Lecture Notes in Discrete Mathematics

Marcel B. Finan
Arkansas Tech University

Preface

This book is designed for a one semester course in discrete mathematics for sophomore or junior level students. The text covers the mathematical concepts that students will encounter in many disciplines such as computer science, engineering, Business, and the sciences.
Besides reading the book, students are strongly encouraged to do all the exercises. Mathematics is a discipline in which working the problems is essential to the understanding of the material contained in this book. Students are strongly encouraged to keep up with the exercises and the sequel of concepts as they are going along, for mathematics builds on itself.
Instructors can request the solutions to the problems via email: mfinan@atu.edu
Finally, I would like to take the opportunity to thank Professor Vadim Ponomarenko from San Diego State University for pointing out to me many errors in the book and for his valuable suggestions.

Marcel B. Finan
May 2001

Contents

Fundamentals of Mathematical Logic

Logic is commonly known as the science of reasoning. The emphasis here will be on logic as a working tool. We will develop some of the symbolic techniques required for computer logic. Some of the reasons to study logic are the following:

- At the hardware level the design of 'logic' circuits to implement instructions is greatly simplified by the use of symbolic logic.
- At the software level a knowledge of symbolic logic is helpful in the design of programs.

1 Propositions and Related Concepts

A **proposition** is any meaningful statement that is either true or false, but not both. We will use lowercase letters, such as $p, q, r, \cdots$, to represent propositions. We will also use the notation

$$p : 1 + 1 = 3$$

to define p to be the proposition $1+1 = 3$. The **truth value** of a proposition is true, denoted by T, if it is a true statement and false, denoted by F, if it is a false statement. Statements that are not propositions include questions and commands.

Example 1.1
Which of the following are propositions? Give the truth value of the propositions.
a. $2 + 3 = 7$.
b. Julius Caesar was president of the United States.
c. What time is it?
d. Be quiet !

Solution.
a. A proposition with truth value (F).
b. A proposition with truth value (F).
c. Not a proposition since no truth value can be assigned to this statement.
d. Not a proposition ■

Example 1.2
Which of the following are propositions? Give the truth value of the propositions.
a. The difference of two primes.
b. $2 + 2 = 4$.
c. Washington D.C. is the capital of New York.
d. How are you?

Solution.
a. Not a proposition.
b. A proposition with truth value (T).
c. A proposition with truth value (F).

d. Not a proposition ■

New propositions called **compound propositions** or **propositional functions** can be obtained from old ones by using **symbolic connectives** which we discuss next. The propositions that form a propositional function are called the **propositional variables.**
Let p and q be propositions. The **conjunction** of p and q, denoted $p \wedge q$, is the proposition: p *and* q. This proposition is defined to be true only when both p and q are true and it is false otherwise. The **disjunction** of p and q, denoted $p \vee q$, is the proposition: p *or* q. The 'or' is used in an inclusive way. This proposition is false only when both p and q are false, otherwise it is true.

Example 1.3
Let

$$\begin{aligned} p: &\quad 5 < 9 \\ q: &\quad 9 < 7. \end{aligned}$$

Construct the propositions $p \wedge q$ and $p \vee q$.

Solution.
The conjunction of the propositions p and q is the proposition

$$p \wedge q : 5 < 9 \text{ and } 9 < 7.$$

The disjunction of the propositions p and q is the proposition

$$p \vee q : 5 < 9 \text{ or } 9 < 7 \ ■$$

Example 1.4
Consider the following propositions

$$\begin{aligned} p: &\quad \text{It is Friday} \\ q: &\quad \text{It is raining.} \end{aligned}$$

Construct the propositions $p \wedge q$ and $p \vee q$.

Solution.
The conjunction of the propositions p and q is the proposition

$$p \wedge q : \text{It is Friday and it is raining.}$$

The disjunction of the propositions p and q is the proposition

$$p \vee q : \text{It is Friday or It is raining} \blacksquare$$

A **truth table** displays the relationships between the truth values of propositions. Next, we display the truth tables of $p \wedge q$ and $p \vee q$.

p	q	p ∧ q
T	T	T
T	F	F
F	T	F
F	F	F

p	q	p ∨ q
T	T	T
T	F	T
F	T	T
F	F	F

Let p and q be two propositions. The **exclusive or** of p and q, denoted $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise. The truth table of the exclusive 'or' is displayed below

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

Example 1.5
a. Construct a truth table for $(p \oplus q) \oplus r$.
b. Construct a truth table for $p \oplus p$.

Solution.
a.

p	q	r	$p \oplus q$	(p ⊕ q) ⊕ r
T	T	T	F	T
T	T	F	F	F
T	F	T	T	F
T	F	F	T	T
F	T	T	T	F
F	T	F	T	T
F	F	T	F	T
F	F	F	F	F

b.

p	p $\oplus$ p
T	F
F	F

■

The final operation on a proposition p that we discuss is the **negation** of p. The negation of p, denoted $\sim p$, is the proposition not p. The truth table of $\sim p$ is displayed below

p	$\sim p$
T	F
F	T

Example 1.6
Consider the following propositions:
p: Today is Thursday.
q: $2 + 1 = 3$.
r: There is no pollution in New Jersey.
Construct the truth table of $[\sim (p \wedge q)] \vee r$.

Solution.

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

■

Example 1.7
Find the negation of the proposition $p : -5 < x \leq 0$.

Solution.
The negation of p is the proposition $\sim p : x > 0$ *or* $x \leq -5$ ■

A compound proposition is called a **tautology** if it is always true, regardless of the truth values of the basic propositions which comprise it.

Example 1.8
a. Construct the truth table of the proposition $(p \wedge q) \vee (\sim p \vee \sim q)$. Determine if this proposition is a tautology.
b. Show that $p \vee \sim p$ is a tautology.

Solution.
a.

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

Thus, the given proposition is a tautology.
b.

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

Again, this proposition is a tautology ■

Two propositions are **equivalent** if they have exactly the same truth values under all circumstances. We write $p \equiv q$.

Example 1.9
a. Show that $\sim (p \vee q) \equiv \sim p \wedge \sim q$.
b. Show that $\sim (p \wedge q) \equiv \sim p \vee \sim q$.
c. Show that $\sim (\sim p) \equiv p$.
a. and b. are known as DeMorgan's laws.

Solution.
a.

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

b.

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

c.

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

■

Example 1.10

a. Show that $p \wedge q \equiv q \wedge p$ and $p \vee q \equiv q \vee p$.

b. Show that $(p \vee q) \vee r \equiv p \vee (q \vee r)$ and $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$.

c. Show that $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ and $(p \vee q) \wedge r \equiv (p \wedge r) \vee (q \wedge r)$.

Solution.

a.

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

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

b.

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

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

c.

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

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

■

Example 1.11
Show that $\sim (p \wedge q) \not\equiv \sim p \wedge \sim q$

Solution.
We will use truth tables to prove the claim.

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

■

A compound proposition that has the value F for all possible values of the propositions in it is called a **contradiction**.

Example 1.12
Show that the proposition $p \wedge \sim p$ is a contradiction.

Solution.

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

■

In propositional functions, the order of operations is that $\sim$ is performed first. The operations $\vee$ and $\wedge$ are executed in any order.

Review Problems

Problem 1.1
Indicate which of the following sentences are propositions.
a. 1,024 is the smallest four-digit number that is perfect square.
b. She is a mathematics major.
c. $128 = 2^6$
d. $x = 2^6$.

Problem 1.2
Consider the propositions:
p: Juan is a math major.
q: Juan is a computer science major.

Use symbolic connectives to represent the proposition "Juan is a math major but not a computer science major."

Problem 1.3
In the following sentence is the word "or" used in its inclusive or exclusive sense? "A team wins the playoffs if it wins two games in a row or a total of three games."

Problem 1.4
Write the truth table for the proposition: $(p \vee (\sim p \vee q)) \wedge \sim (q \wedge \sim r)$.

Problem 1.5
Let t be a tautology. Show that $p \vee t \equiv t$.

Problem 1.6
Let c be a contradiction. Show that $p \vee c \equiv p$.

Problem 1.7
Show that $(r \vee p) \wedge [(\sim r \vee (p \wedge q)) \wedge (r \vee q)] \equiv p \wedge q$.

Problem 1.8
Use De Morgan's laws to write the negation for the proposition: "This computer program has a logical error in the first ten lines or it is being run with an incomplete data set."

Problem 1.9
Use De Morgan's laws to write the negation for the proposition: "The dollar is at an all-time high and the stock market is at a record low."

Problem 1.10
Assume $x \in \mathbb{R}$. Use De Morgan's laws to write the negation for the proposition:$0 \geq x > -5$.

Problem 1.11
Show that the proposition $s = (p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$ is a tautology.

Problem 1.12
Show that the proposition $s = (p \wedge \sim q) \wedge (\sim p \vee q)$ is a contradiction.

Problem 1.13
a. Find simpler proposition forms that are logically equivalent to $p \oplus p$ and $p \oplus (p \oplus p)$.
b. Is $(p \oplus q) \oplus r \equiv p \oplus (q \oplus r)$? Justify your answer.
c. Is $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$? Justify your answer.

Problem 1.14
Show the following:
a. $p \wedge t \equiv p$, where t is a tautology.
b. $p \wedge c \equiv c$, where c is a contradiction.
c. $\sim t \equiv c$ and $\sim c \equiv t$.
d. $p \vee p \equiv p$ and $p \wedge p \equiv p$.

2 Conditional and Biconditional Propositions

Let p and q be propositions. The implication $p \to q$ is the proposition that is false only when p is true and q is false; otherwise it is true. p is called the **hypothesis** and q is called the **conclusion.** The connective $\to$ is called the **conditional** connective.

Example 2.1
Construct the truth table of the implication $p \to q$.

Solution.
The truth table is

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

■

Example 2.2
Show that $p \to q \equiv \sim p \vee q$.

Solution.

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

■

It follows from the previous example that the proposition $p \to q$ is always true if the hypothesis p is false, regardless of the truth value of q. We say that $p \to q$ is **true by default** or **vacuously true**.
In terms of words the proposition $p \to q$ also reads:
(a) if p then q.
(b) p implies q.
(c) p is a sufficient condition for q.
(d) q is a necessary condition for p.
(e) p only if q.

Example 2.3
Use the if-then form to rewrite the statement "I am on time for work if I catch the 8:05 bus."

Solution.
If I catch the 8:05 bus then I am on time for work ■

In propositional functions that involve the connectives $\sim, \wedge, \vee$, and $\rightarrow$ the order of operations is that $\sim$ is performed first and $\rightarrow$ is performed last.

Example 2.4
a. Show that $\sim (p \rightarrow q) \equiv p \wedge \sim q$.
b. Find the negation of the statement " If my car is in the repair shop, then I cannot go to class."

Solution.
a. We use De Morgan's laws as follows.

$$\begin{aligned} \sim (p \rightarrow q) &\equiv \sim (\sim p \vee q) \\ &\equiv \sim (\sim p) \wedge \sim q \\ &\equiv p \wedge \sim q. \end{aligned}$$

b. "My car is in the repair shop and I can get to class." ■

The **converse** of $p \rightarrow q$ is the proposition $q \rightarrow p$. The **opposite** or **inverse** of $p \rightarrow q$ is the proposition $\sim p \rightarrow \sim q$. The **contrapositive** of $p \rightarrow q$ is the proposition $\sim q \rightarrow \sim p$.

Example 2.5
Find the converse, opposite, and the contrapositive of the implication: " If today is Thursday, then I have a test today."

Solution.
The converse: If I have a test today then today is Thursday.
The opposite: If today is not Thursday then I don't have a test today.
The contrapositive: If I don't have a test today then today is not Thursday ■

Example 2.6
Show that $p \rightarrow q \equiv \sim q \rightarrow \sim p$.

Solution.
We use De Morgan's laws as follows.

$$\begin{aligned} p \to q &\equiv \sim p \vee q \\ &\equiv \sim (p \wedge \sim q) \\ &\equiv \sim (\sim q \wedge p) \\ &\equiv \sim\sim q \vee \sim p \\ &\equiv q \vee \sim p \\ &\equiv \sim q \to \sim p \end{aligned}$$ ■

Example 2.7
Using truth tables show the following:
a. $p \to q \not\equiv q \to p$
b. $p \to q \not\equiv \sim p \to \sim q$

Solution.
a. It suffices to show that $\sim p \vee q \not\equiv \sim q \vee p$.

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

b. We will show that $\sim p \vee q \not\equiv p \vee \sim q$.

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

■

Example 2.8
Show that $\sim q \to \sim p \equiv p \to q$

Solution.
We use De Morgan's laws as follows.

$$\begin{aligned} \sim q \to \sim p &\equiv q \vee \sim p \\ &\equiv \sim (\sim q \wedge p) \\ &\equiv \sim (p \wedge \sim q) \\ &\equiv \sim p \vee \sim\sim q \\ &\equiv \sim p \vee q \\ &\equiv p \to q \end{aligned}$$ ■

The **biconditional** proposition of p and q, denoted by $p \leftrightarrow q$, is the propositional function that is true when both p and q have the same truth values and false if p and q have opposite truth values. Also reads, "p if and only if q" or "p is a necessary and sufficient condition for q."

Example 2.9
Construct the truth table for $p \leftrightarrow q$.

Solution.

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

■

Example 2.10
Show that the biconditional proposition of p and q is logically equivalent to the conjunction of the conditional propositions $p \rightarrow q$ and $q \rightarrow p$.

Solution.

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

■

The order of operations for the five logical connectives is as follows:

1. $\sim$
2. $\wedge, \vee$ in any order.
3. $\rightarrow, \leftrightarrow$ in any order.

Review Problems

Problem 2.1
Rewrite the following proposition in if−then form: " This loop will repeat exactly N times if it does not contain a **stop** or a **go to.**"

Problem 2.2
Construct the truth table for the proposition: $\sim p \vee q \to r$.

Problem 2.3
Construct the truth table for the proposition: $(p \to r) \leftrightarrow (q \to r)$.

Problem 2.4
Write negations for each of the following propositions. (Assume that all variables represent fixed quantities or entities, as appropriate.)
a. If P is a square, then P is a rectangle.
b. If today is Thanksgiving, then tomorrow is Friday.
c. If r is rational, then the decimal expansion of r is repeating.
d. If n is prime, then n is odd or n is 2.
e. If $x \geq 0$, then $x > 0$ or $x = 0$.
f. If Tom is Ann's father, then Jim is her uncle and Sue is her aunt.
g. If n is divisible by 6, then n is divisible by 2 and n is divisible by 3.

Problem 2.5
Write the contrapositives for the propositions of Problem 2.4.

Problem 2.6
Write the converse and inverse for the propositions of Problem 2.4.

Problem 2.7
Use the contrapositive to rewrite the proposition " The Cubs will win the penant only if they win tomorrow's game" in if−then form in two ways.

Problem 2.8
Rewrite the proposition : "Catching the 8:05 bus is sufficient condition for my being on time for work" in if−then form.

Problem 2.9
Use the contrapositive to rewrite the proposition "being divisible by 3 is a necessary condition for this number to be divisible by 9" in if−then form in two ways.

Problem 2.10
Rewrite the proposition "A sufficient condition for Hal's team to win the championship is that it wins the rest of the games" in if−then form.

Problem 2.11
Rewrite the proposition "A necessary condition for this computer program to be correct is that it not produce error messages during translation" in if−then form.

3 Rules of Inferential Logic

The main concern of logic is how the truth of some propositions is connected with the truth of another. Thus, we will usually consider a group of related propositions.
An **argument** is a set of two or more propositions related to each other in such a way that all but one of them (the **premises**) are supposed to provide support for the remaining one (the **conclusion**).
The transition from premises to conclusion is the **inference** upon which the argument relies.

Example 3.1
Show that the propositions "The star is made of milk, and strawberries are red. My dog has fleas." do not form an argument.

Solution.
Indeed, the truth or falsity of each of the propositions has no bearing on that of the others ■

Example 3.2
Show that the propositions: "Mark is a lawyer. So Mark went to law school since all lawyers have gone to law school" form an argument.

Solution.
This is an argument. The truth of the conclusion, "Mark went to law school," is inferred or deduced from its premises, "Mark is a lawyer" and "all lawyers have gone to law school." ■

The above argument can be represented as follows: Let
p: Mark is a lawyer.
q: All lawyers have gone to law school.
r: Mark went to law school.
Then

$$\begin{array}{ll} & p \wedge q \\ \therefore & r \end{array}$$

The symbol $\therefore$ is to indicate the inferrenced conclusion.

Now, suppose that the premises of an argument are all true. Then the

conclusion may be either true or false. When the conclusion is true then the argument is said to be **valid.** When the conclusion is false then the argument is said to be **invalid.**
To test an argument for validity one proceeds as follows:
(1) Identify the premises and the conclusion of the argument.
(2) Construct a truth table including the premises and the conclusion.
(3) Find rows in which all premises are true.
(4) In each row of Step (3), if the conclusion is true then the argument is valid; otherwise the argument is invalid.

Example 3.3
Show that the argument

$$\begin{array}{lll} p & \rightarrow & q \\ q & \rightarrow & p \\ \therefore & p \vee q & \end{array}$$

is invalid

Solution.
We construct the truth table as follows.

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

From the last row we see that the premises are true but the conclusion is false. The argument is then invalid ■

Example 3.4 *(Modus Ponens or the method of affirming)*
a. Show that the argument

$$\begin{array}{lll} p & \rightarrow & q \\ p & & \\ \therefore & q & \end{array}$$

is valid.
b. Show that the argument

$$\begin{array}{lll} \sim p \vee q & \rightarrow & r \\ \sim p \vee q & & \\ \therefore & r & \end{array}$$

is valid.

Solution.
a. The truth table is as follows.

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

The first row shows that the argument is valid.
b. Follows from (a) by replacing p with $\sim p \vee q$ and q with r ■

Example 3.5
Show that the argument

$$\begin{array}{lll} p & \to & q \\ q & & \\ \therefore & p & \end{array}$$

is invalid.

Solution.
The truth table is as follows.

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

Because of the third row the argument is invalid. An argument of this form is referred to as **converse error** because the conclusion of the argument would follows from the premises if $p \to q$ is replaced by its converse $q \to p$ ■

Example 3.6 *(Modus Tollens or the method of denial)*
Show that the argument

$$\begin{array}{lll} p & \to & q \\ \sim q & & \\ \therefore & \sim p & \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The last row shows that the argument is valid ■

Example 3.7
Show that the argument

$$\begin{array}{lll} p & \rightarrow & q \\ \sim p & & \\ \therefore & \sim q & \end{array}$$

is invalid.

Solution.
The truth table is as follows.

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

The third row shows that the argument is invalid. This is known as **inverse error** because the conclusion of the argument would follow from the premises if $p \rightarrow q$ is replaced by the inverse $\sim p \rightarrow \sim q$ ■

Example 3.8 *(Disjunctive Addition)*
a. Show that the argument

$$\begin{array}{ll} p & \\ \therefore & p \vee q \end{array}$$

is valid.
b. Show that the argument

$$\begin{array}{ll} q & \\ \therefore & p \vee q \end{array}$$

is valid.

Solution.
a. The truth table is as follows.

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

The first and second rows show that the argument is valid.
b. The first and third rows show that the argument is valid ■

Example 3.9 *(Conjunctive addition)*
Show that

$$\begin{array}{ll} & p, q \\ \therefore & p \wedge q \end{array}$$

Solution.
The truth table is as follows.

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

The first row shows that the argument is valid ■

Example 3.10 *(Conjunctive Simplification)*
a. Show that the argument

$$\begin{array}{ll} & p \wedge q \\ \therefore & p \end{array}$$

is valid.
b. Show that the argument

$$\begin{array}{ll} & p \wedge q \\ \therefore & q \end{array}$$

is valid.

Solution.
a. The truth table is as follows.

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

The first row shows that the argument is valid.
b. The first row shows that the argument is valid ■

Example 3.11 *(Disjunctive Syllogism)*
a. Show that the argument

$$\begin{array}{ll} & p \vee q \\ & \sim q \\ \therefore & p \end{array}$$

is valid.
b. Show that the argument

$$\begin{array}{ll} & p \vee q \\ & \sim p \\ \therefore & q \end{array}$$

is valid.

Solution.
a. The truth table is as follows.

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

The second row shows that the argument is valid.
b. The third row shows that the argument is valid ■

Example 3.12 *(Hypothetical Syllogism)*
Show that the argument

$$\begin{array}{ll} & p \to q \\ & q \to r \\ \therefore & p \to r \end{array}$$

is valid.

Solution.
The truth table is as follows.

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

The first , fifth, seventh, and eighth rows show that the argument is valid ■

Example 3.13 *(Rule of contradiction)*
Show that if c is a contradiction then the following argument is valid for any p.

$$\begin{array}{l} \sim p \to c \\ \therefore \quad p \end{array}$$

Solution.
Constructing the truth table we find

c	p	$\sim p \to c$
F	T	T
F	F	F

The first row shows that the argument is valid ■

Review Problems

Problem 3.1
Use modus ponens or modus tollens to fill in the blanks in the argument below so as to produce valid inferences.

If $\sqrt{2}$ is rational, then $\sqrt{2} = \frac{a}{b}$ for some integers a and b.
It is not true that $\sqrt{2} = \frac{a}{b}$ for some integers a and b.

$\therefore$ _____

Problem 3.2
Use modus ponens or modus tollens to fill in the blanks in the argument below so as to produce valid inferences.

If logic is easy, then I am a monkey's uncle.
I am not a monkey's uncle.
$\therefore$ _____

Problem 3.3
Use a truth table to determine whether the argument below is valid.

$$\begin{array}{r} p \to q \\ q \to p \\ \therefore \quad p \vee q \end{array}$$

Problem 3.4
Use a truth table to determine whether the argument below is valid.

$$\begin{array}{r} p \\ p \to q \\ \sim q \vee r \\ \therefore \quad r \end{array}$$

Problem 3.5
Use symbols to write the logical form of the given argument and then use a truth table to test the argument for validity.

If Tom is not on team A, then Hua is on team B.
If Hua is not on team B, then Tom is on team A.
$\therefore$ Tom is not on team A or Hua is not on team B.

Problem 3.6
Use symbols to write the logical form of the given argument. If the argument is valid, identify the rule of inference that guarantees its validity. Otherwise state whether the converse or the inverse error is made.

If Jules solved this problem correctly, then Jules obtained the answer 2.
Jules obtained the answer 2.
$\therefore$ Jules solved this problem correctly.

Problem 3.7
Use symbols to write the logical form of the given argument. If the argument is valid, identify the rule of inference that guarantees its validity. Otherwise state whether the converse or the inverse error is made.

If this number is larger than 2, then its square is larger than 4.
This number is not larger than 2.
$\therefore$ The square of this number is not larger than 4.

Problem 3.8
Use the valid argument forms of this section to deduce the conclusion from the premises.

$$\begin{aligned} &\sim p \vee q \rightarrow r \\ &s \vee \sim q \\ &\sim t \\ &p \rightarrow t \\ &\sim p \wedge r \rightarrow \sim s \\ \therefore \quad &\sim q \end{aligned}$$

Problem 3.9
Use the valid argument forms of this section to deduce the conclusion from the premises.

$$\begin{aligned} &\sim p \rightarrow r \wedge \sim s \\ &t \rightarrow s \\ &u \rightarrow \sim p \\ &\sim w \\ &u \vee w \\ \therefore \quad &\sim t \vee w \end{aligned}$$

4 Propositions and Quantifiers

Statements such as "$x > 3$" are often found in mathematical assertions and in computer programs. These statements are not propositions when the variables are not specified. However, one can produce propositions from such statements.

A **predicate** is an expression involving one or more variables defined on some domain, called the **domain of discourse**. Substitution of a particular value for the variable(s) produces a proposition which is either true or false. For instance, $P(n) : n$ *is prime* is a predicate on the natural numbers. Observe that $P(1)$ is false, $P(2)$ is true. In the expression $P(x)$, x is called a **free variable**. As x varies the truth value of $P(x)$ varies as well. The set of true values of a predicate $P(x)$ is called the **truth set** and will be denoted by T_P.

Example 4.1
Let $Q(x, y) : x = y+3$ with domain the collection of natural numbers (i.e. the numbers $0, 1, 2, \cdots$). What are the truth values of the propositions $Q(1, 2)$ and $Q(3, 0)$?

Solution.
By substitution in the expression of Q we find: $Q(1, 2)$ is false since $1 = x \neq y + 3 = 5$. On the contrary, $Q(3, 0)$ is true since $x = 3 = 0 + 3 = y + 3$ ■

If $P(x)$ and $Q(x)$ are two predicates with a common domain D then the notation $P(x) \Rightarrow Q(x)$ means that every element in the truth set of $P(x)$ is also an element in the truth set of $Q(x)$.

Example 4.2
Consider the two predicates $P(x) : x$ is a factor of 4 and $Q(x) : x$ is a factor of 8. Show that $P(x) \Rightarrow Q(x)$.

Solution.
Finding the truth set of each predicate we have: $T_P = \{1, 2, 4\}$ and $T_Q = \{1, 2, 4, 8\}$. Since every number appearing in T_P also appears in T_Q we have $P(x) \Rightarrow Q(x)$ ■

If two predicates $P(x)$ and $Q(x)$ with a common domain D are such that $T_P = T_Q$ then we use the notation $P(x) \Leftrightarrow Q(x)$.

Example 4.3
Let $D = \mathbb{R}$. Consider the two predicates $P(x) : -2 \leq x \leq 2$ and $Q(x) : |x| \leq 2$. Show that $P(x) \Leftrightarrow Q(x)$.

Solution.
Indeed, if x in T_P then the distance from x to the origin is at most 2. That is, $|x| \leq 2$ and hence x belongs to T_Q. Now, if x is an element in T_Q then $|x| \leq 2$,i.e. $(x-2)(x+2) \leq 0$. Solving this inequality we find that $-2 \leq x \leq 2$. That is, $x \in T_P$ ■

Another way to generate propositions is by means of **quantifiers.** For example $\forall x \in D, P(x)$ is a proposition which is true if $P(x)$ is true for all values of x in the domain D of P. For example, if k is an nonnegative integer, then the predicate $P(k) : 2k \; is \; even$ is true for all $k \in \mathbb{N}$. We write,

$$\forall k \in \mathbb{N}, (2k \; is \; even).$$

The symbol $\forall$ is called the **universal quantifier.**

The proposition $\forall x \in D, P(x)$ is false if $P(x)$ is false for at least one value of x. In this case x is called a **counterexample**.

Example 4.4
Show that the proposition $\forall x \in \mathbb{R}, x > \frac{1}{x}$ is false.

Solution.
A counterexample is $x = \frac{1}{2}$. Clearly, $\frac{1}{2} < 2 = \frac{1}{\frac{1}{2}}$. ■

Example 4.5
Write in the form $\forall x \in D, P(x)$ the proposition : "every real number is either positive, negative or 0."

Solution.
$\forall x \in \mathbb{R}, x > 0, x < 0, or \; x = 0$. ■

The notation $\exists x \in D, P(x)$ is a proposition that is true if there is at least one value of $x \in D$ where $P(x)$ is true; otherwise it is false. The symbol $\exists$ is called the **existential** quantifier.

Example 4.6
Let $P(x)$ denote the statement "$x > 3$." What is the truth value of the proposition $\exists x \in \mathbb{R}, P(x)$.

Solution.
Since $4 \in \mathbb{R}$ and $4 > 3$, the given proposition is true ■

The proposition $\forall x \in D, P(x) \to Q(x)$ is called the **universal conditional proposition.** For example, the proposition $\forall x \in \mathbb{R}$, if $x > 2$ then $x^2 > 4$ is a universal conditional proposition.

Example 4.7
Rewrite the proposition "if a real number is an integer then it is a rational number" as a universal conditional proposition.

Solution.
$\forall x \in \mathbb{R}$, if x is an integer then x is a rational number ■

Example 4.8
a. What is the negation of the proposition $\forall x \in D, P(x)$?
b. What is the negation of the proposition $\exists x \in D, P(x)$?
c. What is the negation of the proposition $\forall x \in D, P(x) \to Q(x)$?

Solution.
a. $\exists x \in D, \sim P(x)$.
b. $\forall x \in D, \sim P(x)$.
c. Since $P(x) \to Q(x) \equiv (\sim P(x)) \vee Q(x)$, we have $\sim (\forall x \in D, P(x) \to Q(x)) \equiv \exists x \in D, P(x) \wedge \sim Q(x)$ ■

Example 4.9
Consider the universal conditional proposition

$$\forall x \in D,\ if\ P(x)\ then\ Q(x).$$

a. Find the contrapositive.
b. Find the converse.
c. Find the inverse.

Solution.
a. $\forall x \in D,\ if\ \sim Q(x)\ then\ \sim P(x)$.
b. $\forall x \in D,\ if\ Q(x)\ then\ P(x)$.
c. $\forall x \in D,\ if\ \sim P(x)\ then\ \sim Q(x)$ ■

Example 4.10
Write the negation of each of the following propositions:

a. $\forall x \in \mathbb{R}, x > 3 \rightarrow x^2 > 9$.
b. Every polynomial function is continuous.
c. There exists a triangle with the property that the sum of angles is greater than 180°.

Solution.
a. $\exists x \in \mathbb{R}, x > 3\ and\ x^2 \leq 9$.
b. There exists a polynomial that is not continuous everywhere.
c. For any triangle, the sum of the angles is less than or equal to 180° ■

Next, we discuss predicates that contain multiple quantifiers. A typical example is the definition of a limit. We say that $L = \lim_{x \to a} f(x)$ if and only if $\forall \epsilon > 0, \exists$ a positive number δ such that if $|x - a| \leq \delta$ then $|f(x) - L| < \epsilon$.

Example 4.11
a. Let $P(x, y)$ denote the statement "$x + y = y + x$." What is the truth value of the proposition $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R}), P(x, y)$?
b. Let $Q(x, y)$ denote the statement "$x + y = 0$." What is the truth value of the proposition $(\exists y \in \mathbb{R})(\forall x \in \mathbb{R}), Q(x, y)$?

Solution.
a. The given proposition is always true.
b. The proposition is false. For otherwise, one can choose $x \neq -y$ to obtain $0 \neq x + y = 0$ which is impossible ■

Example 4.12
Find the negation of the following propositions:
a. $\forall x \exists y, P(x, y)$.
b. $\exists x \forall y, P(x, y)$.

Solution.
a. $\exists x \forall y, \sim P(x, y)$.
b. $\forall x \exists y, \sim P(x, y)$ ■

Example 4.13
The symbol $\exists!$ stands for the phrase "there exists a unique". Which of the following statements are true and which are false.

a. $\exists! x \in \mathbb{R}, \forall y \in \mathbb{R}, xy = y$.
b. $\exists!$ integer x such that $\frac{1}{x}$ is an integer.

Solution.
a. True. Let $x = 1$.
b. False since 1 and -1 are both integers with integer reciprocals ■

Review Problems

Problem 4.1
By finding a counterexample, show that the proposition: "For all positive integers n and $m, m.n \geq m + n$" is false.

Problem 4.2
Consider the statement

$$\exists x \in \mathbb{R} \; such \; that \; x^2 = 2.$$

Which of the following are equivalent ways of expressing this statement?
a. The square of each real number is 2.
b. Some real numbers have square 2.
c. The number x has square 2, for some real number x.
d. If x is a real number, then $x^2 = 2$.
e. Some real number has square 2.
f. There is at least one real number whose square is 2.

Problem 4.3
Rewrite the following propositions informally in at least two different ways without using the symbols $\exists$ and $\forall$:

a. $\forall$ squares x, x is a rectangle.
b. $\exists$ a set A such that A has 16 subsets.

Problem 4.4
Rewrite each of the following statements in the form "$\exists$___x *such that*___":

a. Some exercises have answers.
b. Some real numbers are rational.

Problem 4.5
Rewrite each of the following statements in the form "$\forall$___, if___$then$___.":

a. All COBOL programs have at least 20 lines.
b. Any valid argument with true premises has a true conclusion.
c. The sum of any two even integers is even.
d. The product of any two odd integers is odd.

Problem 4.6
Which of the following is a negation for "Every polynomial function is continuous"?

a. No polynomial function is continuous.
b. Some polynomial functions are continuous.
c. Every polynomial function fails to be continuous.
d. There is a noncontinuous polynomial function.

Problem 4.7
Determine whether the proposed negation is correct. If it is not, write a correct negation.

Proposition : For all integers n, if n^2 is even then n is even.
Proposed negation : For all integers n, if n^2 is even then n is not even.

Problem 4.8
Let $D = \{-48, -14, -8, 0, 1, 3, 16, 23, 26, 32, 36\}$. Determine which of the following propositions are true and which are false. Provide counterexamples for those propositions that are false.

a. $\forall x \in D$, if x is odd then $x > 0$.
b. $\forall x \in D$, if x is less than 0 then x is even.
c. $\forall x \in D$, if x is even then $x \leq 0$.
d. $\forall x \in D$, if the ones digit of x is 2, then the tens digit is 3 or 4.
e. $\forall x \in D$, if the ones digit of x is 6, then the tens digit is 1 or 2

Problem 4.9
Write the negation of the proposition :$\forall x \in \mathbb{R}$, if $x(x+1) > 0$ then $x > 0$ or $x < -1$.

Problem 4.10
Write the negation of the proposition : If an integer is divisible by 2, then it is even.

Problem 4.11
Given the following true propostion: "$\forall$ real numbers x, $\exists$ an integer n such that $n > x$." For each x given below, find an n to make the predicate $n > x$ true.
a. $x = 15.83$ b. $x = 10^8$ c. $x = 10^{10^{10}}$.

Problem 4.12
Given the proposition: $\forall x \in \mathbb{R}, \exists$ a real number y such that $x + y = 0$.
a. Rewrite this proposition in English without the use of the quantifiers.
b. Find the negation of the given proposition.

Problem 4.13
Given the proposition: $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}$, $x + y = 0$.
a. Rewrite this proposition in English without the use of the quantifiers.
b. Find the negation of the given proposition.

Problem 4.14
Consider the proposition "Somebody is older than everybody." Rewrite this proposition in the form "$\exists$ a person x such that $\forall$ _____."

Problem 4.15
Given the proposition: "There exists a program that gives the correct answer to every question that is posed to it."
a. Rewrite this proposition using quantifiers and variables.
b. Find a negation for the given proposition.

Problem 4.16
Given the proposition: $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $x < y$.
a. Write a proposition by interchanging the symbols $\forall$ and $\exists$.
b. State which is true: the given proposition, the one in part (a), neither, or both.

Problem 4.17
Find the contrapositive, converse, and inverse of the proposition "$\forall x \in \mathbb{R}$, if $x(x + 1) > 0$ then $x > 0$ or $x < -1$."

Problem 4.18
Rewrite the following proposition in if-then form : "Earning a grade of C^- in this course is a sufficient condition for it to count toward graduation."

Problem 4.19
Rewrite the following proposition in if-then form : "Being on time each day is a necessary condition for keeping this job."

Problem 4.20
Rewrite the following proposition without using the words "necessary" or "sufficient" : "Divisibility by 4 is not a necessary condition for divisibility by 2."

5 Arguments with Quantified Premises

In this section we discuss three types of valid arguments that involve the universal quantifier.

• The rule of **universal instantiation**:

$$\begin{array}{rr} & \forall x \in D, P(x) \\ & a \in D \\ \therefore & P(a) \end{array}$$

Example 5.1
Use universal instantiation to fill in valid conclusion for the following argument.

All positive integers are greater than or equal to 1
3 is a positive integer
$\therefore$ _____

Solution.
All positive integers are greater than or equal to 1
3 is a positive integer
$\therefore$ $3 \geq 1$ ■

• **Universal Modus Ponen**:

$$\begin{array}{rr} & \forall x \in D,\ if\ P(x)\ then\ Q(x) \\ & P(a)\ for\ some\ a \in D \\ \therefore & Q(a) \end{array}$$

Example 5.2
Use the rule of the universal modus ponens to fill in valid conclusion for the following argument.

$\forall n \in \mathbb{N}$, if $n = 2k$ for some $k \in \mathbb{N}$ then n is even.
$0 = 2.0$
$\therefore$ _____

Solution.
$\forall n \in \mathbb{N}$, if $n = 2k$ for some $k \in \mathbb{N}$ then n is even.

$0 = 2.0$
$\therefore 0$ is even ■

• **Universal Modus Tollens**:

$$\begin{aligned} &\forall x \in D,\ if\ P(x)\ then\ Q(x) \\ &\sim Q(a)\ for\ some\ a \in D \\ \therefore\ &\sim P(a) \end{aligned}$$

Example 5.3
Use the rule of the universal modus tonens to fill in valid conclusion for the following argument.

All healthy people eat an apple a day.
Harry does not eat an apple a day.
$\therefore$ _____

Solution.
All healthy people eat an apple a day.
Harry does not eat an apple a day.
$\therefore$ Harry is not healthy ■

Next, we discuss a couple of invalid arguments whose premises involve quantifiers.

• **The rule of converse error**:

$$\begin{aligned} &\forall x \in D,\ if\ P(x)\ then\ Q(x) \\ &Q(a)\ for\ some\ a \in D \\ \therefore\ &P(a) \end{aligned}$$

Example 5.4
What kind of error does the following invalid argument exhibit?

