Lecture One

Section 1.1 – Propositional Logic

Introduction

The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments.

The logic rules are used in the design of computer circuits, the construction of computer programs, and the verification of the correctness of programs.

Propositions

A proposition is a declarative sentence (that is, a sentence that declares a fact) that is either true or false, but not both.

All the following declarative sentences are propositions

- ✓ Washington, D.C. is the capital of the United States of America. *True*
- ✓ $1 + 1 = 2$ *True*
- ✓ $2 + 2 = 3$ *False*

Example

Consider the following sentences
1. What time is it?
2. Read this carefully
3. $x + 1 = 2$
4. $x + y = z$

Solution

Sentences 1 and 2 are not propositions because they are not declarative sentences.
Sentences 3 and 4 are not propositions because they are not true (*T*) or false (*F*).

Definition

Let p be a proposition. The negation of p, denoted by $\neg p$ (also denoted by $\overline{p}$), is the statement

"It is not the case that p."

The proposition $\neg p$ is read "not p". The truth value of the negation of p, $\neg p$, is the opposite of the truth value of p.

1

Example

Find the negation of the proposition: "Michael's PC runs Linux" and express this in simple English.

Solution

The negation: Michael's PC does not run Linux

Example

Find the negation of the proposition: "Vandana's smartphone has at least 32GB of memory" and express this in simple English.

Solution

The negation: Vandana's smartphone has less than 32GB of memory
Vandana's smartphone does not have at least 32GB of memory

Table: **Truth table of the Negation of a Proposition**

p	$\neg p$
T	*F*
F	*T*

Definition

Let p and q be propositions. The ***conjunction*** of p and q, denoted by $p \wedge q$, is the proposition "p and q."
The *conjunction* $p \wedge q$ p and q is true for both are true and it's false otherwise.

Example

Find the conjunction of the propositions p and q where p is the proposition "your PC has more than 16GB free hard disk space" and q is the proposition "your PC processor runs faster than 1 GHz."

Solution

The conjunction is $p \wedge q$ and can be expressed as:

   ✓ Your PC has more than 16GB free hard disk space and its processor runs faster than 1 GHz.

For this conjunction to be true, both conditions given must be true.
It is false when one or both of these conditions are false.

Definition

Let p and q be propositions. The ***disjunction*** of p and q, denoted by $p \vee q$, is the proposition "p or q."
The disjunction $p \vee q$ is false when both p and q are false and it's true otherwise.

Truth Table for the Conjunction of Two Propositions.		
p	*q*	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Truth Table for the Disjunction of Two Propositions.		
p	*q*	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example

Find the disjunction of the propositions p and q where p is the proposition "your PC has more than 16GB free hard disk space" and q is the proposition "your PC processor runs faster than 1 GHz."

Solution

The disjunction is $p \vee q$ and can be expressed as:

✓ Your PC has more than 16GB free hard disk space, or the processor in your PC runs faster than 1 GHz.

Definition

Let p and q be propositions. The ***exclusive or*** of p and q, denoted by $p \oplus q$, is the proposition that is true when exactly one of p and q is true and is false otherwise.

Truth Table for the Exclusive Or of Two Propositions.		
p	*q*	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Truth Table for the Conditional Statement $p \rightarrow q$.		
p	*q*	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Definition

Let p and q be propositions. The **conditional statement** $p \rightarrow q$, is the proposition "if p, then q." The conditional statement $p \rightarrow q$ is false when p is true and q is false, and true otherwise. In the conditional statement $p \rightarrow q$, p called the *hypothesis* (or *antecedent* or *premise*) and q is called the *conclusion* (or *consequence*).

If p, then q	*p implies q*
If p, q	*p only if q*
p is sufficient for q	*a sufficient condition for q is p*
q if p	*q whenever p*
q when p	*q necessary for p*
a necessary condition for p is q	*q follows from p*
q unless $\neg p$	

Example

Let p be the statement "Maria learns discrete mathematics" and q the statement "Maria will find a good job". Express the statement $p \rightarrow q$ as a statement in English.

Solution

$p \rightarrow q$ represents the statement:

✓ If Maria learns discrete mathematics, then she will find a good job.

There are many other way to express this conditional statement.

✓ Maria will find a good job when she learns discrete mathematics.
✓ For Maria to get a good job, it is sufficient for her to learn discrete mathematics.
✓ Maria will find a good job unless she does not learn discrete mathematics.

Example

What is the value of the variable x after the statement

$$\textbf{if} \quad 2+2=4 \quad \textbf{then} \quad x := x+1$$

If $x = 0$ before the statement is encountered? (The symbol $:=$ stands for assignment. The statement $x := x+1$ means the assignment of the value of $x+1$ to x.)

Solution

Because 2 + 2 = 4 is true, the assignment statement $x := x+1$ is executed.
Hence, x has the value $0+1=1$ after this statement is encountered.

Converse, Contrapositive, and Inverse.

The *converse* of $p \to q$ is the proposition $q \to p$

The *contrapositive* of $p \to q$ is the proposition $\neg q \to \neg p$

The *inverse* of $p \to q$ is the proposition $\neg p \to \neg q$

Example

What are the contrapositive, the converse, and the inverse of the conditional statement
"The home team wins whenever it is raining?"

Solution

Because "*q* whenever *p*" is one of these ways to express the conditional statement $p \to q$, the original statement can be written as

✓ If it is raining, then the home team wins.

The contrapositive of this conditional statement is:

✓ If the home team does not win, then it is not raining.

The converse: If the home team wins, then it is raining.

The inverse: If it is not raining, then the home team does not win.

Only the contrapositive is equivalent to the original statement.

Definition

Let *p* and *q* be propositions. The ***biconditional statement*** $p \leftrightarrow q$ is the proposition "*p* if and only if *q*."
The biconditional statement $p \leftrightarrow q$ is true when *p* and *q* have the same truth values, and is false otherwise. Biconditional statements are also called ***bi-implications***.

   p is necessary and sufficient for *q*

   If *p* then *q*, and conversely

   p iff *q*

   $p \leftrightarrow q$ has exactly the truth value as $(p \to q) \wedge (q \to p)$

Example

Let *p* be the statement "You can take the flight," and let *q* be the statement "You buy a ticket." Then
$p \leftrightarrow q$ is the statement: "You can take the flight if and only if you buy a ticket."

Solution

This statement is true if *p* and *q* are either both true or false, that is, if you buy a ticket and can take the flight or if you do not buy a ticket and you cannot take the flight.
It is false when *p* and *q* have opposite truth values, that is, when you do not buy a ticket, but you can take the flight, and when you buy a ticket but you cannot take the flight.

Truth Tables of Compound Propositions

Example

Construct the truth table of the compound proposition $(p \vee \neg q) \rightarrow (p \wedge q)$

Solution

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

Precedence of Logical Operators

Precedence of Logical Operators	
Operator	*Precedence*
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

$p \wedge q \vee r$ **means** $(p \wedge q) \vee r$

Logic and Bit Opertions

True Value	Bit
T	1
F	0

Bit Operators OR, AND, and XOR				
x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Definition

A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.

Exercises   *Section* 1.1 – Propositional Logic

1. Which of these sentences are propositions? What are truth values of those that are propositions?

    a) Boston is the capital of Massachusetts.
    b) Miami is the capital of Florida
    c) $2 + 3 = 5$
    d) $5 + 7 = 10$
    e) $x + 2 = 11$
    f) Answer this question
    g) Do not pass go
    h) What time is it?
    i) The moon is made of green cheese

    j) $2^n \geq 100$

2. What is the negation if each of these propositions?

    a) Mei has an MP3 player
    b) There is no pollution in Texas
    c) $2 + 1 = 3$
    d) There are 13 items in a baker's dozen,
    e) 121 is a perfect square

3. Suppose the Smartphone A has 256 MB RAM and 32 GB ROM, and the resolution of its camera is 8 MP; Smartphone B has 288 MB RAM and 64 GB ROM, and the resolution of its camera is 4 MP; Smartphone C has 128 MB RAM and 32 GB ROM, and the resolution of its camera is 5 MP. Determine the truth value of each of these propositions.

    a) Smartphone B has the most RAM of these three smartphones
    b) Smartphone C has more ROM or higher resolution camera than Smartphone B.
    c) Smartphone B has more RAM, more ROM, and a higher resolution camera than Smartphone A.
    d) If Smartphone B has more RAM and more ROM than Smartphone C, then it also has a higher resolution camera.
    e) Smartphone A has more RAM than Smartphone B if and only if Smartphone B has more RAM than Smartphone A.

4. Let p and q be the proposition
    > p: I bought a lottery ticket this week
    > q: I won the million dollar jackpot

    a) $\neg p$
    b) $p \vee q$
    c) $p \rightarrow q$
    d) $p \wedge q$
    e) $p \leftrightarrow q$
    f) $\neg p \rightarrow \neg q$
    g) $\neg p \wedge \neg q$
    h) $\neg p \vee (p \wedge q)$

5. Let p and q be the proposition

> p: Swimming at the New Jersey shore is allowed
>
> q: Sharks have been spotted new the shore

a) $\neg q$ b) $p \wedge q$ c) $\neg p \vee q$ d) $p \rightarrow \neg q$

e) $\neg q \rightarrow p$ f) $\neg p \rightarrow \neg q$ g) $p \leftrightarrow \neg q$ h) $\neg p \wedge (p \vee \neg q)$

6. Let p, q and r be the proposition

> p: You have the flu
>
> q: You miss the final examination
>
> r: You pass the course

Express each of these proposition as an English sentence

a) $p \rightarrow q$ b) $\neg q \leftrightarrow r$ c) $q \rightarrow \neg r$ d) $p \vee q \vee r$

e) $(p \rightarrow \neg r) \vee (q \rightarrow \neg r)$ f) $(p \wedge q) \vee (\neg q \wedge r)$

7. Determine whether each of these conditional statements is true or false.

a) If $1+1 = 2$, then $2 + 2 = 5$
b) If $1 + 1 = 3$, then $2 + 2 = 4$
c) If $1 + 1 = 3$, then $2 + 2 = 5$
d) If monkeys can fly, then $1 + 1 = 3$
e) If $1 + 1 = 3$, then unicorns exist
f) If $1 + 1 = 3$, then dogs can fly
g) If $1 + 1 = 2$, the dogs can fly
h) If $2 + 2 = 4$, then $1 + 2 = 3$

8. Write each of these propositions in the form "p if and only if q" in English
a) If it is hot outside you buy an ice cream cone, and if you buy an ice cream cone it is hot outside.
b) For you to win the contest it is necessary and sufficient that you have only winning ticket.
c) You get promoted only if you have connections, and you have connections only if you get promoted.
d) If you watch television your mind will decay, and conversely.
e) The trains run late on exactly those days when I take it.
f) For you to get an A in this course, it is necessary and sufficient that you learn how to solve discrete mathematics problems.
g) If you read the newspaper every day, you will be informed, and conversely.
h) It rains if it is a weekend day, and it is a weekend day if it rains.
i) You can see the wizard only if the wizard is not in, and the wizard is not in only if you can see him

9. Construct a truth table for each of these compound propositions.

a) $p \wedge \neg p$

b) $p \vee \neg p$

c) $p \rightarrow \neg p$

d) $p \leftrightarrow \neg p$

e) $p \rightarrow \neg q$

f) $\neg p \leftrightarrow q$

g) $(p \vee \neg q) \rightarrow q$

h) $(p \vee q) \rightarrow (p \wedge q)$

i) $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$

j) $(p \rightarrow q) \rightarrow (q \rightarrow p)$

k) $p \oplus (p \vee q)$

l) $(p \wedge q) \rightarrow (p \vee q)$

m) $(q \rightarrow \neg p) \leftrightarrow (p \leftrightarrow q)$

n) $(p \rightarrow q) \vee (\neg p \rightarrow q)$

o) $(p \rightarrow q) \wedge (\neg p \rightarrow q)$

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

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

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

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

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

Section 1.2 – Propositional Equivalences

Introduction

An important type of step used in a mathematical argument is the replacement of a statement with another statement with the same truth value.

Definition

A compound proposition that is always true, no matter what the truth values of the proposition variables that occur in it, is called a ***tautology***. A compound proposition that is always false is called ***contradiction***. A compound proposition that is neither a tautology nor a contradiction is called a ***contingency***.

Example

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	*F*	*T*	*F*
F	*T*	*T*	*F*

$p \vee \neg p$ is always true, it is tautology

$p \wedge \neg p$ is always false, it is contradiction.

Logical Equivalences

Definition

Compound propositions p and q are called ***logically equivalent*** if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent.

De Morgan's Laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$
$\neg(p \vee q) \equiv \neg p \wedge \neg q$

Example

Show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent.

Solution

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

The truth table shows that $\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$ is a tautology and these compound propositions are logically equivalent.

Example

Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Solution

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

The truth table shows that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent.

Example

Show that $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equivalent. This is the *distributive law* of disjunction over conjunction.

Solution

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

The truth table Show that $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equivalent.

In these equivalences, **T** denotes the compound proposition that is always true and **F** denotes the compound proposition that is always false.

Logical Equivalences	
Equivalence	*Name*
$p \wedge T \equiv p$	*Identity laws*
$p \vee F \equiv p$	
$p \vee T \equiv T$	*Domination laws*
$p \wedge F \equiv F$	
$p \vee p \equiv p$	*Idempotent laws*
$p \wedge p \equiv p$	
$\neg(\neg p) \equiv p$	*Double negation law*
$p \vee q \equiv q \vee p$	*Commutative laws*
$p \wedge q \equiv q \wedge p$	
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	*Associative laws*
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	*Distributive laws*
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	*De Morgan's laws*
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	
$p \vee (p \wedge q) \equiv p$	*Absorption laws*
$p \wedge (p \vee q) \equiv p$	
$p \vee \neg p \equiv T$	*Negation laws*
$p \wedge \neg p \equiv F$	

Logical Equivalences Involving Conditional Statements
$p \rightarrow q \equiv \neg p \vee q$
$p \rightarrow q \equiv \neg q \vee \neg p$
$p \vee q \equiv \neg p \rightarrow q$
$p \wedge q \equiv \neg(p \rightarrow \neg q)$
$\neg(p \rightarrow q) \equiv p \wedge \neg q$
$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Logical Equivalences Involving Biconditional Statements
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow r)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

12

$$\neg\left(p_1 \vee p_2 \vee \cdots \vee p_n\right) \equiv \left(\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n\right)$$

$$\neg\left(p_1 \wedge p_2 \wedge \cdots \wedge p_n\right) \equiv \left(\neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n\right)$$

Using De Morgan's Laws

The two logical equivalences known as De Morgan's laws are particularly important. The equivalence $\neg(p \vee q) \equiv \neg p \wedge \neg q$ and similarly $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Example

Use De Morgan's laws to express the negations of "Miguel has a cellphone and he has a laptop computer" and "Heather will go to the concert or Steve will go to the concert."

Solution

Let: p be "Miguel has a cellphone"

q be "Miguel has a laptop computer"

can be expressed as $p \wedge q$

By De Morgan's laws $\neg(p \wedge q)$ is equivalent to $\neg p \vee \neg q$. We can express the negation of our

original statement as "*Miguel does not have a cellphone **or** he does not have a laptop computer*"

Let: r be "Heather will go to the concert"

s be "Steve will go to the concert"

can be expressed as $r \vee s$

By De Morgan's laws $\neg(r \vee s) \equiv \neg r \wedge \neg s$. We can express the negation of our original statement as

"*Heather will not go to the concert **and** Steve will not go to the concert*."

Example

Show that $\neg(p \rightarrow q)$ and $p \wedge \neg q$ are logically equivalent.

Solution

$\neg(p \rightarrow q) \equiv \neg(\neg p \vee q)$

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

$\equiv p \wedge \neg q$

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

Example

Show that $\neg\left(p\vee\left(\neg p\wedge q\right)\right)$ and $\neg p\wedge\neg q$ are logically equivalent by developing a series of logical equivalences.

Solution

$$\neg\left(p\vee\left(\neg p\wedge q\right)\right)\equiv\neg p\wedge\neg\left(\neg p\wedge q\right) \qquad \text{\textit{\textbf{By De Morgan's law}}}$$

$$\equiv\neg p\wedge\left(p\vee\neg q\right) \qquad \text{\textit{\textbf{Double negation law}}}$$

$$\equiv\left(\neg p\wedge p\right)\vee\left(\neg p\wedge\neg q\right) \qquad \text{\textit{\textbf{Distribution law}}}$$

$$\equiv F\vee\left(\neg p\wedge\neg q\right) \qquad \neg p\wedge p\equiv F$$

$$\equiv\left(\neg p\wedge\neg q\right)\vee F \qquad \text{\textit{\textbf{Commutative law for disjunction}}}$$

$$\equiv\neg p\wedge\neg q \qquad \text{\textit{\textbf{Identity law}}}$$

Example

Show that $\left(p\wedge q\right)\rightarrow\left(p\vee q\right)$ is a tautology.

Solution

$$\left(p\wedge q\right)\rightarrow\left(p\vee q\right)\equiv\neg\left(p\wedge q\right)\vee\left(p\vee q\right)$$

$$\equiv\left(\neg p\vee\neg q\right)\vee\left(p\vee q\right) \qquad \text{\textit{\textbf{By De Morgan's law}}}$$

$$\equiv\left(\neg p\vee p\right)\vee\left(\neg q\vee q\right) \qquad \text{\textit{\textbf{By Associative and commutative laws}}}$$

$$\equiv T\vee T$$

$$\equiv T$$

Exercises   *Section* 1.2 – **Propositional Equivalences**

1. Use the truth table to verify these equivalences

    a) $p \wedge T \equiv p$

    b) $p \vee F \equiv p$

    c) $p \wedge F \equiv F$

    d) $p \vee T \equiv T$

    e) $p \vee p \equiv p$

    f) $p \wedge p \equiv p$

2. Show that $\neg(\neg p)$ and p are logically equivalent

3. Use the truth table to verify the commutative laws

    a) $p \vee q \equiv q \vee p$

    b) $p \wedge q \equiv q \wedge p$

4. Use the truth table to verify the associative laws

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

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

5. Show that each of these conditional statements is a tautology by using truth result tables.

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

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

    c) $\neg p \rightarrow (p \rightarrow q)$

    d) $(p \wedge q) \rightarrow (p \rightarrow q)$

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

    f) $\left[\neg p \wedge (p \vee q)\right] \rightarrow q$

    g) $\left[(p \rightarrow q) \wedge (q \rightarrow r)\right] \rightarrow (p \rightarrow r)$

    h) $\left[p \wedge (p \rightarrow q)\right] \rightarrow q$

6. Show that $p \leftrightarrow q$ and $(p \wedge q) \vee (\neg p \wedge \neg q)$ are logically equivalent

7. Show that $\neg(p \leftrightarrow q)$ and $p \leftrightarrow \neg q$ are logically equivalent

8. Show that $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are logically equivalent

9. Show that $\neg p \leftrightarrow q$ and $p \leftrightarrow \neg q$ are logically equivalent

10. Show that $(p \rightarrow q) \vee (p \rightarrow r)$ and $p \rightarrow (q \vee r)$ are logically equivalent

11. Show that $(p \rightarrow r) \vee (q \rightarrow r)$ and $(p \wedge q) \rightarrow r$ are logically equivalent

12. Show that $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ is a tautology

13. Show that $(p \vee q) \vee (\neg p \vee r) \rightarrow (q \vee r)$ is a tautology

14. Show that $\mid$ (NAND) is functionally complete

Section 1.3 – **Predicates and Quantifiers**

Introduction

To express the meaning of a wide range of statements in mathematics and computer science in ways that permit us to reason and explore relationships between object, are called ***predicate logic***.

Predicates

Statements involving variables, such as

"$x > 3$,"   "$x = y + 3$,"   *and* "*computer x is under attack by an intruder.*"

are often found in mathematical assertions, in computer programs, and in system specifications

Example

Let $P(x)$ denote the statement $x > 3$. What are the truth values of $P(4)$ and $P(2)$?

Solution

We obtain the statement $P(4)$ by setting $x = 4$ in the statement $x > 3$. Hence, $P(4)$, which is the statement $4 > 3$ is true.

However, $P(2)$, which is the statement $2 > 3$ is false.

Example

Let $Q(x, y)$ denote the statement $x = y + 3$. What are the truth values of propositions $Q(1,\ 2)$ and $Q(3,\ 0)$?

Solution

To obtain $Q(1,\ 2)$, set $x = 1$ and $y = 2$ in the statement $Q(x, y)$. Hence, $Q(1,\ 2)$ is the statement $1 = 2 + 3$ which is false.

The statement $Q(3,\ 0)$ is the proposition $3 = 0 + 3$ which is true.

Example

Let $A(c,n)$ denote the statement "Computer c is connected to netwrok n," where c is a variable representing a computer and n is a variable representing a network. Suppose that the computer MATH1 is connected to network CAMPUS2, but not to network CAMPUS1. What are the values of $A(MATH1, CAMPUS1)$ and $A(MATH1, CAMPUS2)$?

Solution

Because MATH1 is not connected to the CAMPUS1 network, we see that $A(MATH1, CAMPUS1)$ is false.

However, because MATH1 is connected to the CAMPUS2 network, we see that $A(MATH1, CAMPUS2)$ is true.

🔸 Consider the statement **if** $x > 0$ **then** $x := x + 1$

When this statement is encountered in a program, the value of the variable x at the point in the execution of the program is inserted into $P(x)$, which is $x > 0$. If $P(x)$ is true for this value of x, the assignment statement $x := x + 1$ is executed. So the value of x is increased by 1. If $P(x)$ is false for this value of x, the assignment statement is not executed, so the value of x is not changed.

Preconditions and Postconditions

Predicates are also used to establish the correctness of computer programs, that is, to show that computer programs always produce desired output given valid input.

The statements that describe valid input are known as **preconditions** and the conditions that the output should satisfy when the program has run are known as **postconditions**.

Quantifiers

To create a proposition from a propositional function is called **quantification**. Quantification expresses the extent to which a predicate is true over a range of elements. The words **all, some, many, none** and **few** are used in quantifications.

The area of logic that deals with predicates and quantifiers is called the **predicate calculus**.

There are two quantifiers

➤ Existential Quantifier   "∃" reads "there exists"
➤ Universal Quantifier   "∀" reads "for all"

Each is placed in front of a propositional function and **binds** it to obtain a proposition with semantic value.

Definition

The **_universal quantification_** of $P(x)$ is the statement

"$P(x)$ for all values of x in the domain."

The notation $\forall x\, P(x)$ denotes the universal quantification of $P(x)$. Here $\forall$ is called the universal quantifier. We read $\forall x\, P(x)$ as "for all $x\, P(x)$" or "for every $x\, P(x)$". An element for which $P(x)$ is false is called a counterexample of $\forall x\, P(x)$.

Statement	When True?	When False?
$\forall x\, P(x)$	$P(x)$ *is true for every x.*	*There is an x for which* $P(x)$ *is false.*
$\forall x\, P(x)$	*There is an x for which* $P(x)$ *is true.*	$P(x)$ *is false for every x.*

Example

Let $P(x)$ be the statement "$x+1 > x$". What is the truth value of the quantification $\forall x\, P(x)$, where the domain consists of all real numbers?

Solution

Because $P(x)$ is true for all real numbers x, the quantification $\forall x\, P(x)$ is true.

Example

Let $Q(x)$ be the statement "$x < 2$". What is the truth value of the quantification $\forall x\, Q(x)$, where the domain consists of all real numbers?

Solution

$Q(x)$ is not true for every real number x, because, $Q(3)$ is false.
That is, $x = 3$ is a counterexample for the statement $\forall x\, Q(x)$. Thus $\forall x\, Q(x)$ is false.

