Applied Discrete Structures

Applied Discrete Structures

Al Doerr
University of Massachusetts Lowell

Ken Levasseur
University of Massachusetts Lowell

September, 2016

Acknowledgements

We would like to acknowledge the following users for their helpful comments and suggestions.

- Tibor Beke, UMass Lowell
- Alex DeCourcy, UMass Lowell
- Vince DiChiacchio
- William Jozefczyk
- Ravi Montenegro, UMass Lowell
- Jim Propp, UMass Lowell
- Students at Luzurne County Community College (PA)

I would like to thank Rob Beezer, David Farmer and other participants on the mathbook-xml-support group for their guidance and work on MathBook XML. Thanks to the Pedagogy Subcommittee of the UMass Lowell Transformational Education Committee for their financial assistance in helping getting this project started.

Preface

This version of *Applied Discrete Structures* is being developed using *Mathbook XML*, A lightweight XML application for authors of scientific articles, textbooks and monographs initiated by Rob Beezer, U. of Puget Sound.

*What a difference seven years make!*We embarked on this open-source project in 2010. The choice of Mathematica for "source code" was based on the speed with which we could do the conversion. However, the format was not ideal, with no viable web version available. The project has been well-received in spite of these issues. Validation through the listing of this project on the American Institute of Mathematics has been very helpful. When the MBX project was launched, it was the natural next step. The features of MBX make it far more readable than our first versions, with web, pdf and print copies being far more readable.

Twenty-one years after the publication of the 2nd edition of Applied Discrete Structures for Computer Science, in 1989 the publishing and computing landscape had both changed dramatically. We signed a contract for the second edition with Science Research Associates in 1988 but by the time the book was ready to print, SRA had been sold to MacMillan. Soon after, the rights had been passed on to Pearson Education, Inc. In 2010, the long-term future of printed textbooks is uncertain. In the meantime, textbook prices (both printed and e-books) have increased and a growing open source textbook market movement has started. One of our objectives in revisiting this text is to make it available to our students in an affordable format. In its original form, the text was peer-reviewed and was adopted for use at several universities throughout the country. For this reason, we see Applied Discrete Structures as not only an inexpensive alternative, but a high quality alternative.

As indicated above the computing landscape is very different from the 1980's and accounts for the most significant changes in the text. One of the most common programming languages of the 1980's, Pascal; and we used it to illustrate many of the concepts in the text. Although it isn't totally dead, Pascal is far from the mainstream of computing in the 21st century. In 1989, Mathematica had been out for less than a year âĂŤ now a major force in scientific computing. The open source software movement also started in the 1980's and in 2005, the first version of Sage, an open-source alternative to Mathematica was first released. In Applied Discrete Structures we have replaced "Pascal Notes" with "Mathematica Notes" and "Sage Notes." Finally, 1989 was the year that World Wide Web was invented by Tim Berners-Lee. There wasn't a single www in the 2nd edition. In this version, we intend to make use of extensive web resources, including video demonstrations.

We would like to thank Tony Penta, Sitansu Mittra, and Dan Klain for using the preliminary versions of Applied Discrete Structures. The corrections and input they provided was appreciated.

We repeat the preface to Applied Discrete Structures for Computer Science below. Plans for the instructor's guide, which is mentioned in the preface are uncertain at this time.

Preface to Applied Discrete Structures for Computer Science, 2nd Ed. We feel proud and fortunate that most authorities, including MAA and ACM, have settled

on a discrete mathematics syllabus that is virtually identical to the contents of the first edition of Applied Discrete Structures for Computer Science. For that reason, very few topical changes needed to be made in this new edition, and the order of topics is almost unchanged. The main change is the addition of a large number of exercises at all levels. We have "fine-tuned" the contents by expanding the preliminary coverage of sets and combinatorics, and we have added a discussion of binary integer representation. We have also added an introduction including several examples, to provide motivation for those students who may find it reassuring to know that mathematics has "real" applications. "Appendix BâĂŤIntroduction to Algorithms," has also been added to make the text more self-contained.

How This Book Will Help Students In writing this book, care was taken to use language and examples that gradually wean students from a simpleminded mechanical approach and move them toward mathematical maturity. We also recognize that many students who hesitate to ask for help from an instructor need a readable text, and we have tried to anticipate the questions that go unasked. The wide range of examples in the text are meant to augment the "favorite examples" that most instructors have for teaching the topics in discrete mathematics.

To provide diagnostic help and encouragement, we have included solutions and/or hints to the odd-numbered exercises. These solutions include detailed answers whenever warranted and complete proofs, not just terse outlines of proofs. Our use of standard terminology and notation makes Applied Discrete Structures for Computer Science a valuable reference book for future courses. Although many advanced books have a short review of elementary topics, they cannot be complete.

How This Book Will Help Instructors The text is divided into lecture-length sections, facilitating the organization of an instructor's presentation. Topics are presented in such a way that students' understanding can be monitored through thought-provoking exercises. The exercises require an understanding of the topics and how they are interrelated, not just a familiarity with the key words.

How This Book Will Help the Chairperson/Coordinator The text covers the standard topics that all instructors must be aware of; therefore it is safe to adopt Applied Discrete Structures for Computer Science before an instructor has been selected. The breadth of topics covered allows for flexibility that may be needed due to last-minute curriculum changes.

Since discrete mathematics is such a new course, faculty are often forced to teach the course without being completely familiar with it. An Instructor's Guide is an important feature for the new instructor. *An instructor's guide is not currently available for the open-source version of the project.*

What a Difference Five Years Makes! In the last five years, much has taken place in regards to discrete mathematics. A review of these events is in order to see how they have affected the Second Edition of Applied Discrete Structures for Computer Science. (1) Scores of discrete mathematics texts have been published. Most texts in discrete mathematics can be classified as one-semester or two- semester texts. The two-semester texts, such as Applied Discrete Structures for Computer Science, differ in that the logical prerequisites for a more thorough study of discrete mathematics are developed. (2) Discrete mathematics has become more than just a computer science support course. Mathematics majors are being required to take it, often before calculus. Rather than reducing the significance of calculus, this recognizes that the material a student sees in a discrete mathematics/struc- tures course strengthens his or her understanding of the theoretical aspects of calculus. This is particularly important for today's students, since many high school courses in geometry stress mechanics as opposed to proofs. The typical college freshman is skill-oriented and does not have a high level of mathematical maturity. Discrete mathematics is also more typical of the higher-level courses that a mathematics major is likely to take. (3) Authorities such as MAA, ACM, and A. Ralson have

all refined their ideas of what a discrete mathematics course should be. Instead of the chaos that characterized the early '80s, we now have some agreement, namely that discrete mathematics should be a course that develops mathematical maturity. (4) Computer science enrollments have leveled off and in some cases have declined. Some attribute this to the lay-offs that have taken place in the computer industry; but the amount of higher mathematics that is needed to advance in many areas of computer science has also discouraged many. A year of discrete mathematics is an important first step in overcoming a deficiency in mathematics. (5) The Educational Testing Service introduced its Advanced Placement Exam in Computer Science. The suggested preparation for this exam includes many discrete mathematics topics, such as trees, graphs, and recursion. This continues the trend toward offering discrete mathematics earlier in the overall curriculum.

Acknowledgments The authors wish to thank our colleagues and students for their comments and assistance in writing and revising this text. Among those who have left their mark on this edition are Susan Assmann, Shim Berkovitz, Tony Penta, Kevin Ryan, and Richard Winslow.

We would also like to thank Jean Hutchings, Kathy Sullivan, and Michele Walsh for work that they did in typing this edition, and our department secretaries, Mrs. Lyn Misserville and Mrs. Danielle White, whose cooperation in numerous ways has been greatly appreciated.

We are grateful for the response to the first edition from the faculty and students of over seventy-five colleges and universities. We know that our second edition will be a better learning and teaching tool as a result of their useful comments and suggestions. Our special thanks to the following reviewers: David Buchthal, University of Akron; Ronald L. Davis, Millersville University; John W Kennedy, Pace University; Betty Mayfield, Hood College; Nancy Olmsted, Worcester State College; and Pradip Shrimani, Southern Illinois University. Finally, it has been a pleasure to work with Nancy Osman, our acquisitions editor, David Morrow, our development editor, and the entire staff at SRA.

Sage (sagemath.org) is a free, open source, software system for advanced mathematics. Sage can be used either on your own computer, a local server, or on SageMathCloud (https://cloud.sagemath.com).

Ken LevasseurLowell MA

Contents

Chapter 1

Set Theory I

Goals for Chapter 1

1.1 Set Notation and Relations

1.1.1 The notion of a set

The term set is intuitively understood by most people to mean a collection of objects that are called elements (of the set). This concept is the starting point on which we will build more complex ideas, much as in-geometry where the concepts of point and line are left undefined. Because a set is such a simple notion, you may be surprised to learn that it is one of the most difficult concepts for mathematicians to define to their own liking. For example, the description above is not a proper definition because it requires the definition of a collection. (How would you define "collection"?) Even deeper problems arise when you consider the possibility that a set could contain itself. Although these problems are of real concern to some mathematicians, they will not be of any concern to us. Our first concern will be how to describe a set; that is, how do we most conveniently describe a set and the elements that are in it? If we are going to discuss a set for any length of time, we usually give it a name in the form of a capital letter (or occasionally some other symbol). In discussing set A, if x is an element of A, then we will write $x \in A$. On the other hand, if x is not an element of A, we write $x \notin A$. The most convenient way of describing the elements of a set will vary depending on the specific set.

Enumeration. When the elements of a set are enumerated (or listed) it is traditional to enclose them in braces. For example, the set of binary digits is$\{0, 1\}$ and the set of decimal digits is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The choice of a name for these sets would be arbitrary; but it would be "logical" to call them B and D , respectively. The choice of a set name is much like the choice of an identifier name in programming. Some large sets can be enumerated without actually listing all the elements. For example, the letters of the alphabet and the integers from 1 to 100 could be described as $A = \{a, b, c, \ldots, x, y, z\}$, and $G = \{1, 2, \ldots, 99, 100\}$. The three consecutive "dots" are called an ellipsis. We use them when it is clear what elements are included but not listed. An ellipsis is used in two other situations. To enumerate the positive integers, we would write $\{1, 2, 3, \ldots\}$, indicating that the list goes on infinitely. If we want to list a more general set such as the integers between 1 and n, where n is some undetermined positive integer, we might write $\{1, \ldots, n\}$.

Standard Symbols. Frequently used sets are usually given symbols that are reserved for them alone. For example, since we will be referring to the positive integers throughout this book, we will use the symbol $\mathbb{P}$ instead of writing $\{1, 2, 3, \ldots\}$. A few of the other sets of numbers that we will use frequently are:

- ($\mathbb{N}$): the natural numbers, $\{0, 1, 2, 3, \ldots\}$
- ($\mathbb{Z}$): the integers, $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- ($\mathbb{Q}$): the rational numbers
- ($\mathbb{R}$): the real numbers
- ($\mathbb{C}$): the complex numbers

Set-Builder Notation. Another way of describing sets is to use set-builder notation. For example, we could define the rational numbers as

$$\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$$

Note that in the set-builder description for the rational numbers:

- a/b indicates that a typical element of the set is a "fraction."
- The vertical line, |, is read "such that" or "where," and is used interchangeably with a colon.
- $a, b \in \mathbb{Z}$ is an abbreviated way of saying a and b are integers.
- Commas in mathematics are read as "and."

The important fact to keep in mind in set notation, or in any mathematical notation, is that it is meant to be a help, not a hindrance. We hope that notation will assist us in a more complete understanding of the collection of objects under consideration and will enable us to describe it in a concise manner. However, brevity of notation is not the aim of sets. If you prefer to write $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ instead of $a, b \in \mathbb{Z}$, you should do so. Also, there are frequently many different, and equally good, ways of describing sets. For example, $\{x \in \mathbb{R} \mid x^2 - 5x + 6 = 0$ and $\{x \,|x \in \mathbb{R}, x^2 - 5x + 6 = 0\}$ both describe the solution set $\{2, 3\}$.

A proper definition of the real numbers is beyond the scope of this text. It is sufficient to think of the real numbers as the set of points on a number line. The complex numbers can be defined using set-builder notation as $\mathbb{C} = \{a+bi : a, b \in \mathbb{R}\}$, where $i^2 = -1$.

In the following definition we will leave the word "finite" undefined.

Definition 1.1.1 (Finite Set)**.** A set is a finite set if it has a finite number of elements. Any set that is not finite is an infinite set. Informal definition of "finite set."

Definition 1.1.2 (Cardinality)**.** Let A be a finite set. The number of different elements in A is called its cardinality.

As we will see later, there are different infinite cardinalities. We can't make this distinction until Chapter 7, so we will restrict cardinality to finite sets for now.

1.1.2 Subsets

Definition 1.1.3 (Subset)**.** Let A and B be sets. We say that A is a subset of B if and only if every element of A is an element of B.

Example 1.1.4 (Some Subsets)**.**

1. If $A = \{3, 5, 8\}$ and $B = \{5, 8, 3, 2, 6\}$, then $A \subseteq B$.
2. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

3. If $S = \{3, 5, 8\}$ and $T = \{5, 3, 8\}$, then $S \subseteq T$ and $T \subseteq S$.

Definition 1.1.5 (Set Equality)**.** Let A and B be sets. We say that A is equal to B (notation $A = B$) if and only if every element of A is an element of B and conversely every element of B is an element of A; that is, $A \subseteq B$ and $B \subseteq A$.

Example 1.1.6 (Examples illustrating set equality)**.**

1. In Example 1.1.4, $S = T$. Note that the ordering of the elements is unimportant.

2. The number of times that an element appears in an enumeration doesn't affect a set. For example, if $A = \{1, 5, 3, 5\}$ and $B = \{1, 5, 3\}$, then $A = B$. Warning to readers of other texts: Some books introduce the concept of a multiset, in which the number of occurrences of an element matters.

A few comments are in order about the expression "if and only if" as used in our definitions. This expression means "is equivalent to saying," or more exactly, that the word (or concept) being defined can at any time be replaced by the defining expression. Conversely, the expression that defines the word (or concept) can be replaced by the word.

Occasionally there is need to discuss the set that contains no elements, namely the empty set, which is denoted by $\emptyset$. This set is also called the null set.

It is clear, we hope, from the definition of a subset, that given any set A we have $A \subseteq A$ and $\emptyset \subseteq A$. Both $\emptyset$ and A are called *improper subsets* of A. If $B \subseteq A$, $B \neq \emptyset$, and $B \neq A$, then B is called a *proper subset* of A.

1.1.3 Exercises for Section 1.1

A Exercises

1. List four elements of each of the following sets:

(a) $\{k \in \mathbb{P} \mid k - 1 \text{ is a multiple of } 7\}$

(b) $\{x \mid x \text{ is a fruit and its skin is normally eaten }\}$

(c) $\{x \in \mathbb{Q} \mid x \in \mathbb{Z}\}$

(d) $\{2n \mid n \in \mathbb{Z}, n < 0\}$

(e) $\{s \mid s = 1 + 2 + \cdots + n, n \in \mathbb{P}\}$

Answer. These answers are not unique.

(a) $8, 15, 22, 29$

(b) apple, pear, peach, plum

(c) $1/2, 1/3, 1/4, 1/5$

(d) $-8, -6, -4, -2$

(e) $6, 10, 15, 21$

2. List all elements of the following sets:

(a) $\{\frac{1}{n} \mid n \in \{3, 4, 5, 6\}\}$

(b) $\{\alpha \in \text{ the alphabet } \mid \alpha \text{ precedes F}\}$

(c) $\{-k \mid k \in \mathbb{P}\}$

(d) $\{n^2 \mid n = -2, -1, 0, 1, 2\}$

(e) $\{n \in \mathbb{P} \mid n\text{is a factor of } 24\ \}$

3. Describe the following sets using set-builder notation.

(a) $\{5, 7, 9, \ldots, 77, 79\}$
(b) the rational numbers that are strictly between -1 and 1
(c) the even integers
(d) $\{-18, -9, 0, 9, 18, 27, \ldots\}$

Answer.

(a) $\{2k + 1 \mid k \in \mathbb{Z}, 2 \leqslant k \leqslant 39\}$
(b) $\{x \in \mathbb{Q} \mid -1 < x < 1\}$
(c) $\{2n \mid n \in \mathbb{Z}\}$
(d) $\{9n \mid n \in \mathbb{Z}, -2 \leq n\}$

4. Use set-builder notation to describe the following sets:

(a) $\{1, 2, 3, 4, 5, 6, 7\}$
(b) $\{1, 10, 100, 1000, 10000\}$
(c) $\{1, 1/2, 1/3, 1/4, 1/5, ...\}$
(d) $\{0\}$

5. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, and $C = \{1, 5, 9\}$. Determine which of the following statements are true. Give reasons for your answers.

(a) $3 \in A$
(b) $\{3\} \in A$
(c) $\{3\} \subseteq A$
(d) $B \subseteq A$
(e) $A \subseteq B$
(f) $\emptyset \subseteq C$
(g) $\emptyset \in A$
(h) $A \subseteq A$

Answer.

(a) True
(b) False
(c) True
(d) True
(e) False
(f) True
(g) False
(h) True

C Exercises

6. One reason that we left the definition of a set vague is Russell's Paradox. Many mathematics and logic books contain an account of this paradox. Two references are Stoll and Quine. Find one such reference and read it.

1.2 Basic Set Operations

1.2.1 Definitions

Definition 1.2.1 (Intersection)**.** Let A and B be sets. The intersection of A and B (denoted by $A \cap B$) is the set of all elements that are in both A and B. That is, $A \cap B = \{x : x \in A \text{ and } x \in B)$.

Example 1.2.2 (Some Intersections)**.**

- Let $A = \{1, 3, 8\}$ and $B = \{-9, 22, 3\}$. Then $A \cap B = \{3\}$.
- Solving a system of simultaneous equations such as $x + y = 7$ and $x - y = 3$ can be viewed as an intersection. Let $A = \{(x, y) : x + y = 7, x, y \in \mathbb{R}\}$ and $B = \{(x, y) : x - y - 3, x, y \in \mathbb{R}\}$. These two sets are lines in the plane and their intersection, $A \cap B = \{(5, 2)\}$, is the solution to the system.

- $\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$.

- If $A = \{3, 5, 9\}$ and $B = \{-5, 8\}$, then $A \cap B = \emptyset$.

Definition 1.2.3 (Disjoint Sets)**.** Two sete are disjoint if they have no elements in common (as in Example 1.2.1 d). That is, A and B are disjoint if $A \cap B = \emptyset$.

Definition 1.2.4 (Union)**.** Let A and B be sets. The union of A and B (denoted by $A \cup B$) is the set of all elements that are in A or in B or in both A and B. That is, $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

It is important to note in the set-builder notation for $A \cup B$, the word "or" is used in the inclusive sense; it includes the case where x is in both A and B.

Example 1.2.5 (Some Unions)**.**

- If $A = \{2, 5, 8\}$ and $B = \{7, 5, 22\}$, then $A \cup B = \{2, 5, 8, 7, 22\}$.

- $\mathbb{Z} \cup \mathbb{Q} = \mathbb{Q}$.

- $A \cup \emptyset = A$ for any set A.

Frequently, when doing mathematics, we need to establish a universe or set of elements under discussion. For example, the set $A = \{x : 81x^4 - 16 = 0\}$ contains different elements depending on what kinds of numbers we allow ourselves to use in solving the equation $81x^4 - 16 = 0$. This set of numbers would be our universe. For example, if the universe is the integers, then A is empty. If our universe is the rational numbers, then A is $\{2/3, -2/3\}$ and if the universe is the complex numbers, then A is $\{2/3, -2/3, 2i/3, -2i/3\}$.

Definition 1.2.6 (Universe)**.** The universe, or universal set, is the set of all elements under discussion for possible membership in a set. We normally reserve the letter U for a universe in general discussions.

1.2.2 Set Operations and their Venn Diagams

When working with sets, as in other branches of mathematics, it is often quite useful to be able to draw a picture or diagram of the situation under consideration. A diagram of a set is called a Venn diagram. The universal set U is represented by the interior of a rectangle and the sets by disks inside the rectangle.

Example 1.2.7 (Venn Diagram Examples)**.** (a) $A \cap B$ is illustrated in 1.2.8 by shading the appropriate region.

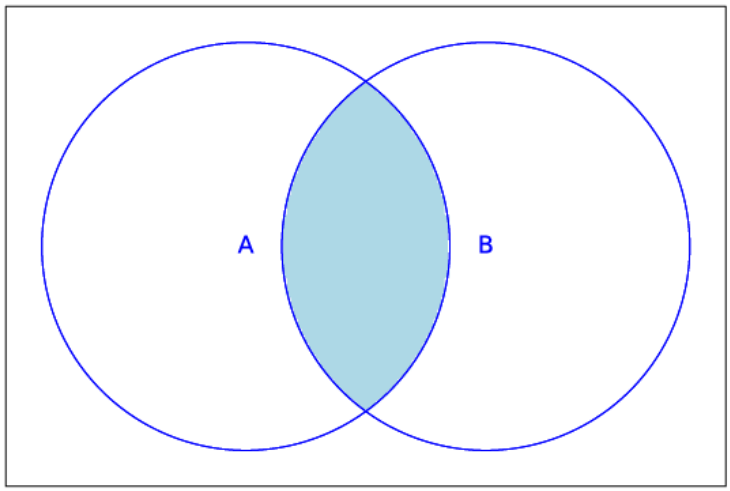


Figure 1.2.8: Venn Diagram for the Intersection of Two Sets

(b) The union $A \cup B$ is illustrated in 1.2.9.

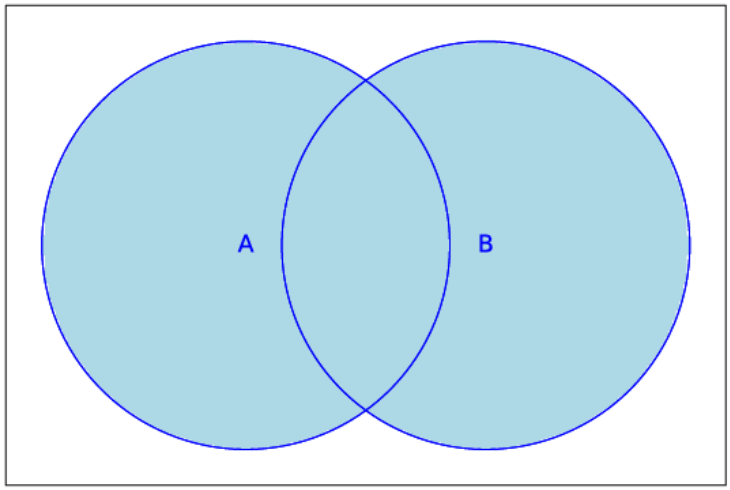


Figure 1.2.9: Venn Diagram for the union $A \cup B$

In a Venn diagram, the region representing $A \cap B$ does not appear empty; however, in some instances it will represent the empty set. The same is true for any other region in a Venn diagram.

Definition 1.2.10 (Complement of a set)**.** Let A and B be sets. The complement of A relative to B (notation $B - A$) is the set of elements that are in B and not in A. That is, $B - A = \{x : x \in B \text{ and } x \notin A\}$. If U is the universal set, then $U - A$ is denoted by A^c and is called simply the complement of A. $A^c = \{x \in U : x \notin A\}$.

Example 1.2.11 (Some Complements)**.**

1. Let $U = \{1, 2, 3, ..., 10\}$ and $A = \{2, 4, 6, 8, 10\}$. Then $U - A = \{1, 3, 5, 7, 9\}$ and $A - U = \emptyset$

2. If $U = \mathbb{R}$, then the complement of the rational numbers is the irrational numbers.

3. $U^c = \emptyset$ and $\emptyset^c = U$.

4. The Venn diagram of $B - A$ is represented in 1.2.12.

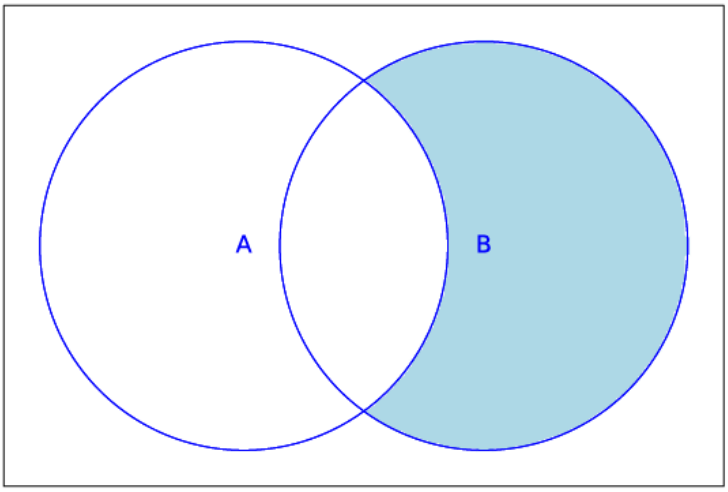


Figure 1.2.12: Venn Diagram for $B - A$

5. The Venn diagram of A^c is represented in 1.2.13.

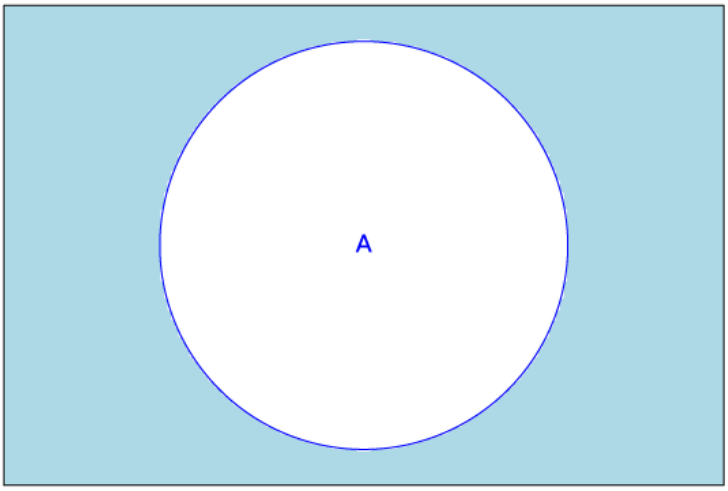


Figure 1.2.13: Venn Diagram for A^c

6. If $B \subseteq A$, then the Venn diagram of $A - B$ is as shown in 1.2.14.

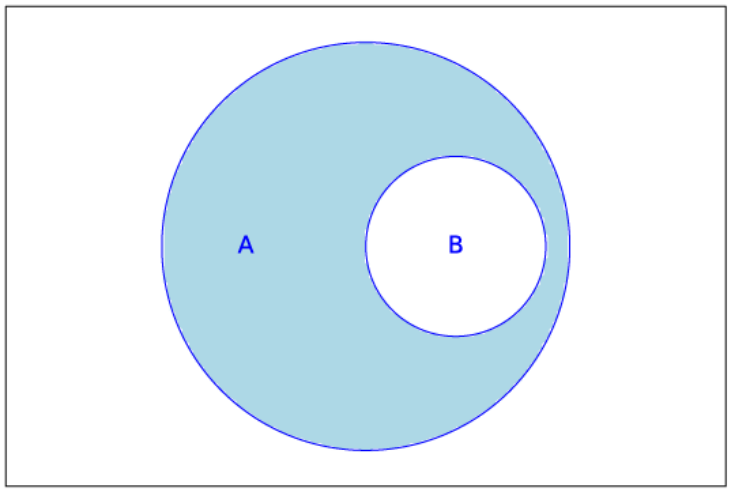


Figure 1.2.14: Venn Diagram for A^c

7. In the universe of integers, the set of even integers, $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$, has the set of odd integers as its complement.

Definition 1.2.15 (Symmetric Difference)**.** Let A and B be sets. The symmetric difference of A and B (denoted by $A \oplus B$) is the set of all elements that are in A and B but not in both. That is, $A \oplus B = (A \cup B) - (A \cap B)$.

Example 1.2.16 (Some Symmetric Differences)**.**

1. Let $A = \{1, 3, 8\}$ and $B = \{2, 4, 8\}$. Then $A \oplus B = \{1, 2, 3, 4\}$.
2. $A \oplus 0 = A$ and $A \oplus A = \emptyset$ for any set A.
3. $\mathbb{R} \oplus \mathbb{Q}$ is the set of irrational numbers.
4. The Venn diagram of $A \oplus B$ is represented in 1.2.17.

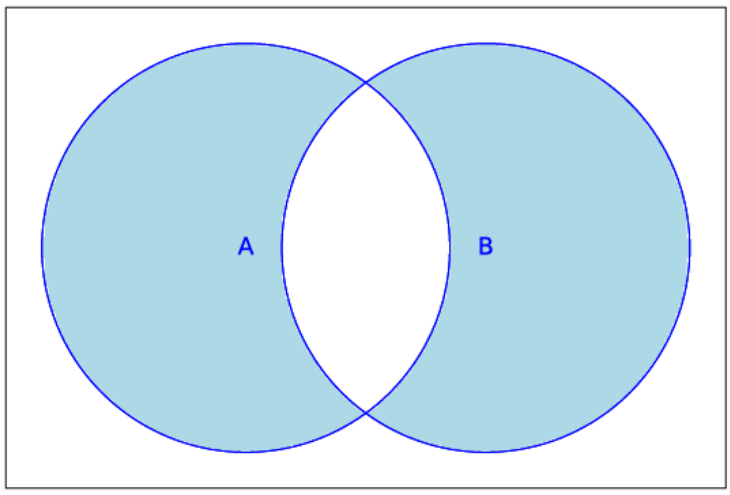


Figure 1.2.17: Venn Diagram for the symmetric difference $A \oplus B$

1.2.2.1 Sage Note: Sets

To work with sets in Sage, a set is an expression of the form Set(*list*). By wrapping a list with set, the order of elements appearing in the list and their duplication are ignored. For example, L1 and L2 are two different lists, but notice how as sets they are considered equal:

```
L1=[3,6,9,0,3]
L2=[9,6,3,0,9]
[L1==L2, Set(L1)==Set(L2) ]
```

```
[False,True]
```

The standard set operations are all methods and/or functions that can act on Sage sets. *You need to evalute the following cell to use the subsequent cell.*

```
A=Set(srange(5,50,5))
B=Set(srange(6,50,6))
[A,B]
```

```
[{35, 5, 40, 10, 45, 15, 20, 25, 30}, {36, 6, 42, 12, 48, 18, 24,
    30}]
```

We can test membership, asking whether 10 is in each of the sets:

```
[10 in A, 10 in B]
```

```
[True, False]
```

The ampersand is used for the intersection of sets. Change it to the vertical bar, |, for union.

```
A & B
```

```
{30}
```

Symmetric difference and set complement are defined as methods in Sage. Here is how to compute the symmetric difference of A with B, followed by their differences.

```
[A.symmetric_difference(B),A.difference(B),B.difference(A)]
```

```
[{35, 36, 5, 6, 40, 42, 12, 45, 15, 48, 18, 20, 24, 25, 10},
 {35, 5, 40, 10, 45, 15, 20, 25},
 {48, 18, 36, 6, 24, 42, 12}]
```

1.2.3 EXERCISES FOR SECTION 1.2

A Exercises

1. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, $C = \{1, 5, 9\}$, and let the universal set be $U = \{0, 1, 2, ..., 9\}$. Determine:

(a) $A \cap B$
(b) $A \cup B$
(c) $B \cup A$
(d) $A \cup C$
(e) $A - B$
(f) $B - A$
(g) A^c
(h) C^c
(i) $A \cap C$
(j) $A \oplus B$

Answer.

(a) $\{2,3\}$
(b) $\{0,2,3\}$
(c) $\{0,2,3\}$
(d) $\{0,1,2,3,5,9\}$
(e) $\{0\}$
(f) $\emptyset$
(g) $\{1,4,5,6,7,8,9\}$
(h) $\{0,2,3,4,6,7,8\}$
(i) $\emptyset$
(j) $\{0\}$

2. Let A, B, and C be as in Exercise 1, let $D = \{3,2\}$, and let $E = \{2,3,2\}$. Determine which of the following are true. Give reasons for your decisions.

(a) $A = B$
(b) $B = C$
(c) $B = D$
(d) $E = D$
(e) $A \cap B = B \cap A$
(f) $A \cup B = B \cup A$
(g) $A - B = B - A$
(h) $A \oplus B = B \oplus A$

3. Let $U = \{1,2,3,...,9\}$. Give examples of sets A, B, and C for which:

(a) $A \cap (B \cap C) = (A \cap B) \cap C$
(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(c) $(A \cup B)^c = A^c \cap B^c$
(d) $A \cup A^c = U$
(e) $A \subseteq A \cup B$
(f) $A \cap B \subseteq A$

Answer. These are all true for any sets A, B, and C.

4. Let $U = \{1,2,3,...,9\}$. Give examples to illustrate the following facts:

(a) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
(b) $A - B \neq B - A$
(c) If $U = A \cup B$ and A ∩ B = ∅, it always follows that $A = U - B$.
(d) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

B Exercises

5. What can you say about A if $U = \{1,2,3,4,5\}$, $B = \{2,3\}$, and (separately)

(a) $A \cup B = \{1,2,3,4\}$
(b) $A \cap B = \{2\}$
(c) $A \oplus B = \{3,4,5\}$

Answer.

(a) $\{1,4\} \subseteq A \subseteq \{1,2,3,4\}$
(b) $\{2\} \subseteq A \subseteq \{1,2,4,5\}$
(c) $A = \{2,4,5\}$

6. Suppose that U is an infinite universal set, and A and B are infinite subsets of U. Answer the following questions with a brief explanation.

(a) Must A^c be finite?
(b) Must $A \cup B$ infinite?
(c) Must $A \cap B$ be infinite?

7. Given that U = all students at a university, D = day students, M = mathematics majors, and G = graduate students. Draw Venn diagrams illustrating this situation and shade in the following sets:

(a) evening students

(b) undergraduate mathematics majors

(c) non-math graduate students

(d) non-math undergraduate students

Answer.

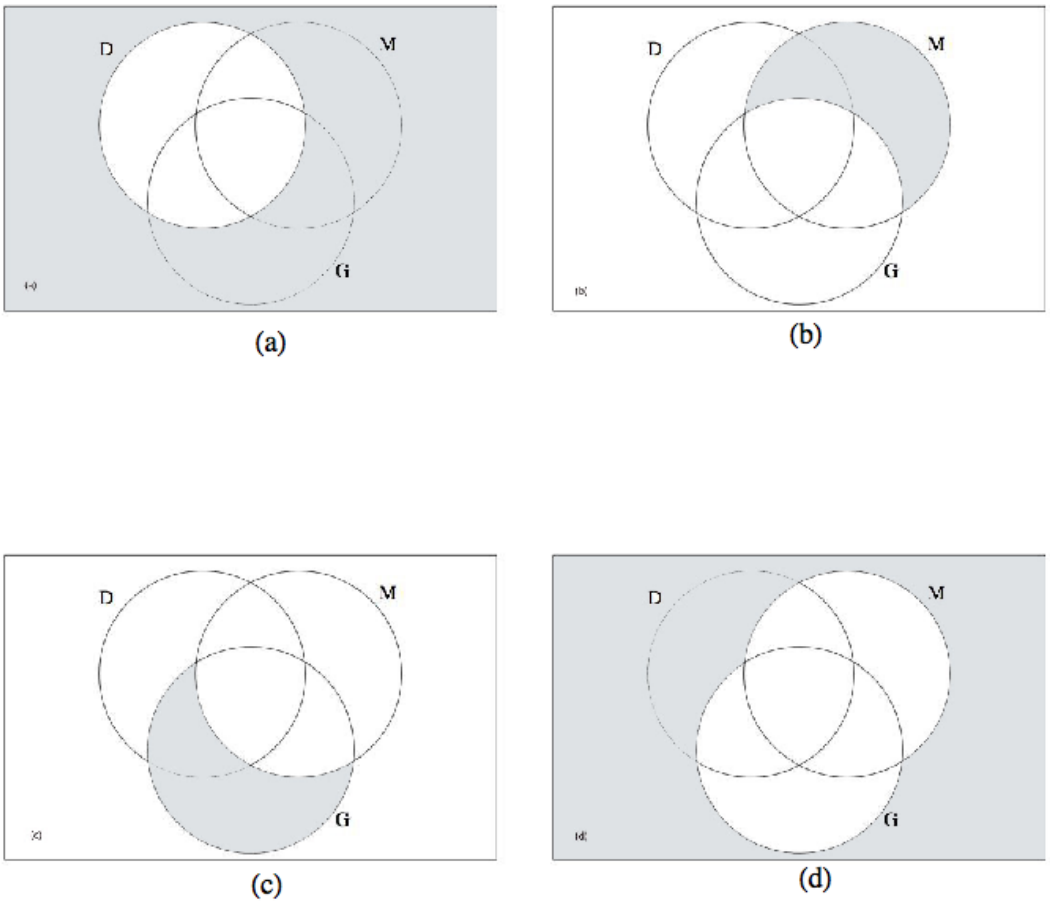


Figure 1.2.18

8. Let the sets D, M, G, and U be as in exercise 7. Let $|U| = 16,000$, $|D| = 9,000$, $|M| = 300$, and $|G| = 1,000$. Also assume that the number of day students who are mathematics majors is 250, fifty of whom are graduate students, that there are 95 graduate mathematics majors, and that the total number of day graduate students is 700. Determine the number of students who are:

(a) evening students

(b) nonmathematics majors

(c) undergraduates (day or evening)

(d) day graduate nonmathematics majors

(e) evening graduate students

(f) evening graduate mathematics majors

(g) evening undergraduate nonmathematics majors

1.3 Cartesian Products and Power Sets

Definition 1.3.1 (Cartesian Product)**.** Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is defined as follows: $A \times B = \{(a, b) \mid a \in A \quad \text{and} \quad b \in B\}$, that is, $A \times B$ is the set of all possible ordered pairs whose first component comes from A and whose second component comes from B.

Example 1.3.2 (Some Cartesian Products)**.** Notation in mathematics is often developed for good reason. In this case, a few examples will make clear why the symbol $\times$ is used for Cartesian products.

- Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Then $A \times B = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}$. Note that $|A \times B| = 6 = |A| \times |B|$.
- $A \times A = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$. Note that $|A \times A| = 9 = |A|^2$.

These two examples illustrate the general rule: If A and B are finite sets, then $|A \times B| = |A| \times |B|$.

We can define the Cartesian product of three (or more) sets similarly. For example, $A \times B \times C = \{(a, b, c) : a \in A, b \in B, c \in C\}$.

It is common to use exponents if the sets in a Cartesian product are the same:

$$A^2 = A \times A$$

$$A^3 = A \times A \times A$$

and in general,

$$A^n = \underbrace{A \times A \times \ldots \times A}_{n \text{ factors}}$$

.

1.3.1 Power Sets

Definition 1.3.3 (Power Set)**.** If A is any set, the power set of A is the set of all subsets of A, denoted $\mathcal{P}(A)$.

The two extreme cases, the empty set and all of A, are both included in $\mathcal{P}(A)$.

Example 1.3.4 (Some Power Sets)**.**

- $\mathcal{P}(\emptyset) = \{\emptyset\}$
- $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$
- $\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

We will leave it to you to guess at a general formula for the number of elements in the power set of a finite set. In Chapter 2, we will discuss counting rules that will help us derive this formula.

1.3.2 Sage Note: Cartesion Products and Power Sets

Here is a simple example of a cartesion product of two sets:

```
A=Set([0,1,2])
B=Set(['a','b'])
P=cartesian_product([A,B]);P
```

```
The cartesian product of ({0, 1, 2}, {'a', 'b'})
```

Here is the cardinality of the cartesian product.

```
P.cardinality()
```

```
6
```

The power set of a set is an iterable, as you can see from the output of this next cell

```
U=Set([0,1,2,3])
subsets(U)
```

```
<generator object powerset at 0x7fec5ffd33c0>
```

You can iterate over a powerset - here is a trivial example.

```
for a in subsets(U):
    print(str(a)+ "␣has␣" +str(len(a))+"␣elements.")
```

```
[] has 0 elements.
[0] has 1 elements.
[1] has 1 elements.
[0, 1] has 2 elements.
[2] has 1 elements.
[0, 2] has 2 elements.
[1, 2] has 2 elements.
[0, 1, 2] has 3 elements.
[3] has 1 elements.
[0, 3] has 2 elements.
[1, 3] has 2 elements.
[0, 1, 3] has 3 elements.
[2, 3] has 2 elements.
[0, 2, 3] has 3 elements.
[1, 2, 3] has 3 elements.
[0, 1, 2, 3] has 4 elements.
```

1.3.3 EXERCISES FOR SECTION 1.3

A Exercises

1. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, $C = \{1, 4\}$, and let the universal set be $U = \{0, 1, 2, 3, 4\}$. List the elements of

(a) $A \times B$

(b) $B \times A$

(c) $A \times B \times C$

(d) $U \times \emptyset$

(e) $A \times A^c$

(f) B^2

(g) B^3

(h) $B \times \mathcal{P}(B)$

Answer.

(a) $\{(0,2),(0,3),(2,2),(2,3),(3,2),(3,3)\}$

(b) $\{(2,0),(2,2),(2,3),(3,0),(3,2),(3,3)\}$

(c) $\{(0,2,1),(0,2,4),(0,3,1),(0,3,4),(2,2,1),(2,2,4),$
$(2,3,1),(2,3,4),(3,2,1),(3,2,4),(3,3,1),(3,3,4)\}$

(d) $\emptyset$

(e) $\{(0,1),(0,4),(2,1),(2,4),(3,1),(3,4)\}$

(f) $\{(2,2),(2,3),(3,2),(3,3)\}$

(g) $\{(2,2,2),(2,2,3),(2,3,2),(2,3,3),(3,2,2),(3,2,3),(3,3,2),(3,3,3)\}$

(h) $\{(2,\emptyset),(2,\{2\}),(2,\{3\}),(2,\{2,3\}),(3,\emptyset),(3,\{2\}),(3,\{3\}),(3,\{2,3\})\}$

2. Suppose that you are about to flip a coin and then roll a die. Let $A = \{HEADS, TAILS\}$ and $B = 1$, 2, 3, 4, 5, 6.

- What is $|A \times B|$?
- How could you interpret the set $A \times B$?

3. List all two-element sets in $\mathcal{P}(\{a,b,c,d\})$

Answer. $\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\} and \{c,d\}$

4. List all three-element sets in $\mathcal{P}(\{a,b,c,d\})$.

5. How many singleton (one-element) sets are there in $\mathcal{P}(A)$ if $|A| = n$?

Answer. There are n singleton subsets, one for each element.

6. A person has four coins in his pocket: a penny, a nickel, a dime, and a quarter. How many different sums of money can he take out if he removes 3 coins at a time?

7. Let $A = \{+,-\}$ and $B = \{00,01,10,11\}$.

- List the elements of $A \times B$
- How many elements do A^4 and $(A \times B)^3$ have?

Answer.

(a) $\{+00,+01,+10,+11,-00,-01,-10,-11\}$

(b) 16 and 512

B Exercises

8. Let $A = \{\bullet, \square, \otimes\}$ and $B = \{\square, \ominus, \bullet\}$.

- List the elements of $A \times B$ and $B \times A$. The parentheses and comma in an ordered pair are not necessary in cases such as this where the elements of each set are individual symbol.
- Identify the intersection of $A \times B$ and $B \times A$. for the case above, and then guess at a general rule for the intersection of $A \times B$ and $B \times A$. where A and B are any two sets.

9. Let A and B be nonempty sets. When are $A \times B$ and $B \times A$. equal?

Answer. They are equal when $A = B$.

1.4 Binary Representation of Positive Integers

Recall that the set of positive integers, $\mathbb{P}$, is $\{1, 2, 3, ...\}$. Positive integers are naturally used to count things. There are many ways to count and many ways to record, or represent, the results of counting. For example, if we wanted to count five hundred twenty-three apples, we might group the apples by tens. There would be fifty-two groups of ten with three single apples left over. The fifty-two groups of ten could be put into five groups of ten tens (hundreds), with two tens left over. The five hundreds, two tens, and three units is recorded as 523. This system of counting is called the base ten positional system, or decimal system. It is quite natural for us to do grouping by tens, hundreds, thousands, ... since it is the method that all of us use in everyday life.

The term positional refers to the fact that each digit in the decimal representation of a number has a significance based on its position. Of course this means that rearranging digits will change the number being described. You may have learned of numeraton systems in which the position of symbols does not have any significance (e.g., the ancient Egyptian system). Most of these systems are merely curiosities to us now.

The binary number system differs from the decimal number system in that units are grouped by twos, fours, eights, etc. That is, the group sizes are powers of two instead of powers of ten. For example, twenty-three can be grouped into eleven groups of two with one left over. The eleven twos can be grouped into five groups of four with one group of two left over. Continuing along the same lines, we find that twenty-three can be described as one sixteen, zero eights, one four, one two, and one one, which is abbreviated 10111_{two}, or simply 10111 if the context is clear.

The process that we used to determine the binary representation of 23 can be described in general terms to determine the binary representation of any positive integer n. A general description of a process such as this one is called an algorithm. Since this is the first algorithm in the book, we will first write it out using less formal language than usual, and then introduce some "algorithmic notation." If you are unfamiliar with algorithms, we refer you to Section A.1.1

1. Start with an empty list of bits.
2. Step Two: Assign the variable k the value n.
3. Step Three: While k's value is positive, continue performing the following three steps until k becomes zero and then stop.
   (a) divide k by 2, obtaining a quotient q (often denoted k div 2) and a remainder r (denoted (k mod 2)).
   (b) attach r to the left-hand side of the list of bits.
   (c) assign the variable k the value q.

Example 1.4.1 (An example of conversion to binary)**.** To determine the binary representation of 41 we take the following steps:

- $41 = 2 \times 20 + 1 \quad List = 1$
- $20 = 2 \times 10 + 0 \quad List = 01$
- $10 = 2 \times 5 + 0 \quad List = 001$
- $5 = 2 \times 2 + 1 \quad List = 1001$
- $2 = 2 \times 1 + 0 \quad List = 01001$
- $1 = 2 \times 0 + 1 \quad List = 101001$

Therefore, $41 = 101001_{\text{two}}$

The notation that we will use to describe this algorithm and all others is called pseudocode, an informal variation of the instructions that are commonly used in many computer languages. Read the following description carefully, comparing it with the informal description above. Appendix B, which contains a general discussion of the components of the algorithms in this book, should clear up any lingering questions. Anything after // are comments.

Algorithm 1.4.2 (Binary Conversion Algorithm)**.** *An algorithm for determining the binary representation of a positive integer.*

Input: a positive integer n.

Output: the binary representation of n in the form of a list of bits, with units bit last, twos bit next to last, etc.

1. *k := n //initialize k*
2. *L := //initialize L to an empty list*
3. *While k > 0 do*
   (a) *q := k div 2 //divide k by 2*
   (b) *r:= k mod 2*
   (c) *L: = prepend r to L //Add r to the front of L*
   (d) *k:= q //reassign k*

Here is a Sage version of the algorithm with two alterations. It outputs a the binary representation as a string, and it handles all integers, not just positive ones.

```
def binary_rep(n):
    if n==0:
        return '0'
    else:
        k=abs(n)
        s=''
        while k>0:
            s=str(k%2)+s
            k=k//2
        if n < 0:
            s='-'+s
        return s

binary_rep(41)
```

```
'101001'
```

Now that you've read this section, you should get this joke.

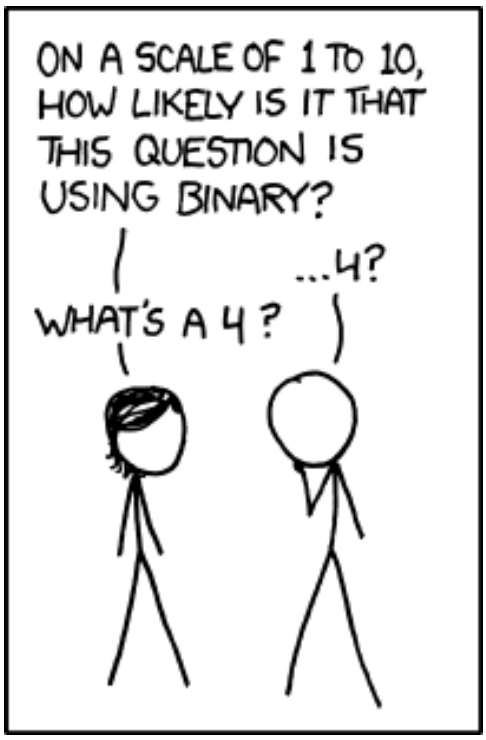


Figure 1.4.3: With permission from Randall Munroe

1.4.1 EXERCISES

A Exercises

1. Find the binary representation of each of the following positive integers by working through the algorithm by hand. You can check your answer using the sage cell above.

(a) 31
(b) 32
(c) 10
(d) 100

Answer.

(a) 11111
(b) 100000
(c) 1010
(d) 1100100

2. Find the binary representation of each of the following positive integers by working through the algorithm by hand. You can check your answer using the sage cell above.

(a) 64
(b) 67
(c) 28
(d) 256

3. What positive integers have the following binary representations?

(a) 10010
(b) 10011
(c) 101010
(d) 10011110000

Answer.

(a) 18
(b) 19
(c) 42
(d) 1264

4. What positive integers have the following binary representations?

(a) 100001
(b) 1001001
(c) 1000000000
(d) 1001110000

5. The number of bits in the binary representations of integers increase by one as the numbers double. Using this fact, determine how many bits the binary representations of the following decimal numbers have without actually doing the full conversion. $(a)2017$ $(b)4000$ $(c)4500$ $(d)2^{50}$

Answer. There is a bit for each power of 2 up to the largest one needed to represent an integer, and you start counting with the zeroth power. For example, 2017 is between $2^{10} = 1024$ and $2^{11} = 2048$, and so the largest power needed is 2^{10}. Therefore there are 11 bits in binary 2017

(a) 11
(b) 12
(c) 13
(d) 51

B Exercises

6. Let m be a positive integer with n-bit binary representation: $a_{n-1}a_{n-2}\cdots a_1a_0$ with $a_{n-1} = 1$ What are the smallest and largest values that m could have?

7. If a positive integer is a multiple of 100, we can identify this fact from its decimal representation, since it will end with two zeros. What can you say about a positive integer if its binary representation ends with two zeros? What if i ends in k zeros?

Answer. A number must be a multiple of four if its binary representation ends in two zeros. If it ends in k zeros, it must be a multiple of 2^k.

8. Can a multiple of ten be easily identified from its binary representation?

1.5 Summation Notation and Generalizations

Most operations such as addition of numbers are introduced as binary operations. That is, we are taught that two numbers may be added together to give us a single number. Before long, we run into situations where more than two numbers are to be added. For example, if four numbers, a_1, a_2, a_3, and a_4 are to be added, their sum may be written down in several ways, such as $((a_1 + a_2) + a_3) + a_4$ or $(a_1 + a_2) + (a_3 + a_4)$. In the first expression, the first two numbers are added, the result is added to the third number, and that result is added to the fourth number. In the second expression the first two numbers and the last two numbers are added and the results of these additions are added. Of course, we know that the final

results will be the same. This is due to the fact that addition of numbers is an associative operation. For such operations, there is no need to describe how more than two objects will be operated on. A sum of numbers such as $a_1 + a_2 + a_3 + a_4$is called a series and is often written $\sum_{k=1}^{4} a_k$ in what is called *summation notation.*

We first recall some basic facts about series that you probably have seen before. A more formal treatment of sequences and series is covered in Chapter 8. The purpose here is to give the reader a working knowledge of summation notation and to carry this notation through to intersection and union of sets and other mathematical operations.

A *finite series* is an expression such as $a_1 + a_2 + a_3 + \cdots + a_n = \sum_{k=1}^{n} a_k$
In the expression $\sum_{k=1}^{n} a_k$:

- The variable k is referred to as the *index*, or the index of summation.
- The expression a_k is the *general term* of the series. It defines the numbers that are being added together in the series.
- The value of k below the summation symbol is the *initial index* and the value above the summation symbol is the *terminal index.*
- It is understood that the series is a sum of the general terms where the index start with the initial index and increases by one up to and including the terminal index.

Example 1.5.1 (Some finite series)**.** (a) $\sum_{i=1}^{4} a_i = a_1 + a_2 + a_3 + a_4$
(b) $\sum_{k=0}^{5} b_k = b_0 + b_1 + b_2 + b_3 + b_4 + b_5$
(c) $\sum_{i=-2}^{2} c_i = c_{-2} + c_{-1} + c_0 + c_1 + c_2$

Example 1.5.2 (More finite series)**.** If the general terms in a series are more specific, the sum can often be simplified. For example,

1. $\sum_{i=1}^{4} i^2 = 1^2 + 2^2 + 3^2 + 4^2 = 30$
2. $$\begin{aligned}\sum_{i=1}^{5}(2i-1) &= (2\ 1-1) + (2\ 2-1) + (2\ 3-1) + (2\ 4-1) + (2\ 5-1)\\ &= 1+3+5+7+9\\ &= 25/endsplit\end{aligned}$$

Summation notation can be generalized to many mathematical operations, for example, $A_1 \cap A_2 \cap A_3 \cap A_4 = \bigcap_{i=1}^{4} A_i$

Definition 1.5.3 (Generalized Set Operations)**.** Let $A_1, A_2, \ldots, A_n$ be sets. Then:

1. $A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$
2. $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$
3. $A_1 \times A_2 \times \cdots \times A_n = \bigtimes_{i=1}^{n} A_i$
4. $A_1 \oplus A_2 \oplus \cdots \oplus A_n = \bigoplus_{i=1}^{n} A_i$

Example 1.5.4 (Some generalized operations)**.** If $A_1 = \{0, 2, 3\}$, $A_2 = \{1, 2, 3, 6\}$, and $A_3 = \{-1, 0, 3, 9\}$, then

$$\bigcap_{i=1}^{4} A_i = A_1 \cap A_2 \cap A_3 = \{3\}$$

and

$$\bigcup_{i=1}^{4} A_i = A_1 \cup A_2 \cup A_3 = \{-1, 0, 1, 2, 3, 6, 9\}$$

With this notation it is quite easy to write lengthy expressions in a fairly compact form. For example, the statement

$$A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$$

becomes

$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) = \bigcup_{i=1}^{n} (A \cap B_n)$$

1.5.1 Exercises

1. Calculate the following series:

(a) $\sum_{i=1}^{3}(2 + 3i)$

(b) $\sum_{i=-2}^{1} i^2$

(c) $\sum_{j=0}^{n} 2^j$ for $n = 1, 2, 3, 4$

(d) $\sum_{k=1}^{n}(2k - 1)$ for $n = 1, 2, 3, 4$

Answer.

(a) 24

(b) 6

(c) $3, 7, 15, 31$

(d) $1, 4, 9, 16$

2. Calculate the following series:

(a) $\sum_{k=1}^{3} i^n$ for$n = 1, 2, 3, 4$

(b) $\sum_{i=1}^{5} 20$

(c) $\sum_{j=0}^{3} \left(n^j + 1\right)$ for $n = 1, 2, 3, 4$

(d) $\sum_{k=-n}^{n} k$ for $n = 1, 2, 3, 4$

3.

(a) Express the formula $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ without using summation notation.

(b) Verify this formula for $n = 3$.

(c) Repeat parts (a) and (b) for $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$

Answer.

(a) $\frac{1}{1(1+1)} + \frac{1}{2(2+1)} + \frac{1}{3(3+1)} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$

(b) $\frac{1}{1(2)} + \frac{1}{2(3)} + \frac{1}{3(4)} = \frac{1}{2} + \frac{1}{6} + \frac{1}{12} = \frac{3}{4} = \frac{3}{3+1}$

(c) $1+2^3+3^3+\cdots+n^3 = \left(\frac{1}{4}\right) n^2(n+1)^2 \quad 1+4+27 = 36 = \left(\frac{1}{4}\right)(3)^2(3+1)^2$

4. Verify the following properties for $n = 3$.

(a) $\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$

(b) $c\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} ca_i$

5. Rewrite the following without summation sign for $n = 3$. It is not necessary that you understand or expand the notation $\begin{pmatrix} n \\ k \end{pmatrix}$ at this point. $(x+y)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} x^{n-k}y^k$

Answer. $(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1}y + \binom{n}{2} x^{n-2}y^2 + \cdots + \binom{n}{n-1} xy^{n-1} + \binom{n}{n} y^n$

6.

(a) Draw the Venn diagram for $\bigcap_{i=1}^{3} A_i$.

(b) Express in "expanded format": $A \cup (\bigcap_{i=1}^{n} B_i) = \bigcap_{i=1}^{n} (A \cup B_n)$.

7. For any positive integer k, let $A_k = \{x \in \mathbb{Q} : k - 1 < x <= k\}$ and $B_k = \{x \in \mathbb{Q} : -k < x < k\}$. What are the following sets?

(a) $\bigcup_{i=1}^{5} A_i$

(b) $\bigcup_{i=1}^{5} B_i$

(c) $\bigcap_{i=1}^{5} A_i$

(d) $\bigcap_{i=1}^{5} B_i$

Answer.

