \forall y\, Q(x, y)$
(c) $\forall x\, \exists y\, Q(x, y)$ (d) $\exists y\, \exists x\, Q(x, y)$
(e) $\exists y\, \forall x\, Q(x, y)$ (f) $\forall x\, \exists y\, Q(x, y)$

1.82 Use quantifier and predicate with more than one variable to express these statements:

(a) Many students in this class can speak Hindi.
(b) There is a student in this class who plays golf.
(c) Some students in this class belong to the same town.
(d) All students in this class have visited Agra.
(e) Every student in this class has chatted with at least one other student, in at least one chat group.

1.83 Translate the following into a logical expression.
(a) Every positive integer has exactly two square roots.
(b) A negative real number does not have a square root that is a real number.
(c) The difference of a real number and itself is zero.
(d) The product of two negative real number is positive.

1.84 Which of the following are statements:
(a) $(x)(A(x) \vee B(x)) \wedge C$ (b) $(x)(A(x) \wedge B(x)) \wedge (\exists x) D(x)$
(c) $(y)(P(y) \wedge Q(y)) \wedge R(y)$

1.85 Indicate free and bound variables with scope of quantifier.
(a) $(x)(A(x) \wedge B(x)) \rightarrow (x) A(x) \wedge B(x)$
(b) $(x)(A(x) \wedge (\exists x) B(x)) \vee ((x) A(x) \rightarrow B(x))$
(c) $(x)(A(x) \leftrightarrow B(x) \wedge (\exists x) R(x)) \wedge D(x)$

1.86 If the universe of discourse is set {1, 2, 3} eliminate the quantifier in the following formulas.
(a) $(x) Q(x)$ (b) $(\exists x) M(x)$
(c) $(x) A(x) \wedge (x) B(x)$ (d) $(x) A(x) \wedge \exists x M(x)$
(e) $(x) \sim A(x) \vee (x) A(x)$

1.87 Demonstrate the following implication.
(i) $(\exists x)(A(x) \wedge B(x)) \rightarrow (\exists x) A(x) \wedge (\exists x) B(x)$
(ii) $(x)(A(x) \vee B(x)) \rightarrow (x) A(x) \vee (\exists x) B(x)$
(iii) $(x)(A(x) \rightarrow B(x)) \wedge (x)(A(x) \rightarrow C(x)) \rightarrow (A(x) \rightarrow C(x))$
(iv) $(\exists x)(P(x) \wedge Q(x) \rightarrow (y) R(y) \rightarrow S(y))$
and $(\exists y)(R(y) \wedge \sim S(y)) \rightarrow (x)(P(x) \rightarrow \sim Q(x))$
(v) $\sim(x)(P(x) \wedge Q(x), (x) P(x) \rightarrow \equiv \sim(x) Q(x)$

1.88 Check the validity of following conclusion
(a) $(x)(A(x) \rightarrow B(x)), (\exists y) A(x)$ $C : (\exists z) B(z)$
(b) $(\exists y)(A(y) \wedge B(y))$ $C : (y) A(y)$
(c) $(\exists y) A(y), (\exists x) B(y)$ $C : (\exists y)(A(y) \wedge B(y))$

1.89 Using *CP* or otherwise, show the following implications:
(a) $((\exists y) P(y) \rightarrow (y) Q(y)) \rightarrow (y)(P(y) \rightarrow Q(y))$
(b) $(y)(A(y) \rightarrow B(y)), (y)(R(y) \rightarrow \sim D(y)) \rightarrow (y)(R(y) \rightarrow \sim A(y))$
(c) $(y)(A(y) \rightarrow B(y)) \rightarrow (y) A(y) \rightarrow (y) B(y)$

1.90 Show that, if m is an odd integer, then m^2 is an odd integer.

1.91 Show that if $3m + 2$ is odd, then m is odd.

1.92 Suppose $P(m)$ represents the statement "If x and y are positive integers with $x \geq y$, then $x^m \geq y^m$. Prove that the proposition $P(0)$ is true.

1.93 Prove that the sum of two rational numbers is rational.

1.94 Prove that, if m is an integer, and m^2 is odd, then m is odd.

1.95 Show that at least two of any eight days must fall on the same day of the week.

1.96 Show that $|ab| = |a|\,|b|$, where a and b are real numbers and $|a|$ represents the absolute value of a, which equals a when $a \geq 0$ and equals $-a$ if $a < 0$.