Example

What is the truth value of $\forall x\, P(x)$, where $P(x)$ is the statement "$x^2 < 10$" and the domain consists of the positive integers not exceeding 4?

Solution

The domain consists of the integers 1, 2, 3, and 4. Since "$4^2 < 10$" is false, it follows that $\forall x\, P(x)$ is false.

Example

What is the truth value of $\forall x \left(x^2 \geq x \right)$, if the domain consists of real number? What is the truth value of this statement of the domain consists of all integers?

Solution

- $\left(\frac{1}{2}\right)^2 \not\geq \frac{1}{2}$, it follows that $\forall x \left(x^2 \geq x \right)$ is false.

   Note: $x^2 \geq x$ *iff* $x^2 - x = x(x-1) \geq 0 \Rightarrow x \leq 0 \quad x \geq 1$

- If the domain consists of the integers, $\forall x \left(x^2 \geq x \right)$ is true, because there are no integers x with
   $0 < x < 1$

Definition

The ***existential quantification*** of $P(x)$ is the proposition

"There exists an element x in the domain such that $P(x)$"

We use the notation $\exists x \, P(x)$ for the existential quantification of $P(x)$. Here $\exists$ is called the ***existential quantifier***.

Example

Let $P(x)$ denote the statement "$x > 3$". What is the truth value of the quantification $\exists x \, P(x)$, where the domain consists of all real numbers?

Solution

Because "$x > 3$" is sometimes true, for instance, when $x = 4$ – the existence quantification of $P(x)$, which is $\exists x \, P(x)$, is true.

Example

Let $Q(x)$ denote the statement "$x = x + 1$". What is the truth value of the quantification $\exists x \, Q(x)$, where the domain consists of all real numbers?

Solution

$Q(x)$ is false for every real number x, the existential quantification of $Q(x)$, which is $\exists x \, Q(x)$, is false.

Example

What is the truth value of $\exists x\, P(x)$, where $P(x)$ is the statement "$x^2 > 10$" and the universe discourse of the positive integers not exceeding 4?

Solution

The domain consists of the integers 1, 2, 3, and 4. Since "$4^2 > 10$" is true, it follows that $\exists x\, P(x)$ is true.

Quantifiers with Restricted Domains

What do the statement $\forall x < 0\, \left(x^2 > 0\right)$, $\forall y \neq 0\, \left(y^3 \neq 0\right)$, and $\forall z > 0\, \left(z^2 = 0\right)$ mean, where the domain in each case consists of the real numbers?

➢ The statement $\forall x < 0\, \left(x^2 > 0\right)$ states that for every real numbers x with $x < 0$, $x^2 < 0$. That is, it states "the square of a negative real number is positive." This statement is the same as $\forall x\, \left(x < 0 \rightarrow x^2 > 0\right)$.

➢ The statement $\forall y \neq 0\, \left(y^3 \neq 0\right)$ states that for every real numbers y with $y \neq 0$, $y^3 \neq 0$. That is, it states "the cube of every nonzero real number is nonzero." This statement is the equivalent to $\forall y\, \left(y \neq 0 \rightarrow y^3 \neq 0\right)$.

➢ The statement $\forall z > 0\, \left(z^2 = 2\right)$ states that for every real numbers z with $z > 0$ such that $z^2 = 2$. That is, it states "There is a positive square root of 2." This statement is the equivalent to $\exists z\, \left(z > 0 \wedge z^2 = 2\right)$.

Binding Variables

When a quantifier is used on the variable x, we say that this occurrence of the variable is bound. An occurrence of a variable that is not bound by a quantifier or set equal to a particular value is said to be *free*.

Logical Equivalences Involving Quantifiers

Definition

Statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain of discourse is used for the variables in these propositional functions. We use the notation $S \equiv T$ involving predicates and quantifiers are logically equivalent.

Negating Quantified Expressions

We will often want to consider the negation of a quantified expression. For instance, consider the negation of the statemnt

   "Every student in your class has taken a course in calculus"

This statement is a universal quantification, namely, $\forall x \, P(x)$

where $P(x)$ is the statement "x has taken a course in calculus" and the domain consists of the students in your class.

The negation of this statement is " It is not the case that every student in your class who has not taken a course in calculus". This is simply the existential quantification of the negation of the original proposition function, namely, $\exists x \, \neg P(x)$.

This example illustrates the following logical equivalence:

$$\neg \forall x \, P(x) \equiv \exists x \, \neg P(x)$$

$$\neg \exists x \, Q(x) \equiv \forall x \, \neg Q(x)$$

De Morgan's Laws for Quantifiers			
Negation	*Equivalent Statement*	*When Is Negation True?*	*When False?*
$\neg \exists x \, P(x)$	$\forall x \, \neg P(x)$	*For every x, $P(x)$ is false*	*There is an x for which $P(x)$ is true*
$\neg \forall x \, P(x)$	$\exists x \, \neg P(x)$	*There is an x for which $P(x)$ is false*	*For every x, $P(x)$ is true*

Example

What are the negations of the statements "There is an honest politician" and "All Americans eat cheeseburgers"?

Solution

Let $H(x)$ denote "x is honest."

Then the statement "there is an honest politician" is represented by $\exists x\, H(x)$

The negation statement is $\neg\exists x\, H(x)$, which is equivalent to $\forall x\, \neg H(x)$.

This negation can be expressed as "All politicians are not honest"

Let $G(x)$ denote "x eats cheeseburgers."

Then the statement "All Americans eat cheeseburgers" is represented by $\forall x\, G(x)$

The negation statement is $\neg\forall x\, G(x)$, which is equivalent to $\exists x\, \neg G(x)$.

This negation can be expressed as "There is an American who does not eat cheeseburgers."

Example

What are the negations of the statements $\forall x\,\left(x^2 > x\right)$ and $\exists x\,\left(x^2 = 2\right)$

Solution

The negation of $\forall x\,\left(x^2 > x\right)$ is the statement $\neg\forall x\,\left(x^2 > x\right) \equiv \exists x\, \neg\left(x^2 > x\right)$

Which can be written as $\exists x\,\left(x^2 \leq x\right)$

The negation of $\exists x\,\left(x^2 = 2\right)$ is the statement $\neg\exists x\,\left(x^2 = 2\right) \equiv \forall x\, \neg\left(x^2 = 2\right)$

Which can be written as $\forall x\,\left(x^2 \neq 2\right)$

Example

Consider these statements, of which the first three are premises and the fourth is a valid conclusion
   "All hummingbirds are richly colored"
   "No large birds live on honey"
   "Birds that do not live on honey are dull in color"
   "Hummingbirds are small"

Let $P(x)$, $Q(x)$, $R(x)$ and $S(x)$ be the statements "x is a hummingbird, " "x is large," "x lives on honey," and " x is richly colored," respectively. Assuming that the domain consists of all birds, express the statements in the argument using quantifiers and $P(x)$, $Q(x)$, $R(x)$ and $S(x)$.

Solution

We can express the statements in the argument as

$$\forall x \big(P(x) \to S(x) \big)$$

$$\neg \exists x \big(Q(x) \wedge R(x) \big)$$

$$\forall x \big(\neg R(x) \to \neg S(x) \big)$$

$$\forall x \big(P(x) \to \neg Q(x) \big)$$

"**small**" is the same as "not large"

"**dull in color**" is the same as "not richly colored"

Exercises   *Section* 1.3 – **Predicates and Quantifiers**

1.   Let $P(x)$ denote the statement "$x \le 4$". What are these truth values?

   a) $P(0)$ b) $P(4)$ c) $P(6)$

2.   Let $P(x)$ be the statement "*the word **x** contains the letter **a***". What are these truth values?

   a) $P(orange)$ b) $P(lemon)$ c) $P(true)$ d) $P(false)$

3.   State the value of x after the statement **if** $P(x)$ **then** $x := 1$ is executed, where $P(x)$ is the statement "$x > 1$", if the value of x when the statement is reached is

   a) $x = 0$ b) $x = 1$ c) $x = 2$

4.   Let $P(x)$ be the statement "***x** spends more than five hours every weekday in class,*" where the domain for x consists of all students. Express each of these quantifications in English.

   a) $\exists x\, P(x)$ b) $\forall x\, P(x)$ c) $\exists x\, \neg P(x)$ d) $\forall x\, \neg P(x)$

5.   Let $N(x)$ be the statement "***x** has visited North Dakota,*" where the domain consists of the students in your class. Express each of these quantifications in English.

   a) $\exists x\, N(x)$ b) $\forall x\, N(x)$ c) $\neg\exists x\, N(x)$ d) $\exists x\, \neg N(x)$

   e) $\neg\forall x\, N(x)$ f) $\forall x\, \neg N(x)$

6.   Let $C(x)$ be the statement "***x** has a cat,*" let $D(x)$ be the statement "***x** has a dog,*", and let $F(x)$ be the statement "***x** has a ferret.*" Express each of these statements in terms of $C(x)$, $D(x)$, $F(x)$, quantifiers, and logical connectives. Let the domain consist of all students in your class.

   a) A student in your class has a cat, a dog, and a ferret.
   b) All students in your class have a cat, a dog, or a ferret.
   c) Some student in your class has a cat and a ferret, but not a dog.
   d) No student in your class has a cat, a dog, and a ferret.
   e) For each of the three animals, cats, dogs, and ferrets, there is a student in your class who has this animal as a pet.

7.   Let $Q(x)$ be the statement "$x + 1 > 2x$". If the domain consists of all integers, what are these truth values?

   a) $Q(0)$ b) $Q(-1)$ c) $Q(1)$ d) $\exists x\, Q(x)$

   e) $\forall x\, Q(x)$ f) $\exists x\, \neg Q(x)$ g) $\forall x\, \neg Q(x)$

8.   Determine the truth value of each of these statements if the domain consists of all integers

   a) $\forall n(n+1 > n)$ b) $\exists n(2n = 3n)$ c) $\exists n(n = -n)$ d) $\forall n(3n \le 4n)$

9.   Determine the truth value of each of these statements if the domain consists of all real numbers

a) $\exists x \left(x^3 = -1 \right)$ b) $\exists x \left(x^4 < x^2 \right)$ c) $\forall x \left((-x)^2 = x^2 \right)$ d) $\forall x (2x > x)$

10. Suppose that the domain of the propositional function $P(x)$ consists of the integers 1, 2, 3, 4, and 5.

Express these statements without using quantifiers, instead using only negations, disjunctions, and conjunctions.

   a) $\exists x \, P(x)$ b) $\forall x \, P(x)$ c) $\neg \exists x \, P(x)$ d) $\neg \forall x \, P(x)$

   e) $\forall x \left((x \neq 3) \rightarrow P(x) \right) \lor \exists x \, \neg P(x)$

11. For each of these statements find a domain for which the statement is true and a domain for which the statement is false.
   a) Everyone is studying discrete mathematics.
   b) Everyone is older than 21 years.
   c) Every two people have the same mother.
   d) No Two different people have the same grandmother.

12. Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.
   a) No one is perfect.
   b) Not everyone is perfect.
   c) All your friends are perfect.
   d) At least one of your friends is perfect.
   e) Everyone is your friend and is perfect.
   f) Not everybody is your friend or someone is not perfect.

13. Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.
   a) Something is not in the correct place.
   b) All tools are in the correct place and are in excellent condition.
   c) Everything is in the correct place and in excellent condition.
   d) Nothing is in the correct place and is in excellent condition.
   e) One of your tools is not in the correct place, but it is in excellent condition.

Section 1.4 – Nested Quantifiers

Introduction

Nested quantifiers commonly occur in mathematics and computer science. Nested quantifiers can sometimes be difficult to understand.

We will see how to use nested quantifiers to express mathematical statements such as "The sum of two positive integers is always positive." We will show how nested quantifiers can be used to translate sentences such as "Everyone has exactly one best friend" into logical statements.

Example

Translate the statement $\forall x \forall y \left((x > 0) \wedge (y < 0) \rightarrow (xy < 0) \right)$

Where the domain for both variables consists of all real numbers.

Solution

This statement says that for every real number x and every real number y, if $x > 0$ and $y < 0$, then $xy < 0$. That is, this statement says that for all real numbers x and y, if x is positive and y is negative, then xy is negative.

This can be stated more succinctly as

"The product of a postitive real number and a negative real numer is always a negative real number."

The Order of Quantifiers

Example

Let $P(x, y)$ be the statement "$x + y = y + x$". What are the truth values of the quantifications $\forall x \forall y\, P(x, y)$ and $\forall y \forall x\, P(x, y)$ where the domain for all variables consists of all real numbers?

Solution

The quantification $\forall x \forall y\, P(x, y)$ denotes the proposition

For all real numbers x, for all real numbers y, $x + y = y + x$

The quantification $\forall y \forall x\, P(x, y)$ denotes the proposition

For all real numbers y, for all real numbers x, $x + y = y + x$

Which they have the same meaning.

Therefore; $\forall x \forall y\, P(x, y)$ and $\forall y \forall x\, P(x, y)$ have the same meaning, and both are true. This illustrates the principle that the order of nested universal quantifiers in a statement without other quantifiers can be changed without changing the meaning of the quantified statement.

Example

Let $P(x, y)$ be the statement "$x + y = 0$". What are the truth values of the quantifications $\exists y \forall x \, P(x, y)$ and $\forall x \exists y \, P(x, y)$ where the domain for all variables consists of all real numbers?

<u>*Solution*</u>

The quantification $\exists y \forall x \, P(x, y)$ denotes the proposition

There is a real number y, such that for every real number x, $P(x, y)$

No matter what value of y is chosen, there is only one value of x for which $x + y = 0$. Because there is no real number y such that $x + y = 0$ for all real numbers x, the statement $\exists y \forall x \, P(x, y)$ is false.

$x + 1 = 0$

The quantification $\forall x \exists y \, P(x, y)$ denotes the proposition

For every real number x, there is a real number y such that $P(x, y)$

✓ *"For all x, there exists a y such that $P(x, y)$"*

$x + y = 0 \implies y = -x$

Hence, the statement $\forall x \exists y \, P(x, y)$ is true.

✓ ***There exists an x such that for all y $P(x, y)$ is true"***

Quantifications of Two variables

Statement	When True?	When False?
$\forall x \forall y \, P(x, y)$ $\forall x \forall y \, P(x, y)$	*$P(x, y)$ is true for every pair x, y*	*There is a pair x, y for which $P(x, y)$ is false.*
$\forall x \exists y \, P(x, y)$	*For every x there is a y for which $P(x, y)$ is true.*	*There is an x such that $P(x, y)$ is false for every y.*
$\exists x \forall y \, P(x, y)$	*There is an x for which $P(x, y)$ is true for every y.*	*For every x there is a y for which $P(x, y)$ is false.*
$\exists x \exists y \, P(x, y)$ $\exists y \exists x \, P(x, y)$	*There is a pair x, y for which $P(x, y)$ is true.*	*$P(x, y)$ is false for every pair x, y*

Example

Let $P(x, y, z)$ be the statement "$x + y = z$". What are the truth values of the statements $\forall x \forall y \exists z \, P(x, y, z)$ and $\exists z \forall x \forall y \, P(x, y, z)$ where the domain for all variables consists of all real numbers?

Solution

The statement $\forall x \forall y \exists z \, P(x, y, z)$ denotes the proposition

For all real numbers x and for all real numbers y there is a real number z such that $x + y = z$

This statement is true.

The statement $\exists z \forall x \forall y \, P(x, y, z)$ denotes the proposition

There is a real number z such that for all real numbers x and for all real numbers y it is true that $x + y = z$

This statement is false, because there is no value of z that satisfies the equation $x + y = z$ for all values of x and y.

Translating Mathematical Statements into Statements Involving Nested Quantifiers

Example

Translate the statement "The sum of two positive integers is always positive" into a logical expression.

Solution

Let x and y be the positive integers variables which: "For all positive integers x and y, $x + y$ is positive."
We can express as:

$$\forall x \forall y \left((x > 0) \wedge (y > 0) \rightarrow (x + y > 0) \right)$$

We also can translate this using the positive integers as the domain.

$$\forall x \forall y \ (x + y > 0)$$

Where the domain for both variables consists of all positive integers

Example

Translate the statement $\forall x\big(C(x)\vee\exists y\big(C(y)\wedge F(x,y)\big)\big)$ into English, Where $C(x)$ is "x has a computer," $F(x, y)$ is "x and y are friends," and the domain for both x and y consists of all students in your school.

Solution

The statement says

For every student x in your school, x has a computer or there is a student y such that y has a computer and x and y are friends.

In other words

Every student in your school has a computer or has a friend who has a computer.

Example

Translate the statement $\exists x\forall y\forall z\big(F(x,y)\wedge F(x,z)\wedge(y\neq z)\big)\rightarrow\neg F(y,z)$ into English, where $F(a,b)$ means a and b are friends and the domain for both x, y and z consists of all students in your school.

Solution

The original statement says:

There is a student x such that for all students y and all students z other than y, if x and y are friends and x and z are friends, then y and z are not friends.

In other words

There is a student none of whose friends are also friends with each other.

Example

Express the statement "Everyone has exactly one best friend" as a logical expression involving predicates, quantifiers with domain consisting of all people, and logical connectives.

Solution

For every person x, x has exactly one best friend y. "$\forall x$ (person x has exactly one best friend)" with domain consisting of all people.
For every person z, if person z is not person y, then z is not the best friend of x.
Let $B(x,y)$ be the statement "y is the best friend of x".

Therefore; the statement can be expressed as:

$$\exists y\big(B(x,y)\wedge\forall z\big((z\neq y)\rightarrow\neg B(x,z)\big)\big)$$

The original statement can be expressed as:

$$\forall x\exists y\big(B(x,y)\wedge\forall z\big((z\neq y)\rightarrow\neg B(x,z)\big)\big)$$

Negating Multiple Quantifiers

The negation rules for single quantifiers:

- $\neg \forall x P(x) = \exists x \neg P(x)$

- $\neg \exists x P(x) = \forall x \neg P(x)$

- Essentially, you change the quantifier(s), and negate what it's quantifying

Example

Express the negation of the statement $\forall x \exists y (xy = 1)$ so that no negation precedes a quantifier

Solution

The negation is: $\neg \forall x \exists y (xy = 1)$

Which is equivalent: $\equiv \exists x \neg \exists y (xy = 1)$

$\equiv \exists x \forall y \neg (xy = 1)$

$\equiv \exists x \forall y (xy \neq 1)$

$\neg \left(\forall x \exists y \forall z P(x, y, z) \right) = \exists x \neg \left(\exists y \forall z P(x, y, z) \right)$

$= \exists x \forall y \neg \left(\forall z P(x, y, z) \right)$

$= \exists x \forall y \exists z \neg P(x, y, z)$

Consider $\neg (\forall x \exists y \, P(x,y)) = \exists x \forall y \, \neg P(x,y)$
- The left side is saying "for all x, there exists a y such that P is true"
- To disprove it (negate it), you need to show that "there exists an x such that for all y, P is false"

Consider $\neg (\exists x \forall y \, P(x,y)) = \forall x \exists y \, \neg P(x,y)$
- The left side is saying "there exists an x such that for all y, P is true"
- To disprove it (negate it), you need to show that "for all x, there exists a y such that P is false"

Exercises   *Section* 1.4 – **Nested Quantifiers**

1. Translate these statements into English, where the domain for each variable consists of all real numbers

    a) $\forall x \exists y (x < y)$

    b) $\exists x \forall y (xy = y)$

    c) $\forall x \forall y (((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$

    d) $\forall x \forall y (((x \geq 0) \wedge (y \geq 0)) \rightarrow (xy \geq 0))$

    e) $\forall x \forall y \exists z (xy = z)$

    f) $\forall x \forall y \exists z (x = y + z)$

2. Let $Q(x, y)$ be the statement "x has sent an e-mail message to y," where the domain for both x and y consists of all students in your class. Express each of these quantifications in English

    a) $\exists x \exists y Q(x, y)$

    b) $\exists x \forall y Q(x, y)$

    c) $\forall x \exists y Q(x, y)$

    d) $\exists y \forall x Q(x, y)$

    e) $\forall y \exists x Q(x, y)$

    f) $\forall x \forall y Q(x, y)$

3. Express each of these statements using predicates, quantifiers, logical connectives, and mathematical operators where the domain consists of all integers.

    a) The product of two negative integers is positive.

    b) The average of two positive integers is positive.

    c) The difference of two negative integers is not necessarily negative.

    d) The absolute value of the sum of two integers does not exceed the sum of the absolute values of these integers.

4. Rewrite these statements so that the negations only appear within the predicates

    a) $\neg \exists y \forall x P(x, y)$

    b) $\neg \forall x \exists y P(x, y)$

    c) $\neg \exists y (Q(y) \wedge \forall x \neg R(x, y))$

5. Express the negations of each of these statements so that all negation symbols immediately precede predicates.

    a) $\forall x \exists y \forall z T(x, y, z)$

    b) $\forall x \exists y P(x, y) \vee \forall x \exists y Q(x, y)$

6. Let $T(x, y)$ mean that student x likes cuisine y, where the domain for x consists of all students at your school and the domain for y consists of all cuisines. Express each of these statements by a simple English sentence.

   a) $\neg T(A, J)$

   b) $\exists x T(x, \text{Korean}) \wedge \forall x Tx(x, \text{Mexican})$

   c) $\exists y (T(\text{Monique}, y) \vee T(\text{Jay}, y))$

   d) $\forall x \forall z \exists y ((x \neq z) \rightarrow \neg(T(x, y) \wedge T(z, y)))$

   e) $\exists x \exists z \forall y (T(x, y) \leftrightarrow T(z, y))$

   f) $\forall x \forall z \exists y (T(x, y) \leftrightarrow T(z, y))$

7. Let $L(x, y)$ be the statement " x loves y", where the domain for both x and y consists of all people in the world. Use quantifiers to express each of these statements.

   a) Everybody loves Jerry.
   b) Everybody loves somebody.
   c) There is somebody whom everybody loves.
   d) Nobody loves everybody.
   e) There is somebody whom Lois does not love.
   f) There is somebody whom no one loves.
   g) There is exactly one person whom everybody loves.
   h) There are exactly two people whom L loves.
   i) Everyone loves himself or herself.
   j) There is someone who loves no one besides himself or herself.

8. Let $S(x)$ be the predicate "x is a student," $F(x)$ the predicate "x is a faculty member," $A(x, y)$ the predicate "x has asked y a question," where the domain consists of all people associated with your school. Use quantifiers to express each of these statements.

   a) Lois asked Professor Fred a question.
   b) Every student has asked Professor Fred a question.
   c) Every faculty member has either asked Professor Fred a question or been asked a question by Professor Miller.
   d) Some student has not asked any faculty member a question.
   e) There is a faculty member who has never been asked a question by a student.
   f) Some student has asked every faculty member a question.
   g) There is a faculty member who has asked every other faculty member a question.
   h) Some student has never been asked a question by a faculty member.

9. Express each of these system specifications using predicates, quantifiers, and logical connectives, if necessary.

   a) Every user has access to exactly one mailbox.
   b) There is a process that continues to run during all error conditions only if the kernel is working correctly.
   c) All users on the campus network can access all websites whose url has a .edu extension.