(a) $\{x \in \mathbb{Q} \mid 0 < x \leq 5\}$

(b) $\{x \in \mathbb{Q} \mid -5 < x < 5\} = B_5$

(c) $\emptyset$

(d) $\{x \in \mathbb{Q} \mid -1 < x < 1\} = B_1$

8. For any positive integer k, let $A = \{x \in \mathbb{Q} : 0 < x < 1/k\}$ and $B_k = \{x \in \mathbb{Q} : 0 < x < k\}$. What are the following sets?

(a) $\bigcup_{i=1}^{\infty} A_i$

(b) $\bigcup_{i=1}^{\infty} B_i$

(c) $\bigcap_{i=1}^{\infty} A_i$

(d) $\bigcap_{i=1}^{\infty} B_i$

9. The symbol Π is used for the product of numbers in the same way that Σ is used for sums. For example, $\prod_{i=1}^{5} x_i = x_1x_2x_3x_4x_5$ Evaluate the following:

(a) $\prod_{i=1}^{3} i^2$

(b) $\prod_{i=1}^{3} (2i+1)$

Answer.

(a) 36

(b) 105

10. Evaluate

(a) $\prod_{k=0}^{3} 2^k$

(b) $\prod_{k=1}^{100} \frac{k}{k+1}$

Chapter 2

Combinatorics

Throughout this book we will be counting things. In this chapter we will outline some of the tools that will help us count.

Counting occurs not only in highly sophisticated applications of mathematics to engineering and computer science but also in many basic applications. Like many other powerful and useful tools in mathematics, the concepts are simple; we only have to recognize when and how they can be applied.

2.1 Basic Counting Techniques - The Rule of Products

2.1.1

One of the first concepts our parents taught us was the "art of counting." We were taught to raise three fingers to indicate that we were three years old. The question of "how many" is a natural and frequently asked question. Combinatorics is the "art of counting." It is the study of techniques that will help us to count the number of objects in a set quickly. Highly sophisticated results can be obtained with this simple concept. The following examples will illustrate that many questions concerned with counting involve the same process.

Example 2.1.1 (How many lunches can you have?)**.** A snack bar serves five different sandwiches and three different beverages. How many different lunches can a person order? One way of determining the number of possible lunches is by listing or enumerating all the possibilities. One systematic way of doing this is by means of a tree, as in the following figure.

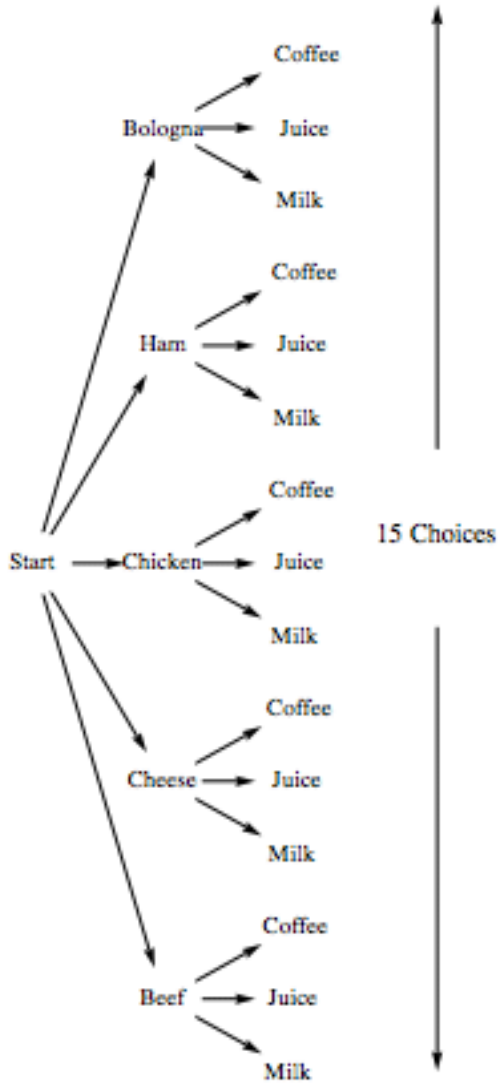


Figure 2.1.2: Tree diagram to enumerate the number of possible lunches.

Every path that begins at the position labeled START and goes to the right can be interpreted as a choice of one of the five sandwiches followed by a choice of one of the three beverages. Note that considerable work is required to arrive at the number fifteen this way; but we also get more than just a number. The result is a complete list of all possible lunches. If we need to answer a question that starts with "How many . . . ," enumeration would be done only as a last resort. In a later chapter we will examine more enumeration techniques.

An alternative method of solution for this example is to make the simple observation that there are five different choices for sandwiches and three different choices

for beverages, so there are $5 \cdot 3 = 15$ different lunches that can be ordered.

A listing of possible lunches a person could have is: (BEEF, milk), (BEEF, juice), (BEEF, coffee), ..., (BOLOGNA, coffee).

Example 2.1.3 (Counting elements in a cartesion product)**.** Let $A = \{a, b, c, d, e\}$ and $B = \{1, 2, 3\}$. From Chapter 1 we know how to list the elements in $A \times B = \{(a, 1), (a, 2), (a, 3), ..., (e, 3)\}$. Since the first entry of each pair can be any one of the five elements a, b, c, d, and e, and since the second can be any one of the three numbers 1, 2, and 3, it is quite clear there are $5 \cdot 3 = 15$ different elements in $A \times B$.

Example 2.1.4 (A True-False Questionnaire)**.** A person is to complete a true-false questionnaire consisting of ten questions. How many different ways are there to answer the questionnaire? Since each question can be answered either of two ways (true or false), and there are a total of ten questions, there are

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10} = 1024$$

different ways of answering the questionnaire. The reader is encouraged to visualize the tree diagram of this example, but not to draw it!

We formalize the procedures developed in the previous examples with the following rule and its extension.

2.1.2 The Rule Of Products:

If two operations must be performed, and If the first operation can always be performed p_1 different ways and the second operation can always be performed p_2 different ways, then there are $p_1 p_2$ different ways that the two operations can be performed.

Note: It is important that p_2 does not depend on the option that is chosen in the first operation. Another way of saying this is that p_2 is independent of the first operation. If p_2 is dependent on the first operation, then the rule of products does not apply.

Example 2.1.5 (Reduced Lunch Possibilities)**.** Assume in 2.1.1, coffee is not served with a beef or chicken sandwiches. Then by inspection of 2.1.2 we see that there are only thirteen different choices for lunch. The rule of products does not apply, since the choice of beverage depends on one's choice of a sandwich.

Extended Rule Of Products. The rule of products can be extended to include sequences of more than two operations. If n operations must be performed, and the number of options for each operation is $p_1, p_2, \ldots, p_n$ respectively, with each p_i independent of previous choices, then the n operations can be performed $p_1 \cdot p_2 \cdots \cdot p_n$ different ways.

Example 2.1.6 (A Multiple Choice Questionnaire)**.** A questionnaire contains four questions that have two possible answers and three questions with five possible answers. Since the answer to each question is independent of the answers to the other questions, the extended rule of products applies and there are $2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^4 \cdot 5^3 = 2000$ different ways to answer the questionnaire.

In Chapter 1 we introduced the power set of a set A, P(A), which is the set of all subsets of A. Can we predict how many elements are in $\mathcal{P}(A)$ for a given finite set A? The answer is yes, and in fact if $|A| = n$, then $\mathcal{P}(A) = 2^n$. The ease with which we can prove this fact demonstrates the power and usefulness of the rule of products. Do not underestimate the usefulness of simple ideas.

Theorem 2.1.7 (Power Set Cardinality Theorem)**.** *If A is a finite set, then $|\mathcal{P}(A)| = 2^{|A|}$*

Proof. $B \in \mathcal{P}(A)|A| = nx \in Ax \in Bx \notin BnA$

$$\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{n \text{ factors}} = 2^n$$

$A\mathcal{P}(A) = 2^n$ □

2.1.3 Exercises

1. In horse racing, to bet the "daily double" is to select the winners of the first two races of the day. You win only if both selections are correct. In terms of the number of horses that are entered in the first two races, how many different daily double bets could be made?

Answer. If there are m horses in race 1 and n horses in race 2 then there are $m \cdot n$ possible daily doubles.

2. Professor Shortcut records his grades using only his students' first and last initials. What is the smallest class size that will definitely force Prof. S. to use a different system?

3. A certain shirt comes in four sizes and six colors. One also has the choice of a dragon, an alligator, or no emblem on the pocket. How many different shirts could you order?

Answer. $72 = 4 \cdot 6 \cdot 3$

4. A builder of modular homes would like to impress his potential customers with the variety of styles of his houses. For each house there are blueprints for three different living rooms, four different bedroom configurations, and two different garage styles. In addition, the outside can be finished in cedar shingles or brick. How many different houses can be designed from these plans?

5. The Pi Mu Epsilon mathematics honorary society of Outstanding University wishes to have a picture taken of its six officers. There will be two rows of three people. How many different way can the six officers be arranged?

Answer. $720 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

6. An automobile dealer has several options available for each of three different packages of a particular model car: a choice of two styles of seats in three different colors, a choice of four different radios, and five different exteriors. How many choices of automobile does a customer have?

7. A clothing manufacturer has put out a mix-and-match collection consisting of two blouses, two pairs of pants, a skirt, and a blazer. How many outfits can you make? Did you consider that the blazer is optional? How many outfits can you make if the manufacturer adds a sweater to the collection?

Answer. If we always include the blazer in the outfit we would have 6 outfits. If we consider the blazer optional then there would be 12 outfits. When we add a sweater we have the same type of choice. Considering the sweater optional produces 24 outfits.

8. As a freshman, suppose you had to take two of four lab science courses, one of two literature courses, two of three math courses, and one of seven physical education courses. Disregarding possible time conflicts, how many different schedules do you have to choose from?

9. (a) Suppose each single character stored in a computer uses eight bits. Then each character is represented by a different sequence of eight 0's and l's called

a bit pattern. How many different bit patterns are there? (That is, how many different characters could be represented?) (b) How many bit patterns are palindromes (the same backwards as forwards)?
(c) How many different bit patterns have an even number of 1's?

Answer.

(a) $2^8 = 256$

(b) $2^4 = 16$. Here we are concerned only with the first four bits, since the last four must be the same.

(c) $2^7 = 128$, you have no choice in the last bit.

10. Automobile license plates in Massachusetts usually consist of three digits followed by three letters. The first digit is never zero. How many different plates of this type could be made?

11. (a) Let $A = \{1, 2, 3, 4\}$. Determine the number of different subsets of A.
(b) Let $A = \{1, 2, 3, 4, 5\}$. Determine the number of proper subsets of A .

Answer.

(a) 16 (b) 30

12. How many integers from 100 to 999 can be written with no 7's?

13. Consider three persons, A, B, and C, who are to be seated in a row of three chairs. Suppose A and B are identical twins. How many seating arrangements of these persons can there be

(a) (a) If you are a total stranger? (b) (b) If you are A and B's mother?

This problem is designed to show you that different people can have different correct answers to the same problem.

Answer.

(a) 3 (b) 6

14. How many ways can a student do a ten-question true-false exam if he or she can choose not to answer any number of questions?

15. Suppose you have a choice of fish, lamb, or beef for a main course, a choice of peas or carrots for a vegetable, and a choice of pie, cake, or ice cream for dessert. If you must order one item from each category, how many different dinners are possible?

Answer. 18

16. Suppose you have a choice of vanilla, chocolate, or strawberry for ice cream, a choice of peanuts or walnuts for chopped nuts, and a choice of hot fudge or marshmallow for topping. If you must order one item from each category, how many different sundaes are possible?

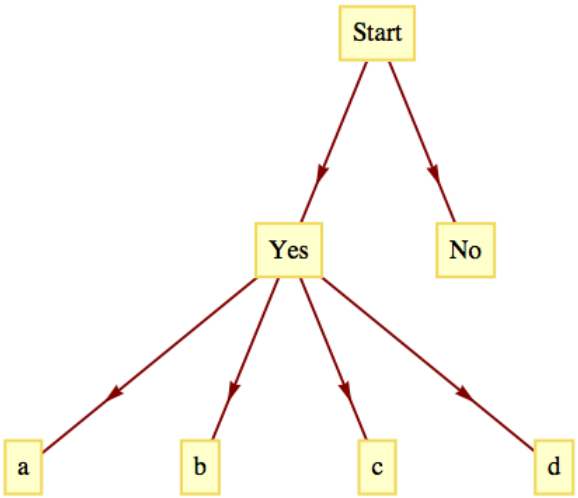
17. A questionnaire contains six questions each having yes-no answers. For each yes response, there is a follow-up question with four possible responses.

(a) Draw a tree diagram that illustrates how many ways a single question in the questionnaire can be answered.

(b) How many ways can the questionnaire be answered?

Answer.

(a)



(b) 5^6

18. Ten people are invited to a dinner party. How many ways are there of seating them at a round table? If the ten people consist of five men and five women, how many ways are there of seating them if each man must be surrounded by two women around the table?

19. How many ways can you separate a set with n elements into two nonempty subsets if the order of the subsets is immaterial? What if the order of the subsets is important?

Answer. $2^{n-1} - 1$ and $2^n - 2$

20. A gardener has three flowering shrubs and four nonflowering shrubs. He must plant these shrubs in a row using an alternating pattern, that is, a shrub must be of a different type from that on either side. How many ways can he plant these shrubs? If he has to plant these shrubs in a circle using the same pattern, how many ways can he plant this circle? Note that one nonflowering shrub will be left out at the end.

2.2 Permutations

A number of applications of the rule of products are of a specific type, and because of their frequent appearance they are given their own designation, permutations. Consider the following examples.

Example 2.2.1 (Ordering the elements of a set)**.** How many different ways can we order the three different elements of the set $A = \{a, b, c\}$? Since we have three choices for position one, two choices for position two, and one choice for the third position, we have, by the rule of products, $3 \cdot 2 \cdot 1 = 6$ different ways of ordering the three letters. We illustrate through a tree diagram.

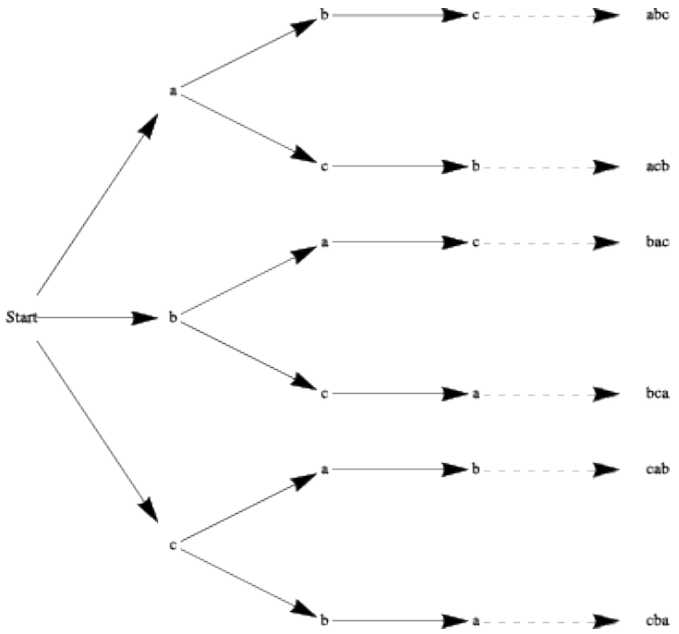


Figure 2.2.2: A tree to enumerate permutations of a three element set.

Each of the six orderings is called a permutation of the set A.

Example 2.2.3 (Ordering a schedule)**.** A student is taking five courses in the fall semester. How many different ways can the five courses be listed? There are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$ different permutations of the set of courses.

In each of the above examples of the rule of products we observe that:

1. We are asked to order or arrange elements from a single set.
2. Each element is listed exactly once in each list (permutation). So if there are n choices for position one in a list, there are $n - 1$ choices for position two, $n - 2$ choices for position three, etc.

Example 2.2.4 (Some orderings of a baseball team)**.** The alphabetical ordering of the players of a baseball team is one permutation of the set of players. Other orderings of the players' names might be done by batting average, age, or height. The information that determines the ordering is called the key. We would expect that each key would give a different permutation of the names. If there are twenty-five players on the team, there are $25 \cdot 24 \cdot 23 \cdot \cdots \cdot 3 \cdot 2 \cdot 1$ different permutations of the players.

This number of permutations is huge. In fact it is 15511210043330985984000000, but writing it like this isn't all that instructive, while leaving it as a product as we originally had makes it easier to see where the number comes from. We just need to find a more compact way of writing these products.

We now develop notation that will be useful for permutation problems.

Definition 2.2.5 (Factorial)**.** If n is a positive integer then n factorial is the product of the first n positive integers and is denoted $n!$. Additionally, we define zero factorial, 0! to be 1.

The first few factorials are

0	1	2	3	4	5	6	7
1	1	2	6	24	120	720	5040

Note that 4! is 4 times 3!, or 24, and 5! is 5 times 4!, or 120. In addition, note that as n grows in size, $n!$ grows extremely quickly. For example, $11! = 39916800$. If the answer to a problem happens to be 25!, as in the previous example, you would never be expected to write that number out completely. However, a problem with an answer of $\frac{25!}{23!}$ can be reduced to $25 \cdot 24$, or 600.

If $|A| = n$, there are $n!$ ways of permuting all n elements of A . We next consider the more general situation where we would like to permute k elements out of a set of n objects, where $k \leq n$.

Example 2.2.6 (Choosing Club Officers)**.** A club of twenty-five members will hold an election for president, secretary, and treasurer in that order. Assume a person can hold only one position. How many ways are there of choosing these three officers? By the rule of products there are $25 \cdot 24 \cdot 23$ ways of making a selection.

Definition 2.2.7 (Permutation)**.** An ordered arrangement of k elements selected from a set of n elements, $0 \leq k \leq n$, where no two elements of the arrangement are the same, is called a permutation of n objects taken k at a time. The total number of such permutations is denoted by $P(n, k)$.

Theorem 2.2.8 (Permutation Counting Formula)**.** *The number of possible permutations of k elements taken from a set of n elements is*

$$P(n,k) = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1) = \prod_{j=0}^{k-1} (n-j) = \frac{n!}{(n-k)!}$$

Proof. Case I: If $k = m$ we have $P(n, n) = n! = \frac{n!}{(n-n)!}$.

Case II: If $0 \leq k < n$,then we have k positions to fill using n elements and

1. Position 1 can be filled by any one of $n - 0 = n$ elements
2. Position 2 can be filled by any one of $n - 1$ elements
3. $\cdots$
4. Position k can be filled by any one of $n - (k - 1) = n - k + 1$ elements

Hence, by the rule of products,

$$P(n,k) = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

. □

It is important to note that the derivation of the permutation formula given above was done solely through the rule of products. This serves to reiterate our introductory remarks in this section that permutation problems are really rule-of-products problems. We close this section with several examples.

Example 2.2.9 (Another example of choosing officers)**.** A club has eight members eligible to serve as president, vice-president, and treasurer. How many ways are there of choosing these officers?

Solution 1: Using the rule of products. There are eight possible choices for the presidency, seven for the vice-presidency, and six for the office of treasurer. By the rule of products there are $8 \cdot 7 \cdot 6 = 336$ ways of choosing these officers.

Solution 2: Using the permutation formula. We want the total number of permutations of eight objects taken three at a time:

$$P(8,3) = \frac{8!}{(8-3)!} = 8 \cdot 7 \cdot 6 = 336$$

Example 2.2.10 (Course ordering, revisited)**.** To count the number of ways to order five courses, we can use the permutation formula. We want the number of permutations of five courses taken five at a time:

$$P(5,5) = \frac{5!}{(5-5)!} = 5! = 120$$

Example 2.2.11 (Ordering of digits under different conditions)**.** Consider only the digits 1, 2, 3, 4, and 5.

1. How many three-digit numbers can be formed if no repetition of digits can occur?

2. How many three-digit numbers can be formed if repetition of digits is allowed?

3. How many three-digit numbers can be formed if only non-consecutive repetition of digits are allowed?

Solutions to (a): Solution 1: Using the rule of products. We have any one of five choices for digit one, any one of four choices for digit two, and three choices for digit three. Hence, $5 \cdot 4 \cdot 3 = 60$ different three-digit numbers can be formed.

Solution 2; Using the permutation formula. We want the total number of permutations of five digits taken three at a time:

$$P(5,3) = \frac{5!}{(5-3)!} = 5 \cdot 4 \cdot 3 = 60$$

Solution to (b): The definition of permutation indicates " ...no two elements in each list are the same." Hence the permutation formula cannot be used. However, the rule of products still applies. We have any one of five choices for the first digit, five choices for the second, and five for the third. So there are $5 \cdot 5 \cdot 5 = 125$ possible different three-digit numbers if repetition is allowed.

Solution to (c): Again, the rule of products applies here. We have any one of five choices for the first digit, but then for the next two digits we have four choices since we are not allowed to repeat the previous digit So there are $5 \cdot 4 \cdot 4 = 80$ possible different three-digit numbers if only non-consecutive repetitions are allowed.

2.2.1 Exercises

1. If a raffle has three different prizes and there are 1,000 raffle tickets sold, how many different ways can the prizes be distributed?

Answer. $P(1000, 3)$

2.

(a) How many three-digit numbers can be formed from the digits 1, 2, 3 if no repetition of digits is allowed? List the three-digit numbers.

(b) How many two-digit numbers can be formed if no repetition of digits is allowed? List them.

(c) How many two-digit numbers can be obtained if repetition is allowed?

3. How many eight-letter words can be formed from the 26 letters in the alphabet? Even without concerning ourselves about whether the words make sense, there are two interpretations of this problem. Answer both.

Answer. With repetition: $26^8 \approx 2.0883 \times 10^{11}$
Without repetition: $P(26, 8) \approx 6.2991\ 10^{10}$

4. Let A be a set with $|A| = n$. Determine

(a) $|A^3|$

(b) $|\{(a, b, c) \mid \text{ each coordinate is different}\}|$

5. The state finals of a high school track meet involves fifteen schools. How many ways can these schools be listed in the program?

Answer. 15!

6. Consider the three-digit numbers that can be formed from the digits 1, 2, 3, 4, and 5 with no repetition of digits allowed.
a. How many of these are even numbers?
b. How many are greater than 250?

7. a. How many ways can the coach at Tall U. fill the five starting positions on a basketball team if each of his 15 players can play any position?
b. What is the answer if the center must be one of two players?

Answer.

(a) $P(15, 5) = 360360$

(b) $2 \cdot 14 \cdot 13 \cdot 12 \cdot 11 = 48048$

8.

(a) How many ways can a gardener plant five different species of shrubs in a circle?

(b) What is the answer if two of the shrubs are the same?

(c) What is the answer if all the shrubs are identical?

9. The president of the Math and Computer Club would like to arrange a meeting with six attendees, the president included. There will be three computer science majors and three math majors at the meeting. How many ways can the six people be seated at a circular table if the president does not want people with the same majors to sit next to one other?

Answer. $2 \cdot P(3, 3) = 12$

10. Six people apply for three identical jobs and all are qualified for the positions. Two will work in New York and the other one will work in San Diego. How many ways can the positions be filled?

11. Let $A = \{1, 2, 3, 4\}$. Determine the cardinality of

(a) $\{(a_1, a_2) \mid a_1 \neq a_2\}$

(b) What is the answer to the previous part if $|A| = n$

(c) If $|A| = n$, determine the number of m-tuples in A, $m \leq n$, where each coordinate is different from the other coordinates.

Answer.

(a) $P(4, 2) = 12$

(b) $P(n; 2) = n(n - 1)$

(c) Case 1: $m > n$. Since the coordinates must be different, this case is impossible.
Case 2: $m \leqslant n.P(n; m)$.

2.3 Partitions of Sets and the Law of Addition

One way of counting the number of students in your class would be to count the number in each row and to add these totals. Of course this problem is simple because there are no duplications, no person is sitting in two different rows. The basic counting technique that you used involves an extremely important first step, namely that of partitioning a set. The concept of a partition must be clearly understood before we proceed further.

Definition 2.3.1 (Partition.)**.** A partition of set A is a set of one or more nonempty subsets of A: $A_1, A_2, A_3, \cdots$, such that every element of A is in exactly one set. Symbolically,

1. $A_1 \cup A_2 \cup A_3 \cup \cdots = A$
2. If $i \neq j$ then $A_i \cap A_j = \emptyset$

The subsets in a partition are often referred to as blocks. Note how our definition allows us to partition infinite sets, and to partition a set into an infinite number of subsets. Of course, if A is finite the number of subsets can be no larger than $|A|$.

Example 2.3.2 (Some partitions of a four element set)**.** Let $A = \{a, b, c, d\}$. Examples of partitions of A are:

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

How many others are there, do you suppose?

There are 15 different partitions. The most efficient way to count them all is to classify them by the size of blocks. For example, the partition $\{\{a\}, \{b\}, \{c, d\}\}$ has block sizes 1, 1, and 2.

Example 2.3.3 (Some Integer Partitions)**.** Two examples of partitions of set of integers $\mathbb{Z}$ are

- $\{\{n\} \mid n \in \mathbb{Z}\}$ and
- $\{\{n \in \mathbb{Z} \mid n < 0\}, \{0\}, \{n \in \mathbb{Z} \mid 0 < 0\}\}$.

The set of subsets $\{\{n \in \mathbb{Z} \mid n \geq 0\}, \{n \in \mathbb{Z} \mid n \leq 0\}\}$ is not a partition because the two subsets have a nonempty intersection. A second example of a non-partition is $\{\{n \in \mathbb{Z} \mid |n| = k\} \mid k = -1, 0, 1, 2, \cdots\}$ because one of the blocks, when $k = -1$ is empty.

One could also think of the concept of partitioning a set as a "packaging problem." How can one "package" a carton of, say, twenty-four cans? We could use: four six-packs, three eight-packs, two twelve-packs, etc. In all cases: (a) the sum of all cans in all packs must be twenty-four, and (b) a can must be in one and only one pack.

2.3.1 The Basic Law Of Addition:

If A is a finite set, and if $\{A_1, A_2, \ldots, A_n\}$ is a partition of A , then

$$|A| = |A_1| + |A_2| + \cdots + |A_n| = \sum_{k=1}^{n} |A_k|$$

The basic law of addition can be rephrased as follows: If A is a finite set where $A_1 \cup A_2 \cup \cdots \cup A_n = A$ and where $A_i \cap A_j$ whenever $i \neq j$, then

$$|A| = |A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$$

Example 2.3.4 (Counting All Students)**.** The number of students in a class could be determined by adding the numbers of students who are freshmen, sophomores, juniors, and seniors, and those who belong to none of these categories. However, you probably couldn't add the students by major, since some students may have double majors.

Example 2.3.5 (Counting Students in Disjoint Classes)**.** The sophomore computer science majors were told they must take one and only one of the following courses, Cryptography, Data Structures, or Javascript, in a given semester. The numbers in each course, respectively, for sophomore CS majors, were 75, 60, 55. How many sophomore C.S. majors are there? The Law of Addition applies here. There are exactly $75 + 60 + 55 = 190$ CS majors since the rosters of the three courses listed above would be a partition of the CS majors.

Example 2.3.6 (Counting Students in Non-disjoint Classes)**.** It was determined that all junior computer science majors take at least one of the following courses: Algorithms, Logic Design, and Compiler Construction. Assume the number in each course was was 75, 60 and 55, respectively for the three courses listed. Further investigation indicated ten juniors took all three courses, twenty-five took Algorithms and Logic Design, twelve took Algorithms and Compiler Construction, and fifteen took Logic Design and Compiler Construction. How many junior C.S. majors are there?

2.3.5 was a simple application of the law of addition, however in this example some students are taking two or more courses, so a simple application of the law of addition would lead to double or triple counting. We rephrase information in the language of sets to describe the situation more explicitly.

A = the set of all junior computer science majors

A_1 = the set of all junior computer science majors who took Algorithms

A_2 = the set of all junior computer science majors who took Logic Design

A_3 = the set of all junior computer science majors who took Compiler Construction

Since all sophomore CS majors must take at least one of the courses, the number we want is:

$$|A| = |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - \text{repeats.}$$

A Venn diagram is helpful to visualize the problem. In this case the universal set U can stand for all students in the university.

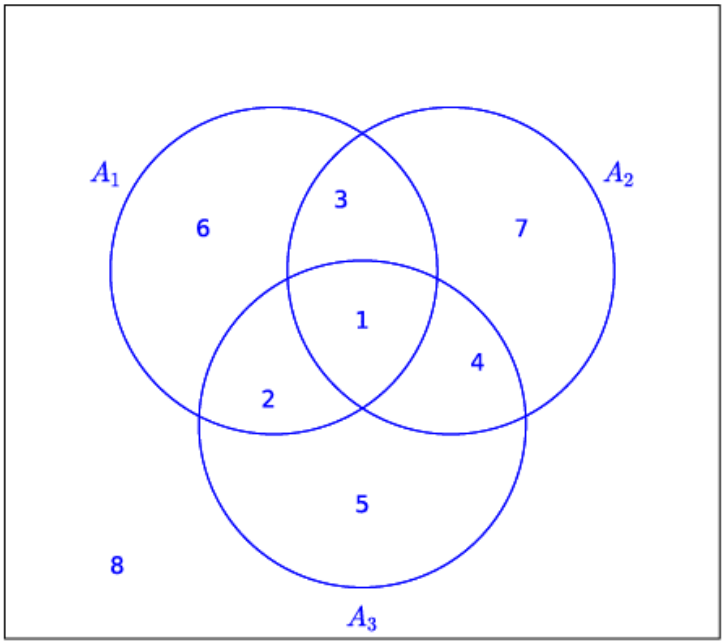


Figure 2.3.7: Venn Diagram

We see that the whole universal set is naturally partitioned into subsets that are labeled by the numbers 1 through 8, and the set A is partitioned into subsets labeled 1 through 7. The region labeled 8 represents all students who are not junior CS majors. Note also that students in the subsets labeled 2, 3, and 4 are double counted, and those in the subset labeled 1 are triple counted. To adjust, we must subtract the numbers in regions 2, 3 and 4. This can be done by subtracting the numbers in the intersections of each pair of sets. However, the individuals in region 1 will have been removed three times, just as they had been originally added three times. Therefore, we must finally add their number back in.

$$\begin{aligned}
|A| &= |A_1 \cup A_2 \cup A_3| \\
&= |A_1| + |A_2| + |A_3| - \text{repeats} \\
&= |A_1| + |A_2| + |A_3| - \text{duplicates} + \text{triplicates} \\
&= |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3| \\
&= 75 + 60 + 55 - 25 - 12 - 15 + 10 = 148
\end{aligned}$$

The ideas used in this latest example gives rise to a basic counting technique:

2.3.2 Laws of Inclusion-Exclusion

Given finite sets A_1, A_2, A_3, then

1. $$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

2. $$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + |A_1 \cap A_2 \cap A_3|$$

The inclusion-exclusion laws extend to more than three sets, as will be explored in the exercises.

In this section we saw that being able to partition a set into disjoint subsets gives rise to a handy counting technique. Given a set, there are many ways to partition depending on what one would wish to accomplish. One natural partitioning of sets is apparent when one draws a Venn diagram. This particular partitioning of a set will be discussed further in Chapters 4 and 13.

2.3.3 Exercises for Section 2.3

1. List all partitions of the set $A = \{a, b, c\}$.

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

2. Which of the following collections of subsets of the plane, $\mathbb{R}^2$, are partitions?

(a) $\{\{(x,y) \mid x+y=c\} \mid c \in \mathbb{R}\}$

(b) The set of all circles in $\mathbb{R}^2$

(c) The set of all circles in $\mathbb{R}^2$ centered at the origin together with the set $\{(0,0)\}$

(d) $\{\{(x,y)\} \mid (x,y) \in \mathbb{R}^2\}$

3. A student, on an exam paper, defined the term partition the following way: "Let A be a set. A partition of A is any set of nonempty subsets $A_1, A_2, A_3, \ldots$ of A such that each element of A is in one of the subsets." Is this definition correct? Why?

Answer. No. By this definition it is possible that an element of A might belong to two of the subsets.

4. Let A_1 and A_2 be subsets of a set U. Draw a Venn diagram of this situation and shade in the subsets $A_1 \cap A_2$, $A_1^c \cap A_2$,$A_1 \cap A_2^c$,and $A_1^c \cap A_2^c$. Use the resulting diagram and the definition of partition to convince yourself that the subset of these four subsets that are nonempty form a partition of U.

5. Show that $\{\{2n \mid n \in \mathbb{Z}\},\{2n+1 \mid n \in \mathbb{Z}\}\}$ is a partition of $\mathbb{Z}$. Describe this partition using only words.

Answer. The first subset is all the even integers and the second is all the odd integers. These two sets do not intersect and they cover the integers completely.

6. (a) A group of 30 students were surveyed and it was found that 18 of them took Calculus and 12 took Physics. If all students took at least one course, how many took both Calculus and Physics? Illustrate using a Venn diagram. (b) What is the answer to the question in part (a) if five students did not take either of the two courses? Illustrate using a Venn diagram.

7. A survey of 90 people, 47 of them played tennis and 42 of them swam. If 17 of the them participated in both activities, how many of them participated in neither.

Answer. Since 17 participated in both activities, 30 of the tennis players only played tennis and 25 of the swimmers only swam. Therefore, $17+30+25 = 72$ of those who were surveyed participated in an activity and so 18 did not.

8. A survey of 300 people found that 60 owned an iPhone 75 owned an Blackberry, and 30 owned an Android phone. Furthermore, 40 owned both an iPhone and Blackberry, 12 owned both an iPhone and Android phone, and 8 owned a Blackberry and an Android phone. Finally, 3 owned all three phones.

(a) How many people surveyed owned none of the three phones?

(b) How many people owned an Blackberry but not an iPhone?

(c) How many owned a Blackberry but not an Android?

9.

(a) Use the Two Set Inclusion-Exclusion Law to derive the Three Set Inclusion-Exclusion Law. Note: a knowledge of basic set laws is needed for this exercise.

(b) State and derive the Inclusion-exclusion law for four sets.

Solution. We assume that $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3| &= |(A_1 \cup A_2) \cup A_3| \quad Why? \\
&= |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| \quad Why? \\
&= |(A_1 \cup A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| \quad Why? \\
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| \\
&\quad - (|A_1 \cap A_3| + |A_2 \cap A_3| - |(A_1 \cap A_3) \cap (A_2 \cap A_3)| \quad Why? \\
&= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| \\
&\quad - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \quad Why?
\end{aligned}$$

The law for four sets is

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3 \cup A_4| = {} & |A_1| + |A_2| + |A_3| + |A_4| \\
& - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| \\
& \quad - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4| \\
& + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \\
& \quad + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\
& - |A_1 \cap A_2 \cap A_3 \cap A_4|
\end{aligned}$$

Derivation:

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3 \cup A_4| &= |(A_1 \cup A_2 \cup A_3) \cup A_4| \\
&= |(A_1 \cup A_2 \cup A_3| + |A_4| - |(A_1 \cup A_2 \cup A_3) \cap A_4| \\
&= |(A_1 \cup A_2 \cup A_3| + |A_4| \\
&\quad - |(A_1 \cap A_4) \cup (A_2 \cap A_4) \cup (A_3 \cap A_4)| \\
&= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| \\
&\quad - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| + |A_4| - |A_1 \cap A_4| \\
&\quad + |A_2 \cap A_4| + |A_3 \cap A_4| - |(A_1 \cap A_4) \cap (A_2 \cap A_4)| \\
&\quad - |(A_1 \cap A_4) \cap (A_3 \cap A_4)| - |(A_2 \cap A_4) \cap (A_3 \cap A_4)| \\
&\quad + |(A_1 \cap A_4) \cap (A_2 \cap A_4) \cap (A_3 \cap A_4)| \\
&= |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \cap A_2| - |A_1 \cap A_3| \\
&\quad - |A_2 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_4| \quad - |A_3 \cap A_4| \\
&\quad + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \\
&\quad + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\
&\quad - |A_1 \cap A_2 \cap A_3 \cap A_4|
\end{aligned}$$

10. To complete your spring schedule, you must add Calculus and Physics. At 9:30, there are three Calculus sections and two Physics sections; while at 11:30,

there are two Calculus sections and three Physics sections. How many ways can you complete your schedule if your only open periods are 9:30 and 11:30?

11. The definition of $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ given in Chapter 1 is awkward. If we use the definition to list elements in $\mathbb{Q}$, we will have duplications such as $\frac{1}{2}$, $\frac{-2}{-4}$ and $\frac{300}{600}$ Try to write a more precise definition of the rational numbers so that there is no duplication of elements.

Answer. Partition the set of fractions into blocks, where each block contains fractions that are numerically equivalent. Describe how you would determine whether two fractions belong to the same block. Redefine the rational numbers to be this partition. Each rational number is a set of fractions.

2.4 Combinations and the Binomial Theorem

2.4.1 Combinations

In Section 2.1 we investigated the most basic concept in combinatorics, namely, the rule of products. Even though in this section we investigate other counting formulas, it is of paramount importance to keep this fundamental process in mind. In Section 2.2 we saw that a subclass of rule-of-products problems appears so frequently that we gave them a special designation, namely, permutations, and we derived a formula as a computational aid to assist us. In this section we will investigate another counting formula that are used to count combinations, which are subsets of a certain size..

In many rule-of-products applications the permutation or order is important, as in the situation of the order of putting on one's socks and shoes; in some cases it is not important, as in placing coins in a vending machine or in the listing of the elements of a set. Order is important in permutations. Order is not important in combinations.

Example 2.4.1 (Counting Permutations)**.** How many different ways are there to permute three letters from the set $A = \{a, b, c, d\}$? From the Permutation Counting Formula there are $P(4, 3) = \frac{4!}{(4-3)!} = 24$ different orderings of three letters from A

Example 2.4.2 (Counting with No Order)**.** How many ways can we select a set of three letters from $A = \{a, b, c, d\}$? Note here that we are not concerned with the order of the three letters. By trial and error, abc, abd, acd, and bcd are the only listings possible. To repeat, we were looking for all three-element subsets of the set A. Order is not important in sets. The notation for choosing 3 elements from 4 is most commonly $\binom{4}{3}$ or occasionally $C(4, 3)$, either of which is read "4 choose 3" or the number of combinations for four objects taken three at a time.

Definition 2.4.3 (Binomial Coefficient)**.** Let n and k be nonnegative integers. The binomial coefficient $\binom{n}{k}$ represents the number of combinations of n objects taken k at a time, and is read "n choose k."

We would now like to investigate the relationship between permutation and combination problems in order to derive a formula for $\binom{n}{k}$

Let us reconsider the Counting with No Order. There are $3! = 6$ different orderings for each of the three-element subsets. The table below lists each subset

of A and all permutations of each subset on the same line.

subset	permutations
abc	$abc, acb, bca, bac, cab, cba$
abd	$abd, adb, bda, bad, dab, dba$
acd	$acd, adc, cda, cad, dac, dca$
bcd	$bcd, bdc, cdb, cbd, dbc, dcb$

Hence, $\binom{4}{3} = \frac{P(4,3)}{3!} = \frac{4!}{(4-3)!\cdot 3!} = 4$

We generalize this result in the following theorem:

Theorem 2.4.4 (Binomial Coefficient Formula)**.** *If n and k are nonnegative integers with $0 \leq k \leq n$, then the number k-element subsets of an n element set is equal to*

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!}$$

Proof. Proof 1: There are $k!$ ways of ordering the elements of any k element set.Therefore,

$$\binom{n}{k} = \frac{P(n,k)}{k!} = \frac{n!}{(n-k)!k!}.$$

Proof 2: To "construct" a permutation of k objects from a set of n elements, we can first choose one of the subsets of objects and second, choose one of the $k!$ permutations of those objects. By the rule of products,

$$P(n,k) = \binom{n}{k} \cdot k!$$

and solving for $\binom{n}{k}$ we get the desired formula. □

Example 2.4.5 (Flipping Coins)**.** Assume an evenly balanced coin is tossed five times. In how many ways can three heads be obtained? This is a combination problem, because the order in which the heads appear does not matter. The number of ways to get three heads is $\binom{5}{3} = \frac{5\cdot 4}{2\cdot 1} = 10$.

Example 2.4.6 (Listing Five Flips, taking order into account)**.** Determine the total number of ways a fair coin can land if tossed five consecutive times. The five tosses can produce any one of the following mutually exclusive, disjoint events: 5 heads, 4 heads, 3 heads, 2 heads, 1 head, or 0 heads. Hence by the law of addition we have:

$$\binom{5}{5} + \binom{5}{4} + \binom{5}{3} + \binom{5}{2} + \binom{5}{1} + \binom{5}{0} = 1 + 5 + 10 + 10 + 5 + 1 = 32$$

ways to observe the five flips

Of course, we could also have applied the extended rule of products, and since there are two possible outcomes for each of the five tosses, we have $2^5 = 32$ ways.

You might think that counting something two ways is a waste of time but solving a problem two different ways often is instructive and leads to valuable insights. In this case, it suggests a general formula for the sum $\sum_{k=0}^{n} \binom{n}{k}$. In the case of $n = 5$, we get 2^5 so it is reasonable to expect that the general sum is 2^n, and it is.

Example 2.4.7 (A Committee of Five)**.** A committee usually starts as an unstructured set of people selected from a larger membership. Therefore, a committee can be thought of as a combination. If a club of 25 members has a five-member social committee, there are $\binom{25}{5} = \frac{2524232221}{5!} = 53130$ different possible social committees.

If any structure or restriction is placed on the way the social committee is to be selected, the number of possible committees will probably change. For example, if the club has a rule that the treasurer must be on the social committee, then the number of possibilities is reduced to $\binom{24}{4} = \frac{24232221}{4!} = 10626$.

If we further require that a chairperson other than the treasurer be selected for the social committee, we have $\binom{24}{4} \cdot 4 = 42504$ different possible social committees. The choice of the four non-treasurers accounts for the factor $\binom{24}{4}$ while the need to choose a chairperson accounts for the 4.

Example 2.4.8 (Binomial Coefficients - Extreme Cases)**.** By simply applying the definition of a Binomial Coefficient as a number of subsets we see that there is $\binom{n}{0} = 1$ way of choosing a combination of zero elements from a set of n. In addition, we see that there is $\binom{n}{n} = 1$ way of choosing a combination of n elements from a set of n.

We could compute these values using the formula we have developed, but no arithmetic is really needed here. Other properties of binomial coefficients that can be derived using the subset definition will be seen in the exercises

2.4.2 The Binomial Theorem

The binomial theorem gives us a formula for expanding $(x + y)^n$, where n is a nonnegative integer. The coefficients of this expansion are precisely the binomial coefficients that we have used to count combinations. Using high school algebra we can expand the expression for integers from 0 to 5:

n	$(x+y)^n$
0	1
1	$x+y$
2	$x^2+2xy+y^2$
3	$x^3+3x^2y+3xy^2+y^3$
4	$x^4+4x^3y+6x^2y^2+4xy^3+y^4$
5	$x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5$

In the expansion of $(x + y)^5$ we note that the coefficient of the third term is $\binom{5}{3} = 10$, and that of the sixth term is $\binom{5}{5} = 1$. We can rewrite the expansion as

$$\binom{5}{0}x^5 + \binom{5}{1}x^4y + \binom{5}{2}x^3y^2 + \binom{5}{3}x^2y^3 + \binom{5}{4}xy^4 + \binom{5}{5}y^5$$

In summary, in the expansion of $(x + y)^n$ we note:

1. The first term is x^n and the last term is y^n.
2. With each successive term, exponents of x decrease by 1 as those of y increase by 1. For any term the sum of the exponents is n.
3. The coefficient of $x^{n-k}y^k$ is $\binom{n}{k}$.
4. The triangular array of numbers in is called Pascal's triangle after the seventeenth-century French mathematician Blaise Pascal. Note that each number in the triangle other than the 1's at the ends of each row is the sum of the two numbers to the right and left of it in the row above.

Theorem 2.4.9 (The Binomial Theorem)**.** *If $n \geq 0$, and x and y are numbers, then*

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

Proof. This theorem will proven using a logical procedure called mathematical induction, which will be introduced in Chapter 3. □

Example 2.4.10 (Identifying a term in an expansion)**.** Find the third term in the expansion of $(x-y)^4$. The third term, when $k=2$, is $\binom{4}{2}x^{4-2}y^2 = 6x^2y^2$.

Example 2.4.11 (A Binomial Expansion)**.** Expand $(3x-2)^3$. If we replace x and y in the Binomial Theorem with $3x$ and -2, respectively, we get

$$\begin{aligned}\sum_{k=0}^{3} \binom{3}{k}(3x)^{n-k}(-2)^k &= \binom{3}{0}(3x)^3(-2)^0 + \binom{3}{1}(3x)^2(-2)^1 + \binom{3}{2}(3x)^1(-2)^2 + \binom{3}{3}(3x)^0(-2)^3 \\ &= 27x^3 - 54x^2 + 36x - 8\end{aligned}$$

2.4.3 *Mathematica* Note

Mathematica has a built-in function for binomial coefficients, `Binomial`. Unlike the examples we've concentrated on that can be done without technology, you can compute extremely large values. For example, a bridge hand is a 13 element subset of a standard 52 card deck. The order in which the cards come to the player doesn't matter. From the point of view of a single player, the number of possible bridge hands is `Binomial[52,13]`, which is easily computed with *Mathematica* with an output of 635013559600

In bridge, the location of a hand in relation to the dealer has some bearing on the game. An even truer indication of the number of possible hands takes into account *each* player's possible hand. It is customary to refer to bridge positions as West, North, East and South. We can apply the rule of product to get the total number of bridge hands with the following logic. West can get any of the $\binom{52}{13}$ hands identified above. Then North get 13 of the remaining 39 cards and so has $\binom{39}{13}$ possible hands. East then gets 13 of the 26 remaining cards, which has $\binom{26}{13}$ possibilities. South gets the remaining cards. Therefore the number of bridge hands is computed by evaluating the expression

```
Binomial[52,13] Binomial[52,13] Binomial[52,13]
```

which is equal to 53644737765488792839237440000

2.4.4 Sage Note

Sage will do the same calculations for bridge hands just as easily. A correct input is provided in the sage cell below.

```
binomial(52,13)*binomial(39,13)*binomial(26,13)
```

```
53644737765488792839237440000
```

2.4.5 Exercises

1. The judiciary committee at a college is made up of three faculty members and four students. If ten faculty members and 25 students have been nominated for the committee, how many judiciary committees could be formed at this point ?

Answer. $C(10,3) \cdot C(25,4) = 1,518,000$

2. Suppose that a single character is stored in a computer using eight bits.
a. How many bit patterns have exactly three 1 's?
b. How many bit patterns have at least two 1 's?

Hint. Think of the set of positions that contain a 1 to turn this is into a question about sets.

Solution. (a) $\binom{8}{3}$ (b) $2^8 - (\binom{8}{0} + \binom{8}{1})$

3. How many subsets of $\{1, 2, 3, \ldots, 10\}$ contain at least seven elements?

Answer. $C(10,7) + C(10,8) + C(10,9) + C(10,10)$

4. The congressional committees on mathematics and computer science are made up of five congressmen each, and a congressional rule is that the two committees must be disjoint. If there are 385 members of congress, how many ways could the committees be selected?

5. Expand $(2x - 3y)^4$

Answer. $16x^4 - 96x^3y + 216x^2y^2 - 216xy^3 + 81y^4$

6. Find the fourth term of the expansion of $(x - 2y)^6$.

7. (a) A poker game is played with 52 cards. How many "hands" of five cards are possible?
(b) If there are four people playing, how many five-card "hands" are possible on the first deal?

Answer.
(a) $C(52,5) = 2,598,960$
(b) $C(52,5) \cdot C(47,5) \cdot C(42,5) \cdot C(37,5)$

8. A flush in a five-card poker hand is five cards of the same suit. How many spade flushes are possible in a 52-card deck? How many flushes are possible in any suit?

9. How many five-card poker hands using 52 cards contain exactly two aces?

Answer. $C(4,2)C(48,3)$

10. In poker, a full house is three-of-a-kind and a pair in one hand; for example, three fives and two queens. How many full houses are possible from a 52-card deck? You can use the sage cell in the Sage Note to do this calculation, but also write your answer in terms of binomial coefficients.

11. A class of twelve computer science students are to be divided into three groups of 3, 4, and 5 students to work on a project. How many ways can this be done if every student is to be in exactly one group?

Answer. $C(12,3) \cdot C(9,4) \cdot C(5,5)$

12. Explain in words why the following equalities are true based on number of subsets, and then verify the equalities using the formula for binomial coefficients.

(a) $\binom{n}{1} = n$

(b) $\binom{n}{k} = \binom{n}{n-k}$, $0 \leq k \leq n$

13. There are ten points, $P_1, P_2, \ldots, P_{10}$ on a plane, no three on the same line.

(a) How many lines are determined by the points?

(b) How many triangles are determined by the points?

Answer.

(a) $C(10, 2) = 45$

(b) $C(10, 3) = 120$

14. How many ways can n persons be grouped into pairs when n is even? Assume the order of the pairs matters, but not the order within the pairs. For example, if $n = 4$, the six different groupings would be

$$\begin{array}{ll} \{1,2\} & \{3,4\} \\ \{1,3\} & \{2,4\} \\ \{1,4\} & \{2,3\} \\ \{2,3\} & \{1,4\} \\ \{2,4\} & \{1,3\} \\ \{3,4\} & \{1,2\} \end{array}$$

15. Use the binomial theorem to prove that if A is a finite set, then $P(A) = 2^{|A|}$

Answer. Assume $|A| = n$. If we let $x = y = 1$ in the Binomial Theorem, we obtain $2^n = C(n; 0) + C(n; 1) + \cdots + C(n; n)$, with the right side of the equality counting all subsets of A containing $0, 1, 2, \ldots, n$ elements. Hence $|P(A)| = 2^{|A|}$

16.

(a) A state's lottery involves choosing six different numbers out of a possible 36. How many ways can a person choose six numbers?

(b) What is the probability of a person winning with one bet?

17. Use the binomial theorem to calculate 9998^3.

Hint. $9998 = 10000 - 2$

Answer. $1000^3 - 3 \cdot 2 \cdot 1000^2 + 3 \cdot 2^2 \cdot 1000 - 2^3 = 999,400,119,992$.

18. In the card game Blackjack, there are one or more players and a dealer. Initially, each player is dealt two cards and the dealer is dealt one card down and one facing up. As in bridge, the order of the hands, but not the order of the cards in the hands, matters. Starting with a single 52 card deck, and three players, how many ways can the first two cards be dealt out? You can use the sage cell in the Sage Note to do this calculation.

Chapter 3

Logic

In this chapter, we will introduce some of the basic concepts of mathematical logic. In order to fully understand some of the later concepts in this book, you must be able to recognize valid logical arguments. Although these arguments will usually be applied to mathematics, they employ the same techniques that are used by a lawyer in a courtroom or a physician examining a patient. An added reason for the importance of this chapter is that the circuits that make up digital computers are designed using the same algebra of propositions that we will be discussing.

3.1 Propositions and Logical Operators

3.1.1 Propositions

Definition 3.1.1 (Proposition)**.** A proposition is a sentence to which one and only one of the terms *true* or *false* can be meaningfully applied.

Example 3.1.2 (Some Propositions)**.** "Four is even,", "$4 \in \{1, 3, 5\}$" and "$43 > 21$" are propositions.

In traditional logic, a declarative statement with a definite truth value is considered a proposition. Although our ultimate aim is to discuss mathematical logic, we won't separate ourselves completely from the traditional setting. This is natural because the basic assumptions, or postulates, of mathematical logic are modeled after the logic we use in everyday life. Since compound sentences are frequently used in everyday speech, we expect that logical propositions contain connectives like the word "and." The statement "Europa supports life or Mars supports life" is a proposition and, hence, must have a definite truth value. Whatever that truth value is, it should be the same as the truth value of "Mars supports life or Europa supports life."

3.1.2 Logical Operations

There are several ways in which we commonly combine simple statements into compound ones. The words/phrases *and*, *or*, *not*, *if ... then...*, and *...if and only if ...* can be added to one or more propositions to create a new proposition. To avoid any confusion, we will precisely define each one's meaning and introduce its standard symbol. With the exception of negation (*not*), all of the operations act on pairs of propositions. Since each proposition has two possible truth values, there are four ways that truth can be assigned to two propositions. In defining the effect that a logical operation has on two propositions, the result must be specified for all

four cases. The most convenient way of doing this is with a truth table, which we will illustrate by defining the word *and*.

3.1.2.1 Conjunction

Definition 3.1.3 (Logical Conjunction)**.** If p and q are propositions, their conjunction, $p$and$q$ (denoted $p \wedge q$), is defined by the truth table

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Notes:

1. To read this truth table, you must realize that any one line represents a case: one possible set of values for p and q.

2. The numbers 0 and 1 are used to denote false and true, respectively. This is consistent with the way that many programming languages treat logical, or Boolean, variables since a single bit, 0 or 1, can represent a truth value. Although *Mathematica*'s logical expressions have a value of True or False, there is a built in function called `Boole` which converts the value to 1 or 0, if desired.

3. For each case, the symbol under p represents the truth value of p. The same is true for q. The symbol under $p \wedge q$ represents its truth value for that case. For example, the second row of the truth table represents the case in which p is false, q is true, and the resulting truth value for $p \wedge q$ is false. As in everyday speech, $p \wedge q$ is true only when both propositions are true.

4. Just as the letters x, y and$z$ are frequently used in algebra to represent numeric variables, p, q and r seem to be the most commonly used symbols for logical variables. When we say that p is a logical variable, we mean that any proposition can take the place of p.

5. One final comment: The order in which we list the cases in a truth table is standardized in this book. If the truth table involves two simple propositions, the numbers under the simple propositions can be interpreted as the two-digit binary integers in increasing order, 00, 01, 10, and 11, for 0, 1, 2, and 3, respectively.

3.1.2.2 Disjunction

Definition 3.1.4 (Logical Disjunction)**.** If p and q are propositions, their disjunction, $p$or$q$ (denoted $p \vee q$), is defined by the truth table

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

3.1.2.3 Negation

Definition 3.1.5 (Logical Negation)**.** If p is a proposition, its negation, not$p$, denoted $\neg p$, and is defined by the truth table

p	$\neg p$
0	1
1	0

Note: Negation is the only standard operator that acts on a single proposition; hence only two cases are needed.

3.1.2.4 The Conditional Operation

Consider the following propositions from everyday speech:

1. I'm going to quit if I don't get a raise.
2. If I pass the final, then I'll graduate.
3. I'll be going to the movies provided that my car starts.

All three propositions are conditional, they can all be restated to fit into the form "If *Condition*, then *Conclusion*." For example, the first statement can be rewritten as "If I don't get a raise, then I'm going to quit."

A conditional statement is meant to be interpreted as a guarantee; if the condition is true, then the conclusion is expected to be true. It says no more and no less.

Definition 3.1.6 (Conditional Statement)**.** The conditional statement "If p then q," denoted $p \to q$, is defined by the truth table

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Table 3.1.7: Truth Table for $p \to q$

Example 3.1.8 (Analysis of a Conditional Proposition)**.** Assume your instructor told you "If you receive a grade of 95 or better in the final examination, then you will receive an A in this course." Your instructor has made a promise to you. If you fulfill his condition, you expect the conclusion (getting an A) to be forthcoming. Suppose your graded final has been returned to you. Has your instructor told the truth or is your instructor guilty of a falsehood?

Case I: Your final exam score was less than 95 (the condition is false) and you did not receive an A (the conclusion is false). The instructor told the truth.

Case II: Your final exam score was less than 95, yet you received an A for the course. The instructor told the truth. (Perhaps your overall course average was excellent.)

Case III: Your final exam score was greater than 95, but you did not receive an A. The instructor lied.

Case IV: Your final exam score was greater than 95, and you received an A. The instructor told the truth.

To sum up, the only case in which a conditional proposition is false is when the condition is true and the conclusion is false.

The order of the condition and conclusion in a conditional proposition is important. If the condition and conclusion are exchanged, a different proposition is produced.

Definition 3.1.9 (Converse)**.** The converse of the proposition $p \to q$ is the proposition $q \to p$.

The converse of "If you receive a grade of 95 or better in the final exam, then you will receive an A in this course," is "If you receive an A in this course, then you received a grade of 95 or better in the final exam." It should be clear that these two statements say different things.

3.1.2.5 The Biconditional Operation

Definition 3.1.10 (Biconditional Proposition)**.** If p and q are propositions, the biconditional statement "p if and only if q," denoted $p \leftrightarrow q$, is defined by the truth table

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Note that $p \leftrightarrow q$ is true when p and q have the same truth values. It is common to abbreviate "if and only if" to "iff."

Although "if ... then..." and " ...if and only if ..." are frequently used in everyday speech, there are several alternate forms that you should be aware of. They are summarized in the following lists.

All of the following are equivalent to "If p then q":

- p implies q.
- q follows from q.
- p, only if q.
- q, if p.
- p is sufficient for q.
- q is necessary for p.

All of the following are equivalent to "p if and only if q":

- p is necessary and sufficient for q.
- p is equivalent to q.
- If p, then q, and if q, then p.
- If p, then q and conversely.