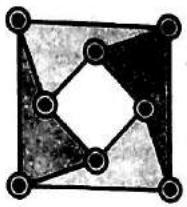
1.97 Prove that the integer m is odd if m^2 is odd.

1.98 Prove that there exist irrational numbers p and q such that p^q is rational.

1.99 Show that every rational number has a multiplicative inverse.

Objective

To discuss the basic concepts of permutations, combinations, discrete probability and conditional probability.



CHAPTER

TWO

PERMUTATIONS, COMBINATIONS, AND DISCRETE PROBABILITY

2.1 INTRODUCTION

In Sec. 1.6 we discussed some results on the size of finite sets. We shall present in this chapter some further results along this line. For example, let A be a finite set of size n. We might wish to know the number of distinct subsets of the set A, that is, the size of the power set of A, $\mathcal{P}(A)$. Furthermore, among all subsets of A, we might wish to know the number of subsets that are of size k. We might also wish to know the number of ordered sets with the components of the ordered sets being the elements of A. For example, let A be a set of 10 senators. The number of subsets in $\mathcal{P}(A)$, which is equal to 2^{10}, is the number of different committees the senators can form [including a committee with no members, corresponding to the empty set in $\mathcal{P}(A)$]. Moreover, the number of subsets of size 6 in $\mathcal{P}(A)$, which is equal to 210, is the number of different 6-member committees they can form. An ordered set of size 3 with distinct components from A might represent the 3 highest vote getters among the 10 senators in the election. There are 720 such ordered sets, corresponding to the 720 different possible outcomes. An ordered set of size 3 with not necessarily distinct components from A might represent the 3 chairpersons of 3 different senate committees consisting of some of the 10 senators. In this chapter, we shall discuss these and related problems in the context of permutations and combinations of objects.

2.2 THE RULES OF SUM AND PRODUCT

By an *experiment*, we mean a physical process that has a number of observable outcomes. Thus, for example, placing a ball in a box, placing a certain number of

balls in a certain number of boxes, selecting a representative among a group of students, assigning offices to professors, placing bets on a horse race, tossing a coin, rolling a pair of dice, and dealing a poker hand are all experiments. For example, for the experiment of placing a ball in a box, there is only one possible outcome. (There is only one way to place a ball in a box.) The two possible outcomes of tossing a coin are *head* and *tail*, the six possible outcomes of rolling a dice are 1, 2, 3, 4, 5, and 6, and both the experiments of dealing a poker hand and selecting five student representatives from 35,000 students have many possible outcomes. When we consider the outcomes of several experiments, we shall follow the rules stated below:

Rule of product. If one experiment has m possible outcomes and another experiment has n possible outcomes, then there are $m \times n$ possible outcomes when both of these experiments take place.

Rule of sum. If one experiment has m possible outcomes and another experiment has n possible outcomes, then there are $m + n$ possible outcomes when exactly one of these experiments takes place.

For example, if there are 52 ways to select a representative for the junior class and 49 ways to select a representative for the senior class, then according to the rule of product, there will be 52×49 ways to select the representatives for both the junior and senior classes. On the other hand, according to the rule of sum, there will be $52 + 49$ ways to select a representative for either the junior or the senior class. As another example, suppose there are seven different courses offered in the morning and five different courses offered in the afternoon. There will be 7×5 choices for students who want to enroll in one course in the morning and one in the afternoon. On the other hand, they will have $7 + 5$ choices if they want to enroll in only one course.

2.3 PERMUTATIONS

Consider the simple problem of placing three balls colored red, blue, and white in 10 boxes numbered 1, 2, 3, ..., 10. We want to know the number of distinct ways in which the balls can be placed in the boxes, if each box can hold only one ball. Let us place the balls one at a time, beginning with the red ball, then the blue ball, and then the white ball. Since the red ball can be placed in any of the 10 boxes, the blue ball can be placed in any of the nine remaining boxes, and the white ball can be placed in any of the eight remaining boxes, the total number of distinct ways to place these balls is $10 \times 9 \times 8 = 720$.