10. Translate each of these nested quantifications into an English statement that expresses a mathematical fact. The domain in each case consists of all real numbers

a) $\exists x \forall y (x + y = y)$

b) $\forall x \forall y (((x \geq 0) \wedge (y < 0)) \rightarrow (x - y > 0))$

c) $\exists x \exists y (((x \leq 0) \wedge (y \leq 0)) \wedge (x - y > 0))$

d) $\forall x \forall y (((x \neq 0) \wedge (y \neq 0)) \leftrightarrow (xy \neq 0))$

11. Determine the truth value of each of these statements if the domain for all variables consists of all integers

a) $\forall n \exists m (n^2 < m)$

b) $\exists n \forall m (n < m^2)$

c) $\forall n \exists m (n + m = 0)$

d) $\exists n \forall m (nm = m)$

e) $\exists n \exists m (n^2 + m^2 = 5)$

f) $\exists n \exists m (n^2 + m^2 = 6)$

g) $\exists n \exists m (n + m = 4 \wedge n - m = 1)$

h) $\exists n \exists m (n + m = 4 \wedge n - m = 2)$

i) $\forall n \forall m \exists p \left(p = \dfrac{m + n}{2}\right)$

Section 1.5 – Introduction to Proofs

Some Terminology

A ***theorem*** is a statement that can be shown to be true. Theorems can also be referred to as facts or results. We demonstrate that a theorem is true with a ***proof***. A proof is a valid argument that establishes the truth of a theorem. The statements used in a proof can include ***axioms*** (or ***postulates***), which are statements we assume to be true.

Less important theorems sometimes are called ***propositions***. A less important theorem that is helpful in the proof of other results is called a ***lemma*** (***plural lemmas or lemmata***).

A ***corollary*** is a theorem that can be established directly from a theorem that has been proved.
A ***conjecture*** is a statement that is being proposed to be true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

Direct Proofs

A direct proof is a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequence steps are constructed using rules of inference, with the final step showing that q must be true.
Consider an implication: $p \rightarrow q$

- If p is false, then the implication is always true.
- Show that if p is true then q is true.

Definition

The integer n is ***even*** if there exists an integer k such that $n = 2k$, and n is ***odd*** if there exists an integer k such that $n = 2k + 1$. Two integers have the ***same parity*** when both are even or both are odd; they have ***opposite parity*** when one is even and the other is odd.

Example

Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd"

Solution

    This states: $\forall n \, P(n) \rightarrow Q(n)$, where

        $P(n)$ is "n is an odd integer"

        $Q(n)$ is "n^2 is an odd"

Using direct proof, we assume that n is odd, is a true statement. By the definition of an odd integer, it follows that $n = 2k + 1$, where k is some integer. We need to show that n^2 is odd.

$$n^2 = (2k+1)^2 \qquad \textcolor{green}{\textbf{\textit{Square both sides}}}$$
$$= 4k^2 + 4k + 1$$
$$= 2\left(2k^2 + 2k\right) + 1 \qquad \textcolor{green}{2k^2 + 2k = K}$$
$$= 2K + 1$$

By the definition of an odd integer, we can conclude that n^2 is also an odd integer.

Example

Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.
(An integer a is a perfect square if there is an integer b such that $a = b^2$.)

Solution

Using direct proof of this theorem, we assume that the hypothesis of this conditional statement is true, namely, we assume that m and n are both perfect squares.
By the definition of a perfect square:

$$\exists s \ni m = s^2 \qquad \text{There is an integer } s \text{ such that } m = s^2$$
$$\exists t \ni n = t^2$$

The goal is to show that nm is also a perfect square.

$$mn = s^2 t^2 = (ss)(tt) = (st)(st) = (st)^2$$

By the definition of a perfect square, it follows that nm is also a perfect square.

Proof by Contraposition

In logic, ***proof by contrapositive*** is a form of proof that establishes the truth or validity of a proposition by demonstrating the truth or validity of the converse of its negated parts.

To prove by contraposition, consider an implication $p \to q$, prove that $\neg q \to \neg p$,

- If the antecedent $\neg q$ is false, then the contrapositive is always true.
- Show that if $\neg q$ is true, then $\neg p$ is true

To perform an indirect proof, do a direct proof on the contrapositive.

Example

Prove that if *n* is an integer and 3*n* + 2 is odd, then *n* is odd.

Solution

The first step in a proof by contraposition is to assume that the conclusion of the conditional statement "3*n* + 2 is odd, then *n* is odd" is false. Assume that *n* is even, then by the definition of an even integer, $n = 2k$ for some integer *k*.

$$3n + 2 = 3(2k) + 2 = 6k + 2 = 2(3k + 1)$$

This show $3n + 2$ is even, because it is a multiple of 2, therefore not odd. This is the negation of the theorem of the conditional statement implies that the hypothesis is false; the original conditional statement is true.

Our proof by contraposition succeeded; we have proved the theorem "If 3*n* + 2 is odd, then *n* is odd."

Example

Prove that if $n = ab$ where *a* and *b* are positive integers, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$.

Solution

By using proof by contraposition, let assume that the conclusion of the conditional statement "if $n = ab$ where *a* and *b* are positive integers, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$ " is false.

$\left(a \le \sqrt{n}\right) \vee \left(b \le \sqrt{n}\right)$ is false.

Using the meaning of disjunction together with De Morgan's law, that implies that both $a \le \sqrt{n}$ and $b \le \sqrt{n}$ are false $\Rightarrow$ $a > \sqrt{n}$ and $b > \sqrt{n}$

Then $ab > \sqrt{n}\sqrt{n} = n \Rightarrow ab \neq n$, which contradicts the statement $n = ab$.

This is the negation of the theorem of the conditional statement implies that the hypothesis is false; the original conditional statement is true. Our proof by contraposition succeeded; we have proved the theorem "If $n = ab$ where *a* and *b* are positive integers, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$."

Vacuous and Trivial Proofs

If p is a conjunction of other hypotheses and we know one or more of these hypotheses is false, then p is false and so $p \rightarrow q$ is **vacuously** true regardless of the truth value of q.

If we know q is true then $p \rightarrow q$ is true regardless of the truth value of p, this called **Trivial Proofs**.

Example

Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

Solution

Using a vacuous proof; $P(0)$ is "If $0 > 1$, then $0^2 > 0$". Indeed, the hypothesis $0 > 1$ is false. This tells us that $P(0)$ is automatically true.

Example

Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

Solution

The proposition $P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement is true. Hence, this conditional statement, which is $P(0)$, is true.

Definition

The real number r is rational if there exist integers p and q with $q \neq 0$ such that $r = \dfrac{p}{q}$. A real number that is not rational is called irrational.

Example

Prove that the sum of two rational numbers is rational. (Note that if we include the implicit quantifiers here, the theorem we want to prove is "For every real number r and every real number s, if r and s are rational numbers, the $r + s$ is rational.)

Solution

From the definition of a rational number, that there exist integers p and q with $q \neq 0$ such that $r = \dfrac{p}{q}$, and integers t and u with $u \neq 0$ such that $s = \dfrac{t}{u}$.

$$r + s = \frac{p}{q} + \frac{t}{u} = \frac{pu + qt}{qu}$$

Because $q \neq 0$ and $u \neq 0$, it follows that $qu \neq 0$. Therefore; we have $r + s$ is rational.

Example

Prove that n is an integer and n^2 is odd, then n is odd

Solution

Suppose that n is an integer and n^2 is odd. Then, $\exists k \in \mathbb{Z} \ni n^2 = 2k + 1$.
$\Rightarrow n = \pm\sqrt{2k+1}$ (which is not useful).

By using proof by contraposition, the statement n is not odd, that means n is even.
That implies that $\exists k \in \mathbb{Z} \ni n = 2k$.

To prove the theorem, we need to show that this hypothesis implies the conclusion that n^2 is not odd, that means n^2 is even.

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2),$$ which implies that n^2 is even.

We have proved that n is an integer and n^2 is odd, then n is odd by a proof of contraposition.

Proofs by Contradiction

The basic ides of a proof of contradiction is to assume that the statement we want to prove is false. That is, the supposition that p is false followed necessarily by the conclusion q from not $\neg p$, where q is false, which implies that p is true.

Given a statement p, assume it is false, assume $\neg p$

- Prove that $\neg p$ cannot occur
  - A contradiction exists
  - Given a statement of the form $p \rightarrow q$
  - To assume it's false, you only have to consider the case where p is true and q is false

Example

Show that at least four of any 22 days must fall on the same day of the week.

Solution

Let p be the proposition "at least four of any 22 days must fall on the same day of the week"
Suppose that $\neg p$ is true $\Rightarrow$ "at most three of the 22 days fall on the same day of the week".
There are 7 days per week $\Rightarrow$ at most 3 of the chosen days could fall on that day. That contradicts the premise that we have 22 days under consideration.

If r is the statement that 22 days are chosen, that we have shown that $\neg p \rightarrow (r \wedge \neg r)$.

We know that p is true. We have proved that at least four of any 22 days must fall on the same day of the week.

Example

Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.

Solution

Let p be the proposition "$\sqrt{2}$ is irrational". Suppose that $\neg p$ is true $\Rightarrow$ "$\sqrt{2}$ is rational".
If $\sqrt{2}$ is rational, $\exists a$ *and* $b \quad \ni \sqrt{2} = \frac{a}{b}$

$$\left(\sqrt{2}\right)^2 = \left(\frac{a}{b}\right)^2 \quad \Rightarrow \quad 2 = \frac{a^2}{b^2} \quad \rightarrow \quad \underline{2b^2 = a^2}$$

It follows that a^2 is even, that implies a must also be even. Therefore, by the definition of an even integer then we can let $a = 2c$ for some integer c. Thus, $2b^2 = 4c^2 \quad \Rightarrow \quad b^2 = 2c^2$

By the definition of even, this means that b^2 is even, that implies b must also be even as well.

The assumption of $\neg p$ leads to the equation $\sqrt{2} = \frac{a}{b}$, where a and b have no common factors, but

both a and b are even, that is, 2 divides both a and b. However, our assumption $\neg p$ leads to the contradiction that 2 divides both a and b and 2 doesn't divide both a and b, $\neg p$ must be false.
That is, the statement p "$\sqrt{2}$ is irrational" is true.

Proofs of Equivalence

To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we must show that $p \to q$ and $q \to p$ are both true. The validity of this approach is based on the tautology

$$(p \leftrightarrow q) \leftrightarrow (p \to q) \wedge (q \to p)$$

Example

Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd"

Solution

Let: p is "n is odd" and q is "n^2 is odd".
The theorem has the form: "p *iff* q". To prove this theorem, we need to show that $p \to q$ and $q \to p$ are both true.

Using direct proof, we assume that n is odd, is a true statement. By the definition of an odd integer, it follows that $n = 2k + 1$, where k is some integer. We need to show that n^2 is odd.

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2\left(2k^2 + 2k\right) + 1 = 2K + 1 \qquad\qquad 2k^2 + 2k = K$$

By the definition of an odd integer, we can conclude that n^2 is also an odd integer. Therefore, $p \to q$ is true.

Suppose that n is an integer and n^2 is odd. Then, $\exists k \in \mathbb{Z} \ni n^2 = 2k + 1 \Rightarrow n = \pm\sqrt{2k+1}$ (which is not useful). By using proof by contraposition, the statement n is not odd, that means n is even. That implies that $\exists k \in \mathbb{Z} \ni n = 2k$.

To prove the theorem, we need to show that this hypothesis implies the conclusion that n^2 is not odd, that means n^2 is even. $n^2 = (2k)^2 = 4k^2 = 2\left(2k^2\right)$, which implies that n^2 is even.

We have proved that n is an integer and n^2 is odd, then n is odd by a proof of contraposition. Therefore, $q \to p$ is true.

Because $p \to q$ and $q \to p$ are both true, we have shown that the theorem is true.

Example

Show that these statements about the integer n are equivalent:

p_1 : *n is even*

p_2 : *n−1 is odd*

p_3 : n^2 *is even*

Solution

We will show that these 3 statements are equivalent by showing that the condition statements $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, $p_3 \rightarrow p_1$ are true.

Using a direct proof to show that $p_1 \rightarrow p_2$.

Suppose that n is even, then $n = 2k$ for some $k \in \mathbb{Z}$.

$$n-1 = 2k-1$$
$$= 2(k-1)+1$$

This means that $n-1$ is odd because it is of the form $2m+1$, where m is the integer $k-1$. Therefore the statement $p_1 \rightarrow p_2$ is true.

Also using a direct proof to show that $p_2 \rightarrow p_3$.

Suppose that $n-1$ is even, then $n-1 = 2k+1$ for some $k \in \mathbb{Z}$.

$$n = 2k+2$$
$$n^2 = (2k+2)^2$$
$$= 4k^2 + 8k + 4$$
$$= 2(2k^2 + 4k + 2)$$

Hence, $n-1$ is even. Therefore the statement $p_2 \rightarrow p_3$ is true.

Using a proof by contraposition to prove $p_3 \rightarrow p_1$. That is, we have to prove that if n is not even, then n^2 is not even.

To prove the theorem, we need to show that this hypothesis implies the conclusion that n^2 is not odd, that means n^2 is even. $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$, which implies that n^2 is even.

We have proved that n is an integer and n^2 is odd, then n is odd by a proof of contraposition. Therefore, $p_3 \rightarrow p_1$ is true.

This completes the proof.

Counterexamples

To show that a statement of the form $\forall x\, P(x)$ is false, we need only find a ***counterexample***, that is, an example of x for which $P(x)$ is false.

Example

Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

Solution

To show that this statement is false, we look for a counterexample, which is a particular integer that is not the sum of the squares of two integers.

To choose a counterexample, we can select 3 because it cannot be written as the sum of the squares of two integers. Let use 0 and 1 which implies $0^2 + 1^2 = 0 + 1 = 1 \neq 3$. Therefore, we can't get 3 as the sum of two terms of which is 0 or 1.

Consequently, we have shown that "Every positive integer is the sum of the squares of two integers" is false.

Mistakes in Proofs

Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it.

Example

What is wrong with this "proof?": If n^2 is positive, then n is positive.

Proof: Suppose that n^2 is positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n is positive.

Solution

Let $P(n)$ be "n is positive" and $Q(n)$ be "n^2 is positive."

The statement can be written: $\forall n\big(P(n) \to Q(n)\big)$.

A counterexample is supplied by $n = -1 \Rightarrow n^2 = 1$ is positive, but n is negative.

Exercises   *Section* 1.5 – **Introduction to Proofs**

1.   Show that the square of an even number is an even number

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

3.   Show that $m^2 = n^2$ if and only if $m = n$ or $m = -n$

4.   Use a direct proof to show that the sum of two odd integers is even.

5.   Use a direct proof to show that the sum of two even integers is even.

6.   Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.

7.   Prove or disprove that the product of two irrational numbers is irrational.

8.   Prove that if x is irrational, then $\dfrac{1}{x}$ is irrational.

9.   Prove that if x is rational and $x \ne 0$, then $\dfrac{1}{x}$ is rational.

10.   Prove the proposition $P(0)$, where $P(n)$ is the proposition "If n is a positive integer greater than 1, then $n^2 > n$." What kind of proof did you use?

11.   Let $P(n)$ be the proposition "If a and b are positive real numbers, then $(a+b)^n \ge a^n + b^n$." Prove that $P(1)$ is true. What kind of proof did you use?

12.   Show that these statements about the integer x are equivalent:
     i) $3x + 2$ *is even*   *ii*) $x + 5$ *is odd*   *iii*) x^2 *is even*

13.   Show that these statements about the real number x are equivalent:
     i) x *is irrational*   *ii*) $3x + 2$ *is irrational*   *iii*) $\frac{x}{2}$ *is irrational*

14.   Prove that at least one of the real numbers a_1, a_2, …, a_n is greater than or equal to the average of these numbers. What kind of proof did you use?

Section 1.6 − Proof Methods and Strategy

Introduction

The strategy behind constructing proofs includes selecting a proof method and then successfully constructing an argument step by step, based on this method.

Exhaustive Proof and Proof by Cases

To prove a conditional statement of the form $\left(p_1 \vee p_2 \vee \cdots \vee p_n \right) \rightarrow q$

The tautology $\left[\left(p_1 \vee p_2 \vee \cdots \vee p_n \right) \rightarrow q \right] \leftrightarrow \left[\left(p_1 \rightarrow q \right) \wedge \left(p_2 \rightarrow q \right) \wedge \cdots \wedge \left(p_n \rightarrow q \right) \right]$

can be used as a rule of inference

Such an argument is called a ***proof by cases***. Sometimes to prove that a conditional statement $p \rightarrow q$ is true, it is convenient to use a disjunction $p_1 \vee p_2 \vee \cdots \vee p_n$ instead of p as the hypothesis of the conditional statement, where p and $p_1 \vee p_2 \vee \cdots \vee p_n$ are equivalent.

Exhaustive Proof

Also known as ***proof by cases***, ***perfect induction***, or the ***brute force method***, is a method of mathematical proof in which the statement to be proved is split into a finite number of cases and each case is checked to see if the proposition in question holds.

Theorem

A proposition that has been proved to be true

- Two special kinds of theorems: Lemma and Corollary.
- Lemma: A theorem that is usually not too interesting in its own right but is useful in proving another theorem.
- Corollary: A theorem that follows quickly from another theorem.

Example

Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$

Solution

Using a proof by exhaustion:

For $n = 1$: $(n+1)^3 = 2^3 = 8 \geq 3^1 = 3$

For $n = 2$: $(n+1)^3 = 3^3 = 27 \geq 3^2 = 9$

For $n = 3$: $(n+1)^3 = 4^3 = 64 \geq 3^3 = 27$

For $n = 4$: $(n+1)^3 = 5^3 = 125 \geq 3^4 = 81$

We have used the method of exhaustion to prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$

Example

Prove that if n is an integer, then $n^2 \geq n$

Solution

Case 1: When $n = 0$, that implies to $0^2 \geq 0$. It follows that $n^2 \geq n$ is true.

Case 2: When $n \geq 1$, $\Rightarrow n \cdot n \geq 1 \cdot n$, we obtain $n^2 \geq n$ It follows that $n^2 \geq n$ is true.

Case 3: When $n \leq -1$, but $n^2 \geq 0$. It follows that $n^2 \geq n$ is true.

Because the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

Example

Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.

Solution

Using the proof by contraposition:
Suppose that x and y are not both even. That is, x is odd or y is odd (or both).
Assume that x is odd, so that $x = 2k + 1$ for some integer k.
Case 1: y even $\Rightarrow y = 2n$
$$x + y = 2k + 1 + 2n = 2(k + n) + 1 \text{ is } odd$$
Case 2: y odd $\Rightarrow y = 2n + 1$
$$xy = (2k + 1)(2n + 1) = 4kn + 2k + 2n + 1 = 2(2kn + k + n) + 1 \text{ is } odd$$
This completes the proof by contraposition.

Existence Proofs

A statement $\exists x\, P(x)$ is called an **existence proof**. There are several ways to proof a theorem of this type.

➢ **Constructive**: Find a specific value of c for which $P(c)$ exists

➢ **Nonconstructive**: Show that such a c exists, but don't actually find it. Assume it does not exist, and show a contradiction

Example

Show that a square exists that is the sum of two other squares

Solution

Proof: $3^2 + 4^2 = 5^2$

Because we have displayed a positive integer that can be written as the sum of two squares, we are done.

Example

Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Solution

Proof: $1729 = 10^3 + 9^3 = 12^3 + 1^3$

We proved that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Example

Show that a cube exists that is the sum of three other cubes

Solution

Proof: $3^3 + 4^3 + 5^3 = 6^3$

We proved that a cube exists that is the sum of three other cubes.

Uniqueness Proofs

A theorem may state that only one such value exists. Theorem statements that involve the word ``unique''
are known as **uniqueness theorems**. Typically the proof of such a statement follows the idea that we
assume there are two elements that satisfy the conclusion of the statement and then show that these
elements are identical.

Existence: We show that an element x with the desired property exists.
Uniqueness: We show that if $y \neq x$, then y does not have the desired property.

Equivalently, we can show that if x and y both have the desired property, then $x = y$.

Example

Show that if x and y are real numbers and $x \neq 0$, then there is a unique real number r such that $xr + y = 0$

Solution

The solution of $xr + y = 0$ is $r = -\dfrac{y}{x}$ because $x\left(-\dfrac{y}{x}\right) + y = -y + y = 0$. Consequently, a real number r

exists for which $xr + y = 0$. This is the existence part of the proof.

Suppose that s is a real number such that $xs + y = 0$, then $xr + y = xs + y$, where $r = -\dfrac{y}{x}$.

$$xr + y = xs + y \quad \Rightarrow \quad xr = xs \ \ (x \neq 0) \quad \rightarrow r = s$$

This means that if $s \neq r$, then $xs + y \neq 0$. This establishes the uniqueness part of the proof.

Proof Strategies

Usually, when you are working on a proof, you should use the logical forms of the givens and goals to
guide you in choosing what proof strategies to use. Generally, if the statement is a conditional statement,
we should try a direct proof; if this fails, we can try an indirect proof. If neither of these approaches
works, you might try a proof by contradiction.

Example

Given two positive numbers x and y, their **arithmetic mean** is $\dfrac{x+y}{2}$ and their **geometric mean** is $\sqrt{xy}$.

When we compare the arithmetic and geometric means of pairs of distinct positive real numbers, we find
that the arithmetic mean is always greater than the geometric mean. For example, when $x = 4$ and $y = 6$,

we have $\dfrac{4+6}{2} = 5 > \sqrt{4 \cdot 6} = \sqrt{24}$. Can we prove that this inequality is always true?

Solution

To prove $\dfrac{x+y}{2} > \sqrt{xy}$

$$\left(\frac{x+y}{2}\right)^2 > \left(\sqrt{xy}\right)^2$$

$$\frac{x^2+2xy+y^2}{4} > xy$$

$$x^2+2xy+y^2 > 4xy$$

$$x^2-2xy+y^2 > 0$$

$$(x-y)^2 > 0$$

It is true inequality, since $(x-y)^2 > 0$ when $x \neq y$, it follows that $\frac{x+y}{2} > \sqrt{xy}$.

Suppose that x and y are distinct positive real numbers. Then $(x-y)^2 > 0$ because the square of a nonzero real number is positive.

$$x^2-2xy+y^2 > 0$$

$$x^2-2xy+y^2+4xy > 4xy$$

$$x^2+2xy+y^2 > 4xy$$

$$(x+y)^2 > 4xy \qquad \textit{divide both sides by 4}$$

$$\frac{(x+y)^2}{4} > xy \qquad \textit{Square roots both sides}$$

$$\frac{x+y}{2} > \sqrt{xy}$$

We conclude that if x and y are distinct positive real numbers, then their arithmetic mean $\frac{x+y}{2}$ is greater than the geometric mean $\sqrt{xy}$

Fermat's **Last Theorem**

The eqaution $\qquad x^n + y^n = z^n$

Has no solutions in integers x, y, and z with $xyz \neq 0$ whenever n is an integer with $n > 2$.

Exercises   *Section* 1.6 − Proof Methods and Strategy

1.   Prove that $n^2 + 1 \geq 2^n$ when n is a positive integer with $1 \leq n \leq 4$

2.   Prove that there are no positive perfect cubes less than 1000 that are the sum of the cubes of two positive integers.

3.   Prove that if x and y are real numbers, then $\max(x, y) + \min(x, y) = x + y$. (*Hint*: Use a proof by cases, with the two cases corresponding to $x \geq y$ and $x < y$, respectively.)

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

5.   Prove that either $2 \cdot 10^{500} + 15$ or $2 \cdot 10^{500} + 16$ is not a perfect square

6.   Prove that there exists a pair of consecutive integers such that one of these integers is a perfect square and the other is a perfect cube.

7.   Suppose that a and b are odd integers with $a \neq b$. Show there is a unique integer c such that $|a - c| = |b - c|$

Section 1.7 – **Sets**

Introduction

A set is an unordered collection of objects, called elements or members of the set. A set is said to contain its elements. We write $a \in A$ to denote that a is an element of the set A. The notation $a \notin A$ denotes that a is not an element of the set A.

Example

Colors of a rainbow: {red, orange, yellow, green, blue, purple}

Example

States of matter {solid, liquid, gas, plasma}

Example

The set V of all vowels in the English alphabet can be written as: $V = \{a, e, i, o, u\}$

Example

The set O of odd positive integers less than 10 can be expressed by $O = \{1, 3, 5, 7, 9\}$

Example

The set of positive integers less than 100 can be denoted by $\{1, 2, 3, \ldots, 99\}$

➢ Another way to describe a set is to use ***set builder*** notation.