3.1.3 Exercises for Section 3.1

A Exercises

1. Let $d =$ "I like discrete structures", $c =$ "I will pass this course" and $s =$ "I will do my assignments." Express each of the following propositions in symbolic form:

(a) I like discrete structures and I will pass this course.

(b) I will do my assignments or I will not pass this course.

(c) It is not true that I like discrete structures and I will do my assignments.

(d) I will not do my assignment and I will not pass this course.

Answer.

(a) $d \wedge c$

(b) $s \vee \neg c$

(c) $\neg(d \wedge s)$

(d) $\neg s \wedge \neg c$

2. For each of the following propositions, identify simple propositions, express the compound proposition in symbolic form, and determine whether it is true or false:

(a) The world is flat or zero is an even integer.

(b) If 432,802 is a multiple of 4, then 432,802 is even.

(c) 5 is a prime number and 6 is not divisible by 4.

(d) $3 \in \mathbb{Z}$ and $3 \in \mathbb{Q}$.

(e) $2/3 \in \mathbb{Z}$ and $2/3 \in \mathbb{Q}$.

(f) The sum of two even integers is even and the sum of two odd integers is odd.

3. Let $p = 2 < 5$, $q =$ "8 is an even integer," and $r =$ "11 is a prime number." Express the following as a statement in English and determine whether the statement is true or false:

(a) $\neg p \vee q$

(b) $p \to q$

(c) $(p \wedge q) \to r$

(d) $p \to q \vee (\neg r)$

(e) $p \to (\neg q) \vee (\neg r)$

(f) $\neg q \to \neg p$

Answer.

(a) $2 > 5$ and 8 is an even integer. False.

(b) If $2 \leqslant 5$ then 8 is an even integer. True.

(c) If $2 \leqslant 5$ and 8 is an even integer then 11 is a prime number. True.

(d) If $2 \leqslant 5$ then either 8 is an even integer or 11 is not a prime number. True.

(e) If $2 \leqslant 5$ then either 8 is an odd integer or 11 is not a prime number. False.

(f) If 8 is not an even integer then $2 > 5$. True.

4. Rewrite each of the following statements using the other conditional forms:

(a) If an integer is a multiple of 4, then it is even.

(b) The fact that a polygon is a square is a sufficient condition that it is a rectangle.

(c) If $x = 5$, then $x^2 = 25$.

(d) If $x^2 - 5x + 6 = 0$, then $x = 2$ or $x = 3$.

(e) $x^2 = y^2$ is a necessary condition for $x = y$.

5. Write the converse of the propositions in exercise 4. Compare the truth of each proposition and its converse.

Answer. Only the converse of d is true.

3.2 Truth Tables and Propositions Generated by a Set

3.2.1 Truth Tables

Consider the compound proposition $c = (p \wedge q) \vee (\neg q \wedge r)$, where p, q, and r are propositions. This is an example of a proposition generated by p, q, and r. We will define this terminology later in the section. Since each of the three simple propositions has two possible truth values, it follows that there are eight different combinations of truth values that determine a value for c. These values can be obtained from a truth table for c. To construct the truth table, we build c from p, q, and r and from the logical operators. The result is the truth table below. Strictly speaking, the first three columns and the last column make up the truth table for c. The other columns are work space needed to build up to c.

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0	0	1	0	0
0	0	1	0	1	1	1
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	0	1	0	0
1	0	1	0	1	1	1
1	1	0	1	0	0	1
1	1	1	1	0	0	1

Table 3.2.1: Truth Table for $c = (p \wedge q) \vee (\neg q \wedge r)$

Note that the first three columns of the truth table are an enumeration of the eight three-digit binary integers. This standardizes the order in which the cases are listed. In general, if c is generated by n simple propositions, then the truth table for c will have 2^n rows with the first n columns being an enumeration of the n digit binary integers. In our example, we can see at a glance that for exactly four of the eight cases, c will be true. For example, if p and r are true and q is false (the sixth case), then c is true.

Let S be any set of propositions. We will give two definitions of a proposition generated by S. The first is a bit imprecise, but should be clear. The second definition is called a *recursive definition*. If you find it confusing, use the first definition and return to the second later.

3.2.2 Propositions Generated by a Set

Definition 3.2.2 (Proposition Generated by a Set)**.** Let S be any set of propositions. A proposition generated by S is any valid combination of propositions in S with conjunction, disjunction, and negation. Or, to be more precise,

1. If $p \in S$, then p is a proposition generated by S, and
2. If x and y are propositions generated by S, then so are (x), $\neg x$, $x \vee y$, and $x \wedge y$.

Note: We have not included the conditional and biconditional in the definition because they can both be generated from conjunction, disjunction, and negation, as we will see later.

If S is a finite set, then we may use slightly different terminology. For example, if $S = \{p, q, r\}$, we might say that a proposition is generated by p, q, and r instead from $\{p, q, r\}$.

3.2.2.1 The Hierarchy of Logical Operations

It is customary to use the following hierarchy for interpreting propositions, with parentheses overriding this order:

- First: Negation
- Second: Conjunction
- Third: Disjunction

Within any level of the hierarchy, work from left to right. Using these rules, $p \wedge q \vee r$ is taken to mean $(p \wedge q) \vee r$. These precedence rules are universal, and are exactly those used by computer languages to interpret logical expressions.

Example 3.2.3 (Examples of the Hierarchy of Logical Operations)**.** A few shortened expressions and their fully parenthesized versions:

1. $p \wedge q \wedge r$ is $(p \wedge q) \wedge r$.
2. $\neg p \vee \neg r$ is $(\neg p) \vee (\neg r)$.
3. $\neg\neg p$ is $\neg(\neg p)$.

A proposition generated by a set S need not include each element of S in its expression. For example, $\neg q \wedge r$ is a proposition generated by p, q, and r.

3.2.3 Exercises for Section 3.2

A Exercises

1. Construct the truth tables of:

(a) $p \vee p$

(b) $p \wedge (\neg p)$

(c) $p \vee (\neg p)$

(d) $p \wedge p$

Answer.

(a)

p	$p \vee p$
0	0
1	1

(b)

p	$\neg p$	$p \wedge p$
0	1	0
1	0	0

(c)

p	$\neg p$	$p \wedge (\neg p)$
0	1	1
1	0	1

(d)

p	$p \wedge p$
0	0
1	1

2. Construct the truth tables of:

(a) $\neg(p \wedge q)$

(b) $p \wedge (\neg q)$

(c) $(p \wedge q) \wedge r$

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

(e) $\neg p \vee \neg q$

(f) $p \vee q \vee r \vee s$

3. Rewrite the following with as few extraneous parentheses as possible:

(a) $(\neg((p) \wedge (r))) \vee (s)$

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

Answer.

(a) $\neg(p \wedge q) \vee s$

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

4. In what order are the operations in the following propositions performed?

(a) $p \vee \neg q \vee r \wedge \neg p$

(b) $p \wedge \neg q \wedge r \wedge \neg p$

5. Determine the number of rows in the truth table of a proposition containing four variables $p, q, r,$ and s.

Answer. $2^4 = 16$ rows.

6. If there are 45 lines on a sheet of paper, and you want to reserve one line for each line in a truth table, how large could $|S|$ be if you can write truth tables of propositions generated by S on the sheet of paper?

3.3 Equivalence and Implication

Consider two propositions generated by p and q: $\neg(p \wedge q)$ and $\neg p \vee \neg q$. At first glance, they are different propositions. In form, they are different, but they have the same meaning. One way to see this is to substitute actual propositions for p and q; such as p: I've been to Toronto; and q: I've been to Chicago.

Then $\neg(p \wedge q)$ translates to "I haven't been to both Toronto and Chicago," while $\neg p \vee \neg q$. is "I haven't been to Toronto or I haven't been to Chicago." Determine the truth values of these propositions. Naturally, they will be true for some people and false for others. What is important is that no matter what truth values they have, $\neg(p \wedge q)$ and $\neg p \vee \neg q$. will have the same truth value. The easiest way to see this is by examining the truth tables of these propositions.

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

Table 3.3.1: Truth Tables for $\neg(p \wedge q)$ and $\neg p \vee \neg q$

In all four cases, $\neg(p \wedge q)$ and $\neg p \vee \neg q$. have the same truth value. Furthermore, when the biconditional operator is applied to them, the result is a value of true in all cases. A proposition such as this is called a tautology.

3.3.1 Tautologies Contradictions

Definition 3.3.2 (Tautology)**.** An expression involving logical variables that is true in all cases is a tautology. The number 1 is used to symbolize a tautology.

Example 3.3.3 (Some Tautologies)**.**

1. $(\neg(p \wedge q)) \leftrightarrow (\neg p \vee \neg q)$.
2. $p \vee \neg p$
3. $(p \wedge q) \rightarrow p$
4. $q \rightarrow (p \vee q)$
5. $(p \vee q) \leftrightarrow (q \vee p)$

Definition 3.3.4 (Contradiction)**.** . An expression involving logical variables that is false for all cases is called a contradiction. The number 0 is used to symbolize a contradiction.

Example 3.3.5 (Some Contradictions)**.** $p \wedge \neg p$ and $(p \vee q) \wedge (\neg p) \wedge (\neg q)$ are contradictions.

3.3.2 Equivalence

Definition 3.3.6 (Equivalence)**.** Let S be a set of propositions and let r and s be propositions generated by S. r and s are equivalent if and only if $r \leftrightarrow s$ is a tautology. The equivalence of r and s is denoted $r \iff s$.

Equivalence is to logic as equality is to algebra. Just as there are many ways of writing an algebraic expression, the same logical meaning can be expressed in many different ways.

Example 3.3.7 (Some Equivalences)**.** The following are all equivalences:

1. $(p \wedge q) \vee (\neg p \wedge q) \iff q$.
2. $p \rightarrow q \iff \neg q \rightarrow \neg p$
3. $p \vee q \iff q \vee p$.

All tautologies are equivalent to one another.

Example 3.3.8 (An equivalence to 1)**.** $p \vee \neg p \iff l$.

All contradictions are equivalent to one another.

Example 3.3.9 (An equivalence to 0)**.** $p \wedge \neg p \iff 0$.

3.3.3 Implication

3.3.3.1 Where is the money?

Consider the two propositions:

x: The money is behind Door A; and
y: The money is behind Door A or Door B.

Imagine that you were told that there is a large sum of money behind one of two doors marked A and B, and that one of the two propositions x and y is true and the other is false. Which door would you choose? All that you need to realize is that if x is true, then y will also be true. Since we know that this can't be the case, y must be the true proposition and the money is behind Door B.

This is an example of a situation in which the truth of one proposition leads to the truth of another. Certainly, y can be true when x is false; but x can't be true when y is false. In this case, we say that x implies y.Consider the truth table of $p \to q$, 4.2.4. If p implies q, then the third case can be ruled out, since it is the case that makes a conditional proposition false.

Definition 3.3.10 (Implication)**.** Let S be a set of propositions and let r and s be propositions generated by S. We say that r implies s if $r \to s$ is a tautology. We write $r \Rightarrow s$ to indicate this implication.

Example 3.3.11 (Disjunctive Addition)**.** A commonly used implication called "disjunctive addition" is $p \Rightarrow (p \vee q)$, which is verified by truth table 3.3.12.

p	q	$p \vee q$	$p \to p \vee q$
0	0	0	1
0	1	1	1
1	0	1	1
1	1	1	1

Table 3.3.12: Truth Table for to verify that $p \Rightarrow (p \vee q)$

If we let p represent "The money is behind Door A" and q represent "The money is behind Door B," $p \Rightarrow (p \vee q)$ is a formalized version of the reasoning used in 3.3.11. A common name for this implication is disjunctive addition. In the next section we will consider some of the most commonly used implications and equivalences.

When we defined what we mean by a Proposition Generated by a Set, we didn't include the conditional and biconditional operators. This was because of the two equivalences $p \to q \Leftrightarrow \neg p \vee q$ and $p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$. Therefore, any proposition that includes the conditional or biconditional operators can be written in an equivalent way using only conjunction, disjunction, and negation. We could even dispense with disjunction since $p \vee q$ is equivalent to a proposition that uses only conjunction and negation.

3.3.4 Exercises for Section 3.3

A Exercises

1. Given the following propositions generated by p, q, and r, which are equivalent to one another?

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

(b) $p \vee (r \vee q)$

(c) $r \wedge p$

(d) $\neg r \vee p$

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

(f) $r \to p$

(g) $r \vee \neg p$

(h) $p \to r$

Answer. $a \Leftrightarrow e, d \Leftrightarrow f, g \Leftrightarrow h$

2.

(a) Construct the truth table for $x = (p \wedge \neg q) \vee (r \wedge p)$.

(b) Give an example other than x itself of a proposition generated by p, q, and r that is equivalent to x.

(c) Give an example of a proposition other than x that implies x.

(d) Give an example of a proposition other than x that is implied by x.

3. Is an implication equivalent to its converse? Verify your answer using a truth table.

Solution. No. In symbolic form the question is: Is $(p \to q) \Leftrightarrow (q \to p)$?

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

This table indicates that an implication is not always equivalent to its converse.

4. Suppose that x is a proposition generated by p, q, and r that is equivalent to $p \vee \neg q$. Write out the truth table for x.

B Exercises

5. How large is the largest set of propositions generated by p and q with the property that no two elements are equivalent?

Solution. Let x be any proposition generated by p and q. The truth table for x has 4 rows and there are 2 choices for a truth value for x for each row, so there are $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ possible propositions.

6. Find a proposition that is equivalent to $p \vee q$ and uses only conjunction and negation.

7. Explain why a contradiction implies any proposition and any proposition implies a tautology.

Answer. $0 \to p$ and $p \to 1$ are tautologies.

8.

Definition 3.3.13 (The Scheffer Stroke)**.** The Scheffer Stroke is the logical operator defined by the following truth table:

p	q	p | q
0	0	1
0	1	1
1	0	1
1	1	0

Table 3.3.14: Truth Table for the Scheffer Stroke

(a) Prove that $p|q$ is equivalent to $\neg(p \wedge q)$.The significance of the Sheffer Stroke is that it is a "universal" operation in that all other logical operations can be built from it.

(b) Prove that $\neg p \Leftrightarrow p|p$.

(c) Build $\wedge$ using only the Sheffer Stroke.

(d) Build $\vee$ using only the Sheffer Stroke.

3.4 The Laws of Logic

In this section, we will list the most basic equivalences and implications of logic. Most of the equivalences listed in Table 3.4.3 should be obvious to the reader. Remember, 0 stands for contradiction, 1 for tautology. Many logical laws are similar to algebraic laws. For example, there is a logical law corresponding to the associative law of addition, $a + (b + c) = (a + b) + c$. In fact, associativity of both conjunction and disjunction are among the laws of logic. Notice that with one exception, the laws are paired in such a way that exchanging the symbols $\wedge$, $\vee$, 1 and 0 for $\vee$, $\wedge$, 0, and 1, respectively, in any law gives you a second law. For example, $p \vee 0 \Leftrightarrow p$ results in $p \wedge 1 \Leftrightarrow p$. This called a *duality principle*. For now, think of it as a way of remembering two laws for the price of one. We will leave it to the reader to verify a few of these laws with truth tables. However, the reader should be careful in applying duality to the conditional operator and implication since the dual involves taking the converse. For example, the dual of $p \wedge q \Rightarrow p$ is $p \vee q \Leftarrow p$, which is usually written $p \Rightarrow p \vee q$

Example 3.4.1 (Verification of an Identity Law)**.**

p	1	$p \wedge 1$	$(p \wedge 1) \leftrightarrow p$
0	1	0	1
1	1	1	1

Table 3.4.2: Truth table to demonstrate the identity law for conjunction.

Some of the logical laws in Table 3.4.4 might be less obvious to you. For any that you are not comfortable with, substitute actual propositions for the logical variables. For example, if p is "John owns a pet store" and q is "John likes pets," the detachment law should make sense.

Commutative Laws	
$p \vee q \Leftrightarrow q \vee p$	$p \wedge q \Leftrightarrow q \wedge p$
Associative Laws	
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
Distributive Laws	
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
Identity Laws	
$p \vee 0 \Leftrightarrow p$	$p \wedge 1 \Leftrightarrow p$
Negation Laws	
$p \wedge \neg p \Leftrightarrow 0$	$p \vee \neg P \Leftrightarrow 1$
Idempotent Laws	
$p \vee p \Leftrightarrow p$	$p \wedge p \Leftrightarrow p$
Null Laws	
$p \wedge 0 \Leftrightarrow 0$	$p \vee 1 \Leftrightarrow 1$
Absorption Laws	
$p \wedge (p \vee q) \Leftrightarrow p$	$p \vee (p \wedge q) \Leftrightarrow p$
DeMorgan's Laws	
$\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$	$\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$
Involution Law	
$\neg(\neg p) \Leftrightarrow p$	

Table 3.4.3: Basic Logical Laws - Equivalences

Detachment	$(p \to q) \wedge p \Rightarrow q$
Indirect Reasoning	$(p \to q) \wedge \neg q \Rightarrow \neg p$
Disjunctive Addition	$p \Rightarrow (p \vee q)$
Conjunctive Simplification	$(p \wedge q) \Rightarrow p$ and $(p \wedge q) \Rightarrow q$
Disjunctive Simplification	$(p \vee q) \wedge \neg p \Rightarrow q$ and $(p \backslash / q) \wedge \neg q \Rightarrow p$
Chain Rule	$(p \to q) \wedge (q \to r) \Rightarrow (p \to r)$
Conditional Equivalence	$p \to q \Leftrightarrow \neg p \vee q$
Biconditional Equivalences	$(p \leftrightarrow q) \Leftrightarrow (p \to q) \wedge (q \to p) \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$
Contrapositive	$(p \to q) \Leftrightarrow (\neg q \to \neg p)$

Table 3.4.4: Basic Logical Laws - Common Implications and Equivalences

3.4.1 Exercises for Section 3.4

A Exercises

1. Write the following in symbolic notation and determine whether it is a

tautology: "If I study then I will learn. I will not learn. Therefore, I do not study."

Answer. Let $s =$ I will study,$t =$ I will learn. The argument is: $((s \to t) \wedge (\neg t)) \to (\neg s)$, call the argument a.

s	t	$s \to t$	$(s \to t) \wedge (\neg t)$	a
0	0	1	1	1
0	1	1	0	1
1	0	0	0	1
1	1	1	0	1

Since a is a tautology, the argument is valid.

2. Show that the common fallacy $(p \to q) \wedge \neg p \Rightarrow \neg q$ is not a law of logic.

3. Describe, in general, how duality can be applied to implications if we introduce the symbol $\Leftarrow$, read "is implied by."

Answer. In any true statement S, replace; $\wedge$ with $\vee$, $\vee$ with $\wedge$, 0 with 1, 1 with 0, $\Leftarrow$ with $\Rightarrow$, and $\Rightarrow$ with $\Leftarrow$. Leave all other connectives unchanged.

4. Write the dual of the following statements:

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

(b) $(p \vee q) \wedge \neg q \Rightarrow p$

3.5 Mathematical Systems

In this section, we present an overview of what a mathematical system is and how logic plays an important role in one. The axiomatic method that we will use here will not be duplicated with as much formality anywhere else in the book, but we hope an emphasis on how mathematical facts are developed and organized will help to unify the concepts we will present. The system of propositions and logical operators we have developed will serve as a model for our discussion. Roughly, a mathematical system can be defined as follows.

Definition 3.5.1 (Mathematical System)**.** A mathematical system consists of:

1. A set or universe, U.
2. Definitions: sentences that explain the meaning of concepts that relate to the universe. Any term used in describing the universe itself is said to be undefined. All definitions are given in terms of these undefined concepts of objects.
3. Axioms: assertions about the properties of the universe and rules for creating and justifying more assertions. These rules always include the system of logic that we have developed to this point.
4. Theorems: the additional assertions mentioned above.

Example 3.5.2 (Euclidean Geometry)**.** In Euclidean geometry the universe consists of points and lines (two undefined terms). Among the definitions is a definition of parallel lines and among the axioms is the axiom that two distinct parallel lines never meet.

Example 3.5.3 (Propositional Calculus)**.** Propositional calculus is a formal name for the logical system that we've been discussing. The universe consists of propositions. The axioms are the truth tables for the logical operators and the key definitions are those of equivalence and implication. We use propositions to describe any other mathematical system; therefore, this is the minimum amount of structure that a mathematical system can have.

Definition 3.5.4 (Theorem)**.** A true proposition derived from axioms of mathematical system is called a theorem.

Theorems are normally expressed in terms of a finite number of propositions, $p_1, p_2, ..., p_n$, called the *premises*, and a proposition,C, called the *conclusion*. These theorems take the form

$$p_1 \wedge p_2 \wedge \cdots \wedge p_n \Rightarrow C$$

or more informally,

$$p_1, p_2, ..., \text{ and } p_n \text{ imply } C$$

For a theorem of this type, we say that the premises imply the conclusion. When a theorem is stated, it is assumed that the axioms of the system are true. In addition, any previously proven theorem can be considered an extension of the axioms and can be used in demonstrating that the new theorem is true. When the proof is complete, the new theorem can be used to prove subsequent theorems. A mathematical system can be visualized as an inverted pyramid with the axioms at the base and the theorems expanding out in various directions.

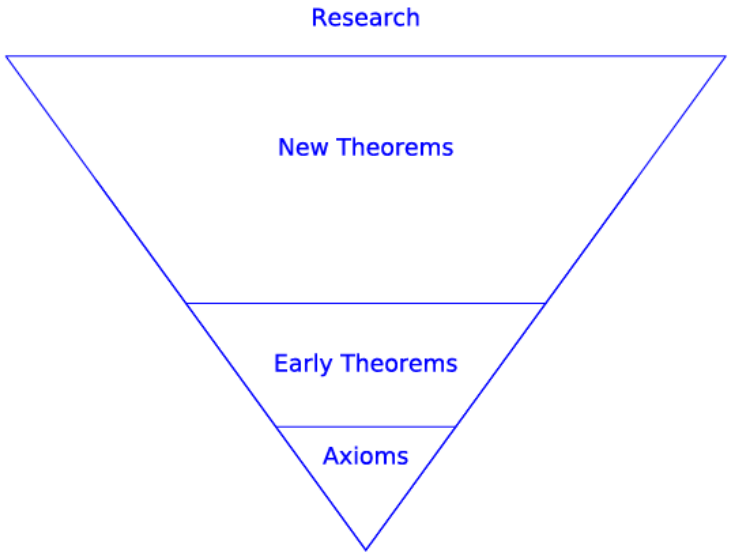


Figure 3.5.5: The body of knowledge in a mathematical system

Definition 3.5.6 (Proof)**.** A proof of a theorem is a finite sequence of logically valid steps that demonstrate that the premises of a theorem imply its conclusion.

Exactly what constitutes a proof is not always clear. For example, a research mathematician might require only a few steps to prove a theorem to a colleague, but might take an hour to give an effective proof to a class of students. Therefore, what constitutes a proof often depends on the audience. But the audience is not the only factor. One of the most famous theorems in graph theory, The Four Color Theorem, was proven in 1976, after over a century of effort by many mathematicians. Part of

the proof consisted of having a computer check many different graphs for a certain property. Without the aid of the computer, this checking would have taken years. In the eyes of some mathematicians, this proof was considered questionable. Shorter proofs have been developed since 1976 and there is no controversy associated with The Four Color Theorem at this time. (The theorem is stated in Chapter 9.)

3.5.1 Proofs In Propositional Calculus

Theoretically, you can prove anything in propositional calculus with truth tables. In fact, the laws of logic stated in Section 5.4 are all theorems. Propositional calculus is one of the few mathematical systems for which any valid sentence can be determined true or false by mechanical means. A program to write truth tables is not too difficult to write; however, what can be done theoretically is not always practical. For example,

$$a, a \to b, b \to c, ..., y \to z \Rightarrow z$$

is a theorem in propositional calculus. However, suppose that you wrote such a program and you had it write the truth table for

$$(a \wedge (a \to b) \wedge (b \to c) \wedge \cdots \wedge (y \to z)) \to z$$

The truth table will have 2^{26} cases. At one million cases per second, it would take approximately one hour to verify the theorem. Now if you decided to check a similar theorem,

$$p_1, p_1 \to p_2, \ldots, p_{99} \to p_{100} \Rightarrow p_{100}$$

you would really have time trouble. There would be $2^{100} \approx 1.26765 \times 10^{30}$ cases to check in the truth table. At one million cases per second it would take approximately 1.46719×10^{19} days to check all cases. For most of the remainder of this section, we will discuss an alternate method for proving theorems in propositional calculus. It is the same method that we will use in a less formal way for proofs in other systems. Formal axiomatic methods would be too unwieldy to actually use in later sections. However, none of the theorems in later chapters would be stated if they couldn't be proven by the axiomatic method.

We will introduce two types of proof here, direct and indirect.

3.5.1.1 Direct Proofs

A *direct proof* is a proof in which the truth of the premises of a theorem are shown to directly imply the truth of the theorem's conclusion.

Example 3.5.7 (A typical direct proof)**.**

Step	Proposition	Justification
1.	$p \vee q$	Premise
2.	$\neg p \to q$	(1), conditional rule
3.	$q \to s$	Premise
4.	$\neg p \to s$	(2), (3), chain rule
5.	$\neg s \to p$	(4), contrapositive
6.	$p \to r$	Premise
7.	$\neg s \to r$	(5), (6), chain rule
8.	$s \vee r$	(7), conditional rule ■

Table 3.5.8: Direct proof of $p \to r, q \to s, p \vee q \Rightarrow s \vee r$

Note that ■ marks the end of a proof.Example 3.5.7 illustrates the usual method of formal proof in a formal mathematical system. The rules governing these proofs are:

1. A proof must end in a finite number of steps.

2. Each step must be either a premise or a proposition that is implied from previous steps using any valid equivalence or implication.

3. For a direct proof , the last step must be the conclusion of the theorem. For an indirect proof (see below), the last step must be a contradiction.

4. Justification Column. The column labeled "justification" is analogous to the comments that appear in most good computer programs. They simply make the proof more readable.

Example 3.5.9 (Two proofs of the same theorem)**.** Here are two direct proofs of $\neg p \vee q, s \vee p, \neg q \Rightarrow s$:

1.	$\neg p \vee q$	Premise
2.	$\neg q$	Premise
3.	$\neg p$	Disjunctive simplification, (1), (2)
4.	$s \vee p$	Premise
5.	s	Disjunctive simplification, (3), (4). ■

Table 3.5.10: Direct proof of $\neg p \vee q, s \vee p, \neg q \Rightarrow s$

You are invited to justify the steps in this second proof:

1.	$\neg p \vee q$
2.	$\neg q \rightarrow \neg p$
3.	$s \vee p$
4.	$p \vee s$
5.	$\neg p \rightarrow s$
6.	$\neg q \rightarrow s$
7.	$\neg q$
8.	s ■

Table 3.5.11: Alternate proof of $\neg p \vee q, s \vee p, \neg q \Rightarrow s$

The conclusion of a theorem is often a conditional proposition. The condition of the conclusion can be included as a premise in the proof of the theorem. The object of the proof is then to prove the consequence of the conclusion. This rule is justified by the logical law

$$p \rightarrow (h \rightarrow c) \Leftrightarrow (p \wedge h) \rightarrow c$$

Example 3.5.12 (Example of a proof with a conditional conclusion)**.** The following proof of $p \rightarrow (q \rightarrow s), \neg r \vee p, q \Rightarrow r \rightarrow s$ includes r as a fourth premise. Inference of truth of s completes the proof.

1.	$\neg r \vee p$	Premise
2.	r	Added premise
3.	p	(1), (2), disjunction simplification
4.	$p \to (q \to s)$	Premise
5.	$q \to s$	(3), (4), detachment
6.	q	Premise
7.	s	(5), (6), detachment. ■

Table 3.5.13: Proof of a theorem with a conditional conclusion.

3.5.1.2 Indirect Proof / Proof by Contradiction

Consider a theorem $P \Rightarrow C$, where P represents $p_1, p_2, ...,$ and p_n, the premises. The method of indirect proof is based on the equivalence $P \to C \Leftrightarrow \neg(P \wedge \neg C)$. In words, this logical law states that if $P \Rightarrow C$, then $P \wedge \neg C$ is always false; that is, $P \wedge \neg C$ is a contradiction. This means that a valid method of proof is to negate the conclusion of a theorem and add this negation to the premises. If a contradiction can be implied from this set of propositions, the proof is complete. For the proofs in this section, a contradiction will often take the form $t \wedge \neg t$.

For proofs involving numbers, a contradiction might be $1 = 0$ or $0 < 0$. Indirect proofs involving sets might conclude with $x \in \emptyset$ or ($x \in A$ and $x \in A^c$). Indirect proofs are often more convenient than direct proofs in certain situations. Indirect proofs are often called *proofs by contradiction*.

Example 3.5.14 (An Indirect Proof)**.** Here is an example of an indirect proof of the theorem in Example 3.5.7.

1.	$\neg(s \vee r)$	Negated conclusion
2.	$\neg s \wedge \neg r$	DeMorgan's Law, (1)
3.	$\neg s$	Conjunctive simplification, (2)
4.	$q \to s$	Premise
5.	$\neg q$	Indirect reasoning, (3), (4)
6.	$\neg r$	Conjunctive simplification, (2)
7.	$p \to r$	Premise
8.	$\neg p$	Indirect reasoning, (6), (7)
9.	$(\neg p) \wedge (\neg q)$	Conjunctive, (5), (8)
10.	$\neg(p \vee q)$	DeMorgan's Law, (9)
11.	$p \vee q$	Premise
12.	0	(10), (11) ■

Table 3.5.15: An Indirect proof of $p \to r, q \to s, p \vee q \Rightarrow s \vee r$

3.5.1.3 Proof Style

The rules allow you to list the premises of a theorem immediately; however, a proof is much easier to follow if the premises are only listed when they are needed.

Example 3.5.16 (Yet Another Indirect Proof)**.** Here is an indirect proof of $a \to b, \neg(b \vee c) \Rightarrow \neg a$.

1.	a	Negation of the conclusion
2.	$a \to b$	Premise
3.	b	(1), (2), detachment
4.	$b \vee c$	(3), disjunctive addition
5.	$\neg(b \vee c)$	Premise
6.	0	(4), (5) ■

Table 3.5.17: Indirect proof of $a \to b, \neg(b \vee c) \Rightarrow \neg a$

As we mentioned at the outset of this section, we are only presenting an overview of what a mathematical system is. For greater detail on axiomatic theories, see Stoll (1961). An excellent description of how propositional calculus plays a part in artificial intelligence is contained in Hofstadter (1980). If you enjoy the challenge of constructing proofs in propositional calculus, you should enjoy the game WFF'N PROOF (1962), by L.E. Allen.

3.5.2 Exercises for Section 3.5

A Exercises

1. Prove with truth tables:

(a) $p \vee q, \neg q \Rightarrow p$

(b) $p \to q, \neg q \Rightarrow \neg p$

Answer.

(a)

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

(b)

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

2. Prove with truth tables:

(a) $q, \neg q \Rightarrow p$

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

B Exercises

3. Give direct and indirect proofs of:

(a) $a \to b, c \to b, d \to (a \vee c), d \Rightarrow b$.

(b) $(p \to q) \wedge (r \to s), (q \to t) \wedge (s \to u), \neg(t \wedge u), p \to r \Rightarrow \neg p$.

(c) $p \to (q \to r), \neg s \backslash / p, q \Rightarrow s \to r.$

(d) $p \to q, q \to r, \neg(p \wedge r), p \vee r \Rightarrow r.$

(e) $\neg q, p \to q, p \vee t \Rightarrow t$

Answer.

(a) i. Direct proof:
ii. $d \to (a \vee c)$
iii. d
iv. $a \vee c$
v. $a \to b$
vi. Indirect proof:
vii. $\neg b$ Negated conclusion
ii. $a \to b$ Premise
iii. $\neg a$ Indirect Reasoning (1), (2)
iv. $c \to b$ Premise
v. $\neg c$ Indirect Reasoning (1), (4)
vi. $(\neg a \wedge \neg c)$ Conjunctive (3), (5)
vii. $\neg(a \vee c)$ DeMorgan's law (6)
viii. $d \to (a \vee c)$ Premise
ix. $\neg d$ Indirect Reasoning (7), (8)
x. d Premise
xi. $\nvdash$ (9), (10) ■

(b) Direct proof:
i. $(p \to q) \wedge (r \to s)$
ii. $p \to q$
iii. $(p \to t) \wedge (s \to u)$
iv. $q \to t$
v. $p \to t$
vi. $r \to s$
vii. $s \to u$
viii. $r \to u$
ix. $p \to r$
x. $p \to u$
xi. $p \to (t \wedge u)$ Use $(x \to y) \wedge (x \to z) \Leftrightarrow x \to (y \wedge z)$
xii. $\neg(t \wedge u) \to \neg p$
xiii. $\neg(t \wedge u)$
xiv. $\neg p$ ■

Indirect proof:
i. p
ii. $p \to q$
iii. q
iv. $q \to t$
v. t
vi. $\neg(t \wedge u)$
vii. $\neg t \vee \neg u$
viii. $\neg u$

ix. $s \to u$
x. $\neg s$
xi. $r \to s$
xii. $\neg r$
xiii. $p \to r$
xiv. r
xv. 0 ■

(c) Direct proof:

i. $\neg s \vee p$ Premise
ii. s Added premise (conditional conclusion)
iii. $\neg(\neg s)$ Involution (2)
iv. p Disjunctive simplification (1), (3)
v. $p \to (q \to r)$ Premise
vi. $q \to r$ Detachment (4), (5)
vii. q Premise
viii. r Detachment (6), (7) ■

Indirect proof:

i. $\neg(s \to r)$ Negated conclusion
ii. $\neg(\neg s \vee r)$ Conditional equivalence (I)
iii. $s \wedge \neg r$ DeMorgan (2)
iv. s Conjunctive simplification (3)
v. $\neg s \vee p$ Premise
vi. $s \to p$ Conditional equivalence (5)
vii. p Detachment (4), (6)
viii. $p \to (q \to r)$ Premise
ix. $q \to r$ Detachment (7), (8)
x. q Premise
xi. r Detachment (9), (10)
xii. $\neg r$ Conjunctive simplification (3)
xiii. 0 Conjunction (11), (12) ■

(d) Direct proof:

i. $p \to q$
ii. $q \to r$
iii. $p \to r$
iv. $p \vee r$
v. $\neg p \vee r$
vi. $(p \vee r) \wedge (\neg p \vee r)$
vii. $(p \wedge \neg p) \vee r$
viii. $0 \vee r$
ix. r■

Indirect proof:

i. $\neg r$ Negated conclusion
ii. $p \vee r$ Premise
iii. p (1), (2)
iv. $p \to q$ Premise
v. q Detachment (3), (4)

vi. $q \to r$ Premise
vii. r Detachment (5), (6)
viii. 0 (1), (7) ■

4. Give direct and indirect proofs of:

(a) $p \to q, \neg r \to \neg q, \neg r \Rightarrow \neg p$.

(b) $p \to \neg q, \neg r \to q, p \Rightarrow r$.

(c) $a \vee b, c \wedge d, a \to \neg c \Rightarrow b$.

5. Are the following arguments valid? If they are valid, construct formal proofs; if they aren't valid, explain why not.

(a) If wages increase, then there will be inflation. The cost of living will not increase if there is no inflation. Wages will increase. Therefore, the cost of living will increase.

(b) If the races are fixed or the casinos are crooked, then the tourist trade will decline. If the tourist trade decreases, then the police will be happy. The police force is never happy. Therefore, the races are not fixed.

Answer.

(a) Let W stand for "Wages will increase,"I stand for "there will be inflation," and C stand for "cost of living will increase." Therefore the argument is: $W \to I$, $\neg I \to \neg C$, $W \Rightarrow C$.. The argument is invalid. The easiest way to see this is through a truth table. Let x be the conjunction of all premises.

W	I	C	$\neg I$	$\neg C$	$W \to I$	$\neg I \to \neg C$	x	$x \to C$
0	0	0	1	1	1	0	0	1
0	0	1	1	0	1	1	0	1
0	1	0	0	1	1	1	0	1
0	1	1	0	0	1	1	0	1
1	0	0	1	1	0	0	0	1
1	0	1	1	0	0	1	0	1
1	1	0	0	1	1	1	1	1
1	1	1	0	0	1	1	1	0

(b) Let r stand for "the races are fixed," c stand for "casinos are crooked," t stand for "the tourist trade will decline," and p stand for "the police will be happy." Therefore, the argument is:

$$(r \vee c) \to t, t \to p, \neg p \to \neg r$$

. The argument is valid. Proof:

i. $t \to p$ Premise
ii. $\neg p$ Premise
iii. $\neg t$ Indirect Reasoning (1), (2)
iv. $(r \vee c) \to t$ Premise
v. $\neg(r \vee c)$ Indirect Reasoning (3), (4)
vi. $(\neg r) \wedge (\neg c)$ DeMorgan (5)
vii. $\neg r$ Conjunction simplification (6) ■

6. Determine the validity of the following argument: For students to do well in a discrete mathematics course, it is necessary that they study hard. Students who do well in courses do not skip classes. Students who study hard do well in courses. Therefore students who do well in a discrete mathematics course do not skip class.

7. Describe how $p_1, p_1 \to p_2, \ldots, p_{99} \to p_{100} \Rightarrow p_{100}$ could be proven in 199 steps.

Answer. $p_1 \to p_k$ and $p_k \to p_{k+1}$ implies $p_1 \to p_{k+1}$. It takes two steps to get to $p_1 \to p_{k+1}$ from $p_1 \to p_k$ This means it takes $2(100-1)$ steps to get to $p_1 \to p_{100}$ (subtract 1 because $p_1 \to p_2$ is stated as a premise). A final step is needed to apply detachment to imply p_{100}

3.6 Propositions over a Universe

Consider the sentence "He was a member of the Boston Red Sox." There is no way that we can assign a truth value to this sentence unless "he" is specified. For that reason, we would not consider it a proposition. However, "he" can be considered a variable that holds a place for any name. We might want to restrict the value of "he" to all names in the major-league baseball record books. If that is the case, we say that the sentence is a proposition over the set of major-league baseball players, past and present.

Definition 3.6.1 (Proposition over a Universe)**.** Let U be a nonempty set. A proposition over U is a sentence that contains a variable that can take on any value in U and that has a definite truth value as a result of any such substitution.

Example 3.6.2 (Some propositions over a variety of universes)**.**

1. A few propositions over the integers are $4x^2 - 3x = 0$, $0 \leq n \leq 5$, and "k is a multiple of 3."
2. A few propositions over the rational numbers are $4x^2 - 3x = 0$, $y^2 = 2$, and $(s-1)(s+1) = s^2 - 1$.
3. A few propositions over the subsets of $\mathbb{P}$ are $(A = \emptyset) \vee (A = \mathbb{P})$, $3 \in A$, and $A \cap \{1, 2, 3\} \neq \emptyset$.

All of the laws of logic that we listed in Section 3.4 are valid for propositions over a universe. For example, if p and q are propositions over the integers, we can be certain that $p \wedge q \Rightarrow p$, because $(p \wedge q) \to p$ is a tautology and is true no matter what values the variables in p and q are given. If we specify p and q to be $p(n) : n < 4$ and $q(n) : n < 8$, we can also say that p implies $p \wedge q$. This is not a usual implication, but for the propositions under discussion, it is true. One way of describing this situation in general is with truth sets.

3.6.1 Truth Sets

Definition 3.6.3 (Truth Set)**.** If p is a proposition over U, the truth set of p is $T_p = \{a \in U \mid p(a) \text{ is true}\}$.

Example 3.6.4 (Truth Set Example)**.** The truth set of the proposition $\{1, 2\} \cap A = \emptyset$, taken as a proposition over the power set of $\{1, 2, 3, 4\}$ is $\{\emptyset, \{3\}, \{4\}, \{3, 4\}\}$.

Example 3.6.5 (Truth sets depend on the universe)**.** Over the universe *mathbbZ* (the integers), the truth set of $4x^2 - 3x = 0$ is $\{0\}$. If the universe is expanded to the rational numbers, the truth set becomes $\{0, 3/4\}$. The term *solution set* is often used for the truth set of an equation such as the one in this example.

Definition 3.6.6 (Tautologys and Contradictions over a Universe)**.** A proposition over U is a tautology if its truth set is U. It is a contradiction if its truth set is empty.

Example 3.6.7 (Tautology, Contradiction over $\mathbb{Q}$)**.** $(s-1)(s+1) = s^2 - 1$ is a tautology over the rational numbers. $x^2 - 2 = 0$ is a contradiction over the rationals.

The truth sets of compound propositions can be expressed in terms of the truth sets of simple propositions. For example, if $a \in T_{p \wedge q}$ if and only if a makes $p \wedge q$ true. This is true iff an only if a makes both p and q true, which which, in turn, is true if and only if $a \in T_p \cap T_q$. This explains why the truth set of the conjunction of two propositions equals the intersection of the truth sets of the two propositions. The following list summarizes the connection between compound and simple truth sets

$$\begin{gathered} T_{p \wedge q} = T_p \cap T_q \\ T_{p \vee q} = T_p \cup T_q \\ T_{\neg p} = {T_p}^c \\ T_{p \leftrightarrow q} = (T_p \cap T_q) \cup ({T_p}^c \cap {T_q}^c) \\ T_{p \to q} = {T_p}^c \cup T_q \end{gathered}$$

Table 3.6.8: Truth Sets of Compound Statements

Definition 3.6.9 (Equivalence of propositions over a universe)**.** : Two propositions are equivalent if $p \leftrightarrow q$ is a tautology. In terms of truth sets, this means that p and q are equivalent if $T_p = T_q$.

Example 3.6.10 (Some pairs of equivalent propositions.)**.**

1. $n + 4 = 9$ and $n = 5$ are equivalent propositions over the integers.
2. $A \cap \{4\} \neq \emptyset$ and $4 \in A$ are equivalent propositions over the power set of the natural numbers.

Definition 3.6.11 (Implication for propositions over a universe)**.** : Implication. If p and q are propositions over U, p implies q if $p \to > q$ is a tautology.

Since the truth set of $p \to q$ is ${T_p}^c \cup T_q$, the Venn diagram for $T_{p \to q}$ in Figure 3.6.1 shows that $p \Rightarrow q$ when $T_p \subseteq T_q$.

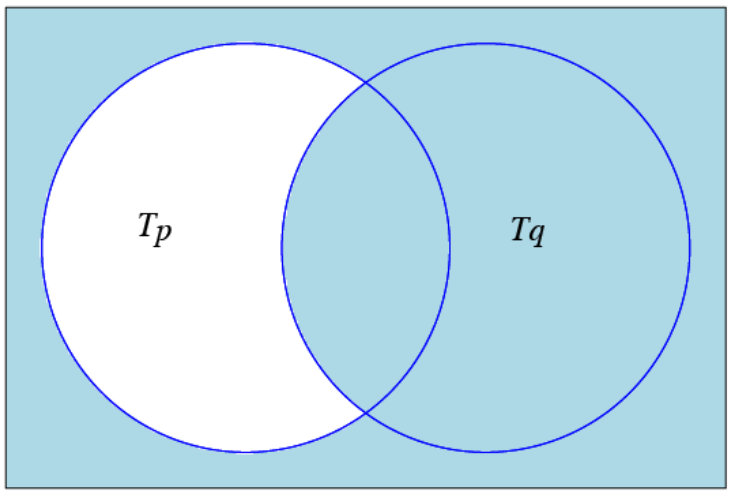


Figure 3.6.12: Venn Diagram for $T_{p \to q}$

Example 3.6.13 (Examples of Implications)**.**

1. Over the natural numbers: $n < 4 \Rightarrow n < 8$ since $\{0, 1, 2, 3, 4\} \subseteq \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
2. Over the power set of the integers: $|A^c| = 1$ implies $A \cap \{0, 1\} \neq \emptyset$
3. $A \subseteq$ even integers $\Rightarrow A \cap$ odd integers $= \emptyset$

3.6.2 Exercises for Section 3.6

A Exercises

1. If $U = \mathcal{P}(\{1, 2, 3, 4\})$, what are the truth sets of the following propositions?

(a) $A \cap \{2, 4\} = \emptyset$.

(b) $3 \in A$ and $1 \notin A$.

(c) $A \cup \{1\} = A$.

(d) A is a proper subset of $\{2, 3, 4\}$.

(e) $|A| = |A^c|$.

Answer.

(a) $\{\{1\}, \{3\}, \{1, 3\}, \emptyset\}$

(b) $\{\{3\}, \{3, 4\}, \{3, 2\}, \{2, 3, 4\}\}$

(c) $\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{1, 2, 3, 4\}\}$

(d) $\{\{2\}, \{3\}, \{4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$

(e) $\{A \subseteq U : |A| = 2\}$

2. Over the universe of positive integers, define

$p(n)$: n is prime and $n < 32$.
$q(n)$: n is a power of 3.
$r(n)$: n is a divisor of 27.

(a) What are the truth sets of these propositions?

(b) Which of the three propositions implies one of the others?

Solution.

(a) i. $T_p = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$
ii. $T_q = \{1, 3, 9, 27, 81, \dots\}$
iii. $T_r = \{1, 3, 9, 27\}$

(b) $r \Rightarrow q$

3. If $U = \{0, 1, 2\}$, how many propositions over U could you list without listing two that are equivalent?

Answer. There are $2^3 = 8$ subsets of U, allowing for the possibility of 2^8 nonequivalent propositions over U.

4. Given the propositions over the natural numbers:

$$p : n < A, \quad q : 2n > 17, \text{ and } \quad r : n \text{ is a divisor of } 18$$

what are the truth sets of:

(a) q

(b) $p \wedge q$

(c) r

(d) $q \to r$

5. Suppose that s is a proposition over $\{1, 2, \ldots, 8\}$. If $T_s = \{1, 3, 5, 7\}$, give two examples of propositions that are equivalent to s.

Answer. Two possible answers: s is odd and $(s-1)(s-3)(s-5)(s-7) = 0$

6.

(a) Determine the truth sets of the following propositions over the positive integers:

$$p(n) : n \text{ is a perfect square and } n < 100$$

$$q(n) : n = |\mathcal{P}(A)| \text{ for some set } A$$

(b) Determine $T_{p \wedge q}$ for p and q above.

7. Let the universe be $\mathbb{Z}$, the set of integers. Which of the following propositions are equivalent over $\mathbb{Z}$?

a: $0 < n^2 < 9$
b: $0 < n^3 < 27$
c: $0 < n < 3$

Solution. b and c

3.7 Mathematical Induction

In this section, we will examine mathematical induction, a technique for proving propositions over the positive integers. Mathematical induction reduces the proof that all of the positive integers belong to a truth set to a finite number of steps.

Example 3.7.1 (Formula for Triangular Numbers)**.** Consider the following proposition over the positive integers, which we will label $p(n)$: The sum of the positive integers from 1 to n is $\frac{n(n+1)}{2}$. This is a well-known formula that is quite simple to verify for a given value of n. For example, $p(5)$ is: The sum of the positive integers from 1 to 5 is $\frac{5(5+1)}{2}$. Indeed, $1+2+3+4+5 = 15 = \frac{5(5+1)}{2}$. However, this doesn't serve as a proof that $p(n)$ is a tautology. All that we've established is that 5 is in the truth set of p. Since the positive integers are infinite, we certainly can't use this approach to prove the formula.

An Analogy: A proof by mathematical induction is similar to knocking over a row of closely spaced dominos that are standing on end. To knock over the five dominos in Figure 3.7.2, all you need to do is push Domino 1 to the right. To be assured that they all will be knocked over, some work must be done ahead of time. The dominos must be positioned so that if any domino is pushed to the right, it will push the next domino in the line.

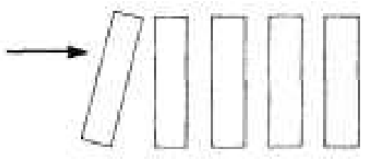


Figure 3.7.2: An analogy for Mathematical Induction

Returning to 3.7.1 imagine the propositions $p(1), p(2), p(3), \ldots$ to be an infinite line of dominos. Let's see if these propositions are in the same formation as the dominos were. First, we will focus on one specific point of the line: $p(99)$ and $p(100)$. We are not going to prove that either of these propositions is true, just that the truth of $p(99)$ implies the truth of $p(100)$. In terms of our analogy, if $p(99)$ is knocked over, it will knock over $p(100)$.

In proving $p(99) \Rightarrow p(\text{l}00)$, we will use $p(99)$ as our premise. We must prove: The sum of the positive integers from 1 to 100 is $\frac{100(100+1)}{2}$. We start by observing that the sum of the positive integers from 1 to 100 is $(1 + 2 + \cdots + 99) + 100$. That is, the sum of the positive integers from 1 to 100 equals the sum of the first ninety-nine plus the final number, 100. We can now apply our premise, $p(99)$, to the sum $1 + 2 + \cdots + 99$. After rearranging our numbers, we obtain the desired expression for $1 + 2 + \cdots + 100$:

$$\begin{aligned} 1 + 2 + \cdots + 99 + 100 &= (1 + 2 + \cdots + 99) + 100 \\ &= \frac{99(99+1)}{2} + 100 \text{ by our assumption of } p(99) \\ &= \frac{99\ 100}{2} + \frac{2\ 100}{2} \\ &= \frac{100\ 101}{2} \\ &= \frac{100(100+1)}{2} \end{aligned}$$

What we've just done is analogous to checking two dominos in a line and finding that they are properly positioned. Since we are dealing with an infinite line, we must check all pairs at once. This is accomplished by proving that $p(n) \Rightarrow p(n+1)$ for all $n \geq 1$:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= (1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \text{ by } p(n) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)((n+1)+1)}{2} \end{aligned}$$

They are all lined up! Now look at $p(1)$: The sum of the positive integers from 1 to l is $\frac{1+1}{2}$. Clearly, $p(1)$ is true. This sets off a chain reaction. Since $p(1) \Rightarrow p(2)$, $p(2)$ is true. Since $p(2) \Rightarrow p(3)$, $p(3)$ is true; and so on. ■

Theorem 3.7.3 (The Principle of Mathematical Induction)**.** *Let $p(n)$ be a proposition over the positive integers, then $p(n)$ is a tautology if*

1. *$p(1)$ is true, and*

2. for all $n \geq 1$, $p(n) \Rightarrow p(n+1)$.

Note: The truth of $p(1)$ is called the *basis* for the induction proof. The premise that p(n) is true in second part is called the *induction hypothesis*. The proof that $p(n)$ implies $p(n+1)$ is called the *induction* step of the proof. Despite our analogy, the basis is usually done first in an induction proof. However, order doesn't really matter.

Example 3.7.4 (Generalized Detachment)**.** Consider the implication over the positive integers.

$$p(n) : q_0 \to q_1, q_1 \to q_2, \ldots, q_{n-1} \to q_n, q_0 \Rightarrow q_n$$

A proof that $p(n)$ is a tautology follows. Basis: $p(1)$ is $q_0 \to q_1, q_0 \Rightarrow q_1$. This is the logical law of detachment which we know is true. If you haven't done so yet, write out the truth table of $((q_0 \to q_1) \wedge q_0) \to q_1$ to verify this step.

Induction: Assume that $p(n)$ is true for some $n \geq 1$. We want to prove that $p(n+1)$ must be true. That is:

$$q_0 \to q_1, q_1 \to q_2, \ldots, q_{n-1} \to q_n, q_n \to q_{n+1}, q_0 \Rightarrow q_{n+1}$$

Here is a direct proof of $p(n+1)$:

Step	Proposition	Justification
1 - $(n+1)$	$q_0 \to q_1, q_1 \to q_2, \ldots, q_{n-1} \to q_n, q_0$	Premises
p$\to p \vee q$		
$n+2$	q_n	$(1) - (n+1)$, $p(n)$
$n+3$	$q_n \to q_{n+1}$	Premise
$n+4$	q_{n+1}	$(n+2), (n+3)$, detachment

■

Example 3.7.5 (An example from Number Theory)**.** For all $n \geq 1$, $n^3 + 2n$ is a multiple of 3. An inductive proof follows:

Basis: $1^3 + 2(1) = 3$ is a multiple of 3. The basis is almost always this easy!

Induction: Assume that $n \geq 1$ and $n^3 + 2n$ is a multiple of 3. Consider $(n+1)^3 + 2(n+1)$. Is it a multiple of 3?

$$\begin{aligned}(n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 3n + 1 + (2n+2) \\ &= n^3 + 2n + 3n^2 + 3n + 3 \\ &= (n^3 + 2n) + 3(n^2 + n + 1)\end{aligned}$$

Yes, $(n+1)^3 + 2(n+1)$ is the sum of two multiples of 3; therefore, it is also a multiple of 3. ■

3.7.1 Variations of Induction

Now we will discuss some of the variations of the principle of mathematical induction. The first simply allows for universes that are similar to $\mathbb{P}$ such as $\{-2, -1, 0, 1, ...\}$ or $\{5, 6, 7, 8, ...\}$.

Theorem 3.7.6 (Principle of Mathematical Induction (Generalized))**.** *If $p(n)$ is a proposition over $\{k_0, k_0+1, k_0+2, \ldots\}$, where k_0 is any integer, then $p(n)$ is a tautology if*

1. *$p(k_0)$ is true, and*

2. *for all $n \geq k_0$, $p(n) \Rightarrow p(n+1)$.*

Example 3.7.7 (A proof of the permutations formula)**.** In Chapter 2, we stated that the number of different permutations of k elements taken from an n element set, $P(n;k)$, can be computed with the formula $\frac{n!}{(n-k)!}$. We can prove this statement by induction on n. For $n \geq 0$, let $q(n)$ be the proposition

$$P(n;k) = \frac{n!}{(n-k)!} \text{ for all } k,\ 0 \leq k \leq n$$

.

Basis: $q(0)$ states that $P(0;0)$ if is the number of ways that 0 elements can be selected from the empty set and arranged in order, then $P(0;0) = \frac{0!}{0!} = 1$. This is true $--$ a general law in combinatorics is that there is exactly one way of doing nothing.

Induction: Assume that $q(n)$ is true for some natural number n. It is left for us to prove that this assumption implies that $q(n+1)$ is true. Suppose that we have a set of cardinality $n+1$ and want to select and arrange k of its elements. There are two cases to consider, the first of which is easy. If $k = 0$, then there is one way of selecting zero elements from the set; hence

$$P(n+1;0) = 1 = \frac{(n+1)!}{(n+1+0)!}$$

and the formula works in this case.

The more challenging case is to verify the formula when k is positive and less than or equal to $n+1$. Here we count the value of $P(n+1;k)$ by counting the number of ways that the first element in the arrangement can be filled and then counting the number of ways that the remaining $k-1$ elements can be filled in using the induction hypothesis.

There are $n+1$ possible choices for the first element. Since that leaves n elements to fill in the remaining $k-1$ positions, there are $P(n;k-1)$ ways of completing the arrangement. By the rule of products,

$$\begin{aligned} P(n+1;k) &= (n+1)P(n;k-1) \\ &= (n+1)\frac{n!}{(n-(k-1))!} \\ &= \frac{(n+1)n!}{(n-k+1)!} \\ &= \frac{(n+1)!}{((n+1)-k)!} \end{aligned}$$

■

A second variation allows for the expansion of the induction hypothesis. The course-of-values principle includes the previous generalization. It is also sometimes called *strong induction.*

Theorem 3.7.8 (The Course-of-Values Principle of Mathematical Induction)**.** *If $p(n)$ is a proposition over $\{k_0, k_0+1, k_0+2, \ldots\}$, where k_0 is any integer, then $p(n)$ is a tautology if*

1. *$p(k_0)$ is true, and*

2. *for all $n \geq k_0$, $p(k_0), p(k_0+1), ..., p(n) \Rightarrow p(n+1)$.*

Example 3.7.9 (Prime Factorization of Integers)**.** A prime number is defined as a positive integer that has exactly two positive divisors, 1 and itself. There are an infinite number of primes. The list of primes starts with $2, 3, 5, 7, 11, \ldots$. The proposition over $\{2, 3, 4, ...\}$ that we will prove here is $p(n)$: n can be written as the product of one or more primes. In most texts, the assertion that $p(n)$ is a tautology would appear as

Theorem 3.7.10 (Existence of Prime Factorizations)**.** *Every positive integer greater than or equal to 2 has a prime decomposition.*

If you were to encounter this theorem outside the context of a discussion of mathematical induction, it might not be obvious that the proof can be done by induction. Recognizing when an induction proof is appropriate is mostly a matter of experience. Now on to the proof!

Basis: Since 2 is a prime, it is already decomposed into primes (one of them).

Induction: Suppose that for some $k \geq 2$ all of the integers $2, 3, ..., k$ have a prime decomposition. Notice the course-of-value hypothesis. Consider $k+1$. Either $k+1$ is prime or it isn't. If $k+1$ is prime, it is already decomposed into primes. If not, then $k+1$ has a divisor, d, other than 1 and $k+1$. Hence, $k+1 = cd$ where both c and d are between 2 and k. By the induction hypothesis, c and d have prime decompositions, $c_1c_2 \cdots c_m$ and $d_1d_2 \cdots d_n$, respectively. Therefore, $k+1$ has the prime decomposition $c_1c_2 \cdots c_m d_1d_2 \cdots d_n$. ■

3.7.2 Historical Note

Mathematical induction originated in the late nineteenth century. Two mathematicians who were prominent in its development were Richard Dedekind and Giuseppe Peano. Dedekind developed a set of axioms that describe the positive integers. Peano refined these axioms and gave a logical interpretation to them. The axioms are usually called the Peano Postulates.