All healthy people eat an apple a day.
Helen eats an apple a day.
$\therefore$ Helen is healthy

Solution.
This invalid argument exhibits the converse error ■

• **The rule of inverse error**:

$$\begin{aligned} & \forall x \in D,\ if\ P(x)\ then\ Q(x) \\ & \sim P(a)\ for\ some\ a \in D \\ \therefore\ & \sim Q(a) \end{aligned}$$

Example 5.5
What kind of error does the following invalid argument exhibit?

All healthy people eat an apple a day.
Hubert is not a healthy person.
$\therefore$ Hubert does not eat an apple a day.

Solution.
This invalid argument exhibits the inverse error ■

Review Problems

Problem 5.1
Use the rule of universal modus ponens to fill in valid conclusion for the argument.

For all real numbers a, b, c, and d, if $b \neq 0$ and $d \neq 0$ then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
$a = 2, b = 3, c = 4$, and $d = 5$ are particular real numbers such that $b \neq 0$ and $d \neq 0$.
$\therefore$ _____

Problem 5.2
Use the rule of universal modus tollens to fill in valid conclusion for the argument.

If a computer is correct, then compilation of the program does not produce error messages.
Compilation of this program produces error messages.
$\therefore$ _____

Problem 5.3
Use the rule of universal modus ponens to fill in valid conclusion for the argument.

All freshmen must take writing.
Caroline is a freshman.
$\therefore$ _____.

Problem 5.4
What kind of error does the following invalid argument exhibit?
All cheaters sit in the back row.
George sits in the back row.
$\therefore$ George is a cheater.

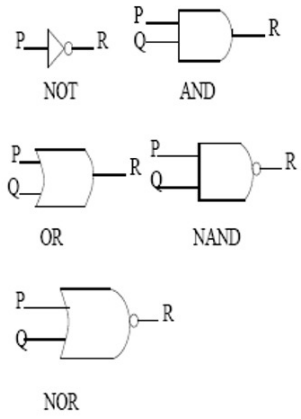
Problem 5.5
What kind of error does the following invalid argument exhibit?
All honest people pay their taxes.
Darth is not honest.
$\therefore$ Darth does not pay his taxes.

6 Project I: Digital Logic Design

In this section we discuss the logic of digital circuits which are considered to be the basic components of most digital systems, such as electronic computers, electronic phones, traffic light controls, etc.
The purpose of digital systems is to manipulate discrete information which are represented by physical quantities such as voltages and current. The smallest representation unit is one **bit**, short for binary digit. Since electronic switches have two physical states, namely high voltage and low voltage we attribute the bit 1 to high voltage and the bit 0 for low voltage.
A **logic gate** is the smallest processing unit in a digital system. It takes one or few bits as input and generates one bit as an output.
A **circuit** is composed of a number of logic gates connected by wires. It takes a group of bits as input and generates one or more bits as output.
The five basic logic gates are the following:

(1) NOT gate (also called **inverter**): Takes an input of 0 to an output of 1 and an input of 1 to an output of 0. The corresponding logical symbol is $\sim P$.
(2) AND gate: Takes two bits, P and Q, and outputs 1 if P and Q are 1 and 0 otherwise. The logical symbol is $P \wedge Q$.
(3) OR gate: outputs 1 if either P or Q is 1 and 0 otherwise. The logical symbol is $P \vee Q$.
(4) NAND gate: outputs a 0 if both P and Q are 1 and 1 otherwise. The symbol is $\sim (P \wedge Q)$. Also, denoted by $P|Q$, where $|$ is called a **Scheffer stroke.**
(5) NOR gate: output a 0 if at least one of P or Q is 1 and 1 otherwise. The symbol is $\sim (P \vee Q)$ or $P \downarrow Q$, where $\downarrow$ is a **Pierce arrow.**

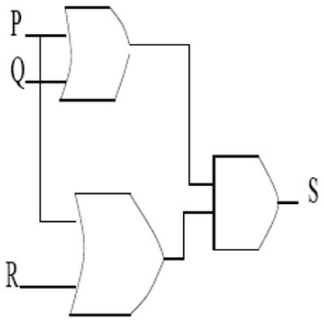
The logic gates have the following graphical representations:



Problem 6.1
Construct the truth tables of the gates discussed in this section.

If you are given a set of input signals for a circuit, you can find its output by tracing through the circuit gate by gate.

Problem 6.2
Give the output signal S for the following circuit, given that $P = 0, Q = 1$, and $R = 0$:



Problem 6.3
Write the input/output table for the circuit of the previous problem.

A variable with exactly two possible values is called a **Boolean variable.** A **Boolean expression** is an expression composed of Boolean variables and connectives (which are the gates in this section).

Problem 6.4
Find the Boolean expression that corresponds to the circuit of Problem 6.2.

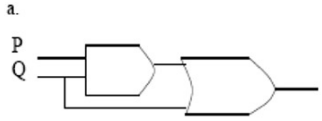
Problem 6.5
Construct the circuit corresponding to the Boolean expression: $(P \wedge Q) \vee \sim R$.

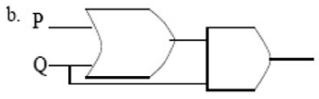
Problem 6.6
For the following input/output table, construct (a) the corresponding Boolean expression and (b) the corresponding circuit:

P	Q	R	S
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

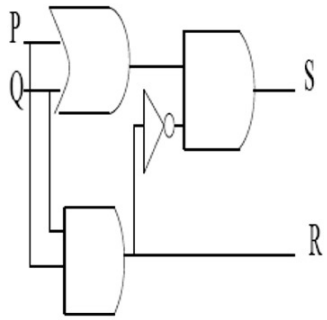
Two digital logic circuits are **equivalent** if, and only if, their corresponding Boolean expressions are logically equivalent.

Problem 6.7
Show that the following two circuits are equivalent:





Problem 6.8
Consider the following circuit



Let P and Q be single binary digits and $P + Q = RS$. Complete the following table

P	Q	R	S
1	1		
1	0		
0	1		
0	0		

The given circuit is called a **half-adder**. It computes the sum of two single binary digits.

Several methods have been used for expressing negative numbers in the computer. The most obvious way is to convert the number to binary and stick on another bit to indicate sign, 0 for positive and 1 for negative. Suppose that integers are stored using this signed-magnitude technique in 8 bits so that the leftmost bit holds the sign while the remaining bits represent the magnitude. Thus, $+41_{10} = 00101001$ and $-41_{10} = 10101001$.
The above procedure has a gap. How one would represent the bit 0? Well, there are two ways for storing 0. One way is 00000000 which represents $+0$ and a second way 10000000 represents -0. A method for representing numbers that avoid this problem is called the **two's complement.** Considering -41_{10} again, first, convert the absolute value to binary obtaining $41_{10} = 00101001$. Then take the complement of each bit obtaining 11010110. This is called the **one complement** of 41. To complete the procedure, increment by 1 the one's complement to obtain $-41_{10} = 11010111$.
Conversion of $+41_{10}$ to two's complement consists merely of expressing the number in binary, i.e. $+41_{10} = 00101001$.

Problem 6.9
Express the numbers 104 and -104 in two's complement representation with 8 bits.

Now, an algorithm to find the decimal representation of the integer with a given 8-bit two's complement is the following:
1. Find the two's complement of the given two's complement,
2. write the decimal equivalent of the result.

Problem 6.10
What is the decimal representation for the integer with two's complement 10101001?

7 Project II: Number Systems

In this section we consider three number systems that are of importance in applications, namely, the decimal system, the binary system, and the hexadecimal system. Decimal numbers are used in communication among human beings whereas binary numbers are used by computers to represent numbers.

Consider first the **decimal system.** If n is a positive integer then n can be written as

$$n = d_k d_{k-1} \cdots d_1 d_0,$$

where the digits $d_0, d_1, \cdots, d_k$ are elements of the set $\{0, 1, 2, \cdots, 9\}$.

The number n can be expressed as a sum of powers of 10 as follows:

$$n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_1 10^1 + d_0 10^0.$$

For example,

$$5049 = 5(10^3) + 0(10^2) + 4(10^1) + 9(10^0).$$

A number in **binary system** is a number n that can be written in the form

$$n = b_k b_{k-1} \cdots b_1 b_0,$$

where b_i is either 0 or 1.

We will use subscripts to tell the base in which a number is represented. Thus, we write $n_2 = b_k b_{k-1} \cdots b_1 b_0$ to indicate that the number n is in base 2.
If n is a number in base 2 then its decimal value (i.e. base 10) is found by the formula:

$$n_2 = b_k(2^k) + b_{k-1}(2^{k-1}) + \cdots + b_1(2^1) + b_0(2^0) = m_{10}.$$

Problem 7.1
Find the decimal value of the following binary numbers:
a. 1100101_2
b. 110110_2

To convert a positive integer n from base 10 to base 2 we use the division algorithm as follows:
(1) $n = q_0(2) + r_0$, where q_0 is the quotient of the division of n by 2 and r_0 is the remainder.
(2) If $q_0 = 0$ then n is already in base 2. If not then divide q_0 by 2 to obtain $q_0 = q_1(2) + r_1$.
(3) If $q_1 = 0$ then $n_{10} = r_1 r_0$. If not repeat the process. Note that the remainders are all less than 2.
Suppose that $q_k = 0$ then

$$n_{10} = r_k r_{k-1} \cdots r_1 r_0.$$

Problem 7.2
Represent the following decimal integers in binary notation:
a. 1297_{10}
b. 458_{10}

Problem 7.3
Evaluate the following sums:
a. $11011101_2 + 1001011010_2$
b. $101101_2 + 11101_2$

Another useful number system is the **hexadecimal system**. The possible digits in an hexadecimal system are :

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$$

where A, B, C, D, E, F stand for $10, 11, 12, 13, 14$, and 15 respectively.
The conversion of a number from base 16 to base 10 is similar to the conversion of numbers from base 2 to base 10. The conversion of a number from base 10 to base 16 is similar to the conversion of a decimal number to base 2.

Problem 7.4
Convert the number $A2BC_{16}$ to base 10.

To convert an integer from base 16 to base 2 one performs the following:
(1) Write each hexadecimal digit of the integer in fixed 4-bit binary notation.
(2) Juxtapose the results.

Problem 7.5
Convert the number $B53DF8_{16}$ to base 2.

To convert an integer from base 2 to base 16:
(1) Group the digits of the binary number into sets of four bits, starting from the right and adding leading zeros as needed.
(2) Convert the binary numbers in (1) to base 16.
(3) Juxtapose the results of (2)

Problem 7.6
Convert the number 101101111000101_2 to base 16.

Fundamentals of Mathematical Proofs

In this chapter we discuss some common methods of proof and the standard terminology that accompanies them.

8 Methods of Direct Proof I

A **mathematical system** consists of axioms, definitions, and undefined terms. An **axiom** is a statement that is assumed to be true. A **definition** is used to create new concepts in terms of existing ones. A **theorem** is a proposition that has been proved to be true. A **lemma** is a theorem that is usually not interesting in its own right but is useful in proving another theorem. A **corollary** is a theorem that follows quickly from a theorem.

Example 8.1
The Euclidean geometry furnishes an example of mathematical system:
• points and lines are examples of undefined terms.
• An example of a definition: Two angles are supplementary if the sum of their measures is 180°.
• An example of an axiom: Given two distinct points, there is exactly one line that contains them.
• An example of a theorem: If two sides of a triangle are equal, then the angles opposite them are equal.
• An example of a corollary: If a triangle is equilateral, then it is equiangular.

An argument that establishes the truth of a theorem is called a **proof**. **Logic** is a tool for the analysis of proofs.

First we discuss methods for proving a theorem of the form "$\exists x$ such that $P(x)$." This theorem guarantees the existence of at least one x for which the predicate $P(x)$ is true. The proof of such a theorem is **constructive**: that is, the proof is either by finding a particular x that makes $P(x)$ true or by exhibiting an algorithm for finding x.

Example 8.2
Show that there exists a positive integer whose square can be written as the sum of the squares of two positive integers.

Solution.
Indeed, one example is $5^2 = 3^2 + 4^2$ ■

Example 8.3
Show that there exists an integer x such that $x^2 = 15,129$.

Solution.
Applying the well-known algorithm of extracting the square root we find that $x = 123$ ■

By a **nonconstructive existence proof** we mean a method that involves either showing the existence of x using a proved theorem (or axioms) or the assumption that there is no such x leads to a contradiction. The disadvantage of nonconstructive method is that it may give virtually no clue about where or how to find x.

Theorems are often of the form "$\forall x \in D$ if $P(x)$ then $Q(x)$." We call $P(x)$ the **hypothesis** and $Q(x)$ the **conclusion**.

Let us first consider a proposition of the form $\forall x \in D, P(x)$. Then this can be written in the form "$\forall x$, if $x \in D$ then $P(x)$." If D is a finite set, then one checks the truth value of $P(x)$ for each $x \in D$. This method is called the **method of exhaustion.**

Example 8.4
Show that for each integer $1 \leq n \leq 10$, $n^2 - n + 11$ is a prime number.

Solution.
The given proposition can be written in the form "$\forall n \in \mathbb{N}$, if $1 \leq n \leq 10$ then

$P(n)$ is prime" where $P(n) = n^2 - n + 11$. Using the method of exhaustion we see that

$$\begin{array}{llll} P(1) = 11 & ; \quad P(2) = 13 & ; \quad P(3) = 17 & ; \quad P(4) = 23 \\ P(5) = 31 & ; \quad P(6) = 41 & ; \quad P(7) = 53 & ; \quad P(8) = 67 \\ P(9) = 83 & ; \quad P(10) = 101. & & \end{array}$$ ■

The most powerful technique for proving a universal proposition is one that works regardless of the size of the domain over which the proposition is quantified. It is called the **method of generalizing from the generic particular.**
The method consists of picking an arbitrary element x of the domain (known as a **generic element**) for which the hypothesis $P(x)$ is satisfied, and then using definitions, previously established results, and the rules of inference to conclude that $Q(x)$ is also true.
By a **direct method of proof** we mean a method that consists of showing that if $P(x)$ is true for $x \in D$ then $Q(x)$ is also true.

The following shows the format of the proof of a theorem.

Theorem 8.1
For all $n, m \in \mathbb{Z}$, if m and n are even then so is $m + n$.

Proof.
Let m and n be two even integers. Then there exist integers k_1 and k_2 such that $n = 2k_1$ and $m = 2k_2$. We must show that $m + n$ is even, that is, an integer multiple of 2. Indeed,

$$\begin{aligned} m + n &= 2k_1 + 2k_2 \\ &= 2(k_1 + k_2) \\ &= 2k \end{aligned}$$

where $k = k_1 + k_2 \in \mathbb{Z}$. Thus, by the definition of even, $m + n$ is even ■

Example 8.5
Prove the following theorem.

Theorem Every integer is a rational number.

Solution.
Proof. Let n be an arbitrary integer. Then $n = \frac{n}{1}$. By the definition of rational numbers, n is rational ■

Theorem 8.2
If $a, b \in \mathbb{Q}$ then $a + b \in \mathbb{Q}$.

Proof.
Let a and b be two rational numbers. Then there exist integers $a_1, a_2, b_1 \neq 0$, and $b_2 \neq 0$ such that $a = \frac{a_1}{b_1}$ and $b = \frac{a_2}{b_2}$. By the property of addition of two fractions we have

$$\begin{aligned} a + b &= \frac{a_1}{b_1} + \frac{a_2}{b_2} \\ &= \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \end{aligned}$$

By letting $p = a_1 b_2 + a_2 b_1 \in \mathbb{Z}$ and $q = b_1 b_2 \in \mathbb{Z}^*$ we get $a + b = \frac{p}{q}$. That is, $a + b \in \mathbb{Q}$ ■

Corollary 8.1
The double of a rational number is rational.

Proof.
Let $a = b$ in the previous theorem we see that $2a = a + a = a + b \in \mathbb{Q}$ ■

Next, we point out of some common mistakes that must be avoided in proving theorems.

• Arguing from examples. The validity of a general statement can not be proved by just using a particular example.

• Using the same letters to mean two different things. For example, suppose that m and n are any two given even integers. Then by writing $m = 2k$ and $n = 2k$ this would imply that $m = n$ which is inconsistent with the statement that m and n are arbitrary.

• Jumping to a conclusion. Let us illustrate by an example. Suppose that we want to show that if the sum of two integers is even so is their difference. Consider the following proof: Suppose that $m + n$ is even. Then there is an integer k such that $m + n = 2k$. Then, $m = 2k - n$ and so $m - n$ is even.
The problem with this proof is that the crucial step $m - n = 2k - n - n =$

$2(k-n)$ is missing. The author of the proof has jumped prematurely to a conclusion.

• Begging the question. By that we mean that the author of a proof uses in his argument a fact that he is supposed to prove.

Finally, to show that a proposition of the form $\forall x \in D$, if $P(x)$ then $Q(x)$ is false it suffices to find an element $x \in D$ where $P(x)$ is true but $Q(x)$ is false. Such an x is called a **counterexample.**

Example 8.6
Disprove the proposition $\forall a, b \in \mathbb{R}$, if $a < b$ then $a^2 < b^2$.

Solution.
A counterexample is the following. Let $a = -2$ and $b = -1$. Then $a < b$ but $a^2 > b^2$ ■

Review Problems

A real number r is called **rational** if there exist two integers a and $b \neq 0$ such that $r = \frac{a}{b}$. A real number that is not rational is called **irrational.**

Problem 8.1
Show that the number $r = 6.321521521...$ is a rational number.

Problem 8.2
Prove the following theorem.

Theorem. The product of two rational numbers is a rational number.

Problem 8.3
Use the previous exercise to prove the following.

Corollary. The square of any rational number is rational.

Problem 8.4
Use the method of constructive proof to show that if r and s are two real numbers with $r < s$ then there exists a real number x such that $r < x < s$.

Problem 8.5
The following Pascal program segment does not find the minimum value in a data set of N integers. Find a counterexample.

```
MINN := 0;
FOR I := 1 TO N DO
    BEGIN
       READLN (A);
       If A < MINN THEN MINN := A
    END
```

9 More Methods of Proof

A **vacuous proof** is a proof of an implication $p \to q$ in which it is shown that p is false.

Example 9.1
Use the method of vacuous proof to show that if $x \in \emptyset$ then David is playing pool.

Solution.
Since the proposition $x \in \emptyset$ is always false, the given proposition is vacuously true ■

A **trivial proof** of an implication $p \to q$ is one in which q is shown to be true without any reference to p.

Example 9.2
Use the method of trivial proof to show that if n is an even integer then n is divisible by 1.

Solution.
Since the proposition n is divisible by 1 is always true, the given implication is trivially true ■

The method of **proof by cases** is a direct method of proving the conditional proposition $p_1 \vee p_2 \vee \cdots \vee p_n \to q$. The method consists of proving the conditional propositions $p_1 \to q, p_2 \to q, \cdots, p_n \to q$.

Example 9.3
Show that if n is a positive integer then $n^3 + n$ is even.

Solution.
We use the method of proof by cases.

Case 1. Suppose that n is even. Then there is $k \in \mathbb{N}$ such that $n = 2k$. In this case, $n^3 + n = 8k^3 + 2k = 2(4k^3 + k)$ which is even.

Case 2. Suppose that n is odd. Then there is a $k \in \mathbb{N}$ such that $n = 2k + 1$. So, $n^3 + n = 2(4k^3 + 6k^2 + 4k + 1)$ which is even ■

Example 9.4
Use the proof by cases to prove the triangle inequality: $|x+y| \leq |x| + |y|$.

Solution.
Case 1. $x \geq 0$ and $y \geq 0$. Then $x + y \geq 0$ and so $|x+y| = x + y = |x| + |y|$.
Case 2. $x \geq 0$ and $y < 0$. Then $x + y < x + 0 < |x| \leq |x| + |y|$. On the other hand, $-(x+y) = -x + (-y) \leq 0 + (-y) = |y| \leq |x| + |y|$. Thus, if $|x+y| = x + y$ then $|x+y| < |x| + |y|$ and if $|x+y| = -(x+y)$ then $|x+y| \leq |x| + |y|$.
Case 3. The case $x < 0$ and $y \geq 0$ is similar to case 2.
Case 4. Suppose $x < 0$ and $y < 0$. Then $x + y < 0$ and therefore $|x+y| = -(x+y) = (-x) + (-y) = |x| + |y|$.
So in all four cases $|x+y| \leq |x| + |y|$. ■

Now, given a real number x, the largest integer n such that $n \leq x < n+1$ is called the **floor of** x and is denoted by $\lfloor x \rfloor$. The smallest integer n such that $n - 1 < x \leq n$ is called the **ceiling of** x and is denoted by $\lceil x \rceil$.

Example 9.5
Compute $\lfloor x \rfloor$ and $\lceil x \rceil$ of the following values of x :
a. 37.999 b. $-\frac{57}{2}$ c. -14.001

Solution.
a. $\lfloor 37.999 \rfloor = 37, \lceil 37.999 \rceil = 38$.
b. $\lfloor -\frac{57}{2} \rfloor = -29, \lceil -\frac{57}{2} \rceil = -28$.
c. $\lfloor -14.001 \rfloor = -15, \lceil -14.001 \rceil = -14$.■

Example 9.6
Use the proof by a counterexample to show that the proposition "$\forall x, y \in \mathbb{R}, \lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$" is false.

Solution.
Let $x = y = 0.5$. Then $\lfloor x + y \rfloor = 1$ and $\lfloor x \rfloor + \lfloor y \rfloor = 0$ ■

The following gives another example of the method of proof by cases.

Theorem 9.1
For any integer n,

$$\lfloor \frac{n}{2} \rfloor = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even} \\ \frac{n-1}{2}, & \text{if } n \text{ is odd} \end{cases}$$

Proof.
Let n be any integer. Then we consider the following two cases.

Case 1. n is odd. In this case, there is an integer k such that $n = 2k + 1$. Hence,

$$\lfloor \frac{n}{2} \rfloor = \lfloor \frac{2k+1}{2} \rfloor = \lfloor k + \frac{1}{2} \rfloor = k$$

since $k \leq k + \frac{1}{2} < k + 1$. Since $n = 2k + 1$, solving this equation for k we find $k = \frac{n-1}{2}$. It follows that

$$\lfloor \frac{n}{2} \rfloor = k = \frac{n-1}{2}.$$

Case 2. Suppose n is even. Then there is an integer k such that $n = 2k$. Hence, $\lfloor \frac{n}{2} \rfloor = \lfloor k \rfloor = k = \frac{n}{2}$. ■

Review Problems

Problem 9.1
Prove that for any integer n the product $n(n+1)$ is even.

Problem 9.2
Prove that the square of any integer has the form $4k$ or $4k+1$ for some integer k

Problem 9.3
Prove that for any integer n, $n(n^2-1)(n+2)$ is divisible by 4.

Theorem 9.2
Given any nonnegative integer n and a positive integer d there exist integers q and r such that $n = dq + r$ and $0 \leq r < d$. The number q is called the **quotient** of the division of n by d and we write $q = n\ div\ d$. The number r is called the **remainder** and we write $r = n\ mod\ d$ or $n \equiv r(mod\ d)$.

Proof.
The proof uses the fact that any nonempty subset of $\mathbb{N}$ has a smallest element. So let $S = \{n - d \cdot k \in \mathbb{N} : k \in \mathbb{Z}\}$. This set is nonempty. Indeed, if $n \in \mathbb{N}$ then $n = n - 0 \cdot d \geq 0$ and if $n < 0$ then $n - d \cdot n = n \cdot (1-d) \geq 0$. Thus, S is a nonempty subset of $\mathbb{N}$ so it has a smallest element, called r. That is, there is an integer q such that $n - d \cdot q = r$ or $n = d \cdot q + r$. It remains to show that $r < d$. Suppose the contrary, i.e. $r \geq d$. Then $n - d \cdot (q+1) = r - d \geq 0$ so that $n - d \cdot (q+1) \in S$. Hence, $r \leq n - d \cdot (q+1) = r - d$, a contradiction. Hence, $r < d$ ■

The following theorem shows a way for finding q and r.

Theorem 9.3
If n is a nonnegative integer and d is a positive integer by letting $q = \lfloor \frac{n}{d} \rfloor$ and $r = n - d\lfloor \frac{n}{d} \rfloor$, we have

$$n = dq + r, \quad and \quad 0 \leq r < d.$$

Proof.
Suppose n is a nonnegative integer, d is a positive integer,$q = \lfloor \frac{n}{d} \rfloor$ and $r = n - d\lfloor \frac{n}{d} \rfloor$. By substitution we have

$$dq + r = d\lfloor \frac{n}{d} \rfloor + n - d\lfloor \frac{n}{d} \rfloor = n.$$

It remains to show that $0 \leq r < d$. By the definition of the floor function we have

$$q \leq \frac{n}{d} < q + 1.$$

Multiplying through by d we find

$$dq \leq n < dq + d.$$

This implies that

$$0 \leq n - dq < d.$$

But

$$r = n - d\lfloor \frac{n}{d} \rfloor = n - dq.$$

Hence, $0 \leq r < d$. This completes a proof of the theorem ■

Problem 9.4
State a necessary and sufficient condition for the floor function of a real number to equal that number

Problem 9.5
Prove that if n is an even integer then $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$.

Problem 9.6
Show that the equality $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$ is not valid for all real numbers x and y.

Problem 9.7
Show that the equality $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$ is not valid for all real numbers x and y.

Problem 9.8
Prove that for all real numbers x and all integers m, $\lceil x + m \rceil = \lceil x \rceil + m$.

Problem 9.9
Show that if n is an odd integer then $\lceil \frac{n}{2} \rceil = \frac{n+1}{2}$.

10 Methods of Indirect Proofs: Contradiction and Contraposition

Recall that in a direct proof one starts with the hypothesis of an implication $p \to q$ and then proves that the conclusion is true. Any other method of proof will be referred to as an indirect proof. In this section we study two methods of indirect proofs, namely, the proof by contradiction and the proof by contrapositive.

• **Proof by contradiction**: We want to show that p is true. We assume it is not and therefore $\sim p$ is true and then derive a contradiction. By the rule of contradiction discussed in Chapter 1, p must be true.

Theorem 10.1
If n^2 is an even integer so is n.

Proof.
Suppose the contrary. That is suppose that n is odd. Then there is an integer k such that $n = 2k + 1$. In this case, $n^2 = 2(2k^2 + 2k) + 1$ is odd and this contradicts the assumption that n^2 is even. Hence, n must be even ■

Theorem 10.2
The number $\sqrt{2}$ is irrational.

Proof.
Suppose not. That is, suppose that $\sqrt{2}$ is rational. Then there exist two integers m and n with no common divisors such that $\sqrt{2} = \frac{m}{n}$. Squaring both sides of this equality we find that $2n^2 = m^2$. Thus, m^2 is even. By Theorem 10.1, m is even. That is, 2 divides m. But then $m = 2k$ for some integer k. Taking the square we find that $2n^2 = m^2 = 4k^2$, that is $n^2 = 2k^2$. This says that n^2 is even and by Theorem 10.1, n is even. We conclude that 2 divides both m and n and this contradicts our assumption that m and n have no common divisors. Hence, $\sqrt{2}$ must be irrational ■

Theorem 10.3
The set of prime numbers is infinite.

Proof.
Suppose not. That is, suppose that the set of prime numbers is finite. Then these prime numbers can be listed, say, $p_1, p_2, \cdots, p_n$. Now, consider the integer $N = p_1 p_2 \cdots p_n + 1$. By the Unique Factorization Theorem, (See Problem 12.5) N can be factored into primes. Thus, there is a prime number p_i such that $p_i | N$. But since $p_i | p_1 p_2 \cdots p_n$ we have $p_i | (N - p_1 p_2 \cdots p_n) = 1$, a contradiction since $p_i > 1$ ■

• **Proof by contrapositive**: We already know that $p \to q \equiv \sim q \to \sim p$. So to prove $p \to q$ we sometimes instead prove $\sim q \to \sim p$.

Theorem 10.4
If n is an integer such that n^2 is odd then n is also odd.

Proof.
Suppose that n is an integer that is even. Then there exists an integer k such that $n = 2k$. But then $n^2 = 2(2k^2)$ which is even ■

Review Problems

Problem 10.1
Use the proof by contradiction to prove the proposition "There is no greatest even integer."

Problem 10.2
Prove by contradiction that the difference of any rational number and any irrational number is irrational.

Problem 10.3
Use the proof by contraposition to show that if a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Problem 10.4
Use the proof by contradiction to show that the product of any nonzero rational number and any irrational number is irrational.

11 Method of Proof by Induction

With the emphasis on structured programming has come the development of an area called **program verification,** which means your program is correct as you are writing it.
One technique essential to program verification is **mathematical induction**, a method of proof that has been useful in every area of mathematics as well.
Consider an arbitrary loop in Pascal starting with the statement

$$FOR\ I\ := 1\ TO\ N\ DO$$

If you want to verify that the loop does something regardless of the particular integral value of N, you need mathematical induction.
Also, sums of the form

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

are very useful in analysis of algorithms and a proof of this formula is mathematical induction.
Next we examine this method. We want to prove that a predicate $P(n)$ is true for any nonnegative integer $n \geq n_0$. The steps of mathematical induction are as follows:

(i) (Basis of induction) Show that $P(n_0)$ is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true.
(iii) (Induction step) Show that $P(n+1)$ is true.

Example 11.1
Use the technique of mathematical induction to show that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad n \geq 1.$$

Solution.
Let $P(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$. Then
(i) (Basis of induction) $P(1) : 1 = \frac{1(1+1)}{2}$. That is, $P(1)$is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $P(n) : 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

(iii) (Induction step) We must show that $P(n+1): 1+2+3+\cdots+n+1 = \frac{(n+1)(n+2)}{2}$. Indeed,

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

Example 11.2 *(Geometric progression)*
a. Use induction to show $P(n): \sum_{k=0}^{n} ar^k = \frac{a(1-r^{n+1})}{1-r},\ n \geq 0$ where $r \neq 1$.
b. Show that $1 + \frac{1}{2} + \cdots + \frac{1}{2^{n-1}} \leq 2$, for all $n \geq 1$.

Solution.
a. We use the method of proof by mathematical induction.

(i) (Basis of induction) $a = a\frac{1-r^{0+1}}{1-r} = \sum_{k=0}^{0} ar^k$. That is, $P(0)$is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $\sum_{k=0}^{n} ar^k = \frac{a(1-r^{n+1})}{1-r}$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $\sum_{k=0}^{n+1} ar^k = \frac{a(1-r^{n+2})}{1-r}$. Indeed,

$$\begin{aligned}\sum_{k=0}^{n+1} ar^k =& \sum_{k=0}^{n} ar^k + ar^{n+1} \\ =& a\frac{1-r^{n+1}}{1-r} + ar^{n+1}\frac{1-r}{1-r} \\ =& a\frac{1-r^{n+1}+r^{n+1}-r^{n+2}}{1-r} \\ =& a\frac{1-r^{n+2}}{1-r}.\end{aligned}$$

b. By a. we have

$$\begin{aligned}1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{n-1}} =& \frac{1-(\frac{1}{2})^n}{1-\frac{1}{2}} \\ =& 2(1-(\frac{1}{2})^n) \\ =& 2 - \frac{1}{2^{n-1}} \\ \leq& 2 \blacksquare\end{aligned}$$

Example 11.3 *(Arithmetic progression)*
Use induction to show that $P(n) : \sum_{k=1}^{n}(a+(k-1)r) = \frac{n}{2}[2a+(n-1)r],\ n \geq 1$.

Solution.
We use the method of proof by mathematical induction.

(i) (Basis of induction) $a = \frac{1}{2}[2a + (1-1)r] = \sum_{k=1}^{1}(a + (k-1)r)$. That is, $P(1)$is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $\sum_{k=1}^{n}(a+(k-1)r) = \frac{n}{2}[2a + (n-1)r]$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $\sum_{k=1}^{n+1}(a + (k-1)r) = \frac{(n+1)}{2}[2a + nr]$. Indeed,

$$\begin{aligned}
\sum_{k=1}^{n+1}(a + (k-1)r) &= \sum_{k=1}^{n}(a + (k-1)r) + a + (n+1-1)r \\
&= \frac{n}{2}[2a + (n-1)r] + a + nr \\
&= \frac{2an + n^2r - nr + 2a + 2nr}{2} \\
&= \frac{2a(n+1) + n(n+1)r}{2} \\
&= \frac{n+1}{2}[2a + nr] \ \blacksquare
\end{aligned}$$

We next exhibit a theorem whose proof uses mathematical induction.

Theorem 11.1
For all integers $n \geq 1$, $2^{2n} - 1$ is divisible by 3.

Proof.
Let $P(n) : 2^{2n} - 1$ is divisible by 3. Then
(i) (Basis of induction) $P(1)$ is true since 3 is divisible by 3.
(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $2^{2n} - 1$ is divisible by 3.
(iii) (Induction step) We must show that $2^{2n+2} - 1$ is divisible by 3. Indeed,

$$\begin{aligned} 2^{2n+2} - 1 =& 2^{2n}(4) - 1 \\ =& 2^{2n}(3+1) - 1 \\ =& 2^{2n} \cdot 3 + (2^{2n} - 1) \\ =& 2^{2n} \cdot 3 + P(n) \end{aligned}$$

Since $3|(2^{2n}-1)$ and $3|(2^{2n} \cdot 3)$ we have $3|(2^{2n} \cdot 3 + 2^{2n} - 1)$. This ends a proof of the theorem ■

Example 11.4
a. Use induction to prove that $n < 2^n$ for all non-negative integers n.
b. Use induction to prove that $2^n < n!$ for all non-negative integers $n \geq 4$.

Solution.
a. Let $P(n) : n < 2^n$ We want to show that $P(n)$ is valid for all $n \geq 0$. By the method of mathematical induction we have
(i) (Basis of induction) $2^0 - 0 = 1 > 0$. That is, $0 < 2^0$. Thus, $P(0)$is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $n < 2^n$.
(iii) (Induction step) We must show that $P(n+1)$ is also true. That is, $n + 1 < 2^{n+1}$. Indeed,

$$\begin{aligned} 2^{n+1} - (n+1) =& 2^n cdot 2 - n - 1 \\ =& 2^n(1+1) - n - 1 \\ =& (2^n - n) + 2^n - 1 \\ >& 2^n - 1 \\ >& 0 \end{aligned}$$

where we used the fact that $2^n - n > 0$.
b. Let $P(n) : 2^n < n!$. We want to show that $P(n)$ is valid for all $n \geq 4$. By the method of mathematical induction we have
(i) (Basis of induction) $4! - 2^4 = 8 > 0$. That is, $P(4)$is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $2^n < n!,\ n \geq 4$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $2^{n+1} < (n+1)!$. Indeed,

$$\begin{aligned}(n+1)!-2^{n+1} =&(n+1)n!-2^n(1+1)\\ =&n!-2^n+nn!-2^n\\ >&nn!-2^n\\ >&n!-2^n\\ >&0\end{aligned}$$

where we have used the fact that if $n \geq 1$ then $nn! \geq n!$ ■

Example 11.5 *(Bernoulli's inequality)*
Let $h > -1$. Use induction to show that

$$(1+nh) \leq (1+h)^n, \quad n \geq 0.$$

Solution.
Let $P(n) : (1+nh) \leq (1+h)^n$. We want to show that $P(n)$ is valid for all nonnegative integers. (i) (Basis of induction) $(1+h)^0 - (1+0h) = 0$. That is, $P(0)$is true.
(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $(1+nh) \leq (1+h)^n$.
(iii) (Induction step) We must show that $P(n+1)$ is true. That is, $(1+(n+1)h) \leq (1+h)^{n+1}$. Indeed,

$$\begin{aligned}(1+h)^{n+1}-(1+(n+1)h) =&(1+h)(1+h)^n-nh-1-h\\ \geq&(1+h)(1+nh)-nh-1-h\\ =&nh^2\\ \geq&0\ \blacksquare\end{aligned}$$

Example 11.6
Define the following sequence of numbers: $a_1 = 2$ and for $n \geq 2$, $a_n = 5a_{n-1}$. Find a formula for a_n and then prove its validity by mathematical induction.

Solution.
Listing the first few terms we find, $a_1 = 2, a_2 = 10, a_3 = 50, a_4 = 250$. Thus, $a_n = 2.5^{n-1}$. We will show that $P(n) : a_n = 2 \cdot 5^{n-1}$ is valid for all $n \geq 1$ by the method of mathematical induction.
(i) (Basis of induction) $a_1 = 2 = 2.5^{1-1}$. That is, $P(1)$ is true.

(ii) (Induction hypothesis) Assume $P(n)$ is true. That is, $a_n = 2.5^{n-1}$
(iii) (Induction step) We must show that $a_{n+1} = 2.5^n$. Indeed,

$$\begin{aligned} a_{n+1} &= 5a_n \\ &= 5(2.5^{n-1}) \\ &= 2.5^n \end{aligned}$$ ■

Review Problems

Problem 11.1
Use the method of induction to show that

$$2 + 4 + 6 + \cdots + 2n = n^2 + n$$

for all integers $n \geq 1$.

Problem 11.2
Use mathematical induction to prove that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all integers $n \geq 0$.

Problem 11.3
Use mathematical induction to show that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for all integers $n \geq 1$.

Problem 11.4
Use mathematical induction to show that

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

for all integers $n \geq 1$.

Problem 11.5
Use mathematical induction to show that

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

for all integers $n \geq 1$.

Problem 11.6
Use the formula

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

to find the value of the sum

$$3 + 4 + \cdots + 1,000.$$

Problem 11.7
Find the value of the geometric sum

$$1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n}.$$

Problem 11.8
Let $S(n) = \sum_{k=1}^{n} \frac{k}{(k+1)!}$. Evaluate $S(1), S(2), S(3), S(4)$, and $S(5)$. Make a conjecture about a formula for this sum for general n, and prove your conjecture by mathematical induction.