For instance, the set O of odd positive integers less than 10 can be written as

$O = \{x \mid x \text{ is an odd positive integer less than } 10\}$

Or, specifying the universe as the set of positive integers, as

$O = \{x \in \mathbb{Z}^{+} \mid x \text{ is an odd and } x < 10\}$

The set of *Natural numbers*: $\qquad\qquad$ $\mathbb{N} = \{0,\ 1,\ 2,\ 3,\ \ldots\}$

The set of *Integers*: $\qquad\qquad\qquad$ $\mathbb{Z} = \{\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \ldots\}$

The set of *positive integers*: $\qquad$ $\mathbb{Z}^+ = \{1,\ 2,\ 3,\ \ldots\}$

The set of *Rational numbers*: $\qquad$ $\mathbb{Q} = \left\{ \dfrac{p}{q} \middle| p \in \mathbb{Z},\ q \in \mathbb{Z},\ and\ q \neq 0 \right\}$

The set of *Real numbers*: $\qquad\qquad$ $\mathbb{R}$

The set of *positive Real numbers*: $\quad$ $\mathbb{R}^+$

The set of *Complex numbers*: $\qquad$ $\mathbb{C}$

Intervals

The notations for intervals of real numbers. When a and b are real numbers with $a < b$, we write

$$[a,\ b] = \{x | a \leq x \leq b\}$$

$$[a,\ b) = \{x | a \leq x < b\}$$

$$(a,\ b] = \{x | a < x \leq b\}$$

$$(a,\ b) = \{x | a < x < b\}$$

$[a,\ b]$ is called **closed interval** from a to b.

$(a,\ b)$ is called **open interval** from a to b.

Definition

Two sets are equal *iff* they have the same elements. Therefore, if A and B are sets, then A and B are equal *iff* $\forall x (x \in A \leftrightarrow x \in B)$. We write $A = B$ if A and B are equal sets

Example

The set $\{1, 3, 5\}$ and $\{3, 5, 1\}$ are equal, because they have the same elements.

➢ Order of the elements of a set are listed does not matter.
$\qquad \{1, 2, 3, 4, 5\} = \{5, 4, 3, 2, 1\}$

The Empty Set

There is a special set that has no elements. This set is called the ***empty set***, or ***null set***, and is denoted by ∅. The empty set can also denoted by { }.

A set with one element is called a ***singleton set***.

Venn Diagrams

In Venn diagrams the ***universal set*** U, which contains all the objects under consideration, is represented by a rectangle.

  Represents sets graphically

     ✓ The box represents the universal set

     ✓ Circles represent the set(s)

  Consider set S, which is the set of all vowels in the alphabet

  The individual elements are usually not written in a Venn diagram
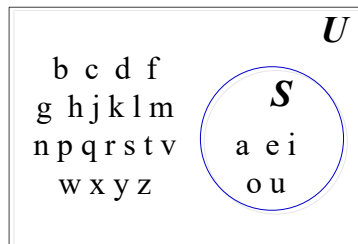
Example

Draw a Venn diagram that represents V, the set of vowels in the English alphabet.

Solution
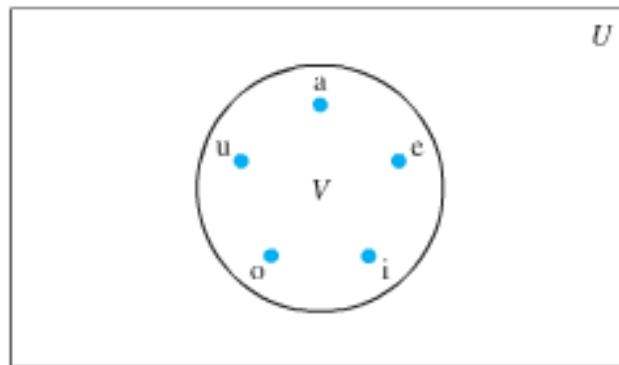
Subset

Set A is a subset of set B (written $A \subseteq B$) if and only if every element of A is also an element of B. Set A is a proper subset (written $A \subset B$) if $A \subseteq B$ and $A \neq B$

We see that $A \subseteq B$ if and only if the quantification:

$\forall x \ (x \in A \rightarrow x \in B)$ is true

Note that to show that A is not a subset of B we need only find one element $x \in A$ with $x \notin B$. Such an x is counterexample to the claim that $x \in A$ implies $x \in B$.

Showing that A is a Subset of B – To show that $A \subseteq B$, show that if x belong to A then a also belong to B.

Showing that A is Not a Subset of B – To show that $A \nsubseteq B$, find a single $x \in A$ such that $x \notin B$.

Example

$\{1, 2, 8\} \subseteq \{1, 2, 3, 4, 5, 6, 7\}$

Proper subsets: Venn diagram $S \subset R$
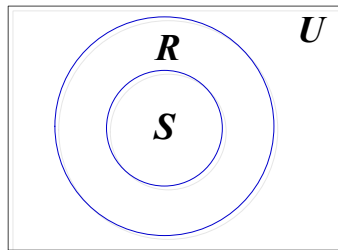
Example

The set of people who have taken discrete mathematics at the school is not a subset of all computer science majors at the school if there is at least one student who has taken discrete mathematics who is not a computer science major.

Theorem

For every set S

   i. $\varnothing \subseteq S$ and

  ii. $S \subseteq S$

Proof (*i*)

Let S be a set. To show $\varnothing \subseteq S$, we must show that $\forall x (x \in \varnothing \rightarrow x \in S)$ is true.

Because the empty set contains no elements, it follows that $x \in \varnothing$ is always false. It follows that the conditional statement $x \in \varnothing \rightarrow x \in S$ is always true, because its hypothesis is always false and a conditional statement with a false hypothesis is true. Therefore, $\forall x (x \in \varnothing \rightarrow x \in S)$ is true.

This complete the proof of (*i*) using a vacuous proof.

Showing Two Sets are Equal – To show that two sets A and B are equals, show that $A \subseteq B$ and $B \subseteq A$.

Example

We have the sets $A = \{\varnothing, \ \{a\}, \ \{b\}, \ \{a,b\}\}$ *and* $B = \{x | x$ *is a subset of the set* $\{a,b\} \}$

Solution

    These two sets are equal, that is, $A = B$.

    Note: $\{a\} \in A$ *but* $a \notin A$

The Size of a Set

Definition

Let S be a set. If there are exactly n distinct elements in S where n is a nonegative integer, we say that S is a finite set and that n is the **cardinality** of S. The cardinality of S is denoted by $|S|$.

- Let A be the set of odd positive integers less than 10. $|A| = 5$

- Let S be the set of of letter in English alphabet. $|S| = 26$

- The null set has no elements. $|\varnothing| = 0$

Definition

A set is said to be infinite if it is not finite.

Example: The set of positive integers is infinite.

Power Sets

Definition

Given a set *S*, the power set of *S* is the set of all subsets of the set *S*. The power set of *S* is denoted by
$$\mathcal{P}(S)$$

Note that the empty set and the set itself are memebers of the set of subsets.

Example

What is the power set of the set {0, 1, 2}?

Solution

$$\mathcal{P}(\{0,1,2\}) = \{\varnothing,\ \{0\},\ \{1\},\ \{2\},\ \{0,1\},\ \{0,2\},\ \{1,2\},\ \{0,1,2\}\}$$

Example

What is the power set of the empty set? What is the power set of the set {∅}?

Solution

$$\mathcal{P}(\varnothing) = \{\varnothing\}$$
$$\mathcal{P}(\{\varnothing\}) = \{\varnothing,\ \{\varnothing\}\}$$

Cartesian Products

Definition

The ***order n-tuple*** $\left(a_1, a_2, \ldots, a_n\right)$ is the ordered collection that has a_1 as its first element, a_2 as its second element, ..., and a_n as its nth element.

Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. Hence

$$A \times B = \{(a, b) | a \in A \land b \in B\}$$

Example

Let A represent the set of all students at a university, and let B represent the set of all courses offered at the university. What is the Cartesian product $A \times B$ and how can it be used?

Solution

The Cartesian product $A \times B$ consists of all the ordered pairs of the form (a, b), where a is a student at the university and b is a course offered at the university. One way to use the set $A \times B$ is to represent all possible enrollments of students in courses at the university.

Example

What is the Cartesian product $A = \{1, 2\}$ and $B = \{a, b, c\}$?

Solution

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

Example

Show that the Cartesian product $B \times A$ is not equal to $A \times B$, where $A = \{1, 2\}$ and $B = \{a, b, c\}$?

Solution

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$
$$B \times A = \{(a, 1), (a, 2), (b, 1), (b\ 2), (c, 1), (c, 2)\}$$

$$\Rightarrow A \times B \neq B \times A$$

Definition

The ***Cartesian product*** of the sets A_1, A_2,..., A_n, denoted by $A_1 \times A_2 \times ... \times A_n$, is the set of ordered n-tuples $(a_1, a_2,..., a_n)$, where a_i belongs to A_i for $i = 1, 2, ..., n$. In other words,

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) \mid a_i \in A_i \ \ for \ i = 1,2,...,n\}$$

Example

What is the Cartesian product $A \times B \times C$, where A = {0, 1}, B = {1, 2}, and C = {0, 1, 2}

Solution

$$A \times B \times C = \{(0, 1, 0), (0, 1, 1), (0, 1, 2),(0, 2, 0), (0, 2, 1), (0, 2, 2),$$
$$(1, 1, 0), (1, 1, 1), (1, 1, 2), (1, 2, 0), (1, 2, 1), (1, 2, 2)\}$$

Example

Suppose that A = {1, 2}, find A^2 and A^3

Solution

$$A^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$$
$$A^3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$$

Example

What are the ordered pairs in the less than or equal relation, which contains (a, b) if $a \leq b$, on the set {0,1,2,3} ?

Solution

The ordered pairs in ***R*** are:

(0, 0), (0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)

Using Set Notation with Quantifiers

For example $\forall x \in S(P(x))$ denotes

Universal quantification of $P(x)$ over all elements in the S

Shorthand for $\forall x(x \in S \rightarrow P(x))$

$\exists x \in S(P(x))$ denotes

Existential quantification of $P(x)$ over all elements in the S

Shorthand for $\exists x(x \in S \wedge P(x))$

Example

What do the statements $\forall x \in R\left(x^2 \geq 0\right)$ and $\exists x \in Z\left(x^2 = 1\right)$ mean?

Solution

The statement $\forall x \in R\left(x^2 \geq 0\right)$ states that for every real numbers x, $x^2 \geq 0$.

This statement can be expressed as "The square of every real number is nonnegative." This is a true statement.

The statement $\exists x \in Z\left(x^2 = 1\right)$ states that there exists an integer x, $x^2 = 1$.

This statement can be expressed as "The is an integer whose square is 1." This is also a true statement because $x = 1$ *or* -1 such an integer.

Exercises   *Section 1.7 – Sets*

1.   List the members of these sets

a) $\{x \mid x \text{ is a real number such that } x^2 = 1\}$

b) $\{x \mid x \text{ is a positive integer less than } 12\}$

c) $\{x \mid x \text{ is the square of an integer and } x < 100\}$

d) $\{x \mid x \text{ is an integer such that } x^2 = 2\}$

2.   Determine whether each these pairs of sets are equal.

a) $\{1,3,3,3,5,5,5,5,5\}, \quad \{5,3,1\}$

b) $\{\{1\}\}, \quad \{1, \{1\}\}$

c) $\varnothing, \quad \{\varnothing\}$

3.   For each of the following sets, determine whether 2 is an element of that set.

a) $\{x \in \mathbb{R} \mid x \text{ is an integer greater than } 1\}$

b) $\{x \in \mathbb{R} \mid x \text{ is the square of an integer}\}$

c) $\{2, \{2\}\}$

d) $\{\{2\}, \{\{2\}\}\}$

e) $\{\{2\}, \{2, \{2\}\}\}$

f) $\{\{\{2\}\}\}$

4.   Determine whether each of these statements is true or false

a) $0 \in \varnothing$

b) $\varnothing \in \{0\}$

c) $\{0\} \subset \varnothing$

d) $\varnothing \subset \{0\}$

e) $\{0\} \in \{0\}$

f) $\{0\} \subset \{0\}$

g) $\{\varnothing\} \subseteq \{\varnothing\}$

h) $x \in \{x\}$

i) $\{x\} \subseteq \{x\}$

j) $\{x\} \in \{x\}$

k) $\{x\} \in \{\{x\}\}$

l) $\varnothing \subseteq \{x\}$

m) $\varnothing \in \{x\}$

5. Use a Venn Diagram to illustrate the relationships $A \subset B$ and $B \subset C$.

6. Use a Venn Diagram to illustrate the relationships $A \subset B$ and $A \subset C$.

7. Suppose that A, B, and C are sets such that $A \subseteq B$ and $B \subseteq C$. Show that $A \subseteq C$

8. What is the cardinality of each of these sets?

 a) $\{a\}$

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

 c) $\{a, \{a\}\}$

 d) $\{a, \{a\}, \{a, \{a\}\}\}$

9. How many elements does each of these sets have where a and b are distinct elements?

 a) $\mathcal{P}(\{a, b, \{a, b\}\})$

 b) $\mathcal{P}(\{\varnothing, a, \{a\}, \{\{a\}\}\})$

 c) $\mathcal{P}(\mathcal{P}(\varnothing))$

10. What is the Cartesian product $A \times B \times C$, where A is the set of all airlines and B and C are both the set of all cities in the United States? Give an example of how this Cartesian product can be used.

11. What is the Cartesian product $A \times B$, where A is the set of all courses offered by the mathematics department and B is the set of mathematics professors at this university? Give an example of how this Cartesian product can be used.

12. Let A be a set. Show that $\varnothing \times A = A \times \varnothing = \varnothing$

Section 1.8 – Set Operations

Union of Two Sets

Let A and B be sets, the **union** of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both.

$$A \cup B = \{x \,|\, x \in A \;\vee\; x \in B\}$$
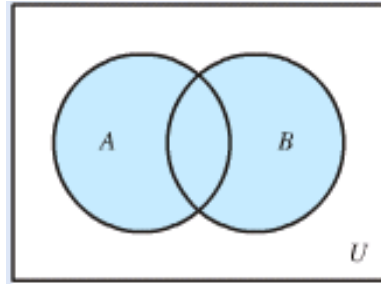
Example

Let $A = \{1,3,5,7,9,11\}$, $B = \{3,6,9,12\}$. Find each set $A \cup B$

Solution

$$A \cup B = \{1,3,5,6,7,9,11,12\}$$

Intersection of Two Sets

Let A and B be sets, the **intersection** of the sets A and B, denoted by $A \cap B$, is the set containing those elements in both A or in B.

$$A \cap B = \{x \,|\, x \in A \;\wedge\; x \in B\}$$
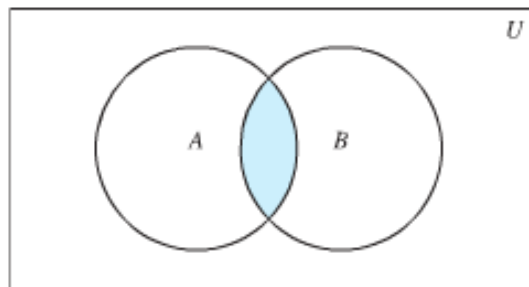
Example

Let $A = \{3,6,9\}$, $B = \{2,4,6,8\}$, find $A \cap B$

Solution

$$A \cap B = \{6\}$$

Disjoint Sets

For any sets A and B, if A and B are **disjoint** sets, then their intersection is the empty set $A \cap B = \phi$
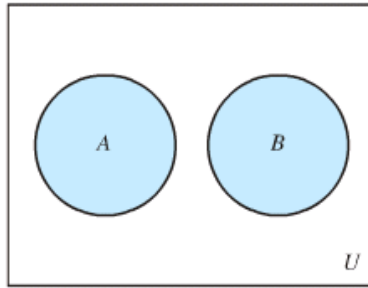
Example

Let $A = \{1,3,5,7,9\}$, $B = \{2,4,6,8,10\}$, find $A \cap B$

Solution

$A \cap B = \varnothing$. Therefore, A and B are disjoint.

Complement of a Set

Let A be any set, with U representing the universal set, then the complement of A.

$$A' \; or \; \overline{A} = \{x \mid x \notin A \; and \; x \in U\}$$
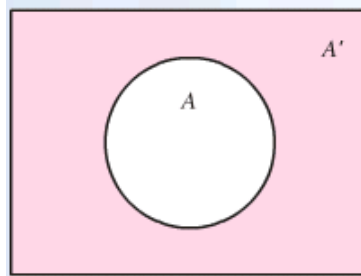
Difference of two Sets

Let A and B be sets, the **difference** of A and B, denoted by $A - B$, is the set containing those elements that are A but not in B. The difference of A and B is also called the complement of B with respect to A.
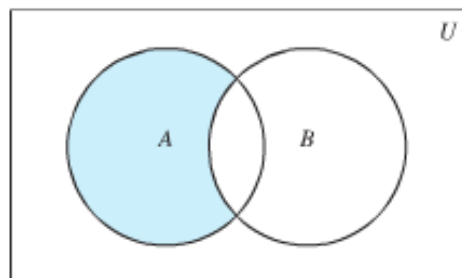
Example

Find {1, 3, 5} − {1, 2, 3}

Solution

    {1, 3, 5} − {1, 2, 3} = {5}

Example

What is the difference of the set of computer science majors at the school and the set of mathematics majors at the school?

Solution

The difference is the set of all computer science majors at your school are not also mathematics majors.

Example

Let A be the set of positive integers greater than 10 (with universal set the set of all positive integers). Find $\overline{A}$

Solution

    $\overline{A} = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10\}$

Set Identities

Identity	Name
$A \cap U = A$ $A \cup \varnothing = A$	Identity laws
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{\left(\overline{A} \right)} = A$	Complementation laws
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap (C)$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$	Complement laws

Example

Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Solution

1. We need to show that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$

   Suppose that $x \in \overline{A \cap B} \;\Rightarrow\; x \notin A \cap B$ (by the definition of complement)

   Using the definition of the intersection, we see that the proposition $\neg\big((x \in A) \wedge (x \in B)\big)$ is true.

$\neg(x \in A) \;or\; \neg(x \in B)$	*By applying De Morgan's law of the proposition*
$x \notin A \;or\; x \notin B$	*Using the definition of the negation of proposition*
$x \in \overline{A} \;or\; x \in \overline{B}$	*Using the complement of a set*
$x \in \overline{A} \cup \overline{B}$	*Using the definition of union*
$\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$	

2. We need to show that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$

   Suppose that $x \in \overline{A} \cup \overline{B} \;\Rightarrow\; x \in \overline{A} \;or\; x \in \overline{B}$ (by the definition of union)

$x \notin A \;or\; x \notin B$	*Using the definition of the complement*

65

$\neg(x \in A) \ \vee \ \neg(x \in B)$ *True*

$\neg(x \in A) \ \wedge \ \neg(x \in B)$ *By applying De Morgan's law of the proposition*

$\neg(x \in A \cap B)$ *Using the definition of the intersection*

$x \in \overline{A \cap B}$ *Using the definition of complement*

That shows that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$

Therefore; $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Example

Use set builder notation and logical equivalences to establish the first De Morgan law $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Solution

$\overline{A \cap B} = \{x \mid x \notin A \cap B\}$ *By definition of complement*

$= \{x \mid \neg(x \in (A \cap B))\}$

$= \{x \mid \neg(x \in A \ \wedge \ x \in B)\}$ *By definition of complement*

$= \{x \mid \neg(x \in A) \vee \neg(x \in B)\}$ *By the first De Morgan law for logical equivalences*

$= \{x \mid x \notin A \ \vee \ x \notin B\}$ *By definition of does not belong symbol*

$= \{x \mid x \in \overline{A} \ \vee \ x \in \overline{B}\}$ *By definition of complement*

$= \{x \mid x \in \overline{A} \cup \overline{B}\}$ *By definition of union*

$= \overline{A} \cup \overline{B}$

Example

Use a membership table to show that $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Solution

A Membership Table for the Distributive Property							
A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Example

Let A, B, and C be sets. Show that $\overline{A\cup(B\cap C)}=\left(\overline{C}\cup\overline{B}\right)\cap\overline{A}$

<u>*Solution*</u>

$\overline{A\cup(B\cap C)}=\overline{A}\cap\overline{\left(B\cap C\right)}$ *By the first De Morgan law*

$=\overline{A}\cap\left(\overline{B}\cup\overline{C}\right)$ *By the second De Morgan law*

$=\left(\overline{B}\cup\overline{C}\right)\cap\overline{A}$ *By the commutative law for intersection*

$=\left(\overline{C}\cup\overline{B}\right)\cap\overline{A}$ *By the commutative law for union*

Generalized Unions and Intersections
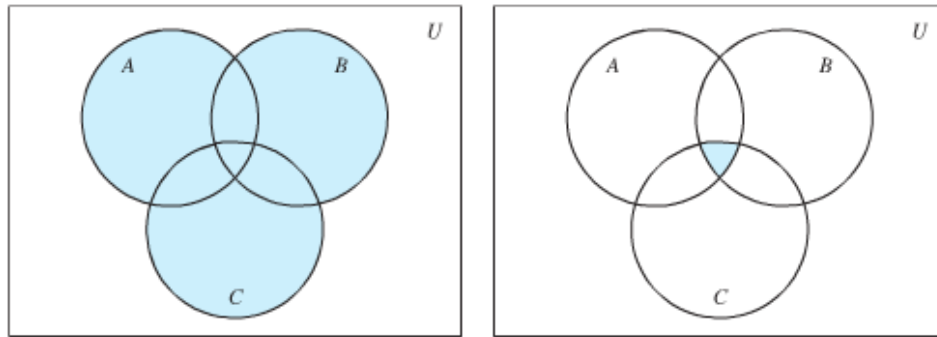
$A\cup(B\cup C)=(A\cup B)\cup C$

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

Example

Let $A = \{0, 2, 4, 6, 8\}$, $B = \{0, 1, 2, 3, 4\}$, and $C = \{0, 3, 6, 9\}$. What are $A\cup B\cup C$ and $A\cap B\cap C$

<u>*Solution*</u>

$A\cup B\cup C=\{0,\ 1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9\}$

$A\cap B\cap C=\{0\}$

Definition

The ***union*** of a collection of sets is the set that contains those elements that are members of at least one set in the collection.

$$A_1\cup A_2\cup\cdots\cup A_n=\bigcup_{i=1}^{n}A_i$$

Definition

The *intersection* of a collection of sets is the set that contains those elements that are members of at all the sets in the collection.