]Peano's Postulates The system of positive integers consists of a nonempty set, P; a least element of P, denoted 1; and a "successor function," s, with the properties

1. If $k \in \mathbb{P}$, then there is an element of $\mathbb{P}$ called the successor of k, denoted $s(k)$.
2. No two elements of $\mathbb{P}$ have the same successor.
3. No element of $\mathbb{P}$ has 1 as its successor.
4. If $S \subseteq \mathbb{P}$, $1 \in S$, and $k \in S \Rightarrow s(k) \in S$, then $S = \mathbb{P}$.

Notes:

- You might recognize $s(k)$ as simply being $k+1$.
- Axiom 4 is the one that makes mathematical induction possible. In an induction proof, we simply apply that axiom to the truth set of a proposition.

3.7.3 Exercises for Section 3.7

A Exercises

1. Prove that the sum of the first n odd integers equals n^2 .

Answer. We wish to prove that $P(n) : 1+3+5+\cdots+(2n-1) = n^2$ is true for $n \geqslant 1$. Recall that the nth odd positive integer is 2n - 1.
Basis: for $n = 1$, $P(n)$ is $1 = 1^2$, which is true

Induction: Assume that for some $n \geqslant 1, P(n)$ is true. Then:

$$\begin{aligned} 1+3+\cdots+(2(n+1)-1) &= (1+3+\cdots+(2n-1))+(2(n+1)-1) \\ &= n^2+(2n+1) \quad \text{by } P(n) \text{ and basic algebra} \\ &= (n+1)^2 \quad \blacksquare \end{aligned}$$

2. Prove that if $n \geq 1$, then $1(1!)+2(2!)+\cdots+n(n!) = (n+1)!-1$.

3. Prove that for $n \geq 1$: $\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$.

Answer. Proof:

- Basis: $1 = 1(2)(3)/6 = 1$
- Induction: $\sum_1^{n+1} k^2 = \sum_1^n k^2 + (n+1)^2$

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

$= \frac{(n+1)(2n^2+7n+6)}{6}$

$= \frac{(n+1)(n+2)(2n+3)}{6}$ $\blacksquare$

4. Prove that for $n \geq 1$: $\sum_{k=0}^{n} 2^k = 2^{n+1}-1$.

5. Use mathematical induction to show that for $n \geq 1$,

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

Answer. Basis: For $n = 1$, we observe that $\frac{1}{(1\cdot 2)} = \frac{1}{(1+1)}$
Induction: Assume that for some $n \geqslant 1$, the formula is true.
Then: $\frac{1}{(1\cdot 2)}+\cdots+\frac{1}{((n+1)(n+2))} = \frac{n}{(n+1)}+\frac{1}{((n+1)(n+2))}$

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

$= \frac{(n+1)^2}{((n+1)(n+2))}$

$= \frac{(n+1)}{(n+2)}$ $\blacksquare$

6. Prove that if $n \geq 2$, the generalized DeMorgan's Law is true:

$$\neg(p_1 \wedge p_2 \wedge ... \wedge p_n) \Leftrightarrow (\neg p_1) \vee (\neg p_2) \vee \cdots \vee (\neg p_n)$$

B Exercises

7. The number of strings of n zeros and ones that contain an even number of ones is 2^{n-1}. Prove this fact by induction for $n \geq 1$.

Answer. Let A_n be the set of strings of zeros and ones of length n (we assume that $|A_n| = 2^n$ is known). Let E_n be the set of the "even" strings, and $E_n^c =$ the odd strings. The problem is to prove that for $n \geqslant 1$, $|E_n| = 2^{n-1}$. Clearly, $|E_1| = 1$, and, if for some $n \geqslant 1, |E_n| = 2^{n-1}$, it follows that $|E_{n+1}| = 2^n$ by the following reasoning.
We partition E_{n+1} according to the first bit: $E_{n+1} = \{1s \mid s \in E_n^c\} \cup \{0s \mid s \in E_n\}$
Since $\{1s \mid s \in E_n^c\}$ and $\{0s \mid s \in E_n\}$ are disjoint, we can apply the addition law. Therefore,

$$\begin{aligned} |E_{n+1}| &= |E_n^c| + |E_n| \\ &= 2^{n-1} + (2^n - 2^{n-1}) = 2^n. \quad \blacksquare \end{aligned}$$

8. Let $p(n)$ be $8^n - 3^n$ is a multiple of 5. Prove that $p(n)$ is a tautology over $\mathbb{N}$.

9. Suppose that there are n people in a room, $n \geq 1$, and that they all shake hands with one another. Prove that $\frac{n(n-1)}{2}$ handshakes will have occurred.

Answer. Assume that for n persons ($n \geqslant 1$), $\frac{(n-1)n}{2}$ handshakes take place. If one more person enters the room, he or she will shake hands with n people,

$$\begin{aligned}\frac{(n-1)n}{2} + n &= \frac{n^2 - n + 2n}{2} \\ &= \frac{n^2 + n}{2} = \frac{n(n+1)}{2} \\ &= \frac{((n+1)-1)(n+1)}{2}\end{aligned}$$

Also, for $n = 1$, there are no handshakes, which matches the conjectured formula:

$$\frac{(1-1)(1)}{2} = 0 \quad \blacksquare.$$

10. Prove that it is possible to make up any postage of eight cents or more using only three- and five-cent stamps.

C Exercises

11. Generalized associativity. It is well known that if a_1, a_2, and a_3 are numbers, then no matter what order the sums in the expression $a_1 + a_2 + a_3$ are taken in, the result is always the same. Call this fact $p(3)$ and assume it is true. Prove using course-of-values induction that if a_1, a_2, ..., and a_n are numbers, then no matter what order the sums in the expression $a_1 + a_2 + \cdots + a_n$ are taken in, the result is always the same.

Solution. Let $p(n)$ be "$a_1 + a_2 + \cdots + a_n$ has the same value no matter how it is evaluated."
Basis: $a_1 + a_2 + a_3$ may be evaluated only two ways. Since $+$ is associative, $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$. Hence, $p(3)$ is true.
Induction: Assume that for some $n \geq 3$, $p(3), p(4), \ldots, p(n)$ are all true. Now consider the sum $a_1 + a_2 + \cdots + a_n + a_{n+1}$. Any of the n additions in this expression can be applied last. If the jth addition is applied last, we have $c_j = (a_1 + a_2 + \cdots + a_j) + (a_{j+1} + \cdots + a_{n+1})$. No matter how the expression to the left and right of the j^{th} addition are evaluated, the result will always be the same by the induction hypothesis, specifically $p(j)$ and $p(n+1-j)$. We now can prove that $c_1 = c_2 = \cdots = c_n$. If $i < j$,

$$\begin{aligned}c_i &= (a_1 + a_2 + \cdots + a_i) + (a_{i+1} + \cdots + a_{n+1}) \\ &= (a_1 + a_2 + \cdots + a_i) + ((a_{i+1} + \cdots + a_j) + (a_{j+1} + \cdots + a_{n+1}) \\ &= ((a_1 + a_2 + \cdots + a_i) + ((a_{i+1} + \cdots + a_j)) + (a_{j+1} + \cdots + a_{n+1}) \\ &= ((a_1 + a_2 + \cdots + a_j)) + (a_{j+1} + \cdots + a_{n+1}) \\ &= c_j \qquad \square\end{aligned}$$

12. Let S be the set of all numbers that can be produced by applying any of the rules below in any order a finite number of times.

- Rule 1: $\frac{1}{2} \in S$
- Rule 2: $1 \in S$
- Rule 3: If a and b have been produced by the rules, then $ab \in S$.

- Rule 4: If a and b have been produced by the rules, then $\frac{a+b}{2} \in S$.

Prove that $a \in S \Rightarrow 0 \leq a \leq 1$.

Hint. The number of times the rules are applied should be the integer that you do the induction on.

13. Proofs involving objects that are defined recursively are often inductive. A recursive definition is similar to an inductive proof. It consists of a basis, usually the simple part of the definition, and the recursion, which defines complex objects in terms of simpler ones. For example, if x is a real number and n is a positive integer, we can define x^n as follows:

- Basis: $x^1 = x$.
- Recursion: if $n \geq 2$, $x^n = x^{n-1}x$.

For example, $x^3 = x^2x = (x^1x)x = (xx)x$.
Prove that if $n, m \in \mathbb{P}$, $x^{m+n} = x^m x^n$. There is much more on recursion in Chapter 8.

Hint. Let $p(m)$ be the proposition that $x^{m+n} = x^m x^n$ for all $n \geq 1$.

Solution. For $m \geqslant 1$, let $p(m)$ be $x^{n+m} = x^n x^m$ for all $n \geqslant 1$. The basis for this proof follows directly from the basis for the definition of exponentiation.
Induction: Assume that for some $m \geqslant 1, p(m)$ is true. Then

$$\begin{aligned} x^{n+(m+1)} &= x^{(n+m)+1} && \text{by associativity of integer addition} \\ &= x^{n+m}x^1 && \text{by recursive definition} \\ &= x^n x^m x^1 && \text{induction hypothesis} \\ &= x^n x^{m+1} && \text{recursive definition} \quad \square \end{aligned}$$

14. Let S be a finite set and let P_n be defined recursively by $P_1 = S$ and $P_n = S \times P_{n-1}$ for $n \geq 2$.

- List the elements of P_3 for the case $S = \{a, b\}$.
- Determine the formula for $|P_n|$, given that $|S| = k$, and prove your formula by induction.

3.8 Quantifiers

As we saw in Section 3.6, if $p(n)$ is a proposition over a universe U, its truth set T_p is equal to a subset of U. In many cases, such as when $p(n)$ is an equation, we are most concerned with whether T_p is empty or not. In other cases, we might be interested in whether $T_p = U$; that is, whether $p(n)$ is a tautology. Since the conditions $T_p \neq \emptyset$ and $T_p = U$ are so often an issue, we have a special system of notation for them.

3.8.1 The Existential Quantifier

Definition 3.8.1 (The Existential Quantifier)**.** If $p(n)$ is a proposition over U with $T_p \neq \emptyset$, we commonly say "There exists an n in U such that $p(n)$ (is true)." We abbreviate this with the symbols $(\exists n)_U(p(n))$. The symbol $\exists$ is called the existential quantifier. If the context is clear, the mention of U is dropped: $(\exists n)(p(n))$.

Example 3.8.2 (Some examples of existential quantifiers)**.**

1. $(\exists k)_{\mathbb{Z}}(k^2 - k - 12 = 0)$ is another way of saying that there is an integer that solves the equation $k^2 - k - 12 = 0$. The fact that two such integers exist doesn't affect the truth of this proposition in any way.

2. $(\exists k)_{\mathbb{Z}}(3k = 102)$ simply states that 102 is a multiple of 3, which is true. On the other hand, $(\exists k)_{\mathbb{Z}}(3k = 100)$ states that 100 is a multiple of 3, which is false.

3. $(\exists x)_{\mathbb{R}}(x^2 + 1 = 0)$ is false since the solution set of the equation $x^2 + 1 = 0$ in the real numbers is empty. It is common to write $(\nexists x)_{\mathbb{R}}(x^2 + 1 = 0)$ in this case.

There are a wide variety of ways that you can write a proposition with an existential quantifier. 3.8.5 contains a list of different variations that could be used for both the existential and universal quantifiers.

3.8.2 The Universal Quantifier

Definition 3.8.3 (The Universal Quantifier)**.** If $p(n)$ is a proposition over U with $T_p = U$, we commonly say "For all n in U, $p(n)$ (is true)." We abbreviate this with the symbols $(\forall n)_U(p(n))$. The symbol $\forall$ is called the universal quantifier. If the context is clear, the mention of U is dropped: $(\forall n)(p(n))$.

Example 3.8.4 (Some Universal Quantifiers)**.**

1. We can say that the square of every real number is non-negative symbolically with a universal quantifier: $(\forall x)_{\mathbb{R}}(x^2 \geq 0)$.

2. $(\forall n)_{\mathbb{Z}}(n + 0 = 0 + n = n)$ says that the sum of zero and any integer n is n. This fact is called the identity property of zero for addition.

Universal Quantifier	Existential Quantifier
$(\forall n)_U(p(n))$	$(\exists n)_U(p(n))$
$(\forall n \in U)(p(n))$	$(\exists n \in U)(p(n))$
$\forall n \in U, p(n)$	$\exists n \in U$ such that $p(n)$
$p(n), \forall n \in U$	$p(n)$ is true for some $n \in U$
$p(n)$ is true for all $n \in U$	

Table 3.8.5: Notational Variations with Quantified Expressions

3.8.3 The Negation of Quantified Propositions

When you negate a quantified proposition, the existential and universal quantifiers complement one another.

Example 3.8.6 (Negation of an Existential Quantifier)**.** Over the universe of animals, define F(x) : x is a fish and W(x) : x lives in the water. We know that the proposition $W(x) \to F(x)$ is not always true. In other words, $(\forall x)(W(x) \to F(x))$ is false. Another way of stating this fact is that there exists an animal that lives in the water and is not a fish; that is,

$$\begin{aligned} \neg(\forall x)(W(x) \to F(x)) &\Leftrightarrow (\exists x)(\neg(W(x) \to F(x))) \\ &\Leftrightarrow (\exists x)(W(x) \wedge \neg F(x)) \end{aligned}$$

Note that the negation of a universally quantified proposition is an existentially quantified proposition. In addition, when you negate an existentially quantified proposition, you get a universally quantified proposition. Symbolically,

$$\neg((\forall n)_U(p(n))) \Leftrightarrow (\exists n)_U(\neg p(n)))$$
$$\neg((\exists n)_U(p(n))) \Leftrightarrow (\forall n)_U(\neg p(n)))$$

Table 3.8.7: Negation of Quantified Expressions

Example 3.8.8 (More Negations of Quantified Expressions)**.**

1. The ancient Greeks first discovered that $\sqrt{2}$ is an irrational number; that is, $\sqrt{2}$ is not a rational number. $\neg((\exists r)_{\mathbb{Q}}(r^2 = 2))$ and $(\forall r)_{\mathbb{Q}}(r^2 \neq 2)$ both state this fact symbolically.

2. $\neg((\forall n)_{\mathbb{P}}(n^2 - n + 41 \text{ is prime}))$ is equivalent to $(\exists n)_{\mathbb{P}}(n^2 - n + 41 \text{ is composite})$. They are both either true or false.

3.8.4 Multiple Quantifiers

If a proposition has more than one variable, then you can quantify it more than once. For example, if $p(x, y) : x^2 - y^2 = (x + y)(x - y)$ is a tautology over the set of all pairs of real numbers because it is true for each pair (x, y) in $\mathbb{R} \times \mathbb{R}$. Another way to look at this proposition is as a proposition with two variables. The assertion that $p(x, y)$ is a tautology could be quantified as $(\forall x)_{\mathbb{R}}((\forall y)_{\mathbb{R}}(p(x, y)))$ or $(\forall y)_{\mathbb{R}}((\forall x)_{\mathbb{R}}(p(x, y)))$

In general, multiple universal quantifiers can be arranged in any order without logically changing the meaning of the resulting proposition. The same is true for multiple existential quantifiers. For example, $p(x, y) : x + y = 4$ and $x - y - 2$ is a proposition over $\mathbb{R} \times \mathbb{R}$. $(\exists x)_{\mathbb{R}}((\exists y)_{\mathbb{R}}(x + y = 4 \text{ and } x - y = 2))$ and $(\exists y)_{\mathbb{R}}$ $((\exists x)_{\mathbb{R}}(x + y = 4 \text{ and } x - y = 2))$ are equivalent. A proposition with multiple existential quantifiers such as this one says that there are simultaneous values for the quantified variables that make the proposition true. A similar example is $q(x, y) : 2x - y - 2$ and $4x - 2y = 5$, which is always false; and the following are all equivalent

$$\begin{aligned}\neg((\exists x)_{\mathbb{R}}((\exists y)_{\mathbb{R}}(q(x, y)))) &\Leftrightarrow \neg(\exists y)_{\mathbb{R}}((\exists x)_{\mathbb{R}}(q(x, y))))\\ &\Leftrightarrow (\forall y)_{\mathbb{R}}(\neg((\exists x)_{\mathbb{R}}(q(x, y)))\\ &\Leftrightarrow ((\forall y)_{\mathbb{R}}((\forall x)_{\mathbb{R}}(\neg q(x, y))))\\ &\Leftrightarrow ((\forall x)_{\mathbb{R}}((\forall y)_{\mathbb{R}}(\neg q(x, y))))\end{aligned}$$

When existential and universal quantifiers are mixed, the order cannot be exchanged without possibly changing the meaning of the proposition. For example, let $\mathbb{R}^+$ be the positive real numbers, $x : (\forall a)_{\mathbb{R}^+}((\exists b)_{\mathbb{R}^+}(ab = 1))$ and $y : (\exists b)_{\mathbb{R}^+}((\forall a)_{\mathbb{R}^+}(ab = 1))$ have different logical values; x is true, while y is false.

Tips on Reading Multiply Quantified Propositions. It is understandable that you would find propositions such as x difficult to read. The trick to deciphering these expressions is to "peel" one quantifier off the proposition just as you would peel off the layers of an onion (but quantifiers shouldn't make you cry). Since the outermost quantifier in x is universal, x says that $z(a) : (\exists b)_{\mathbb{R}^+}(ab = 1)$ is true for each value that a can take on. Now take the time to select a value for a, like 6. For the value that we selected, we get $z(6) : (\exists b)_{\mathbb{R}^+}(6b = 1)$, which is obviously true since $6b = 1$ has a solution in the positive real numbers. We will get that same truth value no matter which positive real number we choose for a; therefore, $z(a)$

is a tautology over $\mathbb{R}^+$ and we are justified in saying that x is true. The key to understanding propositions like x on your own is to experiment with actual values for the outermost variables as we did above.

Now consider y. To see that y is false, we peel off the outer quantifier. Since it is an existential quantifier, all that y says is that some positive real number makes $w(b) : (\forall a)_{\mathbb{R}^+}(ab = 1)$ true. Choose a few values of b to see if you can find one that makes $w(b)$ true. For example, if we pick $b = 2$, we get $(\forall a)_{\mathbb{R}^+}(2a = 1)$, which is false, since $2a$ is almost always different from 1. You should be able to convince yourself that no value of b will make $w(b)$ true. Therefore, y is false.

Another way of convincing yourself that y is false is to convince yourself that $\neg y$ is true:

$$\begin{aligned}\neg((\exists b)_{\mathbb{R}^+}((\forall a)_{\mathbb{R}^+}(ab = 1))) &\Leftrightarrow (\forall b)_{\mathbb{R}^+}\neg((\forall a)_{\mathbb{R}^+}(ab = 1)) \\ &\Leftrightarrow (\forall b)_{\mathbb{R}^+}((\exists a)_{\mathbb{R}^+}(ab \neq 1))\end{aligned}$$

In words, for each value of b, a value for a that makes $ab \neq 1$. One such value is $a = \frac{1}{b} + 1$. Therefore, $\neg y$ is true.

3.8.5 Exercises for Section 3.8

A Exercises

1. Let $C(x)$ be "x is cold-blooded," let $F(x)$ be "x is a fish," and let $S(x)$ be "x lives in the sea."

(a) Translate into a formula: Every fish is cold-blooded.

(b) Translate into English: $(\exists x)(S(x) \wedge \neg F(x))$

(c) $(\forall x)(F(x) \rightarrow S(x))$.

Answer.

(a) $(\forall x)(F(x) \rightarrow G(x))$

(b) There are objects in the sea which are not fish.

(c) Every fish lives in the sea.

2. Let $M(x)$ be "x is a mammal," let $A(x)$ be "x is an animal," and let $W(x)$ be "x is warm-blooded."

(a) Translate into a formula: Every mammal is warm-blooded.

(b) Translate into English: $(\exists x)(A(x) \wedge (\neg M(x)))$.

3. Over the universe of books, define the propositions $B(x)$: x has a blue cover, $M(x)$: x is a mathematics book, $U(x)$: x is published in the United States, and $R(x, y)$: The bibliography of x includes y.
Translate into words:

(a) $(\exists x)(\neg B(x))$.

(b) $(\forall x)(M(x) \wedge U(x) \rightarrow B(x))$.

(c) $(\exists x)(M(x) \wedge \neg B(x))$.

(d) $(\exists y)((\forall x)(M(x) \rightarrow R(x, y)))$.Express using quantifiers:

(e) Every book with a blue cover is a mathematics book.

(f) There are mathematics books that are published outside the United States.

(g) Not all books have bibliographies.

Answer.

(a) There is a book with a cover that is not blue.

(b) Every mathematics book that is published in the United States has a blue cover.

(c) There exists a mathematics book with a cover that is not blue.

(d) There exists a book that appears in the bibliography of every mathematics book.

(e) $(\forall x)(B(x) \to M(x))$

(f) $(\exists x)(M(x) \wedge \neg U(x))$

(g) $(\exists x)((\forall y)(\neg R(x, y))$

4. Let the universe of discourse, U, be the set of all people, and let $M(x, y)$ be "x is the mother of y."
Which of the following is a true statement? Translate it into English.

(a) $(\exists x)_U((\forall y)_U(M(x, y)))$

(b) $(\forall y)_U((\exists x)_U(M(x, y)))$

(c) Translate the following statement into logical notation using quantifiers and the proposition $M(x, y)$: "Everyone has a grandmother."

5. Translate into your own words and indicate whether it is true or false that $(\exists u)_{\mathbb{Z}}(4u^2 - 9 = 0)$.

Answer. The equation $4u^2 - 9 = 0$ has a solution in the integers. (False)

6. Use quantifiers to say that $\sqrt{3}$ is an irrational number.

Hint. Your answer will depend on your choice of a universe

7. What do the following propositions say, where U is the power set of $\{1, 2, \ldots, 9\}$? Which of these propositions are true?

(a) $(\forall A)_U|A| \neq |A^c|$.

(b) $(\exists A)_U(\exists B)_U(|A| = 5, |B| = 5, \text{ and } A \cap B = \emptyset)$

(c) $(\forall A)_U(\forall B)_U(A - B = B^c - A^c)$

Answer.

(a) Every subset of U has a cardinality different from its complement. (True)

(b) There is a pair of disjoint subsets of U both having cardinality 5. (False)

(c) $A - B = B^c - A^c$ is a tautology. (True)

8. Use quantifiers to state that for every positive integer, there is a larger positive integer.

9. Use quantifiers to state that the sum of any two rational numbers is rational.

Answer. $(\forall a)_{\mathbb{Q}}(\forall b)_{\mathbb{Q}}(a + b$ is a rational number.)

10. Over the universe of real numbers, use quantifiers to say that the equation $a + x = b$ has a solution for all values of a and b.

Hint. You will need three quantifiers.

11. Let n be a positive integer. Describe using quantifiers:

(a) $x \in \bigcup_{k=1}^{n} A_k$

(b) $x \in \bigcap_{k=1}^{n} A_k$

Answer. Let $I = \{1, 2, 3, \ldots, n\}$

(a) $(\exists x)_I\,(x \in A_i)$

(b) $(\forall x)_I\,(x \in A_i)$

12. Prove that $(\exists x)(\forall y)(p(x,y)) \Rightarrow (\forall y)(\exists x)(p(x,y))$, but that converse is not true.

3.9 A Review of Methods of Proof

One of the major goals of this chapter is to acquaint the reader with the key concepts in the nature of proof in logic, which of course carries over into all areas of mathematics and its applications. In this section we will stop, reflect, and "smell the roses," so that these key ideas are not lost in the many concepts covered in logic. In Chapter 4 we will use set theory as a vehicle for further practice and insights into methods of proof.

3.9.1 Key Concepts in Proof

All theorems in mathematics can be expressed in form "If P then C" $(P \Rightarrow C)$, or in the form "C_1 if and only if C_2" $(C_1 \Leftrightarrow C_2)$. The latter is equivalent to "If C_1 then C_2," and "If C_2 then C_1."

In "If P then C," P is the premise (or hypothesis) and C is the conclusion. It is important to realize that a theorem makes a statement that is dependent on the premise being true.

There are two basic methods for proving $P \Rightarrow C$:

- *Directly:* Assume P is true and prove C is true.
- *Indirectly (or by contradiction):* Assume P is true and C is false and prove that this leads to a contradiction of some premise, theorem, or basic truth.

The method of proof for "If and only if" theorems is found in the law $(P \leftrightarrow C) \Leftrightarrow ((P \rightarrow C) \wedge (C \rightarrow P))$. Hence to prove an "If and only if" statement one must prove an "if . . . then ..." statement and its converse.

The initial response of most people when confronted with the task of being told they must be able to read and do proofs is often "Why?" or "I can't do proofs." To answer the first question, doing proofs or problem solving, even on the most trivial level, involves being able to read statements. First we must understand the problem and know the hypothesis; second, we must realize when we are done and we must understand the conclusion. To apply theorems or algorithms we must be able to read theorems and their proofs intelligently.

To be able to do the actual proofs of theorems we are forced to learn:

- the actual meaning of the theorems, and
- the basic definitions and concepts of the topic discussed.

For example, when we discuss rational numbers and refer to a number x as being rational, this means we can substitute a fraction $\frac{p}{q}$ in place of x, with the understanding that p and q are integers and $q \neq 0$. Therefore, to prove a theorem about rational numbers it is absolutely necessary that you know what a rational number "looks like."

It's easy to comment on the response, "I cannot do proofs." Have you tried? As elementary school students we may have been awe of anyone who could handle algebraic expressions, especially complicated ones. We learned by trying and applying ourselves. Maybe we cannot solve all problems in algebra or calculus, but we

are comfortable enough with these subjects to know that we can solve many and can express ourselves intelligently in these areas. The same remarks hold true for proofs.

3.9.2 The Art of Proving $P \Rightarrow C$

First one must completely realize what is given, the hypothesis. The importance of this is usually overlooked by beginners. It makes sense, whenever you begin any task, to spend considerable time thinking about the tools at your disposal. Write down the premise in precise language. Similarly, you have to know when the task is finished. Write down the conclusion in precise language. Then you usually start with P and attempt to show that C follows logically. How do you begin? Basically you attack the proof the same way you solve a complicated equation in elementary algebra. You may not know exactly what each and every step is but you must try something. If we are lucky, C follows naturally; if it doesn't, try something else. Often what is helpful is to work backward from C. Finally, we have all learned, possibly the hard way, that mathematics is a participating sport, not a spectator sport. One learns proofs by doing them, not by watching others do them. We give several illustrations of how to set up the proofs of several examples. Our aim here is not to prove the statements given, but to concentrate on the logical procedure.

Example 3.9.1 (The Sum of Odd Integers)**.** We will outline a proof that the sum of any two odd integers is even. Our first step will be to write the theorem in the familiar conditional form: If j and k are odd integers, then $j + k$ is even. The premise and conclusion of this theorem should be clear now. Notice that if j and k are not both odd, then the conclusion may or may not be true. Our only objective is to show thatthe truth of the premise forces the conclusion to be true. Therefore, we can express the integers j and k in the form that all odd integers take; that is:

$$n \in \mathbb{Z} \text{ is odd implies that } (\exists m \in \mathbb{Z})(n = 2m + 1)$$

This observation allows us to examine the sum j + k and to verify that it must be even.

Example 3.9.2 (The Square of an Even Integer)**.** Let $n \in \mathbb{Z}$. We will outline a proof that n^2 is even if and only if n is even.

Outline of a proof: Since this is an "If and only if" theorem we must prove two things:

1. ($\Rightarrow$) If n^2 is even, then n is even. To do this directly, assume that n^2 is even and prove that n is even. To do this indirectly, assume n^2 is even and that n is odd, and reach a contradiction. It turns out that the latter of the two approaches is easiest here.

2. ($\Leftarrow$) If n is even, then n^2 is even. To do this directly, assume that n is even and prove that n^2 is even.

Now that we have broken the theorem down into two parts and know what to prove, we proceed to prove the two implications. The final ingredient that we need is a convenient way of describing even integers. When we refer to an integer n (or m, or k,. . .) as even, we can always replace it with a product of the form $2q$, where q is an integer (more precisely, $(\exists q)_{\mathbb{Z}}(n = 2q)$). In other words, for an integer to be even it must have a factor of two in its prime decomposition.

Example 3.9.3 ($\sqrt{2}$ is irrational)**.** Our final example will be an outline of the proof that the square root of 2 is irrational (not an element of $\mathbb{Q}$). This is an example of the theorem that does not appear to be in the standard $P \Rightarrow C$ form. One

way to rephrase the theorem is: If x is a rational number, then $x^2 \neq 2$. A direct proof of this theorem would require that we verify that the square of every rational number is not equal to 2. There is no convenient way of doing this, so we must turn to the indirect method of proof. In such a proof, we assume that x is a rational number and that $x^2 = 2$. This will lead to a contradiction. In order to reach this contradiction, we need to use the following facts:

- A rational number is a quotient of two integers.
- Every fraction can be reduced to lowest terms, so that the numerator and denominator have no common factor greater than 1.
- If n is an integer, n^2 is even if and only if n is even.

3.9.3 Exercises for Section 3.9

A Exercises

1. Prove that the sum of two odd positive integers is even.

Answer. The given statement can be written in if ... , then ... format as: If x and y are two odd positive integers, then $x + y$ is an even integer.
Proof: Assume x and y are two positive odd integers. It can be shown that $x + y = 2 \cdot$ (some positive integer).
x odd $\Rightarrow x = 2m + 1$ for some $m \in \mathbb{P}$,
y odd $\Rightarrow y = 2n + 1$ for some $n \in \mathbb{P}$.
Then,

$$x + y = (2m + 1) + (2n + 1) = 2((m + n) + 1) = 2 \cdot (\text{some positive integer})$$

Therefore, $x + y$ is even. □

2. Write out a complete proof that if n is an integer, n^2 is even if and only if n is even.

3. Write out a complete proof that $\sqrt{2}$ is irrational.

Answer. Proof: (Indirect) Assume to the contrary, that $\sqrt{2}$ is a rational number. Then there exists $p, q \in \mathbb{Z}, (q \neq 0)$ where $\frac{p}{q} = \sqrt{2}$ and where $\frac{p}{q}$ is in lowest terms, that is, p and q have no common factor other than 1.
$\frac{p}{q} = \sqrt{2} \Rightarrow \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2 \Rightarrow p^2$is an even integer$\Rightarrow p$ is an even integer (see Exercise 2) 4 is a factor of $p^2 \Rightarrow q^2 \Rightarrow$ is even$\Rightarrow q$ is even. Hence both p and q have a common factor, namely 2, which is a contradiction. □

4. Prove that $\sqrt[3]{2}$ is an irrational number.

5. Prove that if x and y are real numbers such that $x + y \leq 1$, then either $x \leq \frac{1}{2}$ or $y \leq \frac{1}{2}$.

Answer. Proof: (Indirect) Assume $x, y \in \mathbb{R}$ and $x + y \leqslant 1$. Assume to the contrary that $\left(x \leqslant \frac{1}{2} \text{or} y \leqslant \frac{1}{2}\right)$ is false, which is equivalent to $x > \frac{1}{2} \text{and} y > \frac{1}{2}$. Hence $x + y > \frac{1}{2} + \frac{1}{2} = 1$. This contradicts the assumption that $x + y \leqslant 1$. ■

6. Use the following definition of absolute value to prove the given statements: If x is a real number, then the absolute value of x, $|x|$, is defined by:

$$|x| = \begin{cases} x & \text{if } x \text{ is greater than or equal to } 0 \\ -x & \text{if } n \text{ is less than } 0 \end{cases}$$

(a) For any real number x, $|x| \geq 0$. Moreover, $|x| = 0$ implies $x = 0$.

(b) For any two real numbers x and y, $|x| \cdot |y| = |xy|$.

(c) For any two real numbers x and y, $|x + y| \leq |x| + |y|$.

Chapter 4

More on Sets

In this chapter we shall look more closely at some basic facts about sets. One question we could ask ourselves is: Can we manipulate sets similarly to the way we manipulated expressions in basic algebra, or to the way we manipulated propositions in logic? In basic algebra we are aware that $a \cdot (b + c) = a \cdot b + a \cdot c$ for all real numbers a, b, and c. In logic we verified an analogue of this statement, namely, $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r))$, where $p, q,$ and r were arbitrary propositions. If A, B, and C are arbitrary sets, is $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$? How do we convince ourselves of it is truth, or discover that it is false? Let us consider some approaches to this problem, look at their pros and cons, and determine their validity. Many of the ideas expressed are true, in general, in mathematics. Later in this chapter, we introduce partitions of sets and minsets.

4.1 Methods of Proof for Sets

If A, B, and C are arbitrary sets, is it always true that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$? There are a variety of ways that we could attempt to prove that this distributive law for intersection over union is indeed true We start with a common "non-proof" and then work toward more acceptable methods.

4.1.1 Examples and Counterexamples

We could, for example, let $A = \{1, 2\}$, $B = \{5, 8, 10\}$, and $C = \{3, 2, 5\}$, and determine whether the distributive law is true for these values of A, B, and C. In doing this we will have only determined that the distributive law is true for this one example. It does not prove the distributive law for all possible sets A, B, and C and hence is an invalid method of proof. However, trying a few examples has considerable merit insofar as it makes us more comfortable with the statement in question, and indeed if the statement is not true for the example, we have disproved the statement.

Definition 4.1.1 (Counterexample)**.** An example that disproves a statement is called a counterexample.

Example 4.1.2 (Disproving distributivity of addition over multiplication)**.** From basic algebra we learned that multiplication is distributive over addition. Is addition distributive over multiplication? That is, is $a+(b \cdot c) = (a+b) \cdot (a+c)$ always true? If we choose the values $a = 3$, $b = 4$, and $c = 1$, we find that $3+(4 \cdot 1) \neq (3+4) \cdot (3+1)$. Therefore, this set of values serves as a counterexample to a distributive law of addition over multiplication.

4.1.2 Proof Using Venn Diagrams

In this method, we illustrate both sides of the statement via a Venn diagram and determine whether both Venn diagrams give us the same "picture," For example, the left side of the distributive law is developed in Figure 4.1.3 and the right side in Figure 4.1.4. Note that the final results give you the same shaded area.

The advantage of this method is that it is relatively quick and mechanical. The disadvantage is that it is workable only if there are a small number of sets under consideration. In addition, it doesn't work very well in a static environment like a book or test paper. Venn diagrams tend to work well if you have a potentially dynamic environment like a blackboard or video.

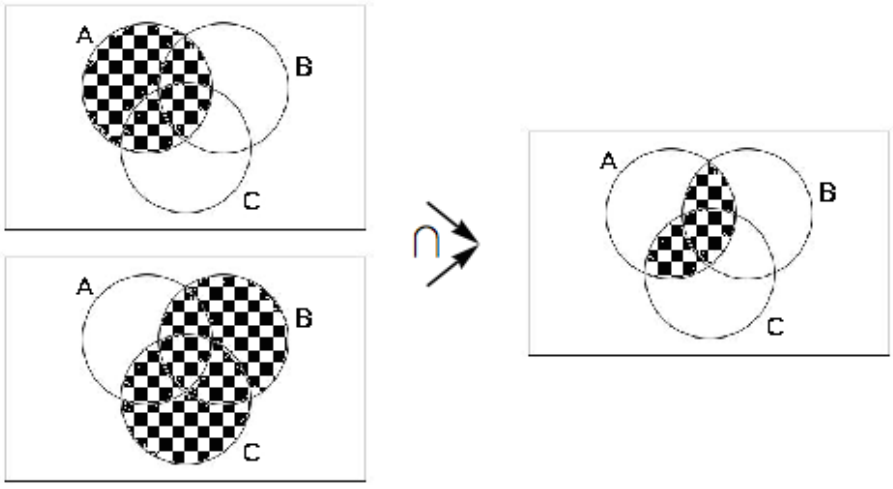


Figure 4.1.3: Development of the left side of the distributive law for sets

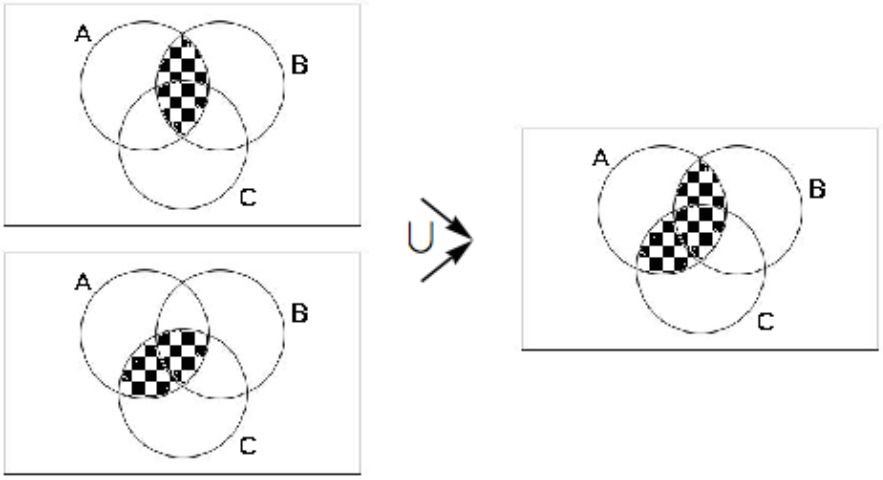


Figure 4.1.4: Development of the right side of the distributive law for sets

4.1.3 Proof using Set-membership Tables

Let A be a subset of a universal set U and let $u \in U$. To use this method we note that exactly one of the following is true: $u \in A$ or $u \notin A$. Denote the situation where $u \in A$ by 1 and that where $u \notin A$ by 0. Working with two sets, A and B, and if $u \in U$, there are four possible outcomes of "where u can be." What are they? The set-membership table for $A \cup B$ is:

A	B	$A \cup B$
0	0	0
0	1	1
1	0	1
1	1	1

Table 4.1.5: Membership Table for $A \cup B$

This table illustrates that $u \in A \cup B$ if and only if $a \in A$ or $u \in B$.

In order to prove the distributive law via a set-membership table, write out the table for each side of the set statement to be proved and note that if S and T are two columns in a table, then the set statement S is equal to the set statement T if and only if corresponding entries in each row are the same.

To prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, first note that the statement involves three sets, A, B, and C, So there are $2^3 = 8$ possibilities for the membership of an element in the sets.

A	B	C	$B \cup C$	$A \cap B$	$A \cap C$	$A \cap (B \cup C)$	$(A \cap B) \cup (A \cap C)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	0	1	1	1
1	1	0	1	1	0	1	1
1	1	1	1	1	1	1	1

Table 4.1.6: Membership table to prove the distributive law of intersection over union

Since each entry in Column 7 is the same as the corresponding entry in Column 8, we have shown that $A \cup (B \cup C) = (A \cap B) \cup (A \cap C)$ for any sets A, B, and C. The main advantage of this method is that it is mechanical. The main disadvantage is that it is reasonable to use only for a relatively small number of sets. If we are trying to prove a statement involving five sets, there are $2^5 = 32$ rows, which would test anyone's patience doing the work by hand.

4.1.4 Proof Using Definitions

This method involves using definitions and basic concepts to prove the given statement. This procedure forces one to learn, relearn, and understand basic definitions and concepts. It helps individuals to focus their attention on the main ideas of each topic and therefore is the most useful method of proof. One does not learn a topic by memorizing or occasionally glancing at core topics, but by using them in a variety of contexts. The word proof panics most people; however, everyone can become comfortable with proofs. Do not expect to prove every statement immediately. In fact, it is not our purpose to prove every theorem or fact encountered, only those that illustrate methods and/or basic concepts. Throughout the text we will focus in on main techniques of proofs. Let's illustrate by proving the distributive law.

Proof Technique 1. State or restate the theorem so you understand what is given (the hypothesis) and what you are trying to prove (the conclusion).

Theorem 4.1.7 (The Distributive Law of Intersection over Union)**.** *If A, B, and C are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

Proof. What we can assume: A, B, and C are sets.

What we are to prove: : $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Commentary: What types of objects am I working with: sets? real numbers? propositions? The answer is sets: sets of elements that can be anything you care to imagine. The universe from which we draw our elements plays no part in the proof of this theorem.

We need to show that the two sets are equal. Let's call them the left-hand set (LHS) and the right-hand set (RHS) To prove that $LHS = RHS$., we must prove two things: (a) $LHS \subseteq RHS$. and (b) $RHS \subseteq L.H.S$.

To prove part a and, similarly, part b, we must show that each element of LHS is an element of RHS. Once we have diagnosed the problem we are ready to begin.

We must prove: (a) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Let $x \in A \cap (B \cup C)$ to show $x \in (A \cap B) \cup (A \cap C)$:

$$\begin{aligned} x \in A \cap (B \cup C) &\Rightarrow x \in A \text{ and } (x \in B \text{ or } x \in C) \\ &\text{def. of union and intersection} \\ &\Rightarrow (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ &\text{distributive law of logic} \\ &\Rightarrow (x \in A \cap B) \text{ or } (x \in A \cap C) \\ &\text{def. of intersection} \\ &\Rightarrow (x \in (A \cap B) \cup (A \cap C) \\ &\text{def. of union} \end{aligned}$$

We must also prove (b) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

$$\begin{aligned} x \in (A \cap B) \cup (A \cap C) &\Rightarrow (x \in A \cap B) \text{or } (x \in A \cap C) \\ &\text{Why?} \\ &\Rightarrow (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C) \\ &\text{Why?} \\ &\Rightarrow x \in A \text{ and } (x \in B \text{ or } x \in C) \\ &\text{Why?} \\ &\Rightarrow x \in A \cap (B \cup C) \\ &\text{Why? } \blacksquare \end{aligned}$$

□

Proof Technique 2

1. To prove that $A \subseteq B$, we must show that if $x \in A$, then $x \in B$.

2. To prove that $A = B$, we must show:

   (a) $A \subseteq B$ and

   (b) $B \subseteq A$.

To further illustrate the Proof-by-Definition technique, let's prove the following theorem.

Theorem 4.1.8 (Another Proof using Definitions)**.** *Let A, B, and C be sets, then $A \times (B \cap C) = (A \times B) \cap (A \times C)$.*

Proof. Commentary; We again ask ourselves: What are we trying to prove? What types of objects are we dealing with? We realize that we wish to prove two facts: (a) $LHS \subseteq RHS$. and (b) $RHS \subseteq LHS$.

To prove part a, and similarly part b, we'll begin the same way. Let $\_\_\_ \in LHS$ to show $\_\_\_ \in RHS$. What should $\_\_\_$ be? What does a typical object in the LHS look like?

Now, on to the actual proof.

Let $(x, y) \in A \times (B \cap C)$ to prove$(x, y) \in (A \times B) \cap (A \times C)$:

$(x, y) \in A \times (B \cap C) \Rightarrow x \in A$ and $y \in (B \cap C)$

Why?

$\Rightarrow x \in A$ and $(y \in B$ and $y \in C)$

Why?

$\Rightarrow (x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$

Why?

$\Rightarrow (x, y) \in (A \times B)$ and $(x, y) \in (A \times C)$

Why?

$\Rightarrow (x, y) \in (A \times B) \cap (A \times C)$

Why?

(b) $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$:
Let $(x, y) \in (A \times B) \cap (A \times C)$ to prove $(x, y) \in A \cap (B \times C)$:

$(x, y) \in (A \times B) \cap (A \times C) \Rightarrow (x, y) \in A \times B$ and $(x, y) \in A \times C$

Why?

$\Rightarrow (x \in A$ and $y \in B)$ and $(x \in A$ and $y \in C)$

Why?

$\Rightarrow x \in A$ and $(y \in B$ and $y \in C)$

Why?

$\Rightarrow x \in A$ and $y \in (B \cap C)$

Why?

$\Rightarrow (x, y) \in A \times (B \cap C)$

Why? ■

□

4.1.5 Exercises for Section 4.1

1. Prove the following:

(a) Let A, B, and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(b) Let A and B be sets. Then $A - B = A \cap B^c$.

(c) Let $A, B,$ and C be sets. If $(A \subseteq B$ and$A \subseteq C)$ then $A \subseteq B \cap C$.

(d) Let A and B be sets. $A \subseteq B$ If and only if $B^c \subseteq A^c$.

(e) Let $A, B,$ and C be sets. If $A \subseteq B$ then $A \times C \subseteq B \times C$.

Answer.

(a) Assume that $x \in A$ (condition of the conditional conclusion $A \subseteq C$). Since $A \subseteq B$, $x \in B$ by the definition of $\subseteq$. $B \subseteq C$ and $x \in B$ implies that $x \in C$. Therefore, if $x \in A$, then $x \in C$. □

(b) (Proof that $A - B \subseteq A \cap B^c$) Let x be in $A - B$. Therefore, x is in A, but it is not in B; that is, $x \in A$ and $x \in B^c \Rightarrow x \in A \cap B^c$. □

(c) ($\Rightarrow$)Assume that $A \subseteq B$ and $A \subseteq C$. Let $x \in A$. By the two premises,$x \in B$ and $x \in C$. Therefore, by the definition of intersection, $x \in B \cap C$. □

(d) ($\Rightarrow$)(Indirect) Assume that $A \subseteq C$ and B^c is not a subset of A^c . Therefore, there exists $x \in B^c$ that does not belong to A^c. $x \notin A^c \Rightarrow x \in A$. Therefore, $x \in A$ and $x \notin B$, a contradiction to the assumption that $A \subseteq B$. □

2. Write the converse of parts (a), (c), and (e) of Exercise 1 and prove or disprove them.

3. Disprove the following, assuming $A, B,$ and C are sets:

(a) $A - B = B - A$.

(b) $A \times B = B \times A$.

(c) $A \cap B = A \cap C$ implies $B = C$.

Answer.

(a) If $A = \mathbb{Z}$ and $B = \emptyset$, $A - B = \mathbb{Z}$, while $B - A = \emptyset$.

(b) If $A = \{0\}$ and $B = \{1\}$, $(0, 1) \in A \times B$, but $(0, 1)$ is not in $B \times A$.

(c) Let $A = \emptyset$, $B = \{0\}$, and $C = \{1\}$.

4. Let $A, B,$ and C be sets. Write the following in "if . . . then . . ." language and prove:

(a) $x \in B$ is a sufficient condition for $x \in A \cup B$.

(b) $A \cap B \cap C = \emptyset$ is a necessary condition for $A \cap B = \emptyset$.

(c) $A \cup B = B$ is a necessary and sufficient condition for $A \subseteq B$.

5. Prove by induction that if A, B_1 B_2 , . . . , B_n, are sets, $n \geq 2$, then $A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$

Solution. Proof: Let $p(n)$ be

$$A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$$

Basis: We must show that $p(2) : A \cap (B_1 \cup B_2) = (A \cap B_1) \cup (A \cap B_2)$ is true. This was done by several methods in section 4.1.
Induction: Assume for some $n \geq 2$ that $p(n)$ is true. Then

$$\begin{aligned} A \cap (B_1 \cup B_2 \cup \cdots \cup B_{n+1}) &= A \cap ((B_1 \cup B_2 \cup \cdots \cup B_n) \cup B_{n+1}) \\ &= (A \cap (B_1 \cup B_2 \cup \cdots \cup B_n)) \cup (A \cap B_{n+1}) \quad \text{by } p(2) \\ &= ((A \cap B_1) \cup \cdots \cup (A \cap B_n)) \cup (A \cap B_{n+1}) \quad \text{by the induction hypothesis} \\ &= (A \cap B_1) \cup \cdots \cup (A \cap B_n) \cup (A \cap B_{n+1}) \quad \square \end{aligned}$$

4.2 Laws of Set Theory

The following basic set laws can be derived using either the Basic Definition or the Set-Membership approach and can be illustrated by Venn diagrams.

Commutative Laws	
(1) $A \cup B = B \cup A$	(1') $A \cap B = B \cap A$
Associative Laws	
(2) $A \cup (B \cup C) = (A \cup B) \cup C$	(2') $A \cap (B \cap C) = (A \cap B) \cap C$
Distributive Laws	
(3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	(3') $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Identity Laws	
(4) $A \cup \emptyset = \emptyset \cup A = A$.	(4') $A \cap U = U \cap A = A$
Complement Laws	
(5) $A \cup A^c = U$	(5') $A \cap A^c = \emptyset$
Idempotent Laws	
(6) $A \cup A = A$	(6') $A \cap A = A$
Null Laws	
(7) $A \cup U = U$	(7') $A \cap \emptyset = \emptyset$
Absorption Laws	
(8) $A \cup (A \cap B) = A$	(8') $A \cap (A \cup B) = A$
DeMorgan's Laws	
(9) $(A \cup B)^c = A^c \cap B^c$	(9') $(A \cap B)^c = A^c \cup B^c$
Involution Law	
(10) $(A^c)^c = A$	

Table 4.2.1: Basic Laws of Set Theory

It is quite clear that most of these laws resemble or, in fact, are analogues of laws in basic algebra and the algebra of propositions.

4.2.1 Proof Using Previously Proven Theorems

Once a few basic laws or theorems have been established, we frequently use them to prove additional theorems. This method of proof is usually more efficient than that of proof by Definition. To illustrate, let us prove the following Corollary to the Distributive Law. The term "corollary" is used for theorems that can be proven with relative ease from previously proven theorems.

Corollary 4.2.2 (A Corollary to the Distributive Law of Sets)**.** *Let A and B be sets. Then $(A \cap B) \cup (A \cap B^c) = A$.*

Proof.

$$\begin{aligned}(A \cap B) \cup (A \cap B^c) &= A \cap (B \cup B^c) \\ &\quad Why? \\ &= A \cap U \\ &\quad Why? \\ &= A \\ &\quad Why?\end{aligned}$$

□

4.2.2 Proof Using the Indirect Method/Contradiction

The procedure one most frequently uses to prove a theorem in mathematics is the Direct Method, as illustrated in Theorems 4.1.1 and 4.1.2. Occasionally there are situations where this method is not applicable. Consider the following:

Theorem 4.2.3 (An Indirect Proof in Set Theory)**.** *Let A, B, C be sets. If $A \subseteq B$ and $B \cap C = \emptyset$, then $A \cap C = \emptyset$.*

Commentary: The usual and first approach would be to assume $A \subseteq B$ and $B \cap C = \emptyset$ is true and to attempt to prove $A \cap C = \emptyset$ is true. To do this you would need to show that nothing is contained in the set $A \cap C$. Think about how you would show that something doesn't exist. It is very difficult to do directly.

The Indirect Method is much easier: If we assume the conclusion is false and we obtain a contradiction — then the theorem must be true. This approach is on sound logical footing since it is exactly the same method of indirect proof that we discussed in Subsection 3.5.1.2

Proof. Assume $A \subseteq B$ and $B \cap C = \emptyset$, and $A \cap C \neq \emptyset$. To prove that this cannot occur, let $x \in A \cap C$.

$$\begin{aligned} x \in A \cap C &\Rightarrow x \in A \text{ and } x \in C \\ &\quad Why? \\ &\qquad \Rightarrow x \in B \text{ and } x \in C \\ &\quad Why? \\ &\qquad \Rightarrow x \in B \cap C \\ &\quad Why? \end{aligned}$$

But this contradicts the second premise. Hence, the theorem is proven. ■ □

4.2.3 Exercises for Section 4.2"

1.

(a) Prove the associative law for intersection (Law 2') with a Venn diagram.

(b) Prove DeMorgan's Law (Law 9) with a membership table.

(c) Prove the Idempotent Law (Law 6) using basic definitions.

Answer.

(a)

(b)

A	B	A^c	B^c	$A \cup B$	$(A \cup B)^c$	$A^c \cap B^c$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

The last two columns are the same so the two sets must be equal.

(c) (i) $x \in A \cup A \Rightarrow (x \in A) \vee (x \in A)$ by the definition of $\cap$. $\Rightarrow x \in A$ by the idempotent law of logic. Therefore, $A \cup A \subseteq A$.
(ii) $x \in A \Rightarrow (x \in A) \vee (x \in A)$ by conjunctive addition $\Rightarrow x \in A \cup A$. Therefore, $A \subseteq A \cup A$ and so we have $A \cup A = A$. □

2.

(a) Prove the Absorption Law (Law 8') with a Venn diagram.

(b) Prove the Identity Law (Law 4) with a membership table.

(c) Prove the Involution Law (Law 10) using basic definitions.

3. Prove the following using the set theory laws, as well as any other theorems proved so far.

(a) $A \cup (B - A) = A \cup B$

(b) $A - B = B^c - A^c$

(c) $A \subseteq B, A \cap C \neq \emptyset \Rightarrow B \cap C \neq \emptyset$

(d) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

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

Answer. For all parts of this exercise, a reason should be supplied for each step. We have supplied reasons only for part a and left them out of the other parts to give you further practice.

(a)

(b)

$$\begin{aligned} A - B &= A \cap B^c \\ &= B^c \cap A \\ &= B^c \cap (A^c)^c \\ &= B^c - A^c \end{aligned}$$

(c) Select any element, $x \in A \cap C$. One such element exists since $A \cap C$ is not empty.

$$\begin{aligned} x \in A \cap C &\Rightarrow x \in A \wedge x \in C \\ &\Rightarrow x \in B \wedge x \in C \\ &\Rightarrow x \in B \cap C \\ &\Rightarrow B \cap C \neq \emptyset \quad \square \end{aligned}$$

(d)

$$\begin{aligned} A \cap (B - C) &= A \cap (B \cap C^c) \\ &= (A \cap B \cap A^c) \cup (A \cap B \cap C^c) \\ &= (A \cap B) \cap (A^c \cup C^c) \\ &= (A \cap B) \cap (A \cup C)^c \\ &= (A - B) \cap (A - C) \quad \square \end{aligned}$$

(e)

$$\begin{aligned} A - (B \cup C) &= A \cap (B \cup C)^c \\ &= A \cap (B^c \cap C^c) \\ &= (A \cap B^c) \cap (A \cap C^c) \\ &= (A - B) \cap (A - C) \quad \square \end{aligned}$$

4. Use previously proven theorems to prove the following.

(a) $A \cap (B \cap C)^c = (A \cap B^c) \cup (A \cap C^c)$

(b) $A \cap (B \cap (A \cap B)^c) = \emptyset$

(c) $(A \cap B) \cup B^c = A \cup B^c$

(d) $A \cup (B - C) = (A \cup B) - (C - A)$.

5. (Hierarchy of Set Operations) The rules that determine the order of evaluation in a set expression that involves more than one operation are similar to the rules for logic. In the absence of parentheses, complementations are done first, intersections second, and unions third. Parentheses are used to override this order. If the same operation appears two or more consecutive times, evaluate from left to right. In what order are the following expressions performed?

(a) $A \cup B^c \cap C$.
(b) $A \cap B \cup C \cap B$.
(c) $A \cup B \cup C^c$

Answer.

(a) $A \cup ((B^c) \cap C)$ (b) $(A \cap B) \cup (C \cap B)$ (c) $(A \cup B) \cup (C^c)$

6. There are several ways that we can use to format the proofs in this chapter. One that should be familiar to you from Chapter 3 is illustrated with the following alternate proof of part (a) in Theorem 4.1.7:

(1)	$x \in A \cap (B \cup C)$	Premise
(2)	$(x \in A) \wedge (x \in B \cup C)$	(1), definition of intersection
(3)	$(x \in A) \wedge ((x \in B) \vee (x \in C))$	(2), definition of union
(4)	$(x \in A) \wedge (x \in B) \vee (x \in A) \wedge (x \in C)$	(3), distribute $\wedge$ over $\vee$
(5)	$(x \in A \cap B) \vee (x \in A \cap C)$	(4), definition of intersection
(6)	$x \in (A \cap B) \cup (A \cap C)$	(5), definition of union ■

Table 4.2.4: An alternate format for the proof of Theorem 4.1.7

Prove part (b) of Theorem 4.1.8 and Theorem 4.2.3 using this format.