Problem 11.9
For each positive integer n let $P(n)$ be the proposition $4^n - 1$ is divisible by 3.
a. Write $P(1)$. Is $P(1)$ true?
b. Write $P(k)$.
c. Write $P(k+1)$.
d. In a proof by mathematical induction that this divisibility property holds for all integers $n \geq 1$, what must be shown in the induction step?

Problem 11.10
For each positive integer n let $P(n)$ be the proposition $2^{3n} - 1$ is divisible by 7. Prove this property by mathematical induction.

Problem 11.11
Show that $2^n < (n+2)!$ for all integers $n \geq 0$.

Problem 11.12
a. Use mathematical induction to show that $n^3 > 2n + 1$ for all integers $n \geq 2$.
b. Use mathematical induction to show that $n! > n^2$ for all integers $n \geq 4$.

Problem 11.13
A sequence $a_1, a_2, \cdots$ is defined recursively by $a_1 = 3$ and $a_n = 7a_{n-1}$ for $n \geq 2$. Show that $a_n = 3 \cdot 7^{n-1}$ for all integers $n \geq 1$.

12 Project III: Elementary Number Theory and Mathematical Proofs

Recall that the set of positive integers together with zero is denoted by $\mathbb{N}$. The set of all integers is denoted by $\mathbb{Z}$ and the set of rational numbers is denoted by $\mathbb{Q}$.

We say that an integer n is **even** if and only if there exists an integer k such that $n = 2k$. An integer n is said to be **odd** if and only if there exists an integer k such that $n = 2k + 1$.

Problem 12.1
Let m and n be two integers.
a. Is $6m + 8n$ an even integer?
b. Is $6m + 4n^2 + 3$ odd?

Let a and b be two integers with $a \neq 0$. We say that b is **divisible** by a, written $a|b$, if there exists an integer k such that $b = ka$. In this case we say that a **divides** b, a is a **factor** of b, and b is a **multiple** of a. For example, $3 \not| 7$ whereas $3|12$.

Problem 12.2
Prove the following theorem.

Theorem 12.1
Let $a \neq 0, b \neq 0$, and c be integers.
(i) If $a|b$ and $a|c$ then $a|(b \pm c)$.
(ii) If $a|b$ then $a|bc$.
(iii) If $a|b$ and $b|c$ then $a|c$.

A positive integer $p > 1$ is called **prime** if 1 and p are the only positive divisors of p. An integer ≥ 2 which is not prime is called a **composite** number. For example, 3 is prime whereas 10 is composite.

Problem 12.3
Let m and n be positive integers with $m > n$. Is $m^2 - n^2$ composite?

Problem 12.4
Write the first 7 prime numbers.

Problem 12.5
If a positive number p is composite then one can always write p as the product of primes, where the prime factors are written in increasing order. This result is known as the **Fundamental Theorem of Arithmetic** or **the Unique Factorization Theorem**. Write the prime factorization of 180.

The following important theorem shows that if a number is not divisible by any prime less than to its square root then the number must be prime.

Theorem 12.2
If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof.
Since n is composite, there is a divisor a of n such that $1 < a < n$. Write $n = ab$. If $a > \sqrt{n}$ and $b > \sqrt{n}$ then $n = ab > \sqrt{n}\sqrt{n} = n$, a false conclusion. Thus, either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Hence, n has a positive divisor which is less than or equal to $\sqrt{n}$. This divisor is either prime or, by the Fundamental Theorem of Arithmetic has a prime divisor. In either case, n has a prime divisor less than or equal to $\sqrt{n}$ ■

Problem 12.6
Use the previous theorem to show that the number 101 is prime.

13 Project IV: The Euclidean Algorithm

Let a and b be two integers not both equal to zero. We say that d is the **greatest common divisor** of a and b, written $d = gcd(a, b)$, if d is the largest integer such that $d|a$ and $d|b$. If $d = 1$ then we say that a and b are **relatively prime.** To find d one writes the prime factorization of both a and b, say $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, then

$$d = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} \cdots p_n^{min(a_n,b_n)}.$$

Problem 13.1
(i) Find $gcd(120, 500)$.
(ii) Show that 17 and 22 are relatively prime.

We say that m is the **least common multiple** of two positive integers a and b, written $m = lcm(a, b)$, if m is the smallest positive integer that is divisible by both a and b. Using the notation above, m is given by

$$m = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \cdots p_n^{max(a_n,b_n)}.$$

Problem 13.2
Find $lcm(120, 500)$.

Problem 13.3
Recall that $a \equiv b \ mod \ n$ if and only if $a - b = kn$ for some integer k.
(i) Show that if $a \equiv b \ mod \ n$ and $c \equiv d \ mod \ n$ then $a + c \equiv b + d \ mod \ n$.
(ii) Show that if $a \equiv b \ mod \ n$ and $c \equiv d \ mod \ n$ then $ac \equiv bd \ mod \ n$.
(iii) What are the solutions of the linear congruence $3x \equiv 4 (mod 7)$?

Lemma 13.1 *(Euclidean Algorithm)*
Let $a, b, q,$ and r be integers such that $a = bq + r$. Then $gcd(a, b) = gcd(b, r)$.

Proof.
Let $d_1 = gcd(a, b)$ and $d_2 = gcd(b, r)$. We will show that $d_1 = d_2$. Since $d_2|b$, $d_2|bq$. Also $d_2|r$. Consequently $d_2|(bq + r)$ that is $d_2|a$. Hence, $d_2 \leq d_1$. A similar argument shows that $d_1 \leq d_2$. We conclude that $d_1 = d_2$ ■

Using Lemma 13.1 we derive an algorithm, called the **Euclidean Algorithm,** for finding the greatest common divisor of two non-negative integers

a and b with $b \neq 0$.
Dividing a by b we obtain

$$a = bq + r_1, \quad where \;\; 0 \leq r_1 < b.$$

By Lemma 13.1 we have $gcd(a, b) = gcd(b, r_1)$. If $r_1 \neq 0$ then we divide b by r_1 to obtain

$$b = r_1 q_1 + r_2, \quad where \;\; 0 \leq r_2 < r_1.$$

Again by Lemma 13.1 we have $gcd(b, r_1) = gcd(r_1, r_2)$. If $r_2 \neq 0$ then we divide r_1 by r_2 to obtain

$$r_1 = r_2 q_2 + r_3, \quad where \;\; 0 \leq r_3 < r_2.$$

By Lemma 13.1 we have $gcd(r_1, r_2) = gcd(r_2, r_3)$. Repeating the above process, ultimately, we will end up with $r_n = r_{n+1} q_{n+1}$. In this case $r_{n+1} = gcd(a, b)$.

Problem 13.4
a. Use the Euclidean algorithm to find $gcd(414, 662)$.
b. Use the Euclidean algorithm to find $gcd(287, 91)$.

14 Project V: Induction and the Algebra of Matrices

In this section, we introduce the concept of a matrix. We also examine four operations on matrices- equality, addition, scalar multiplication, and multiplication.

A **matrix A of size** $m \times n$ is a rectangular array of the form

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix}$$

where the a_{ij}'s are the **entries** of the matrix, m is the number of rows, n is the number of columns. The **zero matrix 0** is the matrix whose entries are all 0. The $n \times n$ **identity matrix** I_n is a square matrix whose main diagonal consists of $1's$ and the off diagonal entries are all 0. A matrix A can be represented with the following compact notation $A = (a_{ij})$. The **ith row** of the matrix A is

$$[a_{i1}, a_{i2}, ..., a_{in}]$$

and the **jth column** is

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

In what follows we discuss the basic arithmetic of matrices.

Two matrices are said to be **equal** if they have the same size and their corresponding entries are all equal. If the matrix A is not equal to the matrix B we write $A \neq B$.

Problem 14.1
Find x_1, x_2 and x_3 such that

$$\begin{pmatrix} x_1 + x_2 + 2x_3 & 0 & 1 \\ 2 & 3 & 2x_1 + 4x_2 - 3x_3 \\ 4 & 3x_1 + 6x_2 - 5x_3 & 5 \end{pmatrix} = \begin{pmatrix} 9 & 0 & 1 \\ 2 & 3 & 1 \\ 4 & 0 & 5 \end{pmatrix}$$

Problem 14.2
Solve the following matrix equation for a, b, c, and d

$$\begin{pmatrix} a-b & b+c \\ 3d+c & 2a-4d \end{pmatrix} = \begin{pmatrix} 8 & 1 \\ 7 & 6 \end{pmatrix}$$

Next, we introduce the operation of addition of two matrices. If A and B are two matrices of the same size, then the **sum** $A+B$ is the matrix obtained by adding together the corresponding entries in the two matrices. Matrices of different sizes cannot be added.

Problem 14.3
Consider the matrices

$$A = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix}, C = \begin{pmatrix} 2 & 1 & 0 \\ 3 & 4 & 0 \end{pmatrix}$$

Compute, if possible, $A+B$, $A+C$ and $B+C$.

If A is a matrix and c is a scalar, then the product cA is the matrix obtained by multiplying each entry of A by c. Hence, $-A = (-1)A$. We define, $A-B = A+(-B)$. The matrix cI_n is called a **scalar** matrix.

Problem 14.4
Consider the matrices

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 1 & 2 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 2 & 7 \\ 1 & -3 & 5 \end{pmatrix}$$

Compute $A - 3B$.

Problem 14.5
Let A be an $m \times n$ matrix. The **transpose** of A, denote by A^T, is the $n \times m$ whose columns are the rows of A. Find the transpose of the matrix

$$A = \begin{pmatrix} 2 & 3 & 4 \\ 1 & 2 & 1 \end{pmatrix}.$$

Now, let A be a matrix of size $m \times n$ and entries a_{ij}; B is a matrix of size $n \times p$ and entries b_{ij}. Then the **product** matrix is a matrix of size $m \times p$ and entries

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$$

that is c_{ij} is obtained by multiplying componentwise the entries of the ith row of A by the entries of the jth column of B. It is very important to keep in mind that the number of columns of the first matrix must be equal to the number of rows of the second matrix; otherwise the product is undefined.

Problem 14.6
Consider the matrices

$$A = \begin{pmatrix} 1 & 2 & 4 \\ 2 & 6 & 0 \end{pmatrix}, B = \begin{pmatrix} 4 & 1 & 4 & 3 \\ 0 & -1 & 3 & 1 \\ 2 & 7 & 5 & 2 \end{pmatrix}.$$

Compute, if possible, AB and BA.

Problem 14.7
Prove by induction on $n \geq 1$ that

$$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}^n = \begin{pmatrix} 2^n & n2^{n-1} \\ 0 & 2^n \end{pmatrix}.$$

Fundamentals of Set Theory

Set is the most basic term in mathematics and computer science. Hardly any discussion in either subject can proceed without *set* or some synonym such as *class* or *collection*. In this chapter we introduce the concept of sets and its various operations and then study the properties of these operations.

15 Basic Definitions

We first consider the following known as the **barber puzzle**: "The army captain orders his company barber to shave all members of the company provided they do not shave themselves. The barber is so busy at first that his own beard begins to be unsightly. Just as he lathers up, the impossibility of his position strikes him: If he shaves himself, he disobeys the captain's order. If he does not shave himself, then by the captain's order he is supposed to shave himself."
A situation like this is known as a **paradox.** To resolve the problem one has to take the barber out of the company. Another well known paradox is

Russell's Paradox. Define the set $A = \{X : X \text{ is a set}, X \notin X\}$.
Since A is a set, saying that $A \in A$ will imply that $A \notin A$ by the definition of A. Saying that $A \notin A$ means that $A \in A$ by the definition of A. Thus in either case the assumption that A is a set leads to an untenable paradox: $A \in A$ and $A \notin A$. Hence, A is not a set.
Such a paradox indicated the necessity of a formal axiomatization of set theory.
We define a **set** A as a collection of well-defined objects (called **elements** or **members** of A) such that for any given object x either one (but not both) of the following holds:

- x belongs to A and we write $x \in A$.
- x does not belong to A, and in this case we write $x \notin A$.

We denote sets by capital letters $A, B, C, \cdots$ and elements by lowercase letters $a, b, c, \cdots$ Sets consisting of sets will be denoted by script letters.
There are two different ways to represent a set. The first one is to list, without repetition, the elements of the set. The other way is to describe a property that characterizes the elements of the set.
We define the **empty** set, denoted by $\emptyset$, to be the set with no elements.

Example 15.1
List the elements of the following sets.
a. $\{x | x$ is a real number such that $x^2 = 1\}$.
b. $\{x | x$ is an integer such that $x^2 - 3 = 0\}$.

Solution.
a. $\{-1, 1\}$.
b. $\emptyset$ ■

Example 15.2
Use a property to give a description of each of the following sets.
a. $\{a, e, i, o, u\}$.
b. $\{1, 3, 5, 7, 9\}$.

Solution.
a. $\{x | x \textit{ is a vowel}\}$.
b. $\{n \in \mathbb{N}^* | n \textit{ is odd and less than } 10\}$ ■

Let A and B be two sets. We say that A is a **subset** of B, denoted by $A \subseteq B$, if and only if every element of A is also an element of B. Symbolically:

$$A \subseteq B \Leftrightarrow \forall x, x \in A \textit{ implies } x \in B$$

If there exists an element of A which is not in B then we write $A \nsubseteq B$.
Now for any set A, the proposition $x \in \emptyset \Rightarrow x \in A$ is vacuously true, hence $\emptyset \subseteq A$.

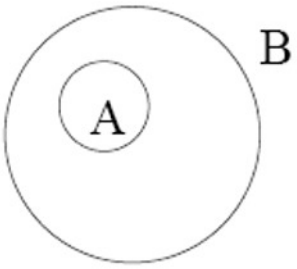
Example 15.3
Suppose that $A = \{2, 4, 6\}$, $B = \{2, 6\}$, and $C = \{4, 6\}$. Determine which of these sets are subsets of which other(s) of these sets.

Solution.
$B \subseteq A$ and $C \subseteq A$ ■

If sets A and B are represented as regions in the plane, relationships between A and B can be represented by pictures, called **Venn diagrams.**

Example 15.4
Represent $A \subseteq B$ using a Venn diagram.

Solution.



■

Two sets A and B are said to be **equal** if and only if $A \subseteq B$ and $B \subseteq A$. We write $A = B$. Thus, to show that $A = B$ it suffices to show the double inclusions mentioned in the definition. For non-equal sets we write $A \neq B$.

Example 15.5
Determine whether each of the following pairs of sets are equal.
(a) $\{1, 3, 5\}$ and $\{5, 3, 1\}$.
(b) $\{\{1\}\}$ and $\{1, \{1\}\}$.

Solution.
(a) $\{1, 3, 5\} = \{5, 3, 1\}$.
(b) $\{\{1\}\} \neq \{1, \{1\}\}$ since $1 \notin \{\{1\}\}$ ■

Let A and B be two sets. We say that A is a **proper** subset of B, denoted by $A \subset B$, if $A \subseteq B$ and $A \neq B$. Thus, to show that A is a proper subset of B we must show that every element of A is an element of B and there is an element of B which is not in A.

Example 15.6
Order the sets of numbers: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{N}$ using $\subset$

Solution.
$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ ■

Example 15.7
Determine whether each of the following statements is true or false.
(a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{x\} \in \{x\}$
(d) $\{x\} \in \{\{x\}\}$ (e) $\emptyset \subseteq \{x\}$ (f) $\emptyset \in \{x\}$

Solution.
(a) True (b) True (c) False (d) True (e) True (f) False ■

If U is a given set whose subsets are under consideration, then we call U a **universal set.**
Let U be a universal set and A, B be two subsets of U. The **absolute complement** of A is the set

$$A^c = \{x \in U | x \notin A\}.$$

The **relative complement** of A with respect to B is the set

$$B - A = \{x \in U | x \in B \text{ and } x \notin A\}.$$

Example 15.8
Let $U = \mathbb{R}$. Consider the sets $A = \{x \in \mathbb{R} | x < -1 \text{ or } x > 1\}$ and $B = \{x \in \mathbb{R} | x \leq 0\}$. Find

a. A^c.
b. $B - A$.

Solution.
a. $A^c = [-1, 1]$.
b. $B - A = [-1, 0]$ ■

Let A and B be two sets. The **union** of A and B is the set

$$A \cup B = \{x | x \in A \text{ or } x \in B\}.$$

where the 'or' is inclusive. This definition can be extended to more than two sets. More precisely, if $A_1, A_2, \cdots$, are sets then

$$\cup_{n=1}^{\infty} A_n = \{x | x \in A_i \ for \ some \ i\}.$$

Let A and B be two sets. The **intersection** of A and B is the set

$$A \cap B = \{x | x \in A \ and \ x \in B\}.$$

If $A \cap B = \emptyset$ we say that A and B are **disjoint** sets. Given the sets $A_1, A_2, \cdots$, we define

$$\cap_{n=1}^{\infty} A_n = \{x | x \in A_i \ for \ all \ i\}.$$

Example 15.9
Let $A = \{a, b, c\}, B = \{b, c, d\}$, and $C = \{b, c, e\}$.

a. Find $A \cup (B \cap C), (A \cup B) \cap C$, and $(A \cup B) \cap (A \cup C)$. Which of these sets are equal?
b. Find $A \cap (B \cup C), (A \cap B) \cup C$, and $(A \cap B) \cup (A \cap C)$. Which of these sets are equal?
c. Find $A - (B - C)$ and $(A - B) - C$. Are these sets equal?

Solution.
a. $A \cup (B \cap C) = A, (A \cup B) \cap C = \{b, c\}, (A \cup B) \cap (A \cup C) = \{b, c\} = (A \cup B) \cap C$.
b. $A \cap (B \cup C) = \{b, c\}, (A \cap B) \cup C = C, (A \cap B) \cup (A \cap C) = \{b, c\} = A \cap (B \cup C)$.
c. $A - (B - C) = A$ and $(A - B) - C = \{a\} \neq A - (B - C)$. ■

Example 15.10
For each $n \geq 1$, let $A_n = \{x \in \mathbb{R} : x < 1 + \frac{1}{n}\}$. Show that

$$\cap_{n=1}^{\infty} A_n = \{x \in \mathbb{R} : x \leq 1\}.$$

Solution.
The proof is by double inclusions method. Let $y \in \{x \in \mathbb{R} : x \leq 1\}$. Then for all positive integer n we have $y \leq 1 < 1 + \frac{1}{n}$. That is, $y \in \cap_{n=1}^{\infty} A_n$. This shows that $\{x \in \mathbb{R} : x \leq 1\} \subseteq \cap_{n=1}^{\infty} A_n$.
Conversely, let $y \in \cap_{n=1}^{\infty} A_n$. Then $y < 1 + \frac{1}{n}$ for all $n \geq 1$. Now take the limit of both sides as $n \to \infty$ to obtain $y \leq 1$. That is, $y \in \{x \in \mathbb{R} : x \leq 1\}$. This shows that $\cap_{n=1}^{\infty} A_n \subseteq \{x \in \mathbb{R} : x \leq 1\}$. ■

Example 15.11
The **symmetric difference** of A and B, denoted by $A\Delta B$, is the set containing those elements in either A or B but not both. Find $A\Delta B$ if $A = \{1, 3, 5\}$ and $B = \{1, 2, 3\}$.

Solution.
$A\Delta B = \{2, 5\}$ ■

The notation $(a_1, a_2, \cdots, a_n)$ is called an **ordered n-tuples**. We say that two n-tuples $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ are equal if and only if $a_1 = b_1, a_2 = b_2, \cdots, a_n = b_n$.
Given n sets $A_1, A_2, \cdots, A_n$ the **Cartesian product** of these sets is the set

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) : a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n\}$$

Example 15.12
Let $A = \{x, y\}, B = \{1, 2, 3\}$, and $C = \{a, b\}$. Find
a. $A \times B \times C$.
b. $(A \times B) \times C$.

Solution.
a.

$$\begin{aligned} A \times B \times C = \; & \{(x,1,a),(x,2,a),(x,3,a),(y,1,a),(y,2,a),\\ & (y,3,a),(x,1,b),(x,2,b),(x,3,b),(y,1,b)\\ & (y,2,b),(y,3,b)\} \end{aligned}$$

b.

$$\begin{aligned} (A \times B) \times C = \; & \{((x,1),a),((x,2),a),((x,3),a),((y,1),a),((y,2),a),\\ & ((y,3),a),((x,1),b),((x,2),b),((x,3),b),((y,1),b)\\ & ((y,2),b),((y,3),b)\} \blacksquare \end{aligned}$$

Next, we introduce one more special kind of sets, denoted by Σ^*. An **alphabet** is a finite nonempty set Σ whose members are called **letters** and with the restrictions that Σ does not contain letters which are themselves strings beginning with other letters of Σ. Thus, $\Sigma = \{a, b, c, ca\}$ is not an alphabet. A **word** is any finite string of letters from Σ. We denote the set of all words using letters from Σ by Σ^*. Any subset of Σ^* is called a **language**. For example, if Σ consists of the twenty six letters of the english alphabet, then the American language can be defined as the subset of Σ^* consisting of

words in the latest edition of the *Webster's World dictionary of the American Language*.
The **empty word** or the **null word** is the string with no letters. It is denoted by ϵ.
We define the **length** of a word w to be the number of letters from Σ in w and we write $|w|$. Note that in order to define the length of a word the restriction given in the definition is needed. To be more precise, suppose that $\Sigma = \{a, b, ab\}$. Then what is the length of the word aab? Is this a word with two letters a and ab or three letters a, a, and b? So obviously there is no way to tell. This ambiguity is resolved by making the restriction stated in the definition of alphabet.
Finally, by Σ^n we mean the set of all words over Σ of length n. That is, Σ^n is the cartesian product of n copies of Σ.

Example 15.13
Let $\Sigma = \{a, b\}$. List all the elements of the set

$$A = \{w \in \Sigma^* : |w| = 2\}.$$

Solution.

$$A = \{aa, ab, ba, bb\} \quad \blacksquare$$

Review Problems

Problem 15.1
Which of the following sets are equal?
a. $\{a, b, c, d\}$
b. $\{d, e, a, c\}$
c. $\{d, b, a, c\}$
d. $\{a, a, d, e, c, e\}$

Problem 15.2
Let $A = \{c, d, f, g\}, B = \{f, j\}$, and $C = \{d, g\}$. Answer each of the following questions. Give reasons for your answers.
a. Is $B \subseteq A$?
b. Is $C \subseteq A$?
c. Is $C \subseteq C$?
d. Is C a proper subset of A?

Problem 15.3
a. Is $3 \in \{1, 2, 3\}$?
b. Is $1 \subseteq \{1\}$?
c. Is $\{2\} \in \{1, 2\}$?
d. Is $\{3\} \in \{1, \{2\}, \{3\}\}$?
e. Is $1 \in \{1\}$?
f. Is $\{2\} \subseteq \{1, \{2\}, \{3\}\}$?
g. Is $\{1\} \subseteq \{1, 2\}$?
h. Is $1 \in \{\{1\}, 2\}$?
i. Is $\{1\} \subseteq \{1, \{2\}\}$?
j. Is $\{1\} \subseteq \{1\}$?

Problem 15.4
Let $A = \{b, c, d, f, g\}$ and $B = \{a, b, c\}$. Find each of the following:
a. $A \cup B$.
b. $A \cap B$.
c. $A - B$.
d. $B - A$.

Problem 15.5
Indicate which of the following relationships are true and which are false:
a. $\mathbb{Z}^+ \subseteq \mathbb{Q}$.

b. $\mathbb{R}^- \subset \mathbb{Q}$.
c. $\mathbb{Q} \subset \mathbb{Z}$.
d. $\mathbb{Z}^+ \cup \mathbb{Z}^- = \mathbb{Z}$.
e. $\mathbb{Q} \cap \mathbb{R} = \mathbb{Q}$.
f. $\mathbb{Q} \cup \mathbb{Z} = \mathbb{Z}$.
g. $\mathbb{Z}^+ \cap \mathbb{R} = \mathbb{Z}^+$
h. $\mathbb{Z} \cup \mathbb{Q} = \mathbb{Q}$.

Problem 15.6
Let $A = \{x, y, z, w\}$ and $B = \{a, b\}$. List the elements of each of the following sets:
a. $A \times B$
b. $B \times A$
c. $A \times A$
d. $B \times B$.

Problem 15.7
Let $\Sigma = \{x, y\}$ be an alphabet.
a. Let L_1 be the language consisting of all strings over Σ that are palindromes and have length ≤ 4. List the elements L_1.
b. Let L_2 be the language consisting of all strings over Σ that begins with x and have length ≤ 3. List the elements L_2.
c. Let L_3 be the language consisting of all strings over Σ with length ≤ 3 and for which all the $x's$ appear to the left of all the $y's$. List the elements L_3.
d. List the elements of Σ^4, the set of all strings of length 4 over Σ.
e. Let $A = \Sigma^3 \cup \Sigma^4$. Describe A, B, and $A \cup B$ in words.

16 Properties of Sets

The following exercise shows that the operation $\subseteq$ is reflexive and transitive, concepts that will be discussed in the next chapter.

Example 16.1
a. Suppose that A, B, C are sets such that $A \subseteq B$ and $B \subseteq C$. Show that $A \subseteq C$.
b. Find two sets A and B such that $A \in B$ and $A \subseteq B$.
c. Show that $A \subseteq A$.

Solution.
a. We need to show that every element of A is an element of C. Let $x \in A$. Since $A \subseteq B$, we hav $x \in B$. But $B \subseteq C$ so that $x \in C$.
b. $A = \{x\}$ and $B = \{x, \{x\}\}$.
c. The proposition if $x \in A$ then $x \in A$ is always true. Thus, $A \subseteq A$ ■

Theorem 16.1
Let A and B be two sets. Then
a. $A \cap B \subseteq A$ and $A \cap B \subseteq B$.
b. $A \subseteq A \cup B$ and $B \subseteq A \cup B$.

Proof.
a. If $x \in A \cap B$ then $x \in A$ and $x \in B$. This still imply that $x \in A$. Hence, $A \cap B \subseteq A$. A similar argument holds for $A \cap B \subseteq B$.
b. The proposition "if $x \in A$ then $x \in A \cup B$" is always true. Hence, $A \subseteq A \cup B$. A similar argument holds for $B \subseteq A \cup B$■

Theorem 16.2
Let A be a subset of a universal set U. Then
a. $\emptyset^c = U$.
b. $U^c = \emptyset$.
c. $(A^c)^c = A$.
d. $A \cup A^c = U$.
e. $A \cap A^c = \emptyset$.

Proof.
a. If $x \in U$ then $x \in U$ and $x \notin \emptyset$. Thus, $U \subseteq \emptyset^c$. Conversely, suppose that $x \in \emptyset^c$. Then $x \in U$ and $x \notin \emptyset$. This implies that $x \in U$. Hence, $\emptyset^c \subseteq U$.

b. It is always true that $\emptyset \subseteq U^c$. Conversely, the proposition "$x \in U$ and $x \notin U$ implies $x \in \emptyset$" is vacuously true since the hypothesis is false. This says that $U^c \subseteq \emptyset$.
c. Let $x \in (A^c)^c$. Then $x \in U$ and $x \notin A^c$. That is, $x \in U$ and ($x \notin U$ or $x \in A$). Since $x \in U$, we have $x \in A$. Hence $(A^c)^c \subseteq A$. Conversely, suppose that $x \in A$. Then $x \in U$ and $x \in A$. That is, $x \in U$ and $x \notin A^c$. Thus, $x \in (A^c)^c$. This shows that $A \subseteq (A^c)^c$.
d. It is clear that $A \cup A^c \subseteq U$. Conversely, suppose that $x \in U$. Then either $x \in A$ or $x \notin A$. But this is the same as saying that $x \in A \cup A^c$.
e. By definition $\emptyset \subseteq A \cap A^c$. Conversely, the conditional proposition "$x \in A$ and $x \notin A$ implies $x \in \emptyset$" is vacuously true since the hypothesis is false. This shows that $A \cap A^c \subseteq \emptyset$ ■

Theorem 16.3
If A and B are subsets of U then
a. $A \cup U = U$.
b. $A \cup A = A$.
c. $A \cup \emptyset = A$.
d. $A \cup B = B \cup A$.
e. $(A \cup B) \cup C = A \cup (B \cup C)$.

Proof.
a. Clearly, $A \cup U \subseteq U$. Conversely, let $x \in U$. Then definitely, $x \in A \cup U$. That is, $U \subseteq A \cup U$.
b. If $x \in A$ then $x \in A$ or $x \in A$. That is, $x \in A \cup A$ and consequently $A \subseteq A \cup A$. Conversely, if $x \in A \cup A$ then $x \in A$. Hence, $A \cup A \subseteq A$.
c. If $x \in A \cup \emptyset$ then $x \in A$ since $x \notin \emptyset$. Thus, $A \cup \emptyset \subseteq A$. Conversely, if $x \in A$ then $x \in A$ or $x \in \emptyset$. Hence, $A \subseteq A \cup \emptyset$.
d. If $x \in A \cup B$ then $x \in A$ or $x \in B$. But this is the same thing as saying $x \in B$ or $x \in A$. That is, $x \in B \cup A$. Now interchange the roles of A and B to show that $B \cup A \subseteq A \cup B$.
e. Let $x \in (A \cup B) \cup C$. Then $x \in (A \cup B)$ or $x \in C$. Thus, ($x \in A$ or $x \in B$) or $x \in C$. This implies $x \in A$ or ($x \in B$ or $x \in C$). Hence, $x \in A \cup (B \cup C)$. The converse is similar ■

Theorem 16.4
Let A and B be subsets of U. Then
a. $A \cap U = A$.

b. $A \cap A = A$.
c. $A \cap \emptyset = \emptyset$.
d. $A \cap B = B \cap A$.
e. $(A \cap B) \cap C = A \cap (B \cap C)$.

Proof.
a. If $x \in A \cap U$ then $x \in A$. That is , $A \cap U \subseteq A$. Conversely, let $x \in A$. Then definitely, $x \in A$ and $x \in U$. That is, $x \in A \cap U$. Hence, $A \subseteq A \cap U$.
b. If $x \in A$ then $x \in A$ and $x \in A$. That is, $A \subseteq A \cap A$. Conversely, if $x \in A \cap A$ then $x \in A$. Hence, $A \cap A \subseteq A$.
c. Clearly $\emptyset \subseteq A \cap \emptyset$. Conversely, if $x \in A \cap \emptyset$ then $x \in \emptyset$. Hence, $A \cap \emptyset \subseteq \emptyset$.
d. If $x \in A \cap B$ then $x \in A$ and $x \in B$. But this is the same thing as saying $x \in B$ and $x \in A$. That is, $x \in B \cap A$. Now interchange the roles of A and B to show that $B \cap A \subseteq A \cap B$.
e. Let $x \in (A \cap B) \cap C$. Then $x \in (A \cap B)$ and $x \in C$. Thus, ($x \in A$ and $x \in B$) and $x \in C$. This implies $x \in A$ and ($x \in B$ and $x \in C$). Hence, $x \in A \cap (B \cap C)$. The converse is similar ■

Theorem 16.5
If A, B, and C are subsets of U then
a. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
b. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof.
a. Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Thus, $x \in A$ and ($x \in B$ or $x \in C$). This implies that ($x \in A$ and $x \in B$) or ($x \in A$ and $x \in C$). Hence, $x \in A \cap B$ or $x \in A \cap C$, i.e. $x \in (A \cap B) \cup (A \cap C)$. The converse is similar.
b. Let $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. Thus, $x \in A$ or ($x \in B$ and $x \in C$). This implies that ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$). Hence, $x \in A \cup B$ and $x \in A \cup C$, i.e. $x \in (A \cup B) \cap (A \cup C)$. The converse is similar ■

Theorem 16.6 *(De Morgan's Laws)*
Let A and B be subsets of U then
a. $(A \cup B)^c = A^c \cap B^c$.
b. $(A \cap B)^c = A^c \cup B^c$.

Proof.
a. Let $x \in (A \cup B)^c$. Then $x \in U$ and $x \notin A \cup B$. Hence, $x \in U$ and ($x \notin A$ and $x \notin B$). This implies that ($x \in U$ and $x \notin A$) and ($x \in U$ and $x \notin B$). It follows that $x \in A^c \cap B^c$. Now, go backward for the converse.
b. Let $x \in (A \cap B)^c$. Then $x \in U$ and $x \notin A \cap B$. Hence, $x \in U$ and ($x \notin A$ or $x \notin B$). This implies that ($x \in U$ and $x \notin B$) or ($x \in U$ and $x \notin A$). It follows that $x \in A^c \cup B^c$. The converse is similar ■

Theorem 16.7
Suppose that $A \subseteq B$. Then
a. $A \cap B = A$.
b. $A \cup B = B$.

Proof.
a. If $x \in A \cap B$ then by the definition of intersection of two sets we have $x \in A$. Hence, $A \cap B \subseteq A$. Conversely, if $x \in A$ then $x \in B$ as well since $A \subseteq B$. Hence, $x \in A \cap B$. This shows that $A \subseteq A \cap B$.
b. If $x \in A \cup B$ then $x \in A$ or $x \in B$. Since $A \subseteq B$ we have $x \in B$. Hence, $A \cup B \subseteq B$. Conversely, if $x \in B$ then $x \in A \cup B$. This shows that $B \subseteq A \cup B$.■

Example 16.2
Let A and B be arbitrary sets. Show that $(A - B) \cap B = \emptyset$.

Solution.
Suppose not. That is, suppose $(A - B) \cap B \neq \emptyset$. Then there is an element x that belongs to both $A - B$ and B. By the definition of $A - B$ we have that $x \notin B$. Thus, $x \in B$ and $x \notin B$ which is a contradiction ■

A collection of nonempty subsets $\{A_1, A_2, \cdots, A_n\}$ of A is said to be a **partition** of A if and only if

(i) $A = \cup_{k=1}^{n} A_k$.
(ii) $A_i \cap A_j = \emptyset$ for all $i \neq j$.

Example 16.3
Let $A = \{1, 2, 3, 4, 5, 6\}, A_1 = \{1, 2\}, A_2 = \{3, 4\}, A_3 = \{5, 6\}$. Show that $\{A_1, A_2, A_3\}$ is a partition of A.

Solution.
(i) $A_1 \cup A_2 \cup A_3 = A$.
(ii) $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = \emptyset$.■

The number of elements of a set is called the **cardinality** of the set. We write $|A|$ to denote the cardinality of the set A. If A has a finite cardinality we say that A is a **finite** set. Otherwise, it is called **infinite**.

Example 16.4
What is the cardinality of each of the following sets.
(a) $\emptyset$.
(b) $\{\emptyset\}$.
(c) $\{a, \{a\}, \{a, \{a\}\}\}$.

Solution.
(a) $|\emptyset| = 0$
(b) $|\{\emptyset\}| = 1$
(c) $|\{a, \{a\}, \{a, \{a\}\}\}| = 3$ ■

Let A be a set. The **power set** of A, denoted by $\mathcal{P}(\mathrm{A})$, is the empty set together with all possible subsets of A.

Example 16.5
Find the power set of $A = \{a, b, c\}$.

Solution.

$$\begin{aligned}\mathcal{P}(\mathrm{A}) \;=\; & \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \\ & \{b, c\}, \{a, b, c\}\} \quad ■\end{aligned}$$

Theorem 16.8
If $A \subseteq B$ then $\mathcal{P}(\mathrm{A}) \subseteq \mathcal{P}(\mathrm{B})$.

Proof.
Let $X \in \mathcal{P}(\mathrm{A})$. Then $X \subseteq A$. Since $A \subseteq B$, we have $X \subseteq B$. Hence, $X \in \mathcal{P}(\mathrm{B})$ ■

Example 16.6
a. Use induction to show that if $|A| = n$ then $|\mathcal{P}(\mathrm{A})| = 2^n$.
b. If $\mathcal{P}(\mathrm{A})$ has 256 elements, how many elements are there in A?

Solution.
a. If $n = 0$ then $A = \emptyset$ and in this case $\mathcal{P}(\mathrm{A}) = \{\emptyset\}$. Thus $|\mathcal{P}(\mathrm{A})| = 1$. As induction hypothesis, suppose that if $|A| = n$ then $|\mathcal{P}(\mathrm{A})| = 2^n$. Let $B = A \cup \{a_{n+1}\}$. Then $\mathcal{P}(\mathrm{B})$ consists of all subsets of A and all subsets of A with the element a_{n+1} added to them. Hence, $|\mathcal{P}(\mathrm{B})| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$.
b. Since $|\mathcal{P}(\mathrm{A})| = 256 = 2^8$, we have $|A| = 8$ ■

Review Problems

Problem 16.1
Let A, B, and C be sets. Prove that if $A \subseteq B$ then $A \cap C \subseteq B \cap C$.

Problem 16.2
Find sets A, B, and C such that $A \cap C = B \cap C$ but $A \neq B$.

Problem 16.3
Find sets A, B, and C such that $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$ but $A \neq B$.

Problem 16.4
Let A and B be two sets. Prove that if $A \subseteq B$ then $B^c \subseteq A^c$.

Problem 16.5
Let A, B, and C be sets. Prove that if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Problem 16.6
Let A, B, and C be sets. Show that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Problem 16.7
Let A, B, and C be sets. Show that $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Problem 16.8
a. Is the number 0 in $\emptyset$? Why?
b. Is $\emptyset = \{\emptyset\}$? Why?
c. Is $\emptyset \in \{\emptyset\}$? Why?