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

For $i = 1, 2, \ldots$, let $A_i = \{i, i+1, i+2, \ldots\}$. Then,

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{1, 2, 3, \ldots\}$$

$$\bigcap_{i=1}^{n} A_i = \bigcap_{i=1}^{n} \{i, i+1, i+2, \ldots\} = \{n, n+1, n+2, \ldots\} = A_n$$

Exercises   *Section* **1.8** − **Set Operations**

1. Let A be the set of students who live within one mile of school and let B be the set of students who walk to classes. Describe the students in each of these sets.
    a) $A \cap B$
    b) $A \cup B$
    c) $A - B$
    d) $B - A$

2. Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{0, 3, 6\}$
    a) $A \cup B$
    b) $A \cap B$
    c) $A - B$
    d) $B - A$

3. Let $A = \{a, b, c, d, e\}$ and $B = \{a, b, c, d, e, f, g, h\}$
    a) $A \cup B$
    b) $A \cap B$
    c) $A - B$
    d) $B - A$

4. Prove the domination laws by showing that
    a) $A \cup U = U$
    b) $A \cap U = A$
    c) $A \cup \varnothing = A$
    d) $A \cap \varnothing = \varnothing$

5. Prove the complement laws by showing that
    a) $A \cup \overline{A} = U$
    b) $A \cap \overline{A} = \varnothing$

6. Show that
    a) $A - \varnothing = A$
    b) $\varnothing - A = \varnothing$

7. Prove the absorption law by showing that if A and B are sets, then
    a) $A \cap (A \cup B) = A$

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

8. Show that if A, B, and C are sets, then $\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$

9. Let A and B be sets. Show that
   a) $(A \cap B) \subseteq A$
   b) $A \subseteq (A \cup B)$
   c) $(A - B) \subseteq A$
   d) $A \cap (B - A) = \varnothing$
   e) $A \cup (B - A) = A \cup B$

10. Draw the Venn diagrams for each of these combinations of the sets A, B, and C.
   a) $A \cap (B - C)$
   b) $(A \cap B) \cup (A \cap C)$
   c) $(A \cap \overline{B}) \cup (A \cap \overline{C})$
   d) $\overline{A} \cap \overline{B} \cap \overline{C}$
   e) $(A - B) \cup (A - C) \cup (B - C)$

11. Show that $A \oplus B = (A \cup B) - (A \cap B)$

12. Show that $A \oplus B = (A - B) \cup (B - A)$

Section 1.9 – Functions

Definition

Let A and B be nonempty sets. A function f from A and B is an assignment of exactly one element of B to each of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f : A \rightarrow B$
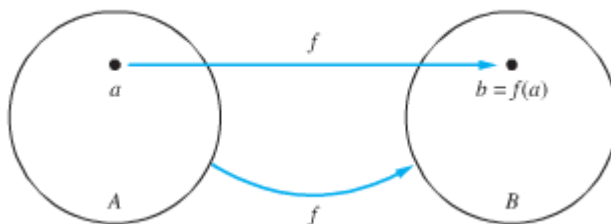
When we define a function we specify its domain, its codomain, and the mapping of elements of the domain to elements in the codomain. Two functions are **equal** when they have the same domain, have the same codomain, and map each element of their common domain to the same element in their common codomain.

Example

What are the domain, codomain, and range of the function that assigns grades to students shown below
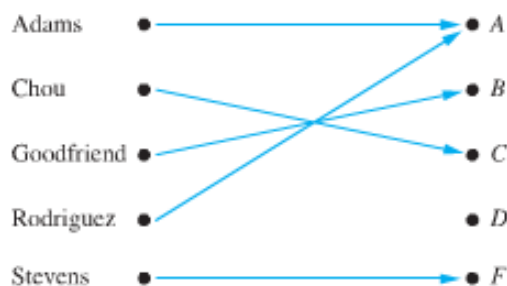
Solution

    The domain is the set G = {Adams, Chou, Goodfriend, Rodriguez, Stevens}

    The codomain is the set {A, B, C, D, F}

    The range of G is the set {A, B, C, F}

Example

Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ assign the square of an integer to this integer. Then $f(x) = x^2$, where the domain of f is the set of all integers, the codomain of f is the set of all integers, and the range of f is the set of all integers that are perfect squares, namely, {0, 1, 4, 9, . . .}

Definition

Let f_1 and f_2 be functions from A to $\mathbf{R}$. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from A to $\mathbf{R}$ defined for all $x \in A$ by

$$\left(f_1 + f_2\right)(x) = f_1(x) + f_2(x)$$

$$\left(f_1 f_2\right)(x) = f_1(x) f_2(x)$$

Example

Let f_1 and f_2 be functions from $\mathbf{R}$ to $\mathbf{R}$ such that $f_1(x) = x^2$ and $f_2 = x - x^2$. What are the functions $f_1 + f_2$ and $f_1 f_2$?

Solution

$$\left(f_1 + f_2\right)(x) = x^2 + \left(x - x^2\right) = x$$

$$\left(f_1 f_2\right)(x) = x^2\left(x - x^2\right) = x^3 - x^4$$

Definition

Let f be function from A to B and Let S be a subset of A. The **image** of S under the function f is the subset of B that consists of the images of the elements of S. We denote the image of S by $f(S)$, so

$$f(S) = \left\{t \mid \exists s \in S\ \left(t = f(s)\right)\right\}$$

We also use the shorthand $\left\{f(S) \mid s \in S\right\}$ to denote this set.

One-to-One and Onto Functions

Definition

A function f is said to be *one-to-one*, or an **injunction**, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. A function is said to be **injective** if it is one-to-one.

Note:

A function f is one-to-one $(1 - 1)$ if different inputs have different outputs that is,

$$if\ a \neq b, \quad then \quad f(a) \neq f(b)$$

A function f is one-to-one $(1 - 1)$ if different outputs the same, the inputs are the same – that is,

$$if\ f(a) = f(b), \quad then \quad a = b$$

72

Remark

We can express that f is one-to-one using the qualifier as $\forall a \forall b (f(a) = f(b) \rightarrow a = b)$ or equivalently $\forall a \forall b (a \neq b \rightarrow f(a) \neq f(b))$, where the universe of disclosure is the domain of the function.

Example

Determine whether the function f from $\{a, b, c, d\}$ to $\{1, 2, 3, 4, 5\}$ with $f(a) = 4$, $f(b) = 5$, $f(c) = 1$, and $f(d) = 3$ is one-to-one.

Solution

The function is one-to-one because f takes on different values of the four elements of its domain.
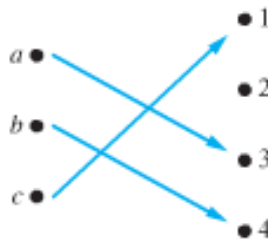
Example

Determine whether the function $f(x) = x^2$ from the set of integers to the set of integers is one-to-one.

Solution

The function is **not** one-to-one because $f(-1) = f(1) = 1$ but $1 \neq -1$

Example

Determine whether the function $f(x) = x + 1$ from the set of real numbers to itself is one-to-one.

Solution

The function is one-to-one because $x + 1 \neq y + 1$ when $x \neq y$

Definition

A function f whose domain and codomain are subsets of the set of real numbers is called **increasing** if $f(x) \leq f(y)$, and **strictly increasing** if $f(x) < f(y)$, whenever $x < y$ and x and y are in the domain of f. Similarly, f is called **decreasing** if $f(x) \geq f(y)$, and **strictly increasing** if $f(x) > f(y)$, whenever $x < y$ and x and y are in the domain of f. (The word **strictly** in this definition indicates a strict inequality.)

Definition

A function f from A to B is called ***onto***, or a ***surjection***, *iff* for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$. A function f is called ***surjective*** if it is onto.

Example

Let f be function from $\{a, b, c, d\}$ to $\{1, 2, 3\}$ defined by $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$.
Is f an onto function?

Solution

Because all three elements of the codomain are images of elements in the domain, we see that f is onto.
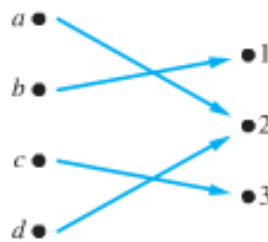
Example

Is the function $f(x) = x^2$ from the set of integers to the set of integers onto?

Solution

The function is ***not*** onto because there is no integer x with $x^2 = -1$.

Example

Is the function $f(x) = x + 1$ from the set of integers to the set of integers onto?

Solution

The function is onto because for every integer y there is an integer x such that $f(x) = y$.
$f(x) = y$ *iff* $x + 1 = y$, which holds if and only if $x = y - 1$

(a) One-to-one, not onto   (b) Onto, not one-to-one   (c) One-to-one, and onto   (d) Neither one-to-one nor onto   (e) Not a function
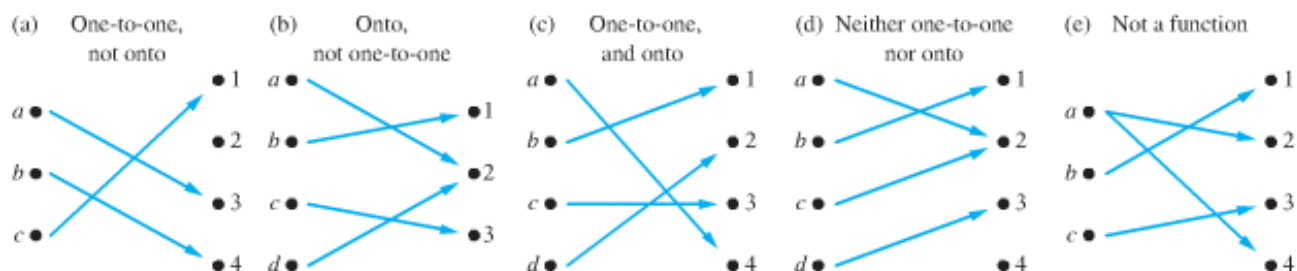
Definition

The function f is *one-to-one correspondence*, or a **bijection**, if it is both one-to-one and onto. We say also that such a function is **bijective**.

Example

Let f be function from $\{a, b, c, d\}$ to $\{1, 2, 3, 4\}$ defined by $f(a) = 4$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. Is f a bijection?

Solution

The function f is one-to-one and onto.
It is one-to-one because no two values in the domain are assigned the same function value.
It is onto because all four elements of the codomain are images of elements in the domain.
Hence, f is a bijection.

Inverse Functions and Compositions of Functions

Definition

Let f be a one-to-one correspondence from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$. The inverse function of f is denoted by f^{-1}. Hence, $f^{-1}(b) = a$ when $f(a) = b$
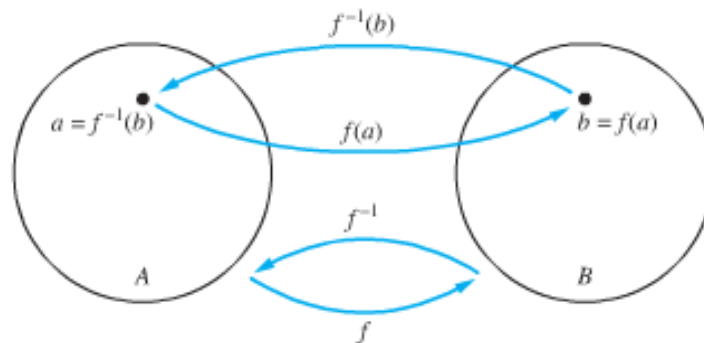
Example

Let f be function from $\{a, b, c\}$ to $\{1, 2, 3\}$ defined by $f(a) = 2$, $f(b) = 3$, and $f(c) = 1$. Is f invertible, and if it is, what is its inverse?

Solution

The function f is invertible since it is a one-to-one.

The inverse function: $f^{-1}(1) = c$, and $f^{-1}(2) = a$, $f^{-1}(3) = b$

Example

Let $f : \mathbb{Z} \to \mathbb{Z}$ be such that $f(x) = x+1$. Is f invertible, and if it is, what is its inverse?

Solution

The function f is invertible since it is a one-to-one.

$$y = x+1 \quad \Rightarrow \quad x = y-1$$

$$f^{-1}(y) = y-1$$

Example

Let $f : \mathbb{R} \to \mathbb{R}$ be such that $f(x) = x^2$ Is f invertible?

Solution

The function is **not** one-to-one. Hence, f is **not** invertible.

Definition

Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The composition of the function f and g, denoted for all $a \in A$ by $f \circ g$, is defined by

$$(f \circ g)(a) = f(g(a))$$
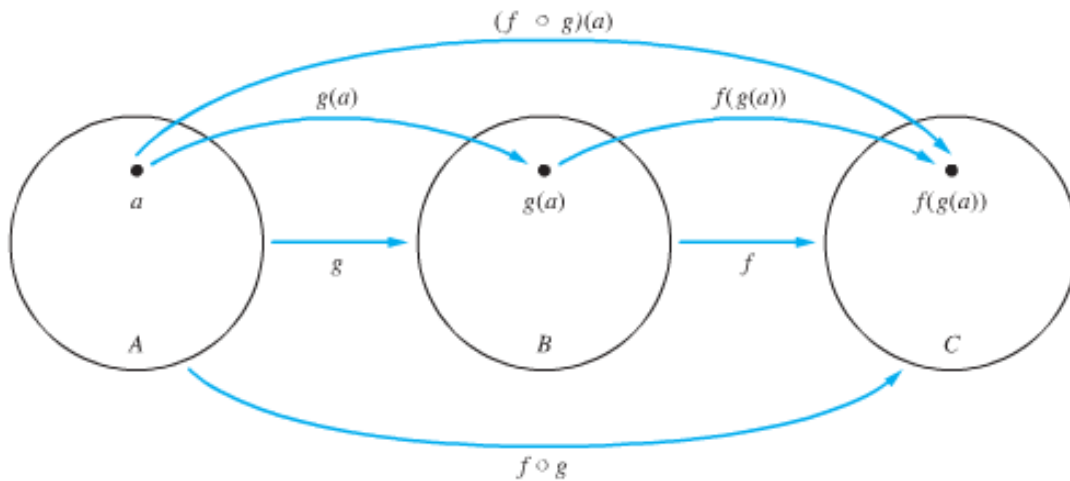
Example

Let g be the function from the set $\{a, b, c\}$ to itself such that $g(a) = b$, $g(b) = c$, and $g(c) = a$.

Let f be the function from the set $\{a, b, c\}$ to the set $\{1, 2, 3\}$ such that $f(a) = 3$, $f(b) = 2$, and $f(c) = 1$. What is the composition of f and g, and what is the composition of g and f?

Solution

$$(f \circ g)(a) = f(g(a)) = f(b) = 2$$

$$(f \circ g)(b) = f(g(b)) = f(c) = 1$$

$$(f \circ g)(c) = f(g(c)) = f(a) = 3$$

$$(g \circ f)(a) = g(f(a)) = g(3) \quad \not\exists.$$

Therefore; $g \circ f$ is not defined, because the range of f is not a subset of the domain of g.

Example

Let f and g be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of f and g, and what is the composition of g and f?

Solution

$$
\begin{aligned}
(f \circ g)(x) &= f(g(x)) \\
&= f(3x + 2) \\
&= 2(3x + 2) + 3 \\
&= \underline{6x + 7}
\end{aligned}
$$

$$(g \circ f)(x) = g(f(x)) = g(2x + 3) = 3(2x + 3) + 2 = \underline{6x + 11}.$$

Exercises   *Section* 1.9 – **Functions**

1. Why is f not a function from $\mathbb{R}$ to $\mathbb{R}$ if

   a) $f(x) = \dfrac{1}{x}$?

   b) $f(x) = \sqrt{x}$?

   c) $f(x) = \pm\sqrt{x^2 + 1}$?

2. Determine whether f is a function from $\mathbb{Z}$ to $\mathbb{R}$ if

   a) $f(x) = \pm x$?

   b) $f(x) = \sqrt{x^2 + 1}$?

   c) $f(x) = \dfrac{1}{x^2 - 4}$?

3. Find the domain and range of these functions. Note that in each case, to find the domain, determine the set of elements assigned values by the function.

   a) The function that assigns to each bit string the number of ones in the string minus the number of zeros in the string.

   b) The function that assigns to each bit string twice the number of zeros in that string.

   c) The function that assigns the number of bits over when a bit string is split into bytes (which are blocks of 8 bits).

4. Determine whether each of these functions from $\{a, b, c, d\}$ to itself is one-to-one and onto.

   a) $f(a) = b$, $f(b) = a$, $f(c) = c$, $f(d) = d$

   b) $f(a) = b$, $f(b) = b$, $f(c) = d$, $f(d) = c$

   c) $f(a) = d$, $f(b) = b$, $f(c) = c$, $f(d) = d$

5. Determine whether the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is onto if

   a) $f(m, n) = m + n$

   b) $f(m, n) = m^2 + n^2$

   c) $f(m, n) = m$

   d) $f(m, n) = |n|$

   e) $f(m, n) = m - n$

6. Determine whether each of these functions is a bijection from $\mathbb{R} \to \mathbb{R}$

   a) $f(x) = 2x + 1$

   b) $f(x) = x^2 + 1$

   c) $f(x) = x^3$

d) $f(x) = \dfrac{x^2+1}{x^2+2}$

e) $f(x) = x^5 + 1$

7. Suppose that g is a function from A to B and f is a function from B to C.

   a) Show that if both f and g are one-to-one functions, then $f \circ g$ is also one-to-one.

   b) Show that if both f and g are onto functions, then $f \circ g$ is also onto.

Lecture Two

Section 2.1 – Sequences and Summations

Sequences

Definition

A sequence is a function from a subset of the set of integers (usually either the set $\{0, 1, 2, \ldots\}$ or the set $\{1, 2, 3, \ldots\}$ to a set S. We use the notation a_n to denote the image of the integer n. We call a_n a term of the sequence.

The sequence $\{a_n\}$, where $a_n = \dfrac{1}{n}$

The list of the terms of this sequence: $1, \dfrac{1}{2}, \dfrac{1}{3}, \dfrac{1}{4}, \ldots$

Definition

A **geometric progression** is a sequence of the form $a, ar, ar^2, \ldots, ar^n, \ldots$ where the *initial* term a and the **common ratio** r are real numbers.

The common ratio for: $6, -12, 24, -48, \ldots, (-2)^{n-1}(6), \ldots$ is $= \dfrac{-12}{6} = -2$

Definition

An **arithmetic progression** is a sequence of the form $a, a+d, a+2d, \ldots, a+nd, \ldots$ where the *initial* term a and the **common difference** d are real numbers.

Recurrence Relations

Definition

A **recurrence relation** for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely, $a_0, a_1, a_2, \ldots, a_{n-1}, \ldots$, for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer. A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation. (A recurrence relation is said to *recursively define* a sequence.)

Example

Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1, 2, 3, \ldots$ and suppose that $a_0 = 2$. What are a_1, a_2, and a_3?

Solution

$$a_1 = a_0 + 3 = 2 + 3 = 5$$
$$a_2 = a_1 + 3 = 5 + 3 = 8$$
$$a_3 = a_2 + 3 = 8 + 3 = 11$$

Example

Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$ and suppose that $a_0 = 3$ and $a_1 = 5$. What are a_2, and a_3?

Solution

$$a_2 = a_1 + a_0 = 5 - 3 = 2$$
$$a_3 = a_2 + a_1 = 2 - 5 = -3$$

Definition

The Fibonacci sequence, $f_0, f_1, f_2, \ldots$, is defined by the initial conditions $f_0 = 0$, $f_1 = 1$, and the recurrence relation

$$f_n = f_{n-1} + f_{n-2} \quad for \quad n = 2, 3, 4, \ldots$$

Example

Find the Fibonacci number $f_2, f_3, f_4, f_5,$ and f_6

Solution

$$f_2 = f_1 + f_0 = 1 + 0 = 1$$
$$f_3 = f_2 + f_1 = 1 + 1 = 2$$
$$f_4 = f_3 + f_2 = 2 + 1 = 3$$
$$f_5 = f_4 + f_3 = 3 + 2 = 5$$
$$f_6 = f_5 + f_4 \, 5 + 3 = 8$$

Example

Determine whether the sequence $\{a_n\}$, where $a_n = 3n$ for every nonnegative integer n, is a solution of the recurrence relation $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$. Answer the same question whenere $a_n = 2^n$ and where $a_n = 5$

<u>**Solution**</u>

Suppose that $a_n = 3n$. Then, for $n \geq 2$,

$$2a_{n-1} - a_{n-2} = 2(3(n-1)) - 3(n-2)$$
$$= 6n - 2 - 3n + 6$$
$$= 3n = a_n \qquad \text{Is a solution of the recurrence relation}$$

Suppose that $a_n = 2^n$. Then, for $n \geq 2$,

$$2a_{n-1} - a_{n-2} = 2 \cdot 2^{n-1} - 2^{n-2} \qquad\qquad \text{or} \qquad a_0 = 1, \quad a_1 = 2, \quad a_2 = 4$$
$$= 2^n\left(2 \cdot 2^{-1} - 2^{-2}\right) \qquad\qquad\qquad 2a_1 - a_0 = 2 \cdot 2 - 1 = 3 \neq a_2$$
$$= 2^n\left(1 - \frac{1}{4}\right)$$
$$= 2^n\left(\frac{3}{4}\right)$$
$$= 3 \cdot 2^{n-2}$$
$$\neq 2^n = a_n \qquad \text{Is **not** a solution of the recurrence relation}$$

Suppose that $a_n = 5$. Then, for $n \geq 2$,

$$2a_{n-1} - a_{n-2} = 2 \cdot 5 - 5 = 5 = a_n$$
Is a solution of the recurrence relation

Example

Find the formalc for the sequences with the following first five terms:

a) $1, \dfrac{1}{2}, \dfrac{1}{4}, \dfrac{1}{8}, \dfrac{1}{16}$

b) 1, 3, 5, 7, 9

c) 1, −1, 1, −1, 1

<u>**Solution**</u>

a) The sequence with $a_n = \dfrac{1}{2^n}$, $n = 0, 1, 2, \ldots$, This proposed sequence is a geometric progression

with $a = 1$ and $r = \dfrac{1}{2}$.

b) Each term is obtained by adding 2 to the previous term, The sequence with $a_n = 2n+1$, $n = 0, 1, 2, \ldots$, This proposed sequence is an arithmetic progression with $a = 1$ and $d = 2$.

c) The terms alternate between 1 and -1, The sequence with $a_n = (-1)^n$, $n = 0, 1, 2, \ldots$, This proposed sequence is an geometric progression with $a = 1$ and $r = -1$.

Example

How can we produce the terms of a sequence if the first 10 terms are 1, 2, 2, 3, 3, 3, 4, 4, 4, 4?

Solution

In this sequence, the integer 1 appears once, the integer 2 appears twice, the integer 3 appears three times, the integer 4 appears four times. A reasonable rule for generating this sequence is that the integer n appears exactly n times.
The sequence generated this is possible match.

Example

How can we produce the terms of a sequence if the first 10 terms are 5, 11, 17, 23, 29, 35, 41, 47, 53, 59?

Solution

$d = 11 - 5 = 6|$

The sequence can be obtained by adding 6 to previous term. This produce to $a_n = 5 + 6(n-1)$.

This sequence is an arithmetic progression with $a = 5$ and $d = 6$.

Example

How can we produce the terms of a sequence if the first 10 terms are 1, 3, 4, 7, 11, 18, 29, 47, 76, 123?

Solution

$4 = 1 + 3$
$7 = 4 + 3$
$11 = 4 + 7$
And so on. We can see that the third term is the sum of the two previous term.
The sequence is determined by the recurrence relation $L_n = L_{n-1} + L_{n-2}$ with initial conditions

$L_1 = 1$ and $L_1 = 2$.

Some Useful Sequences	
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, …
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, …
n^4	1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, …
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, …
3^n	3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, …
$n!$	1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, …
f_n	1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, …

Summations

To find the sum of many terms of an infinite sequence, it is easy to express using ***summation notation***.

$$\sum_{k=1}^{m} a_k = a_1 + a_2 + a_3 + \ldots + a_m$$

$$\sum_{k=m}^{n} a_k \quad or \quad \sum_{m \le k \le n} a_k$$

The index of summation runs through all integers starting with its ***lower limit*** and ending with its ***upper limit***.

The large uppercase Greek letter ***sigma***, Σ, is used to denote summation.