4.3 Minsets

Let B_1 and B_2 be subsets of a set A. Notice that the Venn diagram of Figure 4.3.1 is naturally partitioned into the subsets A_1, A_2, A_3, and A_4. Further we observe that A_1, A_2, A_3, and A_4 can be described in terms of B_1 and B_2 as follows:

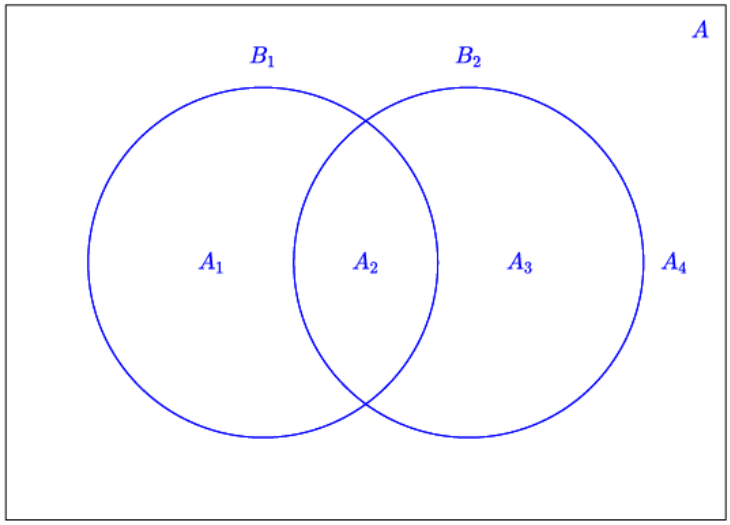


Figure 4.3.1: Venn Diagram of Minsets

$$A_1 = B_1 \cup B_2^c$$
$$A_2 = B_1 \cap B_2$$
$$A_3 = B_1^c \cap B_2$$
$$A_4 = B_1^c \cap B_2^c$$

Table 4.3.2: Minsets generated by two sets

Each A_i is called a minset generated by B_1 and B_2 . We note that each minset is formed by taking the intersection of two sets where each may be either B_k or its complement, B_k^c / Note also, given two sets, there are $2^2 = 4$ minsets.

Minsets are occasionally called *minterms*.

The reader should note that if we apply all possible combinations of the operations intersection, union, and complementation to the sets B_1 and B_2 of Figure 4.3.1, the smallest sets generated will be exactly the minsets, the minimum sets. Hence the derivation of the term minset.

Next consider the Venn diagram containing three sets, B_1, B_2, and B_3. Draw it right now and count the regions! What are the minsets generated by B_1, B_2, and B_3? How many are there? Following the procedures outlined above, we note that

$$B_1 \cap B_2 \cap B_3^c$$
$$B_1 \cap B_2^c \cap B_3$$
$$B_1 \cap B_2^c \cap B_3^c$$

are three of the $2^3 = 8$ minsets. What are the others?

Definition 4.3.3 (Minset)**.** Let $\{B_1, B_2, \ldots, B_n\}$ be a set of subsets of set A. Sets of the form $D_1 \cap D_2 \cap \cdots \cap D_n$, where each D_i, may be either B_i or B_i^c is called a minset generated by B_1, B_2,... and B_n.

Example 4.3.4 (A concrete example of some minsets)**.** Consider the following concrete example. Let $A = \{1, 2, 3, 4, 5, 6\}$ with subsets $B_1 = \{1, 3, 5\}$ and $B_2 = \{1, 2, 3\}$. How can we use set operations applied to B_1 and B_2 and produce a list of sets that contain elements of A efficiently without duplication? As a first attempt, we might try

$$B_1 \cap B_2 = \{1, 3\}$$
$$B_1^c = \{2, 4, 6\}, \text{ and}$$
$$B_2^c = \{4, 5, 6\}.$$

We have produced all elements of A but we have 4 and 6 repeated in two sets. In place of B_1^c and B_2^c, let's try $B_1^c \cap B_2$ and $B_1 \cap B_2^c$, respectively:

$$B_1^c \cap B_2 = \{2\} \text{ and}$$
$$B_1 \cap B_2^c = \{5\}.$$

We have now produced the elements 1, 2, 3, and 5 using $B_1 \cap B_2$, $B_1^c \cap B_2$ and $B_1 \cap B_2^c$ yet we have not listed the elements 4 and 6. Most ways that we could combine B_1 and B_2 such as $B_1 \cup B_2$ or $B_1 \cup B_2^c$ will produce duplications of listed elements and will not produce both 4 and 6. However we note that $B_1^c \cap B_2^c = \{4, 6\}$, exactly the elements we need. Each element of A appears exactly once in one of the four minsets $B_1 \cap B_2$, $B_1^c \cap B_2$, $B_1 \cap B_2^c$ and $B_1^c \cap B_2^c$. Hence, we have a partition of A.

Theorem 4.3.5 (Minset Partition Theorem)**.** *Let A be a set and let B_1, B_2 ... , B_n be subsets of A. The set of nonempty minsets generated by B_1, B_2 ... , B_n is a partition of A.*

Proof. □

One of the most significant fact about minsets is that any subset of A that can be obtained from B_1, B_2 ... , B_n, using the standard set operations can be obtained in a standard form by taking the union of selected minsets.

Definition 4.3.6 (Minset Normal Form)**.** A set is said to be in minset normal form when it is expressed as the union of zero or more distinct nonempty minsets.

Notes:

- The union of zero sets is the empty set, $\emptyset$. *Minset normal form is also called canonical form.*

Example 4.3.7 (Another Concrete Example of Minsets)**.** Let $U = \{-2, -1, 0, 1, 2\}$, $B_1 = \{0, 1, 2\}$, and $B_2 = \{0, 2\}$. Then

$$B_1 \cap B_2 = \{0, 2\}$$
$$B_1^c \cap B_2 = \emptyset$$
$$B_1 \cap B_2^c = \{1\}$$
$$B_1^c \cap B_2^c = \{-2, -1\}$$

In this case, there are only three nonempty minsets, producing the partition $\{\{0, 2\}, \{1\}, \{-2, -1\}\}$. An example of a set that could not be produced from just B_1 and B_2 is the set of even elements of U, $\{-2, 0, 2\}$. This is because -2 and -1 cannot be separated - they are in the same minset and any union of minsets either includes or excludes them both. In general, there are $2^3 = 8$ different minset normal forms because there are three nonempty minsets. This means that only 8 of the $2^5 = 32$ subsets of U could be generated from any two sets B_1 and B_2.

4.3.1 Exercises for Section 4.3

A Exercises

- **1.** Consider the subsets $A = \{1, 7, 8\}$, $B = \{1, 6, 9, 10\}$, and$C = \{1, 9, 10\}$, where $U = \{1, 2, ..., 10\}$.
  (a) List the nonempty minsets generated by $A, B,$ and C.
  (b) How many elements of the power set of U can be generated by A, B, and C? Compare this number with $| \mathcal{P}(U) |$. Give an example of one subset that cannot be generated by A, B, and C.

  Answer.
  (a) $\{1\}, \{2, 3, 4, 5\}, \{6\}, \{7, 8\}, \{9, 10\}$
  (b) 2^5 , as compared with 2^{10}. $\{1, 2\}$ is one of the 992 sets that can't be generated.

  2.
  (a) Partition $\{1, 2, ...9\}$ into the minsets generated by $B_1 = \{5, 6, 7\}$, $B_2 = \{2, 4, 5, 9\}$, and $B_3 = \{3, 4, 5, 6, 8, 9\}$.
  (b) How many different subsets of $\{1, 2, ..., 9\}$ can you create using $B_1, B_2,$ and B_3 with the standard set operations?
  (c) Do there exist subsets C_1, C_2, C_3whose minsets will generate every subset of $\{1, 2, ..., 9\}$?

3. Partition the set of strings of 0's and 1's of length two or less, using the minsets generated by $B_1 = \{s \mid s \text{ has length } 2\}$, and $B_2 = \{s \mid s \text{ starts with a } 0\}$.

Answer. $B_1 = \{00, 01, 10, 11\}$ and $B_2 = \{0, 00, 01\}$ generate minsets $\{00, 01\}, \{0\}, \{10, 11\}$, and $\{\lambda, 1\}$. Note: λ is the null string, which has length zero.

4. Let B_1, B_2, and B_3 be subsets of a universal set U,

(a) Symbolically list all minsets generated by B_1, B_2, and B_3.

(b) Illustrate with a Venn diagram all minsets obtained in part (a).

(c) Express the following sets in minset normal form: B_1^c, $B_1 \cap B_2$, $B_1 \cup B_2^c$.

5.

(a) Partition $A = \{0, 1, 2, 3, 4, 5\}$ with the minsets generated by $B_1 = \{0, 2, 4\}$ and $B_2 = \{1, 5\}$.

(b) How many different subsets of A can you generate from B_1 and B_2?

Answer.

(a) $B_1 \cap B_2 = \emptyset$, $B_1 \cap B_2^c = \{0, 2, 4\}$, $B_1^c \cap B_2 = \{1, 5\}$, $B_1^c \cap B_2^c = \{3\}$

(b) 2^3, since there are 3 nonempty minsets.

6. If $\{B_1, B_2, \ldots, B_n\}$ is a partition of A, how many minsets are generated by $B_1, B_2, \ldots, B_n$?

7. Prove Theorem 4.3.5

Answer. Let $a \in A$. For each i, $a \in B_i$, or $a \in {B_i}^c$, since $B_i \cup {B_i}^c = A$ by the complement law. Let $D_i = B_i$ if $a \in B_i$, and $D = {B_i}^c$ otherwise. Since a is in each D_i, it must be in the minset $D_1 \cap D_2 \cdots \cap D_n$. Now consider two different minsets $M_1 = D_1 \cap D_2 \cdots \cap D_n$, and $M_2 = G_1 \cap G_2 \cdots \cap G_n$, where each D_i and G_i is either B_i or ${B_i}^c$. Since these minsets are not equal, $D_i \neq G_i$, for some i. Therefore, $M_1 \cap M_2 = D_1 \cap D_2 \cdots \cap D_n \cap G_1 \cap G_2 \cdots \cap G_n = \emptyset$, since two of the sets in the intersection are disjoint. Since every element of A is in a minset and the minsets are disjoint, the nonempty minsets must form a partition of A. □

C Exercises

8. Let S be a finite set of n elements. Let B_i „ i = 1, 2, . . . , k be nonempty subsets of S. There are 2^{2^k} minset normal forms generated by the k subsets. The number of subsets of S is 2^n. Since we can make $2^{2^k} > 2^n$ by choosing $k \geq \log_2 n$, it is clear that two distinct minset normal-form expressions do not always equal distinct subsets of S. Even for $k < \log_2 n$, it may happen that two distinct minset normal-form expressions equal the same subset of S. Determine necessary and sufficient conditions for distinct normal-form expressions to equal distinct subsets of S.

4.4 The Duality Principle

In Section 4.2, we observed that each of the Table 4.2.1 labeled 1 through 9 had an analogue 1' through 9'. We notice that each of the laws in one column can be obtained from the corresponding law in the other column by replacing ∪ by ∩, ∩ by ∪, ∅ by U, U by ∅, and leaving the complement unchanged.

Definition 4.4.1 (Duality Principle for Sets.)**.** Let S be any identity involving sets and the operations complement, intersection and union, . If S* is obtained from S by making the substitutions $\cup \to \cap$, $\cap \to \cup$, $\emptyset \to U$, and $U \to \emptyset$, then the Statement S* is also true and it is called the dual of the Statement S.

Example 4.4.2 (Example of a dual)**.** The dual of $(A \cap B) \cup (A \cap B^c) = A$ is $(A \cup B) \cap (A \cup B^c) = A$.

One should not underestimate the importance of this concept. It gives us a whole second set of identities, theorems, and concepts. For example, we can consider the dual of *minsets* and *minset normal form* to obtain what is called *maxsets* and *maxset normal form*.

4.4.1 Exercises for Section 4.4

1. State the dual of:

(a) $A \cup (B \cap A) = A$.

(b) $A \cup ((B^c \cup A) \cap B)^c = U$

(c) $(A \cup B^c)^c \cap B = A^c \cap B$

Answer.

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

(b) $A \cap ((B^c \cap A) \cup B)^c = \emptyset$

(c) $(A \cap B^c)^c \cup B = A^c \cup B$

2. Examine Table 3.4.3 and then write a description of the principle of duality for logic.

3. Write the dual of:

(a) $p \vee \neg((\neg q \vee p) \wedge q) \Leftrightarrow 1$

(b) $(\neg(p \wedge (\neg q)) \vee q \Leftrightarrow (\neg p \vee q)$.

Answer.

(a) $(p \wedge \neg(\neg q \wedge p) \vee g)) \Leftrightarrow 0$

(b) $(\neg(p \vee (\neg q)) \wedge q) \Leftrightarrow ((\neg p) \wedge q)$

4. Use the principle of duality and the definition of minset to write the definition of maxset.

5. Let $A = \{1, 2, 3, 4, 5, 6\}$ and let $B_1 = \{1, 3, 5\}$ and $B_2 = \{1, 2, 3\}$.

(a) Find the maxsets generated by B_1 and B_2. Note the set of maxsets does not constitute a partition of A. Can you explain why?

(b) Write out the definition of maxset normal form.

(c) Repeat Exercise 4.3.1.4 for maxsets.

Answer. The maxsets are:

- $B_1 \cup B_2 = \{1, 2, 3, 5\}$
- $B_1 \cup {B_2}^c = \{1, 3, 4, 5, 6\}$
- ${B_1}^c \cup B_2 = \{1, 2, 3, 4, 6\}$
- ${B_1}^c \cup {B_2}^c = \{2, 4, 5, 6\}$

They do not form a partition of A since it is not true that the intersection of any two of them is empty. A set is said to be in **maxset normal form** when it is expressed as the intersection of distinct nonempty maxsets or it is the universal set U.

6. Is the dual of the expression in Exercise 4.1.5.5 ?

Chapter 5

Introduction to Matrix Algebra

The purpose of this chapter is to introduce you to matrix algebra, which has many applications. You are already familiar with several algebras: elementary algebra, the algebra of logic, the algebra of sets. We hope that as you studied the algebra of logic and the algebra of sets, you compared them with elementary algebra and noted that the basic laws of each are similar. We will see that matrix algebra is also similar. As in previous discussions, we begin by defining the objects in question and the basic operations.

5.1 Basic Definitions and Operations

5.1.1 Matrix Order and Equality

Definition 5.1.1 (matrix)**.** A matrix is a rectangular array of elements of the form

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{pmatrix}$$

A convenient way of describing a matrix in general is to designate each entry via its position in the array. That is, the entry a_{34} is the entry in the third row and fourth column of the matrix A. Depending on the situation, we will decide in advance to which set the entries in a matrix will belong. For example, we might assume that each entry a_{ij} ($1 \leq i \leq m$, $1 \leq j \leq n$) is a real number. In that case we would use $M_{m\times n}(\mathbb{R})$ to stand for the set of all m by n matrices whose entries are real numbers. If we decide that the entries in a matrix must come from a set S, we use $M_{m\times n}(S)$ to denote all such matrices.

Definition 5.1.2 (The Order of a Matrix)**.** A matrix A that has m rows and n columns is called an $m \times n$ (read "m by n") matrix, and is said to have order $m \times n$.

Since it is rather cumbersome to write out the large rectangular array above each time we wish to discuss the generalized form of a matrix, it is common practice to replace the above by $A = (a_{\text{ij}})$. In general, matrices are often given names that are capital letters and the corresponding lower case letter is used for individual entries. For example the entry in the third row, second column of a matrix called C would be c_{32}.

Example 5.1.3 (Orders of Some Matrices)**.** $A = \begin{pmatrix} 2 & 3 \\ 0 & -5 \end{pmatrix}$, $B = \begin{pmatrix} 0 \\ \frac{1}{2} \\ 15 \end{pmatrix}$, and $D = \begin{pmatrix} 1 & 2 & 5 \\ 6 & -2 & 3 \\ 4 & 2 & 8 \end{pmatrix}$ are 2×2, 3×1, and 3×3 matrices, respectively.

Since we now understand what a matrix looks like, we are in a position to investigate the operations of matrix algebra for which users have found the most applications.

First we ask ourselves: Is the matrix $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ equal to the matrix $B = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$? No, they are not because the corresponding entries in the second row, second column of the two matrices are not equal.

Next, is $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ equal to $B = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}$? No, although the corresponding entries in the first two columns are identical, B doesn't have a third column to compart to that of A. We formalize these observations in the following definition.

Definition 5.1.4 (Equality of Matrices)**.** A matrix A is said to be equal to matrix B (written $A = B$) if and only if:

1. A and B have the same order, and
2. all corresponding entries are equal: that is, $a_{\text{ij}} = b_{\text{ij}}$ for all appropriate i and j.

5.1.2 Matrix Addition and Scalar Multiplication

The first two operations we introduce are very natural and are not likely cause much confusion. The first is matrix addition. It seems natural that if $A = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 4 \\ -5 & 2 \end{pmatrix}$, then

$$A + B = \begin{pmatrix} 1+3 & 0+4 \\ 2-5 & -1+2 \end{pmatrix} = \begin{pmatrix} 4 & 4 \\ -3 & 1 \end{pmatrix}.$$

However, if $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 0 \\ 2 & 8 \end{pmatrix}$, is there a natural way to add them to give us $A + B$? No, the orders of the two matrices must be identical.

Definition 5.1.5 (Matrix Addition)**.** Let A and B be $m \times n$ matrices. Then $A + B$ is an $m \times n$ matrix where$(A + B)_{\text{ij}} = a_{\text{ij}} + b_{\text{ij}}$ (read "The ith jth entry of the matrix $A + B$ is obtained by adding the ith jth entry of A to the ith jth entry of B)." If the orders of A and B are not identical, $A + B$ is not defined.

In short, $A + B$ is defined if and only if A and B are of the same order.

Another frequently used operation is that of multiplying a matrix by a number, commonly called a scalar in this context. Scalars normally come from the same set as the entries in a matrix. For example, if $A \in M_{m \times n}(\mathbb{R})$, a scalar can be any real number.

Example 5.1.6 (A Scalar Product)**.** If $c = 3$ and if $A = \begin{pmatrix} 1 & -2 \\ 3 & 5 \end{pmatrix}$ and we wish to find cA, it seems natural to multiply each entry of A by 3 so that $3A = \begin{pmatrix} 3 & -6 \\ 9 & 15 \end{pmatrix}$, and this is precisely the way scalar multiplication is defined.

Definition 5.1.7 (Scalar Multiplication)**.** Let A be an $m \times n$ matrix and c a scalar. Then cA is the $m \times n$ matrix obtained by multiplying c times each entry of A; that is $(cA)_{ij} = ca_{ij}$.

5.1.3 Matrix Multiplication

For a video introduction to matrix multiplication, go to

http://faculty.uml.edu/klevasseur/ads2/videos/matrixmultiplication

A definition that is more awkward to motivate (and we will not attempt to do so here) is the product of two matrices. In time, the reader will see that the following definition of the product of matrices will be very useful, and will provide an algebraic system that is quite similar to elementary algebra.

Definition 5.1.8 (Matrix Multiplication)**.** Let A be an $m \times n$ matrix and let B be an $n \times p$ matrix. The product of $A$and B, denoted by AB, is an $m \times p$ matrix whose ith row jth column entry is

$$\begin{aligned}(AB)_{ij} &= a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} \\ &= \sum_{k=1}^{n} a_{ik}b_{kj}\end{aligned}$$

for $1 \leq i \leq m$ and $1 \leq j \leq p$.

The mechanics of computing one entry in the product of two matrices is illustrated in Figure 5.1.9.

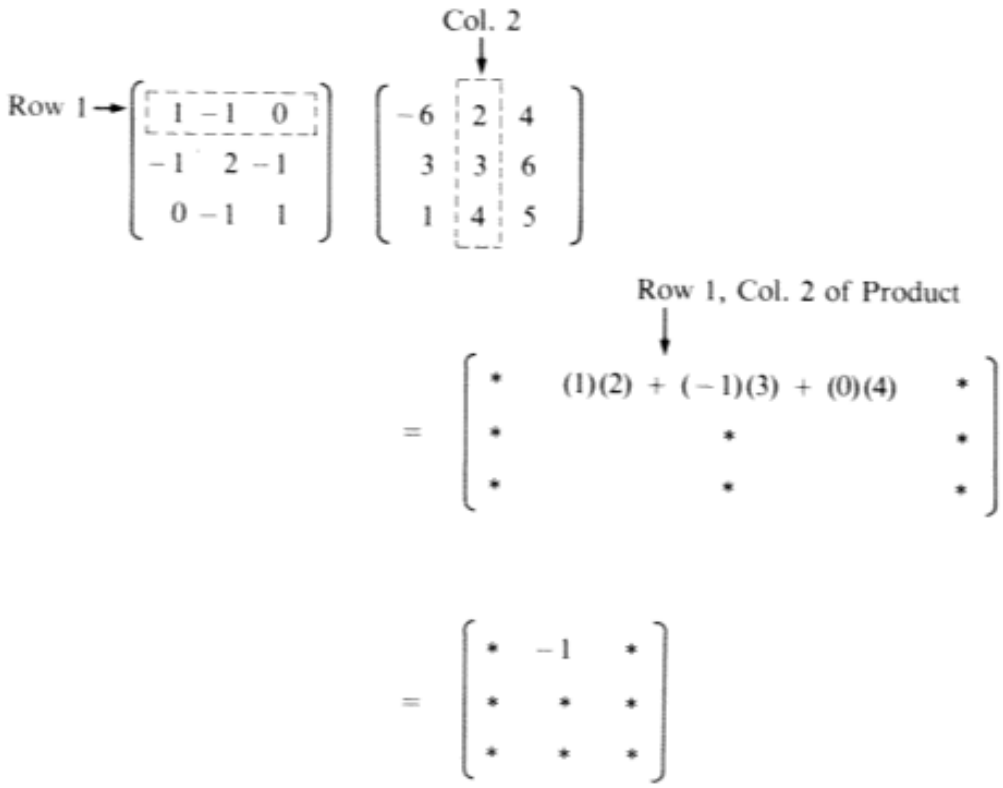


Figure 5.1.9: Computation of one entry in the product of two 3 by 3 matrices

The computation of a product can take a considerable amount of time in comparison to the time required to add two matrices. Suppose that A and B are $n \times n$ matrices; then $(AB)_{ij}$ is determined performing n multiplications and $n-1$ additions. The full product takes n^3 multiplications and $n^3 - n^2$ additions. This compares with n^2 additions for the sum of two $n \times n$ matrices. The product of two 10 by 10 matrices will require 1,000 multiplications and 900 additions, clearly a job that you would assign to a computer. The sum of two matrices requires a more modest 100 additions. This analysis is based on the assumption that matrix multiplication will be done using the formula that is given in the definition. There are more advanced methods that, in theory, reduce operation counts. For example, Strassen's algorithm (https://en.wikipedia.org/wiki/Strassen_algorithm) computes the product of two n by n matrices in $7 \cdot 7^{\log_2 n} - 6 \cdot 4^{\log_2 n} \approx 7n^{2.808}$ operations. There are practical issues involved in actually using the algorithm in many situations. For example, round-off error can be more of a problem than with the standard formula.

Example 5.1.10 (A Matrix Product)**.** Let $A = \begin{pmatrix} 1 & 0 \\ 3 & 2 \\ -5 & 1 \end{pmatrix}$, a 3×2 matrix, an let $B = \begin{pmatrix} 6 \\ 1 \end{pmatrix}$, a 2×1 matrix. Then AB is a 3×1 matrix:

$$(AB = \begin{pmatrix} 1 & 0 \\ 3 & 2 \\ -5 & 1 \end{pmatrix} \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 6 + 0 \cdot 1 \\ 3 \cdot 6 + 2 \cdot 1 \\ -5 \cdot 6 + 1 \cdot 1 \end{pmatrix} = \begin{pmatrix} 6 \\ 20 \\ -29 \end{pmatrix}$$

Remarks:

1. The product AB is defined only if A is an $m \times n$ matrix and B is an $n \times p$ matrix; that is, the two "inner" numbers must be the equal. Furthermore, the order of the product matrix AB is the "outer" numbers, in this case $m \times p$.

2. It is wise to first determine the order of a product matrix. For example, if A is a 3×2 matrix and B is a 2×2 matrix, then AB is a 3×2 matrix of the form

$$AB = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \\ c_{31} & c_{32} \end{pmatrix}$$

Then to obtain, for example, C_{31}, we multiply corresponding entries in the third row of A times the first column of B and add the results.

Example 5.1.11 (Multiplication with a diagonal matrix)**.** Let $A = \begin{pmatrix} -1 & 0 \\ 0 & 3 \end{pmatrix}$, and $B = \begin{pmatrix} 3 & 10 \\ 2 & 1 \end{pmatrix}$. Then

$$AB = \begin{pmatrix} -1 \cdot 3 + 0 \cdot 2 & -1 \cdot 10 + 0 \cdot 1 \\ 0 \cdot 3 + 3 \cdot 2 & 0 \cdot 10 + 3 \cdot 1 \end{pmatrix} = \begin{pmatrix} -3 & -10 \\ 6 & 3 \end{pmatrix}$$

The net effect is to multiply the first row of B by -1 and the second row of B by 3.

Note: $BA = \begin{pmatrix} -3 & 30 \\ -2 & 3 \end{pmatrix} \neq AB$. The columns of B are multiplied by -1 and 3 when the order is switched.

Remarks:

- An $n \times n$ matrix is called a *square matrix*.
- If A is a square matrix, AA is defined and is denoted by A^2 , and $AAA = A^3$, etc.
- The $m \times n$ matrices whose entries are all 0 are denoted by $\mathbf{0}_{m \times n}$, or simply $\mathbf{0}$, when no confusion arises regarding the order.

5.1.4 Exercises

1. Let $A = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 3 & -5 \end{pmatrix}$, and $C = \begin{pmatrix} 0 & 1 & -1 \\ 3 & -2 & 2 \end{pmatrix}$

(a) Compute AB and BA.

(b) Compute $A + B$ and $B + A$.

(c) If $c = 3$, show that $c(A + B) = cA + cB$.

(d) Show that $(AB)C = A(BC)$.

(e) Compute A^2C.

(f) Compute $B + \mathbf{0}$

(g) Compute $A\mathbf{0}_{2\times 2}$ and $\mathbf{0}_{2\times 2}A$, where $\mathbf{0}_{2\times 2}$ is the 2×2 zero matrix

(h) Compute $0A$, where 0 is the real number (scalar) zero.

(i) Let $c = 2$ and $d = 3$. Show that$(c + d)A = cA + dA$.

Answer. For parts c, d and i of this exercise, only a verification is needed. Here, we supply the result that will appear on both sides of the equality.

(a) $AB = \begin{pmatrix} -3 & 6 \\ 9 & -13 \end{pmatrix}$ $BA = \begin{pmatrix} 2 & 3 \\ -7 & -18 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 0 \\ 5 & -2 \end{pmatrix}$

(c) $\begin{pmatrix} 3 & 0 \\ 15 & -6 \end{pmatrix}$

(d) $\begin{pmatrix} 18 & -15 & 15 \\ -39 & 35 & -35 \end{pmatrix}$

(e) $\begin{pmatrix} -12 & 5 & -5 \\ 5 & -25 & 25 \end{pmatrix}$

(f) $B + 0 = B$

(g) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(h) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(i) $\begin{pmatrix} 5 & -5 \\ 10 & 15 \end{pmatrix}$

2. Let $A = \begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 5 \\ 3 & 2 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 2 & 3 \\ 1 & 1 & 2 \\ -1 & 3 & -2 \end{pmatrix}$, and $C = \begin{pmatrix} 2 & 1 & 2 & 3 \\ 4 & 0 & 1 & 1 \\ 3 & -1 & 4 & 1 \end{pmatrix}$
Compute, if possible;

(a) $A - B$

(b) AB

(c) $AC - BC$

(d) $A(BC)$

(e) $CA - CB$

(f) $C \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix}$

3. Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. Find a matrix B such that $AB = I$ and $BA = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Answer. $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/3 \end{pmatrix}$

4. Find AI and BI where I is as in Exercise 3, where $A = \begin{pmatrix} 1 & 8 \\ 9 & 5 \end{pmatrix}$ and $B = \begin{pmatrix} -2 & 3 \\ 5 & -7 \end{pmatrix}$. What do you notice?

5. Find A^3 if $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. What is A^{15} equal to?

Answer. $A^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 27 \end{pmatrix}$ $A^{15} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 32768 & 0 \\ 0 & 0 & 14348907 \end{pmatrix}$

6.

(a) Determine I^2 and I^3if $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

(b) What is I^n equal to for any $n \geq 1$?

(c) Prove your answer to part (b) by induction.

7.

(a) If $A = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, and $B = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$, show that $AX = B$ is a way of expressing the system $2x_1 + x_2 = 3$

$x_1 - x_2 = 1$ using matrices.

(b) Express the following systems of equations using matrices:

i. $2x_1 - x_2 = 4$

$x_1 + x_2 = 0$

ii. $x_1 + x_2 + 2x_3 = 1$

$x_1 + 2x_2 - x_3 = -1$

$x_1 + 3x_2 + x_3 = 5$

iii. $x_1 + x_2 \ = 3$

$x_2 \ = 5$

$x_1 \ + 3x_3 = 6$

Answer.

(a) $Ax = \begin{pmatrix} 2x_1 + 1x_2 \\ 1x_1 - 1x_2 \end{pmatrix}$ equals $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ if and only if both of the equalities $2x_1 + x_2 = 3$ and $x_1 - x_2 = 1$ are true.

(b) (i) $A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $B = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ $B = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}$

(d) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 3 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ $B = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}$

5.2 Special Types of Matrices

We have already investigated, in exercises in the previous section, one special type of matrix. That was the zero matrix, and found that it behaves in matrix algebra in an analogous fashion to the real number 0; that is, as the additive identity. We will now investigate the properties of a few other special matrices.

Definition 5.2.1 (Diagonal Matrix)**.** A square matrix D is called a diagonal matrix if $d_{ij} = 0$ whenever $i \neq j$.

Example 5.2.2 (Some diagonal matrices)**.** $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -5 \end{pmatrix}$, and $I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ are all diagonal matrices.

In the example above, the 3×3 diagonal matrix I whose diagonal entries are all 1's has the distinctive property that for any other 3×3 matrix A we have $AI = IA = A$. For example:

Example 5.2.3 (Multiplying by the Identity Matrix)**.** If $A = \begin{pmatrix} 1 & 2 & 5 \\ 6 & 7 & -2 \\ 3 & -3 & 0 \end{pmatrix}$, then

$$AI = \begin{pmatrix} 1 & 2 & 5 \\ 6 & 7 & -2 \\ 3 & -3 & 0 \end{pmatrix} \text{ and}$$

$$IA = \begin{pmatrix} 1 & 2 & 5 \\ 6 & 7 & -2 \\ 3 & -3 & 0 \end{pmatrix}.$$

In other words, the matrix I behaves in matrix algebra like the real number 1; that is, as a multiplicative identity. In matrix algebra, the matrix I is called simply the identity matrix. Convince yourself that if A is any $n \times n$ matrix $AI = IA = A$.

Definition 5.2.4 (Identity Matrix)**.** The $n \times n$ diagonal matrix I_n whose diagonal components are all 1's is called the identity matrix. If the context is clear, simply I.

In the set of real numbers we recall that, given a nonzero real number x, there exists a real number y such that $xy = yx = 1$. We know that real numbers commute under multiplication so that the two equations can be summarized as $xy = 1$. Further we know that $y = x^{-1} = \frac{1}{x}$. Do we have an analogous situation in $M_{n\times n}(\mathbb{R})$? Can we define the multiplicative inverse of an $n \times n$ matrix A? It seems natural to imitate the definition of multiplicative inverse in the real numbers.

Definition 5.2.5 (Matrix Inverse)**.** Let A be an $n \times n$ matrix. If there exists an $n \times n$ matrix B such that $AB = BA = I$, then B is a multiplicative inverse of A (called simply an inverse of A) and is denoted by A^{-1}

When we are doing computations involving matrices, it would be helpful to know that when we find A^{-1}, the answer we obtain is the only inverse of the given matrix. This would let us refer to *the* inverse of a matrix. We refrained from saying that in the definition, but the theorem below justifies it.

Remark: Those unfamiliar with the laws of matrices should go over the proof of Theorem 5.4.1 after they have familiarized themselves with the Laws of Matrix Algebra in Section 5.5.

Theorem 5.2.6 (Inverses are unique)**.** *The inverse of an $n \times n$ matrix A, when it exists, is unique.*

Proof. Let A be an $n \times n$ matrix. Assume to the contrary, that A has two (different) inverses, say B and C. Then

$$\begin{aligned} B &= BI \\ &\quad \text{Identity property of } I \\ &= B(A) \\ &\quad \text{Assumption that } C \text{ is an inverse of } A \\ &= (BA)C \\ &\quad \text{Associativity of matrix multiplication} \\ &= IC \\ &\quad \text{Assumption that } B \text{ is an inverse of } A \\ &= C \\ &\quad \text{Identity property of } I \end{aligned}$$

□

Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. What is A^{-1} ? Without too much difficulty, by trial and error, we determine that $A^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{3} \end{pmatrix}$. This might lead us to guess that the inverse is found by taking the reciprocal of all nonzero entries of a matrix. Alas, it isn't that easy!

If $A = \begin{pmatrix} 1 & 2 \\ -3 & 5 \end{pmatrix}$, the "reciprocal rule" would tell us that the inverse of A is $B = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{-1}{3} & \frac{1}{5} \end{pmatrix}$. Try computing AB and you will see that you don't get the identity matrix. So, what *is* A^{-1}? In order to understand more completely the notion of the inverse of a matrix, it would be beneficial to have a formula that would enable us to compute the inverse of at least a 2×2 matrix. To do this, we introduce the definition of the determinant of a 2×2 matrix. Appendix A gives a more complete description of the determinant of a 2×2 and higher-order matrices.

Definition 5.2.7 (Determinant of a 2 by 2 Matrix)**.** Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The determinant of A is the number $\det A = ad - bc$.

In addition to $\det A$, common notation for the determinant of matrix $A$is $|A|$. This is particularly common when writing outthe whole matrix, which case we would write $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ for the determinant of the general 2×2 matrix.

Example 5.2.8 (Some Determinants of two by two matrices)**.** If $A = \begin{pmatrix} 1 & 2 \\ -3 & 5 \end{pmatrix}$ then $\det A = 1 \cdot 5 - 2 \cdot (-3) = 11$.

If $B = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ then $\det B = 1 \cdot 4 - 2 \cdot 2 = 0$

Theorem 5.2.9 (Inverse of 2 by 2 Matrix)**.** *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *If* $\det A \neq 0$, *then* $A^{-1} = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Proof. □

Example 5.2.10 (Finding Inverses)**.** Can we find the inverses of the matrices in Example 5.2.8?

If $A = \begin{pmatrix} 1 & 2 \\ -3 & 5 \end{pmatrix}$ then

$$A^{-1} = \frac{1}{11} \begin{pmatrix} 5 & -2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} \frac{5}{11} & -\frac{2}{11} \\ \frac{3}{11} & \frac{1}{11} \end{pmatrix}$$

The reader should verify that $AA^{-1} = A^{-1}A = I$.

The second matrix, B has a determinant equal to zero. We we tried to apply the formula in Theorem 5.2.9, we would be dividing by zero. For this reason, the formula can't be applied and in fact B^{-1} does not exist.

Remarks:

- In general, if A is a 2×2 matrix and if $\det A = 0$, then A^{-1} does not exist.

- A formula for the inverse of $n \times n$ matrices $n \geq 3$ can be derived that also involves $\det A$, Hence, in general, if the determinant of a matrix is zero, the matrix does not have an inverse. However the formula for even a 3×3 matrix is very long and is not the most efficient way to compute the inverse of a matrix.
- In Chapter 12 we will develop a technique to compute the inverse of a higher-order matrix, if it exists.
- Matrix inversion comes first in the hierarchy of matrix operations; therefore, AB^{-1} is $A(B^{-1})$.

5.2.1 Exercises

1. For the given matrices A find A^{-1} if it exists and verify that $AA^{-1} = A^{-1}A = I$. If A^{-1} does not exist explain why.

(a) $A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$

(b) $A = \begin{pmatrix} 6 & -3 \\ 8 & -4 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$

(d) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

(e) Use the definition of the inverse of a matrix to find A^{-1}: $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & -5 \end{pmatrix}$

Answer.

(a) $\begin{pmatrix} -1/5 & 3/5 \\ 2/5 & -1/5 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$

(c) No inverse exists.

(d) $A^{-1} = A$

(e) $\begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1/5 \end{pmatrix}$

2. For the given matrices A find A^{-1} if it exists and verify that $AA^{-1} = A^{-1}A = I$ If A^{-1} does not exist explain why.

(a) $A = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$

(b) $A = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$

(d) $A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, were $a > b > 0$.

3.

(a) Let $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & -3 \\ 2 & 1 \end{pmatrix}$. Verify that $(AB)^{-1} = B^{-1}A^{-1}$.

(b) Let A and B be $n \times n$ invertible matrices. Prove that $(AB)^{-1} = B^{-1}A^{-1}$. Why is the right side of the above statement written "backwards"? Is this necessary? Hint: Use Theorem 5.2.6

Answer. Let A and B be n by n invertible matrices.

$$\begin{aligned}\left(B^{-1}A^{-1}\right)(AB) &= \left(B^{-1}\right)\left(A^{-1}(AB)\right)\\ &= \left(B^{-1}\right)\left(\left(A^{-1}A\right)B\right)\\ &= \left(\left(B^{-1}\right)IB\right)\\ &= B^{-1}(B)\\ &= I\end{aligned}$$

Similarly, $(AB)\left(B^{-1}A^{-1}\right) = I$.
By Theorem 5.2.6, $B^{-1}A^{-1}$ is the only inverse of AB. If we tried to invert AB with $A^{-1}B^{-1}$, we would be unsuccessful since we cannot rearrange the order of the matrices.

4. Let Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Derive the formula for A^{-1}.

5. (Linearity of Determinants)

(a) Let A and B be as in Exercise 5.2.1.3. Show that $\det(AB) = (\det A)(\det B)$.

(b) It can be shown that the statement in part (a) is true for all $n \times n$ matrices. Let A be any invertible $n \times n$ matrix. Prove that $\det\left(A^{-1}\right) = (\det A)^{-1}$. Note: The determinant of the identity matrix I_n is 1 for all n.

(c) Verify that the equation in part (b) is true for the matrix in exercise l(a) of this section.

Answer. $1 = \det I = \det\left(AA^{-1}\right) = \det A \ \det A^{-1}$. Now solve for $\det A^{-1}$.

6. Prove by induction that for $n \geq 1$, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & b^n \end{pmatrix}$.

7. Use the assumptions in Exercise 5.2.1.5 to prove by induction that if $n \geq 1$, $\det\left(A^n\right) = (\det A)^n$.

Answer. Basis: $(n = 1) : \det A^1 = \det A = (\det A)^1$
Induction: Assume $\det A^n = (\det A)^n$ for some $n \geq 1$.

$$\begin{aligned}\det A^{n+1} &= \det\left(A^n A\right) && \text{by the definition of exponents}\\ &= \det\left(A^n\right)\det(A) && \text{by exercise 5}\\ &= detA)^n(\det A) && \text{by the induction hypothesis}\\ &= (\det A)^{n+1}\end{aligned}$$

8. Prove: If the determinant of a matrix A is zero, then A does not have an inverse. Hint: Use the indirect method of proof and exercise 5.

9.

(a) Let A, B, and D be $n \times n$ matrices. Assume that B is invertible. If $A = BDB^{-1}$, prove by induction that $A^m = BD^mB^{-1}$ is true for $m \geq 1$.

(b) Given that $A = \begin{pmatrix} -8 & 15 \\ -6 & 11 \end{pmatrix} = B \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} B^{-1}$ where $B = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ what is A^{10}?

Answer.

(a) Assume $A = BDB^{-1}$
Basis: $(m = 1)$: $A^1 = A = BD^1B^{-1}$ is given.
Induction: Assume that for some positive integer m, $A^m = BD^mB^{-1}$

$$\begin{aligned} A^{m+1} &= A^m A \\ &= (BD^mB^{-1})(BDB^{-1}) \quad \text{by the induction hypothesis} \\ &= (BD^m(B^{-1}B)(DB^{-1}) \quad \text{by associativity} \\ &= BD^mDB^{-1} \quad \text{by the definition of inverse} \\ &= BD^{m+1}B^{-1} \quad \square \end{aligned}$$

(b) $A^{10} = BD^{10}B^{-1} = \begin{pmatrix} -9206 & 15345 \\ -6138 & 10231 \end{pmatrix}$

5.3 Laws of Matrix Algebra

The following is a summary of the basic laws of matrix operations. Assume that the indicated operations are defined; that is, that the orders of the matrices A, B and C are such that the operations make sense.

(1)	Communtative Law of Addition	$A + B = B + A$
(2)	Associative Law of Addition	$A + (B + C) = (A + B) + C$
(3)	Distrutive Law of a Scalar over Matrices	$c(A + B) = cA + cB$, where $c \in \mathbb{R}$.
(4)	Distrutive Law of Scalars over a Matrix	$(c_1 + c_2)\, A = c_1A + c_2A$, where $c_1, c_2 \in \mathbb{R}$.
(5)	Associative Law of Scalar Multiplication	$c_1\,(c_2A) = (c_1 \cdot c_2)\, A$, where $c_1, c_2 \in \mathbb{R}$.
(6)	Zero Matrix Annihilates all Products	$\mathbf{0}A = \mathbf{0}$, where $\mathbf{0}$ is the zero matrix.
(7)	Zero Scalar Annihilates all Products	$0A = \mathbf{0}$, where 0 on the left is the scalar zero.
(8)	Zero Matrix is an identity for Addition	$A + 0 = A$.
(9)	Negation produces additive inverses	$A + (-1)A = \mathbf{0}$.
(10)	Right Distrutive Law of Matrix Multiplication	$A(B + C) = AB + AC$.
(11)	Left Distrutive Law of Matrix Multiplication	$(B + C)A = BA + CA$.
(12)	Associative Law of Multiplication	$A(BC) = (AB)C$.
(13)	Identity Matrix is a Multiplicative Identity	$IA = A$ and $AI = A$.
(14)	Involution Property of Inverses	If A^{-1} exists,$\left(A^{-1}\right)^{-1} = A$.
(15)	Inverse of Product Rule	If A^{-1} and B^{-1} exist, $(AB)^{-1} = B^{-1}A^{-1}$

Table 5.3.1: Laws of Matrix Algebra

Example 5.3.2 (More Precise Statement of one Law)**.** If we wished to write out each of the above laws more completely, we would specify the orders of the matrices. For example, Law 10 should read:

> Let A, B, and C be $m \times n$, $n \times p$, and $n \times p$ matrices, respectively, then $A(B + C) = AB + AC$

Remarks:

- Notice the absence of the "law" $AB = BA$. Why? It is missing because it isn't true!
- Is it really necessary to have both a right (No. 11) and a left (No. 10) distributive law? Why?Yes, because matrix multiplication is not commutative.

5.3.1 Exercises

1. Rewrite the above laws specifying as in Example 5.3.2 the orders of the matrices.

Answer. Let A and B be m by n matrices. Then $A + B = B + A$,Let A, B, and C be m by n matrices. Then $A + (B + C) = (A + B) + C$.Let A and B be m by n matrices, and let $c \in \mathbb{R}$. Then $c(A + B) = cA + cB$,Let A be an m by n matrix, and let $c_1, c_2 \in \mathbb{R}$. Then $(c_1 + c_2) A = c_1 A + c_2 A$.Let A be an m by n matrix, and let $c_1, c_2 \in \mathbb{R}$. Then $c_1 (c_2 A) = (c_1 c_2) A$Let $\mathbf{0}$ be the zero matrix, of size m by n, and let A be a matrix of size n by r. Then $\mathbf{0}A = \mathbf{0} =$ the m by r zero matrix.Let A be an m by n matrix, and $0 =$ the number zero. Then $0A = 0 =$ the m by n zero matrix.Let A be an m by n matrix, and let $\mathbf{0}$ be the m by n zero matrix. Then $A + \mathbf{0} = A$. Let A be an m by n matrix. Then $A + (-1)A = \mathbf{0}$, where $\mathbf{0}$ is the m by n zero matrix.Let A, B, and C be m by n, n by r, and n by r matrices respectively. Then $A(B + C) = AB + AC$.Let A, B, and C be m by n, r by m, and r by m matrices respectively. Then $(B+C)A = BA+CA$.Let A, B, and C be m by n, n by r, and r by p matrices respectively. Then $A(BC) = (AB)C$.Let A be an m by n matrix, I_m the m by m identity matrix, and I_n the n by n identity matrix. Then $I_m A = A I_n = A$Let A be an n by n matrix. Then if A^{-1} exists, $\left(A^{-1}\right)^{-1} = A$.Let A and B be n by n matrices. Then if A^{-1} and B^{-1} exist, $(AB)^{-1} = B^{-1}A^{-1}$.

2. Verify each of the Laws of Matrix Algebra using examples.

3. Let $A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 7 & 6 \\ 2 & -1 & 5 \end{pmatrix}$, and $C = \begin{pmatrix} 0 & -2 & 4 \\ 7 & 1 & 1 \end{pmatrix}$. Compute the following as efficiently as possible by using any of the Laws of Matrix Algebra:

(a) $AB + AC$

(b) A^{-1}

(c) $A(B + C)$

(d) $\left(A^2\right)^{-1}$

(e) $(C + B)^{-1}A^{-1}$

Answer.

(a) $AB + AC = \begin{pmatrix} 21 & 5 & 22 \\ -9 & 0 & -6 \end{pmatrix}$

(b) $A(B + C) = AB + BC$

(c) $A^{-1} = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} = A$

(d) $\left(A^2\right)^{-1} = (AA)^{-1} = (A^{-1}A) = I^{-1} = I$ by part c

4. Let $A = \begin{pmatrix} 7 & 4 \\ 2 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & 5 \\ 2 & 4 \end{pmatrix}$. Compute the following as efficiently as possible by using any of the Laws of Matrix Algebra:

(a) AB

(b) $A + B$

(c) $A^2 + AB + BA + B^2$

(d) $B^{-1}A^{-1}$

(e) $A^2 + AB$

5. Let A and B be $n \times n$ matrices of real numbers. Is $A^2 - B^2 = (A - B)(A + B)0008$? Explain

5.4 Matrix Oddities

We have seen that matrix algebra is similar in many ways to elementary algebra. Indeed, if we want to solve the matrix equation $AX = B$ for the unknown X, we imitate the procedure used in elementary algebra for solving the equation $ax = b$. Notice how exactly the same properties are used in the following detailed solutions of both equations.

Equation in the real algebra		Equation in matrix algebra
$ax = b$		$AX = B$
$a^{-1}(ax) = a^{-1}b$ if $a \neq 0$		$A^{-1}(AX) = A^{-1}B$ if A^{-1} exists
$\left(a^{-1}a\right)x = a^{-1}b$	Associative Property	$\left(A^{-1}A\right)X = A^{-1}B$
$1x = a^{-1}b$	Inverse Property	$IX = A^{-1}B$
$x = a^{-1}b$	Identity Property	$X = A^{-1}B$

Certainly the solution process for $AX = B$ is the same as that of $ax = b$.

The solution of $xa = b$ is $x = ba^{-1} = a^{-1}b$. In fact, we usually write the solution of both equations as x = $\frac{b}{a}$. In matrix algebra, the solution of $XA = B$ is $X = BA^{-1}$, which is not necessarily equal to $A^{-1}B$. So in matrix algebra, since the commutative law (under multiplication) is not true, we have to be more careful in the methods we use to solve equations.

It is clear from the above that if we wrote the solution of $AX = B$ as $X = \frac{B}{A}$, we would not know how to interpret $\frac{B}{A}$. Does it mean $A^{-1}B$ or BA^{-1}? Because of this, A^{-1} is never written as $\frac{1}{A}$.

5.4.1 Matrix Oddities

Some of the main dissimilarities between matrix algebra and elementary algebra are that in matrix algebra:

1. AB may be different from BA.

2. There exist matrices A and B such that $AB = \mathbf{0}$, and yet $A \neq \mathbf{0}$ and $B \neq \mathbf{0}$.

3. There exist matrices A where $A \neq \mathbf{0}$, and yet $A^2 = \mathbf{0}$.

4. There exist matrices A where $A^2 - A$ with $A \neq I$ and $A \neq \mathbf{0}$

5. There exist matrices A where $A^2 = I$, where $A \neq I$ and $A \neq -I$

5.4.2 Exercises

1. Discuss each of the "Matrix Oddities" with respect to elementary algebra.

Answer. In elementary algebra (the algebra of real numbers), each of the given oddities does not exist.

- AB may be different from BA. Not so in elementary algebra, since $ab = ba$ by the commutative law of multiplication.
- There exist matrices A and B such that $AB = \mathbf{0}$, yet $A \neq \mathbf{0}$and $B \neq \mathbf{0}$. In elementary algebra, the only way $ab = 0$ is if either a or b is zero. There are no exceptions.
- There exist matrices A, $A \neq \mathbf{0}$, yet $A^2 = \mathbf{0}$. In elementary algebra, $a^2 = 0 \Leftrightarrow a = 0$.
- There exist matrices $A^2 = A$. where $A \neq \mathbf{0}$ and $A \neq I$. In elementary algebra, $a^2 = a \Leftrightarrow a = 0$ or 1.
- There exist matrices A where $A^2 = I$ but $A \neq I$ and $A \neq -I$. In elementary algebra, $a^2 = 1 \Leftrightarrow a = 1$ or -1.

2. Determine 2×2 matrices which show that each of the "Matrix Oddities" are true.

3. Prove the following implications, if possible:

(a) $A^2 = A$ and $\det A \neq 0 \Rightarrow A = I$

(b) $A^2 = I$ and $\det A \neq 0 \Rightarrow A = I$ or $A = -I$.

Answer.

(a) $\det A \neq 0 \Rightarrow A^{-1}$ exists, and if you multiply the equation $A^2 = A$ on both sides by A^{-1} , you obtain $A = I$.

(b) Counterexample: $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

4. Let $M_{n\times n}(\mathbb{R})$ be the set of real $n \times n$ matrices. Let $P \subseteq M_{n\times n}(\mathbb{R})$ be the subset of matrices defined by $A \in P$ if and only if $A^2 = A$. Let $Q \subseteq P$ be defined by $A \in Q$ if and only if $\det A \neq 0$.

(a) Determine the cardinality of Q.

(b) Consider the special case $n = 2$ and prove that a sufficient condition for $A \in P \subseteq M_{2\times 2}(\mathbb{R})$ is that A has a zero determinant (i.e., A is singular) and $tr(A) = 1$ where $tr(A) = a_{11} + a_{22}$ is the sum of the main diagonal elements of A.

(c) Is the condition of part b a necessary condition?

5. Write each of the following systems in the form $AX = B$, and then solve the systems using matrices.

(a) $2x_1 + x_2 = 3$
$x_1 - x_2 = 1$

(b) $2x_1 - x_2 = 4$
$x_1 - x_2 = 0$

(c) $2x_1 + x_2 = 1$
$x_1 - x_2 = 1$

(d) $2x_1 + x_2 = 1$
$x_1 - x_2 = -1$

(e) $3x_1 + 2x_2 = 1$
$6x_1 + 4x_2 = -1$

Answer.

(a) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 4/3$, and $x_2 = 1/3$

(b) $A^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix}$ $x_1 = 4$, and $x_2 = 4$

(c) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 2/3$, and $x_2 = -1/3$

(d) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 0$, and $x_2 = 1$

(e) The matrix of coefficients for this system has a zero determinant; therefore, it has no inverse. The system cannot be solved by this method. In fact, the system has no solution.

6. Recall that $p(x) = x^2 - 5x + 6$ is called a polynomial, or more specifically, a polynomial over $\mathbb{R}$, where the coefficients are elements of $\mathbb{R}$ and $x \in \mathbb{R}$. Also, think of the method of solving, and solutions of, $x^2 - 5x + 6 = 0$. We would like to define the analogous situation for 2×2 matrices. First define where A is a 2×2 matrix $p(A) = A^2 - 5A + 6I$. Discuss the method of solving and the solutions of $A^2 - 5A + 6I = \mathbf{0}$.

7. (For those who know calculus)

(a) Write the series expansion for e^a centered around $a = 0$.

(b) Use the idea of exercise 6 to write what would be a plausible definion of e^A where A is an $n \times n$ matrix.

(c) If $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}$, use the series in part (b) to show that $e^A = \begin{pmatrix} e & e-1 \\ 0 & 1 \end{pmatrix}$ and $e^B = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

(d) Show that $e^A e^B \neq e^B e^A$

(e) Show that $e^{A+B} = \begin{pmatrix} e & 0 \\ 0 & 1 \end{pmatrix}$

(f) Is $e^A e^B = e^{A+B}$?

Chapter 6

Relations

One understands a set of objects completely only if the structure of that set is made clear by the interrelationships between its elements. For example, the individuals in a crowd can be compared by height, by age, or through any number of other criteria. In mathematics, such comparisons are called relations. The goal of this chapter is to develop the language, tools, and concepts of relations.

6.1 Basic Definitions

In Chapter 1 we introduced the concept of the Cartesian product of sets. Let's assume that a person owns three shirts and two pairs of slacks. More precisely, let $A = \{\text{blue shirt}, \text{tan shirt}, \text{mint green shirt}\}$ and $B = \{\text{grey slacks}, \text{tan slacks}\}$. Then $A \times B$ is the set of all six possible combinations of shirts and slacks that the individual could wear. However, an individual may wish to restrict himself or herself to combinations which are color coordinated, or "related." This may not be all possible pairs in $A \times B$ but will certainly be a subset of $A \times B$. For example, one such subset may be $\{(\text{blue shirt}, \text{grey slacks}), (\text{blue shirt}, \text{tan slacks}), (\text{mint green shirt}, \text{tan slacks})\}$.

Definition 6.1.1 (Relation)**.** Let A and B be sets. A relation from A into B is any subset of $A \times B$.

Example 6.1.2 (A simple example)**.** Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. Then $\{(1, 4), (2, 4), (3, 5)\}$ is a relation from A into B. Of course, there are many others we could describe; 64, to be exact.

Example 6.1.3 (Divisibility Example)**.** Let $A = \{2, 3, 5, 6\}$ and define a relation r from A into A by $(a, b) \in r$ if and only if a divides evenly into b. The set of pairs that qualify for membership is $r = \{(2, 2), (3, 3), (5, 5), (6, 6), (2, 6), (3, 6)\}$.

Definition 6.1.4 (Relation on a Set)**.** A relation from a set A into itself is called a relation on A.

The relation "divides" in Example 6.1.3 is will appear throughout the book. Here is a general definition on the whole set of integers.

Definition 6.1.5 (Divides)**.** Let $a, b \in \mathbb{Z}$. We say that a divides b, denoted $a \mid b$, if and only if there exists an integer k such that $ak = b$.

Be very careful in writing about the relation "divides." The vertical line symbol use for this relation, if written carelessly, can look like division. While $a \mid b$ is either true or false, a/b is a number.

Based on the equation $ak = b$, we can say that $a|b$ is equivalent to $k = \frac{b}{a}$, or a divides evenly into b. In fact the "divides" is short for "divides evenly into." You

might find the equation $k = \frac{b}{a}$ initially easier to understand, but in the long run we will find the equation $ak = b$ more convenient.

Sometimes it is helpful to illustrate a relation with a graph. Consider Example 6.1.2. A graph of r can be drawn as in Figure 6.1.6. The arrows indicate that 1 is related to 4 under r. Also, 2 is related to 4 under r, and 3 is related to 5, while the upper arrow denotes that r is a relation from the whole set A into the set B.

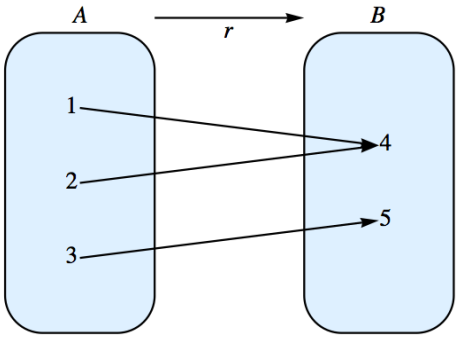


Figure 6.1.6: The graph of a relation

A typical element in a relation r is an ordered pair (x, y). In some cases, r can be described by actually listing the pairs which are in r, as in the previous examples. This may not be convenient if r is relatively large. Other notations are used with certain well-known relations. Consider the "less than or equal" relation on the real numbers. We could define it as a set of ordered pairs this way:

$$\leq = \{(x, y) | x \leq y\}$$

. However, the notation $x \leq y$ is clear and self-explanatory; it is a more natural, and hence preferred, notation to use than $(x, y) \in \leq$.

Many of the relations we will work with "resemble" the relation $\leq$, so xsy is a common way to express the fact that x is related to y through the relation s.

Relation Notation Let s be a relation from a set A into a set B. Then the fact that $(x, y) \in s$ is frequently written xsy.

With $A = \{2, 3, 5, 8\}$, $B = \{4, 6, 16\}$, and $C = \{1, 4, 5, 7\}$, let r be the relation "divides," from A into B; and let s be the relation $\leq$ from B into C. So $r = \{(2, 4), (2, 6), (2, 16), (3, 6), (8, 16)\}$ and $s = \{(4, 4), (4, 5), (4, 7), (6, 7)\}$.