Problem 16.9
Let A and B be two sets. Prove that $(A - B) \cap (A \cap B) = \emptyset$.

Problem 16.10
Let A and B be two sets. Show that if $A \subseteq B$ then $A \cap B^c = \emptyset$.

Problem 16.11
Let A, B and C be three sets. Prove that if $A \subseteq B$ and $B \cap C = \emptyset$ then $A \cap C = \emptyset$.

Problem 16.12
Find two sets A and B such that $A \cap B = \emptyset$ but $A \times B \neq \emptyset$.

Problem 16.13
Suppose that $A = \{1, 2\}$ and $B = \{2, 3\}$. Find each of the following:
a. $\mathcal{P}(\mathrm{A} \cap \mathrm{B})$.
b. $\mathcal{P}(\mathrm{A})$.
c. $\mathcal{P}(\mathrm{A} \cup \mathrm{B})$.
d. $\mathcal{P}(\mathrm{A} \times \mathrm{B})$.

Problem 16.14
a. Find $\mathcal{P}(\emptyset)$.
b. Find $\mathcal{P}(\mathcal{P}(\emptyset))$.
c. Find $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.

Problem 16.15
Determine which of the following statements are true and which are false. Prove each statement that is true and give a counterexample for each statement that is false.
a. $\mathcal{P}(\mathrm{A} \cup \mathrm{B}) = \mathcal{P}(\mathrm{A}) \cup \mathcal{P}(\mathrm{B})$.
b. $\mathcal{P}(\mathrm{A} \cap \mathrm{B}) = \mathcal{P}(\mathrm{A}) \cap \mathcal{P}(\mathrm{B})$.
c. $\mathcal{P}(\mathrm{A}) \cup \mathcal{P}(\mathrm{B}) \subseteq \mathcal{P}(\mathrm{A} \cup \mathrm{B})$.
d. $\mathcal{P}(\mathrm{A} \times \mathrm{B}) = \mathcal{P}(\mathrm{A}) \times \mathcal{P}(\mathrm{B})$.

17 Project VI: Boolean Algebra

A **Boolean algebra** is a nonempty set S together with two operations $\oplus$ and $\odot$ that satisfy the following axioms:

- $a \oplus b \in S$ and $a \odot b \in S$ for all $a, b \in S$.
- $a \oplus b = b \oplus a$ and $a \odot b = b \odot a$, $\forall a, b \in S$.
- $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ and $a \odot (b \odot c) = (a \odot b) \odot c)$, $\forall a, b, c \in S$.
- $a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c)$ and $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ $\forall a, b, c \in S$.
- There exist distinct elements 0 and 1 in S such that $a \oplus 0 = a$ and $a \odot 1 = a$ $\forall a \in S$.
- For each $a \in S$ there exists an element $\overline{a}$ such that $a \oplus \overline{a} = 1$ and $a \odot \overline{a} = 0$. We call $\overline{a}$ the **complement** or the **negation** of a.

We write $(S, \oplus, \odot)$.

Problem 17.1
Show that if S is a collection of propositions with finite propositional variables then $(S, \vee, \wedge)$ is a Boolean algebra.

Problem 17.2
Show that for a given nonempty set S, $(\mathcal{P}(\mathrm{S}), \cup, \cap)$ is a Boolean algebra.

Relations and Functions

The reader is familiar with many relations which are used in mathematics and computer science, i.e. "is a subset of", " is less than" and so on.
One frequently wants to compare or contrast various members of a set, perhaps to arrange them in some appropriate order or to group together those with similar properties. The mathematical framework to describe this kind of organization of sets is the theory of relations.
There are three kinds of relations which we discuss in this chapter: (i) equivalence relations, (ii) order relations, (iii) functions.

18 Equivalence Relations

Let A be a given set. An **ordered pair** (a, b) of elements in A is defined to be the set $\{a, \{a, b\}\}$. The element a (resp. b) is called the **first** (resp. **second**) **component**.

Example 18.1
a. Show that if $a \neq b$ then $(a, b) \neq (b, a)$.
b. Show that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

Solution.
a. If $a \neq b$ then $\{a, \{a, b\}\} \neq \{b, \{a, b\}\}$. That is, $(a, b) \neq (b, a)$.
b. $(a, b) = (c, d)$ if and only if $\{a, \{a, b\}\} = \{c, \{c, d\}\}$ and this is equivalent to $a = c$ and $\{a, b\} = \{c, d\}$ by the definition of equality of sets. Thus, $a = c$ and $b = d$. ■

Example 18.2
Find x and y such that $(x + y, 0) = (1, x - y)$.

Solution.
By the previous exercise we have the system

$$\begin{cases} x + y = 1 \\ x - y = 0 \end{cases}$$

Solving by the method of elimination one finds $x = \frac{1}{2}$ and $y = \frac{1}{2}$. ■

If A and B are sets, we let $A \times B$ denote the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. We call $A \times B$ the **Cartesian product** of A and B.

Example 18.3
a. Show that if A is a set with m elements and B is a set of n elements then $A \times B$ is a set of mn elements.
b. Show that if $A \times B = \emptyset$ then $A = \emptyset$ or $B = \emptyset$.

Solution.
a. Consider an ordered pair (a, b). There are m possibilities for a. For each fixed a, there are n possibilities for b. Thus, there are $m \times n$ ordered pairs (a, b). That is, $|A \times B| = mn$.
b. We use the proof by contrapositive. Suppose that $A \neq \emptyset$ and $B \neq \emptyset$. Then there is at least an $a \in A$ and an element $b \in B$. That is, $(a, b) \in A \times B$ and this shows that $A \times B \neq \emptyset$. A contradiction to the assumption that $A \times B = \emptyset$■

Example 18.4
Let $A = \{1, 2\}, B = \{1\}$. Show that $A \times B \neq B \times A$.

Solution.
We have $A \times B = \{(1, 1), (2, 1)\} \neq \{(1, 1), (1, 2)\} = B \times A$.■

A **binary relation** R from a set A to a set B is a subset of $A \times B$. If $(a, b) \in R$ we write aRb and we say that a is related to b. If a is not related to b we write $a \not R b$. In case $A = B$ we call R a **binary relation** on A.
The set

$$Dom(R) = \{a \in A | (a, b) \in R \ for \ some \ b \in B\}$$

is called the **domain** of R. The set

$$Range(R) = \{b \in B | (a, b) \in R \ for \ some \ a \in A\}$$

is called the **range** of R.

Example 18.5
a. Let $A = \{2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$. Define the relation R by aRb if and only if *a divides b*. Find, $R, Dom(R), Range(R)$.
b. Let $A = \{1, 2, 3, 4\}$. Define the relation R by aRb if and only if $a \leq b$. Find, $R, Dom(R), Range(R)$.

Solution.
a. $R = \{(2, 4), (2, 6), (3, 3), (3, 6), (4, 4)\}$, $Dom(R) = \{2, 3, 4\}$, and $Range(R) = \{3, 4, 6\}$.
b. $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$, $Dom(R) = A$, $Range(R) = A$. ■

A **function** is a special case of a relation. A function from A to B, denoted by $f : A \to B$, is a relation from A to B such that for every $x \in A$ there is a unique $y \in B$ such that $(x, y) \in f$. The element y is called the **image** of x and we write $y = f(x)$. The set A is called the **domain** of f and the set of all images of f is called the **range** of f. Functions will be discussed in more detail in Section 20.

Example 18.6
a. Show that the relation

$$f = \{(1, a), (2, b), (3, a)\}$$

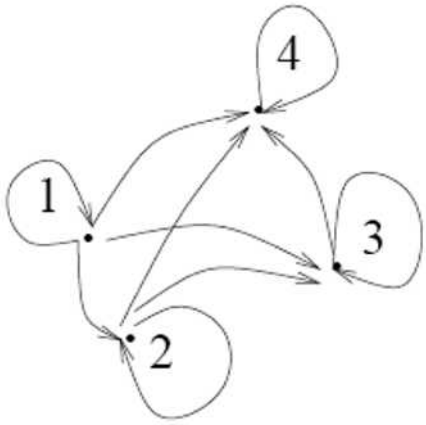
defines a function from $A = \{1, 2, 3\}$ to $B = \{a, b, c\}$. Find its range.
b. Show that the relation $f = \{(1, a), (2, b), (3, c), (1, b)\}$ does not define a function from $A = \{1, 2, 3\}$ to $B = \{a, b, c\}$.

Solution.
a. Note that each element of A has exactly one image. Hence, f is a function with domain A and range $Range(f) = \{a, b\}$.
b. The relation f does not define a function since the element 1 has two images, namely a and b. ■

An informative way to picture a relation on a set is to draw its **digraph.** To draw a digraph of a relation on a set A, we first draw dots or **vertices** to represent the elements of A. Next, if $(a, b) \in R$ we draw an arrow (called a **directed edge**) from a to b. Finally, if $(a, a) \in R$ then the directed edge is simply a **loop**.

Example 18.7
Draw the directed graph of the relation in part (b) of Problem 18.5.

Solution.



■

Next we discuss three ways of building new relations from given ones. Let R be a relation from a set A to a set B. The **inverse** of R is the relation R^{-1} from $Range(R)$ to $Dom(R)$ such that

$$R^{-1} = \{(b, a) \in B \times A : (a, b) \in R\}.$$

Example 18.8
Let $R = \{(1, y), (1, z), (3, y)\}$ be a relation from $A = \{1, 2, 3\}$ to $B = \{x, y, z\}$.
a. Find R^{-1}.
b. Compare $(R^{-1})^{-1}$ and R.

Solution.
a. $R^{-1} = \{(y, 1), (z, 1), (y, 3)\}$.
b. $(R^{-1})^{-1} = R$. ■

Let R and S be two relations from a set A to a set B. Then we define the relations $R \cup S$ and $R \cap S$ by

$$R \cup S = \{(a, b) \in A \times B | (a, b) \in R \text{ or } (a, b) \in S\},$$

and

$$R \cap S = \{(a, b) \in A \times B | (a, b) \in R \text{ and } (a, b) \in S\}.$$

Example 18.9
Given the following two relations from $A = \{1, 2, 4\}$ to $B = \{2, 6, 8, 10\}$:

aRb if and only if $a|b$.
aSb if and only if $b - 4 = a$.

List the elements of $R, S, R \cup S$, and $R \cap S$.

Solution.
We have

$$\begin{aligned} R =& \{(1,2),(1,6),(1,8),(1,10),(2,2),(2,6),(2,8),(2,10),(4,8)\} \\ S =& \{(2,6),(4,8)\} \\ R \cup S =& R \\ R \cap S =& S \end{aligned}$$ ■

Now, if we have a relation R from A to B and a relation S from B to C we can define the relation $S \circ R$, called the **composition** relation, to be the relation from A to C defined by

$$S \circ R = \{(a, c) | (a, b) \in R \text{ and } (b, c) \in S \text{ for some } b \in B\}.$$

Example 18.10
Let

$$\begin{aligned} R =& \{(1,2),(1,6),(2,4),(3,4),(3,6),(3,8)\} \\ S =& \{(2,u),(4,s),(4,t),(6,t),(8,u)\} \end{aligned}$$

Find $S \circ R$.

Solution.

$$S \circ R = \{(1,u),(1,t),(2,s),(2,t),(3,s),(3,t),(3,u)\}$$ ■

We next define four types of binary relations. A relation R on a set A is called **reflexive** if $(a, a) \in R$ for all $a \in A$. In this case, the digraph of R has a loop at each vertex.

Example 18.11
a. Show that the relation $a \leq b$ on the set $A = \{1, 2, 3, 4\}$ is reflexive.
b. Show that the relation on $\mathbb{R}$ defined by aRb if and only if $a < b$ is not reflexive.

Solution.
a. By Example 18.7, each vertex has a loop.
b. Indeed, for any real number a we have $a - a = 0$ and not $a - a < 0$. ■

A relation R on A is called **symmetric** if whenever $(a, b) \in R$ then we must have $(b, a) \in R$. The digraph of a symmetric relation has the property that whenever there is a directed edge from a to b, there is also a directed edge from b to a.

Example 18.12
a. Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, c), (c, b), (d, d)\}$. Show that R is symmetric.
b. Let $\mathbb{R}$ be the set of real numbers and R be the relation aRb if and only if $a < b$. Show that R is not symmetric.

Solution.
a. bRc and cRb so R is symmetric.
b. $2 < 4$ but $4 \not< 2$. ■

A relation R on a set A is called **antisymmetric** if whenever $(a, b) \in R$ and $a \neq b$ then $(b, a) \notin R$. The digraph of an antisymmetric relation has the property that between any two vertices there is at most one directed edge.

Example 18.13
a. Let $\mathbb{N}$ be the set of nonnegative integers and R the relation aRb if and only if a divides b. Show that R is antisymmetric.
b. Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, c), (c, b), (d, d)\}$. Show that R is not antisymmetric.

Solution.
a. Suppose that $a|b$ and $b|a$. We must show that $a = b$. Indeed, by the definition of division, there exist positive integers k_1 and k_2 such that $b = k_1 a$ and $a = k_2 b$. This implies that $a = k_2 k_1 a$ and hence $k_1 k_2 = 1$. Since k_1 and k_2 are positive integers, we must have $k_1 = k_2 = 1$. Hence, $a = b$.

b. bRc and cRb with $b \neq c$. ■

A relation R on a set A is called **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$. The digraph of a transitive relation has the property that whenever there are directed edges from a to b and from b to c then there is also a directed edge from a to c.

Example 18.14
a. Let $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, c), (c, b), (d, d)\}$. Show that R is not transitive.
b. Let $\mathbb{Z}$ be the set of integers and R the relation aRb if a divides b. Show that R is transitive.

Solution.
a. $(b, c) \in R$ and $(c, b) \in R$ but $(b, b) \notin R$.
b. Suppose that $a|b$ and $b|c$. Then there exist integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 b$. Thus, $c = (k_1 k_2)a$ which means that $a|c$. ■

Now, let $A_1, A_2, \cdots, A_n$ be a partition of a set A. That is, the $A_i's$ are subsets of A that satisfy
(i) $\cup_{i=1}^{n} A_i = A$
(ii) $A_i \cap A_j = \emptyset$ for $i \neq j$.
Define on A the binary relation $x\ R\ y$ if and only if x and y belongs to the same set A_i for some $1 \leq i \leq n$.

Theorem 18.1
The relation R defined above is reflexive, symmetric, and transitive.

Proof.
• R is reflexive: If $x \in A$ then by (i) $x \in A_k$ for some $1 \leq k \leq n$. Thus, x and x belong to A_k so that $x\ R\ x$.
• R is symmetric: Let $x, y \in A$ such that $x\ R\ y$. Then there is an index k such that $x, y \in A_k$. But then $y, x \in A_k$. That is, $y\ R\ x$.
• R is transitive: Let $x, y, z \in A$ such that $x\ R\ y$ and $y\ R\ z$. Then there exist indices i and j such that $x, y \in A_i$ and $y, z \in A_j$. Since $y \in A_i \cap A_j$, by (ii) we must have $i = j$. This implies that $x, y, z \in A_i$ and in particular $x, z \in A_i$. Hence, $x\ R\ z$. ■

A relation that is reflexive, symmetric, and transitive on a set A is called an **equivalence relation on A.** For example, the relation "=" is an equivalence relation on $\mathbb{R}$.

Example 18.15
Let $\mathbf{Z}$ be the set of integers and $n \in \mathbf{Z}$. Let R be the relation on $\mathbf{Z}$ defined by aRb if $a - b$ is a multiple of n. We denote this relation by $a \equiv b \ (mod\ n)$ read "a congruent to b modulo n." Show that R is an equivalence relation on $\mathbf{Z}$.

Solution.
$\equiv$ is reflexive: For all $a \in \mathbf{Z}$, $a - a = 0 \cdot n$. That is, $a \equiv a \ (mod\ n)$.
$\equiv$ is symmetric: Let $a, b \in \mathbf{Z}$ such that $a \equiv b \ (mod\ n)$. Then there is an integer k such that $a - b = kn$. Multiply both sides of this equality by (-1) and letting $k' = -k$ we find that $b - a = k'n$. That is $b \equiv a \ (mod\ n)$.
$\equiv$ is transitive: Let $a, b, c \in \mathbf{Z}$ be such that $a \equiv b \ (mod\ n)$ and $b \equiv c \ (mod\ n)$. Then there exist integers k_1 and k_2 such that $a - b = k_1 n$ and $b - c = k_2 n$. Adding these equalities together we find $a - c = kn$ where $k = k_1 + k_2 \in \mathbf{Z}$ which shows that $a \equiv c \ (mod\ n)$. ■

Theorem 18.2
Let R be an equivalence relation on A. For each $a \in A$ let

$$[a] = \{x \in A | xRa\}$$

$$A/R = \{[a] | a \in A\}.$$

Then the union of all the elements of A/R is equal to A and the intersection of any two distinct members of A/R is the empty set. That is, the family A/R forms a partition of A.

Proof.
By the definition of $[a]$ we have that $[a] \subseteq A$. Hence, $\cup_{a \in A}[a] \subseteq A$. We next show that $A \subseteq \cup_{a \in A}[a]$. Indeed, let $a \in A$. Since A is reflexive, $a \in [a]$ and consequently $a \in \cup_{b \in A}[b]$. Hence, $A \subseteq \cup_{b \in A}[b]$. It follows that $A = \cup_{a \in A}[a]$. This establishes (i).
It remains to show that if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$ for $a, b \in A$. Suppose the contrary. That is, suppose $[a] \cap [b] \neq \emptyset$. Then there is an element $c \in [a] \cap [b]$. This means that $c \in [a]$ and $c \in [b]$. Hence, $a \ R \ c$ and $b \ R \ c$. Since R is symmetric and transitive, $a \ R \ b$. We will show that the conclusion $a \ R \ b$ leads to

$[a] = [b]$. The proof is by double inclusions. Let $x \in [a]$. Then $x \ R \ a$. Since $a \ R \ b$ and R is transitive, $x \ R \ b$ which means that $x \in [b]$. Thus, $[a] \subseteq [b]$. Now interchange the letters a and b to show that $[b] \subseteq [a]$. Hence, $[a] = [b]$ which contradicts our assumption that $[a] \neq [b]$. This establishes (ii). Thus, A/R is a partition of A.■

The sets $[a]$ defined in the previous exercise are called the **equivalence classes** of A given by the relation R. The element a in $[a]$ is called a **representative** of the equivalence class $[a]$.

Review Problems

Problem 18.1
Let $X = \{a, b, c\}$. Recall that $\mathcal{P}(X)$ is the power set of X. Define a binary relation $\mathcal{R}$ on $\mathcal{P}(X)$ as follows:

$$A, B \in \mathcal{P}(x),\ A\ \mathcal{R}\ B \Leftrightarrow |A| = |B|.$$

a. Is $\{a, b\}\mathcal{R}\{b, c\}$?
b. Is $\{a\}\mathcal{R}\{a, b\}$?
c. Is $\{c\}\mathcal{R}\{b\}$?

Problem 18.2
Let $\Sigma = \{a, b\}$. Then Σ^4 is the set of all strings over Σ of length 4. Define a relation R on Σ^4 as follows:

$$s, t \in \Sigma^4,\ s\ R\ t \Leftrightarrow \text{ s has the same first two characters as t.}$$

a. Is *abaa* R *abba*?
b. Is *aabb* R *bbaa*?
c. Is *aaaa* R *aaab*?

Problem 18.3
Let $A = \{4, 5, 6\}$ and $B = \{5, 6, 7\}$ and define the binary relations R, S, and T from A to B as follows:

$$(x, y) \in A \times B, (x, y) \in R \Leftrightarrow x \geq y.$$

$$(x, y) \in A \times B, x\ S\ y \Leftrightarrow 2|(x - y).$$

$$T = \{(4, 7), (6, 5), (6, 7)\}.$$

a. Draw arrow diagrams for R, S, and T.
b. Indicate whether any of the relations S, R, or T are functions.

Problem 18.4
Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ and define the binary relation R as follows:

$$(x, y) \in A \times B, (x, y) \in R \Leftrightarrow x < y.$$

List the elements of the sets R and R^{-1}.

Problem 18.5
Let $A = \{2, 4\}$ and $B = \{6, 8, 10\}$ and define the binary relations R and S from A to B as follows:

$$(x, y) \in A \times B, (x, y) \in R \Leftrightarrow x|y.$$

$$(x, y) \in A \times B, x \ S \ y \Leftrightarrow y - 4 = x.$$

List the elements of $A \times B, R, S, R \cup S$, and $R \cap S$.

Problem 18.6
Consider the binary relation on $\mathbb{R}$ defined as follows:

$$x, y \in R, \ x \ R \ y \Leftrightarrow x \geq y.$$

Is R reflexive? symmetric? transitive?

Problem 18.7
Consider the binary relation on $\mathbb{R}$ defined as follows:

$$x, y \in R, \ x \ R \ y \Leftrightarrow xy \geq 0.$$

Is R reflexive? symmetric? transitive?

Problem 18.8
Let $\Sigma = \{0, 1\}$ and $A = \Sigma^*$. Consider the binary relation on A defined as follows:

$$x, y \in A, \ x \ R \ y \Leftrightarrow |x| < |y|,$$

where $|x|$ denotes the length of the string x. Is R reflexive? symmetric? transitive?

Problem 18.9
Let $A \neq \emptyset$ and $\mathcal{P}(A)$ be the power set of A. Consider the binary relation on $\mathcal{P}(A)$ defined as follows:

$$X, Y \in \mathcal{P}(A), \ X \ R \ Y \Leftrightarrow X \subseteq Y.$$

Is R reflexive? symmetric? transitive?

Problem 18.10
Let E be the binary relation on $\mathbf{Z}$ defined as follows:

$$a \; E \; b \Leftrightarrow m \equiv n \; (mod \; 2).$$

Show that E is an equivalence relation on $\mathbf{Z}$ and find the different equivalence classes.

Problem 18.11
Let I be the binary relation on $\mathbb{R}$ defined as follows:

$$a \; I \; b \Leftrightarrow a - b \in \mathbf{Z}.$$

Show that I is an equivalence relation on $\mathbb{R}$ and find the different equivalence classes.

Problem 18.12
Let A be the set all straight lines in the cartesian plane. Let $||$ be the binary relation on A defined as follows:

$$l_1 || l_2 \Leftrightarrow l_1 \text{ is parallel to } l_2.$$

Show that $||$ is an equivalence relation on A and find the different equivalence classes.

Problem 18.13
Let $A = \mathbb{N} \times \mathbb{N}$. Define the binary relation R on A as follows:

$$(a, b) \; R \; (c, d) \Leftrightarrow a + d = b + c.$$

a. Show that R is reflexive.
b. Show that R is symmetric.
c. Show that R is transitive.
d. List five elements in $[(1, 1)]$.
e. List five elements in $[(3, 1)]$.
f. List five elements in $[(1, 2)]$.
g. Describe the distinct equivalence classes of R.

Problem 18.14
Let R be a binary relation on a set A and suppose that R is symmetric and transitive. Prove the following: If for every $x \in A$ there is a $y \in A$ such that $x \; R \; y$ then R is reflexive and hence an equivalence relation on A.

19 Partial Order Relations

A relation $\leq$ on a set A is called **a partial order** if $\leq$ is reflexive, antisymmetric, and transitive. In this case we call A a **poset.**

Example 19.1
Show that the set $\mathbb{Z}$ of integers together with the relation of inequality $\leq$ is a poset.

Solution.
$\leq$ is reflexive: For all $x \in \mathbb{Z}$ we have $x \leq x$ since $x = x$.
$\leq$ is antisymmetric: By the trichotomy law of real numbers, for a given pair of numbers x and y only one of the following is true: $x < y, x = y$, or $x > y$. So if $x \leq y$ and $y \leq x$ then we must have $x = y$.
$\leq$ is transitive: By the transitivity property of $<$ in $\mathbb{R}$ if $x < y$ and $y < z$ then $x < z$. Thus, if $x \leq y$ and $y \leq z$ then the definition of $\leq$ and the above property imply that $x \leq z$. ■

Example 19.2
Show that the relation $a|b$ in $\mathbb{N}^*$ is a partial order relation.

Solution.
Reflexivity: Since $a = 1 \cdot a$, we have $a|a$.
Antisymmetry: Suppose that $a|b$ and $b|a$. Then there exist positive integers k_1 and k_2 such that $b = k_1 a$ and $a = k_2 b$. Hence, $a = k_1 k_2 a$ which implies that $k_1 k_2 = 1$. Since $k_1, k_2 \in \mathbb{N}^*$, we must have $k_1 = k_2 = 1$; that is, $a = b$.
Transitivity: Suppose that $a|b$ and $b|c$. Then there exist positive integers k_1 and k_2 such that $b = k_1 a$ and $c = k_2 b$. Thus, $c = k_1 k_2 a$ which means that $a|c$. ■

Example 19.3
Let $\mathcal{A}$ be a collection of subsets. Let R be the relation defined by

$$A \; R \; B \Leftrightarrow A \subseteq B.$$

Show that $\mathcal{A}$ is a poset.

Solution.
$\subseteq$ is reflexive: For any set $X \in \mathcal{A}$, $X \subseteq X$.

$\subseteq$ is antisymmetric: By the definition of $=$ if $X \subseteq Y$ and $Y \subseteq X$ then $X = Y$, where $X, Y \in \mathcal{A}$.
$\subseteq$ is transitive: We have seen in Chapter 3 that if $X \subseteq Y$ and $Y \subseteq Z$ then $X \subseteq Z$. ■

To figure out which of two words comes first in an English dictionary, one compares their letters one by one from left to right. If all the letters have been the same to a certain point and one word runs out of letters, that word comes first in the dictionary. For example, *play* comes before *playground*. If all the letters up to a certain point are the same and the next letters differ, then the word whose next letter is located earlier in the alphabet comes first in the dictionary. For example, *playground* comes before *playmate*. This type of order relation is called **lexicographic** or **dictionary** order. A general definition is the following:

Let Σ^* be the set of words with letters from an ordered set Σ. Define the relation $\leq$ on Σ^* as follows: for all $w, z \in \Sigma^*, w \leq z$ if and only if either

(a)$z = wu$ for some $u \in \Sigma^*$, or
(b)$w = xu$ and $z = xv$ where $u, v \in \Sigma^*$ such that the first letter of u precedes the first letter of v in the ordering of Σ.
Then it can be shown that $\leq$ is a partial order relation on Σ^*.

Example 19.4
Let $\Sigma = \{a, b\}$ and suppose that Σ has the partial order relation $R = \{(a, a), (a, b), (b, b)\}$. Let $\leq$ be the corresponding lexicographic order on Σ^*. Indicate which of the following statements are true.

a. $aab \leq aaba$.
b. $bbab \leq bba$.
c. $\epsilon \leq aba$.
d. $aba \leq abb$.
e. $bbab \leq bbaa$.
f. $ababa \leq ababaa$.
g. $bbaba \leq bbabb$.

Solution.
a. True since $aaba = (aab)a$.

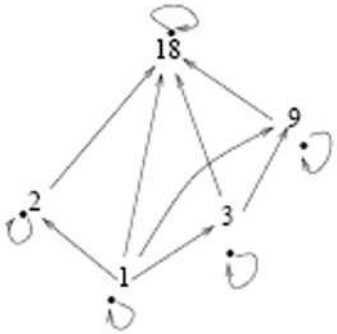
b. False since $bba \leq bbab$.
c. True since $aba = \epsilon aba$.
d. True since $aba = (ab)a, abb = (ab)b$ and $a\ R\ b$.
e. False since $bbaa \leq bbab$.
f. True since $ababaa = (ababa)a$.
g. True since $bbaba = (bbab)a, bbabb = (bbab)b$ and $a\ R\ b$. ■

Another simple pictorial representation of a partial order is the so called **Hasse diagram.** The Hasse diagram of a partial order on the set A is a drawing of the points of A and some of the arrows of the digraph of the order relation. We assume that the directed edges of the Hasse diagram point upward. There are rules to determine which arrows are drawn and which are omitted, namely,

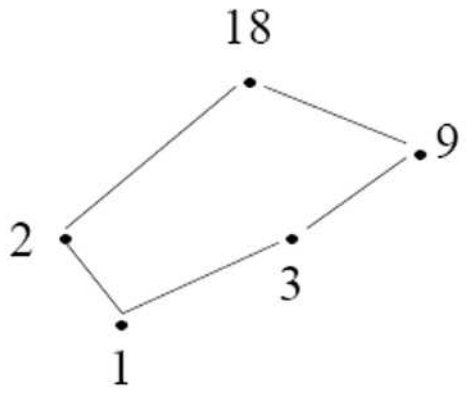
- omit all arrows that can be inferred from transitivity
- omit all loops
- draw arrows without "heads".

Example 19.5
Let $A = \{1, 2, 3, 9, 18\}$ and the "divides" relation on A. Draw the Hasse diagram of this relation.

Solution.
The directed graph of the given relation is



The corresponding Hasse diagram is given by

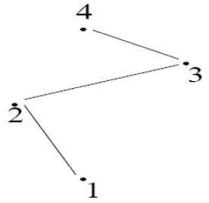


■

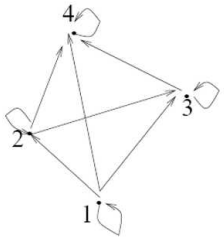
Now, given the Hasse diagram of a partial order relation one can find the digraph as follows:

• reinsert the direction markers on the arrows making all arrows point upward
• add loops at each vertex
• for each sequence of arrows from one point to a second point and from that second point to a third point, add an arrow from the first point to the third.

Example 19.6
Let $A = \{1, 2, 3, 4\}$ be a poset. Find the directed graph corresponding to the following Hasse diagram on A.



Solution.



■

Next, if A is a poset then we say that a and b are **comparable** if either $a \leq b$ or $b \leq a$. If every pair of elements of A are comparable then we call $\leq$ a **total order**.

Example 19.7
Consider the "divides" relation defined on the set $A = \{5, 15, 30\}$. Prove that this relation is a total order on A.

Solution.
The fact that the "divides" relation is a partial order is easy to verify. Since $5|15, 5|30$, and $15|30$, any pair of elements in A are comparable. Thus, the "divides" relation is a total order on A. ■

Example 19.8
Show that the "divides" relation on $\mathbb{N}^*$ is not a total order.

Solution.
A counterexample of two noncomparable numbers are 2 and 3, since 2 does not divide 3 and 3 does not divide 2. ■

Review Problems

Problem 19.1
Let $\Sigma = \{a, b\}$ and let Σ^* be the set of all strings over Σ. Define the relation R on Σ^* as follows: for all $s, t \in \Sigma^*$,

$$s \; R \; t \Leftrightarrow l(s) \leq l(t),$$

where $l(x)$ denotes the length of the word x. Is R antisymmetric? Prove or give a counterexample.

Problem 19.2
Define a relation R on $\mathbf{Z}$ as follows: for all $m, n \in \mathbf{Z}$

$$m \; R \; n \Leftrightarrow m + n \; is \; even.$$

Is R a partial order? Prove or give a counterexample.

Problem 19.3
Define a relation R on $\mathbb{R}$ as follows: for all $m, n \in \mathbb{R}$

$$m \; R \; n \Leftrightarrow m^2 \leq n^2.$$

Is R a partial order? Prove or give a counterexample.

Problem 19.4
Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S$ as follows: for all ordered pairs (a, b) and (c, d) in $S \times S$

$$(a, b) \; R \; (c, d) \Leftrightarrow a \leq c \; and \; b \leq d.$$

Draw the Hasse diagram for R.

Problem 19.5
Consider the "divides" relation defined on the set $A = \{1, 2, 2^2, \cdots, 2^n\}$, where n is a nonnegative integer.
a. Prove that this relation is a total order on A.
b. Draw the Hasse diagram for this relation when $n = 3$.

20 Functions: Definitions and Examples

A function is a special case of a relation. A **function** f from a set A to a set B is a relation from A to B such that for every $x \in A$ there is a unique $y \in B$ such that $(x, y) \in f$. For $(x, y) \in f$ we use the notation $y = f(x)$. We call y the **image** of x under f. The set A is called the **domain** of f whereas B is called the **codomain**. The collection of all images of f is called the **range** of f.

Example 20.1
Show that the relation $f = \{(1, a), (2, b), (3, a)\}$ defines a function from $A = \{1, 2, 3\}$ to $B = \{a, b, c\}$. Find its range.

Solution.
Since every element of A has a unique image, f is a function. Its range consists of the elements a and b. ■

Example 20.2
Show that the relation $f = \{(1, a), (2, b), (3, c), (1, b)\}$ does not define a function from $A = \{1, 2, 3\}$ to $B = \{a, b, c\}$.

Solution.
Indeed, since 1 has two images in B, f is not a function. ■

Example 20.3
A **sequence** of elements of a set A is a function from $\mathbb{N}^*$ to A. We write (a_n) and we call a_n the nth term of the sequence.
a. Define the sequence $a_n = n, n \geq 1$. Compute $\sum_{k=1}^{n} a_k$.
b. Define the sequence $a_n = n^2$. Compute the sum $\sum_{k=1}^{n} a_k$.

Solution.
a. Let $S_n = \sum_{k=1}^{n} a_k$. Then write S_n in two different ways, namely, $S_n = 1 + 2 + \cdots + n$ and $S_n = n + (n-1) + \cdots + 1$. Adding, we obtain $2S_n = (n+1) + (n+1) + \cdots + (n+1) = n(n+1)$. Thus, $S_n = \frac{n(n+1)}{2}$.
b. First note that $(n+1)^3 - n^3 = 3n^2 + 3n + 1$. From this we obtain the following chain of equalities:

$$\begin{array}{rcrcrcrcr}
2^3 & - & 1^3 & = & 3(1)^2 & + & 3(1) & + & 1 \\
3^3 & - & 2^3 & = & 3(2)^2 & + & 3(2) & + & 1 \\
\vdots & & & & & & & & \\
(n+1)^3 & - & n^3 & = & 3n^2 & + & 3n & + & 1
\end{array}$$

Adding these equalities we find

$$3\sum_{k=1}^{n} k^2 + 3\sum_{k=1}^{n} k + n = (n+1)^3 - 1.$$

Using a. we find

$$3\sum_{k=1}^{n} k^2 + \frac{3n(n+1)}{2} + n = n^3 + 3n^2 + 3n.$$

Simple arithmetic shows that

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.\blacksquare$$

Example 20.4
Let $A = \{a, b, c\}$. Define the function $f : \mathcal{P}(A) \to \mathbb{N}$ by $f(X) = |X|$. Find the range of f.

Solution.
By applying f to each member of $\mathcal{P}(A)$ we find $Range(f) = \{0, 1, 2, 3\}$. ■

Example 20.5
Consider the alphabet $\Sigma = \{a, b\}$ and the function $f : \Sigma^* \to \mathbf{Z}$ defined as follows: for any string $s \in \Sigma^*$

$$f(s) = the\ number\ of\ a's\ in\ s.$$

Find $f(\epsilon), f(ababb)$, and $f(bbbaa)$.

Solution.
$f(\epsilon) = 0, f(ababb) = 2$, and $f(bbbaa) = 2$. ■

Example 20.6 *(Equality of Functions)*
Two functions f and g defined on the same domain D are said to be **equal** if and only if $f(x) = g(x)$ for all $x \in D$. Show that the functions $f, g : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = |x|$ and $g(x) = \sqrt{x^2}$ are equal.

Solution.
A simple argument by the method of proof by cases shows that $\sqrt{x^2} = |x|$. ■

Example 20.7 *(Hamming distance function)*
Let $\Sigma = \{0, 1\}$ and Σ^n be the set of all strings of 0's and 1's of length n. Define the function $H : \Sigma^n \times \Sigma^n \to \mathbb{N}$ as follows: for any $(s, t) \in \Sigma^n \times \Sigma^n$

$$H(s, t) = \textit{number of positions in which } s \textit{ and } t \textit{ have different values.}$$

For the case $n = 5$, find $H(00101, 01110)$ and $H(10001, 01111)$.

Solution.
$H(00101, 01110) = 3$ and $H(10001, 01111) = 4$. ■

Example 20.8 *(Boolean functions)*
An **n-place Boolean function** f is a function from the Cartesian product $\{0, 1\}^n$ to $\{0, 1\}$. Consider the 3-place Boolean function $f : \{0, 1\}^3 \to \{0, 1\}$ defined by

$$f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \ mod \ 2.$$

Describe f using an input/output table.

Solution.

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

■

Example 20.9 *(Encoding and Decoding functions)*
Let $\Sigma = \{0, 1\}$ and Σ^* be the set of all strings of 0's and 1's. Let L be the set of all strings over Σ that consist of consecutive triples of identical bits. Thus, $111000 \in L$. A message consisting of 0's and 1's is encoded by writing each bit in it three times. The encoded message is decoded by replacing each section of three identical bits by the one bit to which all three are equal.
We define the encoding function $E : \Sigma^* \to L$ by

$$E(s) = \textit{the string obtained from } s \textit{ by replacing each bit of } s \textit{ by the same bit written three times}$$

and we define the decoding function $D : L \to \Sigma^*$ by

$$D(s) \quad = \textit{the string obtained from } s \textit{ by replacing consecutive triple of bits of } s \textit{ by a single copy of that bit.}$$

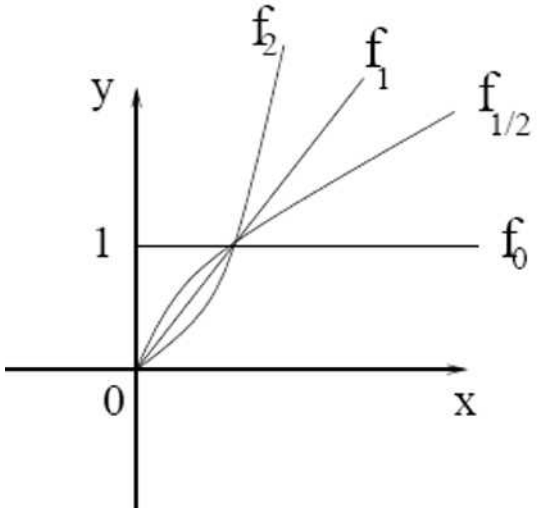
Find $E(0110)$ and $D(111111000111)$.