Example

Use the summation notation to express the sun of the first 100 terms of the sequence $\{a_j\}$, where $a_j = \dfrac{1}{j}$

for $j = 1, 2, 3, \ldots$

Solution

$$\sum_{j=1}^{100} \frac{1}{j}$$

Example

What is the value of $\displaystyle\sum_{j=1}^{5} j^2$

Solution

$$\sum_{j=1}^{5} j^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2$$

$$= 1 + 4 + 9 + 16 + 25$$

$$= 55$$

Example

What is the value of $\displaystyle\sum_{k=4}^{8} (-1)^k$

Solution

$$\sum_{k=4}^{8} (-1)^k = (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8$$

$$= 1 + (-1) + 1 + (-1) + 1$$

$$= 1$$

Theorem

If a and r are real numbers and $r \neq 0$, then

$$\sum_{j=0}^{n} ar^j = \begin{cases} \dfrac{ar^{n+1} - a}{r - 1} & \text{if } r \neq 1 \\ (n+1)a & \text{if } r11 \end{cases}$$

Proof

Let $\displaystyle S_n = \sum_{j=0}^{n} ar^j$

$$rS_n = r \sum_{j=0}^{n} ar^j$$

$$= \sum_{j=0}^{n} ar^{j+1}$$

$$= \sum_{k=1}^{n+1} ar^k \qquad \textit{Shifting the index of summation with } k = j+1$$

$$= \sum_{k=0}^{n} ar^k + \left(ar^{n+1} - a \right)$$

$$= S_n + \left(ar^{n+1} - a \right)$$

$$rS_n = S_n + \left(ar^{n+1} - a \right)$$

$$(r-1)S_n = ar^{n+1} - a$$

$$S_n = \frac{ar^{n+1} - a}{r-1}$$

If $r = 1$, then the $S_n = \sum_{j=0}^{n} a(1)^j = \sum_{j=0}^{n} a = (n+1)a$

Double summations

Double summations arise in many contexts (as in the analysis of nested loops in computer programs). An example of a double summation is

$$\sum_{i=1}^{4} \sum_{j=1}^{3} ij$$

To evaluate the double sum, first expand the inner summation and then continue by computing the outer summation

$$\sum_{i=1}^{4} \sum_{j=1}^{3} ij = \sum_{i=1}^{4} \left(i + 2i + 3i \right)$$

$$= \sum_{i=1}^{4} 6i$$

$$= 6 + 12 + 18 + 24$$

$$= 60$$

Some Useful Summation Formulae	
Sum	Closed Form
$\displaystyle\sum_{k=0}^{n} ar^k \quad (r \neq 0)$	$\dfrac{ar^{n+1}-a}{r-1}, \quad r \neq 1$
$\displaystyle\sum_{k=1}^{n} k$	$\dfrac{n(n+1)}{2}$
$\displaystyle\sum_{k=1}^{n} k^2$	$\dfrac{n(n+1)(2n+1)}{6}$
$\displaystyle\sum_{k=1}^{n} k^3$	$\dfrac{n^2(n+1)^2}{4}$
$\displaystyle\sum_{k=0}^{\infty} x^k, \quad |x|<1$	$\dfrac{1}{1-x}$
$\displaystyle\sum_{k=1}^{\infty} kx^{k-1}, \quad |x|<1$	$\dfrac{1}{(1-x)^2}$

Example

What is the value of $\displaystyle\sum_{s\in[0,2,4]} s$

Solution

$$\sum_{s\in[0,2,4]} s = 0+2+4 \underline{\underline{= 6}}$$

Example

What is the value of $\displaystyle\sum_{k=50}^{100} k^2$

Solution

$$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2 \qquad\qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$= \frac{100\cdot101\cdot201}{6} - \frac{49\cdot50\cdot99}{6} = 338,350 - 40,425 \underline{\underline{= 297,925}}$$

88

Exercises   *Section* **2.1 – Sequences and Summations**

1.   Find these terms of the sequence $\{a_n\}$, where $a_n = 2 \cdot (-3)^n + 5^n$

   a) a_0 b) a_1 c) a_4 d) a_5

2.   What is the term a_8 of the sequence $\{a_n\}$, if a_n equals

   a) 2^{n-1} b) 7   c) $1 + (-1)^n$ d) $-(2)^n$

3.   What are the terms a_0, a_1, a_2, *and* a_3 of the sequence $\{a_n\}$, if a_n equals

   a) $2^n + 1$ b) $(n+1)^{n+1}$ c) $\frac{n}{2}$ d) $\frac{n}{2} + \frac{n}{2}$

   e) $(-2)^n$ f) 3   g) $7 + 4^n$ h) $2^n + (-2)^n$

4.   Find at least three different sequences beginning with the terms 1, 2, 4 whose terms are generated by a simple formula or rule.

5.   Find at least three different sequences beginning with the terms 3, 5, 7 whose terms are generated by a simple formula or rule.

6.   Find the first five terms of the sequence defined by each of these recurrence relations and initial conditions.

   a) $a_n = 6a_{n-1}$, $a_0 = 2$

   b) $a_n = a_{n-1}^2$, $a_1 = 2$

   c) $a_n = a_{n-1} + 3a_{n-2}$, $a_0 = 1$, $a_1 = 2$

   d) $a_n = na_{n-1} + n^2 a_{n-2}$, $a_0 = 1$, $a_1 = 1$

   e) $a_n = a_{n-1} + a_{n-3}$, $a_0 = 1$, $a_1 = 2$, $a_2 = 0$

7.   Find the first six terms of the sequence defined by each of these recurrence relations and initial conditions.

   a) $a_n = -2a_{n-1}$, $a_0 = -1$

   b) $a_n = a_{n-1} - a_{n-2}$, $a_0 = 2$, $a_1 = -1$

   c) $a_n = 3a_{n-1}^2$, $a_0 = 1$

   d) $a_n = na_{n-1} + n^2 a_{n-2}$, $a_0 = -1$, $a_1 = 0$

   e) $a_n = a_{n-1} - a_{n-2} + a_{n-3}$, $a_0 = 1$, $a_1 = 2$, $a_2 = 2$

8. Let $a_n = 2^n + 5 \cdot 3^n$ for $n = 0, 1, 2, \ldots$

    a) Find $a_0, a_1, a_2, a_3,$ and a_4

    b) Show that $a_2 = 5a_1 - 6a_0$, $a_3 = 5a_2 - 6a_1$, and $a_4 = 5a_3 - 6a_2$

    c) Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers n with $n \geq 2$

9. Is the sequence $\{a_n\}$ a solution of the recurrence relation $a_n = 8a_{n-1} - 16a_{n-2}$ if

    a) $a_n = 0$?

    b) $a_n = 1$?

    c) $a_n = 2^n$?

    d) $a_n = 4^n$?

    e) $a_n = n4^n$?

    f) $a_n = 2 \cdot 4^n + 3n4^n$?

    g) $a_n = (-4)^n$?

    h) $a_n = n^2 4^n$?

10. Is the sequence $\{a_n\}$ a solution of the recurrence relation $a_n = a_{n-1} + 2a_{n-2} + 2n - 9$ if

    i) $a_n = -n + 2$

    j) $a_n = 5(-1)^n - n + 2$

    k) $a_n = 3(-1)^n + 2^n - n + 2$

    l) $a_n = 7 \cdot 2^n - n + 2$

11. A person deposits \$1,000.00 in an account that yields 9% interest compounded annually.

    a) Set up a recurrence relation for the amount in the account at the end of n years.

    b) Find an explicit formula for the amount in the account at the end of n years.

    c) How much money will the account contain after 100 years?

12. Suppose that the number of bacteria in a colony triples every hour.

    a) Set up a recurrence relation for the number of bacteria after n hours have elapsed.

    b) If 100 bacteria are used to begin new colony, how many bacteria will be in the colony in 10 hours?

13. A factory makes custom sports cars at an increasing rate. In the first month only one car is made, in the second month two cars are made, and so on, with n cars made in the nth month.

a) Set up a recurrence relation for the number of cars produced in the first n months by this factory.

b) How many cars are produced in the first year?

c) Find an explicit formula for the number of cars produced in the first n months by this factory

14. For each of these lists of integers, provide a simple formula or rule that generates the terms of an integer sequence that begins with the given list. Assuming that your formula or rule is correct, determine the next three terms of the sequence.

a) 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 1, …

b) 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 8, 8, …

c) 1, 0, 2, 0, 4, 0, 8, 0, 16, 0, …

d) 3, 6, 12, 24, 48, 96, 192, …

e) 15, 8, 1, −6, −13, −20, −27, …

f) 3, 5, 8, 12, 17, 23, 30, 38, 47, …

g) 2, 16, 54, 128, 250, 432, 686, …

h) 2, 3, 7, 25, 121, 721, 5041, 40321, …

i) 3, 6, 11, 18, 27, 38, 51, 66, 83, 102, …

j) 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, …

k) 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, …

Section 2.2 – **Algorithms**

Introduction

Definition

An *algorithm* is a finite sequence of precise instructions for performing a computation or for solving a problem.

- ➢ A program is one type of algorithm
  - O All programs are algorithms
  - O Not all algorithms are programs!
- ➢ Directions to somebody's house is an algorithm
- ➢ A recipe for cooking a cake is an algorithm
- ➢ The steps to compute the cosine of 90° is an algorithm

Properties of Algorithms

Input: An algorithm has input values from a specified set.

Output: From each set of input values an algorithm produces output values from a specified set. The output values are the solution to the problem.

Definiteness: The steps of an algorithm must be defined precisely.

Correctness: An algorithm should produce the correct output values for each set of input values.

Finiteness: An algorithm should produce the desired output after a finite (but perhaps large) number of steps for any input in the set.

Effectiveness: It must be possible to perform each step of an algorithm exactly and in a finite amount of time.

Generality: The procedure should be applicable for all problems of the desired form, not just for a particular set of input values.

Algorithm 1 – **Finding the Maximum Element in a Finite Sequence**

Given a list, how do we find the maximum element in the list?

To express the algorithm, we'll use pseudocode

- ✓ Pseudocode is kinda like a programming language, but not really

Example

Show that Algorithm 1 for finding the maximum element in a finite sequence of integers has all the properties listed.

Solution

The input to Algorithm 1 is a sequence of integers. The output is the largest integer in the sequence. Each step of the algorithm is precisely defined, because only assignments, a finite loop, and conditional statements occur.

The values of the variable *max* equals the maximum terms when the algorithm terminates.

The initial value of max is the first term; as successive terms of the sequence are examined. This argument shows that when all the terms have been examined, max equal the value of the largest term and it will take *n* steps.

Algorithm 1 is general, because it can be used to find the maximum of any finite sequence of integers.

Procedure max $\{a_1, a_2, \ldots, a_n\}$

max:= a_1

for $i := 2$ to *n*

    if max $< a_i$ *then* max $:= a_i$

return *max*{*max* is the largest element}

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
4	1	7	0	5	2	9	3	6	8

i ▪0
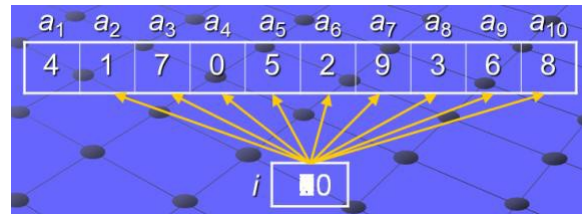
Searching Algorithms

Given a list, find a specific element in the list. There are two types:

1. Linear search
2. Binary search

Algorithm 2 – Linear Search

Given a list which does not have to be sorted, find element in the list

procedure linear_search (*x*: integer; $a_1, a_2, \ldots, a_n$: integers)

$i := 1$

while ($i \leq n$ and $\left(i \leq n \ and \ x \neq a_i \right)$

    $i := i + 1$

if $i \leq n$ *then* location $:= i$

else location $:= 0$

{*location* is the subscript of the term that equals *x*, or it is 0 if *x* is not found}

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
4	1	7	0	5	2	9	3	6	8

i ▪0
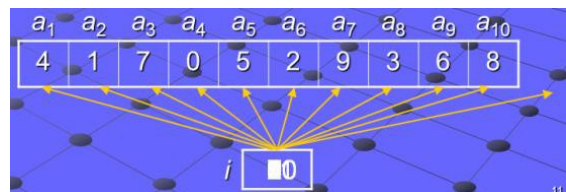
Algorithm 3 – **Binary Search**

Given a list which *must* be sorted, find element in the list

    procedure linear_search (x: integer; a_1, a_2, …, a_n : increasing integers)

    $i := 1$ { i is left endpoint of search interval }

    $j := n$ { j is right endpoint of search interval }

    while $i < j$

    begin

        $m := \lfloor (i+j)/2 \rfloor$ { m is the point in the middle }

        if $x > a_m$ *then* $i := m+1$

            else $j := m$

    end

    if $x = a_i$ *then* location $:= i$

    else location $:= 0$

    {*location* is the subscript of the term that equals x, or it is 0 if x is not found}

        $x = \boxed{14}$ *location* $\boxed{7}$

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
2	4	6	8	10	12	14	16	18	20
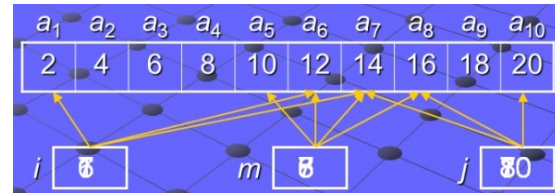
Sorting

Ordering the elements of a list is a problem that occurs in many contexts. Suppose that we have a list of elements of a set. Suppose that we have a way to order elements of the set. *Sorting* is putting these elements into a list in which the elements are in increasing order.

There are two types:

- ✓ **Bubble sort**
- ✓ **Insertion sort**

Bubble Sort

The *bubble sort* is one of the simplest sorting algorithms, but not one of the most efficient. It takes successive elements and "***bubbles***" them up the list.

Example

Use the bubble sort to put 3, 2, 4, 1, 5 into increasing order.

Solution

First Pass	3	2	2	2
	2	3	3	3
	4	4	4	1
	1	1	1	4
	5	5	5	5

Second Pass	2	2	2
	3	3	1
	4	1	3
	1	4	4
	5	5	5

Third Pass	2	1
	1	2
	3	3
	4	4
	5	5

Fourth Pass	1
	2
	3
	4
	5

Algorithm 4 – **Bubble**

> **procedure** bubblesort (a_1, a_2, ..., a_n : real numbers with $n \geq 2$)
>
> **for** $i := 1$ **to** $n - 1$
>
> **for** $j := 1$ **to** $n - i$
>
> **if** $a_j > a_j + 1$
>
> **then** interchange a_j and $a_j + 1$

95

Bubble sort running time

Outer for loop does $n - 1$ iterations

Inner for loop does:

        $n - 1$ iterations the first time

        $n - 2$ iterations the second time

Total: $(n-1)+(n-2)+\ldots+2+1 = \dfrac{n^2-n}{2}$

The bubble sort will take about n^2 time.

Insertion sort

The *insertion sort* is another simple sorting algorithm, but inefficient. It starts with a list with one element, and inserts new elements into their proper place in the sorted part of the list

Algorithm 5 – **Insertion sort**

> **procedure** insertion_sort $\left(a_1, a_2, \ldots, a_n\right)$
>
>   **for** $j := 2$ **to** n *take successive elements in the list*
>
>   **begin**
>
> $i := 1$ *find where that element should be*
>
>   **while** $a_j > a_i$ *in the sorted portion of the list*
>
> $i := i + 1$
>
> $m := a_i$ *move all elements in the sorted portion of the list*
>
>   **for** $k := 0$ **to** $j\text{-}i\text{-}1$ *that are greater than the current element up by one*
>
> $a_{j-k} := a_{j-k-1}$
>
> $a_i := m$ *put the current element into it's proper place*
>
>   **end** $\left\{a_1, a_2, \ldots, a_n \text{ are sorted}\right\}$ *in the sorted portion of the list*

The *insertion* sort will take about n^2 time.

Comparison of Running Times

Searches

- *Linear*: n steps
- *Binary*: $\log_2 n$ steps

- *Binary* search is about as fast as you can get

Sorts

- *Bubble:* n^2 steps
- *Insertion:* n^2 steps
- There are other, more efficient, sorting techniques
  - In principle, the fastest are heap sort, quick sort, and merge sort
  - These each take $n \cdot \log_2 n$ steps
  - In practice, quick sort is the fastest, followed by merge sort

Algorithm 6 – **Greedy Change-Making Algorithm**

$\boldsymbol{procedure}$ change (c_1, c_2, …, c_r : values of denominations of coins, where $c_1 > c_2 > … > c_r$; n: a

positive integer)

$\boldsymbol{for}$ $i := 1$ $\boldsymbol{to}$ r

    $d_i := 0$ *d_i counts the coins of denomination c_i used*

    $\boldsymbol{While}$ $n \geq c_i$

        $d_i := d_i + 1$ *Add a coin of denomination c_i*

        $n := n - c_i$

{ d_i is the number of coins of denomination c_i in the change for $i = 1, 2, …, r$}

Definition

If n is a positive integer, then n cents in change using quarters, dimes, nickels, and pennies using the fewest coins possible has at most two dimes, at most one nickel, at most four pennies, and cannot have two dimes and a nickel. The amount of change in dimes, nickels, and pennies cannot exceed 24 cents

Theorem

The greedy algorithm (–6) produces change using the fewest coins possible.

Exercises   Section 2.2 – Algorithms

1.   List all the steps used by the Algorithm 1 to find the maximum of the list

1, 8, 12, 9, 11, 2, 14, 5, 10, 4.

2.   Devise an algorithm that finds the sum of all the integers in a list.

3.   Describe an algorithm that takes as an input a list of n integers and produces as output the largest difference obtained by subtracting an integer in the list from the one following it.

4.   Describe an algorithm that takes as an input a list of n integers in non-decreasing order and produces the list of all values that occur more than once.

5.   Describe an algorithm that takes as an input a list of n integers and finds the location of the last even integer in the list or returns 0 if there are no even integers in the list.

6.   Describe an algorithm that interchanges the values of the variables x and y, using only assignments. What is the minimum number of assignment statements needed to do this?

7.   List all the steps used to search for 9 in the sequence 1, 3, 4, 5, 6, 7, 9, 11 using

    a) a linear search   *b*) a binary earch

8.   Describe an algorithm that inserts an integer x in the appropriate position into the list $a_1, a_2, \ldots, a_n$ of integers that are in increasing order.

Section 2.3 – Divisibility and Modular Arithmetics

Division

Definition

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integers. When a divides b we say that a is a factor or divisor of b, and that b is multiple of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Example

Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution

We see that $3 \nmid 7$, because 7/3 is not integer.

$3 \mid 12$ because 12/3 = 4.

Example

Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Solution

The positive integers divisible by d are all the integers of the form dk, where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

Theroem

Let a, b, and c integers, where $a \neq 0$. Then

   i)   If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

   ii)   If $a \mid b$, then $a \mid bc$ for all integers c;

   iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof (*i*)

Suppose If $a \mid b$ and $a \mid c$. Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t)$$

Therefore, a divides $b + c$.

Corollary

If a, b, and c integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

The Division Algorithm

Theroem

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Definition

In the equality given in the division algorithm, **d** is called the **divisor**, **a** called the **dividend**, **q** is called the **quotient**, and **r** is called the **remainder**. This notation is used to express the quotient and remainder:

$$q = a \ \textbf{div} \ d, \qquad r = a \ \textbf{mod} \ d$$

Example

What are the quotient and remainder when 101 is divided by 11?

Solution

$$101 = 11 \cdot 9 + 2$$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \ \textbf{div} \ 11$, and the remainder is $2 = 101 \ \textbf{mod} \ 11$.

Example

What are the quotient and remainder when -11 is divided by 3?

Solution

$$-11 = 3(-4) + 1$$

Hence, the quotient when -11 is divided by 3 is $-4 = -11$ *div* 3,

and the remainder is $1 = -11$ *mod* 3.

Modular Arithmetic

Definition

If a and b are integers and m is positive integer, then a is **congruent** to b **modulo** m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is *congruent* to b *modulo* m. We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$

Theorem

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if

a **mod** m $=$ b **mod** m

Example

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution

Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod{6}$.

$24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof

If $a \equiv b \pmod{m}$ that implies by the definition of congruence to $m | (a - b)$. Which is that there is an integer k such that $a - b = km \implies a = b + km$.

Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod{m}$

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad and \qquad ac \equiv bd \pmod{m}$$

Proof

Using direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the theorem that are integers s and t with $b = a + sm \quad and \quad d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t) \qquad \Rightarrow a + c \equiv b + d \pmod{m}$$

And

$$bd = (a + sm)(c + tm) = ac + m(at + sc + stm) \qquad \Rightarrow ac \equiv bd \pmod{m}$$

Corollary

Let a and b be integers, and let m be a positive integer. Then

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Arithmetic Modulo m

We define addition by: $a +_m b = (a + b) \bmod m$ and multiplication by $a \cdot_m b = (a \cdot b) \bmod m$

Exercises   *Section* **2.3 – Divisibility and Modular Arithmetics**

1.   Does 17 divide each of these numbers?

   a) 68   ***b***) 84   ***c***) 35   ***d***) 1001

2.   Prove that if *a* is an integer other than 0, then

   a) 1 *divides a*   ***b***) *a divides* 0

3.   Show that if $a \mid b$ and $b \mid a$, where *a* and *b* are integers, then $a = b$ or $a = -b$.

4.   Show that if *a*, *b*, and *c* are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$

5.   What are the quotient and remainder when

   a)   19 is divided by 7?
   b)   −111 is divided by 11?
   c)   789 is divided by 23?
   d)   1001 is divided by 13?
   e)   0 is divided by 19?
   f)   3 is divided by 5?
   g)   −1 is divided by 3?
   h)   4 is divided by 1?

6.   What time does a 12-hour clock read

   a)   80 hours after it reads 11:00?
   b)   40 hours before it reads 12:00?
   c)   100 hours after it reads 6:00?

7.   What time does a 24-hour clock read

   a)   100 hours after it reads 2:00?
   b)   45 hours before it reads 12:00?
   c)   168 hours after it reads 19:00?

8.   Suppose *a* and *b* are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer *c* with $0 \leq c \leq 12$ such that

   a) $c \equiv 9a \pmod{13}$
   b) $c \equiv 11b \pmod{13}$
   c) $c \equiv a + b \pmod{13}$
   d) $c \equiv 2a + 3b \pmod{13}$
   e) $c \equiv a^2 + b^2 \pmod{13}$
   f) $c \equiv a^3 - b^3 \pmod{13}$

9. Suppose a and b are integers, $a \equiv 11 \ (\textbf{\textit{mod}}\ 19)$, and $b \equiv 3\ (\textbf{\textit{mod}}\ 19)$. Find the integer c with $0 \le c \le 10$ such that

    a) $c \equiv a - b\ (\textbf{\textit{mod}}\ 19)$

    b) $c \equiv 7a + 3b\ (\textbf{\textit{mod}}\ 19)$

    c) $c \equiv 2a^2 + 3b^2\ (\textbf{\textit{mod}}\ 19)$

    d) $c \equiv a^3 + 4b^3\ (\textbf{\textit{mod}}\ 19)$

10. Let m be a positive integer. Show that $a \equiv b (\text{mod}\ m)$ if $a \bmod m = b \bmod m$

11. Show that if n and k are positive integers, then $\lceil n/k \rceil = \left\lfloor \dfrac{n-1}{k} \right\rfloor + 1$

12. Evaluate these quantities
    a) $-17 \ \textbf{\textit{mod}}\ 2$
    b) $144\ \textbf{\textit{mod}}\ 7$
    c) $-101\ \textbf{\textit{mod}}\ 13$
    d) $199\ \textbf{\textit{mod}}\ 19$
    e) $13\ \textbf{\textit{mod}}\ 3$
    f) $-97\ \textbf{\textit{mod}}\ 11$

13. Find a **div** m and a **mod** m when
    a) $a = 228,\ m = 119$
    b) $a = 9009,\ m = 223$
    c) $a = -10101,\ m = 333$
    d) $a = -765432,\ m = 38271$

14. Find the integer a such that

    a) $a \equiv -15 (\textbf{\textit{mod}}\ 27)\ and\ -26 \le a \le 0$

    b) $a \equiv 24 (\textbf{\textit{mod}}\ 31)\ and\ -15 \le a \le 15$

    c) $a \equiv 99 (\textbf{\textit{mod}}\ 41)\ and\ 100 \le a \le 140$

    d) $a \equiv 43 (\textbf{\textit{mod}}\ 23)\ and\ -22 \le a \le 0$

    e) $a \equiv 17 (\textbf{\textit{mod}}\ 29)\ and\ -14 \le a \le 14$

15. Decide whether each of these integers is congruent to 5 modulo 17.
    $a)\ 37$ $b)\ 66$ $c) -17$ $d) - 67$

16. Find each of these values.
    a) $(-133 \ \textbf{mod}\ 23 + 261\ \textbf{mod}\ 23)\ \textbf{mod}\ 23$

b) $(457 \bmod 23 \cdot 182 \bmod 23) \bmod 23$

c) $(177 \bmod 31 + 270 \bmod 31) \bmod 31$

d) $\left(19^2 \bmod 41\right) \bmod 9$

e) $\left(32^3 \bmod 13\right)^2 \bmod 11$

f) $\left(99^2 \bmod 32\right)^3 \bmod 15$

g) $\left(3^4 \bmod 17\right)^2 \bmod 11$

h) $\left(19^3 \bmod 23\right)^2 \bmod 31$

i) $\left(89^3 \bmod 79\right)^4 \bmod 26$

Section 2.4 – Integer Representations and Algorithms

Representations of integers

Theorem

Let b be an integer greater that 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b_k + a_{k-1} b_{k-1} + \cdots + a_1 b + a_0$$

Where k is a nonnegative integer a_0, a_1, ..., a_k are nonnegative integers less than b, and $a_k \neq 0$

Example

What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?