The result of this numerical example can be generalized immediately:

Suppose we are to place r distinctly colored balls in n distinctly numbered boxes with the condition that a box can hold only one ball. Since the first ball can be placed in any one of the n boxes, the second ball can be placed in any one of the remaining $(n-1)$ boxes, ..., and the rth ball can be placed in any one of the remaining $(n-r+1)$ boxes, the total number of distinct ways to place the balls is

$$n(n-1)(n-2)\ldots(n-r+1)$$

which can also be written as*

$$\frac{n!}{(n-r)!}$$

We use the notation $P(n, r)$ for the quantity $n(n-1)(n-2)\ldots(n-r+1)$.

The following examples show that the problem of placing balls in boxes is not as uninteresting as it might seem.

Example 2.1 In how many ways can three examinations be scheduled within a five-day period so that no two examinations are scheduled on the same day? Considering the three examinations as distinctly colored balls and the five days as distinctly numbered boxes, we obtain the result $5 \times 4 \times 3 = 60$. ■

Example 2.2 Suppose that we have seven rooms and want to assign four of them to four programmers as offices and use the remaining three rooms for computer terminals. The assignment can be made in $7 \times 6 \times 5 \times 4 = 840$ different ways because we can view the problem as that of placing four distinct balls (the programmers) into seven distinct boxes (the rooms), with the three boxes that are left empty being the rooms for computer terminals. (We assume that the programmers are distinct but that all computer terminals are identical.) ■

A problem equivalent to placing balls in boxes is that of arranging or permuting distinct objects. By permuting r of n distinct objects, we mean to arrange r of these n objects in some order. For example, there are six ways to permute two of the three objects a, b, c. They are ab, ba, ac, ca, bc, and cb. Since to arrange r of n objects amounts to filling r positions with r of the n objects, there are n choices of an object for the first position, $n-1$ choices of an object (from the $n-1$ remaining objects) for the second position, ..., and $n-r+1$ choices of an object (from the $n-r+1$ remaining objects) for the rth position. Consequently, there are $n(n-1)\ldots(n-r+1)$ ways to arrange r of n objects in order.† In the terminology of ordered sets, there are $n(n-1)\ldots(n-r+1)$ ordered r-tuples that have *distinct* components which are elements from a set of size n.

Consider the following examples:

Example 2.3 Let us determine the number of four-digit decimal numbers that contain no repeated digits. Since this is a problem of arranging 4 of the 10 digits

* $n!$ reads "n factorial" and is defined to be $n(n-1)(n-2)\ldots 2 \times 1$. We also have the convention that 0! is equal to 1.

† A slightly different point of view, which might cause some initial confusion but will prove to be useful eventually, is to consider the problem as that of placing balls in boxes. Consider n boxes corresponding to the n objects, and r balls corresponding to the r positions in the arrangement. The placement of a ball in a certain box is equivalent to putting the object corresponding to the box in a position corresponding to the ball in an arrangement. Consequently, the number of ways to permute r of n objects is $P(n, r)$.

0, 1, 2, ..., 9, the answer is $P(10, 4) = 5040$. Among these 5040 numbers, $9 \times 8 \times 7 = 504$ of them have a leading 0. Consequently, $5040 - 504 = 4536$ of them do not have a leading 0. The result can also be computed as

$$9 \times 9 \times 8 \times 7 = 4536$$

using the argument that the first digit can be any one of the nine digits 1, 2, ..., 9, the second digit can be any of the *nine* remaining digits, and so on. ■

Example 2.4 We note that the number of ways in which we can make up strings of four distinct letters followed by three distinct digits is

$$P(26, 4) \times P(10, 3) = 258{,}336{,}000$$ ■

Let us return to the problem of placing 3 distinctly colored balls into 10 distinctly numbered boxes. Suppose a box can hold as many balls as we wish. Since the red ball can be placed in any of the 10 boxes, as can the blue ball, and as can the white ball, the total number of ways of placement is

$$10 \times 10 \times 10 = 1000$$

In general, there are n^r ways to place r colored balls into n numbered boxes if a box can hold as many balls as we wish.