Solution.
We have $E(0110) = 000111111000$ and $D(111111000111) = 1101$. ■

Now, let A and B be subsets of $\mathbb{R}$. A function $f : A \to B$ is called a **real-valued function of a real variable.** In this case, each ordered pair $(x, f(x))$ can be represented by a point in the Cartesian plane. The collection of all such points is called the **graph** of f.

Example 20.10
Consider the power function $f_a(x) = x^a$, where $a, x \in \mathbb{R}^+ \cup \{0\}$. Graph on the same Cartesian plane the functions $f_0(x), f_1(x), f_{\frac{1}{2}}(x)$, and $f_2(x)$.

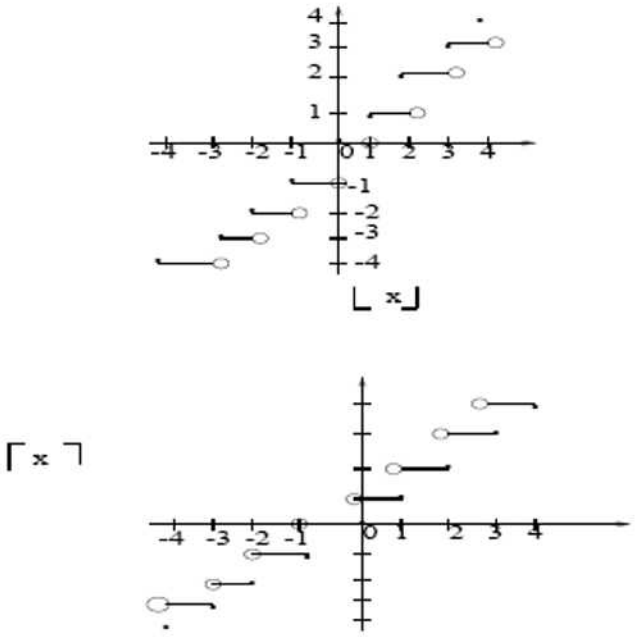
Solution.



■

Example 20.11
Graph the functions $f(x) = \lfloor x \rfloor$ and $g(x) = \lceil x \rceil$ on the closed interval $[-4, 4]$.

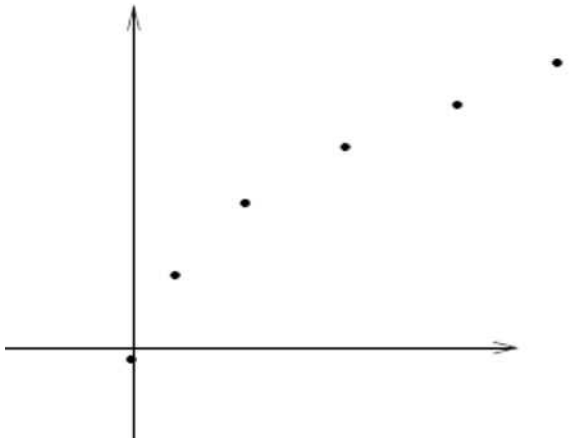
Solution.



■

Example 20.12
Graph the function $f : \mathbb{N} \to \mathbb{R}$ defined by $f(n) = \sqrt{n}$.

Solution.



■

Example 20.13
Let D_f be the domain of a function f and $S \subseteq D_f$. We say that f is **increasing** on S if and only if, for all $x_1, x_2 \in S$, if $x_1 < x_2$ then $f(x_1) < f(x_2)$. Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x - 3$ is increasing on $\mathbb{R}$.

Solution.
Indeed, for any real numbers x_1 and x_2 such that $x_1 < x_2$, we have $2x_1 - 3 < 2x_2 - 3$. That is, $f(x_1) < f(x_2)$ so that f is increasing. ■

Example 20.14
Let D_f be the domain of a function f and $S \subseteq D_f$. We say that f is **decreasing** on S if and only if, for all $x_1, x_2 \in S$, if $x_1 < x_2$ then $f(x_1) > f(x_2)$. Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \frac{x+2}{x+1}$ is decreasing on $(-\infty, -1)$ and $(-1, \infty)$.

Solution.
Indeed, for any real numbers $x_1, x_2 \in (-\infty, -1)$ or $x_1, x_2 \in (-1, \infty)$ such that $x_1 < x_2$, we have $(x_1 + 1)(x_2 + 1) > 0$. This implies, that $f(x_1) - f(x_2) = \frac{x_2 - x_1}{(x_1+1)(x_2+1)} > 0$. Thus, f is decreasing on the given intervals. ■

Review Problems

Problem 20.1
Let $f, g : \mathbb{R} \to \mathbb{R}$ be the functions $f(x) = 2x$ and $g(x) = \frac{2x^3+2x}{x^2+1}$. Show that $f = g$.

Problem 20.2
Let $H, K : \mathbb{R} \to \mathbb{R}$ be the functions $H(x) = \lfloor x \rfloor + 1$ and $K(x) = \lceil x \rceil$. Does $H = K$? Explain.

Problem 20.3
Find functions defined on the set of nonnegative integers that define the sequences whose first six terms are given below.
a. $1, -\frac{1}{3}, \frac{1}{5}, -\frac{1}{7}, \frac{1}{9}, -\frac{1}{11}$.
b. $0, -2, 4, -6, 8, -10$.

Problem 20.4
Let $A = \{1, 2, 3, 4, 5\}$ and let $F : \mathcal{P}(A) \to \mathbb{Z}$ be defined as follows:

$$F(X) = \begin{cases} 0 & \textit{if } X \textit{ has an even number of elements} \\ 1 & \textit{if } X \textit{ has an odd number of elements} \end{cases}$$

Find the following

a. $F(\{1, 3, 4\})$
b. $F(\emptyset)$.
c. $F(\{2, 3\})$.
d. $F(\{2, 3, 4, 5\})$.

Problem 20.5
Let $\Sigma = \{a, b\}$ and Σ^* be the set of all strings over Σ.
a. Define $f : \Sigma^* \to \mathbb{Z}$ as follows:

$$f(s) = \begin{cases} \textit{the number of } b\textit{'s to the left of the leftmost } a \textit{ in } s \\ 0 \quad \textit{if } s \textit{ contains no } a\textit{'s} \end{cases}$$

Find $f(aba), f(bbab)$, and $f(b)$. What is the range of f?
b. Define $g : \Sigma^* \to \Sigma^*$ as follows:

$g(s) =$ *the string obtained by writing the characters of* s *in reverse order.*

Find $g(aba), g(bbab)$, and $g(b)$. What is the range of g?

Problem 20.6
Let E and D be the encoding and decoding functions.
a. Find $E(0110)$ and $D(111111000111)$.
b. Find $E(1010)$ and $D(000000111111)$.

Problem 20.7
Let H denote the Hamming distance function on Σ^5.
a. Find $H(10101, 00011)$.
b. Find $H(00110, 10111)$.

Problem 20.8
Consider the three-place Boolean function $f : \{0,1\}^3 \to \{0,1\}$ defined as follows:

$$f(x_1, x_2, x_3) = (3x_1 + x_2 + 2x_3) \ mod \ 2$$

a. Find $f(1,1,1)$ and $f(0,1,1)$.
b. Describe f using an input/output table.

Problem 20.9
Draw the graphs of the power functions $f_{\frac{1}{3}}(x)$ and $f_{\frac{1}{4}}(x)$ on the same set of axes. When, $0 < x < 1$, which is greater: $x^{\frac{1}{3}}$ or $x^{\frac{1}{4}}$? When $x > 1$, which is greater $x^{\frac{1}{3}}$ or $x^{\frac{1}{4}}$?

Problem 20.10
Graph the function $f(x) = \lceil x \rceil - \lfloor x \rfloor$ on the interval $(-\infty, \infty)$.

Problem 20.11
Graph the function $f(x) = x - \lfloor x \rfloor$ on the interval $(-\infty, \infty)$.

Problem 20.12
Graph the function $h : \mathbb{N} \to \mathbb{R}$ defined by $h(n) = \lfloor \frac{n}{2} \rfloor$.

Problem 20.13
Let $k : \mathbb{R} \to \mathbb{R}$ be the function defined by the formula $k(x) = \frac{x-1}{x}$ for all nonzero real numbers x.
a. Show that k is increasing on $(0, \infty)$.
b. Is k increasing or decreasing on $(-\infty, 0)$? Prove your answer.

21 Bijective and Inverse Functions

Let $f : A \to B$ be a function. We say that f is **injective** or **one-to-one** if and only if for all $x, y \in A$, if $f(x) = f(y)$ then $x = y$. Using the concept of contrapositive, a function f is injective if and only if for all $x, y \in A$, if $x \neq y$ then $f(x) \neq f(y)$. Taking the negation of this last conditional implication we see that f is not injective if and only if there exist two distinct elements a and b of A such that $f(a) = f(b)$.

Example 21.1
a. Show that the identity function I_A on a set A is injective.
b. Show that the function $f : \mathbf{Z} \to \mathbf{Z}$ defined by $f(n) = n^2$ is not injective.

Solution.
a. Let $x, y \in A$. If $I_A(x) = I_A(y)$ then $x = y$ by the definition of I_A. This shows that I_A is injective.
b. Since $1^2 = (-1)^2$ and $1 \neq -1$, f is not injective.■

Example 21.2 *(Hash Functions)*
Let $m > 1$ be a positive integer . Show that the function $h : \mathbf{Z} \to \mathbf{Z}$ defined by $h(n) = n \ mod \ m$ is not injective.

Solution.
Indeed, since $m > 1$, we have $2m+1 \neq m+1$ and $h(m+1) = h(2m+1) = 1$. So h is not injective. ■

Example 21.3
Show that if $f : \mathbb{R} \to \mathbb{R}$ is increasing then f is one-to-one.

Solution.
Suppose that $x_1 \neq x_2$. Then without loss of generality we can assume that $x_1 < x_2$. Since f is increasing, $f(x_1) < f(x_2)$. That is, $f(x_1) \neq f(x_2)$. Hence, f is one-to-one. ■

Example 21.4
Show that the composition of two injective functions is also injective.

Solution.
Let $f : A \to B$ and $g : B \to C$ be two injective functions. We will show that $g \circ f : A \to C$ is also injective. Indeed, suppose that $(g \circ f)(x_1) = (g \circ f)(x_2)$

for $x_1, x_2 \in A$. Then $g(f(x_1)) = g(f(x_2))$. Since g is injective, $f(x_1) = f(x_2)$. Now, since f is injective, $x_1 = x_2$. This completes the proof that $g \circ f$ is injective. ■

Now, for any function $f : A \to B$ we have $Range(f) \subseteq B$. If equality holds then we say that f is **surjective** or **onto.** It follows from this definition that a function f is surjective if and only if for each $y \in B$ there is an $x \in A$ such that $f(x) = y$. By taking the negation of this we see that f is not onto if there is a $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

Example 21.5
a. Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x - 5$ is surjective.
b. Show that the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 3n - 5$ is not surjective.

Solution.
a. Let $y \in \mathbb{R}$. Is there an $x \in \mathbb{R}$ such that $f(x) = y$? That is, $3x - 5 = y$. But solving for x we find $x = \frac{y+5}{3} \in \mathbb{R}$ and $f(x) = y$. Thus, f is onto.
b. Take $m = 3$. If f is onto then there should be an $n \in \mathbb{Z}$ such that $f(n) = 3$. That is, $3n - 5 = 3$. Solving for n we find $n = \frac{8}{3}$ which is not an integer. Hence, f is not onto. ■

Example 21.6 *(Projection Functions)*
Let A and B be two nonempty sets. The functions $pr_A : A \times B \to A$ defined by $pr_A(a, b) = a$ and $pr_B : A \times B \to B$ defined by $pr_B(a, b) = b$ are called **projection** functions. Show that pr_A and pr_B are surjective functions.

Solution.
We prove that pr_A is surjective. Indeed, let $a \in A$. Since B is not empty, there is a $b \in B$. But then $(a, b) \in A \times B$ and $pr_A(a, b) = a$. Hence, pr_A is surjective. The proof that pr_B is surjective is similar. ■

Example 21.7
Show that the composition of two surjective functions is also surjective.

Solution.
Let $f : A \to B$ and $g : B \to C$, where $Range(f) \subseteq C$, be two surjective functions. We will show that $g \circ f : A \to D$ is also surjective. Indeed, let $z \in D$. Since g is surjective, there is a $y \in B$ such that $g(y) = z$. Since f is

surjective, then there is an $x \in A$ such that $f(x) = y$. Thus, $g(f(x)) = z$. This shows that $g \circ f$ is surjective. ■

Now, we say that a function f is **bijective** or **one-to-one correspondence** if and only if f is both injective and surjective. A bijective function on a set A is called a **permutation.**

Example 21.8
a. Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x - 5$ is a bijective function.
b. Show that the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not bijective.

Solution.
a. First we show that f is injective. Indeed, suppose that $f(x_1) = f(x_2)$. Then $3x_1 - 5 = 3x_2 - 5$ and this implies that $x_1 = x_2$. Hence, f is injective. f is surjective by Example 21.5 (a).
b. f is not injective since $f(-1) = f(1)$ but $-1 \neq 1$. Hence, f is not bijective.
■

Example 21.9
Show that the composition of two bijective functions is also bijective.

Solution.
This follows from Example 21.4 and Example 21.7 ■

Theorem 21.1
Let $f : X \to Y$ be a bijective function. Then there is a function $f^{-1} : Y \to X$ with the following properties:

a. $f^{-1}(y) = x$ if and only if $f(x) = y$.
b. $f^{-1} \circ f = I_X$ and $f \circ f^{-1} = I_Y$ where I_X denotes the identity function on X.
c. f^{-1} is bijective.

Proof.
For each $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$ since f is bijective. Thus, we can define a function $f^{-1} : Y \to X$ by $f^{-1}(y) = x$ where $f(x) = y$.
a. Follows from the definition of f^{-1}.

b. Indeed, let $x \in X$ such that $f(x) = y$. Then $f^{-1}(y) = x$ and $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I_X(x)$. Since x was arbitrary, $f^{-1} \circ f = I_X$. The proof that $f \circ f^{-1} = I_Y$ is similar.
c. We show first that f^{-1} is injective. Indeed, suppose $f^{-1}(y_1) = f^{-1}(y_2)$. Then $f(f^{-1}(y_1)) = f(f^{-1}(y_2))$; that is, $(f \circ f^{-1})(y_1) = (f \circ f^{-1})(y_2)$. By b. we have $I_Y(y_1) = I_Y(y_2)$. From the definition of I_Y we obtain $y_1 = y_2$. Hence, f^{-1} is injective. We next show that f^{-1} is surjective. Indeed, let $y \in Y$. Since f is onto there is a unique $x \in X$ such that $f(x) = y$. By the definition of f^{-1}, $f^{-1}(y) = x$. Thus, for every element $y \in Y$ there is an element $x \in X$ such that $f^{-1}(y) = x$. This says that f^{-1} is surjective and completes a proof of the theorem ■

Example 21.10
Show that $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x - 5$ is bijective and find a formula for its inverse function.

Solution.
We have already proved that f is bijective. We will just find the formula for its inverse function f^{-1}. Indeed, if $y \in Y$ we want to find $x \in X$ such that $f^{-1}(y) = x$, or equivalently, $f(x) = y$. This implies that $3x - 5 = y$ and solving for x we find $x = \frac{y+5}{3}$. Thus, $f^{-1}(y) = \frac{y+5}{3}$ ■

Review Problems

Problem 21.1
a. Define $g : \mathbf{Z} \to \mathbf{Z}$ by $g(n) = 3n - 2$.
(i) Is g one-to-one? Prove or give a counterexample.
(ii) Is g onto? Prove or give a counterexample.
b. Define $G : \mathbb{R} \to \mathbb{R}$ by $G(x) = 3x - 2$. Is G onto? Prove or give a counterexample.

Problem 21.2
Determine whether the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \frac{x+1}{x}$ is one-to-one or not.

Problem 21.3
Determine whether the function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = \frac{x}{x^2+1}$ is one-to-one or not.

Problem 21.4
Let $f : \mathbb{R} \to \mathbf{Z}$ be the floor function $f(x) = \lfloor x \rfloor$.
a. Is f one-to-one? Prove or give a counterexample.
b. Is f onto? Prove or give a counterexample.

Problem 21.5
Let $\Sigma = \{0, 1\}$ and let $l : \Sigma^* \to \mathbb{N}$ denote the length function.
a. Is l one-to-one? Prove or give a counterexample.
b. Is l onto? Prove or give a counterexample.

Problem 21.6
If $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ are one-to-one functions, is $f + g$ also one-to-one? Justify your answer.

Problem 21.7
Define $F : \mathcal{P}\{a, b, c\} \to \mathbb{N}$ to be the number of elements of a subset of $\mathcal{P}\{a, b, c\}$.
a. Is F one-to-one? Prove or give a counterexample.
b. Is F onto? Prove or give a counterexample.

Problem 21.8
If $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ are onto functions, is $f + g$ also onto? Justify your answer.

Problem 21.9
Let $\Sigma = \{a, b\}$ and let $l : \Sigma^* \to \mathbb{N}$ be the length function. Let $f : \mathbb{N} \to \{0, 1, 2\}$ be the hash function $f(n) = n \, mod \, 3$. Find $(f \circ l)(abaa)$, $(f \circ l)(baaab)$, and $(f \circ l)(aaa)$.

Problem 21.10
Show that the function $F^{-1} : \mathbb{R} \to \mathbb{R}$ given by $F^{-1}(y) = \frac{y-2}{3}$ is the inverse of the function $F(x) = 3x + 2$.

Problem 21.11
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is one-to-one, must both f and g be one-to-one? Prove or give a counterexample.

Problem 21.12
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is onto, must both f and g be onto? Prove or give a counterexample.

Problem 21.13
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is one-to-one, must f be one-to-one? Prove or give a counterexample.

Problem 21.14
If $f : X \to Y$ and $g : Y \to Z$ are functions and $g \circ f : X \to Z$ is onto, must g be onto? Prove or give a counterexample.

Problem 21.15
Let $f : W \to X, g : X \to Y$ and $h : Y \to Z$ be functions. Must $h \circ (g \circ f) = (h \circ g) \circ f$? Prove or give a counterexample.

Problem 21.16
Let $f : X \to Y$ and $g : Y \to Z$ be two bijective functions. Show that $(g \circ f)^{-1}$ exists and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

22 Recursion

A **recurrence relation** for a sequence $a_0, a_1, \cdots$ is a relation that defines a_n in terms of $a_0, a_1, \cdots, a_{n-1}$. The formula relating a_n to earlier values in the sequence is called the **generating rule**. The assignment of a value to one of the a's is called an **initial condition.**

Example 22.1
The Fibonacci sequence

$$1, 1, 2, 3, 5, \cdots$$

is a sequence in which every number after the first two is the sum of the preceding two numbers. Find the generating rule and the initial conditions.

Solution.
The initial conditions are $a_0 = a_1 = 1$ and the generating rule is $a_n = a_{n-1} + a_{n-2}, n \geq 2$. ■

Example 22.2
Let $n \geq 0$ and find the number s_n of words from the alphabet $\Sigma = \{0, 1\}$ of length n not containing the pattern 11 as a subword.

Solution.
Clearly, $s_0 = 1$(empty word) and $s_1 = 2$. We will find a recurrence relation for $s_n, n \geq 2$. Any word of length n with letters from Σ begins with either 0 or 1. If the word begins with 0, then the remaining $n-1$ letters can be any sequence of 0's or 1's except that 11 cannot happen. If the word begins with 1 then the next letter must be 0 since 11 can not happen; the remaining $n-2$ letters can be any sequence of 0's and 1's with the exception that 11 is not allowed. Thus the above two categories form a partition of the set of all words of length n with letters from Σ and that do not contain 11. This implies the recurrence relation

$$s_n = s_{n-1} + s_{n-2}, \quad n \geq 2$$■

A **solution** to a recurrence relation is an explicit formula for a_n in terms of n.
The most basic method for finding the solution of a sequence defined recursively is by using **iteration.** The iteration method consists of starting with the initial values of the sequence and then calculate successive terms of the

sequence until a pattern is observed. At that point one guesses an explicit formula for the sequence and then uses mathematical induction to prove its validity.

Example 22.3
Find a solution for the recurrence relation

$$\begin{aligned} a_0 &= 1 \\ a_n &= a_{n-1} + 2, \quad n \geq 1 \end{aligned}$$

Solution.
Listing the first five terms of the sequence one finds

$$\begin{aligned} a_0 &= 1 \\ a_1 &= 1 + 2 \\ a_2 &= 1 + 4 \\ a_3 &= 1 + 6 \\ a_4 &= 1 + 8 \end{aligned}$$

Hence, a guess is $a_n = 2n + 1, n \geq 0$. It remains to show that this formula is valid by using mathematical induction.

Basis of induction: For $n = 0, a_0 = 1 = 2(0) + 1$.
Induction hypothesis: Suppose that $a_n = 2n + 1$.
Induction step: We must show that $a_{n+1} = 2(n+1) + 1$. By the definition of a_{n+1} we have $a_{n+1} = a_n + 2 = 2n + 1 + 2 = 2(n + 1) + 1$. ■

Example 22.4
Consider the arithmetic sequence

$$a_n = a_{n-1} + d, \quad n \geq 1$$

where a_0 is the initial value. Find an explicit formula for a_n.

Solution. Listing the first four terms of the sequence after a_0 we find

$$\begin{aligned} a_1 &= a_0 + d \\ a_2 &= a_0 + 2d \\ a_3 &= a_0 + 3d \\ a_4 &= a_0 + 4d \end{aligned}$$

Hence, a guess is $a_n = a_0 + nd$. Next, we prove the validity of this formula by induction.

Basis of induction: For $n = 0, a_0 = a_0 + (0)d$.
Induction hypothesis: Suppose that $a_n = a_0 + nd$.
Induction step: We must show that $a_{n+1} = a_0 + (n+1)d$. By the definition of a_{n+1} we have $a_{n+1} = a_n + d = a_0 + nd + d = a_0 + (n+1)d$. ■

Example 22.5
Consider the geometric sequence

$$a_n = ra_{n-1}, \quad n \geq 1$$

where a_0 is the initial value. Find an explicit formula for a_n.

Solution.
Listing the first four terms of the sequence after a_0 we find

$$\begin{aligned} a_1 &= ra_0 \\ a_2 &= r^2 a_0 \\ a_3 &= r^3 a_0 \\ a_4 &= r^4 a_0 \end{aligned}$$

Hence, a guess is $a_n = r^n a_0$. Next, we prove the validity of this formula by induction.

Basis of induction: For $n = 0, a_0 = r^0 a_0$.
Induction hypothesis: Suppose that $a_n = r^n a_0$.
Induction step: We must show that $a_{n+1} = r^{n+1} a_0$. By the definition of a_{n+1} we have $a_{n+1} = ra_n = r(r^n a_0) = r^{n+1} a_0$. ■

Example 22.6
Find a solution to the recurrence relation

$$\begin{aligned} a_0 &= 0 \\ a_n &= a_{n-1} + (n-1), \quad n \geq 1 \end{aligned}$$

Solution.
Writing the first five terms of the sequence we find

$$\begin{aligned} a_0 =& 0 \\ a_1 =& 0 \\ a_2 =& 0+1 \\ a_3 =& 0+1+2 \\ a_4 =& 0+1+2+3 \end{aligned}$$

We guess that

$$a_n = 0+1+2+\cdots+(n-1) = \frac{n(n-1)}{2}.$$

We next show that the formula is valid by using induction on $n \geq 0$.

Basis of induction: $a_0 = 0 = \frac{0(0-1)}{2}$.
Induction hypothesis: Suppose that $a_n = \frac{n(n-1)}{2}$.
Induction step: We must show that $a_{n+1} = \frac{n(n+1)}{2}$. Indeed,

$$\begin{aligned} a_{n+1} =& a_n + n \\ =& \frac{n(n-1)}{2} + n \\ =& \frac{n(n+1)}{2} \ \blacksquare \end{aligned}$$

Example 22.7
Consider the recurrence relation

$$\begin{aligned} a_0 =& 1 \\ a_n =& 2a_{n-1} + n, \ n \geq 1 \end{aligned}$$

Is it true that $a_n = 2^n + n$ is a solution to the given recurrence relation?

Solution.
This is false since $a_2 = 2a_1 + 2 = 2(2a_0 + 1) + 2 = 8 \neq 2^2 + 2$ ■

Example 22.8
Define a sequence, $a_1, a_2, \cdots$, recursively as follows:

$$\begin{aligned} a_1 =& 1 \\ a_n =& 2 \cdot a_{\lfloor \frac{n}{2} \rfloor}, \quad n \geq 2 \end{aligned}$$

a. Use iteration to guess an explicit formula for this sequence.
b. Use induction to prove the validity of the formula found in a.

Solution.
Computing the first few terms of the sequence we find

$$\begin{aligned} a_1 =& 1 \\ a_2 =& 2 \\ a_3 =& 2 \\ a_4 =& 4 \\ a_5 =& 4 \\ a_6 =& 4 \\ a_7 =& 4 \\ a_8 =& \cdots = a_{15} = 8 \end{aligned}$$

Hence, for $2^i \leq n < 2^{i+1}, a_n = 2^i$. Moreover, $i \leq \log_2 n < i+1$ so that $i = \lfloor \log_2 n \rfloor$ and a formula for a_n is

$$a_n = 2^{\lfloor \log_2 n \rfloor}, \ n \geq 1.$$

b. We prove the above formula by mathematical induction.

Basis of induction: For $n = 1$, $a_1 = 1 = 2^{\lfloor \log_2 1 \rfloor}$.
Induction hypothesis: Suppose that $a_n = 2^{\lfloor \log_2 n \rfloor}$.
Induction step: We must show that $a_{n+1} = 2^{\lfloor \log_2 (n+1) \rfloor}$. Indeed, for n odd (i.e. $n+1$ even) we have

$$\begin{aligned} a_{n+1} =& 2 \cdot a_{\lfloor \frac{n+1}{2} \rfloor} \\ =& 2 \cdot a_{\frac{n+1}{2}} \\ =& 2 \cdot 2^{\lfloor \log_2 \frac{n+1}{2} \rfloor} \\ =& 2^{\lfloor \log_2 (n+1) - 1 \rfloor + 1} \\ =& 2^{\lfloor \log_2 (n+1) \rfloor - 1 + 1} \\ =& 2^{\lfloor \log_2 (n+1) \rfloor} \end{aligned}$$

A similar argument holds when n is even. ■

When iteration does not apply, other methods are available for finding explicit formulas for special classes of recursively defined sequences. The method explained below works for sequences of the form

$$a_n = Aa_{n-1} + Ba_{n-2} \tag{22.1}$$

where n is greater than or equal to some fixed nonnegative integer k and A and B are real numbers with $B \neq 0$. Such an equation is called a **second-order linear homogeneous recurrence relation with constant coefficients**.

Example 22.9
Does the Fibonacci sequence satisfy a second-order linear homogeneous relation with constant coefficients?

Solution.
Recall that the Fibonacci sequence is defined recursively by $a_n = a_{n-1} + a_{n-2}$ for $n \geq 2$ and $a_0 = a_1 = 1$. Thus, a_n satisfies a second-order linear homogeneous relation with $A = B = 1$ ■

The following theorem gives a technique for finding solutions to (22.1).

Theorem 22.1
Equation (22.1) is satisfied by the sequence $1, t, t^2, \cdots, t^n, \cdots$ where $t \neq 0$ if and only if t is a solution to the **characteristic equation**

$$t^2 - At - B = 0 \tag{22.2}$$

Proof.
($\Longrightarrow$): Suppose that t is a nonzero real number such that the sequence $1, t, t^2, \cdots$ satisfies (22.1). We will show that t satisfies the equation $t^2 - At - B = 0$. Indeed, for $n \geq k$ we have

$$t^n = At^{n-1} + Bt^{n-2}.$$

Since $t \neq 0$ we can divide through by t^{n-2} and obtain $t^2 - At - B = 0$.
($\Longleftarrow$) : Suppose that t is a nonzero real number such that $t^2 - At - B = 0$. Multiply both sides of this equation by t^{n-2} to obtain

$$t^n = At^{n-1} + Bt^{n-2}.$$

This says that the sequence $1, t, t^2, \cdots$ satisfies (22.1) ■

Example 22.10
Consider the recurrence relation

$$a_n = a_{n-1} + 2a_{n-2}, \quad n \geq 2.$$

Find two sequences that satisfy the given generating rule and have the form $1, t, t^2, \cdots$.

Solution.
According to the previous theorem t must satisfy the characteristic equation

$$t^2 - t - 2 = 0.$$

Solving for t we find $t = 2$ or $t = -1$. So the two solutions to the given recurrence sequence are $1, 2, 2^2, \cdots, 2^n, \cdots$ and $1, -1, \cdots, (-1)^n, \cdots$ ■

Are there other solutions than the ones provided by Theorem 22.1? The answer is yes according to the following theorem.

Theorem 22.2
If s_n and t_n are solutions to (22.1) then for any real numbers C and D the sequence

$$a_n = Cs_n + Dt_n, \quad n \geq 0$$

is also a solution.

Proof.
Since s_n and t_n are solutions to (22.1), for $n \geq 2$ we have

$$\begin{aligned} s_n =& As_{n-1} + Bs_{n-2} \\ t_n =& At_{n-1} + Bt_{n-2} \end{aligned}$$

Therefore,

$$\begin{aligned} Aa_{n-1} + Ba_{n-2} =& A(Cs_{n-1} + Dt_{n-1}) + B(Cs_{n-2} + Dt_{n-2}) \\ =& C(As_{n-1} + Bs_{n-2}) + D(At_{n-1} + Bt_{n-2}) \\ =& Cs_n + Dt_n = a_n \end{aligned}$$

so that a_n satisfies (22.1) ■

Example 22.11
Find a solution to the recurrence relation

$$\begin{aligned} a_0 =& 1, a_1 = 8 \\ a_n =& a_{n-1} + 2a_{n-2}, \quad n \geq 2. \end{aligned}$$

Solution.
By the previous theorem and Example 22.10, $a_n = C2^n + D(-1)^n,\ n \geq 2$ is a solution to the recurrence relation

$$a_n = a_{n-1} + 2a_{n-2}.$$

If a_n satisfies the system then we must have

$$\begin{aligned} a_0 &= C2^0 + D(-1)^0 \\ a_1 &= C2^1 + D(-1)^1 \end{aligned}$$

This yields the system

$$\begin{cases} C + D &= 1 \\ 2C - D &= 8 \end{cases}$$

Solving this system to find $C = 3$ and $D = -2$. Hence, $a_n = 3 \cdot 2^n - 2(-1)^n$.
■

Example 22.12
Find an explicit formula for the Fibonacci sequence

$$\begin{aligned} a_0 =& a_1 = 1 \\ a_n =& a_{n-1} + a_{n-2} \end{aligned}$$

Solution.
The roots of the characteristic equation

$$t^2 - t - 1 = 0$$

are $t = \frac{1-\sqrt{5}}{2}$ and $t = \frac{1+\sqrt{5}}{2}$. Thus,

$$a_n = C(\frac{1+\sqrt{5}}{2})^n + D(\frac{1-\sqrt{5}}{2})^n$$

is a solution to

$$a_n = a_{n-1} + a_{n-2}.$$

Using the values of a_0 and a_1 we obtain the system

$$\begin{cases} C+D & = & 1 \\ C(\frac{1+\sqrt{5}}{2})+D(\frac{1-\sqrt{5}}{2}) & = & 1. \end{cases}$$

Solving this system to obtain

$$C=\frac{1+\sqrt{5}}{2\sqrt{5}} \quad and \quad D=-\frac{1-\sqrt{5}}{2\sqrt{5}}.$$

Hence,

$$a_n=\frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^{n+1}-\frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^{n+1}\blacksquare$$

Next, we discuss the case when the characteristic equation has a single root.

Theorem 22.3
Let A and B be real numbers and suppose that the characteristic equation

$$t^2-At-B=0$$

has a single root r. Then the sequences $\{1,r,r^2,\cdots\}$ and $\{0,r,2r^2,3r^3,\cdots,nr^n,\cdots\}$ both satisfy the recurrence relation

$$a_n=Aa_{n-1}+Ba_{n-2}.$$

Proof.
Since r is a root to the characteristic equation, the sequence $\{1,r,r^2,\cdots\}$ is a solution to the recurrence relation

$$a_n=Aa_{n-1}+Ba_{n-2}.$$

Now, since r is the only solution to the characteristic equation we have

$$(t-r)^2=t^2-At-B.$$

This implies that $A=2r$ and $B=-r^2$. Let $s_n=nr^n, \quad n\geq 0$. Then

$$\begin{aligned} As_{n-1}+Bs_{n-2} =& A(n-1)r^{n-1}+B(n-2)r^{n-2} \\ =& 2r(n-1)r^{n-1}-r^2(n-2)r^{n-2} \\ =& 2(n-1)r^n-(n-2)r^n \\ =& nr^n=s_n \end{aligned}$$

So s_n is a solution to $a_n=Aa_{n-1}+Ba_{n-2}$. ■

Example 22.13
Find an explicit formula for

$$\begin{aligned} a_0 =& 1, a_1 = 3 \\ a_n =& 4a_{n-1} - 4a_{n-2}, \quad n \geq 2 \end{aligned}$$

Solution.
Solving the characteristic equation

$$t^2 - 4t + 4 = 0$$

we find the single root $r = 2$. Thus,

$$a_n = C2^n + Dn2^n$$

is a solution to the equation $a_n = 4a_{n-1} - 4a_{n-2}$. Since $a_0 = 1$ and $a_1 = 3$, we obtain the following system of equations:

$$\begin{aligned} C =& 1 \\ 2C + 2D =& 3 \end{aligned}$$

Solving this system to obtain $C = 1$ and $D = \frac{1}{2}$. Hence, $a_n = 2^n + \frac{n}{2}2^n$. ■

Example 22.14
Let $A_1, A_2, \cdots, A_n$ be subsets of a set S.
a. Give a recursion definition for $\cup_{i=1}^{n} A_i$.
b. Give a recursion definition for $\cap_{i=1}^{n} A_i$.

Solution.
a. $\cup_{i=1}^{1} A_i = A_1$ and $\cup_{i=1}^{n} A_i = (\cup_{i=1}^{n-1} A_i) \cup A_n, \quad n \geq 2$.
b. $\cap_{i=1}^{1} A_i = A_1$ and $\cap_{i=1}^{n} A_i = (\cap_{i=1}^{n-1} A_i) \cap A_n, \quad n \geq 2$.■

Example 22.15
Use mathematical induction to prove the following generalized De Morgan's law.

$$(\cup_{i=1}^{n} A_i)^c = \cap_{i=1}^{n} A_i^c$$

Solution.
Basis of induction: $(\cup_{i=1}^{1} A_i)^c = A_1^c = \cap_{i=1}^{1} A_i^c$.

Induction hypothesis: Suppose that $(\cup_{i=1}^{n} A_i)^c = \cap_{i=1}^{n} A_i^c$.
Induction step: We must show that $(\cup_{i=1}^{n+1} A_i)^c = \cap_{i=1}^{n+1} A_i^c$. Indeed,

$$\begin{aligned}(\cup_{i=1}^{n+1} A_i)^c =&((\cup_{i=1}^{n} A_i) \cup A_{n+1})^c \\ =&(\cup_{i=1}^{n} A_i)^c) \cap A_{n+1}^c \\ =&(\cap_{i=1}^{n} A_i^c) \cap A_{n+1}^c \\ =&\cap_{i=1}^{n+1} A_i^c \ \blacksquare\end{aligned}$$

Example 22.16
Let $a_1, a_2, \cdots, a_n$ be numbers.
a. Give a recursion definition for $\sum_{i=1}^{n} a_i$.
b. Give a recursion definition for $\Pi_{i=1}^{n} a_i$.

Solution.
a. $\sum_{i=1}^{1} a_i = a_1$ and $\sum_{i=1}^{n} a_i = (\sum_{i=1}^{n-1} a_i) + a_n, \quad n \geq 2$.
b. $\Pi_{i=1}^{1} a_i = a_1$ and $\Pi_{i=1}^{n} a_i = (\Pi_{i=1}^{n-1} a_i) \cdot a_n, \quad n \geq 2$.$\blacksquare$

Example 22.17
A function is said to be defined **recursively** or to be a **recursive function** if its rule of definition refers to itself. Define the factorial function recursively.

Solution.
We have

$$\begin{aligned}f(0) =&1 \\ f(n) =&nf(n-1), \quad n \geq 1 \ \blacksquare\end{aligned}$$

Example 22.18
Let $G : \mathbb{N} \to \mathbf{Z}$ be the relation given by

$$G(n) = \begin{cases} 1, & \text{if } n = 1 \\ 1 + G(\frac{n}{2}), & \text{if n is even} \\ G(3n-1), & \text{if } n > 1 \text{ is odd} \end{cases}$$

Show that G is not a function.