Notice that in Figure 6.1.7 that we can, for certain elements of A, go through elements in B to results in C. That is:

$$\begin{gathered} 2|4 \text{ and } 4 \leq 4 \\ 2|4 \text{ and } 4 \leq 5 \\ 2|4 \text{ and } 4 \leq 7 \\ 2|6 \text{ and } 6 \leq 7 \\ 3|6 \text{ and } 6 \leq 7 \end{gathered}$$

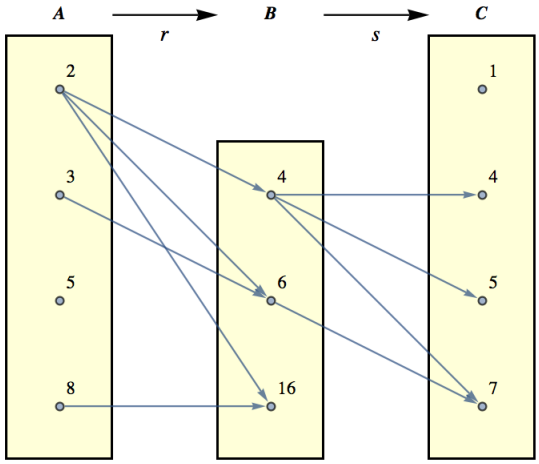


Figure 6.1.7: Relation Composition - a graphical view

Based on this observation, we can define a new relation, call it rs, from A into C. In order for (a, c) to be in rs, it must be possible to travel along a path in Figure 6.1.2 from a to c. In other words, $(a, c) \in rs$ if and only if $(\exists b)_B(arb \text{ and } bsc)$. The name rs was chosen because it reminds us that this new relation was formed by the two previous relations r and s. The complete listing of all elements in rs is $\{(2, 4), (2, 5), (2, 7), (3, 7)\}$. We summarize in a definition.

Definition 6.1.8 (Composition of Relations)**.** Let r be a relation from a set A into a set B, and let s be a relation from B into a set C. The composition of r with s, written rs, is the set of pairs of the form $(a, c) \in A \times C$, where $(a, c) \in rs$ if and only if there exists $b \in B$ such that $(a, b) \in r$ and $(b, c) \in s$.

Remark: A word of warning to those readers familiar with composition of functions. (For those who are not, disregard this remark. It will be repeated at an appropriate place in the next chapter.) As indicated above, the traditional way of describing a composition of two relations is rs where r is the first relation and s the second. However, function composition is traditionally expressed in the opposite order; that is, $s \circ r$, where r is the first function and s is the second.

6.1.1 Exercises

1. For each of the following relations r defined on $\mathbb{P}$, determine which of the given ordered pairs belong to r.

(a) xry iff $x|y$; (2, 3), (2, 4), (2, 8), (2, 17)

(b) xry iff $x \leq y$; (2, 3), (3, 2), (2, 4), (5, 8)

(c) xry iff $y = x^2$; (1,1), (2, 3), (2, 4), (2, 6)

Answer.

(a) $(2, 4), (2, 8)$

(b) $(2, 3), (2, 4), (5, 8)$

(c) $(1, 1), (2, 4)$

2. The following relations are on $\{\{1, 3, 5\}\}$. Let r be the relation xry iff $y = x + 2$ and s the relation xsy iff $x \leq y$.

(a) List all elements in rs.

(b) List all elements in sr.

(c) Illustrate rs and sr via a diagram.

(d) Is the relation (set) rs equal to the relation sr? Why?

3. Let $A = \{1, 2, 3, 4, 5\}$ and define r on A by xry iff $x + 1 = y$. We define $r^2 = rr$ and $r^3 = r^2r$. Find:

(a) r

(b) r^2

(c) r^3

Answer.

(a) $r = \{(1, 2), (2, 3), (3, 4), (4, 5)\}$

(b) $r^2 = \{(1, 3), (2, 4), (3, 5)\} = \{(x, y) : y = x + 2, x, y \in A\}$

(c) $r^3 = \{(1, 4), (2, 5)\} = \{(x, y) : y = x + 3, x, y \in A\}$

4. Given s and t, relations on $\mathbb{Z}$,$s = \{(1, n) : n \in \mathbb{Z}\}$ and $t = \{(n, 1) : n \in \mathbb{Z}\}$, what are st and ts? Hint: Even when a relation involves infinite sets, you can often get insights into them by drawing partial graphs.

5. Let ρ be the relation on the power set, $\mathcal{P}(S)$, of a finite set S of cardinality n. Define ρ by $(A, B) \in \rho$ iff $A \cap B = \emptyset$.

(a) Consider the specific case $n = 3$, and determine the cardinality of the set ρ.

(b) What is the cardinality of ρ for an arbitrary n? Express your answer in terms of n. (Hint: There are three places that each element of S can go in building an element of ρ.)

Answer.

(a) When $n = 3$, there are 27 pairs in the relation.

(b) Imagine building a pair of disjoint subsets of S. For each element of S there are three places that it can go: into the first set of the ordered pair, into the second set, or into neither set. Therefore the number of pairs in the relation is 3^n, by the product rule.

6. Let r_1, r_2, and r_3 be relations on any set A. Prove that if $r_1 \subseteq r_2$then $r_1r_3 \subseteq r_2r_3$.

6.2 Graphs of Relations on a Set

In this section we introduce directed graphs as a way to visualize relations on a set.

Let $A = \{0, 1, 2, 3\}$, and let

$$r = \{(0, 0), (0, 3), (1, 2), (2, 1), (3, 2), (2, 0)\}$$

In representing this relation as a graph, elements of A are called the vertices of the graph. They are typically represented by labeled points or small circles. We connect vertex a to vertex b with an arrow, called an edge, going from vertex a to vertex b if and only if arb. This type of graph of a relation r is called a **directed graph** or **digraph**. Figure 6.2.1 is a digraph for r. Notice that since 0 is related to itself, we draw a "self-loop" at 0.

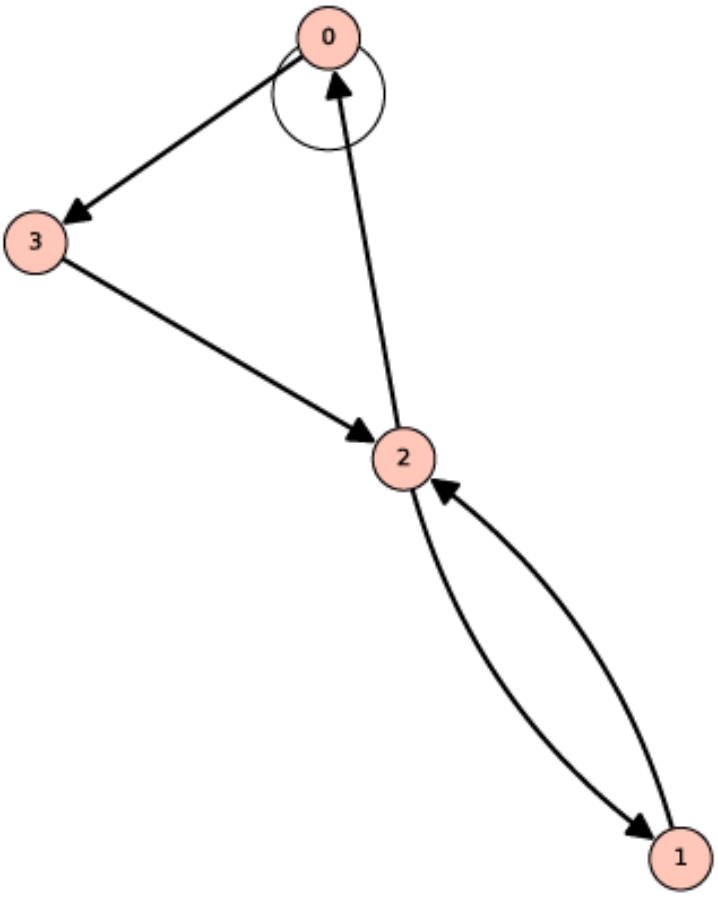


Figure 6.2.1: Digraph of a relation

The actual location of the vertices in a digraph is immaterial. The actual location of vertices we choose is called an **embedding of a graph**. The main idea is to place the vertices in such a way that the graph is easy to read. After drawing a rough-draft graph of a relation, we may decide to relocate the vertices so that the final result will be neater. Figure 6.2.1 could also be presented as in Figure 6.2.2.

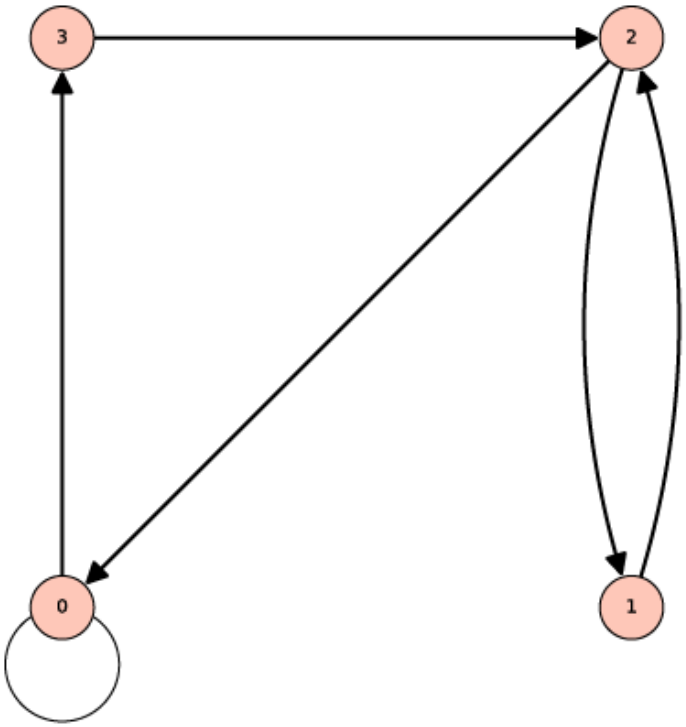


Figure 6.2.2: Alternate embedding of of the previous directed graph

A vertex of a graph is also called a node, point, or a junction. An edge of a graph is also referred to as an arc, a line, or a branch. Do not be concerned if two graphs of a given relation look different as long as the connections between vertices are are the same in two graphs.

Example 6.2.3 (Another directed graph.)**.** Consider the relation s whose digraph is Figure 6.2.4. What information does this give us? The graph tells us that s is a relation on $A = \{1, 2, 3\}$ and that $s = \{(1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 3)\}$,

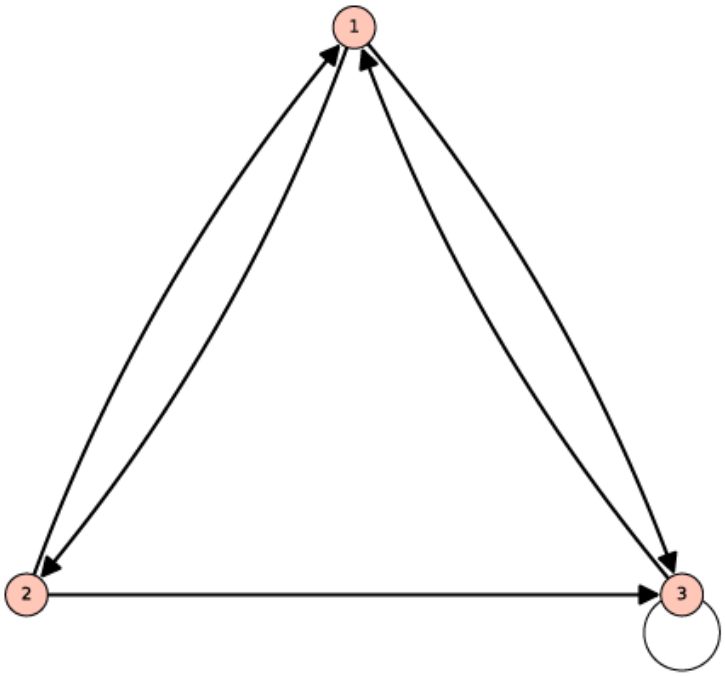


Figure 6.2.4: Digraph of the relation s

Example 6.2.5 (Ordering subsets of a two element universe)**.** Let $B = \{1, 2\}$, and let $A = \mathcal{P}(B) = \{0, \{1\}, \{2\}, \{1, 2\}\}$. Then $\subseteq$ is a relation on A whose digraph is Figure 6.2.6.

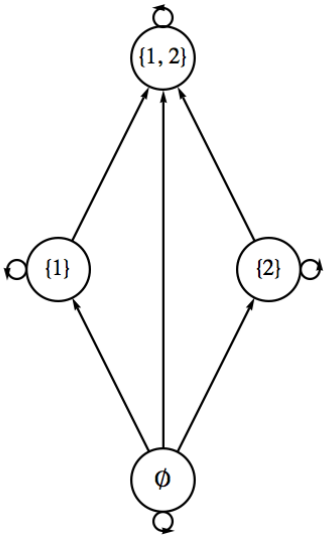


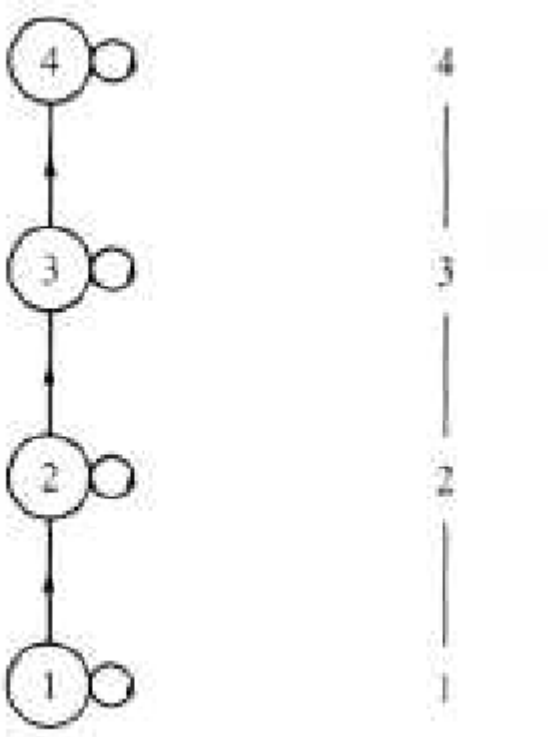
Figure 6.2.6: Graph for set containment on subsets of $\{1, 2\}$

We will see in the next section that since $\subseteq$ has certain structural properties that describe "partial orderings." We will be able to draw a much simpler type graph than this one, but for now the graph above serves our purposes.

6.2.1 Exercises

1. Let $A = \{1, 2, 3, 4\}$, and let r be the relation $\leq$ on A Draw a digraph for r.

Answer.



2. Let $B = \{1, 2, 3, 4, 6, 8, 12, 24\}$, and let s be the relation "divides," on B. Draw a digraph for s.

3. Let $A = \{1, 2, 3, 4, 5\}$. Define t on A by atb if and only if $b - a$ is even. Draw a digraph for t.

Answer. See Figure 13.1.1 of Section 13.1.

4.

(a) Let A be the set of strings of 0's and 1's of length 3 or less. Define the relation of d on A by xdy if x is contained within y. For example, $01d101$. Draw a digraph for this relation.

(b) Do the same for the relation p defined by xpy if x is a prefix of y. For example, $10p101$, but $01p101$ is false.

5. Recall the relation in Exercise 5 of Section 6.1, ρ defined on the power set, $\mathcal{P}(S)$, of a set S. The definition was $(A, B) \in \rho$ iff $A \cap B = \emptyset$. Draw the digraph for ρ where $S = \{a, b\}$.

Answer. A Hasse diagram cannot be used because not every set is related to itself. Also, $\{a\}$ and $\{b\}$ are related in both directions.

6. Let $C = \{1, 2, 3, 4, 6, 8, 12, 24\}$ and define t on C by atb if and only if a and b share a common divisor greater than 1. Draw a digraph for t.

6.3 Properties of Relations

Consider the set $B = \{1, 2, 3, 4, 6, 12, 36, 48\}$ and the relations "divides" and $\leq$ on B. We notice that these two relations on B have three properties in common:

- Every element in B divides itself and is less than or equal to itself. This is called the reflexive property.
- If we search for two elements from B where the first divides the second and the second divides the first, then we are forced to choose the the two numbers to be the same. In other words, no two *different* numbers are related in both directions. The reader can verify that a similar fact is true for the relation $\leq$ on B. This is called the antisymmetric property.
- Next if we choose three numbers from B such that the first divides the second and the second divides the third, then we always find that the first number to divides the third. Again, the same is true if we replace "divides" with "is less than or equal to." This is called the transitive property.

Relations that satisfy these properties are of special interest to us. Formal definitions of the properties follow.

Definition 6.3.1 (Reflexive Relation)**.** Let A be a set and let r be a relation on A. r is **reflexive** if and only if ara for all $a \in A$.

Definition 6.3.2 (Antisymmetric Relation)**.** Let A be a set and let r be a relation on A. Then r is **antisymmetric** if and only if whenever arb and $a \neq b$ then bra is false.

An equivalent condition for antisymmetry is that if arb and bra then $a = b$. You are encouraged to convince yourself that this is true. This condition is often more convenient to prove than the definition, even thought the definition is probably easier to understand.

A word of warning about antisymmetry: Students frequently find it difficult to understand this definition. Keep in mind that this term is defined through an "If . .. then . . ." statement. The question that you must ask is: Is it true that whenever there are elements a and b from A where arb and $a \neq b$, it follows that b is not related to a? If so, then the relation is antisymmetric.

Another way to determine whether a relation is antisymmetric is to examine (or imagine) its digraph. The relation is not antisymmetric if there exists a pair of vertices that are connected by edges in both directions.

Definition 6.3.3 (Transitive Relation)**.** Let A be a set and let r be a relation on A. r is **transitive** if and only if whenever arb and brc then arc.

6.3.1 Partial Orderings

Not all relations have all three of the properties discussed above, but those that do are a special type of relation.

Definition 6.3.4 (Partial Ordering)**.** A relation on a set A that is reflexive, antisymmetric, and transitive is called a partial ordering on A. A set on which there is a partial ordering relation defined is called a **partially ordered set** or **poset**.

Example 6.3.5 (Set Containment as a Partial Ordering)**.** Let A be a set. Then $\mathcal{P}(A)$ together with the relation $\subseteq$ (set containment) is a poset. To prove this we observe that the three properties hold, as discussed in Chapter 4.

- Let $B \in \mathcal{P}(A)$. The fact that $B \subseteq B$ follows from the definition of subset. Hence, set containment is reflexive.

- Let $B_1, B_2 \in \mathcal{P}(A)$ and assume that $B_1 \subseteq B_2$ and $B_1 \neq B_2$. Could it be that $B_2 \subseteq B_1$? No. There must be some element $a \in A$ such that $a \notin B_1$, but $a \in B_2$. This is exactly what we need to conclude that B_2 is not contained in B_1. Hence, set containment is antisymmetric.

- Let $B_1, B_2, B_3 \in \mathcal{P}(A)$ and assume that $B_1 \subseteq B_2$ and $B_2 \subseteq B_3$. Does it follow that $B_1 \subseteq B_3$? Yes, if $a \in B_1$, then $a \in B_2$ because $B_1 \subseteq B_2$. Now that we have $a \in B_2$ and we have assumed $B_2 \subseteq B_3$, we conclude that $a \in B_3$. Therefore, $B_1 \subseteq B_3$ and so set containment is transitive.

Figure 6.2.6 is the graph for the "set containment" relation on $\{1, 2\}$.

6.3.1.1 Hasse Diagrams

Figure 6.2.6 is helpful insofar as it reminds us that each set is a subset of itself and shows us at a glance the relationship between the various subsets in $\mathcal{P}(\{1, 2\})$. However, when a relation is a partial ordering, we can streamline a graph like this one. The streamlined form of a graph is called a **Hasse diagram** or **ordering diagram**. A Hasse diagram takes into account the following facts.

- By the reflexive property, each vertex must be related to itself, so the arrows from a vertex to itself (called "self-loops") are not drawn in a Hasse diagram. They are simply assumed.

- By the antisymmetry property, connections between two distinct elements in a directed graph can only go one way, if at all. When there is a connection, we agree to always place the second element above the first (as we do above with the connection from $\{1\}$ to $\{1, 2\}$). For this reason, we can just draw a connection without an arrow, just a line.

- By the transitive property, if there are edges connecting one element up to a second element and the second element up to a third element, then there will be a direct connection from the first to the third. We see this in Figure 6.2.6 with $\emptyset$ connected to $\{1\}$and then $\{1\}$ connected to $\{1, 2\}$. Notice the edge connecting $\emptyset$ to $\{1, 2\}$. Whenever we identify this situation, remove the connection from the first to the third in a Hasse diagram and simply observe that an upward path of any length implies that the lower element is related to the upper one.

Using these observations as a guide, we can draw a Hasse diagram for $\subseteq$ on $\{1, 2\}$ as in Figure 6.3.2.

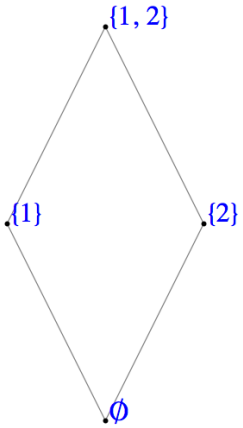


Figure 6.3.6: Hasse diagram for set containment on subsets of $\{1, 2\}$

Example 6.3.7 (Definition of a relation using a Hasse diagram)**.** Consider the partial ordering relation s whose Hasse diagram is Figure 6.3.8.

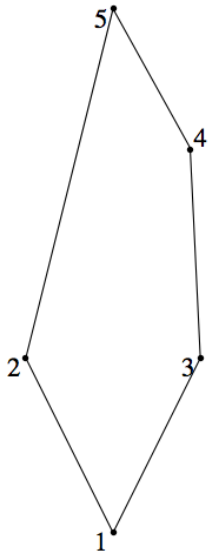


Figure 6.3.8: Hasse diagram for for the pentagonal poset

How do we read this diagram? What is A? What is s? What does the digraph of s look like? Certainly $A = \{1, 2, 3, 4, 5\}$ and $1s2$, $3s4$, $1s4$, $1s5$, etc., Notice that $1s5$ is implied by the fact that there is a path of length three upward from 1 to 5. This follows from the edges that are shown and the transitive property that is presumed in a poset. Since $1s3$ and $3s4$, we know that $1s4$. We then combine $1s4$ with $4s5$ to infer $1s5$. Without going into details why, here is a complete list of pairs defined by s.

$$s = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (1, 4), (1, 5), (1, 2), (3, 4), (3, 5), (4, 5), (2, 5)\}$$

A digraph for s is Figure 6.3.9. It is certainly more complicated to read and difficult to draw than the Hasse diagram.

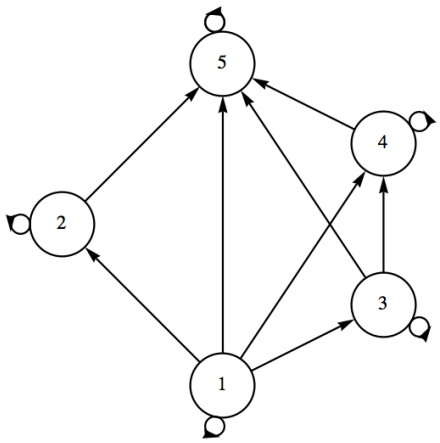


Figure 6.3.9: Digraph for for the pentagonal poset

A classic example of a partial ordering relation is $\leq$ on the real numbers, $\mathbb{R}$. Indeed, when graphing partial ordering relations, it is natural to "plot" the elements from the given poset starting with the "least" element to the "greatest" and to use terms like "least," "greatest," etc. Because of this the reader should be forewarned that some texts use the symbol $\leq$ for arbitrary partial orderings. This can be quite confusing for the novice, so we continue to use generic letters r, s, etc.

6.3.2 Equivalence Relations

Another common property of relations is symmetry.

Definition 6.3.10 (Symmetric Relation)**.** Let r be a relation on a set A. r is **symmetric** if and only if whenever arb, it follows that bra.

Consider the relation of equality defined on any set A. Certainly $a = b$ implies that$b = a$ so equality is a symmetric relation on A.

Surprisingly, equality is also an antisymmetric relation on A. This is due to the fact that the condition that defines the antisymmetry property, $a = b$ and $a \neq b$, is a contradiction. Remember, a conditional proposition is always true when the condition is false. So a relation can be both symmetric and antisymmetric on a set! Again recall that these terms are *not* negatives of one other. That said, there are very few important relations other than equality that are both symmetric and antisymmetric.

Definition 6.3.11 (Equivalence Relation)**.** A relation r on a set A is called an equivalence relation if and only if it is reflexive, symmetric, and transitive.

The classic example of an equivalence relation is equality on a set A. In fact, the term equivalence relation is used because those relations which satisfy the definition behave quite like the equality relation. Here is another important equivalence relation.

Example 6.3.12 (Equivalent Fractions)**.** Let $\mathbb{Z}^*$ be the set of nonzero integers. One of the most basic equivalence relations in mathematics is the relation q on $\mathbb{Z} \times \mathbb{Z}^*$ defined by $(a, b)q(c, d)$ if and only if $ad = bc$. We will leave it to the reader to, verify that q is indeed an equivalence relation. Be aware that since the elements of $\mathbb{Z}\times\mathbb{Z}^*$ are ordered pairs, proving symmetry involves four numbers and transitivity involves six numbers. Two ordered pairs, (a, b) and (c, d), are related if the fractions $\frac{a}{b}$ and $\frac{c}{d}$ are numerically equal.

Our next example involves the following fundamental relations on the set of integers.

Definition 6.3.13 (Congruence Modulo m)**.** Let m be a positive integer, $m \geq 2$. We define **congruence modulo m** to be the relation $\equiv_m$ defined on the integers by

$$a \equiv_m b \Leftrightarrow m \mid (a - b)$$

We observe the following about congurence modulo m:

- This relation is reflexive, for if $a \in \mathbb{Z}$, $m \mid (a - a) \Rightarrow a \equiv_m a$.
- This relation is symmetric. We can prove this through the following chain of implications.

$$\begin{aligned} a \equiv_m b &\Rightarrow m \mid (a - b) \\ &\Rightarrow \text{For some } k \in \mathbb{Z}, a - b = mk \\ &\Rightarrow b - a = m(-k) \\ &\Rightarrow m \mid (b - a) \\ &\Rightarrow b \equiv_m a \end{aligned}$$

- Finally, this relation is transitive. We leave it to the reader to prove that if $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

Frequently, you will see the equivalent notation $a \equiv b (\text{mod } m)$ for congruence modulo m.

Example 6.3.14 (Random Relations usually have no properties)**.** Consider the relation s described by the digraph in Figure 6.3.15. This was created by randomly selecting whether or not two elements from $\{a, b, c\}$ were related or not.

- This relation is not reflexive, Why?
- It is not antisymmetric, Why?
- Also, it is not symmetric, Why?
- It is not transitive, Why?
- Is s an equivalence relation or a partial ordering? It is neither for every possible reason.

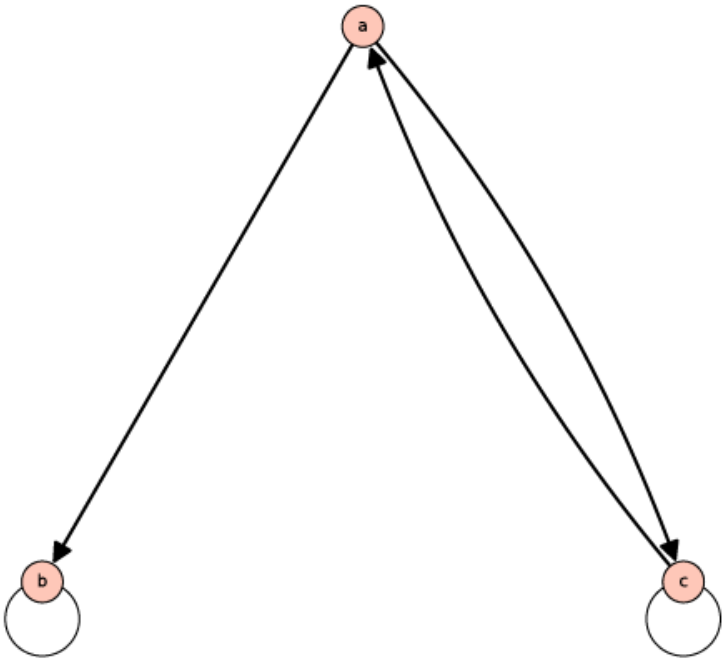


Figure 6.3.15: Digraph of a random relation r

Not every random choice of a relation will be so totally negative, but as the underlying set increases, the likelihood any of the properties are true begins to vanish.

6.3.3 Exercises

1.

(a) Let $B = \{a, b\}$ and $U = \mathcal{P}(B)$. Draw a Hasse diagram for $\subseteq$ on U.

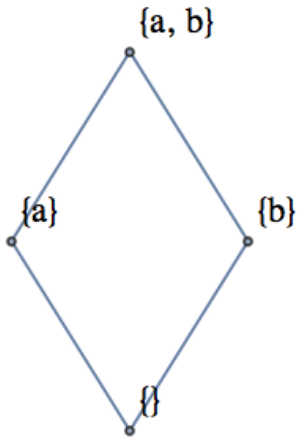
(b) Let $A = \{1, 2, 3, 6\}$. Show that divides, $|$, is a partial ordering on A.

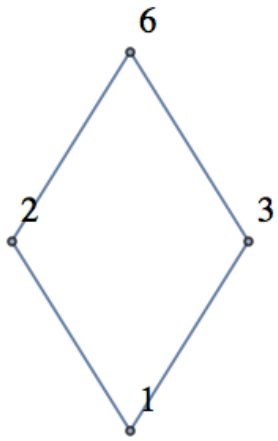
(c) Draw a Hasse diagram for divides on A.

(d) Compare the graphs of parts a and c.

Answer.

(a)





(b) The graphs are the same if we disregard the names of the vertices.

2. Repeat Exercise 1 with $B = \{a, b, c\}$ and $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

3.

(a) Consider the relations defined by the digraphs in Figure B.0.2. Determine whether the given relations are reflexive, symmetric, antisymmetric, or transitive. Try to develop procedures for determining the validity of these properties from the graphs,

(b) Which of the graphs are of equivalence relations or of partial orderings?

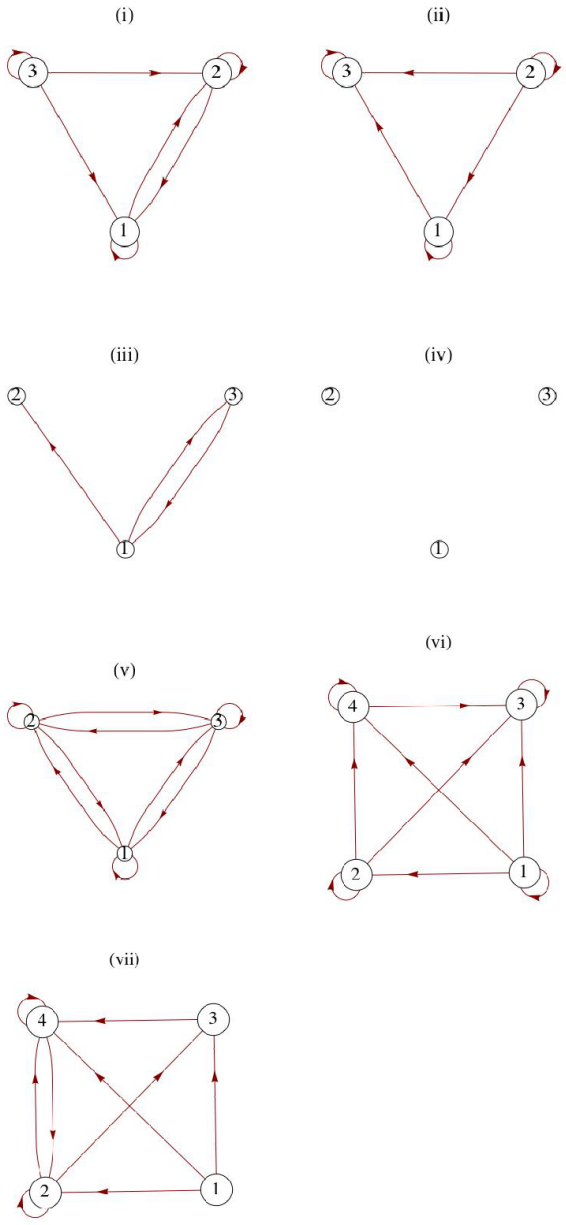


Figure 6.3.16: Some diagraphs of relations

Answer.

(a)

Part	reflexive?	symetric?	antisymmetric?	transitive?
i	yes	no	no	yes
ii	yes	no	yes	yes
iii	no	yes	no	yes
iv	no	yes	yes	yes
v	yes	yes	no	yes
vi	yes	no	yes	yes
vii	no	no	no	no

(b) Graphs ii and vi show partial ordering relations. Graph v is of an equivalence relation.

4. Determine which of the following are equivalence relations and/or partial ordering relations for the given sets:

(a) $A = \{$ lines in the plane$\}$: xry if and only if x is parallel to y.

(b) $A = \mathbb{R}$; xry if and only if $|x - y| \leq 7$.

5. Consider the relation on $\{1, 2, 3, 4, 5, 6\}$ defined by $r = \{(i, j) :| i - j |= 2\}$.

(a) Is r reflexive?

(b) Is r symmetric?

(c) Is r transitive?

(d) Draw a graph of r.

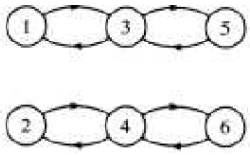
Answer.

(a) No, since $| 1 - 1 |= 0 \neq 2$, for example

(b) Yes, because $| i - j |=| j - i |$.

(c) No, since $| 2 - 4 |= 2$ and $| 4 - 6 |= 2$, but $| 2 - 6 |= 4 \neq 2$, for example.

(d)



6. For the set of cities on a map, consider the relation xry if and only if city x is connected by a road to city y. A city is considered to be connected to itself, and two cities are connected even though there are cities on the road between them. Is this an equivalence relation or a partial ordering? Explain.

7. Let $A = \{0, 1, 2, 3\}$ and let

$$r = \{(0,0), (1,1), (2,2), (3,3), (1,2), (2,1), (3,2), (2,3), (3,1), (1,3)\}$$

(a) Verify that r is an equivalence relation on A.

(b) Let $a \in A$ and define $c(a) = \{b \in A \mid arb\}$. $c(a)$ is called the **equivalence class of** a **under** r. Find $c(a)$ for each element $a \in A$.

(c) Show that $\{c(a) \mid a \in A\}$ forms a partition of A for this set A.

(d) Let r be an equivalence relation on an arbitrary set A. Prove that the set of all equivalence classes under r constitutes a partition of A.

Answer.

(a)

(b) $c(0) = \{0\}, c(1) = \{1, 2, 3\} = c(2) = c(3)$

(c) $c(0) \cup c(1) = A$ and $c(0) \cap c(1) = \emptyset$

(d) Let A be any set and let r be an equivalence relation on A. Let a be any element of A. $a \in c(a)$ since r is reflexive, so each element of A is in some equivalence class. Therefore, the union of all equivalence classes equals A. Next we show that any two equivalence classes are either identical or disjoint and we are done. Let $c(a)$ and $c(b)$ be two equivalence classes,

and assume that $c(a) \cap c(b) \neq \emptyset$. We want to show that $c(a) = c(b)$. To show that $c(a) \subseteq c(b)$, let $x \in c(a)$. $x \in c(a) \Rightarrow arx$. Also, there exists an element, y, of A that is in the intersection of $c(a)$ and $c(b)$ by our assumption. Therefore,

$$\begin{aligned} ary \wedge bry &\Rightarrow ary \wedge yrb \quad r \text{ is symmetric} \\ &\Rightarrow arb \quad \text{transitivity of } r \end{aligned}$$

Next,

$$\begin{aligned} arx \wedge arb &\Rightarrow xra \wedge arb \\ &\Rightarrow xrb \\ &\Rightarrow brx \\ &\Rightarrow x \in c(b) \end{aligned}$$

Similarly, $c(b) \subseteq c(a)$ $\square$

8. Define r on the power set of $\{1, 2, 3\}$ by $ArB \Leftrightarrow |A| = |B|$. Prove that r is an equivalence relation. What are the equivalence classes under r?

9. Consider the following relations on $\mathbb{Z}_8 = \{0, 1, ..., 7\}$. Which are equivalence relations? For the equivalence relations, list the equivalence classes.

(a) arb iff the English spellings of a and b begin with the same letter.

(b) asb iff $a - b$ is a positive integer.

(c) atb iff $a - b$ is an even integer.

Answer.

(a) Equivalence Relation, $c(0) = \{0\}, c(1) = \{1\}, c(2) = \{2, 3\} = c(3), c(4) = \{4, 5\} = c(5)$, and $c(6) = \{6, 7\} = c(7)$

(b) Not an Equivalence Relation.

(c) Equivalence Relation, $c(0) = \{0, 2, 4, 6\} = c(2) = c(4) = c(6)$ and $c(1) = \{1, 3, 5, 7\} = c(3) = c(5) = c(7)$

10.

(a) Prove that conguence modulo m is a transitive?

(b) What are the equivalence classes under conguence modulo 2?

(c) What are the equivalence classes under conguence modulo 10?

11. In this exercise, we prove that implication is a partial ordering. Let A be any set of propositions.

(a) Verify that $q \rightarrow q$ is a tautology, thereby showing that $\Rightarrow$ is a reflexive relation on A.

(b) Prove that $\Rightarrow$ is antisymmetric on A. Note: we do not use $=$ when speaking of propositions, but rather equivalence, $\Leftrightarrow$.

(c) Prove that $\Rightarrow$ is transitive on A.

(d) Given that q_i is the proposition $n < i$ on $\mathbb{N}$, draw the Hasse diagram for the relation $\Rightarrow$ on $\{q_1, q_2, q_3, \ldots\}$.

Answer.

(a)

(b) The proof follows from the biconditional equivalence in Table 3.4.2.

(c) Apply the chain rule.

(d)

12. Let $S = \{1, 2, 3, 4, 5, 6, 7\}$ be a poset $(S, \leq)$ with the Hasse diagram shown below. Another relation $r \subseteq S \times S$ is defined as follows: $(x, y) \in r$ if and only if there exists $z \in S$ such that $z < x$ and $z < y$ in the poset $(S, \leq)$.

(a) Prove that r is reflexive.

(b) Prove that r is symmetric.

(c) A compatible with respect to relation r is any subset Q of set S such that $x \in Q$ and $y \in Q \Rightarrow (x, y) \in r$. A compatible g is a maximal compatible if Q is not a proper subset of another compatible. Give all maximal compatibles with respect to relation r defined above.

(d) Discuss a characterization of the set of maximal compatibles for relation r when $(S, \leq)$ is a general finite poset. What conditions, if any, on a general finite poset $(S, \leq)$ will make r an equivalence relation?

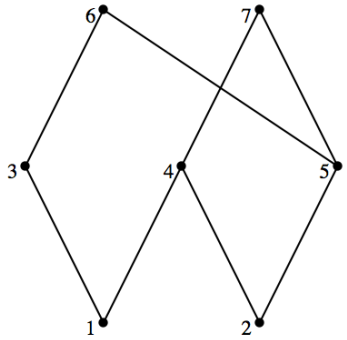


Figure 6.3.17: Hasse diagram for r in Exercise 6.3.3.12

6.4 Matrices of Relations

We have discussed two of the many possible ways of representing a relation, namely as a digraph or as a set of ordered pairs. In this section we will discuss the representation of relations by matrices.

Definition 6.4.1 (Adjacency Matrix)**.** Let $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ be finite sets of cardinality m and n, respectively. Let r be a relation from A into B. Then r can be represented by the $m \times n$ matrix R defined by

$$R_{ij} = \begin{cases} 1 & \text{if } a_i r b_j \\ 0 & \text{otherwise} \end{cases}$$

R is called the **adjacency matrix** (or the relation matrix) of r.

For example, let $A = \{2, 5, 6\}$ and let r be the relation $\{(2, 2), (2, 5), (5, 6), (6, 6)\}$ on A. Since r is a relation from A into the same set A (the B of the definition), we have $a_1 = 2$, $a_2 = 5$, and $a_3 = 6$, while $b_1 = 2$, $b_2 = 5$, and $b_3 = 6$. Next, since

- $2r2$, we have $R_{11} = 1$
- $2r5$, we have $R_{12} = 1$
- $5r6$, we have $R_{23} = 1$
- $6r6$, we have $R_{33} = 1$

All other entries of R are zero, so

$$R = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

From the definition of r and of composition, we note that

$$r^2 = \{(2, 2), (2, 5), (2, 6), (5, 6), (6, 6)\}$$

The adjacency matrix of r^2 is

$$R^2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

We do not write R^2 only for notational purposes. In fact, R^2 can be obtained from the matrix product RR; however, we must use a slightly different form of arithmetic.

Definition 6.4.2 (Boolean Arithmetic)**.** Boolean arithmetic is the arithmetic defined on $\{0, 1\}$ using Boolean addition and Boolean multiplication, defined by

$$\begin{array}{lll} 0+0=0 & 0+1=1+0=1 & 1+1=1 \\ 0\cdot 0=0 & 0\cdot 1=1\cdot 0=0 & 1\cdot 1=1 \end{array}$$

Notice that from Chapter 3, this is the "arithmetic of logic," where + replaces "or" and $\cdot$ replaces "and."

Example 6.4.3 (Composition by Multiplication)**.** If $R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Then using Boolean arithmetic, $RS = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $SR = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Theorem 6.4.4 (Composition is Matrix Multiplication)**.** *Let A_1, A_2, and A_3 be finite sets where r_1 is a relation from A_1 into A_2 and r_2 is a relation from A_2 into A_3. If R_1 and R_2 are the adjacency matrices of r_1 and r_2 , respectively, then the product R_1R_2 using Boolean arithmetic is the adjacency matrix of the composition r_1r_2.*

Remark: A convenient help in constructing the adjacency matrix of a relation from a set A into a set B is to write the elements from A in a column preceding the first column of the adjacency matrix, and the elements of B in a row above the first row. Initially, R in Example 6.4.1 would be

$$\begin{array}{c} \\ 2 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccc} 2 & 5 & 6 \end{array} \\ \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} \end{array}$$

To fill in the matrix, R_{ij} is 1 if and only if$(a_i, b_j) \in r$. So that, since the pair $(2, 5) \in r$, the entry of R corresponding to the row labeled 2 and the column labeled 5 in the matrix is a 1.

Example 6.4.5 (Relations and Information)**.** This final example gives an insight into how relational data base programs can systematically answer questions pertaining to large masses of information. Matrices R (on the left) and S (on the right) define the relations r and s where arb if software a can be run with operating system b, and bsc if operating system b can run on computer c.

$$\begin{array}{c} \\ \text{P1} \\ \text{P2} \\ \text{P3} \\ \text{P4} \end{array} \begin{array}{c} \begin{array}{cccc} \text{OS1} & \text{OS2} & \text{OS3} & \text{OS4} \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \end{array} \qquad \begin{array}{c} \\ \text{OS1} \\ \text{OS2} \\ \text{OS3} \\ \text{OS4} \end{array} \begin{array}{c} \begin{array}{ccc} \text{C1} & \text{C2} & \text{C3} \end{array} \\ \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array}$$

Although the relation between the software and computers is not implicit from the data given, we can easily compute this information. The matrix of rs is RS, which is

$$\begin{array}{c} \\ \text{P1} \\ \text{P2} \\ \text{P3} \\ \text{P4} \end{array} \begin{array}{c} \begin{array}{ccc} \text{C1} & \text{C2} & \text{C3} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array}$$

This matrix tells us at a glance which software will run on the computers listed. In this case, all software will run on all computers with the exception of program P2, which will not run on the computer C3, and program P4, which will not run on the computer C1.

6.4.1 Exercises

1. Let $A_1 = \{1, 2, 3, 4\}$, $A_2 = \{4, 5, 6\}$, and $A_3 = \{6, 7, 8\}$. Let r_1 be the relation from A_1 into A_2 defined by $r_1 = \{(x, y) \mid y - x = 2\}$, and let r_2 be the relation from A_2 into A_3 defined by $r_2 = \{(x, y) \mid y - x = 1\}$.

(a) Determine the adjacency matrices of r_1 and r_2.

(b) Use the definition of composition to find $r_1 r_2$.

(c) Verify the result in part by finding the product of the adjacency matrices of r_1 and r_2.

Answer.

(a)
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \quad \text{and} \quad \begin{array}{c} \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccc} 6 & 7 & 8 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

(b) $r_1 r_2 = \{(3, 6), (4, 7)\}$

(c)
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} 6 & 7 & 8 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

2.

(a) Determine the adjacency matrix of each relation given via the digraphs in Exercise 3 of Section 6.3.

(b) Using the matrices found in part (a) above, find r^2 of each relation in Exercise 3 of Section 6.3.

(c) Find the digraph of r^2 directly from the given digraph and compare your results with those of part (b).

3. Suppose that the matrices in Example 6.4.3 are relations on $\{1, 2, 3, 4\}$. What relations do R and S describe?

Answer.

R : xry if and only if $|x - y| = 1$
S : xsy if and only if x is less than y.

4. Let D be the set of weekdays, Monday through Friday, let W be a set of employees $\{1, 2, 3\}$ of a tutoring center, and let V be a set of computer languages for which tutoring is offered, $\{A(PL), B(asic), C(++), J(ava), L(isp), P(ython)\}$. We define s (schedule) from D into W by dsw if w is scheduled to work on day d. We also define r from W into V by wrl if w can tutor students in language l. If s and r are defined by matrices

$$S = \begin{array}{c} \\ M \\ T \\ W \\ R \\ F \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \end{array} \quad \text{and } R = \begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccc} A & B & C & J & L & P \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

(a) compute SR using Boolean arithmetic and give an interpretation of the relation it defines, and

(b) compute SR using regular arithmetic and give an interpretation of what the result describes.

5. How many different reflexive, symmetric relations are there on a set with three elements?

Hint. Consider the possible matrices.

Answer. The diagonal entries of the matrix for such a relation must be 1. When the three entries above the diagonal are determined, the entries below are also determined. Therefore, there are 2^3 fitting the description.

6. Let $A = \{a, b, c, d\}$. Let r be the relation on A with adjacency matrix

$$\begin{array}{c} \\ a \\ b \\ c \\ c \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

(a) Explain why r is a partial ordering on A.

(b) Draw its Hasse diagram.

7. Define relations p and q on $\{1, 2, 3, 4\}$ by $p = \{(a, b) \mid |a - b| = 1\}$ and $q = \{(a, b) \mid a - b \text{ is even}\}$

(a) Represent p and q as both graphs and matrices.

(b) Determine pq, p^2, and q^2; and represent them clearly in any way.

Answer.

(a)
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \quad \text{and} \quad \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

(b) $PQ =$
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$P^2 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} = Q^2$$

8.

(a) Prove that if r is a transitive relation on a set A, then $r^2 \subseteq r$.

(b) Find an example of a transitive relation for which $r^2 \neq r$.

9. We define $\leq$ on the set of all $n \times n$ relation matrices by the rule that if R and S are any two $n \times n$ relation matrices, $R \leq S$ if and only if $R_{ij} \leq S_{ij}$ for all $1 \leq i, j \leq n$.

(a) Prove that $\leq$ is a partial ordering on all $n \times n$ relation matrices.

(b) Prove that $R \leq S \Rightarrow R^2 \leq S^2$, but the converse is not true.

(c) If R and S are matrices of equivalence relations and $R \leq S$, how are the equivalence classes defined by R related to the equivalence classes defined by S?

Answer.

(a) Reflexive: $R_{ij} = R_{ij}$ for all i, j, therefore $R_{ij} \leq R_{ij}$
Antisymmetric: Assume $R_{ij} \leq S_{ij}$ and $S_{ij} \leq R_{ij}$ for all $1 \leq i, j \leq n$. Therefore, $R_{ij} = S_{ij}$ for all $1 \leq i, j \leq n$ and so $R = S$
Transitive: Assume R, S, and T are matrices where $R_{ij} \leq S_{ij}$ and $S_{ij} \leq T_{ij}$, for all $1 \leq i, j \leq n$. Then $R_{ij} \leq T_{ij}$ for all $1 \leq i, j \leq n$, and so $R \leq T$.

(b)

$$\begin{aligned} \left(R^2\right)_{ij} &= R_{i1}R_{1j} + R_{i2}R_{2j} + \cdots + R_{in}R_{nj} \\ &\leq S_{i1}S_{1j} + S_{i2}S_{2j} + \cdots + S_{in}S_{nj} \\ &= \left(S^2\right)_{ij} \Rightarrow R^2 \leq S^2 \end{aligned}$$

To verify that the converse is not true we need only one example. For $n = 2$, let $R_{12} = 1$ and all other entries equal 0, and let S be the zero matrix. Since R^2 and S^2 are both the zero matrix, $R^2 \leq S^2$, but since $R_{12} > S_{12}, R \leq S$ is false.

(c) The matrices are defined on the same set $A = \{a_1, a_2, \ldots, a_n\}$. Let $c(a_i), i = 1, 2, \ldots, n$ be the equivalence classes defined by R and let $d(a_i)$ be those defined by S. Claim: $c(a_i) \subseteq d(a_i)$.

$$\begin{aligned} a_j \in c(a_i) &\Rightarrow a_i r a_j \\ &\Rightarrow R_{ij} = 1 \Rightarrow S_{ij} = 1 \\ &\Rightarrow a_i s a_j \\ &\Rightarrow a_j \in d(a_i) \end{aligned}$$

6.5 Closure Operations on Relations

In Section 6.1, we studied relations and one important operation on relations, namely composition. This operation enables us to generate new relations from

previously known relations. In Section 6.3, we discussed some key properties of relations. We now wish to consider the situation of constructing a new relation r^+ from an existing relation r where, first, r^+ contains r and, second, r^+ satisfies the transitive property.

Consider a telephone network in which the main office a is connected to, and can communicate to, individuals b and c. Both b and c can communicate to another person, d; however, the main office cannot communicate with d. Assume communication is only one way, as indicated. This situation can be described by the relation $r = \{(a,b),(a,c),(b,d),(c,d)\}$. We would like to change the system so that the main office a can communicate with person d and still maintain the previous system. We, of course, want the most economical system.

This can be rephrased as follows; Find the smallest relation r^+which contains r as a subset and which is transitive; $r^+ = \{(a,b),(a,c),(b,d),(c,d),(a,d)\}$.

Definition 6.5.1 (Transitive Closure)**.** Let A be a set and r be a relation on A. The transitive closure of r, denoted by r^+ , is the smallest transitive relation that contains r as a subset.

Let $A = \{1,2,3,4\}$, and let $\mathcal{S} = \{(1,2),(2,3),(3,4)\}$ be a relation on A. This relation is called the successor relation on A since each element is related to its successor. How do we compute $\mathcal{S}^+$? By inspection we note that $(1,3)$ must be in $\mathcal{S}^+$. Let's analyze why. This is so because $(1,2) \in \mathcal{S}$ and $(2,3) \in \mathcal{S}$, and the transitive property forces $(1,3)$ to be in $\mathcal{S}^+$.

In general, it follows that if $(a,b) \in \mathcal{S}$ and $(b,c) \in S$, then $(a,c) \in \mathcal{S}^+$. This condition is exactly the membership requirement for the pair (a,c) to be in the composition $\mathcal{S}\mathcal{S} = \mathcal{S}^2$. So every element in $\mathcal{S}^2$ must be an element in $\mathcal{S}^+$. So we now know that, $\mathcal{S}^+$ contains at least $\mathcal{S} \cup \mathcal{S}^2$. In particular, for this example, since $\mathcal{S} = \{(1,2),(2,3),(3,4)\}$ and $\mathcal{S}^2 = \{(1,3),(2,4)\}$, we have

$$\mathcal{S} \cup \mathcal{S}^2 = \{(1,2),(2,3),(3,4),(1,3),(2,4)\}$$

Is the relation $\mathcal{S} \cup \mathcal{S}^2$ transitive? Again, by inspection, $(1,4)$ is not an element of $\mathcal{S} \cup \mathcal{S}^2$, but $(1,3) \in \mathcal{S}^2$ and $(3,4) \in \mathcal{S}$. Therefore, the composition $\mathcal{S}^2\mathcal{S} = \mathcal{S}^3$ produces $(1,4)$, and it must be an element of $\mathcal{S}^+$ since $(1,3)$ and $(3,4)$ are required to be in $\mathcal{S}^+$. This shows that $\mathcal{S}^3 \subseteq \mathcal{S}^+$. This process must be continued until the resulting relation is transitive. If A is finite, as is true in this example, the transitive closure will be obtained in a finite number of steps. For this example,

$$\mathcal{S}^+ = \mathcal{S} \cup \mathcal{S}^2 \cup \mathcal{S}^3 = \{(1,2),(2,3),(3,4),(1,3),(2,4),(1,4)\}$$

Theorem 6.5.2 (Transitive Closure on a Finite Set)**.** *If r is a relation on a set A and $|A| = n$, then the transitive closure of r is the union of the first n powers of r. That is,*

$$r^+ = r \cup r^2 \cup r^3 \cup \cdots \cup r^n$$

.

Let's now consider the matrix analogue of the transitive closure.
Consider the relation
$r = \{(1,4),(2,1),(2,2),(2,3),(3,2),(4,3),(4,5),(5,1)\}$
on the set $A = \{1,2,3,4,5\}$. The matrix of r is

$$R = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Recall that $r^2, r^3, \ldots$ can be determined through computing the matrix powers $R^2, R^3, \ldots$. For our example,

$$R^2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad R^3 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

$$R^4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \quad R^5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

How do we relate $\bigcup_{i=1}^{5} r^i$ to the powers of R?

Theorem 6.5.3 (Matrix of a Transitive Closure)**.** *Let r be a relation on a finite set and let R^+ be the matrix of r^+ , the transitive closure of r. Then $R^+ = R + R^2 + \cdots + R^n$, using Boolean arithmetic.*

Using this theorem, we find R^+ is the 5×5 matrix consisting of all $1's$, thus, r^+ is all of $A \times A$.

6.5.1 Warshall's Algorithm

Let r be a relation on the set $\{1, 2, \ldots, n\}$ with relation matrix R. The matrix of the transitive closure R^+, can be computed by the equation $R^+ = R + R^2 + \cdots + R^n$. By using ordinary polynomial evaluation methods, you can compute R^+ with $n-1$ matrix multiplications:

$$R^+ = R(I + R(I + (\cdots R(I + R)\cdots)))$$

For example, if $n = 3$, $R = R(I + R(I + R))$.

We can make use of the fact that if T is a relation matrix, $T + T = T$ due to the fact that $1 + 1 = 1$ in Boolean arithmetic. Let $S_k = R + R^2 + \cdots + R^k$. Then

$$\begin{aligned} R &= S_1 \\ S_1(I + S_1) &= R(I + R) = R + R^2 = S_2 \\ S_2(I + S_2) &= (R + R^2)(I + R + R^2) \\ &= (R + R^2) + (R^2 + R^3) + (R^3 + R^4) \\ &= R + R^2 + R^3 + R^4 = S_4 \end{aligned}$$

Similarly,

$$S_4(I + S_4) = S_8$$

and by induction we can prove

$$S_{2^k}(I + S_{2^k}) = S_{2^{k+1}}$$

Notice how each matrix multiplication doubles the number of terms that have been added to the sum that you currently have computed. In algorithmic form, we can compute R^+ as follows.

Algorithm 6.5.4 (Transitive Closure Algorithm)**.** *Let R be a relation matrix and let R^+ be its transitive closure matrix, which is to be computed as matrix T*

```
1.0. S = R
2.0  T= S*(I+S)
3.0 While T != S
                3.1 S = T
                3.2 T= S*(I+S) // using Boolean arithmetic
4.0 Return T
```

Notes:

- Often the higher-powered terms in S_n do not contribute anything to R^+. When the condition $T = S$ becomes true in Step 3, this is an indication that no higher-powered terms are needed.

- To compute R^+ using this algorithm, you need to perform no more than $\lceil \log_2 n \rceil$ matrix multiplications, where $\lceil x \rceil$ is the least integer that is greater than or equal to x. For example, if r is a relation on 25 elements, no more than $\lceil \log_2 25 \rceil = 5$ matrix multiplications are needed.

A second algorithm, Warshall's Algorithm, reduces computation time to the time that it takes to perform one matrix multiplication.

Algorithm 6.5.5 (Warshall's Algorithm)**.** *Let R be an $n \times n$ relation matrix and let R^+ be its transitive closure matrix, which is to be computed as matrix T using boolean arithmetic*

```
1.0 T = R
2.0 for k = 1 to n:
     for i = 1 to n:
      for j = 1 to n:
        T[i,j]= T[i,j] + T[i,k] * T[k,j]
3.0 Return T
```

6.5.2 Exercises

1. Let A and $\mathcal{S}$ be as defined above. Compute $\mathcal{S}^+$ using the matrix representation of $\mathcal{S}$. Verify your results by checking against the result obtained directly from the definition of transitive closure.

2. Let $A = \{1, 2, 3, 4, 6, 12\}$ and $t = \{(a, b) \mid b/a \text{ is a prime number}\}$. determine t^+ by any means but represent it as a matrix.