We consider now some other examples:

Example 2.5 If we are to schedule three examinations within a five-day period with no restriction on the number of examinations scheduled each day, the total number of ways is $5^3 = 125$. ■

Example 2.6 Let us determine the number of subsets of a set A whose size is r. Consider the problem of placing the r elements of A in two boxes. Corresponding to each placement, we can define a subset of A by taking the elements placed in box 1 and discarding the elements placed in box 2. Since there are 2^r ways to place the r elements, there are 2^r subsets in $\mathcal{P}(A)$. ■

Similarly, in terms of permutation of objects, we say that, if there are n distinct kinds of objects with an infinite supply of each kind, then there are n^r ways to arrange r of these n kinds of objects, because there are n choices of an object for the first position, n choices of an object for the second position, ..., and n choices of an object for the rth position. Again, in the terminology of ordered sets, there are n^r ordered r-tuples with their components being elements from a set of size n. For example, there are 10^4 four-digit decimal sequences. Consequently, $10^4 - P(10, 4) = 4960$ of them contain one or more repeated digits.

Example 2.7 We observe first that there are 2^r r-digit binary sequences. We now ask among the 2^r r-digit binary sequences how many of them have an even number of 1s? We can pair off these binary sequences such that two sequences in a pair differ only in the rth digits. Clearly, one of the two sequences in a pair has an even number of 1s and the other has an odd number of 1s. It follows that there are $\frac{1}{2} \cdot 2^r$ r-digit binary sequences that contain an even number of 1s.

There is a slightly different way to derive the same result. There are 2^{r-1} $(r-1)$-digit binary sequences. To an $(r-1)$-digit sequence that has an even number of 1s, we can append a 0 to obtain an r-digit sequence that has an even number of 1s. To an $(r-1)$-digit sequence that has an odd number of 1s, we can append a 1 to obtain an r-digit sequence that has an even number of 1s. Furthermore, in these two ways, we shall obtain all r-digit sequences that have an even number of 1s. Consequently, there are 2^{r-1} of them. Such an idea can be employed to enhance the reliability of computers. Inside a computer, data are represented by sequences of binary digits. In the course of manipulating and transmitting these binary sequences, an error is said to occur if a 0 becomes a 1, or a 1 becomes a 0. So that errors will be detected, we shall use $(r-1)$-digit binary sequences to represent the data and append an rth digit to each sequence so that the resultant r-digit sequence always has an even number of 1s. The occurrence of an error (as a matter of fact, the occurrence of an odd number of errors) will yield a binary sequence with an odd number of 1s. The detection of a binary sequence with an odd number of 1s will signify the presence of an error condition.

We now ask for the number of r-digit quintary sequences (sequences made up of the digits 0, 1, 2, 3, 4) that contain an even number of 1s. We note that among the 5^r r-digit quintary sequences, there are 3^r of them that contain only the digits 2, 3, and 4. These sequences are, of course, counted as sequences containing an even number of 1s. The remaining $5^r - 3^r$ sequences can be divided into groups according to the patterns of 2s, 3s, and 4s in the sequences. (For instance, all sequences of the form $23xx344xx2xxx$ will be in one group, where each x is either 0 or 1.) Since half of the sequences in each group has an even number of 1s, the total number of r-digit quintary sequences with an even number of 1s is $3^r + \frac{1}{2}(5^r - 3^r)$. ■

Example 2.8 Suppose we print all five-digit numbers on slips of paper with one number on each slip. However, since the digits 0, 1, 6, 8, and 9 become 0, 1, 9, 8, and 6 when they are read upside down, there are pairs of numbers that can share the same slip if the slips are read right side up or upside down. For example, we can make up one slip for the numbers 89166 and 99168. The question is then how many distinct slips will we have to make up for all five-digit numbers. We note first that there are 10^5 distinct five-digit numbers. Among these numbers, 5^5 of them can be read either right side up or upside down. (They are made up of the digits 0, 1, 6, 8, and 9.) However, there are numbers that read the same either right side up or upside down, for example, 16091, and there are $3(5^2)$ such numbers. (The center digit of these numbers must be either 1, 0, or 8; furthermore, the fifth digit must be the first digit turned upside down, and the fourth digit must be the second digit turned upside down.) Consequently, there are $5^5 - 3(5^2)$ numbers that can be read either right side up or upside down but will read differently. These numbers can be divided into pairs so that every pair of numbers can share one slip. It follows that the total number of distinct slips we need is $10^5 - [5^5 - 3(5^2)]/2$. ■