Solution.
Assume that G is a function so that $G(5)$ exists. Listing the first five values

of G we find

$$\begin{aligned}
G(1) =& 1 \\
G(2) =& 2 \\
G(3) =& G(8) = 1 + G(4) = 2 + G(2) = 4 \\
G(4) =& 1 + G(2) = 3 \\
G(5) =& G(14) = 1 + G(7) \\
=& 1 + G(20) \\
=& 2 + G(10) \\
=& 3 + G(5)
\end{aligned}$$

But the last equality implies that $0 = 3$ which is impossible. Hence, G does not define a function. ■

Review Problems

Problem 22.1
Find the first four terms of the following recursively defined sequence:

$$\begin{aligned} v_1 =& 1, v_2 = 2 \\ v_n =& v_{n-1} + v_{n-2} + 1, \quad n \geq 3. \end{aligned}$$

Problem 22.2
Prove each of the following for the Fibonacci sequence:
a. $F_k^2 - F_{k-1}^2 = F_k F_{k+1} - F_{k+1} F_{k-1}, \quad k \geq 1.$
b. $F_{k+1}^2 - F_k^2 - F_{k-1}^2 = 2F_k F_{k-1}, \quad k \geq 1.$
c. $F_{k+1}^2 - F_k^2 = F_{k-1} F_{k+2}, \quad k \leq 1.$
d. $F_{n+2} F_n - F_{n+1}^2 = (-1)^n$ for all $n \geq 0$.

Problem 22.3
Find $\lim_{n\to\infty} \frac{F_{n+1}}{F_n}$ where $F_0, F_1, F_2, \cdots$ is the Fibonacci sequence. (Assume that the limit exists.)

Problem 22.4
Define $x_0, x_1, x_2, \cdots$ as follows:

$$x_n = \sqrt{2 + x_{n-1}}, \quad x_0 = 0.$$

Find $\lim_{n\to\infty} x_n$.

Problem 22.5
a. Make a list of all bit strings of lengths zero, one, two, three, and four that do not contain the pattern 111.
b. For each $n \geq 0$ let $d_n =$ the number of bit strings of length n that do not contain the bit pattern 111. Find d_0, d_1, d_2, d_3, and d_4.
c. Find a recurrence relation for $d_0, d_1, d_2, \cdots$
d. Use the results of (b) of (c) to find the number of bit strings of length five that do not contain the pattern 111.

Problem 22.6
Find a formula for each of the following sums:
a. $1 + 2 + \cdots + (n-1), \quad n \geq 2.$
b. $3 + 2 + 4 + 6 + 8 + \cdots + 2n, \quad n \geq 1.$
c. $3 \cdot 1 + 3 \cdot 2 + 3 \cdot 3 + \cdots 3 \cdot n, \quad n \geq 1.$

Problem 22.7
Find a formula for each of the following sums:
a. $1 + 2 + 2^2 + \cdots + 2^{n-1}, \quad n \geq 1.$
b. $3^{n-1} + 3^{n-2} + \cdots + 3^2 + 3 + 1, \quad n \geq 1.$
c. $2^n + 3 \cdot 2^{n-2} + 3 \cdot 2^{n-3} + \cdots + 3 \cdot 2^2 + 3 \cdot 2 + 3, \quad n \geq 1.$
d. $2^n - 2^{n-1} + 2^{n-2} - 2^{n-3} + \cdots + (-1)^{n-1} \cdot 2 + (-1)^n, \quad n \geq 1.$

Problem 22.8
Use iteration to guess a formula for the following recursively defined sequence and then use mathematical induction to prove the validity of your formula: $c_1 = 1, c_n = 3c_{n-1} + 1$, for all $n \geq 2$.

Problem 22.9
Use iteration to guess a formula for the following recursively defined sequence and then use mathematical induction to prove the validity of your formula: $w_0 = 1, w_n = 2^n - w_{n-1}$, for all $n \geq 2$.

Problem 22.10
Determine whether the recursively defined sequence: $a_1 = 0$ and $a_n = 2a_{n-1} + n - 1$ satisfies the recursive formula $a_n = (n-1)^2, \ n \geq 1$.

Problem 22.11
Which of the following are second-order homogeneous recurrence relations with constant coefficients?
a. $a_n = 2a_{n-1} - 5a_{n-2}$.
b. $b_n = nb_{n-1} + b_{n-2}$.
c. $c_n = 3c_{n-1} \cdot c_{n-2}^2$.
d. $d_n = 3d_{n-1} + d_{n-2}$.
e. $r_n = r_{n-1} - r_{n-2} - 2$.
f. $s_n = 10s_{n-2}$.

Problem 22.12
Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$a_n = C \cdot 2^n + D, \quad n \geq 0$$

where C and D are real numbers.
a. Find C and D so that $a_0 = 1$ and $a_1 = 3$. What is a_2 in this case?
b. Find C and D so that $a_0 = 0$ and $a_1 = 2$. What is a_2 in this case?

Problem 22.13

Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$a_n = C \cdot 2^n + D, \quad n \geq 0$$

where C and D are real numbers. Show that for any choice of C and D,

$$a_n = 3a_{n-1} - 2a_{n-2}, \quad n \geq 2.$$

Problem 22.14
Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$\begin{aligned} a_0 =& 1, a_1 = 2 \\ a_n =& 2a_{n-1} + 3a_{n-2}, \quad n \geq 2. \end{aligned}$$

Find an explicit formula for the sequence.

Problem 22.15
Let $a_0, a_1, a_2, \cdots$ be the sequence defined by the recursive formula

$$\begin{aligned} a_0 =& 1, a_1 = 4 \\ a_n =& 2a_{n-1} - a_{n-2}, \quad n \geq 2. \end{aligned}$$

Find an explicit formula for the sequence.

Problem 22.16
The triangle inequality for absolute value states that for all real numbers a and b, $|a+b| \leq |a|+|b|$. Use the recursive definition of summation, the triangle inequality, the definition of absolute value, and mathematical induction to prove that for all positive integers n, if $a_1, a_2, \cdots, a_n$ are real numbers then

$$|\sum_{k=1}^{n} a_k| \leq \sum_{k=1}^{n} |a_k|.$$

Problem 22.17
Use the recursive definition of union and intersection to prove the following general distributive law: For all positive integers n, if A and $B_1, B_2, \cdots, B_n$ are sets then

$$A \cap (\cup_{k=1}^{n} B_k) = \cup_{k=1}^{n} (A \cap B_k).$$

Problem 22.18
Use mathematical induction to prove the following generalized De Morgan's law.

$$(\cap_{i=1}^{n} A_i)^c = \cup_{i=1}^{n} A_i^c$$

Problem 22.19
Show that the relation $F : \mathbb{N} \to \mathbf{Z}$ given by the rule

$$F(n) = \begin{cases} 1 & \text{if } n = 1. \\ F(\frac{n}{2}) & \text{if n is even} \\ 1 - F(5n-9) & \text{if } n \text{ is odd and } n > 1 \end{cases}$$

does not define a function.

23 Project VII: Applications to Relations

Part I: Relational Database

The "bi" in binary relation R refers to the fact that R is a subset of the cartesian product of two sets. Let $A_1, A_2, \cdots, A_n$ be given sets. If R is a subset of $A_1 \times A_2 \times \cdots \times A_n$ then we call R an **n-ary** relation. An n-ary relation can be represented by a table or a set of ordered n-tuples.

Example 23.1

ID#	Name	Position	Age
22012	Johnsonbaugh	c	22
93831	Glover	of	24
58199	Battey	p	18
84341	Cage	c	30
01180	Homer	lb	37
26710	Score	p	22
61049	Johnsonbaugh	of	30
39826	Singleton	2b	31

A **database** is a collection of records that are manipulated by a computer. **Database management systems** are programs that help users access the information in databases. The **relational database model** is based on the concept of an n-ary relation.
When an n-ary relation is represented by a table then the columns in this table are called **attributes**. In the above table, the attributes are ID Number, Name, Position, and Age. A single attribute or a combination of attributes for a relation is called a **key** if the values of the attributes uniquely define an n-tuple. For example, in the above table, we can take the attribute ID Number as a key since every person has a unique identification number. The attribute Name is not a key because different persons can have the same name. For the same reason, we cannot take the attribute Age as a key. A database management system responds to **queries**. A query is a request for information from the database. For example, "Find all persons that are 22 years old".

Problem 23.1
a. Express the above 4-ary relation as a set of 4-tuples.
b. Answer the query: PLAYER[Name]
c. Answer the query: PLAYER[Name, Position]

Part II: Representing a Relation by a Matrix.

Let A be a set with n elements and R be a binary relation on A. Define the $n \times n$ matrix $M(R) = (m_{ij})$ as follows:

$$m_{ij} = \begin{cases} 1 & if \quad (a_i, b_j) \in R \\ 0 & if \quad (a_i, b_j) \notin R \end{cases}$$

If the numbers on the main diagonal of $M(R)$ are all equal to 1 then R is reflexive. If $M(R)^T = M(R)$, where $M(R)^T$ is the transpose of $M(R)$, then the relation R is symmetric. If $m_{ij} = 0$ or $m_{ji} = 0$ for $i \neq j$ then R is antisymmetric.

Problem 23.2
Let $A = \{1, 2, 3\}$ and $R = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$. Find $M(R)$ and use it to determine if the relation R is reflexive, symmetric or antisymmetric.

Part III: Cryptology
An important application to congruences is cryptology, which is the study of secret messages.

(a) The process of making a message secret is called **encryption**. This process consists of assigning the alphabet $A, B, C, \cdots, Z$ by the integers $0, 1, 2, \cdots, 25$. Then the encrypted version of the message, the letter represented by p is replaced with the letter represented by the remainder of the division of $(p + 3)$ by 26.

Problem 23.3
What is the encrypted message produced from the message "MEET YOU IN THE PARK"?

(b) **Decryption** is the process of determining the original message. In this case the letter represented by p is replaced by the letter represented by the remainder of the division of $(p - 3)$ by 26.

Problem 23.4
What is the message produced from the encrypted message "PHHW BRX LQ WKH SDUN"?

24 Project VIII: Well-Ordered Sets and Lattices

Let $[A, \leq]$ be a poset. Let $B \subseteq A$. An element $b \in B$ is called a **least element** of B if and only if $b \leq x$ for all $x \in B$. If $x \leq b$ for all $x \in B$ then we call b the **greatest element** of B.

Problem 24.1
Consider the set $\mathbb{N}$ with the inequality relation $\leq$. Let $B = \{2, 4, 5, 6, 7, 8, 9\}$. What is the least element of B? What is the greatest element of B?

A poset $[A, \leq]$ is said to be **well-ordered** if and only if $\leq$ is a total order and every subset of A has a least element.

Problem 24.2
a. Show that $(\mathbb{N}, \leq)$ is well-ordered.
b. Show that $(\mathbb{Z}, \leq)$ is not well-ordered.

An element $a \in A$ is called a **lower bound** of B if $a \leq x$ for all $x \in B$. We call $a \in A$ an **upper bound** of B if $x \leq a$ for all $x \in B$. Note that a lower bound or an upper bound is not unique.

Problem 24.3
Consider the poset $[\mathbb{N}, \leq]$. Let $B = \{2, 4, 8, 10\}$. Find a lower bound of B as well as an upper bound.

The greatest element of the set of lower bounds of B is called the **greatest lower bound**, in symbol $g.l.b(B)$. The least element of the set of upper bounds of B is called the **least upper bound**, in symbol $l.u.b(B)$.

Problem 24.4
Consider the poset $[\mathbb{R}, \leq]$ and $B = (-1, 1)$. Find $g.l.b(B)$ and $l.u.b(B)$.

A **lattice** is a poset $[A, \leq]$ such that every pair of elements in A have a l.u.b and g.l.b in A.

Problem 24.5
Show that $[\mathbb{R}, \leq]$ is a lattice.

Problem 24.6
Let $A = \{2, 3, 4, 9, 12, 18\}$ and R be the binary relation "divides" on A. Show that $[A, R]$ is not a lattice.

25 Project IX: The Pigeonhole Principle

The **Pigeonhole principle** asserts that if n pigeons fly into k holes with $n > k$ then some of the pigeonholes contain at least two pigeons. The reason this statement is true can be seen by arguing by contradiction. If the conclusion is false, each pigeonhole contains at most one pigeon and, in this case, we can account for at most k pigeons. Since there are more pigeons than holes, we have a contradiction.

Problem 25.1
Ten persons have first names George, William, and Laura and last names Bush, Perry, and Gramm. Show that at least two persons have the same first and last names.

A mathematical way to formulate the pigeonhole principle is given by the following exercise

Problem 25.2
Let S be a finite set and $\{A_1, A_2, \cdots, A_n\}$ be a partition of S. Use the method of contradiction to show that there is an index $1 \leq i \leq n$ such that $|A_i| \geq \frac{|S|}{n}$.

One can use the previous exercise to solve the following exercise.

Problem 25.3
Let S and T be two finite sets such that $|S| > k|T|$ where k is a positive integer. Show that for any function $f : S \to T$ there is a $t \in T$ such that the set $\{s \in S : f(s) = t\}$ has more than k elements.
Hint: Show that the family $A_t = \{s \in S : f(s) = t\}$, where $t \in T$, partitions S into n sets with $n \leq |T|$. Then apply the previous exercise.

As a consequence of the above exercise we have

Problem 25.4
If S and T are finite sets such that $|S| > |T|$ then any function $f : S \to T$ is not one-to-one.

26 Project X: Countable Sets

We say that two sets have the same **cardinality** if and only if there is a bijective function between them. A set A is called **countably infinite** if and only if A has the same cardinality as the set $\mathbb{N}^*$ of positive integers. A set A is called **countable** if it is either finite or countably infinite. A set that is not countable is said to be **uncountable**. Examples of uncountable sets are $\mathbb{R}$ and the intervals in $\mathbb{R}$..
The purpose of this project is to look at some countably infinite sets.

Problem 26.1
Show that the function $f : \mathbb{N}^* \to \mathbb{N}$ given by $f(n) = n - 1$ is a bijective function. Thus, $\mathbb{N}$ is countably infinite.

Problem 26.2
Show that the function $f : \mathbb{N}^* \to \mathbf{Z}$ defined by

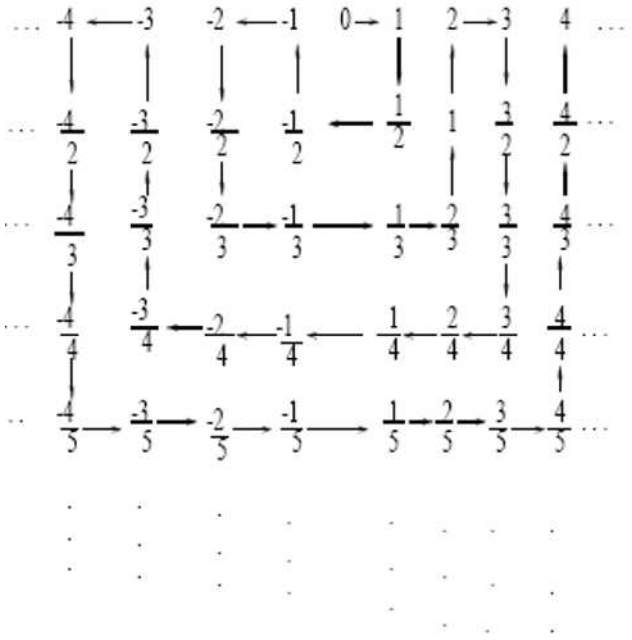
$$f(n) = \begin{cases} \frac{n}{2} & if\ n\ is\ even \\ \frac{1-n}{2} & if\ n\ is\ odd \end{cases}$$

is bijective. Hence, $\mathbf{Z}$ is countably infinite.

Problem 26.3
Show that the function $f : \mathbf{Z} \to 2\mathbf{Z}$ defined by $f(n) = 2n$ is a bijective function. Hence, the set of even integers is countably infinite.

Problem 26.4
Show that the set of rational numbers $\mathbb{Q}$ is countably infinite.

Hint:



)

27 Project XI: Finite-State Automaton

A finite-state machine can be looked at as a mathematical model that can accept input, store and process information and produce output. Examples include digital computers, compilers, vending machines, coin changers, telephones, and elevators.

This model has an input/output unit, and, consequently, has a way of communicating with the world using a set of symbols. Let I be the set of input symbols and O, the set of output symbols. In the case of an elevator I might be up, down, and floor selection, while O might be stops on particular floors. Besides input and output symbols, there is a set of states S for our model. A state is like a snapshot of what is happening in the machine at a particular instant. An elevator might be in a state of going down to the first floor to pick up a passenger or in a state of stopping on the third floor on the way up to the fifth floor. There are always an initial state of our model, denoted by s_0, and final or accepting state(s).

Also, our model has a function, called the next state function. This function returns the next state based on the present state and input. For instance, if the elevator is in the state of moving up to the fifth floor and has an input of someone pressing the down button on the third floor, it goes to a state that says, "Remember, when coming back down to stop and pick up someone on the third floor."

The above discussion is formalized as follows:

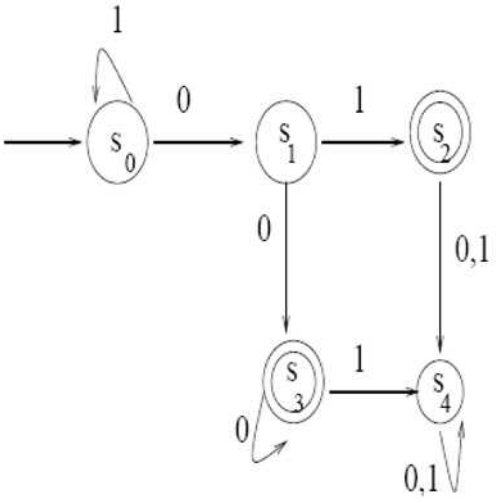
A **finite-state automaton** A consists of five objects:

1. a set I, called the **input alphabet**, of input symbols;
2. a set O, called the **output alphabet**, of output symbols;
3. a set S of **states** the machine can be in;
4. a subset of S whose elements are called **accepting states**;
5. a next-state function or **transition function** $N : S \times I \to S$. If $s \in S$ and $m \in I$ then $N(s, m)$ is the state to which A goes if m is input to A when A is in state s. The **initial state** of the machine is s_0.

The operation of a finite-state machine is commonly described by a diagram called a **transition diagram.** The edges are labeled with inputs and nodes with states. A double circle stands for the final or accepting state(s).

Problem 27.1

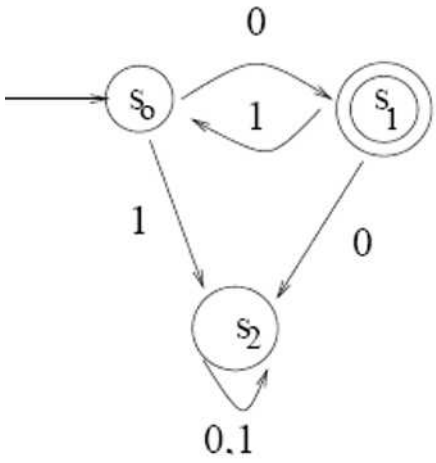
Consider the finite-state automaton defined by the transition diagram



a. What are the elements of S?
b. What are the input symbols?
c. What is the initial state?
d. What are the accepting states?
e. Find $N(s_3, 1)$ and $N(s_3, 0)$.

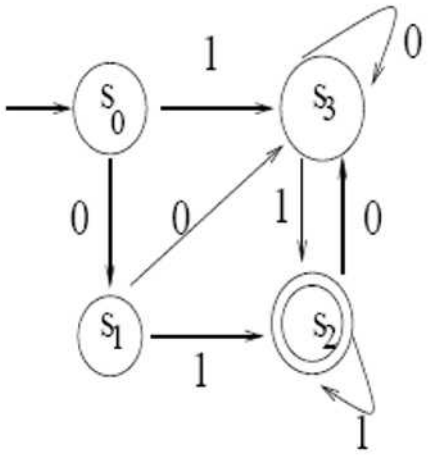
Let A be a finite-state automaton with input alphabet I. Let I^* be the set of all words with letters from I. A word $w \in I^*$ is said to be **accepted by** A if, and only if, A goes to an accepting state when the symbols of w are input to A in sequence starting when A is in its initial state. The **language accepted by** A, denoted by $L(A)$, is the set of all words that are accepted by A.

Problem 27.2
Consider the finite-state automaton defined by the following transition diagram.
a. To what states does A go if the symbols of the following words are input to A in sequence starting from the initial state?
(i) 1101 (ii) 0011 (iii) 0101010.
b. Which of the words in part (a) send A to an accepting state?
c. Show that $L(A) = \{0(10)^n : n \geq 0\}$ where $(10)^n = 1010\cdots$ with n copies of 10 juxtaposed into one word.



Let A be a finite-state automaton with input alphabet I and states S. Let $N^* : S \times I^* \to S$ be the function defined as follows: $N^*(s, w)$ is the state to which A goes if the symbols of w are input to A in sequence starting when A is in state s. We call N^* the **eventual -state function.**

Problem 27.3
A finite-state automaton A, given by the transition diagram below, has transition function N and eventual-state function N^*.
a. Find $N(s_2, 0)$ and $N(s_1, 0)$.
b. Find $N^*(s_2, 11010)$ and $N^*(s_0, 01000)$.



Problem 27.4
Design a finite-state machine that recognizes words of the form $01, 011, 0111, 01111, \cdots$.

Introduction to the Analysis of Algorithms

Informally, an **algorithm** is any well-defined computational procedure that takes a set of values as **input** and produces a set of values as **output.**
The subject of the analysis of algorithms consists of the study of efficiency of algorithms. Two aspects of the algorithm efficiency are: the amount of time required to execute the algorithm and the memory space it consumes. In this chapter we introduce the basic techniques for calculating time efficiency.

28 Time Complexity and O-Notation

The primary efficiency criterion for analyzing the efficiency of an algorithm is the **running time** of the algorithm as a function of the number of values it processes. The running time of an algorithm is not measured by counting the minutes and seconds for the algorithm written in a particular language and running on a particular machine. Rather it is defined to be an estimate of the number of operations performed by the algorithm given a particular number of input values.
Generally, given an algorithm that performs a task, we will be interested in estimating the running time as a function of the problem size. For example, let us consider the **sequential search** of an item X from a list of n items. Here, we say that the problem size is n. Let $T(n)$ be a measure of the time required to execute an algorithm of problem size n. We call $T(n)$ the **time complexity function** of the algorithm. If n is sufficiently small then the algorithm will not have a long running time. Thus, the interesting question is: "How fast does $T(n)$ increase as n increases?" This is called the **asymptotic behavior** of the time complexity function.
In our time analysis we will restrict ourselves to the **worst case** behavior of

an algorithm; that is, the longest running time for any input of size n.
Since we are considering asymptotic efficiency of algorithms, basically we will be focusing on the leading term of $T(n)$. For example, if $T(n) = 4n^3 - 2n^2 + n + 5$ then $T(n) = n^3(4 - \frac{2}{n} + \frac{1}{n^2} + \frac{5}{n^3})$ and for large n we have $T(n) \sim n^3$. We say that $T(n)$ has a **growth of order** n^3.
We say that one algorithm is more efficient than another if its worst case running time has a lower order of growth.

Example 28.1
Estimate the time complexity of the following algorithm:

$i := 1$
$p := 1$
for $i := 1$ **to** n
    $p := p \cdot i$
$i := i + 1$
next i

Solution.
Prior to entering the loop, it takes two assignment statements to initialize the variables i and p. The loop is executed n times, and each time it executes the two assignment statements in the body of the loop with a total of two arithmetic operations. Thus, the time complexity of the algorithm is given by

$$T(n) = 4n + 2$$

so the growth is of order n.■

Example 28.2
What is the run-time complexity based on n for the following program segment:

for $i := 1$ **To** n
    for $j := 1$ **To** n
        A(i,j) := x
    next j
next i

Solution.
The inner loop is executed n times and the outer loop also is executed n

times. Hence, $T(n) = n^2$ so that the growth is of order n^2.■

In the above two problems we found a precise expression for the time complexity of the algorithm. What usually interests us is the order of growth. We next introduce some of the concepts of growth orders. Let $g : \mathbb{N} \to \mathbb{R}$. We define the set

$O(g(n)) = \{f(n) :$ *there exist positive constants* n_0 *and* C *such that* $|f(n)| \leq C|g(n)|,$ *for* $n \geq n_0\}$.

We say that a function f is **order at most g** or f **big-oh of** g if and only if $f(n) \in O(g(n))$. Sometimes we write $f(n) = O(g(n))$. Graphically, this means that for $n \geq n_0$ the graph of f is below the graph of g.

Example 28.3
Show that the time complexity found in Example 28.1 is $O(n)$.

Solution.
To show that $T(n) = O(n)$ we must produce constants C and n_0 such that $T(n) \leq Cn$ for $n \geq n_0$. Indeed, $T(n) \leq 5n$ for $n \geq 2$ so that $n_0 = 2$ and $C = 5$. ■

Example 28.4
Show that the run-time complexity based on n for the following program segement is $O(n^2)$.

```
s := 0
for i := 1 To n
    for j := 1 To i
        s := s + j · (i − j + 1)
    next j
next i
```

Solution.
Prior to entering the loop there is one assignment statement. Now, there are two additions, one subtraction, one multiplication and one assignment for each iteration of the inner loop. The total number of time the inner loop is executed is

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

Hence, $T(n) = 5 \cdot \frac{n(n+1)}{2} + 1 \leq 5n^2,\ n \geq 1$ so that $C = 5$ and $n_0 = 2$. Hence, $T(n) \in O(n^2)$. ■

We say that a function f is of **polynomial complexity** if and only if $f \in O(n^p)$ for some $p \in \mathbb{N}$. If $p = 0$ then we say that f is of **constant** complexity. If $p = 1$ we say that the complexity is **linear**.

Example 28.5
Show that

$$1 + 2 + 3 + \cdots + n = O(n^2).$$

Solution.
Indeed, since $n \geq 1$ we have

$$1 + 2 + 3 + \cdots + n \leq n + n + n + \cdots + n = n^2$$

so that $C = 1$ and $n_0 = 1$. ■

Example 28.6
Show that $n^3 \notin O(n^2)$.

Solution.
We proceed by contradiction. Suppose that $n^3 \in O(n^2)$. Then there exist constants C and n_0 such that $n^3 \leq Cn^2$ for all $n \geq n_0$. Dividing through by n^2 to obtain $n \leq C$. This leads to a contradiction since the left-hand side can be made as large as we please whereas the right-hand side is constant. ■

Example 28.7
Show that if $f(n) \in O(g(n))$ and $g(n) \in O(h(n))$ then $f(n) \in O(h(n))$.

Solution.
Since $f(n) \in O(g(n))$, there exist n_1 and C_1 such that $|f(n)| \leq C_1|g(n)|$ for all $n \geq n_1$. Similarly, there exist constants C_2 and n_2 such that $|g(n)| \leq C_2|h(n)|$ for all $n \geq n_2$. Let $n_0 = max\{n_1, n_2\}$ and $C = C_1C_2$. Then for $n \geq n_0$ we have

$$|f(n)| \leq C_1|g(n)| \leq C_1C_2|h(n)| = C|h(n)|\blacksquare$$

Example 28.8
Suppose we want to arrange the elements of a one dimensional array $a[1], a[2], \cdots, a[n]$ in increasing order. An **insertion sort** compares every pair of elements, switching the values of those that are out of order, $a[i-1] > a[i]$.
a. How many possible pairs are compared?
b. What is the maximum number of exchanges?
c. What is time the complexity of this algorithm in the worst case?
d. Is this a polynomial-time algorithm?

Solution.
a. The number of possible pairs to compare in the algorithm is

$$1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

b. From part a. it follows that the maximum number of exchanges is $\frac{n(n-1)}{2}$.
c. $T(n) = \frac{n(n-1)}{2}$.
d. For $n \geq 1, T(n) \leq \frac{n^2}{2}$ so that $T(n) \in O(n^2)$. ■

Next, we recall the following definition from calculus. If $L = \lim_{x\to\infty} f(x)$ then for any $\epsilon > 0$ there is a positive integer N such that $|f(x) - L| < \epsilon$ whenever $n \geq N$.
Using this definition, we have the following important theorem.

Theorem 28.1
Suppose that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = L$ with $L \geq 0$. Then $f(n) \in O(g(n))$. Moreover,
a. if $L > 0$ then $g(n) \in O(f(n))$, and
b. if $L = 0$ then $g(n) \notin O(f(n))$.

Proof.
Let $\epsilon = 1$. Then there is a positive integer n_0 such that $|\frac{f(n)}{g(n)} - L| < 1$ whenever $n \geq n_0$. This implies that $|\frac{f(n)}{g(n)}| < 1 + L$ for $n \geq n_0$. Hence, $|f(n)| < C|g(n)|$ where $C = (1 + L)$ and $n \geq n_0$. But this is just saying that $f(n) \in O(g(n))$.
a. Now, suppose that $L > 0$. Then $\lim_{n\to\infty} \frac{g(n)}{f(n)} = \frac{1}{L}$. Interchange the roles of f and g in the previous argument to find that $|g(n)| < C|f(n)|$ where $C = 1 + \frac{1}{L}$ and $n \geq n_0$ for some positive integer n_0. Hence, $g(n) \in O(f(n))$.
b. Now suppose that $L = 0$. We use contradiction to show that $g(n) \notin O(f(n))$. So suppose that $g(n) \in O(f(n))$. Then there exist positive constants

C and M_1 such that $|g(n)| \leq C|f(n)|$ for all $n \geq M_1$. On the other hand, by letting $\epsilon = \frac{1}{C}$ we can find a positive integer M_2 such that $|\frac{f(n)}{g(n)}| < \epsilon$ whenever $n \geq M_2$. Let $n_0 = max\{M_1, M_2\}$. Then for $n \geq n_0$ we have

$$C < |\frac{g(n)}{f(n)}| \leq C$$

which is a contradiction. Hence, we must have $g(n) \notin O(f(n))$. ■

Review Problems

Problem 28.1
Find the worst case running time of the following segment of an algorithm:
for $i := 1$ **to** n
  for $j := 1$ **to** $\lfloor \frac{i+1}{2} \rfloor$
    $a := (n - i) \cdot (n - j)$
  next j
next i

Problem 28.2
Find the worst case running time of the following segment of an algorithm:

for $i := 1$ **to** n
  for $j := 1$ **to** $2n$
    for $k := 1$ **to** n
      $x := i \cdot j \cdot k$
    next k
  next j
next i

Problem 28.3
Construct a table showing the result of each step when insertion sort is applied to the array $a[1] = 6, a[2] = 2, a[3] = 1, a[4] = 8, a[5] = 4$.

Problem 28.4
How many comparisons actually occur when insertion sort is applied to the array of the previous exercise?

Problem 28.5
Selection sort is another algorithm for arranging the elements of a one-dimensional array $a[1], a[2], \cdots, a[n]$ in increasing order. The sorting works by selecting the smallest item in the list, moving it to the front of the list, and then finding the smallest of the remaining items and moving it to the second position in the list, and so on. When two items in the list, say $a[k]$ and $a[m]$, have to be interchanged, we write $switch(a[k], a[m])$. The following is the selection algorithm:

for $i := 1$ **to** $n - 1$

```
  min := i
  for j := i + 1 to n
     if a[min] > a[j] then
     switch(a[min], a[j])
  next j
next i
```

Construct a table showing the result of each step when selection sort is applied to the array $a[1] = 5, a[2] = 3, a[3] = 4, a[4] = 6, a[5] = 2$.

Problem 28.6
How many comparisons actually occur when selection sort is applied to the array of the previous exercise?

Problem 28.7
Show that $\lfloor \sqrt{n} \rfloor \in O(\sqrt{n})$.

Problem 28.8
Show that

$$1^2 + 2^2 + \cdots + n^2 \in O(n^3).$$

Problem 28.9
Show that

$$1^3 + 2^3 + \cdots + n^3 \in O(n^4).$$

Problem 28.10
a. Use mathematical induction to show that

$$1^{\frac{1}{3}} + 2^{\frac{1}{3}} + \cdots + n^{\frac{1}{3}} \leq n^{\frac{4}{3}}$$

for all $n \geq 1$.
b. What can you conclude from part (a) about the order of the above sum?

29 Logarithmic and Exponential Complexities

In this section we assume that the reader is familiar with the definitions and rules of both exponential and logarithmic functions. Unless explicitly stated, all logarithms in this chapter are to base 2 mainly because of the following theorem

Theorem 29.1
For any $a > 1$, $O(\log_a n) = O(\log_2 n)$.

Proof.
We must show that there exist constants C_1, C_2 and n_0 such that $\log_a n \leq C_1 \log_2 n$ and $\log_2 n \leq C_2 \log_a n$ for all $n \geq n_0$. By the change of bases formula we have

$$\log_a n = \frac{\log_2 n}{\log_2 a}.$$

Now, let $C_1 = \frac{1}{\log_2 a}, C_2 = \log_2 a$, and $n_0 = 1$. ■

If $f(n) \in O(\log_2 n)$ we say that $f(n)$ has **logarithmic** complexity. A function $f(n)$ is said to be of **exponential complexity** if and only if $f(n) \in O(a^n)$ for some $a > 1$.

Example 29.1
Show that $n + n \log_2 n \in O(n \log_2 n)$.

Solution.
Since $\lim_{n\to\infty} \frac{n}{n \log_2 n} = 0$, there is a positive integer n_0 such that $n < n \log_2 n$ for all $n \geq n_0$. Thus,$n + n \log_2 n < 2nlog_2n = Cn \log_2 n, \;\; n \geq n_0$. This shows that $n + n \log_2 n \in O(n \log_2 n)$. ■

Example 29.2
a. Show that $n! = O(n^n)$.
b. Show that $n = O(2^n)$.
c. Use b. to show that $\log_2 n = O(n)$.

Solution.
a. Since $n - i \leq n$ for $0 \leq i \leq n$ we have

$$\begin{aligned} n! &= n(n-1)(n-2)\cdots 2 \cdot 1 \\ &\leq \; n \cdot n \cdot n \cdots n \cdot n = n^n \end{aligned}$$

It follows that $n! = O(n^n)$.
b. We show by induction on $n \geq 0$ that $n \leq 2^n$.

Basis of induction: For $n = 0$ we have $0 \leq 2^0$.
Induction hypothesis: Suppose that $n \leq 2^n$.
Induction step: We must show that $n + 1 \leq 2^{n+1}$. Indeed,

$$\begin{aligned} n + 1 &\leq n + n \\ &\leq 2^n + 2^n = 2^{n+1} \end{aligned}$$

Hence, $n = O(2^n)$.
c. Take the logarithm of both sides of b. to obtain $\log_2 n \leq n, \quad n \geq 1$. That is, $\log_2 n = O(n)$. ■

Example 29.3
a. Show that $\log_2 n! = O(n \log_2 n)$.
b. Show that $n \log_2 n = O(\log_2 n!)$.

Solution.
a. We have shown that $n! = O(n^n)$. That is, $n! \leq n^n$ for $n \geq 1$. Take logarithm of both sides to obtain $\log_2 n! \leq n \log_2 n$. That is, $\log_2 n! = O(n \log_2 n)$.
b. It is easy to see that $(n - i)(i + 1) \geq n$ for all $0 \leq i \leq n - 1$. In this case

$$\begin{aligned} (n!)^2 &= [n \cdot (n-1) \cdots 2 \cdot 1][1 \cdot 2 \cdots (n-1) \cdot n] \\ &= (n \cdot 1)[(n-1) \cdot 2] \cdots [2 \cdot (n-1)](1 \cdot n) \\ &\geq n \cdot n \cdots n \cdot n \\ &= n^n. \end{aligned}$$

Now take the logarithm of both sides to obtain $n \log_2 n \leq 2 \log_2 n!$. That is, $n \log_2 n = O(\log_2 n!)$. ■

Example 29.4
a. Show that if $f_1(n) \in O(g(n))$ and $f_2(n) \in O(g(n))$ then $f_1(n) + f_2(n) \in O(g(n))$.
b. Show that if $f_1(n) \in O(g_1(n))$ and $f_2(n) \in O(g_2(n))$ then $f_1(n) \cdot f_2(n) \in O(g_1(n) \cdot g_2(n))$.
c. Use a. and b. to show that

$$3n \log_2 n! + (n^2 + 3) \log_2 n = O(n^2 \log_2 n).$$

Solution.
a. Since $f_1(n) \in O(g(n))$, there exist n_1 and C_1 such that $|f_1(n)| \leq C_1|g(n)|$ for all $n \geq n_1$. Similarly, there exist constants C_2 and n_2 such that $|f_2(n)| \leq C_2|g(n)|$ for all $n \geq n_2$. Let $n_0 = max\{n_1, n_2\}$ and $C = C_1 + C_2$. Then for $n \geq n_0$ we have

$$|f_1(n) + f_2(n)| \leq C_1|g(n)| + C_2|g(n)| = C|g(n)|.$$

b. Now since $f_1(n) \in O(g_1(n))$, there exist n_1 and C_1 such that $|f_1(n)| \leq C_1|g_1(n)|$ for all $n \geq n_1$. Similarly, there exist constants C_2 and n_2 such that $|f_2(n)| \leq C_2|g_2(n)|$ for all $n \geq n_2$. Let $n_0 = max\{n_1, n_2\}$ and $C = C_1 \cdot C_2$. Then for $n \geq n_0$ we have

$$|f_1(n) \cdot f_2(n)| \leq C|g_1(n)g_2(n)|.$$

c. Using b. above and a. of the previous exercise we have $3n \log_2 n! = O(n^2 \log_2 n)$. Since $(n^2 + 3) \log_2 n = O(n^2 \log_2 n)$, by a. and b. the result follows. ■

Review Problems

Problem 29.1
Show that $1 + 2 + 2^2 + \cdots + 2^n \in O(2^{n+1})$.