Solution

$$(1\ 0101\ 1111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$
$$= 351$$

Octal and Hexadecimal Expansions

Base 8 expansions are called *octal* expansions.
Base 16 expansions are called *hexadecimal* expansions.

Example

What is the decimal expansion of the number with octal expansion $(7016)_8$?

Solution

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0$$
$$= 3598$$

Example

What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Solution

$$(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0$$
$$= 175627$$

Base Conversion

The algorithm for constructing the base b expansion of an integer n, divide n by b to obtain a quotient and remainder, that is,

$$n = bq_0 + a_0, \qquad 0 \le a_0 \le b$$
$$q_0 = bq_1 + a_1, \qquad 0 \le a_1 \le b$$

Example

Find the octal expansion of $(12345)_{10}$

Solution

$$12345 = 8 \cdot 1543 + 1$$
$$1543 = 8 \cdot 192 + 7$$
$$192 = 8 \cdot 24 + 0$$
$$24 = 8 \cdot 3 + 0$$
$$3 = 8 \cdot 0 + 3$$
$$(12345)_{10} = (30071)_8$$

Example

Find the hexadecimal expansion of $(177130)_{10}$

Solution

$$177130 = 16 \cdot 11070 + 10 \qquad (10 = A)$$
$$11070 = 16 \cdot 691 + 14 \qquad (14 = E)$$
$$691 = 16 \cdot 43 + 3$$
$$43 = 16 \cdot 2 + 11 \qquad (11 = B)$$
$$2 = 16 \cdot 0 + 2$$
$$(177130)_{10} = (2B3EA)_{16}$$

Example

Find the bianry expansion of $(241)_{10}$

Solution

$$241 = 2 \cdot 120 + 1$$
$$120 = 2 \cdot 60 + 0$$
$$60 = 2 \cdot 30 + 0$$
$$30 = 2 \cdot 15 + 0$$

$$15 = 2 \cdot 7 + 1$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 2 \cdot 0 + 1$$

$$(241)_{10} = (11110001)_2$$

Representation of the Integers 0 *through* 15.																
Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example

Find the octal and hexadecimal expansions of $(11\,1110\,1011\,1100)_2$

Solution

Octal: $(11\,1110\,1011\,1100)_2 = (011\,111\,010\,111\,100)_2$

$$= (37274)_8$$

Hexadecimal: $(11\,1110\,1011\,1100)_2 = (0011\,1110\,1011\,1100)_2$

$$= (3EBC)_{16}$$

Example

Find the binary expansions of $(765)_8$ and $(A8D)_{16}$

Solution

$$(765)_8 = (111\,110\,101)_2$$
$$(A8D)_{16} = (1010\,1000\,1101)_2$$

Algorithms for Integer Operations

Addition Algorithm

To add a and b, first add their rightmost bits. This gives

$$a_0 + b_0 = c_0 \cdot 2 + s_0$$

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$$

Example

Add $a = (1110)_2$ *and* $b = (1011)_2$

Solution

$$a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1 \qquad \Rightarrow \quad c_0 = 0, \ s_0 = 1$$

$$a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0 \qquad \Rightarrow \quad c_1 = 1, \ s_1 = 0$$

$$a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0 \qquad \Rightarrow \quad c_2 = 1, \ s_2 = 0$$

$$a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1 \qquad \Rightarrow \quad c_3 = 1, \ s_3 = 1$$

Therefore, $s = a + b = (11001)_2$

		1	1	1	
(carry) c					
		1	1	1	0
	+	1	0	1	1
s		1	1	0	0	1

Example

How many additions of bits are required to use Algorithm 2 to add two integers with n bits (or less) in their binary representations?

Solution

Two integers are added by successively adding pairs of bits. Adding each pair of bits and the carry requires two additions of bits. Thus, the total number of additions of bits used is less than twice the number of bits in the expansion. Hence, the number of additions of bits used by Algorithm 2 to add two n-bit integers is $O(n)$.

Multiplication Algorithm

$$ab = a\left(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1}\right)$$
$$= a\left(b_0 2^0\right) + a\left(b_1 2^1\right) + \cdots + a\left(b_{n-1} 2^{n-1}\right)$$

Algorithm: Multiplication of Integers

for $j := 0$ ***to*** $n - 1$

        if $b_j = 1$ **then** $c_j := a$ shifted j places

        else $c_j := 0$

$p := 0$

for $j := 0$ **to** $n - 1$

        $p := p + c_j$

Return p {p is the value of ab}

Example

Find the product of $a = (110)_2$ and $b = (101)_2$

Solution

$$
\begin{array}{r}
110 \\
\times\,101 \\
\hline
110 \\
000 \\
110 \\
\hline
11110
\end{array}
$$

Modular Exponential

It is important to find b^n **mod** m efficiently, where b, n and m are large integers.

$$b^n = b^{a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0} = b^{a_{k-1} \cdot 2^{k-1}} \cdots \cdot b^{a_1 \cdot 2} \cdot b^{a_0}$$

Example

Compute 3^{11}

Solution

$$11 = (1011)_2 \quad \rightarrow \quad 3^{11} = 3^8 3^2 3^1$$

$$3^2 = 9, \quad 3^4 = 81, \quad 3^8 = (81)^2 = 6561$$

$$3^{11} = 3^8 3^2 3^1$$
$$= 6561 \cdot 9 \cdot 3$$
$$= 177,147$$

Example

Use Algorithm 5 to find 3^{644} **mod** 645

Solution

$i = 0$	$a_0 = 0$	$x = 1$	$Power = 3^2 \textbf{ mod } 645 = 9 \textbf{ mod } 645 = 9$
$i = 1$	$a_1 = 0$	$x = 1$	$Power = 9^2 \textbf{ mod } 645 = 81 \textbf{ mod } 645 = 81$
$i = 2$	$a_2 = 1$	$x = 1 \cdot 81 \textbf{ mod } 645 = 81$	$Power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$
$i = 3$	$a_3 = 0$	$x = 81$	$Power = 111^2 \textbf{ mod } 645 = 12,321 \textbf{ mod } 645 = 66$
$i = 4$	$a_4 = 0$	$x = 81$	$Power = 66^2 \textbf{ mod } 645 = 4356 \textbf{ mod } 645 = 486$
$i = 5$	$a_5 = 0$	$x = 81$	$Power = 486^2 \textbf{ mod } 645 = 236,196 \textbf{ mod } 645 = 126$
$i = 6$	$a_6 = 0$	$x = 81$	$Power = 126^2 \textbf{ mod } 645 = 15,876 \textbf{ mod } 645 = 396$
$i = 7$	$a_7 = 1$	$x = (81 \cdot 396) \textbf{ mod } 645 = 471$	$Power = 396^2 \textbf{ mod } 645 = 156,816 \textbf{ mod } 645 = 81$
$i = 8$	$a_8 = 0$	$x = 471$	$Power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$
$i = 9$	$a_9 = 1$	$x = (471 \cdot 111) \textbf{ mod } 645 = 36$	

This shows that following steps of Algorithm 5 produces the result 3^{644} **mod** $645 = 36$

Exercises   *Section* 2.4 – Integer Representations and Algorithms

1. Convert the decimal expansion of each of these integers to a binary expansion
   - a) 321
   - b) 1023
   - c) 100632
   - d) 231
   - e) 4532

2. Convert binary the expansion of each of these integers to a decimal expansion
   - a) $(1\,1011)_2$
   - b) $(10\,1011\,0101)_2$
   - c) $(11\,1011\,1110)_2$
   - d)
   - e) $(1111\,1100\,0001\,1111)_2$
   - f) $(1\,1111)_2$
   - g) $(10\,0000\,0001)_2$
   - h)
   - i) $(10\,0101\,0101)_2$
   - i) $(110\,1001\,0001\,0000)_2$
   - k)

3. Convert the binary expansion of each of these integers to an octal expansion
   - a) $(1111\,0111)_2$
   - b) $(1010\,1010\,1010)_2$
   - c) $(111\,0111\,0111\,0111)_2$
   - d) $(101\,0101\,0101\,0101)_2$

4. Convert the octal expansion of each of these integers to a binary expansion
   - a) $(572)_8$
   - b) $(1604)_8$
   - c) $(423)_8$
   - d) $(2417)_8$

5. Convert the hexadecimal expansion of each of these integers to a binary expansion
   - a) $(80E)_{16}$
   - b) $(135AB)_{16}$
   - c) $(ABBA)_{16}$
   - d) $(DEFACED)_{16}$
   - e) $(BADFACED)_{16}$
   - f) $(ABCDEF)_{16}$

6. Show that the binary expansion of a positive integer can be obtained from its hexadecimal expansion by translating each hexadecimal digit into a block of four binary digits.

7. Show that the binary expansion of a positive integer can be obtained from its octal expansion by translating each octal digit into a block of three binary digits.

8. Explain how to convert from binary to base 64 expansions and from base 64 expansions to binary expansions and from octal to base 64 expansions and from base 64 expansions to octal expansions

9. Find the sum and product of each of these pairs of numbers. Express your answers as a base 3 expansions
   - a) $(112)_3$, $(210)_3$
   - b) $(2112)_3$, $(12021)_3$
   - c) $(20001)_3$, $(1111)_3$
   - d) $(120021)_3$, $(2002)_3$

10. Find the sum and product of each of these pairs of numbers. Express your answers as an octal expansion.

a) $(763)_8$, $(147)_8$ b) $(6001)_8$, $(272)_8$

c) $(1111)_8$, $(777)_8$ d) $(54321)_8$, $(3456)_8$

11. Find the sum and product of each of these pairs of numbers. Express your answers as an hexadecimal expansion.

a) $(1AE)_{16}$, $(BBC)_{16}$ b) $(20CBA)_{16}$, $(A01)_{16}$

c) $(ABCDE)_{16}$, $(1111)_{16}$ d) $(E0000E)_{16}$, $(BAAA)_{16}$

Section 2.5 – **Primes and Greatest Common Divisors**

Primes

Definition

An integer p greater than 1 is called **prime** of the only positive factors of p are 1 or p.
A positive integer that is greater than 1 and is not prime is called composite.

Example

The integer 7 is prime because its only positive factors are 1 and 7.
The integer 9 is composite because its is divisible by 3.

Theorem – **The Fundamental Theorem of Arithmetic**

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Example

Find the prime factorization of 100, 641, 999, and 1024.

Solution

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$$
$$641 = 641$$
$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$
$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$$

Trial Division

Theroem

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

Proof

If n is composite, then it has a factor a (by definition of a composite integer) with $1 < a < n$. Hence, by the definition of a factor, we have $n = ab, \quad b\,(\textit{positive integer}) > 1$.

If $a > \sqrt{n} \quad and \quad b > \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction. Consequently,

$a \leq \sqrt{n} \text{ and } b \leq \sqrt{n}$. Because both a and b are divisors of n, we see that n has a positive divisor not

exceeding $\sqrt{n}$. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime

divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

Example

Show that 101 is prime

Solution

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer). It follows that 101 is prime.

Example

Find the prime factorization of 7007

Solution

None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $\frac{7007}{7} = 1001$, and

$\frac{1001}{7} = 143$, $\frac{143}{11} = 13$. Because 13 is prime, the procedure is completed.

It follows that the prime factorization is $7007 = 7^2 \cdot 11 \cdot 13$

The Sieve of *Eratosthenes*

The **Sieve of Eratosthenes** can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Next, delete all the integers, other than 5, divisible by 5.
d. Next, delete all the integers, other than 7, divisible by 7.
e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are: {2,3,7,11,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

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

To see this, note that if $n = ab$, then $a \leq \sqrt{n}$ *or* $b \leq \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i.

The Sieve of Eratosthenes

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

The infinitude of Primes

It has long been known that there are infinitely many primes. This means that whenever $p_1, p_2, \ldots, p_n$ are the n smallest primes, we know there is a larger.

Theorem

There are infinitely may primes.

Proof: Assume finitely many primes: $p_1, p_2, \ldots, p_n$

Let $q = p_1 p_2 \cdots p_n + 1$. Either q is prime or by the fundamental theorem of arithmetic it is a product of primes. But none of the primes p_i divides q since if $p_i \mid q$, then p_i divide $q - p_1 p_2 \cdots p_n = 1$ .Hence, there is a prime not on the list $p_1, p_2, \ldots, p_n$ It is either q, or if q is composite, it is a prime

factor of q. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ are all the primes. Consequently, there are infinitely many primes.

Mersenne **Primes**

Definition

Prime numbers of the form $2^p - 1$, where p is prime, are called ***Mersenne primes***.

Example

$2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, $2^7 - 1 = 127$ are Mersenne primes.

$2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.

There is an efficient test for determining if $2^p - 1$ is prime. The largest known prime numbers are Mersenne primes. 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.

Distribution of Primes

Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the *prime number theorem* was proved which gives an asymptotic estimate for the number of primes not exceeding x.

Theorem – **Prime Number**

The ratio of the number of primes not exceeding x and $\dfrac{x}{\ln x}$ approaches 1 as x grows without bound. ($\ln x$ is the natural logarithm of x),

The theorem tells us that the number of primes not exceeding x, can be approximated by $\dfrac{x}{\ln x}$.

The odds that a randomly selected positive integer less than n is prime are approximately

$$\left(n / \ln n / n \right) = \frac{1}{\ln n}$$

Greatest Common Divisor

Definition

Let *a* and *b* be integers, not both zero. The largest integer *d* such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of *a* and *b*. The greatest common divisor of *a* and *b* is denoted by $\gcd(a,b)$.

One can find greatest common divisors of small numbers by inspection.

Example

What is the greatest common divisor of 24 and 36?

Solution

$\gcd(24,26) = 12$

Example

What is the greatest common divisor of 17 and 22?

Solution

$\gcd(17,22) = 1$

Definition

The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1.

Example 17 and 22

Definition

The integers a_1, a_2, …, a_n are *pairwise relatively prime* if $\gcd\left(a_i, a_j\right) = 1$ whenever $1 \leq i \leq j \leq n$.

Example

Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution

Because $\gcd(10,17) = 1$, $\gcd(10,21) = 1$, and $\gcd(17,21) = 1$, 10, 17, and 21 are pairwise relatively prime.

Example

Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution

Because $\gcd(10,24) = 2$, 10, 19, and 24 are not pairwise relatively prime.

Least Common Multiple

Definition

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by lcm(a,b).

The least common multiple can also be computed from the prime factorizations.

$$lcm(a,\ b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}$$

This number is divided by both a and b and no smaller number is divided by a and b.

Example

$$lcm\left(2^3 3^5 7^2,\ 2^4 3^3\right) = 2^{\max(3,4)} \cdot 3^{\max(5,3)} \cdot 7^{\max(2,0)}$$

$$= 2^4 \cdot 3^5 \cdot 7^2$$

Theorem

Let a and b be positive integers. Then $ab = \gcd(a,b) \cdot lcm(a,b)$

Euclidean Algorithm

The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(a,c) when $a > b$ and c is the remainder when a is divided by b.

Lemma 1

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a,b) = \gcd(b,r)$

Proof

Suppose that d divides both a and b. Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be any common divisor of b and r. Suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of a and b must also be a common divisor of b and r. Therefore, $\gcd(a,b) = \gcd(b,r)$.

Example

Find $gcd(91, 287)$

$287 = 91 \cdot 3 + 14$ *Divide **287** by **91***

$91 = 14 \cdot 6 + 7$ *Divide **91** by **14***

$14 = 7 \cdot 2 + 0$ *Divide **14** by **7***

$gcd(287, 91) = 7$

Example

Find $gcd(414, 662)$

Solution

$662 = 414 \cdot 1 + 248$ *Divide **662** by **414***

$414 = 248 \cdot 1 + 166$ *Divide **414** by **248***

$248 = 166 \cdot 1 + 82$ *Divide **248** by **166***

$166 = 82 \cdot 2 + 2$ *Divide **166** by **82***

$82 = 2 \cdot 41 + 0$ *Divide **82** by **2***

$gcd(414, 662) = 2$

Euclidean Algorithm

procedure $gcd(a, b$: positive integers)

$x := a$

$x := b$

while $y \neq 0$

    $r := x \bmod y$

    $x := y$

    $y := r$

return x $\{gcd(a,b)$ is $x\}$

GCDs **as Linear Combinations**

Bézout's Theorem

If a and b are positive integers, then there exist integers s and t such that $gcd(a,b) = sa + tb$.

Definition

If *a* and *b* are positive integers, then integers *s* and *t* such that $\gcd(a,b) = sa + tb$ are called ***Bézout coefficients*** of *a* and *b*. The equation $\gcd(a,b) = sa + tb$ is called ***Bézout's identity***.

Example

Express $\gcd(252,198) = 18$ as a linear combination of 252 and 198.

Solution

First use the Euclidean algorithm to show $\gcd(252,198) = 18$

i. $252 = 1 \cdot 198 + 54$
ii. $198 = 3 \cdot 54 + 36$
iii. $54 = 1 \cdot 36 + 18$
iv. $36 = 2 \cdot 18$

Now working backwards, from *iii* and *i* above

$18 = 54 - 1 \cdot 36$
$36 = 198 - 3 \cdot 54$

Substituting the 2nd equation into the 1st yields:

$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$

Substituting $54 = 252 - 1 \cdot 198$ (from *i*)) yields:

$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the ***extended Euclidean algorithm***, is developed in the exercises.

Lemma 2

If *a*, *b*, and *c* are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof

Assume $\gcd(a, b) = 1$ and $a \mid bc$
Since $\gcd(a, b) = 1$, by Bézout's Theorem there are integers *s* and *t* such that $sa + tb = 1$.
Multiplying both sides of the equation by *c*, yields $sac + tbc = c$. $a \mid tbc$ and *a* divides $sac + tbc$ since $a \mid sac$ and $a \mid tbc$. We conclude $a \mid c$, since $sac + tbc = c$.

Lemma 3

If *p* is prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some *i*.

- Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

Uniqueness of Prime Factorization

We will prove that a prime factorization of a positive integer where the primes are in nondecreasing order is unique.

Proof   (*by contradiction*)

Suppose that the positive integer n can be written as a product of primes in two distinct ways:

$$n = p_1 p_2 \cdots p_s \text{ and } n = q_1 q_2 \cdots q_t$$

Remove all common primes from the factorizations to get

$$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$$

By Lemma 3, it follows that p_{i_1} divides q_{j_k}, for some k, contradicting the assumption that p_{i_1} and q_{j_k} are distinct primes.

Hence, there can be at most one factorization of n into primes in nondecreasing order.

Dividing Congruences by an Integer

Theorem

Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

Proof

Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

Exercises   *Section* 2.5 – **Primes and Greatest Common Divisors**

1. Determine whether each of these integers is prime.

    a) 21 b) 29 c) 71 d) 97 e) 111
    f) 143 g) 19 h) 27 i) 93 j) 101
    k) 107 l) 113

2. Find the prime factorization of each these integers.

    a) 88 b) 126 c) 729 d) 1001 e) 1111
    f) 909,090 g) 39 h) 81 i) 101 j) 143
    k) 289 l) 899

3. Find the prime factorization of 10!

4. Show that if $a^m + 1$ is composite if a and m are integers greater than 1 and m is odd. [*Hint*: Show that $x + 1$ is a factor of the polynomial $a^m + 1$ if m is odd]

5. Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer n. [*Hint*: First show the polynomial identity $x^m + 1 = \left(x^k + 1\right)\left(x^{k(t-1)} - x^{k(t-2)} + \cdots - x^k + 1\right)$ holds, where $m = kt$ and t is odd]

6. Which positive integers less than 12 are relatively prime to 12?

7. Which positive integers less than 30 are relatively prime to 30?

8. Determine whether the integers in each of these sets are pairwise relatively prime.

    a) 21, 34, 55 b) 14, 17, 85 c) 25, 41, 49, 64 d) 17, 18, 19, 23
    e) 11, 15, 19 f) 14, 15, 21 g) 12, 17, 31, 37 h) 7, 8, 9, 11

9. We call a positive integer ***perfect*** if it equals the sum of its positive divisors other than itself

    a) Show that 6 and 28 are perfect.
    b) Show that $2^{p-1}\left(2^p - 1\right)$ is a perfect number when $2^p - 1$ is prime

10. Show that if $2^n - 1$ is prime, then n is prime. *Hint*: Use the identity
    $$2^{ab} - 1 = \left(2^a - 1\right) \cdot \left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right)$$

11. Determine whether each of these integers is prime, verifying some of Mersenne's claims

    a) $2^7 - 1$ b) $2^9 - 1$ c) $2^{11} - 1$ d) $2^{13} - 1$

12. What are the greatest common divisors of these pairs of integers?

    a) $2^2 \cdot 3^3 \cdot 5^5$, $2^5 \cdot 3^3 \cdot 5^2$

    b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

    c) 17, 17^{17}

    d) $2^2 \cdot 7$, $5^3 \cdot 13$

    e) 0, 5

    f) $2 \cdot 3 \cdot 5 \cdot 7$, $2 \cdot 3 \cdot 5 \cdot 7$

    g) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

    h) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

    i) 23^{31}, 23^{17}

    j) $41 \cdot 43 \cdot 53$, $41 \cdot 43 \cdot 53$

    k) 1111, 0

13. What is the least common multiple of each pair

    a) $2^2 \cdot 3^3 \cdot 5^5$, $2^5 \cdot 3^3 \cdot 5^2$

    b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, $2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$

    c) 17, 17^{17}

    d) $2^2 \cdot 7$, $5^3 \cdot 13$

    e) 0, 5

    f) $2 \cdot 3 \cdot 5 \cdot 7$, $2 \cdot 3 \cdot 5 \cdot 7$

    g) $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

    h) $11 \cdot 13 \cdot 17$, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

    i) 23^{31}, 23^{17}

    j) $41 \cdot 43 \cdot 53$, $41 \cdot 43 \cdot 53$

    k) 1111, 0

14. Find gcd(1000, 625) and lcm(1000, 625) and verify that $\gcd(100,\ 625) \cdot lcm(100,\ 625) = 1000 \cdot 625$

15. Find gcd(92928, 123552) and lcm(92928, 123552) and verify that
$\gcd(92928,\ 123552) \cdot lcm(92928,\ 123552) = 92928 \bullet 123552$

16. Use the Euclidean algorithm to find

    a) $\gcd(1,\ 5)$ *b)* $\gcd(100,\ 101)$ *c)* $\gcd(123,\ 277)$ *d)* $\gcd(1529,\ 14039)$

    e) $\gcd(1529,\ 14038)$ *f)* $\gcd(12,\ 18)$ *g)* $\gcd(111,\ 201)$ *h)* $\gcd(1001,\ 1331)$

    i) $\gcd(12345,\ 54321)$ *j)* $\gcd(1000,\ 5040)$ *k)* $\gcd(9888,\ 6060)$

17. Prove that the product of any three consecutive integers is divisible by 6.

18. Show that if *a, b*, and *m* are integers such that $m \geq 2$ and $a \equiv b \pmod{m}$, then

$$\gcd(a,\ m) = \gcd(b,\ m)$$

19. Prove or disprove that $n^2 - 79n + 1601$ is prime whenever *n* is a positive integer.

Section 2.6 – **Applications of Congurences**

Hashing Functions

Definition

A *hashing function h* assigns memory location $h(k)$ to the record that has k as its key.