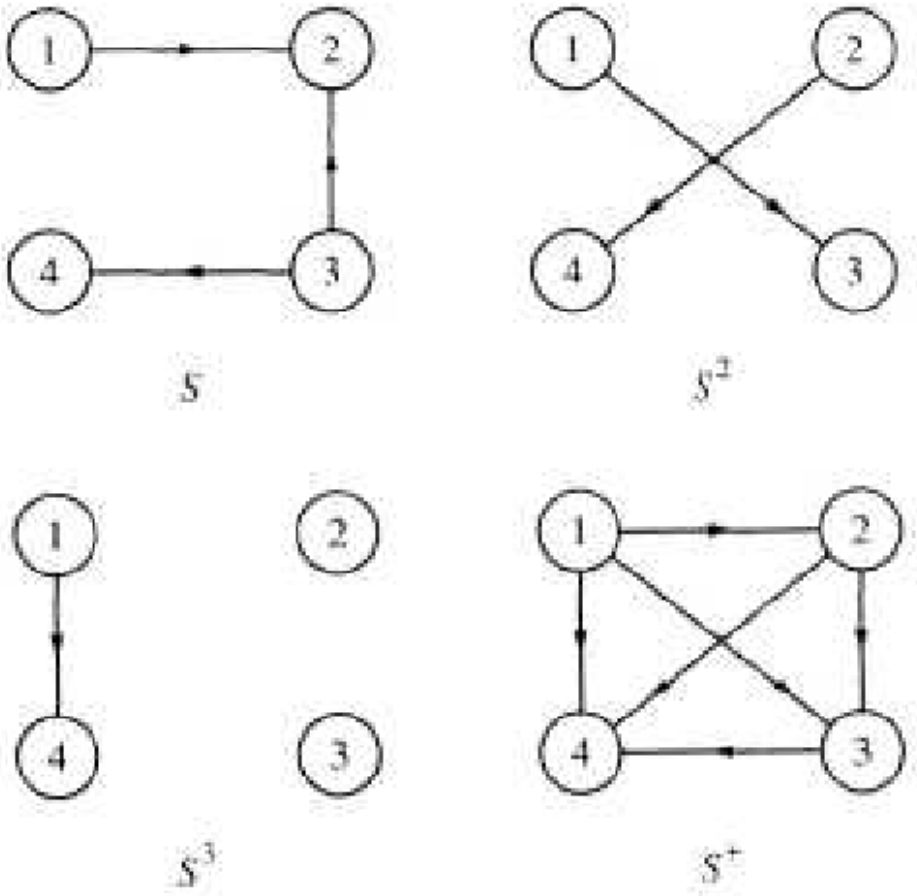
3.

(a) Draw digraphs of the relations $\mathcal{S}$, $\mathcal{S}^2$, $\mathcal{S}^3$, and $\mathcal{S}^+$ where $\mathcal{S}$ is defined above.

(b) Verify that in terms of the graph of $\mathcal{S}$, $a\mathcal{S}^+b$ if and only if b is reachable from a along a path of any finite nonzero length.

Answer.

(a)



(b) Example, $1s4$ and using S one can go from 1 to 4 using a path of length 3.

4. Let r be the relation represented by the following digraph.

(a) Find r^+ using the definition based on order pairs.

(b) Determine the digraph of r^+ directly from the digraph of r.

(c) Verify your result in part (b) by computing the digraph from your result in part (a).

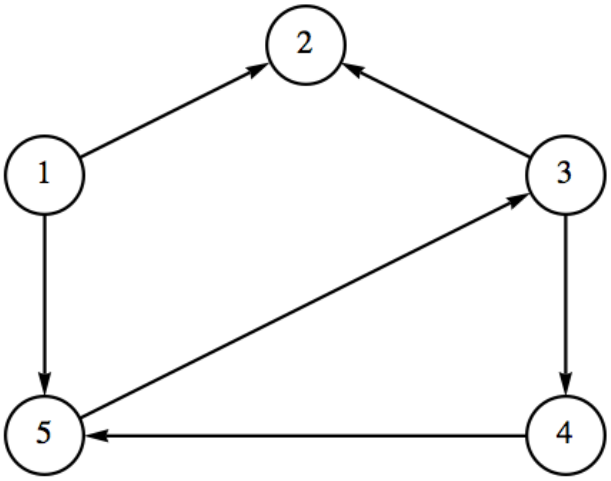


Figure 6.5.6: Digraph of r in exercise 4.

5.

(a) Define reflexive closure and symmetric closure by imitating the definition of transitive closure.

(b) Use your definitions to compute the reflexive and symmetric closures of examples in the text.

(c) What are the transitive reflexive closures of these examples?

(d) Convince yourself that the reflexive closure of the relation $<$ on the set of positive integers $\mathbb{P}$ is $\leq$.

Answer. Definition: Reflexive Closure. Let r be a relation on A. The reflexive closure of r is the smallest reflexive relation that contains r.
Theorem: The reflexive closure of r is the union of r with $\{(x, x) : x \in A\}$

6. What common relations on $\mathbb{Z}$ are the transitive closures of the following relations?

(a) aSb if and only if $a + 1 = b$.

(b) aRb if and only if $|a - b| = 2$.

7.

(a) Let A be any set and r a relation on A, prove that $(r^+)^+ = r^+$.

(b) Is the transitive closure of a symmetric relation always both symmetric and reflexive? Explain.

Answer.

(a) By the definition of transitive closure, r^+ is the smallest relation which contains r; therefore, it is transitive. The transitive closure of r^+, $(r^+)^+$, is the smallest transitive relation that contains r^+. Since r^+ is transitive, $(r^+)^+ = r^+$.

(b) The transitive closure of a symmetric relation is symmetric, but it may not be reflexive. If one element is not related to any elements, then the transitive closure will not relate that element to others.

Appendix A

Algorithms

A.1 Appendix - Algorithms

Computer programs, bicycle assembly instructions, knitting instructions, andrecipes all have several things in common. They all tell us how to do something; and the usual format is as a list of steps or instructions. In addition, theyare usually prefaced with a description of the raw materials that are needed (the input) to produce the end result (the output). We use the term algorithm to describe such lists of instructions. We assume that the reader may be unfamiliar with algorithms, so the first section of this appendix will introduce some of the components of the algorithms that appear in this book. Since we would like our algorithms to become computer programs in many cases, the notation will resemble a computer language such as Python or Sage; but our notation will be slightly less formal. In some cases we will also translate the pseudocode to Sage. Our goal will be to give mathematically correct descriptions of how to accomplish certain tasks. To this end, the second section of this appendix is an introduction to the Invariant Relation Theorem, which is a mechanism for algorithm verification that is related to Mathematical Induction

A.1.1 An Introduction to Algorithms

Most of the algorithms in this book will contain a combination of three kinds of steps: the assignment step, the conditional step, and the loop.

A.1.1.1 Assignments

In order to assign a value to a variable, we use an assignment step, which takes the form:

Variable = Expression to be computed

The equals sign in most languages is used for assignment but some languages may use variations such as `:=` or a left pointing arrow. Logical equality, which produces a boolean result and would be used in conditional or looping steps, is most commonly expressed with a double-equals, `==`.

An example of an assignment is `k = n - 1` which tells us to subtract 1 from the value of `n` and assign that value to variable `k`. During the execution of an algorithm, a variable may take on only one value at a time. Another example of an assignment is `k = k - 1`. This is an instruction to subtract one from the value of `k` and then reassign that value to `k`.

A.1.1.2 Conditional steps

Frequently there are steps that must be performed in an algorithm if and only if a certain condition is met. The conditional or "if ... then" step is then employed. For example, suppose that in step 2 of an algorithm we want to assure that the values of variables x and y satisfy the condition `x <= y`. The following step would accomplish this objective.

```
2. If x > y:
   2.1 t = x
   2.2 x = y
   2.3 y = t
```

Steps 2.1 through 2.3 would be bypassed if the condition `x > y` were false before step 2.

One slight variation is the "if ... then ... else" step, which allows us to prescribe a step to be taken if the condition is false. For example, if you wanted to exercise today, you might look out the window and execute the following algorithm.

```
1. If it is cold or raining:
                exercise indoors
        else:
                go outside and run
2. Rest
```

A.1.1.3 Loops

The conditional step tells us to do something once if a logical condition is true. A loop tells us to repeat one or more steps, called the body of the loop, while the logical condition is true. Before every execution of the body, the condition is tested. The following flow diagram serves to illustrate the steps in a While loop.

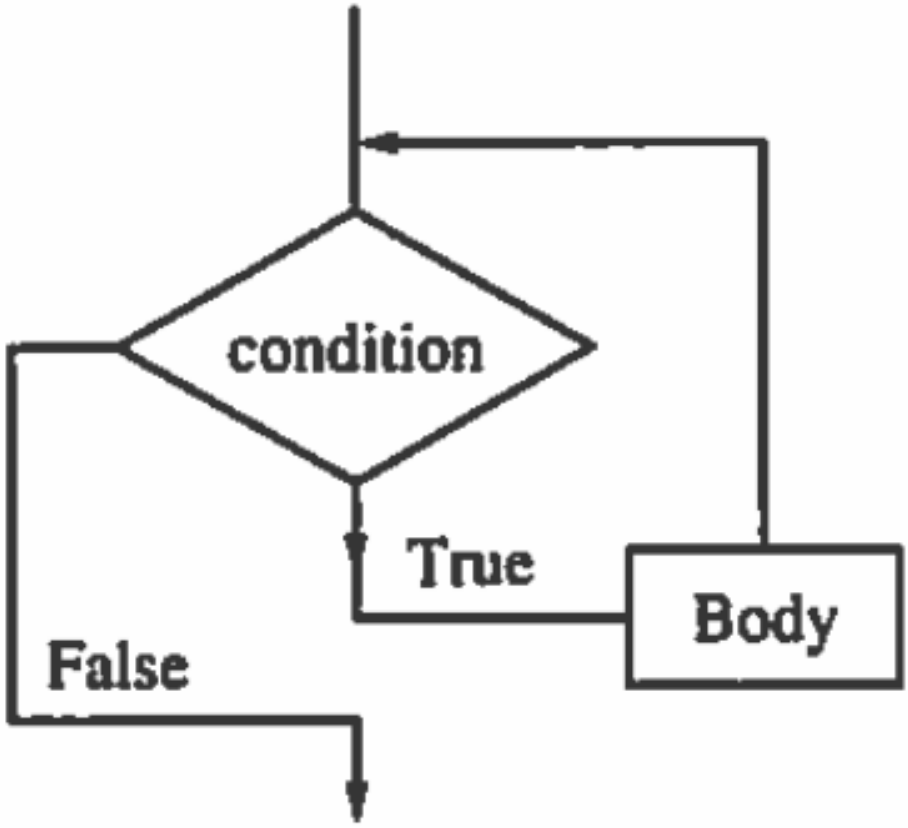


Figure A.1.1: Flow diagram for a while loop

Suppose you wanted to solve the equation $f(x) = 0$. The following initial assignment and loop could be employed.

```
1. c = your first guess
2. While f(c) != 0:
                c = another guess
```

Caution: One must always guard against the possibility that the condition of a While loop will never become false. Such "infinite loops" are the bane of beginning programmers. The loop above could very well be such a situation, particularly if the equation has no solution, or if the variable takes on real values

In cases where consecutive integer values are to be assigned to a variable, a different loop construction, a *For loop*, is often employed. For example, suppose we wanted to assign variable `k` each of the integer values from `m` to `n` and for each of these values perform some undefined steps. We could accomplish this with a While loop:

```
1. k := m
2. While k <= n:
        2.1 execute some steps
        2.2 k = k + l
```

Alternatively, we can perform these steps is with a For loop.

```
For k = m to n:
        execute some  steps
```

For loops such as this one have the advantage of being shorter than the equivalent While loop. The While loop construction has the advantage of being able to handle more different situations than the For loop.

A.1.1.4 Exercises for An Introduction to Algorithms

A Exercises

1. What are the inputs and outputs of the algorithms listed in the first sentence of this section?

2. What is wrong with this algorithm?

```
Input: a and b, integers
Output: the value of c will be a - b
(1) c = 0
(2) While a > b:
                (2.1) a := a - l
                (2.2) c := c + l
```

Answer. The algorithm only works when `a > b`.

3. Describe, in words, what the following algorithm does:

```
Input: k, a positive integer
Output: s = ?
(1) s = 0
(2) While k > 0:
    (2.1) s = s + k
    (2.2) k = k - 1
```

B Exercises

4. Write While loops to replace the For loops in the following partial algorithms:

(a)

```
(1) S := 0
(2) For k = 1 to 5:
    S : = S + k^2
```

(b) The floor of a number is the greatest integer less than or equal to that number.

```
(1) m = a positive integer greater than 1
(2) B = floor(sqrt(m))
(3) For i = 2 to B:
                If i divides evenly into m, jump to
                    step 5
(4) print "m is a prime" and exit
(5) print "m is composite"  and exit
```

5. Describe in words what the following algorithm does:

```
Input: n, a positive integer
Output: k?
(1) f= 0
(2) k=n
(3) While k is even:
        (3.1) f = f+ 1
        (3.2) k = k div 2
```

6. Fix the algorithm in Exercise 2.

A.1.2 The Invariant Relation Theorem

Consider the following algorithm implemented in Sage to compute $a^m \, mod \, n$, given an arbitrary integer a, non-negative exponent m, and a modulus n, $n \geq 0$. The default sample evaluation computes $2^5 \, mod \, 7 = 32 \, mod \, 7 = 4$, but you can edit the final line for other inputs.

```
def slow_exp(a,m,n):
        b=1
        k=m
        while k>0:
                b=(b*a)%n  # % is integer remainder (mod) operation
                k-=1
        return b

slow_exp(2,5,7)
```

It should be fairly clear that this algorithm will successfully compute $a^m (mod \, n)$ since it mimics the basic definition of exponentiation. However, this algorithm is highly inefficient. The algorithm that is most commonly used for the task of exponentiation is the following one, also implemented in Sage.

```
def fast_exp(a,m,n):
        t=a
        b=1
        k=m
        while k>0:
                if k%2==1: b=(b*t)%n
                t=(t^2)%n
                k=k//2  # // is the integer quotient operation
        return b

fast_exp(2,5,7)
```

The only difficulty with the "fast algorithm" is that it might not be so obvious that it works. When implemented, it can be verified by example, but an even more rigorous verification can be done using the Invariant Relation Theorem. Before stating the theorem, we define some terminology.

Definition A.1.2 (Pre and Post Values)**.** Given a variable x, the pre value of x, denoted $\grave{x}$, is the value before an iteration of a loop. The post value, denoted $\acute{x}$, is the value after the iteration.

Example A.1.3 (Pre and post values in the fast exponentiation algorithm.)**.** In the fast exponentiation algorithm, the relationships between the pre and post values of the three variables are as follows.

$$\acute{b} \equiv \grave{b}\grave{t}^{\grave{k} mod \, 2} (mod \, n)$$

$$\acute{t} \equiv \grave{t}^2 (mod \, n)$$

$$\acute{k} = \grave{k}//2$$

Definition A.1.4 (Invariant Relation)**.** Given a algorithm's inputs and a set of variables that are used in the algorithm, an *invariant relation* is a set one or more equations that are true prior to entering a loop and remain true in every iteration of the loop.

Example A.1.5 (Invariant Relation for Fast Exponentiation)**.** We claim that the invariant relation in the fast algorithm is $bt^k = a^m (mod\, n)$. We will prove that his is indeed true below.

Theorem A.1.6 (The Invariant Relation Theorem)**.** *Given a loop within an algorithm, if R is a relation with the properties*

1. *R is true before entering the loop*
2. *the truth of R is maintained in any iteration of the loop*
3. *the condition for exiting the loop will always be reached in a finite number of iterations.*

then R will be true upon exiting the loop.

Proof. The condition that the loop ends in a finite number of iterations lets us apply mathematical induction with the induction variable being the number of iterations. We leave the details to the reader. □

We can verify the correctness of the fast exponentiation algorithm using the Invariant Relation Theorem. First we note that prior to entering the loop, $bt^k = 1a^m = a^m (mod\, n)$. Assuming the relation is true at the start of any iteration, that is $\grave{b}\grave{t}^{\grave{k}} = a^m (mod\, n)$, then

$$\begin{aligned}
\acute{b}\acute{t}^{\acute{k}} &\equiv (\grave{b}\grave{t}^{\grave{k}\, mod\, 2})(\grave{t}^2)^{\grave{k}//2} (mod\, n) \\
&\equiv \grave{b}\grave{t}^{2(\grave{k}//2)+\grave{k}\, mod\, 2} (mod\, n) \\
&\equiv \grave{b}\grave{t}^{\grave{k}} (mod\, n) \\
&\equiv a^m (mod\, n)
\end{aligned}$$

Finally, the value of k will decrease to zero in a finite number of steps because the number of binary digits of k decreases by one with each iteration. At the end of the loop,

$$b = bt^0 = bt^k \equiv a^m (mod\, n)$$

which verifies the correctness of the algorithm.

A.1.2.1 Exercises for the Algorithms Appendix

A Exercises

1. How are the pre and post values in the slow exponentiation algorithm related?What is the invariant relation between the variables in the slow algorithm?

2. Verify the correctness of the following algorithm to compute the greatest common divisor of two integers that are not both zero.

```
def gcd(a,b):
        r0=a
        r1=b
        while r1 !=0:
                t= r0 % r1
                r0=r1
                r1=t
        return r0

gcd(1001,154)  #test
```

Hint. The invariant of this algorithm is $gcd(r0, r1) = gcd(a, b)$.

3. Verify the correctness of the Binary Conversion Algorithm in Chapter 1.

Appendix B

Hints and Solutions to Selected Exercises

1.1.3 Exercises for Section 1.1

1. List four elements of each of the following sets:

(a) $\{k \in \mathbb{P} \mid k-1 \text{ is a multiple of } 7\}$

(b) $\{x \mid x \text{ is a fruit and its skin is normally eaten }\}$

(c) $\{x \in \mathbb{Q} \mid x \in \mathbb{Z}\}$

(d) $\{2n \mid n \in \mathbb{Z}, n < 0\}$

(e) $\{s \mid s = 1 + 2 + \cdots + n, n \in \mathbb{P}\}$

These answers are not unique.

(a) $8, 15, 22, 29$

(b) apple, pear, peach, plum

(c) $1/2, 1/3, 1/4, 1/5$

(d) $-8, -6, -4, -2$

(e) $6, 10, 15, 21$

3. Describe the following sets using set-builder notation.

(a) $\{5, 7, 9, \ldots, 77, 79\}$

(b) the rational numbers that are strictly between -1 and 1

(c) the even integers

(d) $\{-18, -9, 0, 9, 18, 27, \ldots\}$

(a) $\{2k+1 \mid k \in \mathbb{Z}, 2 \leqslant k \leqslant 39\}$

(b) $\{x \in \mathbb{Q} \mid -1 < x < 1\}$

(c) $\{2n \mid n \in \mathbb{Z}\}$

(d) $\{9n \mid n \in \mathbb{Z}, -2 \leq n\}$

5. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, and $C = \{1, 5, 9\}$. Determine which of the following statements are true. Give reasons for your answers.

(a) $3 \in A$
(b) $\{3\} \in A$
(c) $\{3\} \subseteq A$
(d) $B \subseteq A$
(e) $A \subseteq B$
(f) $\emptyset \subseteq C$
(g) $\emptyset \in A$
(h) $A \subseteq A$

(a) True
(b) False
(c) True
(d) True
(e) False
(f) True
(g) False
(h) True

1.2.3 EXERCISES FOR SECTION 1.2

1. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, $C = \{1, 5, 9\}$, and let the universal set be $U = \{0, 1, 2, ..., 9\}$. Determine:

(a) $A \cap B$
(b) $A \cup B$
(c) $B \cup A$
(d) $A \cup C$
(e) $A - B$
(f) $B - A$
(g) A^c
(h) C^c
(i) $A \cap C$
(j) $A \oplus B$

(a) $\{2, 3\}$
(b) $\{0, 2, 3\}$
(c) $\{0, 2, 3\}$
(d) $\{0, 1, 2, 3, 5, 9\}$
(e) $\{0\}$
(f) $\emptyset$
(g) $\{1, 4, 5, 6, 7, 8, 9\}$
(h) $\{0, 2, 3, 4, 6, 7, 8\}$
(i) $\emptyset$
(j) $\{0\}$

3. Let $U = \{1, 2, 3, ..., 9\}$. Give examples of sets A, B, and C for which:

(a) $A \cap (B \cap C) = (A \cap B) \cap C$
(b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
(c) $(A \cup B)^c = A^c \cap B^c$
(d) $A \cup A^c = U$
(e) $A \subseteq A \cup B$
(f) $A \cap B \subseteq A$

These are all true for any sets A, B, and C.

5. What can you say about A if $U = \{1, 2, 3, 4, 5\}$, $B = \{2, 3\}$, and (separately)

(a) $A \cup B = \{1, 2, 3, 4\}$
(b) $A \cap B = \{2\}$
(c) $A \oplus B = \{3, 4, 5\}$

(a) $\{1, 4\} \subseteq A \subseteq \{1, 2, 3, 4\}$
(b) $\{2\} \subseteq A \subseteq \{1, 2, 4, 5\}$

(c) $A = \{2, 4, 5\}$

7. Given that U = all students at a university, D = day students, M = mathematics majors, and G = graduate students. Draw Venn diagrams illustrating this situation and shade in the following sets:

(a) evening students

(b) undergraduate mathematics majors

(c) non-math graduate students

(d) non-math undergraduate students

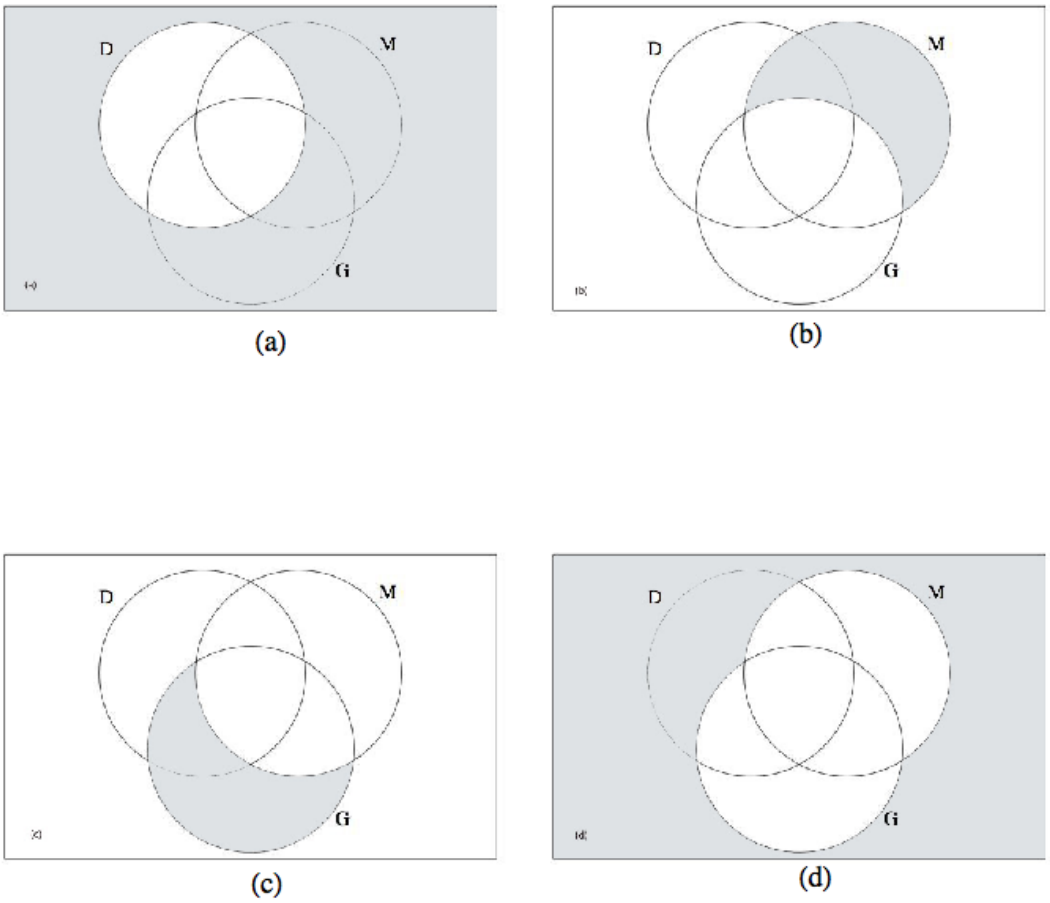


Figure B.0.1

1.3.3 EXERCISES FOR SECTION 1.3

1. Let $A = \{0, 2, 3\}$, $B = \{2, 3\}$, $C = \{1, 4\}$, and let the universal set be $U = \{0, 1, 2, 3, 4\}$. List the elements of

(a) $A \times B$

(b) $B \times A$

(c) $A \times B \times C$

(d) $U \times \emptyset$

(e) $A \times A^c$

(f) B^2

(g) B^3

(h) $B \times \mathcal{P}(B)$

(a) $\{(0,2),(0,3),(2,2),(2,3),(3,2),(3,3)\}$

(b) $\{(2,0),(2,2),(2,3),(3,0),(3,2),(3,3)\}$

(c) $\{(0,2,1),(0,2,4),(0,3,1),(0,3,4),(2,2,1),(2,2,4),$
$(2,3,1),(2,3,4),(3,2,1),(3,2,4),(3,3,1),(3,3,4)\}$

(d) $\emptyset$

(e) $\{(0,1),(0,4),(2,1),(2,4),(3,1),(3,4)\}$

(f) $\{(2,2),(2,3),(3,2),(3,3)\}$

(g) $\{(2,2,2),(2,2,3),(2,3,2),(2,3,3),(3,2,2),(3,2,3),(3,3,2),(3,3,3)\}$

(h) $\{(2,\emptyset),(2,\{2\}),(2,\{3\}),(2,\{2,3\}),(3,\emptyset),(3,\{2\}),(3,\{3\}),(3,\{2,3\})\}$

3. List all two-element sets in $\mathcal{P}(\{a,b,c,d\})$
$\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\} and \{c,d\}$

5. How many singleton (one-element) sets are there in $\mathcal{P}(A)$ if $|A| = n$?
There are n singleton subsets, one for each element.

7. Let $A = \{+,-\}$ and $B = \{00,01,10,11\}$.

- List the elements of $A \times B$
- How many elements do A^4 and $(A \times B)^3$ have?

(a) $\{+00,+01,+10,+11,-00,-01,-10,-11\}$

(b) 16 and 512

9. Let A and B be nonempty sets. When are $A \times B$ and $B \times A$. equal?
They are equal when $A = B$.

1.4.1 EXERCISES

1. Find the binary representation of each of the following positive integers by working through the algorithm by hand. You can check your answer using the sage cell above.

(a) 31
(c) 10
(b) 32
(d) 100

(a) 11111
(c) 1010
(b) 100000
(d) 1100100

3. What positive integers have the following binary representations?

(a) 10010
(c) 101010
(b) 10011
(d) 10011110000

(a) 18
(c) 42
(b) 19
(d) 1264

5. The number of bits in the binary representations of integers increase by one as the numbers double. Using this fact, determine how many bits the binary representations of the following decimal numbers have without actually doing the full conversion. $(a)2017$ $(b)4000$ $(c)4500$ $(d)2^{50}$

There is a bit for each power of 2 up to the largest one needed to represent an integer, and you start counting with the zeroth power. For example, 2017 is between $2^{10} = 1024$ and $2^{11} = 2048$, and so the largest power needed is 2^{10}. Therefore there are 11 bits in binary 2017

(a) 11
(c) 13
(b) 12
(d) 51

7. If a positive integer is a multiple of 100, we can identify this fact from its decimal representation, since it will end with two zeros. What can you say about a positive integer if its binary representation ends with two zeros? What if i ends in k zeros?

A number must be a multiple of four if its binary representation ends in two zeros. If it ends in k zeros, it must be a multiple of 2^k.

1.5.1 Exercises

1. Calculate the following series:

(a) $\sum_{i=1}^{3}(2+3i)$
(c) $\sum_{j=0}^{n} 2^j$ for $n = 1, 2, 3, 4$
(b) $\sum_{i=-2}^{1} i^2$
(d) $\sum_{k=1}^{n}(2k-1)$ for $n = 1, 2, 3, 4$

(a) 24

(b) 6

(c) $3, 7, 15, 31$

(d) $1, 4, 9, 16$

3.

(a) Express the formula $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$ without using summation notation.

(b) Verify this formula for $n = 3$.

(c) Repeat parts (a) and (b) for $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$

(a) $\frac{1}{1(1+1)} + \frac{1}{2(2+1)} + \frac{1}{3(3+1)} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$

(b) $\frac{1}{1(2)} + \frac{1}{2(3)} + \frac{1}{3(4)} = \frac{1}{2} + \frac{1}{6} + \frac{1}{12} = \frac{3}{4} = \frac{3}{3+1}$

(c) $1 + 2^3 + 3^3 + \cdots + n^3 = \left(\frac{1}{4}\right) n^2(n+1)^2 \quad 1 + 4 + 27 = 36 = \left(\frac{1}{4}\right)(3)^2(3+1)^2$

5. Rewrite the following without summation sign for $n = 3$. It is not necessary that you understand or expand the notation $\begin{pmatrix} n \\ k \end{pmatrix}$ at this point. $(x+y)^n = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} x^{n-k} y^k$

$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1}y + \binom{n}{2} x^{n-2}y^2 + \cdots + \binom{n}{n-1} xy^{n-1} + \binom{n}{n} y^n$

7. For any positive integer k, let $A_k = \{x \in \mathbb{Q} : k - 1 < x <= k\}$ and $B_k = \{x \in \mathbb{Q} : -k < x < k\}$. What are the following sets?

(a) $\bigcup_{i=1}^{5} A_i$

(b) $\bigcup_{i=1}^{5} B_i$

(c) $\bigcap_{i=1}^{5} A_i$

(d) $\bigcap_{i=1}^{5} B_i$

(a) $\{x \in \mathbb{Q} \mid 0 < x \leq 5\}$

(b) $\{x \in \mathbb{Q} \mid -5 < x < 5\} = B_5$

(c) $\emptyset$

(d) $\{x \in \mathbb{Q} \mid -1 < x < 1\} = B_1$

9. The symbol Π is used for the product of numbers in the same way that Σ is used for sums. For example, $\prod_{i=1}^{5} x_i = x_1x_2x_3x_4x_5$ Evaluate the following:

(a) $\prod_{i=1}^{3} i^2$

(b) $\prod_{i=1}^{3} (2i+1)$

(a) 36

(b) 105

2.1.3 Exercises

1. In horse racing, to bet the "daily double" is to select the winners of the first two races of the day. You win only if both selections are correct. In terms of the number of horses that are entered in the first two races, how many different daily double bets could be made?

If there are m horses in race 1 and n horses in race 2 then there are $m \cdot n$ possible daily doubles.

3. A certain shirt comes in four sizes and six colors. One also has the choice of a dragon, an alligator, or no emblem on the pocket. How many different shirts could you order?

$72 = 4 \cdot 6 \cdot 3$

5. The Pi Mu Epsilon mathematics honorary society of Outstanding University wishes to have a picture taken of its six officers. There will be two rows of three people. How many different way can the six officers be arranged?

$720 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

7. A clothing manufacturer has put out a mix-and-match collection consisting of two blouses, two pairs of pants, a skirt, and a blazer. How many outfits can you make? Did you consider that the blazer is optional? How many outfits can you make if the manufacturer adds a sweater to the collection?

If we always include the blazer in the outfit we would have 6 outfits. If we consider the blazer optional then there would be 12 outfits. When we add a sweater we have the same type of choice. Considering the sweater optional produces 24 outfits.

9. (a) Suppose each single character stored in a computer uses eight bits. Then each character is represented by a different sequence of eight 0's and l's called a bit pattern. How many different bit patterns are there? (That is, how many different characters could be represented?) (b) How many bit patterns are palindromes (the same backwards as forwards)?

(c) How many different bit patterns have an even number of 1's?

(a) $2^8 = 256$

(b) $2^4 = 16$. Here we are concerned only with the first four bits, since the last four must be the same.

(c) $2^7 = 128$, you have no choice in the last bit.

11. (a) Let $A = \{1, 2, 3, 4\}$. Determine the number of different subsets of A. (b) Let $A = \{1, 2, 3, 4, 5\}$. Determine the number of proper subsets of A .

(a) 16

(b) 30

13. Consider three persons, A, B, and C, who are to be seated in a row of three chairs. Suppose A and B are identical twins. How many seating arrangements of these persons can there be

(a) (a) If you are a total stranger?

(b) (b) If you are A and B's mother?

This problem is designed to show you that different people can have different correct answers to the same problem.

(a) 3 (b) 6

15. Suppose you have a choice of fish, lamb, or beef for a main course, a choice of peas or carrots for a vegetable, and a choice of pie, cake, or ice cream for dessert. If you must order one item from each category, how many different dinners are possible?

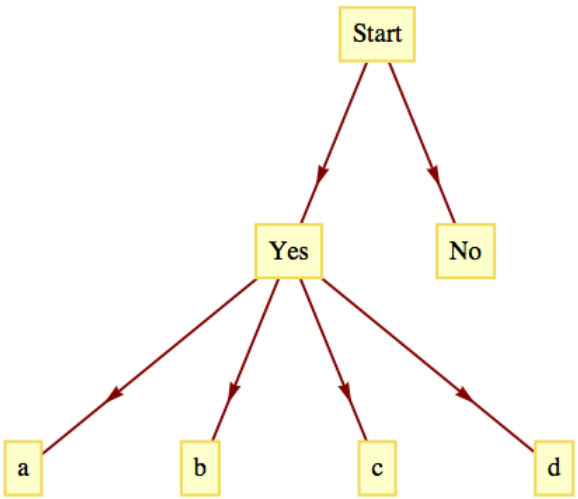
18

17. A questionnaire contains six questions each having yes-no answers. For each yes response, there is a follow-up question with four possible responses.

(a) Draw a tree diagram that illustrates how many ways a single question in the questionnaire can be answered.

(b) How many ways can the questionnaire be answered?

(a)



(b) 5^6

19. How many ways can you separate a set with n elements into two nonempty subsets if the order of the subsets is immaterial? What if the order of the subsets is important?

$2^{n-1} - 1$ and $2^n - 2$

2.2.1 Exercises

1. If a raffle has three different prizes and there are 1,000 raffle tickets sold, how many different ways can the prizes be distributed?

$P(1000, 3)$

3. How many eight-letter words can be formed from the 26 letters in the alphabet? Even without concerning ourselves about whether the words make sense, there are two interpretations of this problem. Answer both.

With repetition: $26^8 \approx 2.0883 \times 10^{11}$

Without repetition: $P(26, 8) \approx 6.2991\ 10^{10}$

5. The state finals of a high school track meet involves fifteen schools. How many ways can these schools be listed in the program?

15!

7. a. How many ways can the coach at Tall U. fill the five starting positions on a basketball team if each of his 15 players can play any position?

b. What is the answer if the center must be one of two players?

(a) $P(15, 5) = 360360$

(b) $2 \cdot 14 \cdot 13 \cdot 12 \cdot 11 = 48048$

9. The president of the Math and Computer Club would like to arrange a meeting with six attendees, the president included. There will be three computer science majors and three math majors at the meeting. How many ways can the six people be seated at a circular table if the president does not want people with the same majors to sit next to one other?

$2 \cdot P(3, 3) = 12$

11. Let $A = \{1, 2, 3, 4\}$. Determine the cardinality of

(a) $\{(a_1, a_2) \mid a_1 \neq a_2\}$

(b) What is the answer to the previous part if $|A| = n$

(c) If $|A| = n$, determine the number of m-tuples in A, $m \leq n$, where each coordinate is different from the other coordinates.

(a) $P(4, 2) = 12$

(b) $P(n; 2) = n(n - 1)$

(c) Case 1: $m > n$. Since the coordinates must be different, this case is impossible.

Case 2: $m \leqslant n.P(n; m)$.

2.3.3 Exercises for Section 2.3

1. List all partitions of the set $A = \{a, b, c\}$.

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

3. A student, on an exam paper, defined the term partition the following way: "Let A be a set. A partition of A is any set of nonempty subsets $A_1, A_2, A_3, \ldots$ of A such that each element of A is in one of the subsets." Is this definition correct? Why?

No. By this definition it is possible that an element of A might belong to two of the subsets.

5. Show that $\{\{2n \mid n \in \mathbb{Z}\}, \{2n + 1 \mid n \in \mathbb{Z}\}\}$ is a partition of $\mathbb{Z}$. Describe this partition using only words.

The first subset is all the even integers and the second is all the odd integers. These two sets do not intersect and they cover the integers completely.

7. A survey of 90 people, 47 of them played tennis and 42 of them swam. If 17 of the them participated in both activities, how many of them participated in neither.

Since 17 participated in both activities, 30 of the tennis players only played tennis and 25 of the swimmers only swam. Therefore, $17 + 30 + 25 = 72$ of those who were surveyed participated in an activity and so 18 did not.

9.

(a) Use the Two Set Inclusion-Exclusion Law to derive the Three Set Inclusion-Exclusion Law. Note: a knowledge of basic set laws is needed for this exercise.

(b) State and derive the Inclusion-exclusion law for four sets.

We assume that $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3| &= |(A_1 \cup A_2) \cup A_3| \quad Why? \\
&= |A_1 \cup A_2| + |A_3| - |(A_1 \cup A_2) \cap A_3| \quad Why? \\
&= |(A_1 \cup A_2| + |A_3| - |(A_1 \cap A_3) \cup (A_2 \cap A_3)| \quad Why? \\
&= |A_1| + |A_2| - |A_1 \cap A_2| + |A_3| \\
&\quad - (|A_1 \cap A_3| + |A_2 \cap A_3| - |(A_1 \cap A_3) \cap (A_2 \cap A_3)| \quad Why? \\
&= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| \\
&\quad - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| \quad Why?
\end{aligned}$$

The law for four sets is

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4| \\
- |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| \\
- |A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4| \\
+ |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \\
+ |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\
- |A_1 \cap A_2 \cap A_3 \cap A_4|
\end{aligned}$$

Derivation:

$$\begin{aligned}
|A_1 \cup A_2 \cup A_3 \cup A_4| &= |(A_1 \cup A_2 \cup A_3) \cup A_4| \\
&= |(A_1 \cup A_2 \cup A_3| + |A_4| - |(A_1 \cup A_2 \cup A_3) \cap A_4| \\
&= |(A_1 \cup A_2 \cup A_3| + |A_4| \\
&\quad - |(A_1 \cap A_4) \cup (A_2 \cap A_4) \cup (A_3 \cap A_4)| \\
&= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| \\
&\quad - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| + |A_4| - |A_1 \cap A_4| \\
&\quad + |A_2 \cap A_4| + |A_3 \cap A_4| - |(A_1 \cap A_4) \cap (A_2 \cap A_4)| \\
&\quad - |(A_1 \cap A_4) \cap (A_3 \cap A_4)| - |(A_2 \cap A_4) \cap (A_3 \cap A_4)| \\
&\quad + |(A_1 \cap A_4) \cap (A_2 \cap A_4) \cap (A_3 \cap A_4)| \\
&= |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \cap A_2| - |A_1 \cap A_3| \\
&\quad - |A_2 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_4| \quad - |A_3 \cap A_4| \\
&\quad + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| \\
&\quad + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| \\
&\quad - |A_1 \cap A_2 \cap A_3 \cap A_4|
\end{aligned}$$

11. The definition of $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ given in Chapter 1 is awkward. If we use the definition to list elements in $\mathbb{Q}$, we will have duplications such as $\frac{1}{2}$, $\frac{-2}{-4}$ and $\frac{300}{600}$ Try to write a more precise definition of the rational numbers so that there is no duplication of elements.

Partition the set of fractions into blocks, where each block contains fractions that are numerically equivalent. Describe how you would determine whether two fractions belong to the same block. Redefine the rational numbers to be this partition. Each rational number is a set of fractions.

2.4.5 Exercises

1. The judiciary committee at a college is made up of three faculty members and four students. If ten faculty members and 25 students have been nominated for the committee, how many judiciary committees could be formed at this point ?

$C(10,3) \cdot C(25,4) = 1,518,000$

2. Suppose that a single character is stored in a computer using eight bits.

a. How many bit patterns have exactly three 1 's?

b. How many bit patterns have at least two 1 's?

Think of the set of positions that contain a 1 to turn this is into a question about sets.

(a) $\binom{8}{3}$ (b) $2^8 - (\binom{8}{0} + \binom{8}{1})$

3. How many subsets of $\{1, 2, 3, \ldots, 10\}$ contain at least seven elements?

$C(10,7) + C(10,8) + C(10,9) + C(10,10)$

5. Expand $(2x - 3y)^4$

$16x^4 - 96x^3y + 216x^2y^2 - 216xy^3 + 81y^4$

7. (a) A poker game is played with 52 cards. How many "hands" of five cards are possible?

(b) If there are four people playing, how many five-card "hands" are possible on the first deal?

(a) $C(52,5) = 2,598,960$

(b) $C(52,5) \cdot C(47,5) \cdot C(42,5) \cdot C(37,5)$

9. How many five-card poker hands using 52 cards contain exactly two aces?

$C(4,2)C(48,3)$

11. A class of twelve computer science students are to be divided into three groups of 3, 4, and 5 students to work on a project. How many ways can this be done if every student is to be in exactly one group?

$C(12,3) \cdot C(9,4) \cdot C(5,5)$

13. There are ten points, $P_1, P_2, \ldots, P_{10}$ on a plane, no three on the same line.

(a) How many lines are determined by the points?

(b) How many triangles are determined by the points?

(a) $C(10,2) = 45$

(b) $C(10,3) = 120$

15. Use the binomial theorem to prove that if A is a finite set, then $P(A) = 2^{|A|}$

Assume $|A| = n$. If we let $x = y = 1$ in the Binomial Theorem, we obtain $2^n = C(n;0) + C(n;1) + \cdots + C(n;n)$, with the right side of the equality counting all subsets of A containing $0, 1, 2, \ldots, n$ elements. Hence $|P(A)| = 2^{|A|}$

17. Use the binomial theorem to calculate 9998^3.

$9998 = 10000 - 2$

$1000^3 - 3 \cdot 2 \cdot 1000^2 + 3 \cdot 2^2 \cdot 1000 - 2^3 = 999,400,119,992.$

3.1.3 Exercises for Section 3.1

1. Let $d =$ "I like discrete structures", $c =$ "I will pass this course" and $s =$ "I will do my assignments." Express each of the following propositions in symbolic form:

(a) I like discrete structures and I will pass this course.

(b) I will do my assignments or I will not pass this course.

(c) It is not true that I like discrete structures and I will do my assignments.

(d) I will not do my assignment and I will not pass this course.

(a) $d \wedge c$

(b) $s \vee \neg c$

(c) $\neg(d \wedge s)$

(d) $\neg s \wedge \neg c$

3. Let $p = 2 < 5$, $q =$ "8 is an even integer," and $r =$ "11 is a prime number." Express the following as a statement in English and determine whether the statement is true or false:

(a) $\neg p \vee q$

(b) $p \rightarrow q$

(c) $(p \wedge q) \rightarrow r$

(d) $p \rightarrow q \vee (\neg r)$

(e) $p \rightarrow (\neg q) \vee (\neg r)$

(f) $\neg q \rightarrow \neg p$

(a) $2 > 5$ and 8 is an even integer. False.

(b) If $2 \leqslant 5$ then 8 is an even integer. True.

(c) If $2 \leqslant 5$ and 8 is an even integer then 11 is a prime number. True.

(d) If $2 \leqslant 5$ then either 8 is an even integer or 11 is not a prime number. True.

(e) If $2 \leqslant 5$ then either 8 is an odd integer or 11 is not a prime number. False.

(f) If 8 is not an even integer then $2 > 5$. True.

5. Write the converse of the propositions in exercise 4. Compare the truth of each proposition and its converse.

Only the converse of d is true.

3.2.3 Exercises for Section 3.2

1. Construct the truth tables of:

(a) $p \vee p$

(b) $p \wedge (\neg p)$

(c) $p \vee (\neg p)$

(d) $p \wedge p$

(a)

p	$p \vee p$
0	0
1	1

(b)

p	$\neg p$	$p \wedge p$
0	1	0
1	0	0

(c)

p	$\neg p$	$p \wedge (\neg p)$
0	1	1
1	0	1

(d)

p	$p \wedge p$
0	0
1	1

3. Rewrite the following with as few extraneous parentheses as possible:

(a) $(\neg((p) \wedge (r))) \vee (s)$

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

(a) $\neg(p \wedge q) \vee s$

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

5. Determine the number of rows in the truth table of a proposition containing four variables $p, q, r,$ and s.

$2^4 = 16$ rows.

3.3.4 Exercises for Section 3.3

1. Given the following propositions generated by p, q, and r, which are equivalent to one another?

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

(b) $p \vee (r \vee q)$

(c) $r \wedge p$

(d) $\neg r \vee p$

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

(f) $r \to p$

(g) $r \vee \neg p$

(h) $p \to r$

$a \Leftrightarrow e, d \Leftrightarrow f, g \Leftrightarrow h$

3. Is an implication equivalent to its converse? Verify your answer using a truth table.

No. In symbolic form the question is: Is $(p \to q) \Leftrightarrow (q \to p)$?

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

This table indicates that an implication is not always equivalent to its converse.

5. How large is the largest set of propositions generated by p and q with the property that no two elements are equivalent?

Let x be any proposition generated by p and q. The truth table for x has 4 rows and there are 2 choices for a truth value for x for each row, so there are $2 \cdot 2 \cdot 2 \cdot 2 = 2^4$ possible propositions.

7. Explain why a contradiction implies any proposition and any proposition implies a tautology.

$0 \to p$ and $p \to 1$ are tautologies.

3.4.1 Exercises for Section 3.4

1. Write the following in symbolic notation and determine whether it is a tautology: "If I study then I will learn. I will not learn. Therefore, I do not study."

Let $s =$ I will study,$t =$ I will learn. The argument is: $((s \to t) \wedge (\neg t)) \to (\neg s)$, call the argument a.

s	t	$s \to t$	$(s \to t) \wedge (\neg t)$	a
0	0	1	1	1
0	1	1	0	1
1	0	0	0	1
1	1	1	0	1

Since a is a tautology, the argument is valid.

3. Describe, in general, how duality can be applied to implications if we introduce the symbol $\Leftarrow$, read "is implied by."

In any true statement S, replace; $\wedge$ with $\vee$, $\vee$ with $\wedge$, 0 with 1, 1 with 0, $\Leftarrow$ with $\Rightarrow$, and $\Rightarrow$ with $\Leftarrow$. Leave all other connectives unchanged.

3.5.2 Exercises for Section 3.5

1. Prove with truth tables:

(a) $p \vee q, \neg q \Rightarrow p$

(b) $p \to q, \neg q \Rightarrow \neg p$

(a)

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

(b)

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

3. Give direct and indirect proofs of:

(a) $a \to b, c \to b, d \to (a \vee c), d \Rightarrow b$.

(b) $(p \to q) \wedge (r \to s), (q \to t) \wedge (s \to u), \neg(t \wedge u), p \to r \Rightarrow \neg p$.

(c) $p \to (q \to r), \neg s \backslash / p, q \Rightarrow s \to r$.

(d) $p \to q, q \to r, \neg(p \wedge r), p \vee r \Rightarrow r$.

(e) $\neg q, p \to q, p \vee t \Rightarrow t$

(a) i. Direct proof:
ii. $d \to (a \vee c)$
iii. d
iv. $a \vee c$
v. $a \to b$
vi. Indirect proof:
~~vii.~~ $\neg b$ Negated conclusion
ii. $a \to b$ Premise
iii. $\neg a$ Indirect Reasoning (1), (2)
iv. $c \to b$ Premise
v. $\neg c$ Indirect Reasoning (1), (4)
vi. $(\neg a \wedge \neg c)$ Conjunctive (3), (5)
vii. $\neg(a \vee c)$ DeMorgan's law (6)
viii. $d \to (a \vee c)$ Premise
ix. $\neg d$ Indirect Reasoning (7), (8)
x. d Premise
xi. $\nvdash$ (9), (10) ■

(b) Direct proof:
i. $(p \to q) \wedge (r \to s)$
ii. $p \to q$
iii. $(p \to t) \wedge (s \to u)$
iv. $q \to t$

v. $p \to t$
vi. $r \to s$
vii. $s \to u$
viii. $r \to u$
ix. $p \to r$
x. $p \to u$
xi. $p \to (t \wedge u)$ Use $(x \to y) \wedge (x \to z) \Leftrightarrow x \to (y \wedge z)$
xii. $\neg(t \wedge u) \to \neg p$
xiii. $\neg(t \wedge u)$
xiv. $\neg p$ ■

Indirect proof:

i. p
ii. $p \to q$
iii. q
iv. $q \to t$
v. t
vi. $\neg(t \wedge u)$
vii. $\neg t \vee \neg u$
viii. $\neg u$
ix. $s \to u$
x. $\neg s$
xi. $r \to s$
xii. $\neg r$
xiii. $p \to r$
xiv. r
xv. 0 ■

(c) Direct proof:

i. $\neg s \vee p$ Premise
ii. s Added premise (conditional conclusion)
iii. $\neg(\neg s)$ Involution (2)
iv. p Disjunctive simplification (1), (3)
v. $p \to (q \to r)$ Premise
vi. $q \to r$ Detachment (4), (5)
vii. q Premise
viii. r Detachment (6), (7) ■

Indirect proof:

i. $\neg(s \to r)$ Negated conclusion
ii. $\neg(\neg s \vee r)$ Conditional equivalence (I)
iii. $s \wedge \neg r$ DeMorgan (2)
iv. s Conjunctive simplification (3)

v. $\neg s \vee p$ Premise

vi. $s \rightarrow p$ Conditional equivalence (5)

vii. p Detachment (4), (6)

viii. $p \rightarrow (q \rightarrow r)$ Premise

ix. $q \rightarrow r$ Detachment (7), (8)

x. q Premise

xi. r Detachment (9), (10)

xii. $\neg r$ Conjunctive simplification (3)

xiii. 0 Conjunction (11), (12) ■

(d) Direct proof:

i. $p \rightarrow q$

ii. $q \rightarrow r$

iii. $p \rightarrow r$

iv. $p \vee r$

v. $\neg p \vee r$

vi. $(p \vee r) \wedge (\neg p \vee r)$

vii. $(p \wedge \neg p) \vee r$

viii. $0 \vee r$

ix. r■

Indirect proof:

i. $\neg r$ Negated conclusion

ii. $p \vee r$ Premise

iii. p (1), (2)

iv. $p \rightarrow q$ Premise

v. q Detachment (3), (4)

vi. $q \rightarrow r$ Premise

vii. r Detachment (5), (6)

viii. 0 (1), (7) ■

5. Are the following arguments valid? If they are valid, construct formal proofs; if they aren't valid, explain why not.

(a) If wages increase, then there will be inflation. The cost of living will not increase if there is no inflation. Wages will increase. Therefore, the cost of living will increase.

(b) If the races are fixed or the casinos are crooked, then the tourist trade will decline. If the tourist trade decreases, then the police will be happy. The police force is never happy. Therefore, the races are not fixed.

(a) Let W stand for "Wages will increase,"I stand for "there will be inflation," and C stand for "cost of living will increase." Therefore the argument is: $W \to I$, $\neg I \to \neg C$, $W \Rightarrow C$.. The argument is invalid. The easiest way to see this is through a truth table. Let x be the conjunction of all premises.

W	I	C	$\neg I$	$\neg C$	$W \to I$	$\neg I \to \neg C$	x	$x \to C$
0	0	0	1	1	1	0	0	1
0	0	1	1	0	1	1	0	1
0	1	0	0	1	1	1	0	1
0	1	1	0	0	1	1	0	1
1	0	0	1	1	0	0	0	1
1	0	1	1	0	0	1	0	1
1	1	0	0	1	1	1	1	1
1	1	1	0	0	1	1	1	0

(b) Let r stand for "the races are fixed," c stand for "casinos are crooked," t stand for "the tourist trade will decline," and p stand for "the police will be happy." Therefore, the argument is:

$$(r \vee c) \to t, t \to p, \neg p \to \neg r$$

. The argument is valid. Proof:

i. $t \to p$ Premise

ii. $\neg p$ Premise

iii. $\neg t$ Indirect Reasoning (1), (2)

iv. $(r \vee c) \to t$ Premise

v. $\neg(r \vee c)$ Indirect Reasoning (3), (4)

vi. $(\neg r) \wedge (\neg c)$ DeMorgan (5)

vii. $\neg r$ Conjunction simplification (6) ■

7. Describe how $p_1, p_1 \to p_2, \ldots, p_{99} \to p_{100} \Rightarrow p_{100}$ could be proven in 199 steps.

$p_1 \to p_k$ and $p_k \to p_{k+1}$ implies $p_1 \to p_{k+1}$. It takes two steps to get to $p_1 \to p_{k+1}$ from $p_1 \to p_k$ This means it takes $2(100-1)$ steps to get to $p_1 \to p_{100}$ (subtract 1 because $p_1 \to p_2$ is stated as a premise). A final step is needed to apply detachment to imply p_{100}

3.6.2 Exercises for Section 3.6

1. If $U = \mathcal{P}(\{1,2,3,4\})$, what are the truth sets of the following propositions?

(a) $A \cap \{2,4\} = \emptyset$.

(b) $3 \in A$ and $1 \notin A$.

(c) $A \cup \{1\} = A$.

(d) A is a proper subset of $\{2,3,4\}$.

(e) $|A| = |A^c|$.

(a) $\{\{1\},\{3\},\{1,3\},\emptyset\}$

(b) $\{\{3\},\{3,4\},\{3,2\},\{2,3,4\}\}$

(c) $\{\{1\},\{1,2\},\{1,3\},\{1,4\},\{1,2,3\},\{1,2,4\},\{1,3,4\},\{1,2,3,4\}\}$

(d) $\{\{2\},\{3\},\{4\},\{2,3\},\{2,4\},\{3,4\}\}$

(e) $\{A \subseteq U : |A| = 2\}$

2. Over the universe of positive integers, define

$p(n)$: n is prime and $n < 32$.
$q(n)$: n is a power of 3.
$r(n)$: n is a divisor of 27.

(a) What are the truth sets of these propositions?

(b) Which of the three propositions implies one of the others?

(a) i. $T_p = \{2,3,5,7,11,13,17,19,23,29,31\}$
ii. $T_q = \{1,3,9,27,81,\dots\}$
iii. $T_r = \{1,3,9,27\}$

(b) $r \Rightarrow q$

3. If $U = \{0,1,2\}$, how many propositions over U could you list without listing two that are equivalent?

There are $2^3 = 8$ subsets of U, allowing for the possibility of 2^8 nonequivalent propositions over U.

5. Suppose that s is a proposition over $\{1,2,\dots,8\}$. If $T_s = \{1,3,5,7\}$, give two examples of propositions that are equivalent to s.

Two possible answers: s is odd and $(s-1)(s-3)(s-5)(s-7) = 0$

7. Let the universe be $\mathbb{Z}$, the set of integers. Which of the following propositions are equivalent over $\mathbb{Z}$?

a: $0 < n^2 < 9$
b: $0 < n^3 < 27$
c: $0 < n < 3$

b and c

3.7.3 Exercises for Section 3.7

1. Prove that the sum of the first n odd integers equals n^2 .

We wish to prove that $P(n) : 1 + 3 + 5 + \cdots + (2n-1) = n^2$ is true for $n \geqslant 1$. Recall that the nth odd positive integer is 2n - 1.

Basis: for $n = 1$, $P(n)$ is $1 = 1^2$, which is true

Induction: Assume that for some $n \geqslant 1, P(n)$ is true. Then:

$$\begin{aligned} 1 + 3 + \cdots + (2(n+1)-1) &= (1 + 3 + \cdots + (2n-1)) + (2(n+1)-1) \\ &= n^2 + (2n+1) \quad \text{by } P(n) \text{ and basic algebra} \\ &= (n+1)^2 \quad \blacksquare \end{aligned}$$

3. Prove that for $n \geq 1$: $\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$.

Proof:

- Basis: $1 = 1(2)(3)/6 = 1$
- Induction: $\sum_1^{n+1} k^2 = \sum_1^n k^2 + (n+1)^2$

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

$= \frac{(n+1)(2n^2+7n+6)}{6}$

$= \frac{(n+1)(n+2)(2n+3)}{6}$ ■

5. Use mathematical induction to show that for $n \geq 1$,

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

Basis: For $n = 1$, we observe that $\frac{1}{(1\cdot 2)} = \frac{1}{(1+1)}$
Induction: Assume that for some $n \geqslant 1$, the formula is true.
Then: $\frac{1}{(1\cdot 2)} + \cdots + \frac{1}{((n+1)(n+2))} = \frac{n}{(n+1)} + \frac{1}{((n+1)(n+2))}$

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

$= \frac{(n+1)^2}{((n+1)(n+2))}$

$= \frac{(n+1)}{(n+2)}$ ■

7. The number of strings of n zeros and ones that contain an even number of ones is 2^{n-1}. Prove this fact by induction for $n \geq 1$.

Let A_n be the set of strings of zeros and ones of length n (we assume that $|A_n| = 2^n$ is known). Let E_n be the set of the "even" strings, and E_n^c = the odd strings. The problem is to prove that for $n \geqslant 1$, $|E_n| = 2^{n-1}$. Clearly, $|E_1| = 1$, and, if for some $n \geqslant 1, |E_n| = 2^{n-1}$, it follows that $|E_{n+1}| = 2^n$ by the following reasoning.