Problem 29.2
Show that $\frac{2n}{3} + \frac{2n}{3^2} + \frac{2n}{3^3} + \cdots + \frac{2n}{3^n} \in O(n)$.

Problem 29.3
Show that $n^2 + 2n \in O(2^n)$.

Problem 29.4
a. Show that $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \ln n, \quad n \geq 2$.
b. Use part a. to show that for $n \geq 3$

$$1 + \frac{1}{2} + \cdots + \frac{1}{n} \leq \ln n.$$

c. Use b. to show that $n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} \in O(n \ln n)$.

Problem 29.5
Show that $2^n \in O(n!)$.

30 Θ- and Ω-Notations

The O-notation asymptotically bounds a function from above. When we have bounds from above and below, we use Θ notation. For a given function $g(n)$, we denote by $\Theta(g(n))$ to be the set of all functions f such that there exist positive constants C_1, C_2, and n_0 such that $C_1|g(n)| \leq |f(n)| \leq C_2|g(n)|$ for all $n \geq n_0$. If $f \in \Theta(g(n))$ we write $f(n) = \Theta(g(n))$.

Example 30.1
Show that $\frac{1}{2}n^2 - 3n = \Theta(n^2)$.

Solution.
Let C_1 and C_2 be positive constants such that

$$C_1 n^2 \leq \frac{1}{2}n^2 - 3n \leq C_2 n^2.$$

This is equivalent to

$$C_1 \leq \frac{1}{2} - \frac{3}{n} \leq C_2.$$

Since $\frac{1}{2} - \frac{3}{n} \leq \frac{1}{2}$ for all $n \geq 1$, we choose $C_2 \geq \frac{1}{2}$. Since $\frac{1}{2} - \frac{3}{n} \geq \frac{1}{4}$ for all $n \geq 12$, we choose $C_1 \leq \frac{1}{4}$. Finally, we choose $n_0 = 12$. ■

Example 30.2
Show that $6n^3 \neq \Theta(n^2)$.

Solution.
We use the argument by contradiction. Suppose that $6n^3 = \Theta(n^2)$. Then there exist positive constants C_1, C_2 and n_0 such that

$$C_1 n^2 \leq 6n^3 \leq C_2 n^2$$

for all $n \geq n_0$. The right-hand side inequality yields $6n \leq C_2$ for $n \geq n_0$. This says that the left-hand side can be made as large as we want whereas the right-hand side is fixed. A contradiction. ■

Theorem 30.1
For given two functions $f(n)$ and $g(n)$, $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $g(n) = O(f(n))$.

Proof.
Suppose that $f(n) = \Theta(g(n))$. Then there exist positive constants C_1, C_2, and n_0 such that $C_1|g(n)| \leq |f(n)| \leq C_2|g(n)|$ for all $n \geq n_0$. The left-hand side inequality implies that $g(n) = O(f(n))$ whereas the right-hand side inequality implies that $f(n) = O(g(n))$. Now go backward for the converse. ■

Just as O provides an asymptotic upper bound on a function, $\Omega-$notation provides an asymptotic lower bound. For a given function $g(n)$, let $\Omega(g(n))$ denote the set of all funtions $f(n)$ such that there exist positive constants C and n_0 such that $C|g(n)| \leq |f(n)|$ for all $n \geq n_0$. For $f(n) \in \Omega(g(n))$ we write $f(n) = \Omega(g(n))$.

Example 30.3
Show that $\log_2 n! = \Omega(n \log_2 n)$.

Solution.
Since $(n!)^2 \geq n^n$ for all $n \geq 1$ we find $n \log_2 n \leq 2 \log_2 n!$. That is, $\frac{1}{2} n \log_2 n \leq \log_2 n!$ for $n \geq 1$. This says that $\log_2 n! = \Omega(n \log_2 n)$. ■

Theorem 30.2
For given two functions $f(n)$ and $g(n)$, $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.

Proof.
Suppose first that $f(n) = \Theta(g(n))$. Then there exist positive constants C_1, C_2 and n_0 such that $C_1|g(n)| \leq |f(n)| \leq C_2|g(n)|$ for $n \geq n_0$. The right-hand side inequality implies that $f(n) = O(g(n))$ whereas the left-hand side inequality implies that $f(n) = \Omega(g(n))$.
Conversely, suppose that $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$. Then there exist constants C_1, C_2, n_1 and n_2 such that $|f(n)| \leq C_2|g(n)|$ for $n \geq n_2$ and $C_1|g(n)| \leq |f(n)|$ for $n \geq n_1$. Let $n_0 = max\{n_1, n_2\}$. Then for $n \geq n_0$ we have $C_1|g(n)| \leq |f(n)| \leq C_2|g(n)|$. That is, $f(n) = \Theta(g(n))$. ■

Example 30.4
Let $f(n)$ and $g(n)$ be two given functions. We say that $f(n) = o(g(n))$ if and only if $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.
a. Show that if $f(n) = o(g(n))$ then $f(n) = O(g(n))$.
b. Find two functions $f(n)$ and $g(n)$ such that $f(n) = O(g(n)$ but $f(n) \neq o(g(n))$.

Solution.
a. Suppose that $f(n) = o(g(n))$. Then there is a positive integer n_0 such that $|\frac{f(n)}{g(n)}| \leq 1$ for $n \geq n_0$. That is, $|f(n)| \leq |g(n)|$ for all $n \geq n_0$. Hence, $f(n) = O(g(n))$.
b. Let $f(n) = 2n^2$ and $g(n) = n^2$. ■

Fundamentals of Counting and Probability Theory

The major goal of this chapter is to establish several techniques for counting large finite sets without actually listing their elements. Also, the fundamentals of probability theory are discussed.

31 Elements of Counting

For a set X, $|X|$ denotes the number of elements of X. It is easy to see that for any two sets A and B we have the following result known as the **Inclusion - Exclusion Principle**

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Indeed, $|A|$ gives the number of elements in A including those that are common to A and B. The same holds for $|B|$. Hence, $|A| + |B|$ includes twice the number of common elements. Hence, to get an accurate count of the elements of $A \cup B$, it is necessary to subtract $|A \cap B|$ from $|A| + |B|$.
Note that if A and B are disjoint then $|A \cap B| = 0$ and consequently $|A \cup B| = |A| + |B|$.

Example 31.1 *(The Addition Rule)*
Show by induction on n, that if $\{A_1, A_2, \cdots, A_n\}$ is a collection of pairwise disjoint sets then

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

Solution.
Basis of induction: For $n = 2$ the result holds by the Inclusion-Exclusion

Principle.
Induction hypothesis: Suppose that for any collection $\{A_1, A_2, \cdots, A_n\}$ of pairwise disjoint sets we have

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

Induction step: Let $\{A_1, A_2, \cdots, A_n, A_{n+1}\}$ be a collection of pairwise disjoint sets. Since $(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1} = (A_1 \cap A_{n+1}) \cup \cdots \cup (A_n \cap A_{n+1}) = \emptyset$, by the Inclusion-Exclusion Principle and the induction hypothesis we have

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| &= |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| \\ &= |A_1| + |A_2| + \cdots + |A_n| + |A_{n+1}| \quad \blacksquare \end{aligned}$$

Example 31.2
A total of 35 programmers interviewed for a job; 25 knew FORTRAN, 28 knew PASCAL, and 2 knew neither languages. How many knew both languages?

Solution.
Let A be the group of programmers that knew FORTRAN, B those who knew PASCAL. Then $A \cap B$ is the group of programmers who knew both languages. By the Inclusion-Exclusion Principle we have

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

That is,

$$33 = 25 + 28 - |A \cap B|.$$

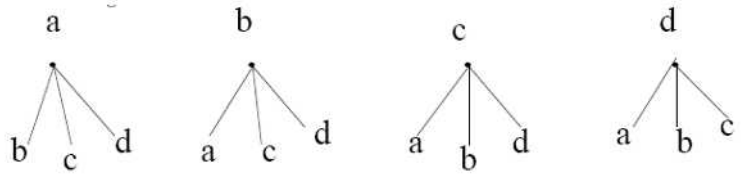
Solving for $|A \cap B|$ we find $|A \cap B| = 20$. $\blacksquare$
Another important rule of counting is the **multiplication rule**. It states that if a decision consists of k steps, where the first step can be made in n_1 different ways, the second step in n_2 ways, $\cdots$, the kth step in n_k ways, then the decision itself can be made in $n_1 n_2 \cdots n_k$ ways.

Example 31.3
a. How many possible outcomes are there if 2 distinguishable dice are rolled?
b. Suppose that a state's license plates consist of 3 letters followed by four digits. How many different plates can be manufactured? (no repetitions)

Solution.
a. By the multiplication rule there are $6 \times 6 = 36$ possible outcomes.
b. By the multiplication rule there are $26 \times 25 \times 24 \times 10 \times 9 \times 8 \times 7$ possible license plates. ■

Example 31.4
Let $\Sigma = \{a, b, c, d\}$ be an alphabet with 4 letters. Let Σ^2 be the set of all words of length 2 with letters from Σ. Find the number of all words of length 2 where the letters are not repeated. First use the product rule. List the words by means of a **tree diagram**.

Solution.
By the multiplication rule there are $4 \times 3 = 12$ different words. Constructing a tree diagram



we find that the words are

$$\{ab, ac, ad, ba, bc, bd, ca, cb, cd, da, db, dc\}\blacksquare$$

An **r-permutation** of n objects, in symbol $P(n, r)$, is an ordered selection of r objects from a given n objects.

Example 31.5
a. Use the product rule to show that $P(n, r) = \frac{n!}{(n-r)!}$.
b. Find all possible 2-permutations of the set $\{1, 2, 3\}$.

Solution.
a. We can treat a permutation as a decision with r steps. The first step can be made in n different ways, the second in $n - 1$ different ways, ..., the rth in $n - r + 1$ different ways. Thus, by the multiplication rule there are $n(n-1)\cdots(n-r+1)$ r-permutations of n objects. That is, $P(n, r) = n(n-1)\cdots(n-r+1) = \frac{n!}{(n-r)!}$.
b. $P(3, 2) = \frac{3!}{(3-2)!} = 6$. ■

Example 31.6
How many license plates are there that start with three letters followed by 4 digits (no repetitions)?

Solution.
$P(26,3) \cdot P(10,4) = 78,624,000$. ■

An **r-combination** of n objects, in symbol $C(n,r)$, is an unordered selection of r of the n objects. Thus, $C(n,r)$ is the number of ways of choosing r objects from n given objects without taking order in account. But the number of different ways that r objects can be ordered is $r!$. Since there are $C(n,r)$ groups of r objects from a given n objects, the number of ordered selection of r objects from n given objects is $r!C(n,r) = P(n,r)$. Thus

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

Example 31.7
In how many different ways can a hand of 5 cards be selected from a deck of 52 cards?(no repetition)

Solution.
$C(52,5) = 2,598,960$. ■

Example 31.8
Prove the following identities:
a. $C(n,0) = C(n,n) = 1$ and $C(n,1) = C(n,n-1) = n$.
b. Symmetry property: $C(n,r) = C(n,n-r), r \leq n$.
c. Pascal's identity: $C(n+1,k) = C(n,k-1) + C(n,k), n \geq k$.

Solution.
a. Follows immediately from the definition of of $C(n,r)$.
b. Indeed, we have

$$\begin{aligned} C(n,n-r) &= \frac{n!}{(n-r)!(n-n+r)!} \\ &= \frac{n!}{r!(n-r)!} \\ &= C(n,r) \end{aligned}$$

c.

$$\begin{aligned} C(n,k-1)+C(n,k) &= \frac{n!}{(k-1)!(n-k+1)!}+\frac{n!}{k!(n-k)!} \\ &= \frac{n!k}{k!(n-k+1)!}+\frac{n!(n-k+1)}{k!(n-k+1)!} \\ &= \frac{n!}{k!(n-k+1)!}(k+n-k+1) \\ &= \frac{(n+1)!}{k!(n+1-k)!}=C(n+1,k) \quad \blacksquare \end{aligned}$$

Pascal's identity allows one to construct the following triangle known as Pascal's triangle (for $n=4$) as follows

$$\begin{array}{ccccccccc} 1 & & & & & & & & \\ 1 & \to & 1 & & & & & & \\ 1 & \to & 2 & \to & 1 & & & & \\ 1 & \to & 3 & \to & 3 & \to 1 & & & \\ 1 & \to & 4 & \to & 6 & \to 4 & \to & 1 \end{array}$$

The following theorem provides an expansion of $(x+y)^n$ where n is a non-negative integer.

Theorem 31.1 *(Binomial Theorem)*
Let x and y be variables, and let n be a positive integer. Then

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

where $C(n,k)$ is called the **binomial coefficient**.

Proof.
The proof is by induction.

Basis of induction: For $n=1$ we have

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

Induction hypothesis: Suppose that the theorem is true for n.
Induction step: Let us show that it is still true for $n+1$. That is

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

Indeed, we have

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n = x(x+y)^n + y(x+y)^n \\
&= x\sum_{k=0}^{n} C(n,k)x^{n-k}y^k + y\sum_{k=0}^{n} C(n,k)x^{n-k}y^k \\
&= \sum_{k=0}^{n} C(n,k)x^{n-k+1}y^k + \sum_{k=0}^{n} C(n,k)x^{n-k}y^{k+1} \\
&= C(n,0)x^{n+1} + C(n,1)x^n y + C(n,2)x^{n-1}y^2 \\
&+ \cdots + C(n,n)xy^n + C(n,0)x^n y \\
&+ C(n,1)x^{n-1}y^2 + \cdots + C(n,n-1)xy^n \\
&+ C(n,n)y^{n+1} \\
&= C(n+1,0)x^{n+1} + C(n+1,1)x^n y + C(n+1,2)x^{n-1}y^2 \\
&+ \cdots + C(n+1,n)xy^n + C(n+1,n+1)y^{n+1} \\
&= \sum_{k=0}^{n+1} C(n+1,k)x^{n-k+1}y^k.
\end{aligned}$$

Example 31.9
Expand $(x+y)^6$ using the binomial theorem.

Solution.
By the Binomial Theorem and Pascal's triangle we have

$$(x+y)^6 = x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6 \blacksquare$$

Example 31.10
a. Show that $\sum_{k=0}^{n} C(n,k) = 2^n$.
b. Show that $\sum_{k=0}^{n} (-1)^k C(n,k) = 0$.

Solution.
a. Letting $x = y = 1$ in the binomial theorem we find

$$2^n = (1+1)^n = \sum_{k=0}^{n} C(n,k).$$

b. This follows from the binomial theorem by letting $x = 1$ and $y = -1$ $\blacksquare$

Review Problems

Problem 31.1
a. How many ways can we get a sum of 4 or a sum of 8 when two distinguishable dice are rolled?
b. How many ways can we get a sum of 8 when two undistinguishable dice are rolled?

Problem 31.2
a. How many 4-digit numbers can be formed using the digits, $1, 2, \cdots, 9$ (with repetitions)? How many can be formed if no digit can be repeated?
b. How many different license plates are there that involve $1, 2$, or 3 letters followed by 4 digits (with repetitions)?

Problem 31.3
a. In how many ways can 4 cards be drawn, with replacement, from a deck of 52 cards?
b. In how many ways can 4 cards be drawn, without replacement, from a deck of 52 cards?

Problem 31.4
In how many ways can 7 women and 3 men be arranged in a row if the three men must always stand next to each other.

Problem 31.5
A menu in a Chinese restaurant allows you to order exactly two of eight main dishes as part of the dinner special. How many different combinations of main dishes could you order?

Problem 31.6
Find the coefficient of a^5b^7 in the binomial expansion of $(a - 2b)^{12}$.

Problem 31.7
Use the binomial theorem to prove that

$$3^n = \sum_{k=0}^{n} 2^k C(n, k).$$

32 Basic Probability Terms and Rules

Probability theory is one of the serious branches of mathematics with applications to many sciences, namely the theory of statistics. This section introduces the most basic ideas of probability.

An **experiment** is any operation whose outcomes cannot be predicted with certainty. The **sample space** S of an experiment is the set of all possible outcomes for the experiment. For example, if you roll a die one time then the experiment is the roll of the die. A sample space for this experiment is $S = \{1, 2, 3, 4, 5, 6\}$ where each digit represents a face of the die.

An **event** is any subset of a sample space. Thus, if S is the sample space then the collection of all possible events is the power set $\mathcal{P}(S)$.

The **Probability** of an event E is the measure of occurrence of E. It is a number between 0 and 1. If the event is impossible to occur then its probability is 0. If the occurrence is certain then the probability is 1. The closer to 1 the probability is, the more likely the event is. The probability of occurrence of an event E (called its **success**) will be denoted by $P(E)$. Thus, $0 \leq P(E) \leq 1$. If an event has no outcomes, that is as a subset of S if $E = \emptyset$ then $P(\emptyset) = 0$. On the other hand, if $E = S$ then $P(S) = 1$.

Example 32.1
Which of the following numbers cannot be the probability of some event? (a) 0.71 (b)-0.5 (c) 150% (d) $\frac{4}{3}$.

Solution.
(a) Yes. (b) No. Since the number is negative. (c) No since the number is greater than 1. (d) No. ■

Various probability concepts exist nowadays. The **classical** probability concept applies only when all possible outcomes are **equally likely**, in which case we use the formula

$$P(E) = \frac{number\ of\ outcomes\ favorable\ to\ event}{total\ number\ of\ outcomes} = \frac{|E|}{|S|},$$

where $|E|$ is the number of elements in E.

Example 32.2
What is the probability of drawing an ace from a well-shuffled deck of 52 playing cards?

Solution.
$P(Ace) = \frac{4}{52} = \frac{1}{13}$. ■

Example 32.3
What is the probability of rolling a 3 or a 4 with a fair die?

Solution.
$P(3\ or\ 4) = \frac{2}{6} = \frac{1}{3}$. ■

A major shortcoming of the classical probability concept is its limited applicability, for there are many situations in which the various outcomes cannot all be regarded as equally likely. This would be the case, for instance, when we wonder whether a person will get a raise or when we want to predict the outcome of an election. A widely used probability concept is the **estimated** probability which uses the relative frequency of an event and is given by the formula:

$$P(E) = Relative\ \ frequency = \frac{f}{n},$$

where f is the frequency of the event and n is the size of the sample space.

Example 32.4
Records show (over a period of time) that 468 of 600 jets from Dallas to Phoenix arrived on time. Estimate the probability that any one jet from Dallas to Phoenix will arrive on time.

Solution.
$P(E) = \frac{f}{n} = \frac{468}{600} = \frac{39}{50}$ ■

We define the probability of nonoccurrence of an event E (called its **failure**) by the formula

$$P(E^c) = 1 - P(E).$$

Note that

$$P(E) + P(E^c) = 1.$$

Example 32.5
The probability that a college student without a flu shot will get the flu is 0.45. What is the probability that a college student without the flu shot will not get the flu?

Solution.
The probability is $1 - 0.45 = .55$. ■

Next, we discuss some of the rules of probability. The **union** of two events A and B is the event $A \cup B$ whose outcomes are either in A or in B. The **intersection** of two events A and B is the event $A \cap B$ whose outcomes are outcomes of both events A and B. Two events A and B are said to be **mutually exclusive** if they have no outcomes in common. In this case $A \cap B = \emptyset$.

Example 32.6
If A and B are mutually exclusive then what is $P(A \cap B)$?

Solution.
$P(\emptyset) = 0$. ■

Theorem 32.1
For any events A and B the probability of $A \cup B$ is given by the addition rule

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

If A and B are mutually exclusive then by Example 32.6 the above formula reduces to

$$P(A \cup B) = P(A) + P(B).$$

Proof.
By the Inclusion-Exclusion Principle we have

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Thus,

$$\begin{aligned} P(A \cup B) =& \frac{|A \cup B|}{|S|} \\ =& \frac{|A|}{|S|} + \frac{|B|}{|S|} - \frac{|A \cap B|}{|S|} \\ =& P(A) + P(B) - P(A \cap B) \blacksquare \end{aligned}$$

Example 32.7
For any event E of a sample space S show that $P(E) = \sum_{x \in E} P(x)$.

Solution.
This follows from the previous theorem ■

Example 32.8
$M\&M$ plain candies come in a variety of colors. According to the manufacturer, the color distribution is:
(a) Orange: 15% (b) Green: 10% (c) Red: 20% (d) Yellow: 20% (e) Brown: 30% (f) Tan: 5%.
Suppose you have a large bag of plain candies and you reach in and take one candy at random. Find

1. P(orange candy Or tan candy). Are these outcomes mutually exclusive?

2. P(not brown candy).

Solution.
1. P(orange candy Or tan candy) = .15 + .05 = .2 = 20%. The outcomes are mutually exclusive.
2. P(not brown candy) = 1 − .3 = .7 = 70% ■

Example 32.9
If A is the event "drawing an ace" from a deck of cards and B is the event "drawing a spade". Are A and B mutually exclusive? Find $P(A \cup B)$.

Solution.
The events are not mutually exclusive since there is an ace that is also a spade.

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{4}{52} + \frac{13}{52} - \frac{1}{52} = 31\%\blacksquare$$

Now, given two events A and B belonging to the same sample space S. The **conditional probability** $P(A|B)$ denotes the probability that event A will occur given that event B has occurred. It is given by the formula

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

Example 32.10
Consider the experiment of tossing two dice. What is the probability that the sum of two dice equals six given that the first die is a four?

Solution.
The possible outcomes of our experiment are

$$\{(4,1),(4,2),(4,3),(4,4),(4,5),(4,6)\}.$$

Thus, the probability that the sum is six given that the first die is four is $\frac{1}{6}$. Assuming that the experiment consists of tossing the two dice then by letting B be the event that the first die is 4 and A be the event that the sum of the two dice is 6 then

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{36}}{\frac{6}{36}} = \frac{1}{6} \blacksquare$$

If $P(A|B) = P(A)$, we say that the two events A and B are **independent**. That is, the occurrence of A is independent whether or not B occurs. If two events are not independent, we say that they are **dependent**.

Example 32.11
Show that A and B are independent if and only if

$$P(A \cap B) = P(A) \cdot P(B).$$

Solution.
Suppose that A and B are independent. Then $P(A) = P(A|B) = \frac{P(A \cap B)}{P(B)}$. That is, $P(A \cap B) = P(A) \cdot P(B)$. Conversely, if $P(A \cap B) = P(A) \cdot P(B)$ then $P(A|B) = \frac{P(A \cap B)}{P(B)} = P(A)$. $\blacksquare$

Example 32.12
You roll two fair dice: a green one and a red one.
a. Are the outcomes on the dice independent?
b. Find P(5 on green die and 3 on red die).
c. Find P(3 on green die and 5 on red die).
d. Find P((5 on green die and 3 on red die) or (3 on green die and 5 on red die)).

Solution.
a. Yes.
b. P(5 on green die and 3 on red die) $= \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$.
c. P(3 on green die and 5 on red die) $= \frac{1}{36}$.
d. P((5 on green die and 3 on red die) or (3 on green die and 5 on red die)) $= \frac{1}{36} + \frac{1}{36} = \frac{1}{18}$. ■

Example 32.13
Show that

$$P(B|A) = \frac{P(B) \cdot P(A|B)}{P(A)}.$$

Solution.
This follows from the fact that $P(A \cap B) = P(B \cap A)$ and the formula of $P(A|B)$ given above. ■

Example 32.14
Prove Bayes' Theorem

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A^c)P(A^c)}.$$

Solution.
Note first that $\{A^c \cap B, A \cap B\}$ form a partition of B. Thus,

$$P(B) = P(A \cap B) + P(A^c \cap B).$$

Now by the previous example we have

$$\begin{aligned} P(A|B) =& \frac{P(A) \cdot P(B|A)}{P(B)} \\ =& \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A^c)P(A^c)} \end{aligned}$$ ■

Example 32.15
Consider two urns. The first contains two white and seven black balls and the second contains five white and six black balls. We flip a fair coin and then draw a ball from the first urn or the second urn depending on whether the outcome was head or tail. What is the conditional probability that the outcome of the toss was head given that a white ball was selected?

Solution.
Let W be the event that a white ball is drawn, and let H be the event that the coin comes up heads. The desired probability $P(H|W)$ may be calculated as follows:

$$\begin{aligned} P(H|W) =& \frac{P(H \cap W)}{P(W)} \\ =& \frac{P(W|H)P(H)}{P(W)} \\ =& \frac{P(W|H)P(H)}{P(W|H)P(H) + P(W|H^c)P(H^c)} \\ =& \frac{\frac{2}{9}\frac{1}{2}}{\frac{2}{9}\frac{1}{2} + \frac{5}{11}\frac{1}{2}} \\ =& \frac{22}{67} \blacksquare \end{aligned}$$

It frequently occurs that in performing an experiment we are mainly interested in some functions of the outcome as opposed to the outcome itself. For example, in tossing dice we are interested in the sum of the dice and are not really concerned about the actual outcome. These real-valued functions defined on the sample space are known as **random variables.** If the range is a finite subset of $\mathbb{N}$ then the random variable is called **discrete**. Otherwise, the random variable is said to be **continuous.** Discrete random variables are usually the result of a count whereas a continuous random variable is usually the result of a measurement.
A **probability distribution** is a correspondence that assigns probabilities to the values of a random variable. The graph of a probability distribution is called a **histogram**.

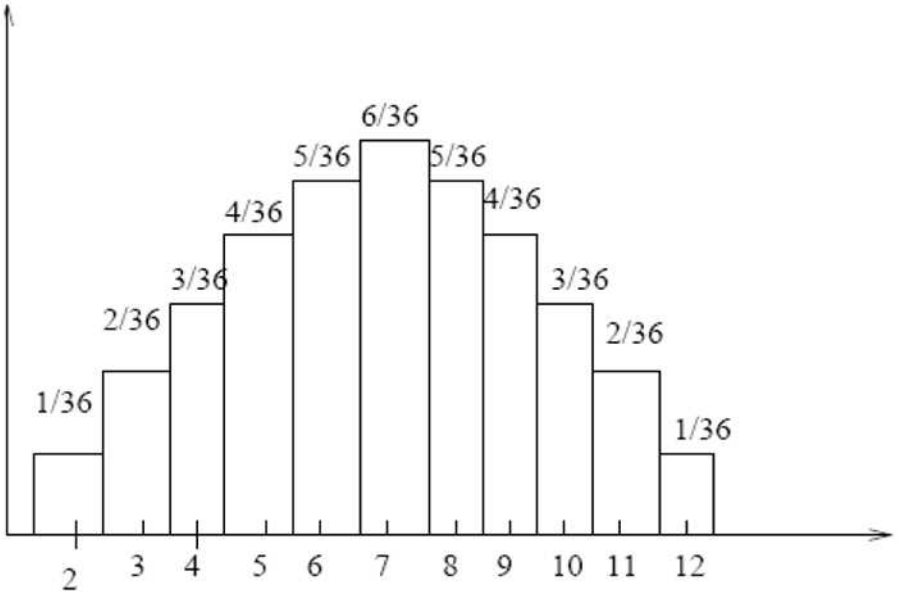
Example 32.16
Let f denote the random variable that is defined as the sum of two fair dice. Find the probability distribution of f.

Solution.
$P(f = 2) = P(\{(1, 1)\}) = \frac{1}{36}$,
$P(f = 3) = P(\{(1, 2), (2, 1)\}) = \frac{2}{36}$,
$P(f = 4) = P(\{(1, 3), (2, 2), (3, 1)\}) = \frac{3}{36}$,
$P(f = 5) = P(\{(1, 4), (2, 3), (3, 2), (4, 1)\}) = \frac{4}{36}$,

$P(f = 6) = P(\{(1, 5, (5, 1), (2, 4), (4, 2), (3, 3)\}) = \frac{5}{36}$,
$P(f = 7) = P(\{(1, 6), (6, 1), (2, 5), (5, 2), (4, 3), (3, 4)\}) = \frac{6}{36}$,
$P(f = 8) = P(\{(2, 6), (6, 2), (3, 5), (5, 3), (4, 4)\}) = \frac{5}{36}$,
$P(f = 9) = P(\{(3, 6), (6, 3), (4, 5), (5, 4)\}) = \frac{4}{36}$,
$P(f = 10) = P(\{(4, 5), (5, 4), (5, 5)\}) = \frac{3}{36}$,
$P(f = 11) = P(\{(5, 6), (6, 5)\}) = \frac{2}{36}$,
$P(f = 12) = P(\{(6, 6)\}) = \frac{1}{36}$. ■

Example 32.17
Construct the histogram of the random variable of Example 32.19.

Solution.



■

For a discrete random variable f we define the **expected value** (or **mean**) of f by the formula

$$E(f) = \sum_{x \in S} f(x)P(x)$$

In other words, $E(f)$ is a weighted average of the possible values that f can take on, each value being weighted by the probability that f assumes that value.

Example 32.18
Find $E(f)$ where f is the outcome when we roll a fair die.

Solution.
Since $P(1) = P(2) = \cdots = P(6) = \frac{1}{6}$ we find

$$E(f) = 1(\frac{1}{6}) + 2(\frac{1}{6}) + \cdots + 6(\frac{1}{6}) = \frac{7}{2} \blacksquare$$

Another quantity of interest is the **variance** of a random variable f, denoted by $Var(f)$, which is defined by

$$Var(f) = E[(f - E(f))^2].$$

In other words, the variance measures the expected square of the deviation of f from its expected value. The **standard deviation** of a random variable f is the quantity defined to be the square root of the variance.

Example 32.19
Show that if f and g are random variables then $E(f + cg) = E(f) + cE(g)$ where c is a constant.

Solution.
Indeed,

$$\begin{aligned} E(f + cg) =& \sum_{x \in S} (f + cg)(x)P(x) \\ =& \sum_{x \in S} f(x)P(x) + c \sum_{x \in S} g(x)P(x) \\ =& E(f) + cE(g) \blacksquare \end{aligned}$$

Theorem 32.2

$$Var(f) = E(f^2) - (E(f))^2.$$

Proof.
Indeed, using the previous example we have

$$\begin{aligned} Var(f) =& E(f^2 - 2E(f)f + (E(f))^2) \\ =& E(f^2) - 2E(f)E(f) + (E(f))^2 \\ =& E(f^2) - (E(f))^2 \blacksquare \end{aligned}$$

Example 32.20
Calculate $Var(f)$ when f represents the outcome when a fair die is rolled.

Solution.
First note that

$$E(f^2) = (f(1))^2 P(1) + \cdots + (f(6))^2 P(6) = \frac{91}{6}.$$

By the above theorem we have

$$Var(f) = E(f^2) - (E(f))^2 = \frac{91}{6} - (\frac{7}{2})^2 = \frac{35}{12} \blacksquare$$

Review Problems

Problem 32.1
What is the probability of drawing a red card from a well-shuffled deck of 52 playing cards?

Problem 32.2
If we roll a fair die, what are the probabilities of getting
a. a 1 or a 6;
b. an even number?

Problem 32.3
A department store's records show that 782 of 920 women who entered the store on a Saturday afternoon made at least one purchase. Estimate the probability that a woman who enters the store on a Saturday afternoon will make at least one purchase.

Problem 32.4
Which of the following are mutually exclusive? Explain your answers.
a. A driver getting a ticket for speeding and a ticket for going through a red light.
b. Being foreign-born and being President of the United States.

Problem 32.5
If A and B are the events that a consumer testing service will rate a given stereo system very good or good, $P(A) = 0.22$, $P(B) = 0.35$. Find
a. $P(A^c)$;
b. $P(A \cup B)$;
c. $P(A \cap B)$.

Problem 32.6
If the probabilities are 0.20, 0.15, and 0.03 that a student will get a failing grade in Statistics, in English, or in both, what is the probability that the student will get a failing grade in at least one of these subjects?

Problem 32.7
If the probability that a research project will be well planned is 0.60 and the probability that it will be well planned and well executed is 0.54, what is the probability that a well planned research project will be well executed?

Problem 32.8
Given three events A, and B such that $P(A) = 0.50, P(B) = 0.30$, and $P(A \cap B) = 0.15$. Show that the events A and B are independent.

Problem 32.9
There are 16 equally likely outcomes by flipping four coins. Let f represent the number of heads. Find the probability distribution and graph the corresponding histogram.

33 Binomial Random Variables

In this section we discuss an important example of a discrete random variable. **Binomial experiments** are problems that consist of a fixed number of trials n, with each trial having exactly two possible outcomes: **Success** and **failure.** The probability of a success is denoted by $p = P(S)$ and that of a failure by $q = P(F)$. Moreover, p and q are related by the formula

$$p + q = 1.$$

Also, we assume that the trials are **independent**, that is what happens in one trial does not affect the probability of a success in any other trial. The central question of a binomial experiment is to find the probability of r successes out of n trials. Now, anytime we make selections from a population without replacement, we do not have independent trials. For example, selecting a ball from a box that contains balls of two different colors. If the selection is without replacement then the trials are dependent.

Example 33.1
The registrar of a college noted that for many years the withdrawal rate from an introductory chemistry course has been 35% each term. We wish to find the probability that 55 students out of 80 will complete the course.

a. What makes a trial?
b. What is a success? a failure?
c. What are the values of n, p, q, r?

Solution.
a. The decision of each student to withdraw or complete the course can be thought of as a trial. Thus, there are a total of 80 trials.
b. S = completing the course, F = withdrawing from course.
c. $n = 80, p = .65, q = .35, r = 55$. ■

Example 33.2
Harper's Index states that 10% of all adult residents in Washington D.C., are lawyers. For a random sample of 15 adult Washington, D.C., residents, we want to find the probability that 3 are lawyers.

a. What makes a trial?

b. What is a success? a failure?
c. What are the values of n, p, q, r?

Solution.
a. A trial is whether an adult resident of Washington, D.C. is a lawyer or not.
b. S = being a lawyer, F = not being a lawyer.
c. $n = 15, p = .1, q = .9, r = 3$. ■

As mentioned earlier, the central problem of a binomial experiment is to find the probability of r successes out of n independent trials. We next see how to find these probabilities.
Recall from Section 31 the formula for finding the number of combinations of n distinct objects taken r at a time

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

We call the number $C(n, r)$ the **binomial coefficient**. One commonly used procedure for finding these coefficients is by means of **Pascal's triangle.**

Now, the probability of r successes out of n independent trials is given by the **binomial distribution formula**

$$P(r) = C(n, r)p^r q^{n-r}$$

where $p = P(S)$ and $q = P(F) = 1 - p$. The validity of the above equation may be verified by first noting that the probability of any particular sequence of the n outcomes with r successes and $n-r$ failures is, by the independence of trials, $p^r(1-p)^{n-r}$. Since $C(n, r)$ counts the number of outcomes that have r successes and $n - r$ failures, the equation above follows.

Example 33.3
Find the probability that in tossing a fair coin three times there will appear (a) 3 heads, (b)2 heads and 1 tail, (c) 2 tails and 1 head, and (d) 3 tails.

Solution.
a. $P(3) = C(3, 3)(.5)^3(.5)^{3-3} = \frac{1}{8}$.
b. $P(2) = C(3, 2)(.5)^2(.5) = \frac{3}{8}$.
c. $P(1) = C(3, 1)(.5)(.5)^2 = \frac{3}{8}$.
d. $P(0) = C(3, 0)(.5)^3 = \frac{1}{8}$ ■

Example 33.4
The probability that an entering college student will graduate is 0.4. Determine the probability that out of 5 students (a) none, (b) 1, (c) at least 1, (d) all will graduate.

Solution.
(a) $C(5,0)(.6)^5$.
(b) $C(5,1)(.4)(.6)^4$.
(c) $1 - C(5,0)(.6)^5$.
(d) $C(5,5)(.4)^5$. ■

Example 33.5
Find the probability of guessing correctly at least 6 of the 10 answers on a true-false examination.

Solution.
$P(6) + P(7) + P(8) + P(9) + P(10)$. ■

We next derive formulas for finding the expected value and standard deviation for the binomial random variable.

Theorem 33.1
a. The mean of a binomial random variable is given by $\mu = np$.
b. The variance of a binomial random variable is given by $\sigma^2 = npq$.

Proof.
a. Using the definition of μ we have

$$\begin{aligned}
\mu =& \sum_{i=0}^{n} iP(i) \\
=& \sum_{i=1}^{n} iC(n,i)p^i q^{n-i} \\
=& np \sum_{i=1}^{n} \frac{(n-1)!}{(i-1)!(n-i)} p^{i-1} q^{n-i} \\
=& np \sum_{i=1}^{n} \frac{(n-1)!}{i!(n-i)} p^i q^{n-i-1} \\
=& np \sum_{i=0}^{n-1} C(n-1,i)p^i q^{n-i-1} \\
=& np \sum_{i=0}^{n-1} \\
=& np(p+q)^{n-1} = np.
\end{aligned}$$

b. Note first that $i^2 = i(i-1) + i$. Then

$$\begin{aligned}
E(X^2) =& \sum_{i=0}^{n} i^2 P(i) \\
=& \sum_{i=0}^{n} i(i-1)C(n,i)p^i q^{n-i} + \mu \\
=& \sum_{i=2}^{n} \frac{n!}{(n-i)!(i-2)!} p^i q^{n-i} + \mu \\
=& n(n-1)p^2 \sum_{i=2}^{n} \frac{(n-2)!}{(n-i)!(i-2)!} p^i q^{n-i} + \mu \\
=& n(n-1)p^2 \sum_{j=0}^{n-2} C(n-2,j)p^j q^{n-2-j} + \mu \\
=& n(n-1)p^2(p+q)^{n-2} + \mu \\
=& n(n-1)p^2 + \mu
\end{aligned}$$

It follows that

$$\begin{aligned}\sigma^2 =& E(X^2) - \mu^2 \\ =& n(n-1)p^2 + np - n^2p^2 \\ =& npq \ \blacksquare\end{aligned}$$

Review Problems

Problem 33.1
At Community Hospital, the nursing staff is large enough so that 80% of the time a nurse can respond to a room call within 3 minutes. Last night there were 73 room calls. We wish to find the probability nurses responded to 62 of them within 3 minutes.

a. What makes a trial?
b. What is a success? a failure?
c. What are the values of n, p, q, r?

Problem 33.2
Find the probability that in a family of 4 children there will be (a) at least 1 boy and (b) at least 1 boy and 1 girl. Assume that the probability of a male birth is $\frac{1}{2}$.

Problem 33.3
An insurance salesperson sells policies to 5 men, all of identical age and in good health. According to the actuarial tables, the probability that a man of this particular age will be alive 30 years is $\frac{2}{3}$. Find the probability that in 30 years (a) all 5 men, (b) at least 3 men, (c) only 2 men, (d) none will be alive.

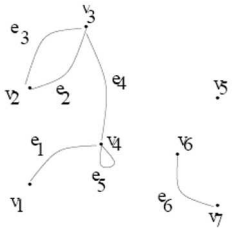
Elements of Graph Theory

In this chapter we present the basic concepts related to graphs and trees such as the degree of a vertex, connectedness, Euler and Hamiltonian circuits, isomorphisms of graphs, rooted and spanning trees.

34 Graphs, Paths, and Circuits

An **undirected graph** G consists of a set V_G of **vertices** and a set E_G of **edges** such that each edge $e \in E_G$ is associated with an unordered pair of vertices, called its **endpoints**.
A **directed graph** or **digraph** G consists of a set V_G of vertices and a set E_G of edges such that each edge $e \in E_G$ is associated with an ordered pair of vertices.
We denote a graph by $G = (V_G, E_G)$.
Two vertices are said to be **adjacent** if there is an edge connecting the two vertices. Two edges associated to the same vertices are called **parallel**. An edge incident to a single vertex is called a **loop.** A vertex that is not incident on any edge is called an **isolated** vertex. A graph with neither loops nor parallel edges is called a **simple** graph.

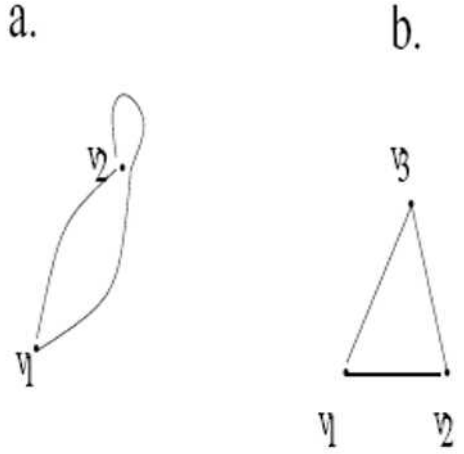
Example 34.1
Consider the following graph G



a. Find E_G and V_G.
b. List the isolated vertices.
c. List the loops.
d. List the parallel edges.
e. List the vertices adjacent to v_3..
f. Find all edges incident on v_4.

Solution.
a. $E_G = \{e_1, e_2, e_3, e_4, e_5, e_6\}$ and $V_G = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$.
b. There is only one isolated vertex, v_5.
c. There is only one loop, e_5.
d. $\{e_2, e_3\}$.
e. $\{v_2, v_4\}$.
f. $\{e_1, e_4, e_5\}$. ■

Example 34.2
Which one of the following graphs is simple.

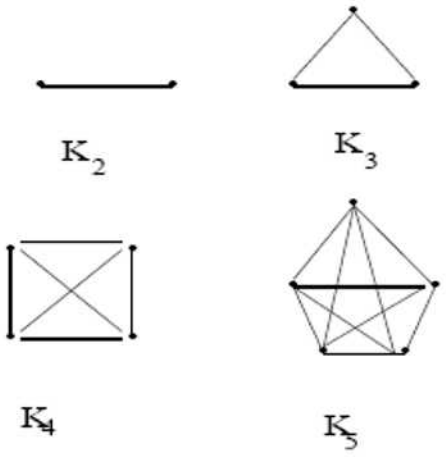


Solution.
a. G is not simple since it has a loop and parallel edges.
b. G is simple. ■

A **complete graph** on n vertices, denoted by K_n, is the simple graph that contains exactly one edge between each pair of distinct vertices.

Example 34.3
Draw K_2, K_3, K_4, and K_5.

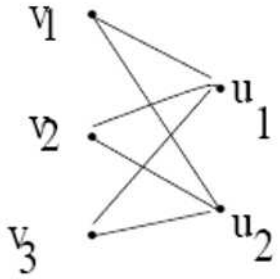
Solution.



■

A graph in which the vertices can be partitioned into two disjoint sets V_1 and V_2 with every edge incident on one vertex in V_1 and one vertex of V_2 is called **bipartite graph**.

Example 34.4
a. Show that the graph G is bipartite.



b. Show that K_3 is not bipartite.

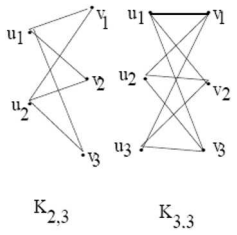
Solution.
a. Clear from the definition and the graph.
b. Any two sets of vertices of K_3 will have one set with at least two vertices. Thus, according to the definition of bipartite graph, K_3 is not bipartite. ■

A **complete bipartite graph** $K_{m,n}$, is the graph that has its vertex set partitioned into two disjoint subsets of m and n vertices, respectively. More-

over, there is an edge between two vertices if and only if one vertex is in the first set and the other vertex is in the second set.

Example 34.5
Draw $K_{2,3}, K_{3,3}$.

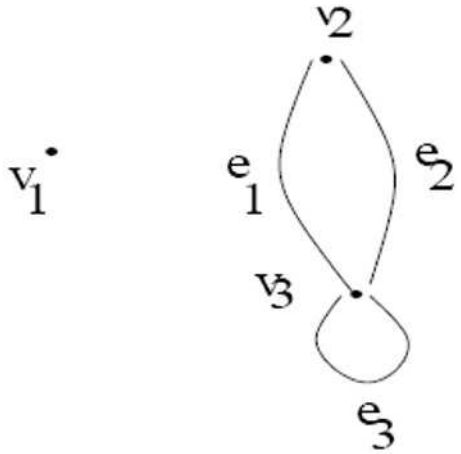
Solution.



■

The **degree** of a vertex v in an undirected graph, in symbol $deg(v)$, is the number of edges incident on it. By definition, a loop at a vertex contributes twice to the degree of that vertex. The **total degree of G** is the sum of the degrees of all the vertices of G.

Example 34.6
What are the degrees of the vertices in the following graph



Solution.
$deg(v_1) = 0, deg(v_2) = 2, deg(v_3) = 4$. ■

Theorem 34.1
For any graph $G = (V_G, E_G)$ we have

$$2|E_G| = \sum_{v \in V(G)} deg(v).$$

Proof.
Suppose that $V_G = \{v_1, v_2, \cdots, v_n\}$ and $|E_G| = m$. Let $e \in E_G$. If e is a loop then it contributes 2 to the total degree of G. If e is not a loop then let v_i and v_j denote the endpoints of e. Then e contributes 1 to $deg(v_i)$ and contributes 1 to the $deg(v_j)$. Therefore, e contributes 2 to the total degree of G. Since e was chosen arbitrarily, this shows that each edge of G contributes 2 to the total degree of G. Thus,

$$2|E_G| = \sum_{v \in V(G)} deg(v) \blacksquare$$

The following is easily deduced from the previous theorem.

Theorem 34.2
In any graph there are an even number of vertices of odd degree.

Proof.
Let $G = (V_G, E_G)$ be a graph. By the previous theorem, the sum of all the degrees of the vertices is $T = 2|E_G|$, an even number. Let E be the sum of the numbers $deg(v)$, each which is even and O the sum of numbers $deg(v)$ each which is odd. Then $T = E + O$. That is, $O = T - E$. Since both T and E are even, O is also even. This implies that there must be an even number of the odd degrees. Hence, there must be an even number of vertices with odd degree. ■

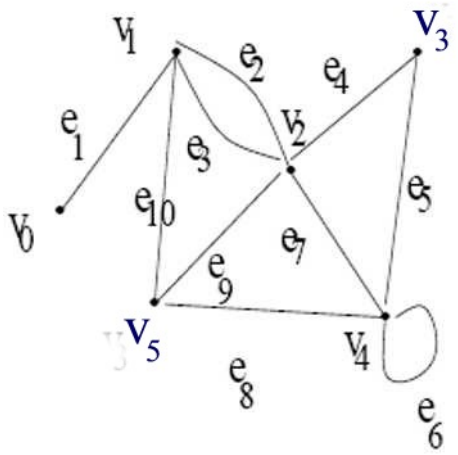
Example 34.7
Find a formula for the number of edges in K_n.

Solution.
Since G is complete, each vertex is adjacent to the remaining vertices. Thus, the degree of each of the n vertices is $n - 1$, and we have the sum of the degrees of all of the vertices being $n(n-1)$. By Theorem 34.1, $n(n-1) = 2|E_G|$.

This completes a proof of the theorem ■

In an undirected graph G a sequence P of the form $v_0e_1v_1e_2\cdots v_{n-1}e_nv_n$ with no edge repeated is called a **path of length n** or a path connecting v_0 to v_n. If P is a path such that $v_0 = v_n$ then it is called a **circuit** or a **cycle**. A path or circuit is **simple** if it does not contain the same vertex more than once. A graph that does not contain any circuit is called **acyclic**.

Example 34.8
In the graph below, determine whether the following sequences are paths, simple paths, circuits, or simple circuits.

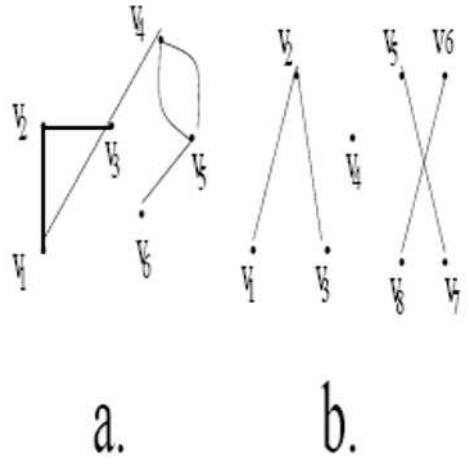


a. $v_0e_1v_1e_{10}v_5e_9v_2e_2v_1$.
b. $v_3e_5v_4e_8v_5e_{10}v_1e_3v_2$.
c. $v_1e_2v_2e_3v_1$.
d. $v_5e_9v_2e_4v_3e_5v_4e_6v_4e_8v_5$.

Solution.
a. a path (no repeated edge), not a simple path (repeated vertex v_1), not a circuit
b. a simple path
c. a simple circuit
d. a circuit, not a simple circuit (vertex v_4 is repeated) ■

An undirected graph is called **connected** if there is a path between every pair of distinct vertices of the graph. A graph that is not connected is said to be **disconnected**.

Example 34.9
Determine which graph is connected and which one is disconnected.



Solution.
a. Connected.
b. Disconnected since there is no path connecting the vertices v_1 and v_4. ■

A simple path that contains all edges of a graph G is called an **Euler path**. If this path is also a circuit, it is called an **Euler circuit.**

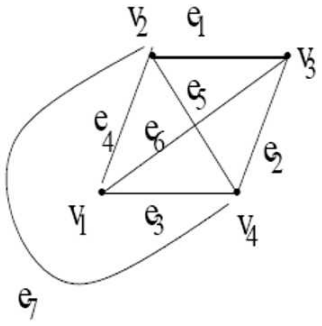
Theorem 34.3
If a graph G has an Euler circuit then every vertex of the graph has even degree.

Proof.
Let G be a graph with an Euler circuit. Start at some vertex on the circuit and follow the circuit from vertex to vertex, erasing each edge as you go along it. When you go through a vertex you erase one edge going in and one edge going out, or else you erase a loop. Either way, the erasure reduces the degree of the vertex by 2. Eventually every edge gets erased and all the vertices have degree 0. So all vertices must have had even degree to begin with. ■

It follows from the above theorem that if a graph has a vertex with odd degree then the graph can not have an Euler circuit.
The following provides a converse to the above theorem.

Theorem 34.4 *(Euler Theorem)*
If all the vertices of a connected graph have even degree, then the graph has an Euler circuit.

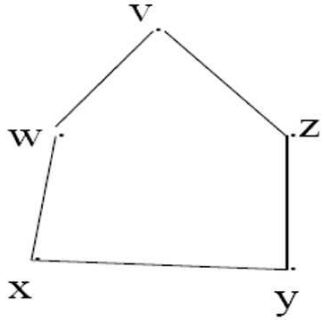
Example 34.10
Show that the following graph has no Euler circuit.



Solution.
Vertices v_1 and v_3 both have degree 3, which is odd. Hence, by the remark following the previous theorem, this graph does not have an Euler circuit. ■

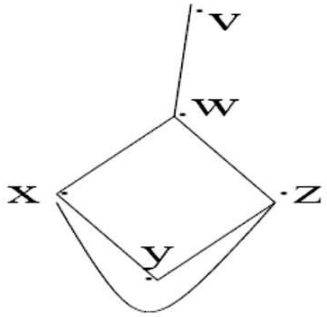
A path is called a **Hamiltonian path** if it visits every vertex of the graph exactly once. A circuit that visits every vertex exactly once except for the last vertex which duplicates the first one is called a **Hamiltonian circuit.**

Example 34.11
Find a Hamiltonian circuit in the graph



Solution.
vwxyzv ■

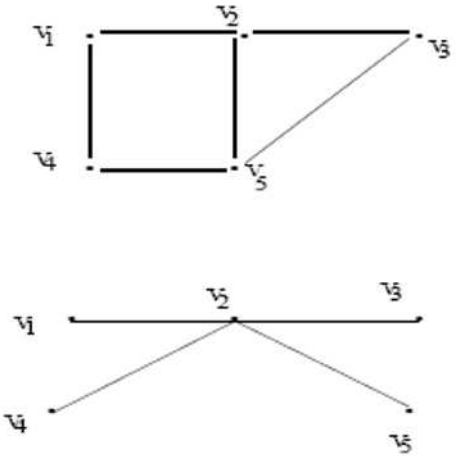
Example 34.12
Show that the following graph has a Hamiltonian path but no Hamiltonian circuit.



Solution.
$vwxyz$ is a Hamiltonian path. There is no Hamiltonian circuit since no cycle goes through v. ■

Review Problems

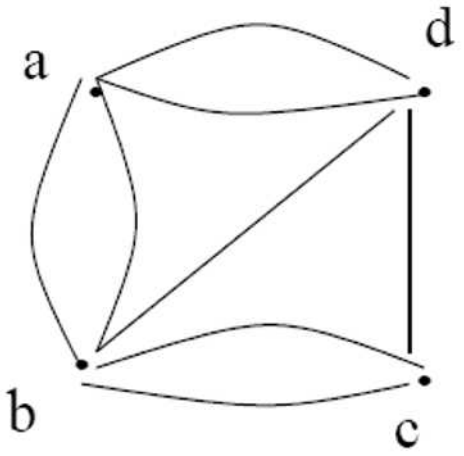
Problem 34.1
The **union** of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the graph $G_1 \cup G_2 = (V_1 \cup V_2, E_1 \cup E_2)$. The **intersection** of two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the graph $G_1 \cap G_2 = (V_1 \cap V_2, E_1 \cap E_2)$.
Find the union and the intersection of the graphs



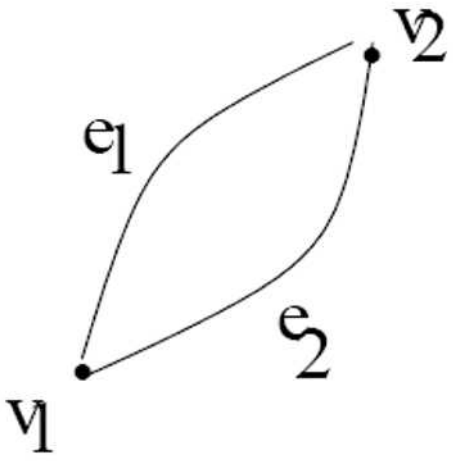
Problem 34.2
Graphs can be represented using matrices. The **adjacency** matrix of a graph G with n vertices is an $n \times n$ matrix A_G such that each entry a_{ij} is the number of edges connecting v_i and v_j. Thus, $a_{ij} = 0$ if there is no edge from v_i to v_j.
a. Draw a graph with the adjacency matrix

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

b. Use an adjacency matrix to represent the graph

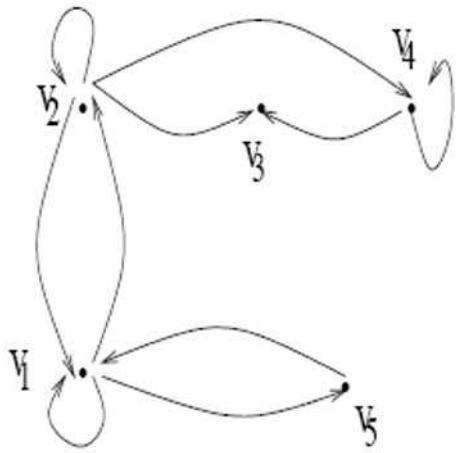


Problem 34.3
A graph $H = (V_H, E_H)$ is a **subgraph** of $G = (V_G, E_G)$ if and only if $V_H \subseteq V_G$ and $E_H \subseteq E_G$.
Find all nonempty subgraphs of the graph



When (u, v) is an edge in a directed graph G then u is called the **initial vertex** and v is called the **terminal vertex.** In a directed graph, the **in-degree** of a vertex v, denoted by $deg^-(v)$, is the number of edges with v as their terminal vertex. Similarly, the **out-degree** of v, denoted by $deg^+(v)$, is the number of edges with v as an initial vertex. Note that $deg(v) = deg^+(v) + deg^-(v)$.

Problem 34.4
Find the in-degree and out-degree of each of the vertices in the graph G with directed edges.

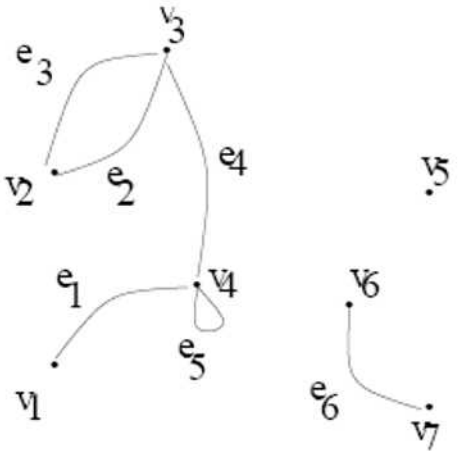


Problem 34.5
Show that for a digraph $G = (V_G, E_G)$ we have

$$|E_G| = \sum_{v \in V(G)} deg^-(v) = \sum_{v \in V(G)} deg^+(v).$$

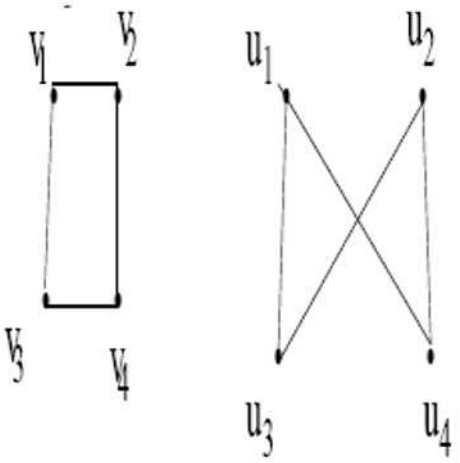
Another useful matrix representation of a graph is known as the **incidence matrix.** It is constructed as follows. We label the rows with the vertices and the columns with the edges. The entry for row v and column e is 1 if e is incident on v and 0 otherwise. If e is a loop at v we assign the value 2. It is easy to see that the sum of entries of each column is 2 and that the sum of entries of a row gives the degree of the vertex corresponding to that row.

Problem 34.6
Find the incidence matrix corresponding to the graph



Problem 34.7
If each vertex of an undirected graph has degree k then the graph is called a **regular** graph of degree k.
How many edges are there in a graph with 10 vertices each of degree 6?

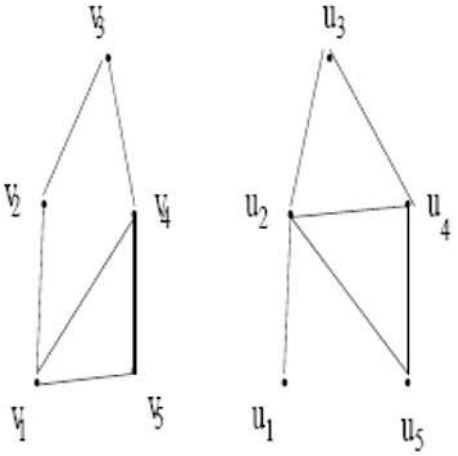
Problem 34.8
Two simple graphs G_1 and G_2 are **isomorphic**, in symbol, $G_1 \simeq G_2$, if there is one-to-one onto function, $f : V(G_1) \to V(G_2)$ and $(u, v) \in E_{G_1}$ if and only if $(f(u), f(v)) \in E_{G_2}$. Show that the following graphs are isomorphic.



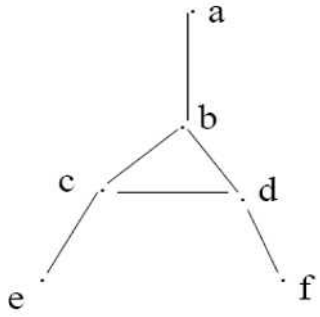
Warning: The number of vertices, the number of edges, and the degrees of the vertices are all invariants under isomorphism. If any of these quantities

differ in two graphs, these graphs cannot be isomorphic. However, when these invariants are the same, it does not necessarily mean that the two graphs are isomorphic.
The isomorphism between two graphs $G_1 = (V_{G_1}, E_{G_1})$ and $G_2 = (V_{G_2}, E_{G_2})$ with parallel edges or loops requires two bijections $f : V_{G_1} \to V_{G_2}$ and $g : E_{G_1} \to E_{G_2}$ such that if $e \in E_{G_1}$ is an edge with endpoints (u, v) then $g(e) \in E_{G_2}$ is an edge with endpoints $(f(u), f(v))$.

Problem 34.9
Show that the following graphs are not isomorphic.



Problem 34.10
Show that the following graph has no Hamiltonian path.



35 Trees

An undirected graph is called a **tree** if each pair of distinct vertices has exactly one path between them. Thus, a tree has no parallel edges and no loops.
We next show a result that is needed for the proof of our first main theorem of trees.

Theorem 35.1
Any tree with more than one vertex has one vertex of degree 1.

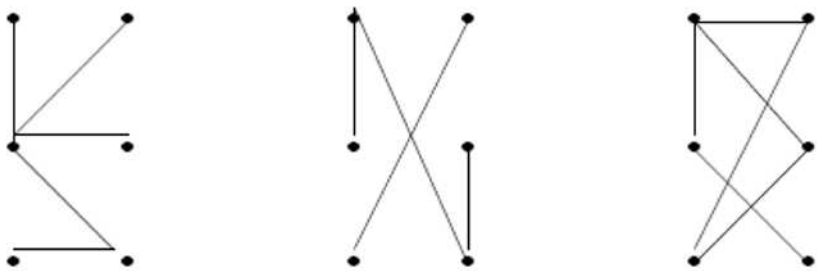
Proof.
Let T be a tree with a number of vertices ≥ 1. Pick a vertex v at random and search outward from v on a path along edges from one vertex to another looking for a vertex of degree one. As each new vertex is reached, check whether it has degree 1. If so, a vertex of degree 1 has been found. If not, it is possible to exit from the new vertex along a different edge from that used to reach the vertex. Because T is a tree, it is circuit-free, and so the path never returns to a previously used vertex. Since the number of vertices of T is finite, the process of building a path must eventually terminate. When that happens, the final vertex of the path must have degree 1 ■

The following is the first of the two main theorems about trees:

Theorem 35.2
A tree with n vertices has exactly $n - 1$ edges.

Proof.
The proof is by induction on $n \geq 1$. Let $P(n)$ be the property: Any tree with n vertices has $n - 1$ edges.
Basis of induction: $P(1)$ is valid since a tree with one vertex has zero edges.
Induction hypothesis: Suppose that $P(n)$ holds up to $n \geq 1$.
Induction Step: We must show that any tree with $n + 1$ vertices has n edges. Indeed, let T be any tree with $n+1$ vertices. Since $n+1 \geq 2$, by the previous theorem, T has a vertex v of degree 1. Let T_0 be the graph obtained by removing v and the edge attached to v. Then T_0 is a tree with n vertices. By the induction hypothesis, T_0 has $n - 1$ edges and so T has n edges ■

Example 35.1
Which of the following graphs are trees?



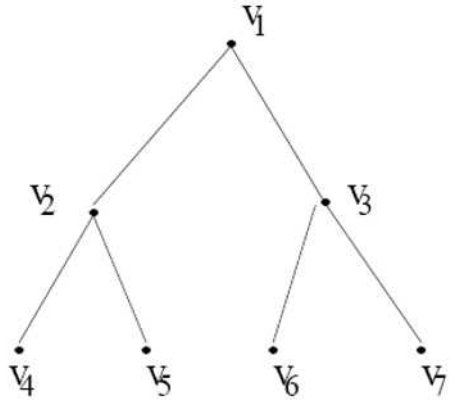
Solution.
The first graph satisfies the definition of a tree. The second and third graphs do not satisfy the conclusion of Theorem 35.2 and therefore they are not trees. ■

The second major theorem about trees is the following theorem whose proof is omitted.

Theorem 35.3
Any connected graph with n vertices and $n-1$ edges is a tree.

A **rooted tree** is a tree in which a particular vertex is designated as the **root.** The **level of a vertex** v is the length of the simple path from the root to v. The **height** of a rooted tree is the maximum level number that occurs.

Example 35.2
Find the level of each vertex and the height of the following rooted tree.



Solution.
v_1 is the root of the given tree.

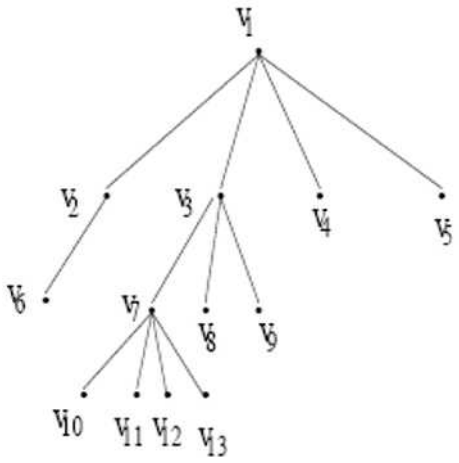
vertex	*level*
v_2	1
v_3	1
v_4	2
v_5	2
v_6	2
v_7	2

The height of the tree is 2. ■

Let T be a rooted tree with root v_0. Suppose $(v_0, v_1, \cdots, v_n)$ is a simple path in T and x, y, z are three vertices. Then
(a) v_{n-1} is the **parent** of v_n.
(b) $v_0, v_1, \cdots, v_{n-1}$ are the **ancestors** of v_n.
(c) v_n is the **child** of v_{n-1}.
(d) If x is an ancestor of y then y is a **descendant** of x.
(e) If x and y are children of z then x and y are **siblings**.
(f) If x has no children, then x is a **leaf**.
(g) The **subtree** of T rooted at x is the graph with vertex set V and edge set E, where V is x together with the descendants of x and

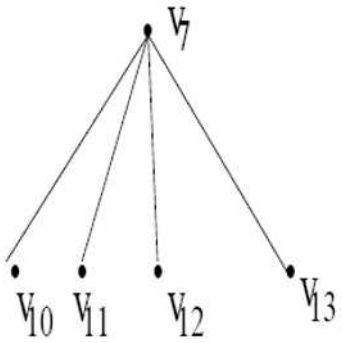
$$E = \{e | e \textit{ is an edge on a simple path from } x \textit{ to some vertex in } V\}.$$

Example 35.3
Consider the rooted tree



a. Find the parent of v_6.
b. Find the ancestors of v_{13}.
c. Find the children of v_3.
d. Find the descendants of v_{11}.
e. Find an example of a siblings.
f. Find the leaves.
g. Construct the subtree rooted at v_7.

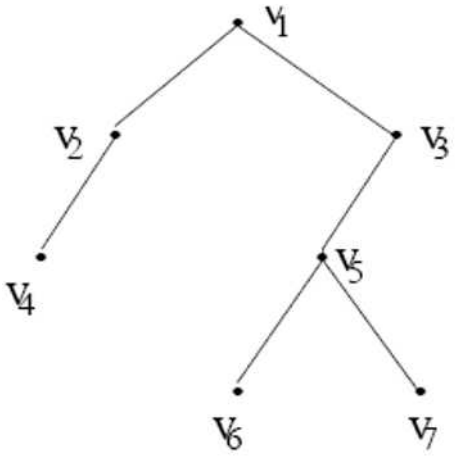
Solution.
a. v_2.
b. v_1, v_3, v_7.
c. v_7, v_8, v_9.
d. None.
e. $\{v_2, v_3, v_4, v_5\}$.
f. $\{v_4, v_5, v_6, v_8, v_9, v_{10}, v_{11}, v_{12}, v_{13}\}$.
g.



■

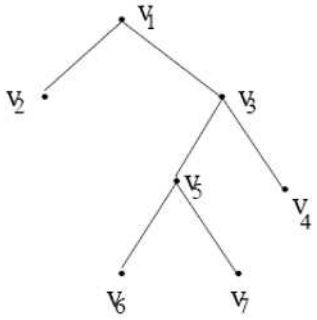
A **binary tree** is a rooted tree such that each vertex has at most two children. Moreover, each child is designated as either a **left child** or a **right child**.

Example 35.4
a. Show that the following tree is a binary tree.



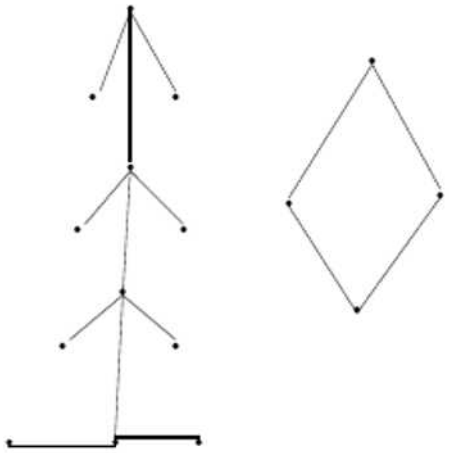
b. Find the left child and the right child of vertex v_5.
c. A **full binary tree** is a binary tree in which each vertex has either two children or zero children. Construct an example of a full binary tree.

Solution.
a. Follows from the definition of a binary tree.
b. The left child is v_6 and the right child is v_7.
c.



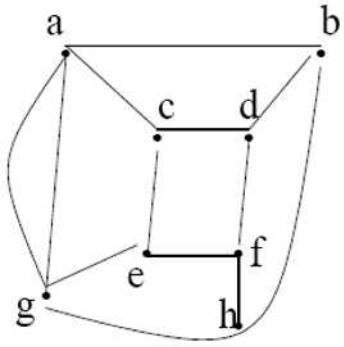
■

Example 35.5
A **forest** is a simple graph with no circuits. Which of the following graphs is a forest?



Solution.
The first graph is a forest whereas the second is not. ■

Example 35.6
a. Let T be a subgraph of a graph G such that T is a tree containing all of the vertices of G. Such a tree is called a **spanning tree**. Find a spanning tree of the following graph.



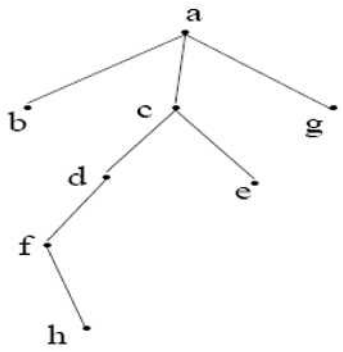
b. The following algorithm finds a spanning tree. In this algorithm S denotes a sequence. Let G be a connected graph with vertices ordered

$$v_1, v_2, , \cdots , v_n$$

1. Let T be the tree with root v_1 and no edges.
2. Add to T all edges (v_1, x) and vertices on which they are incident, provided

that (v_1, x) does not produce a circuit. If no edges can be added, stop (T is a spanning tree)
3. Replace S by the children in T of S ordered consistently with the original ordering. Go to step 2.
Use the above algorithm to find the spanning tree of part a.

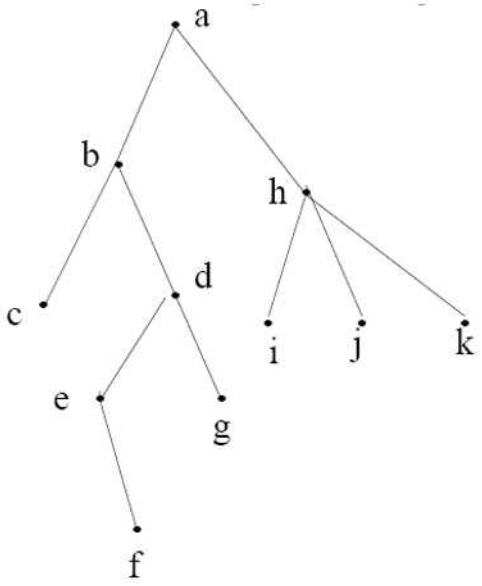
Solution.
a.



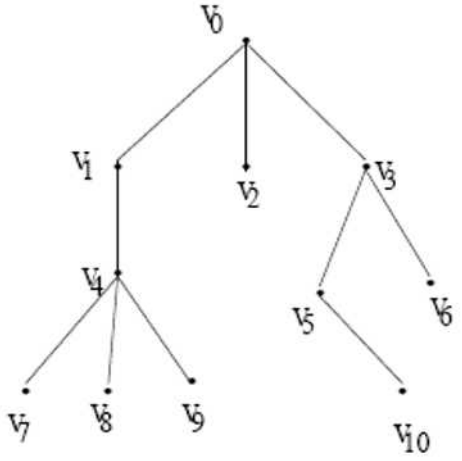
■

Review Problems

Problem 35.1
Find the level of each vertex and the height of the following rooted tree.



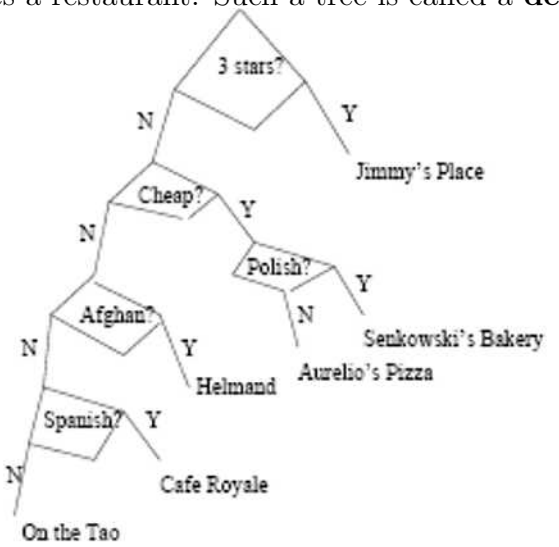
Problem 35.2
Consider the rooted tree



a. Find the parent of v_6.
b. Find the ancestors of v_{10}.

c. Find the children of v_4.
d. Find the descendants of v_1.
e. Find all the siblings.
f. Find the leaves.
g. Construct the subtree rooted at v_1.

Problem 35.3
The binary tree below gives an algorithm for choosing a restaurant. Each internal vertex asks a question. If we begin at the root, answer each question, and follow the appropriate edge, we will eventually arrive at a terminal vertex that chooses a restaurant. Such a tree is called a **decision tree.**



Construct a decision tree that sorts three given numbers a_1, a_2, a_3 in ascending order.

Problem 35.4
A **binary search tree** is a binary tree T in which data are associated with the vertices. The data are arranged so that, for each vertex v in T, each data item in the left subtree of v is less than the data item in v and each data item in the right subtree of v is greater than the data item in v. Using numerical order, form a binary search tree for a number in the set $\{1, 2, \cdots, 15\}$.

Problem 35.5
Procedures for systematically visiting every vertex of a tree are called **traversal algorithms**. In the **preorder traversal,** the root r is listed first and

then the subtrees $T_1, T_2, \cdots, T_n$ are listed, from left to right, in order of their roots. The preorder traversal begins by visiting r. It continues by traversing T_1 in preorder, thenT_2 in preorder, and so on, until T_n is traversed in preorder. In which order does a preorder traversal visit the vertices in the following rooted tree?