We partition E_{n+1} according to the first bit: $E_{n+1} = \{1s \mid s \in E_n^c\} \cup \{0s \mid s \in E_n\}$

Since $\{1s \mid s \in E_n^c\}$ and $\{0s \mid s \in E_n\}$ are disjoint, we can apply the addition law. Therefore,

$$\begin{aligned} |E_{n+1}| &= |E_n^c| + |E_n| \\ &= 2^{n-1} + (2^n - 2^{n-1}) = 2^n. \end{aligned}$$ ■

9. Suppose that there are n people in a room, $n \geq 1$, and that they all shake hands with one another. Prove that $\frac{n(n-1)}{2}$ handshakes will have occurred.

Assume that for n persons ($n \geqslant 1$), $\frac{(n-1)n}{2}$ handshakes take place. If one more person enters the room, he or she will shake hands with n people,

$$\begin{aligned} \frac{(n-1)n}{2} + n &= \frac{n^2 - n + 2n}{2} \\ &= \frac{n^2 + n}{2} = \frac{n(n+1)}{2} \\ &= \frac{((n+1)-1)(n+1)}{2} \end{aligned}$$

Also, for $n = 1$, there are no handshakes, which matches the conjectured formula:

$$\frac{(1-1)(1)}{2} = 0$$ ■.

11. Generalized associativity. It is well known that if a_1, a_2, and a_3 are numbers, then no matter what order the sums in the expression $a_1 + a_2 + a_3$ are taken in, the result is always the same. Call this fact $p(3)$ and assume it is true. Prove using course-of-values induction that if a_1, a_2, ..., and a_n are numbers, then no matter what order the sums in the expression $a_1 + a_2 + \cdots + a_n$ are taken in, the result is always the same.

Let $p(n)$ be "$a_1 + a_2 + \cdots + a_n$ has the same value no matter how it is evaluated."

Basis: $a_1 + a_2 + a_3$ may be evaluated only two ways. Since $+$ is associative, $(a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$. Hence, $p(3)$ is true.

Induction: Assume that for some $n \geq 3$, $p(3), p(4), \ldots, p(n)$ are all true. Now consider the sum $a_1 + a_2 + \cdots + a_n + a_{n+1}$. Any of the n additions in this expression can be applied last. If the jth addition is applied last, we have $c_j = (a_1 + a_2 + \cdots + a_j) + (a_{j+1} + \cdots + a_{n+1})$. No matter how the expression to the left and right of the j^{th} addition are evaluated, the result will always be the same by the induction hypothesis, specifically $p(j)$ and $p(n + 1 - j)$. We now can prove that $c_1 = c_2 = \cdots = c_n$. If $i < j$,

$$\begin{aligned} c_i &= (a_1 + a_2 + \cdots + a_i) + (a_{i+1} + \cdots + a_{n+1}) \\ &= (a_1 + a_2 + \cdots + a_i) + ((a_{i+1} + \cdots + a_j) + (a_{j+1} + \cdots + a_{n+1}) \\ &= ((a_1 + a_2 + \cdots + a_i) + ((a_{i+1} + \cdots + a_j)) + (a_{j+1} + \cdots + a_{n+1}) \\ &= ((a_1 + a_2 + \cdots + a_j)) + (a_{j+1} + \cdots + a_{n+1}) \\ &= c_j \qquad \square \end{aligned}$$

12. Let S be the set of all numbers that can be produced by applying any of the rules below in any order a finite number of times.

- Rule 1: $\frac{1}{2} \in S$
- Rule 2: $1 \in S$
- Rule 3: If a and b have been produced by the rules, then $ab \in S$.
- Rule 4: If a and b have been produced by the rules, then $\frac{a+b}{2} \in S$.

Prove that $a \in S \Rightarrow 0 \leq a \leq 1$.

The number of times the rules are applied should be the integer that you do the induction on.

13. Proofs involving objects that are defined recursively are often inductive. A recursive definition is similar to an inductive proof. It consists of a basis, usually the simple part of the definition, and the recursion, which defines complex objects in terms of simpler ones. For example, if x is a real number and n is a positive integer, we can define x^n as follows:

- Basis: $x^1 = x$.
- Recursion: if $n \geq 2$, $x^n = x^{n-1}x$.

For example, $x^3 = x^2x = (x^1x)x = (xx)x$.

Prove that if $n, m \in \mathbb{P}$, $x^{m+n} = x^m x^n$. There is much more on recursion in Chapter 8.

Let $p(m)$ be the proposition that $x^{m+n} = x^m x^n$ for all $n \geq 1$.

For $m \geqslant 1$, let $p(m)$ be $x^{n+m} = x^n x^m$ for all $n \geqslant 1$. The basis for this proof follows directly from the basis for the definition of exponentiation.

Induction: Assume that for some $m \geqslant 1, p(m)$ is true. Then

$$\begin{aligned} x^{n+(m+1)} &= x^{(n+m)+1} && \text{by associativity of integer addition} \\ &= x^{n+m}x^1 && \text{by recursive definition} \\ &= x^n x^m x^1 && \text{induction hypothesis} \\ &= x^n x^{m+1} && \text{recursive definition} \quad \square \end{aligned}$$

3.8.5 Exercises for Section 3.8

1. Let $C(x)$ be "x is cold-blooded," let $F(x)$ be "x is a fish," and let $S(x)$ be "x lives in the sea."

(a) Translate into a formula: Every fish is cold-blooded.

(b) Translate into English: $(\exists x)(S(x) \wedge \neg F(x))$

(c) $(\forall x)(F(x) \rightarrow S(x))$.

(a) $(\forall x)(F(x) \rightarrow G(x))$

(b) There are objects in the sea which are not fish.

(c) Every fish lives in the sea.

3. Over the universe of books, define the propositions $B(x)$: x has a blue cover, $M(x)$: x is a mathematics book, $U(x)$: x is published in the United States, and $R(x, y)$: The bibliography of x includes y.

Translate into words:

(a) $(\exists x)(\neg B(x))$.

(b) $(\forall x)(M(x) \wedge U(x) \rightarrow B(x))$.

(c) $(\exists x)(M(x) \wedge \neg B(x))$.

(d) $(\exists y)((\forall x)(M(x) \rightarrow R(x, y)))$.Express using quantifiers:

(e) Every book with a blue cover is a mathematics book.

(f) There are mathematics books that are published outside the United States.

(g) Not all books have bibliographies.

(a) There is a book with a cover that is not blue.

(b) Every mathematics book that is published in the United States has a blue cover.

(c) There exists a mathematics book with a cover that is not blue.

(d) There exists a book that appears in the bibliography of every mathematics book.

(e) $(\forall x)(B(x) \rightarrow M(x))$

(f) $(\exists x)(M(x) \wedge \neg U(x))$

(g) $(\exists x)((\forall y)(\neg R(x,y))$

5. Translate into your own words and indicate whether it is true or false that $(\exists u)_{\mathbb{Z}}(4u^2 - 9 = 0)$.

The equation $4u^2 - 9 = 0$ has a solution in the integers. (False)

6. Use quantifiers to say that $\sqrt{3}$ is an irrational number.

Your answer will depend on your choice of a universe

7. What do the following propositions say, where U is the power set of $\{1, 2, \ldots, 9\}$? Which of these propositions are true?

(a) $(\forall A)_U |A| \neq |A^c|$.

(b) $(\exists A)_U (\exists B)_U (|A| = 5, |B| = 5, \text{ and } A \cap B = \emptyset)$

(c) $(\forall A)_U (\forall B)_U (A - B = B^c - A^c)$

(a) Every subset of U has a cardinality different from its complement. (True)

(b) There is a pair of disjoint subsets of U both having cardinality 5. (False)

(c) $A - B = B^c - A^c$ is a tautology. (True)

9. Use quantifiers to state that the sum of any two rational numbers is rational.

$(\forall a)_{\mathbb{Q}} (\forall b)_{\mathbb{Q}} (a + b$ is a rational number.)

10. Over the universe of real numbers, use quantifiers to say that the equation $a + x = b$ has a solution for all values of a and b.

You will need three quantifiers.

11. Let n be a positive integer. Describe using quantifiers:

(a) $x \in \bigcup_{k=1}^{n} A_k$

(b) $x \in \bigcap_{k=1}^{n} A_k$

Let $I = \{1, 2, 3, \ldots, n\}$

(a) $(\exists x)_I \, (x \in A_i)$

(b) $(\forall x)_I \, (x \in A_i)$

3.9.3 Exercises for Section 3.9

1. Prove that the sum of two odd positive integers is even.

The given statement can be written in if ... , then ... format as: If x and y are two odd positive integers, then $x + y$ is an even integer.

Proof: Assume x and y are two positive odd integers. It can be shown that $x + y = 2 \cdot$ (some positive integer).

x odd $\Rightarrow x = 2m + 1$ for some $m \in \mathbb{P}$,

y odd $\Rightarrow y = 2n + 1$ for some $n \in \mathbb{P}$.

Then,

$$x + y = (2m + 1) + (2n + 1) = 2((m + n) + 1) = 2 \cdot (\text{some positive integer})$$

Therefore, $x + y$ is even. $\square$

3. Write out a complete proof that $\sqrt{2}$ is irrational.

Proof: (Indirect) Assume to the contrary, that $\sqrt{2}$ is a rational number. Then there exists $p, q \in \mathbb{Z}, (q \neq 0)$ where $\frac{p}{q} = \sqrt{2}$ and where $\frac{p}{q}$ is in lowest terms, that is, p and q have no common factor other than 1.

$\frac{p}{q} = \sqrt{2} \Rightarrow \frac{p^2}{q^2} = 2 \Rightarrow p^2 = 2q^2 \Rightarrow p^2$is an even integer$\Rightarrow$ p is an even integer (see Exercise 2) 4 is a factor of $p^2 \Rightarrow q^2 \Rightarrow$ is even$\Rightarrow$ q is even. Hence both p and q have a common factor, namely 2, which is a contradiction. □

5. Prove that if x and y are real numbers such that $x + y \leq 1$, then either $x \leq \frac{1}{2}$ or $y \leq \frac{1}{2}$.

Proof: (Indirect) Assume $x, y \in \mathbb{R}$ and $x + y \leqslant 1$. Assume to the contrary that $\left(x \leqslant \frac{1}{2} \text{or} y \leqslant \frac{1}{2}\right)$ is false, which is equivalent to $x > \frac{1}{2} \text{and} y > \frac{1}{2}$. Hence $x + y > \frac{1}{2} + \frac{1}{2} = 1$. This contradicts the assumption that $x + y \leqslant 1$. ■

4.1.5 Exercises for Section 4.1

1. Prove the following:

(a) Let A, B, and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

(b) Let A and B be sets. Then $A - B = A \cap B^c$.

(c) Let $A, B,$ and C be sets. If ($A \subseteq B$ and$A \subseteq C$) then $A \subseteq B \cap C$.

(d) Let A and B be sets. $A \subseteq B$ If and only if $B^c \subseteq A^c$.

(e) Let $A, B,$ and C be sets. If $A \subseteq B$ then $A \times C \subseteq B \times C$.

(a) Assume that $x \in A$ (condition of the conditional conclusion $A \subseteq C$). Since $A \subseteq B$, $x \in B$ by the definition of $\subseteq$. $B \subseteq C$ and $x \in B$ implies that $x \in C$. Therefore, if $x \in A$, then $x \in C$. □

(b) (Proof that $A - B \subseteq A \cap B^c$) Let x be in $A - B$. Therefore, x is in A, but it is not in B; that is, $x \in A$ and $x \in B^c \Rightarrow x \in A \cap B^c$. □

(c) ($\Rightarrow$)Assume that $A \subseteq B$ and $A \subseteq C$. Let $x \in A$. By the two premises,$x \in B$ and $x \in C$. Therefore, by the definition of intersection, $x \in B \cap C$. □

(d) ($\Rightarrow$)(Indirect) Assume that $A \subseteq C$ and B^c is not a subset of A^c . Therefore, there exists $x \in B^c$ that does not belong to A^c. $x \notin A^c \Rightarrow x \in A$. Therefore, $x \in A$ and $x \notin B$, a contradiction to the assumption that $A \subseteq B$. □

3. Disprove the following, assuming $A, B,$ and C are sets:

(a) $A - B = B - A$.

(b) $A \times B = B \times A$.

(c) $A \cap B = A \cap C$ implies $B = C$.

(a) If $A = \mathbb{Z}$ and $B = \emptyset$, $A - B = \mathbb{Z}$, while $B - A = \emptyset$.

(b) If $A = \{0\}$ and $B = \{1\}$, $(0, 1) \in A \times B$, but $(0, 1)$ is not in $B \times A$.

(c) Let $A = \emptyset$, $B = \{0\}$, and $C = \{1\}$.

5. Prove by induction that if A, B_1 B_2 , . . . , B_n, are sets, $n \geq 2$, then $A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$

Proof: Let $p(n)$ be

$$A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$$

Basis: We must show that $p(2) : A \cap (B_1 \cup B_2) = (A \cap B_1) \cup (A \cap B_2)$ is true. This was done by several methods in section 4.1.

Induction: Assume for some $n \geq 2$ that $p(n)$ is true. Then

$$\begin{aligned} A \cap (B_1 \cup B_2 \cup \cdots \cup B_{n+1}) &= A \cap ((B_1 \cup B_2 \cup \cdots \cup B_n) \cup B_{n+1}) \\ &= (A \cap (B_1 \cup B_2 \cup \cdots \cup B_n)) \cup (A \cap B_{n+1}) \quad \text{by } p(2) \\ &= ((A \cap B_1) \cup \cdots \cup (A \cap B_n)) \cup (A \cap B_{n+1}) \quad \text{by the induction hypothesis} \\ &= (A \cap B_1) \cup \cdots \cup (A \cap B_n) \cup (A \cap B_{n+1}) \quad \square \end{aligned}$$

4.2.3 Exercises for Section 4.2"

1.

(a) Prove the associative law for intersection (Law 2') with a Venn diagram.

(b) Prove DeMorgan's Law (Law 9) with a membership table.

(c) Prove the Idempotent Law (Law 6) using basic definitions.

(a)

(b)

A	B	A^c	B^c	$A \cup B$	$(A \cup B)^c$	$A^c \cap B^c$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

The last two columns are the same so the two sets must be equal.

(c) (i) $x \in A \cup A \Rightarrow (x \in A) \vee (x \in A)$ by the definition of $\cap$. $\Rightarrow x \in A$ by the idempotent law of logic. Therefore, $A \cup A \subseteq A$.

(ii) $x \in A \Rightarrow (x \in A) \vee (x \in A)$ by conjunctive addition $\Rightarrow x \in A \cup A$. Therefore, $A \subseteq A \cup A$ and so we have $A \cup A = A$. $\square$

3. Prove the following using the set theory laws, as well as any other theorems proved so far.

(a) $A \cup (B - A) = A \cup B$

(b) $A - B = B^c - A^c$

(c) $A \subseteq B, A \cap C \neq \emptyset \Rightarrow B \cap C \neq \emptyset$

(d) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

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

For all parts of this exercise, a reason should be supplied for each step. We have supplied reasons only for part a and left them out of the other parts to give you further practice.

(a)

(b)

$$\begin{aligned} A - B &= A \cap B^c \\ &= B^c \cap A \\ &= B^c \cap (A^c)^c \\ &= B^c - A^c \end{aligned}$$

(c) Select any element, $x \in A \cap C$. One such element exists since $A \cap C$ is not empty.

$$\begin{aligned} x \in A \cap C &\Rightarrow x \in A \wedge x \in C \\ &\Rightarrow x \in B \wedge x \in C \\ &\Rightarrow x \in B \cap C \\ &\Rightarrow B \cap C \neq \emptyset \quad \square \end{aligned}$$

(d)

$$\begin{aligned} A \cap (B - C) &= A \cap (B \cap C^c) \\ &= (A \cap B \cap A^c) \cup (A \cap B \cap C^c) \\ &= (A \cap B) \cap (A^c \cup C^c) \\ &= (A \cap B) \cap (A \cup C)^c \\ &= (A - B) \cap (A - C) \quad \square \end{aligned}$$

(e)

$$\begin{aligned} A - (B \cup C) &= A \cap (B \cup C)^c \\ &= A \cap (B^c \cap C^c) \\ &= (A \cap B^c) \cap (A \cap C^c) \\ &= (A - B) \cap (A - C) \quad \square \end{aligned}$$

5. The rules that determine the order of evaluation in a set expression that involves more than one operation are similar to the rules for logic. In the absence of parentheses, complementations are done first, intersections second, and unions third. Parentheses are used to override this order. If the same operation appears two or more consecutive times, evaluate from left to right. In what order are the following expressions performed?

(a) $A \cup B^c \cap C$.

(b) $A \cap B \cup C \cap B$.

(c) $A \cup B \cup C^c$

(a) $A \cup ((B^c) \cap C)$ (b) $(A \cap B) \cup (C \cap B)$ (c) $(A \cup B) \cup (C^c)$

4.3.1 Exercises for Section 4.3

1. Consider the subsets $A = \{1, 7, 8\}$, $B = \{1, 6, 9, 10\}$, and$C = \{1, 9, 10\}$, where $U = \{1, 2, ..., 10\}$.

(a) List the nonempty minsets generated by $A, B,$ and C.

(b) How many elements of the power set of U can be generated by A, B, and C? Compare this number with $| \mathcal{P}(U) |$. Give an example of one subset that cannot be generated by A, B, and C.

(a) $\{1\}, \{2, 3, 4, 5\}, \{6\}, \{7, 8\}, \{9, 10\}$

(b) 2^5 , as compared with 2^{10}. $\{1, 2\}$ is one of the 992 sets that can't be generated.

3. Partition the set of strings of 0's and 1's of length two or less, using the minsets generated by $B_1 = \{s \mid s \text{ has length } 2\}$, and $B_2 = \{s \mid s \text{ starts with a } 0\}$.

$B_1 = \{00, 01, 10, 11\}$ and $B_2 = \{0, 00, 01\}$ generate minsets $\{00, 01\}, \{0\}, \{10, 11\}$, and $\{\lambda, 1\}$. Note: λ is the null string, which has length zero.

5.

(a) Partition $A = \{0, 1, 2, 3, 4, 5\}$ with the minsets generated by $B_1 = \{0, 2, 4\}$ and $B_2 = \{1, 5\}$.

(b) How many different subsets of A can you generate from B_1 and B_2?

(a) $B_1 \cap B_2 = \emptyset$, $B_1 \cap B_2^c = \{0, 2, 4\}$, $B_1^c \cap B_2 = \{1, 5\}$, $B_1^c \cap B_2^c = \{3\}$

(b) 2^3, since there are 3 nonempty minsets.

7. Prove Theorem 4.3.5

Let $a \in A$. For each i, $a \in B_i$, or $a \in {B_i}^c$, since $B_i \cup {B_i}^c = A$ by the complement law. Let $D_i = B_i$ if $a \in B_i$, and $D = {B_i}^c$ otherwise. Since a is in each D_i, it must be in the minset $D_1 \cap D_2 \cdots \cap D_n$. Now consider two different minsets $M_1 = D_1 \cap D_2 \cdots \cap D_n$, and $M_2 = G_1 \cap G_2 \cdots \cap G_n$, where each D_i and G_i is either B_i or ${B_i}^c$. Since these minsets are not equal, $D_i \neq G_i$, for some i. Therefore, $M_1 \cap M_2 = D_1 \cap D_2 \cdots \cap D_n \cap G_1 \cap G_2 \cdots \cap G_n = \emptyset$, since two of the sets in the intersection are disjoint. Since every element of A is in a minset and the minsets are disjoint, the nonempty minsets must form a partition of A. □

4.4.1 Exercises for Section 4.4

1. State the dual of:

(a) $A \cup (B \cap A) = A$.

(b) $A \cup ((B^c \cup A) \cap B)^c = U$

(c) $(A \cup B^c)^c \cap B = A^c \cap B$

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

(b) $A \cap ((B^c \cap A) \cup B)^c = \emptyset$

(c) $(A \cap B^c)^c \cup B = A^c \cup B$

3. Write the dual of:

(a) $p \vee \neg((\neg q \vee p) \wedge q) \Leftrightarrow 1$

(b) $(\neg(p \wedge (\neg q)) \vee q \Leftrightarrow (\neg p \vee q)$.

(a) $(p \wedge \neg(\neg q \wedge p) \vee g)) \Leftrightarrow 0$

(b) $(\neg(p \vee (\neg q)) \wedge q) \Leftrightarrow ((\neg p) \wedge q)$

5. Let $A = \{1, 2, 3, 4, 5, 6\}$ and let $B_1 = \{1, 3, 5\}$ and $B_2 = \{1, 2, 3\}$.

(a) Find the maxsets generated by B_1 and B_2. Note the set of maxsets does not constitute a partition of A. Can you explain why?

(b) Write out the definition of maxset normal form.

(c) Repeat Exercise 4.3.1.4 for maxsets.

The maxsets are:

- $B_1 \cup B_2 = \{1, 2, 3, 5\}$
- $B_1 \cup {B_2}^c = \{1, 3, 4, 5, 6\}$
- ${B_1}^c \cup B_2 = \{1, 2, 3, 4, 6\}$
- ${B_1}^c \cup {B_2}^c = \{2, 4, 5, 6\}$

They do not form a partition of A since it is not true that the intersection of any two of them is empty. A set is said to be in **maxset normal form** when it is expressed as the intersection of distinct nonempty maxsets or it is the universal set U.

5.1.4 Exercises

1. Let $A = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 3 & -5 \end{pmatrix}$, and $C = \begin{pmatrix} 0 & 1 & -1 \\ 3 & -2 & 2 \end{pmatrix}$

(a) Compute AB and BA.

(b) Compute $A + B$ and $B + A$.

(c) If $c = 3$, show that $c(A + B) = cA + cB$.

(d) Show that $(AB)C = A(BC)$.

(e) Compute A^2C.

(f) Compute $B + \mathbf{0}$

(g) Compute $A\mathbf{0}_{2\times 2}$ and $\mathbf{0}_{2\times 2}A$, where $\mathbf{0}_{2\times 2}$ is the 2×2 zero matrix

(h) Compute $0A$, where 0 is the real number (scalar) zero.

(i) Let $c = 2$ and $d = 3$. Show that$(c + d)A = cA + dA$.

For parts c, d and i of this exercise, only a verification is needed. Here, we supply the result that will appear on both sides of the equality.

(a) $AB = \begin{pmatrix} -3 & 6 \\ 9 & -13 \end{pmatrix}$ $BA = \begin{pmatrix} 2 & 3 \\ -7 & -18 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 0 \\ 5 & -2 \end{pmatrix}$

(c) $\begin{pmatrix} 3 & 0 \\ 15 & -6 \end{pmatrix}$

(d) $\begin{pmatrix} 18 & -15 & 15 \\ -39 & 35 & -35 \end{pmatrix}$

(e) $\begin{pmatrix} -12 & 5 & -5 \\ 5 & -25 & 25 \end{pmatrix}$

(f) $B + 0 = B$

(g) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(h) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(i) $\begin{pmatrix} 5 & -5 \\ 10 & 15 \end{pmatrix}$

3. Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$. Find a matrix B such that $AB = I$ and $BA = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\begin{pmatrix} 1/2 & 0 \\ 0 & 1/3 \end{pmatrix}$

5. Find A^3 if $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. What is A^{15} equal to?

$A^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 27 \end{pmatrix}$ $A^{15} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 32768 & 0 \\ 0 & 0 & 14348907 \end{pmatrix}$

7.

(a) If $A = \begin{pmatrix} 2 & 1 \\ 1 & -1 \end{pmatrix}$, $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, and $B = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$, show that $AX = B$ is a way of expressing the system $2x_1 + x_2 = 3$

$x_1 - x_2 = 1$ using matrices.

(b) Express the following systems of equations using matrices:

i. $2x_1 - x_2 = 4$

$x_1 + x_2 = 0$

ii. $x_1 + x_2 + 2x_3 = 1$

$x_1 + 2x_2 - x_3 = -1$

$x_1 + 3x_2 + x_3 = 5$

iii. $x_1 + x_2 \ = 3$

$x_2 \ = 5$

$x_1 \ + 3x_3 = 6$

(a) $Ax = \begin{pmatrix} 2x_1 + 1x_2 \\ 1x_1 - 1x_2 \end{pmatrix}$ equals $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$ if and only if both of the equalities $2x_1 + x_2 = 3$ and $x_1 - x_2 = 1$ are true.

(b) (i) $A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ $B = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 1 & 3 & 1 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ $B = \begin{pmatrix} 1 \\ -1 \\ 5 \end{pmatrix}$

(d) $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 3 \end{pmatrix}$ $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ $B = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix}$

5.2.1 Exercises

1. For the given matrices A find A^{-1} if it exists and verify that $AA^{-1} = A^{-1}A = I$. If A^{-1} does not exist explain why.

(a) $A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$

(b) $A = \begin{pmatrix} 6 & -3 \\ 8 & -4 \end{pmatrix}$

(c) $A = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}$

(d) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

(e) Use the definition of the inverse of a matrix to find A^{-1}: $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & -5 \end{pmatrix}$

(a) $\begin{pmatrix} -1/5 & 3/5 \\ 2/5 & -1/5 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$

(c) No inverse exists.

(d) $A^{-1} = A$

(e) $\begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1/5 \end{pmatrix}$

3.

(a) Let $A = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 3 & -3 \\ 2 & 1 \end{pmatrix}$. Verify that $(AB)^{-1} = B^{-1}A^{-1}$.

(b) Let A and B be $n \times n$ invertible matrices. Prove that $(AB)^{-1} = B^{-1}A^{-1}$. Why is the right side of the above statement written "backwards"? Is this necessary? Hint: Use Theorem 5.2.6

Let A and B be n by n invertible matrices.

$$\begin{aligned} \left(B^{-1}A^{-1}\right)(AB) &= \left(B^{-1}\right)\left(A^{-1}(AB)\right) \\ &= \left(B^{-1}\right)\left(\left(A^{-1}A\right)B\right) \\ &= \left(\left(B^{-1}\right)IB\right) \\ &= B^{-1}(B) \\ &= I \end{aligned}$$

Similarly, $(AB)\left(B^{-1}A^{-1}\right) = I$.

By Theorem 5.2.6, $B^{-1}A^{-1}$ is the only inverse of AB. If we tried to invert AB with $A^{-1}B^{-1}$, we would be unsuccessful since we cannot rearrange the order of the matrices.

5.

(a) Let A and B be as in Exercise 5.2.1.3. Show that $\det(AB) = (\det A)(\det B)$.

(b) It can be shown that the statement in part (a) is true for all $n \times n$ matrices. Let A be any invertible $n \times n$ matrix. Prove that $\det\left(A^{-1}\right) = (\det A)^{-1}$. Note: The determinant of the identity matrix I_n is 1 for all n.

(c) Verify that the equation in part (b) is true for the matrix in exercise l(a) of this section.

$1 = \det I = \det\left(AA^{-1}\right) = \det A \ \det A^{-1}$. Now solve for $\det A^{-1}$.

7. Use the assumptions in Exercise 5.2.1.5 to prove by induction that if $n \geq 1$, $\det\left(A^n\right) = (\det A)^n$.

Basis: $(n = 1) : \det A^1 = \det A = (\det A)^1$

Induction: Assume $\det A^n = (\det A)^n$ for some $n \geq 1$.

$$\begin{aligned}
\det A^{n+1} &= \det\left(A^n A\right) && \text{by the definition of exponents} \\
&= \det\left(A^n\right)\det(A) && \text{by exercise 5} \\
&= detA)^n(\det A) && \text{by the induction hypothesis} \\
&= (\det A)^{n+1}
\end{aligned}$$

9.

(a) Let A, B, and D be $n \times n$ matrices. Assume that B is invertible. If $A = BDB^{-1}$, prove by induction that $A^m = BD^mB^{-1}$ is true for $m \geq 1$.

(b) Given that $A = \begin{pmatrix} -8 & 15 \\ -6 & 11 \end{pmatrix} = B \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} B^{-1}$ where $B = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ what is A^{10}?

(a) Assume $A = BDB^{-1}$

Basis: $(m = 1)$: $A^1 = A = BD^1B^{-1}$ is given.

Induction: Assume that for some positive integer m, $A^m = BD^mB^{-1}$

$$\begin{aligned}
A^{m+1} &= A^m A \\
&= (BD^mB^{-1})(BDB^{-1}) && \text{by the induction hypothesis} \\
&= (BD^m(B^{-1}B)(DB^{-1}) && \text{by associativity} \\
&= BD^mDB^{-1} && \text{by the definition of inverse} \\
&= BD^{m+1}B^{-1} && \square
\end{aligned}$$

(b) $A^{10} = BD^{10}B^{-1} = \begin{pmatrix} -9206 & 15345 \\ -6138 & 10231 \end{pmatrix}$

5.3.1 Exercises

1. Rewrite the above laws specifying as in Example 5.3.2 the orders of the matrices.

Let A and B be m by n matrices. Then $A+B=B+A$,Let A, B, and C be m by n matrices. Then $A+(B+C)=(A+B)+C$.Let A and B be m by n matrices, and let $c\in\mathbb{R}$. Then $c(A+B)=cA+cB$,Let A be an m by n matrix, and let $c_1,c_2\in\mathbb{R}$. Then $(c_1+c_2)\,A=c_1A+c_2A$.Let A be an m by n matrix, and let $c_1,c_2\in\mathbb{R}$. Then $c_1\,(c_2A)=(c_1c_2)\,A$Let $\mathbf{0}$ be the zero matrix, of size m by n, and let A be a matrix of size n by r. Then $\mathbf{0}A=\mathbf{0}=$ the m by r zero matrix.Let A be an m by n matrix, and $0=$ the number zero. Then $0A=0=$ the m by n zero matrix.Let A be an m by n matrix, and let $\mathbf{0}$ be the m by n zero matrix. Then $A+\mathbf{0}=A$. Let A be an m by n matrix. Then $A+(-1)A=\mathbf{0}$, where $\mathbf{0}$ is the m by n zero matrix.Let A, B, and C be m by n, n by r, and n by r matrices respectively. Then $A(B+C)=AB+AC$.Let A, B, and C be m by n, r by m, and r by m matrices respectively. Then $(B+C)A=BA+CA$.Let A, B, and C be m by n, n by r, and r by p matrices respectively. Then $A(BC)=(AB)C$.Let A be an m by n matrix, I_m the m by m identity matrix, and I_n the n by n identity matrix. Then $I_mA=AI_n=A$Let A be an n by n matrix. Then if A^{-1} exists, $\left(A^{-1}\right)^{-1}=A$.Let A and B be n by n matrices. Then if A^{-1} and B^{-1} exist, $(AB)^{-1}=B^{-1}A^{-1}$.

3. Let $A=\begin{pmatrix}1&2\\0&-1\end{pmatrix}$, $B=\begin{pmatrix}3&7&6\\2&-1&5\end{pmatrix}$, and $C=\begin{pmatrix}0&-2&4\\7&1&1\end{pmatrix}$. Compute the following as efficiently as possible by using any of the Laws of Matrix Algebra:

(a) $AB+AC$

(b) A^{-1}

(c) $A(B+C)$

(d) $\left(A^2\right)^{-1}$

(e) $(C+B)^{-1}A^{-1}$

(a) $AB+AC=\begin{pmatrix}21&5&22\\-9&0&-6\end{pmatrix}$

(b) $A(B+C)=AB+BC$

(c) $A^{-1}=\begin{pmatrix}1&2\\0&-1\end{pmatrix}=A$

(d) $\left(A^2\right)^{-1}=(AA)^{-1}=(A^{-1}A)=I^{-1}=I$ by part c

5.4.2 Exercises

1. Discuss each of the "Matrix Oddities" with respect to elementary algebra.

In elementary algebra (the algebra of real numbers), each of the given oddities does not exist.

- AB may be different from BA. Not so in elementary algebra, since $ab=ba$ by the commutative law of multiplication.

- There exist matrices A and B such that $AB = \mathbf{0}$, yet $A \neq \mathbf{0}$and $B \neq \mathbf{0}$. In elementary algebra, the only way $ab = 0$ is if either a or b is zero. There are no exceptions.
- There exist matrices A, $A \neq \mathbf{0}$, yet $A^2 = \mathbf{0}$. In elementary algebra, $a^2 = 0 \Leftrightarrow a = 0$.
- There exist matrices $A^2 = A$. where $A \neq \mathbf{0}$ and $A \neq I$. In elementary algebra, $a^2 = a \Leftrightarrow a = 0$ or 1.
- There exist matrices A where $A^2 = I$ but $A \neq I$ and $A \neq -I$. In elementary algebra, $a^2 = 1 \Leftrightarrow a = 1$ or -1.

3. Prove the following implications, if possible:

(a) $A^2 = A$ and $\det A \neq 0 \Rightarrow A = I$

(b) $A^2 = I$ and $\det A \neq 0 \Rightarrow A = I$ or $A = -I$.

(a) $\det A \neq 0 \Rightarrow A^{-1}$ exists, and if you multiply the equation $A^2 = A$ on both sides by A^{-1} , you obtain $A = I$.

(b) Counterexample: $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

5. Write each of the following systems in the form $AX = B$, and then solve the systems using matrices.

(a) $2x_1 + x_2 = 3$
$x_1 - x_2 = 1$

(b) $2x_1 - x_2 = 4$
$x_1 - x_2 = 0$

(c) $2x_1 + x_2 = 1$
$x_1 - x_2 = 1$

(d) $2x_1 + x_2 = 1$
$x_1 - x_2 = -1$

(e) $3x_1 + 2x_2 = 1$
$6x_1 + 4x_2 = -1$

(a) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 4/3$, and $x_2 = 1/3$

(b) $A^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & -2 \end{pmatrix}$ $x_1 = 4$, and $x_2 = 4$

(c) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 2/3$, and $x_2 = -1/3$

(d) $A^{-1} = \begin{pmatrix} 1/3 & 1/3 \\ 1/3 & -2/3 \end{pmatrix}$ $x_1 = 0$, and $x_2 = 1$

(e) The matrix of coefficients for this system has a zero determinant; therefore, it has no inverse. The system cannot be solved by this method. In fact, the system has no solution.

6.1.1 Exercises

1. For each of the following relations r defined on $\mathbb{P}$, determine which of the given ordered pairs belong to r.

(a) xry iff $x|y$; (2, 3), (2, 4), (2, 8), (2, 17)

(b) xry iff $x \leq y$; (2, 3), (3, 2), (2, 4), (5, 8)

(c) xry iff $y = x^2$; (1,1), (2, 3), (2, 4), (2, 6)

(a) $(2, 4), (2, 8)$

(b) $(2, 3), (2, 4), (5, 8)$

(c) $(1, 1), (2, 4)$

3. Let $A = \{1, 2, 3, 4, 5\}$ and define r on A by xry iff $x+1 = y$. We define $r^2 = rr$ and $r^3 = r^2r$. Find:

(a) r

(b) r^2

(c) r^3

(a) $r = \{(1, 2), (2, 3), (3, 4), (4, 5)\}$

(b) $r^2 = \{(1, 3), (2, 4), (3, 5)\} = \{(x, y) : y = x + 2, x, y \in A\}$

(c) $r^3 = \{(1, 4), (2, 5)\} = \{(x, y) : y = x + 3, x, y \in A\}$

5. Let ρ be the relation on the power set, $\mathcal{P}(S)$, of a finite set S of cardinality n. Define ρ by $(A, B) \in \rho$ iff $A \cap B = \emptyset$.

(a) Consider the specific case $n = 3$, and determine the cardinality of the set ρ.

(b) What is the cardinality of ρ for an arbitrary n? Express your answer in terms of n. (Hint: There are three places that each element of S can go in building an element of ρ.)

(a) When $n = 3$, there are 27 pairs in the relation.

(b) Imagine building a pair of disjoint subsets of S. For each element of S there are three places that it can go: into the first set of the ordered pair, into the second set, or into neither set. Therefore the number of pairs in the relation is 3^n, by the product rule.

6.2.1 Exercises

1. Let $A = \{1, 2, 3, 4\}$, and let r be the relation $\leq$ on A Draw a digraph for r.

3. Let $A = \{1, 2, 3, 4, 5\}$. Define t on A by atb if and only if $b - a$ is even. Draw a digraph for t.

See Figure 13.1.1 of Section 13.1.

5. Recall the relation in Exercise 5 of Section 6.1, ρ defined on the power set, $\mathcal{P}(S)$, of a set S. The definition was $(A, B) \in \rho$ iff $A \cap B = \emptyset$. Draw the digraph for ρ where $S = \{a, b\}$.

A Hasse diagram cannot be used because not every set is related to itself. Also, $\{a\}$ and $\{b\}$ are related in both directions.

6.3.3 Exercises

1.

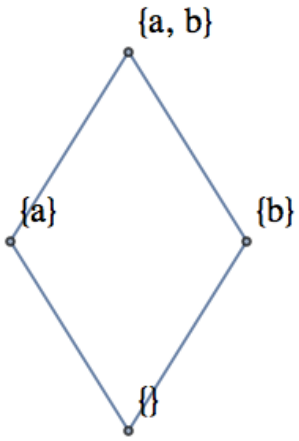
(a) Let $B = \{a, b\}$ and $U = \mathcal{P}(B)$. Draw a Hasse diagram for $\subseteq$ on U.

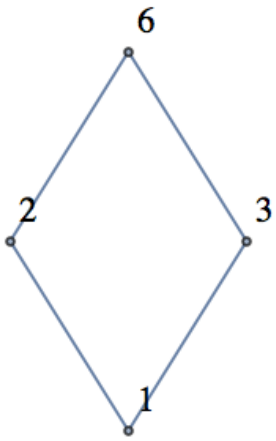
(b) Let $A = \{1, 2, 3, 6\}$. Show that divides, $|$, is a partial ordering on A.

(c) Draw a Hasse diagram for divides on A.

(d) Compare the graphs of parts a and c.

(a)





(b) The graphs are the same if we disregard the names of the vertices.

3.

(a) Consider the relations defined by the digraphs in Figure B.0.2. Determine whether the given relations are reflexive, symmetric, antisymmetric, or transitive. Try to develop procedures for determining the validity of these properties from the graphs,

(b) Which of the graphs are of equivalence relations or of partial orderings?

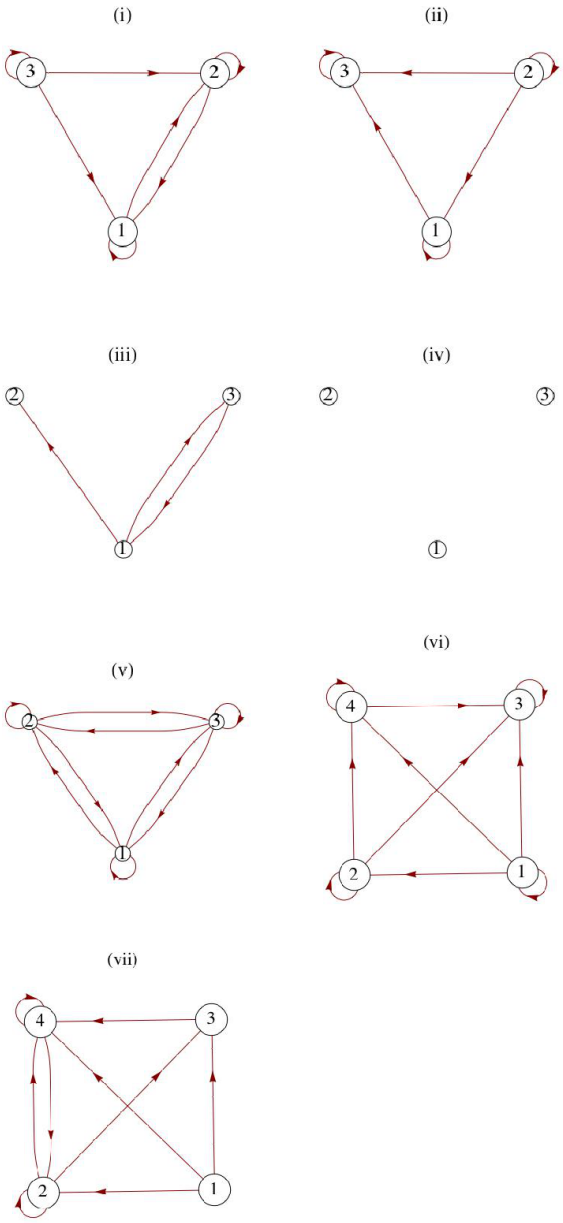


Figure B.0.2: Some diagraphs of relations

(a)

Part	reflexive?	symetric?	antisymmetric?	transitive?
i	yes	no	no	yes
ii	yes	no	yes	yes
iii	no	yes	no	yes
iv	no	yes	yes	yes
v	yes	yes	no	yes
vi	yes	no	yes	yes
vii	no	no	no	no

(b) Graphs ii and vi show partial ordering relations. Graph v is of an equivalence relation.

5. Consider the relation on $\{1,2,3,4,5,6\}$ defined by $r = \{(i,j) :| \ i-j \ |= 2\}$.

(a) Is r reflexive?

(b) Is r symmetric?

(c) Is r transitive?

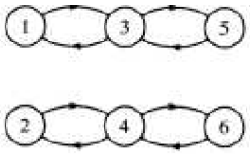
(d) Draw a graph of r.

(a) No, since $| \ 1-1 \ |= 0 \neq 2$, for example

(b) Yes, because $| \ i-j \ |=| \ j-i \ |$.

(c) No, since $| \ 2-4 \ |= 2$ and $| \ 4-6 \ |= 2$, but $| \ 2-6 \ |= 4 \neq 2$, for example.

(d)



7. Let $A = \{0,1,2,3\}$ and let

$$r = \{(0,0),(1,1),(2,2),(3,3),(1,2),(2,1),(3,2),(2,3),(3,1),(1,3)\}$$

(a) Verify that r is an equivalence relation on A.

(b) Let $a \in A$ and define $c(a) = \{b \in A \mid arb\}$. $c(a)$ is called the **equivalence class of** a **under** r. Find $c(a)$ for each element $a \in A$.

(c) Show that $\{c(a) \mid a \in A\}$ forms a partition of A for this set A.

(d) Let r be an equivalence relation on an arbitrary set A. Prove that the set of all equivalence classes under r constitutes a partition of A.

(a)

(b) $c(0) = \{0\}, c(1) = \{1,2,3\} = c(2) = c(3)$

(c) $c(0) \cup c(1) = A$ and $c(0) \cap c(1) = \emptyset$

(d) Let A be any set and let r be an equivalence relation on A. Let a be any element of A. $a \in c(a)$ since r is reflexive, so each element of A is in some equivalence class. Therefore, the union of all equivalence classes equals A. Next we show that any two equivalence classes are either identical or disjoint and we are done. Let $c(a)$ and $c(b)$ be two equivalence classes, and assume that $c(a) \cap c(b) \neq \emptyset$. We want to show that $c(a) = c(b)$. To show that $c(a) \subseteq c(b)$,

let $x \in c(a)$. $x \in c(a) \Rightarrow arx$. Also, there exists an element, y, of A that is in the intersection of $c(a)$ and $c(b)$ by our assumption. Therefore,

$$\begin{aligned} ary \wedge bry &\Rightarrow ary \wedge yrb \quad r \text{ is symmetric} \\ &\Rightarrow arb \quad \text{transitivity of } r \end{aligned}$$

Next,

$$\begin{aligned} arx \wedge arb &\Rightarrow xra \wedge arb \\ &\Rightarrow xrb \\ &\Rightarrow brx \\ &\Rightarrow x \in c(b) \end{aligned}$$

Similarly, $c(b) \subseteq c(a)$ $\square$

9. Consider the following relations on $\mathbb{Z}_8 = \{0, 1, ..., 7\}$. Which are equivalence relations? For the equivalence relations, list the equivalence classes.

(a) arb iff the English spellings of a and b begin with the same letter.

(b) asb iff $a - b$ is a positive integer.

(c) atb iff $a - b$ is an even integer.

(a) Equivalence Relation, $c(0) = \{0\}, c(1) = \{1\}, c(2) = \{2, 3\} = c(3), c(4) = \{4, 5\} = c(5)$, and $c(6) = \{6, 7\} = c(7)$

(b) Not an Equivalence Relation.

(c) Equivalence Relation, $c(0) = \{0, 2, 4, 6\} = c(2) = c(4) = c(6)$ and $c(1) = \{1, 3, 5, 7\} = c(3) = c(5) = c(7)$

11. In this exercise, we prove that implication is a partial ordering. Let A be any set of propositions.

(a) Verify that $q \rightarrow q$ is a tautology, thereby showing that $\Rightarrow$ is a reflexive relation on A.

(b) Prove that $\Rightarrow$ is antisymmetric on A. Note: we do not use $=$ when speaking of propositions, but rather equivalence, $\Leftrightarrow$.

(c) Prove that $\Rightarrow$ is transitive on A.

(d) Given that q_i is the proposition $n < i$ on $\mathbb{N}$, draw the Hasse diagram for the relation $\Rightarrow$ on $\{q_1, q_2, q_3, \ldots\}$.

(a)

(b) The proof follows from the biconditional equivalence in Table 3.4.2.

(c) Apply the chain rule.

(d)

6.4.1 Exercises

1. Let $A_1 = \{1, 2, 3, 4\}$, $A_2 = \{4, 5, 6\}$, and $A_3 = \{6, 7, 8\}$. Let r_1 be the relation from A_1 into A_2 defined by $r_1 = \{(x, y) \mid y - x = 2\}$, and let r_2 be the relation from A_2 into A_3 defined by $r_2 = \{(x, y) \mid y - x = 1\}$.

(a) Determine the adjacency matrices of r_1 and r_2.

(b) Use the definition of composition to find $r_1 r_2$.

(c) Verify the result in part by finding the product of the adjacency matrices of r_1 and r_2.

(a)
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array} \quad \text{and} \quad \begin{array}{c} \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccc} 6 & 7 & 8 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

(b) $r_1 r_2 = \{(3, 6), (4, 7)\}$

(c)
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} 6 & 7 & 8 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \end{array}$$

3. Suppose that the matrices in Example 6.4.3 are relations on $\{1, 2, 3, 4\}$. What relations do R and S describe?

R : xry if and only if $|x - y| = 1$
S : xsy if and only if x is less than y.

5. How many different reflexive, symmetric relations are there on a set with three elements?

Consider the possible matrices.

The diagonal entries of the matrix for such a relation must be 1. When the three entries above the diagonal are determined, the entries below are also determined. Therefore, there are 2^3 fitting the description.

7. Define relations p and q on $\{1, 2, 3, 4\}$ by $p = \{(a, b) \mid |a - b| = 1\}$ and $q = \{(a, b) \mid a - b \text{ is even}\}$

(a) Represent p and q as both graphs and matrices.

(b) Determine pq, p^2, and q^2; and represent them clearly in any way.

(a)
$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \quad \text{and} \quad \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

(b)
$$PQ = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

$$P^2 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} = Q^2$$

9. We define $\leq$ on the set of all $n \times n$ relation matrices by the rule that if R and S are any two $n \times n$ relation matrices, $R \leq S$ if and only if $R_{ij} \leq S_{ij}$ for all $1 \leq i, j \leq n$.

(a) Prove that $\leq$ is a partial ordering on all $n \times n$ relation matrices.

(b) Prove that $R \leq S \Rightarrow R^2 \leq S^2$, but the converse is not true.

(c) If R and S are matrices of equivalence relations and $R \leq S$, how are the equivalence classes defined by R related to the equivalence classes defined by S?

(a) Reflexive: $R_{ij} = R_{ij}$ for all i, j, therefore $R_{ij} \leq R_{ij}$

Antisymmetric: Assume $R_{ij} \leq S_{ij}$ and $S_{ij} \leq R_{ij}$ for all $1 \leq i, j \leq n$. Therefore, $R_{ij} = S_{ij}$ for all $1 \leq i, j \leq n$ and so $R = S$

Transitive: Assume R, S, and T are matrices where $R_{ij} \leq S_{ij}$ and $S_{ij} \leq T_{ij}$, for all $1 \leq i, j \leq n$. Then $R_{ij} \leq T_{ij}$ for all $1 \leq i, j \leq n$, and so $R \leq T$.

(b)

$$\begin{aligned}\left(R^2\right)_{ij} &= R_{i1}R_{1j} + R_{i2}R_{2j} + \cdots + R_{in}R_{nj} \\ &\leq S_{i1}S_{1j} + S_{i2}S_{2j} + \cdots + S_{in}S_{nj} \\ &= \left(S^2\right)_{ij} \Rightarrow R^2 \leq S^2\end{aligned}$$

To verify that the converse is not true we need only one example. For $n = 2$, let $R_{12} = 1$ and all other entries equal 0, and let S be the zero matrix. Since R^2 and S^2 are both the zero matrix, $R^2 \leq S^2$, but since $R_{12} > S_{12}, R \leq S$ is false.

(c) The matrices are defined on the same set $A = \{a_1, a_2, \ldots, a_n\}$. Let $c(a_i), i = 1, 2, \ldots, n$ be the equivalence classes defined by R and let $d(a_i)$ be those defined by S. Claim: $c(a_i) \subseteq d(a_i)$.

$$\begin{aligned}a_j \in c(a_i) &\Rightarrow a_i r a_j \\ &\Rightarrow R_{ij} = 1 \Rightarrow S_{ij} = 1 \\ &\Rightarrow a_i s a_j \\ &\Rightarrow a_j \in d(a_i)\end{aligned}$$

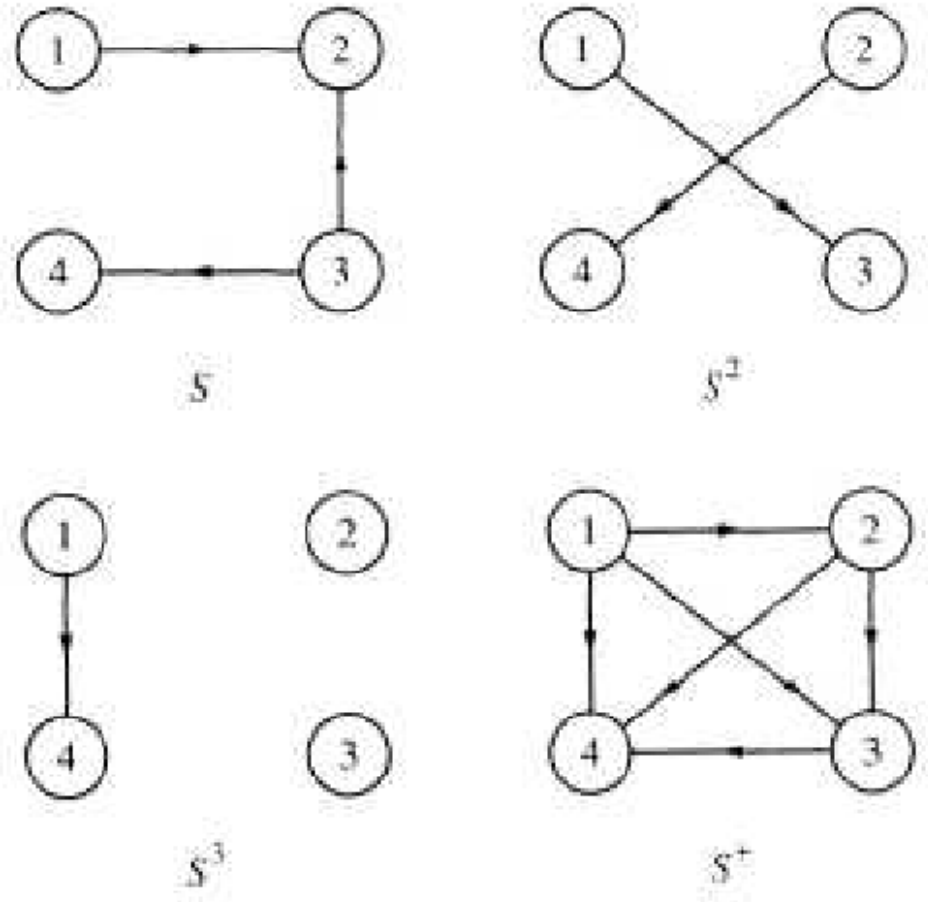
6.5.2 Exercises

3.

(a) Draw digraphs of the relations $\mathcal{S}$, $\mathcal{S}^2$, $\mathcal{S}^3$, and $\mathcal{S}^+$ where $\mathcal{S}$ is defined above.

(b) Verify that in terms of the graph of $\mathcal{S}$, $a\mathcal{S}^+b$ if and only if b is reachable from a along a path of any finite nonzero length.

(a)



(b) Example, $1s4$ and using S one can go from 1 to 4 using a path of length 3.

5.

(a) Define reflexive closure and symmetric closure by imitating the definition of transitive closure.

(b) Use your definitions to compute the reflexive and symmetric closures of examples in the text.

(c) What are the transitive reflexive closures of these examples?

(d) Convince yourself that the reflexive closure of the relation $<$ on the set of positive integers $\mathbb{P}$ is $\leq$.

Definition: Reflexive Closure. Let r be a relation on A. The reflexive closure of r is the smallest reflexive relation that contains r.

Theorem: The reflexive closure of r is the union of r with $\{(x, x) : x \in A\}$

7.

(a) Let A be any set and r a relation on A, prove that $(r^+)^+ = r^+$.

(b) Is the transitive closure of a symmetric relation always both symmetric and reflexive? Explain.

(a) By the definition of transitive closure, r^+ is the smallest relation which contains r; therefore, it is transitive. The transitive closure of r^+, $(r^+)^+$, is the smallest transitive relation that contains r^+. Since r^+ is transitive, $(r^+)^+ = r^+$.

(b) The transitive closure of a symmetric relation is symmetric, but it may not be reflexive. If one element is not related to any elements, then the transitive closure will not relate that element to others.

Exercises for An Introduction to Algorithms

2. What is wrong with this algorithm?

```
Input: a and b, integers
Output: the value of c will be a - b
(1) c = 0
(2) While a > b:
                (2.1) a := a - l
                (2.2) c := c + l
```

The algorithm only works when `a > b`.

Exercises for the Algorithms Appendix

2. Verify the correctness of the following algorithm to compute the greatest common divisor of two integers that are not both zero.

```
def gcd(a,b):
        r0=a
        r1=b
        while r1 !=0:
                t= r0 % r1
                r0=r1
                r1=t
        return r0

gcd(1001,154)  #test
```

The invariant of this algorithm is $gcd(r0, r1) = gcd(a, b)$.

Appendix C

Notation

The following table defines the notation used in this book. Page numbers or references refer to the first appearance of each symbol.

Symbol	Description	Page
$x \in A$	x is an element of A	1
$x \notin A$	x is not an element of A	1
$\|A\|$	The number of elements in a finite set A.	2
$A \subseteq B$	A is a subset of B.	2
$\emptyset$	the empty set	3
$A \cap B$	The intersection of A and B.	4
$A \cup B$	The union of A and B.	5
$B - A$	The complement of A relative to B.	6
A^c	The complement of A relative to the universe.	6
$A \oplus B$	The symmetric difference of A and B.	8
$A \times B$	The cartesian product of A with B.	12
$\mathcal{P}(A)$	The power set of A, the set of all subsets of A.	12
$n!$	n factorial, the product of the first n postitive integers	28
$\binom{n}{k}$	n choose k, the number of k element subsets of an n element set.	37
$p \wedge q$	the conjunction, p and q	44
$p \vee q$	the disjunction, p or q	44
$\neg p$	the negation of p, "not p"	45
$p \rightarrow q$	The conditional proposition If p then q.	45
$p \leftrightarrow q$	The biconditional proposition p if and only if q	46
1	symbol for a tautology	51
0	symbol for a contradiction	51
$r \iff s$	r is logically equivalent to s	51
$r \Rightarrow s$	r implies s	52
$p \mid q$	the Scheffer Stroke of p and q	54
T_p	the truth set of p	65
$(\exists n)_U(p(n))$	The statement that $p(n)$ is true for at least one value of n	75
$(\forall n)_U(p(n))$	The statement that $p(n)$ is always true.	76
$\mathbf{0}_{m \times n}$	the m by n zero matrix	107
I_n	The $n \times n$ identity matrix	110
A^{-1}	A inverse, the multiplicative inverse of A	110
$\det A$ or $\|A\|$	The determinant of A	111
$a \mid b$	a divides b, or a divides evenly into b	119

(Continued on next page)

Symbol	Description	Page
xsy	x is related to y through the relation s	120
rs	the composition of relation r with relation s	121
$a \equiv_m b$	a is congruent to b modulo m	131
$c(a)$	the equivalence class of a under r	194
r^+	The transitive closure of r	143
$\grave{x}, \acute{x}$	pre and post values of a variable x	153

Appendix D

Lists of Elements

D.1 List of Theorems

(Continued on next page)

D.2 List of Definitions

(Continued on next page)

Chapter 4 More on Sets

Chapter 5 Introduction to Matrix Algebra

Chapter 6 Relations

Chapter A.1 Appendix - Algorithms

Index