A common hashing function is $h(k) = k \bmod m$, where m is the number of memory locations. Because this hashing function is onto, all memory locations are possible.

Example

Find the memory locations assigned by the hashing function $h(k) = k \bmod 111$ to the records of customers with Social Security numbers 064212848, 037149212, and 107405723.

Solution

This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

$h(064212848) = 064212848 \bmod 111 = 14$
$h\,(037149212) = 037149212 \bmod 111 = 65$
$h\,(107405723) = 107405723 \bmod 111 = 14,$

But since location 14 is already occupied, the record is assigned to the next available position, which is 15.

The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location. For collision resolution, we can use a *linear probing function*:

$$h(k,\,i) = \big(h(k),\,i\big) \bmod m, \text{ where } i \text{ from 0 to m} - 1.$$

There are many other methods of handling with collisions. You may cover these in a later CS course.

Pseudorandom Numbers

Randomly chosen numbers are needed for many purposes, including computer simulations.
Pseudorandom numbers are not truly random since they are generated by systematic methods.
The **linear congruential** *method* is one commonly used procedure for generating pseudorandom numbers.
Four integers are needed: the *modulus m*, the *multiplier a*, the *increment c*, and *seed* x_0, with $2 \le a < m$, $0 \le c < m$, $0 \le x_0 < m$. We generate a sequence of pseudorandom numbers $\{x_m\}$, with $0 \le x_n < m$ for all n, by successively using the recursively defined function

$$x_{n+1} = \left(ax_n + c\right) \bmod m$$

Example

Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.

Solution

Compute the terms of the sequence by successively using the congruence $x_{n+1} = \left(7x_n + 4\right) \bmod 9$, with $x_0 = 3$.

$x_1 = \left(7x_0 + 4\right) \bmod 9 = \left(7 \cdot 3 + 4\right) \bmod 9 = 25 \bmod 9 = 7$

$x_2 = \left(7x_1 + 4\right) \bmod 9 = \left(7 \cdot 7 + 4\right) \bmod 9 = 53 \bmod 9 = 8$

$x_3 = \left(7x_2 + 4\right) \bmod 9 = \left(7 \cdot 8 + 4\right) \bmod 9 = 60 \bmod 9 = 6$

$x_4 = \left(7x_3 + 4\right) \bmod 9 = \left(7 \cdot 6 + 4\right) \bmod 9 = 46 \bmod 9 = 1$

$x_5 = \left(7x_4 + 4\right) \bmod 9 = \left(7 \cdot 1 + 4\right) \bmod 9 = 11 \bmod 9 = 2$

$x_6 = \left(7x_5 + 4\right) \bmod 9 = \left(7 \cdot 2 + 4\right) \bmod 9 = 18 \bmod 9 = 0$

$x_7 = \left(7x_6 + 4\right) \bmod 9 = \left(7 \cdot 0 + 4\right) \bmod 9 = 4 \bmod 9 = 4$

$x_8 = \left(7x_7 + 4\right) \bmod 9 = \left(7 \cdot 4 + 4\right) \bmod 9 = 32 \bmod 9 = 5$

$x_9 = \left(7x_8 + 4\right) \bmod 9 = \left(7 \cdot 5 + 4\right) \bmod 9 = 39 \bmod 9 = 3$

The sequence generated is 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, … It repeats after generating 9 terms.

➤ Commonly, computers use a linear congruential generator with increment $c = 0$. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Check Digits: UPCs

A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example

Retail products are identified by their *Universal Product Codes* (*UPCs*). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$$

  a) Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

  b) Is 041331021641 a valid UPC?

Solution

  a) $3\cdot7+9+3\cdot3+5+3\cdot7+3+3\cdot4+3+3\cdot1+0+3\cdot4+x_{12} \equiv 0 \pmod{10}$

    $98+x_{12} \equiv 0 \pmod{10}$

    $x_{12} \equiv 0 \pmod{10}$.   So, the check digit is 2.

  b) $3\cdot0+4+3\cdot1+3+3\cdot3+1+3\cdot0+2+3\cdot1+6+3\cdot4+1 \equiv 0 \pmod{10}$

    $44 \equiv 4 \not\equiv \pmod{10}$

    Hence, 041331021641 is not a valid UPC.

Exercises   *Section* 2.6 – **Applications of Congurences**

1. Find the memory locations assigned by the hashing function $h(k) = k$ **mod** 97 to the records of customers with Social Security numbers?

    a) 034567981   b) 183211232   c) 220195744   d) 987255335

    e) 104578690   f) 432222187   g) 372201919   h) 501338753

2. A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function $h(k) = k$ **mod** 31, where k is the number formed from the first three digits on a visitor's license plate.

    a) Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates: 317, 918, 007, 100, 111, 310

    b) Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

3. Find the sequence of pseudorandom numbers generated by the linear congruential generator

    a) $x_{n+1} = \left(3x_n + 2\right)$ **mod** 13 with seed $x_0 = 1$.

    b) $x_{n+1} = \left(4x_n + 1\right)$ **mod** 7 with seed $x_0 = 3$.

4. Find the sequence of pseudorandom numbers generated by using the pure multiplicative generator $x_{n+1} = 3x_n$ **mod** 11 with seed $x_0 = 2$.

5. The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are $0 - 07 - 119881$. What is the check digit for that book?

6. The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is $0 - 321 - 500Q1 - 8$, where Q is a digit. Find the value of Q.

7. The USPS sells money orders identified by 11-digit number $x_1, x_2, \ldots, x_{11}$. The first ten digits identify the money order: x_{11} is a check digit that satisfies $x_{11} = x_1 + x_2 + \cdots + x_{10}$ **mod** 9. Find the check digit for the USPS money orders that have identification number that start with these ten digits

    a) 7555618873   b) 6966133421   c) 8018927435   d) 3289744134

    e) 74051489623   f) 88382013445   g) 56152240784   h) 66606631178

8. Determine which single digit errors are detected by the USPS money order code.

9. Determine which transposition errors are detected by the USPS money order code.

Lecture Three

Section 3.1 – Mathematical Induction

Introduction

Suppose we have an infinite ladder:

1. We can reach the first rung of the ladder.
2. If we can reach a particular rung of the ladder, then we can reach the next rung.

From (1), we can reach the first rung. Then by applying (2), we can reach the second rung. Applying (2) again, the third rung. And so on. We can apply (2) any number of times to reach any particular rung, no matter how high up.

This example motivates proof by mathematical induction.
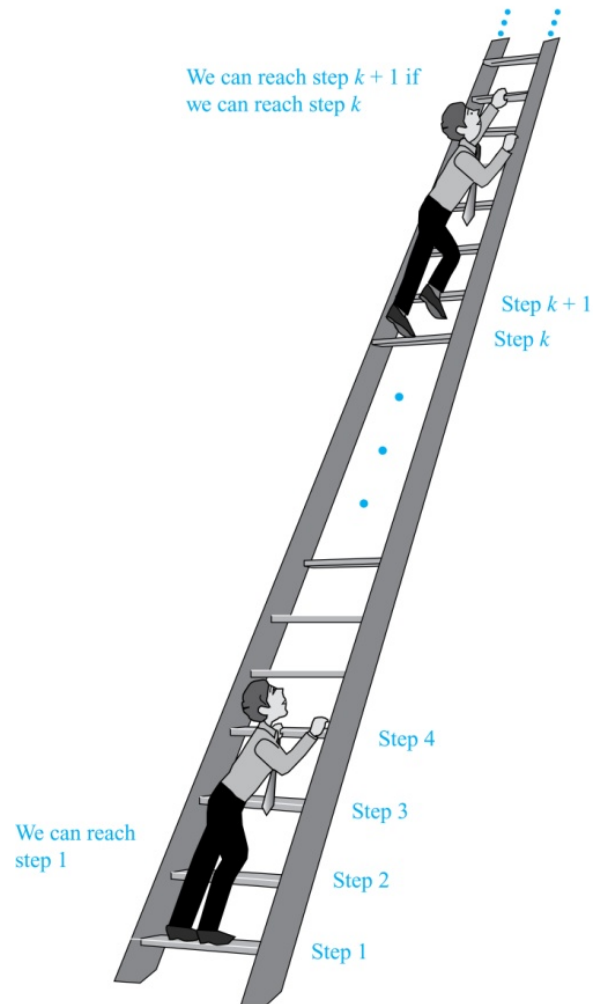
Mathematical Induction

Principle of Mathematical Induction

To prove that $P(n)$ is true for all positive integers n, we complete these steps:

- *Basis Step*: Show that $P(1)$ is true.
- *Inductive Step*: Show that $P(k) \rightarrow P(k + 1)$ is true for all positive integers k.

To complete the inductive step, assuming the *inductive hypothesis* that $P(k)$ holds for an arbitrary integer k, show that must $P(k + 1)$ be true.

Climbing an Infinite Ladder Example:

BASIS STEP: By (1), we can reach rung 1.
INDUCTIVE STEP: Assume the inductive hypothesis that we can reach rung k. Then by (2), we can reach rung $k + 1$.
Hence, $P(k) \rightarrow P(k + 1)$ is true for all positive integers k. We can reach every rung on the ladder.

131

Examples of Proofs by Mathematical induction

Mathematical induction can be expressed as the rule of inference

$$\left(P(1) \wedge \forall k \left(P(k) \rightarrow P(k+1) \right) \right) \rightarrow \forall n P(n)$$

where the domain is the set of positive integers.

In a proof by mathematical induction, we don't assume that $P(k)$ is true for all positive integers! We show that if we assume that $P(k)$ is true, then $P(k+1)$ must also be true.
Proofs by mathematical induction do not always start at the integer 1. In such a case, the basis step begins at a starting point b where b is an integer.

Validity of Mathematical Induction

Mathematical induction is valid because of the well ordering property, which states that every nonempty subset of the set of positive integers has a least element. Here is the proof:
- Suppose that $P(1)$ holds and $P(k) \rightarrow P(k+1)$ is true for all positive integers k.
- Assume there is at least one positive integer n for which $P(n)$ is false. Then the set S of positive integers for which $P(n)$ is false is nonempty.
- By the well-ordering property, S has a least element, say m.
- We know that m cannot be 1 since $P(1)$ holds.
- Since m is positive and greater than 1, $m - 1$ must be a positive integer. Since $m - 1 < m$, it is not in S, so $P(m-1)$ must be true.
- But then, since the conditional $P(k) \rightarrow P(k+1)$ for every positive integer k holds, $P(m)$ must also be true. This contradicts $P(m)$ being false.
- Hence, $P(n)$ must be true for every positive integer n

Example

Show that if n is a positive integer, then $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$

Solution

Basis Step: $P(1)$ is true since $1 = \dfrac{1(1+1)}{2} = 1$.

Inductive Step: Assume true for $P(k)$. The inductive hypothesis is $1 + 2 + \cdots + k = \dfrac{k(k+1)}{2}$

Under this assumption, $\quad 1 + 2 + \cdots + k + (k+1) = \dfrac{(k+1)\left[(k+1)+1\right]}{2} = \dfrac{(k+1)(k+2)}{2}$

$$1 + 2 + \cdots + k + (k+1) = \dfrac{k(k+1)}{2} + (k+1)$$

$$= \dfrac{k(k+1) + 2(k+1)}{2}$$

$$= \dfrac{(k+1)(k+2)}{2} \quad \checkmark$$

The last equation shows that $P(k+1)$ is true under the assumption that $P(k)$ is true. This completes the inductive step.

Example

Conjecture and prove correct a formula for the sum of the first n positive odd integers. Then prove your conjecture.

Solution

The sums of the first n positive odd integers for $n = 1, 2, 3, 4, 5$ are
$$1 = 1,\ 1 + 3 = 4,\ 1 + 3 + 5 = 9,\ 1 + 3 + 5 + 7 = 16,\ 1 + 3 + 5 + 7 + 9 = 25.$$

Basis Step: $P(1)$ is true since $1^2 = 1$.

Inductive Step: $P(k) \rightarrow P(k+1)$ for every positive integer k.

Assume the inductive hypothesis holds and then show that $P(k)$ holds has well.

Inductive Hypothesis: $1 + 3 + 5 + \cdots + (2k-1) = k^2$

So, assuming $P(k)$, it follows that:

$$1 + 3 + 5 + \cdots + (2k-1) + (2k+1) = k^2 + (2k+1)$$
$$= k^2 + 2k + 1$$
$$= (k+1)^2 \quad \checkmark$$

Hence, we have shown that $P(k+1)$ follows from $P(k)$. Therefore the sum of the first n positive odd integers is n^2.

Example

Use mathematical induction to show that $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ for all nonnegative integers n.

Solution

Basis Step: For $\boldsymbol{n = 0} \Rightarrow 1 \overset{?}{=} 2^{0+1} - 1 = 2 - 1 = 1$; hence P_0 is true.

Inductive Step: $1 + 2 + 2^2 + \ldots + 2^k = 2^{k+1} - 1$ is true for every positive integer k.

$$1 + 2 + 2^2 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1?$$

$$1 + 2 + 2^2 + \ldots + 2^k + 2^{k+1} = \left(2^{k+1} - 1\right) + 2^{k+1}$$
$$= 2 \cdot 2^{k+1} - 1$$
$$= 2^{k+2} - 1 \quad \checkmark$$

Hence P_{k+1} is true.

By mathematical induction, the statement $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ is true

133

Example

Use mathematical induction to prove this formula for the sum of a finite number of terms of a geometric progression with initial term a and common ratio r:

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \ldots + ar^n = \frac{ar^{n+1} - a}{r-1} \qquad when \ r \neq 1$$

for all nonnegative integers n.

Solution

Basis Step: For $\boldsymbol{n = 0} \Rightarrow \dfrac{ar^{0+1} - a}{r-1} = \dfrac{ar - a}{r-1} = \dfrac{a(r-1)}{r-1} = a$; hence P_0 is true.

Inductive Step: $a + ar + ar^2 + \ldots + ar^k = \dfrac{ar^{k+1} - a}{r-1}$ is true for every positive integer k.

$$a + ar + ar^2 + \ldots + ar^k + ar^{k+1} = \frac{ar^{k+2} - a}{r-1} \ \textcolor{red}{?}$$

$$a + ar + ar^2 + \ldots + ar^k + ar^{k+1} = \frac{ar^{k+1} - a}{r-1} + ar^{k+1}$$

$$= \frac{ar^{k+1} - a + ar^{k+1}(r-1)}{r-1}$$

$$= \frac{ar^{k+1} - a + ar^{k+2} - ar^{k+1}}{r-1}$$

$$= \frac{-a + ar^{k+2}}{r-1}$$

$$= \frac{ar^{k+2} - a}{r-1} \quad \checkmark$$

Hence P_{k+1} is true.

By mathematical induction, the statement

$$\sum_{j=0}^{n} ar^j = a + ar + ar^2 + \ldots + ar^n = \frac{ar^{n+1} - a}{r-1}, \quad when \ r \neq 1 \ \text{is true}$$

Proving Inequalities

Example

Prove that the statement is true for every positive integer n. $n < 2^n$

Solution

   Basis Step: For $n = 1 \Rightarrow 1 \overset{?}{<} 2^1$ ✓ $\Rightarrow P_1$ is true.

   Inductive Step. Assume that P_k is true $k < 2^k$

   We need to prove that P_{k+1} is true, that is $k + 1 < 2^{k+1}$

$$k + 1 < k + k = 2k$$
$$< 2 \cdot 2^k$$
$$= 2^{k+1}$$ ✓

   Thus, P_{k+1} is true.

   By mathematical induction, the statement $n < 2^n$ is true.

Example

Prove that the statement is true for every positive integer n. $2^n < n!$ for every integer n with $n \geq 4$

Solution

   Basis Step: For $n = 4 \Rightarrow 2^4 \overset{?}{<} 4! \Rightarrow 16 < 24$ ✓ $\Rightarrow P_4$ is true.

   Inductive Step. Assume that P_k is true $2^k < k!$

   We need to prove that P_{k+1} is true, that is $2^{k+1} < (k+1)!$

$$2^{k+1} = 2^k \cdot 2 = 2 \cdot 2^k$$
$$< 2 \cdot k!$$
$$< (k+1)k! \qquad\qquad 2 < k+1$$
$$= (k+1)!$$ ✓

   Thus, P_{k+1} is true.

   By mathematical induction, the statement $2^n < n!$ is true.

Harmonic **Numbers**

Example

The harmonic numbers H_j, $j = 1, 2, 3, \ldots$ are defined by

$$H_j = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{j}$$

Use the mathematical method to show that $H_{2^n} \geq 1 + \frac{n}{2}$ for all nonnegative integers n.

Solution

   Basis Step: For $n = 0 \Rightarrow H_{2^0} = H_1 = 1 \geq 1 + \frac{0}{2} = 1$ ✓ $\Rightarrow P_0$ is true.

   Inductive Step. Assume that P_k is true $H_{2^k} \geq 1 + \frac{k}{2}$

     We need to prove that P_{k+1} is true, that is $H_{2^{k+1}} \geq 1 + \frac{k+1}{2}$

$$\begin{aligned}
H_{2^{k+1}} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k} + \frac{1}{2^k + 1} + \cdots + \frac{1}{2^{k+1}} \\[2mm]
&= H_{2^k} + \frac{1}{2^k + 1} + \cdots + \frac{1}{2^{k+1}} \\[2mm]
&\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2^k + 1} + \cdots + \frac{1}{2^{k+1}} \\[2mm]
&\geq \left(1 + \frac{k}{2}\right) + 2^k \cdot \frac{1}{2^{k+1}} \qquad\qquad \left(each\ 2^k\right) \geq \frac{1}{2^{k+1}} \\[2mm]
&\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2} \\[2mm]
&= 1 + \frac{k+1}{2} \checkmark
\end{aligned}$$

   Thus, P_{k+1} is true.

By mathematical induction, the statement $H_{2^n} \geq 1 + \frac{n}{2}$ is true.

Example

Use mathematical induction to prove that $n^3 - n$ is divisible by 3, for every positive integer n.

Solution

Let $P(n)$ be the proposition that $n^3 - n$ is divisible by 3.

Basis Step: For $n = 1 \Rightarrow 1^3 - 1 = 0$ which is divisible by 3 $\Rightarrow P_1$ is true.

Inductive Step. Assume that P_k holds $k^3 - k$ is divisible by 3

We need to prove that P_{k+1} is true, that is $(k+1)^3 - (k+1)$ is divisible by 3

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1$$
$$= k^3 - k + 3k^2 + 3k$$
$$= \left(k^3 - k\right) + 3\left(k^2 + k\right)$$

$\left(k^3 - k\right)$ is divisible by 3, by the inductive hypothesis,

$3\left(k^2 + k\right)$ is divisible by 3, since it is an integer multiplied by 3.

Thus, P_{k+1} is true.

By mathematical induction, the statement $n^3 - n$ is divisible by 3 is true, for every positive integer n.

Example

Use mathematical induction to prove that $7^{n+2} + 8^{2n+1}$ is divisible by 57, for every nonnegative integer n.

Solution

Basis Step: For $n = 0 \Rightarrow 7^2 + 8^1 = 49 + 8 = 57$ which is divisible by 57 $\Rightarrow P_0$ is true.

Inductive Step: Assume that P_k holds $7^{k+2} + 8^{2k+1}$ is divisible by 57

We need to prove that P_{k+1} is true, that is $7^{k+1+2} + 8^{2(k+1)+1} = 7^{k+3} + 8^{2k+3}$ is also divisible by 57

$$7^{k+3} + 8^{2k+3} = 7 \cdot 7^{k+2} + 8^2 \cdot 8^{2k+1}$$
$$= 7 \cdot 7^{k+2} + 64 \cdot 8^{2k+1}$$
$$= 7 \cdot 7^{k+2} + 7 \cdot 8^{2k+1} + 57 \cdot 8^{2k+1}$$
$$= 7 \cdot \left(7^{k+2} + 8^{2k+1}\right) + 57 \cdot 8^{2k+1}$$

$\left(7^{k+2} + 8^{2k+1} \right)$ is divisible by 57, by the inductive hypothesis,

$57 \cdot 8^{2k+1}$ is divisible by 57, since it is an integer multiplied by 57.

Thus, P_{k+1} is true.

By mathematical induction, the statement $7^{n+2} + 8^{2n+1}$ is divisible by 57 is true, for every positive integer n.

Number of Subsets of a Finite Set

Inductive Hypothesis

For an arbitrary nonnegative integer k, every set with k elements has 2^k subsets.

Let T be a set with $k + 1$ elements. Then $T = S \cup \{a\}$, where $a \in T$ and $S = T - \{a\}$. Hence $|T| = k$.

For each subset X of S, there are exactly two subsets of T, i.e., X and $X \cup \{a\}$.
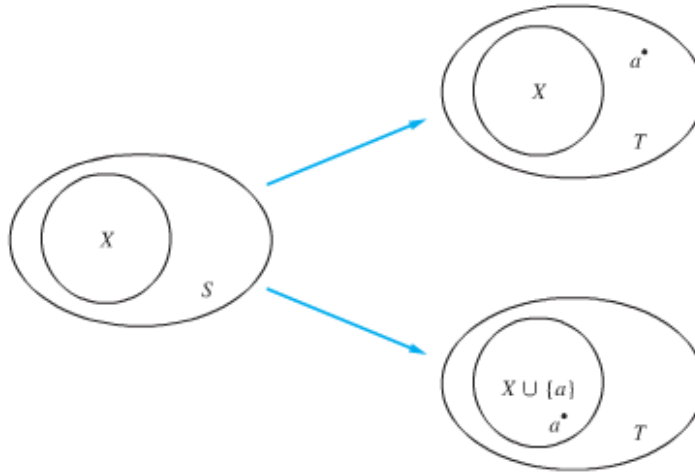
By the inductive hypothesis S has 2^k subsets. Since there are two subsets of T for each subset of S, the number of subsets of T is $2 \cdot 2^k = 2^{k+1}$

Example

Show that every $2^n \times 2^n$ checkerboard with one square removed can be tiled using right triominoes. A right triomino is an L-shaped tile which covers three squares at a time.

Solution

Let $P(n)$ be the proposition that every $2^n \times 2^n$ checkerboard with one square removed can be tiled using right triominoes. Use mathematical induction to prove that $P(n)$ is true for all positive integers n.

Basis Step: $P(1)$ is true, because each of the four 2×2 checkerboards with one square removed can be tiled using one right triomino.

Inductive Step: Assume that $P(k)$ is true for every $2^k \times 2^k$ checkerboard, for some positive integer k. with one square removed can be tiled using right triominoes.

Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Split this checkerboard into four checkerboards of size $2^k \times 2^k$, by dividing it in half in both directions.
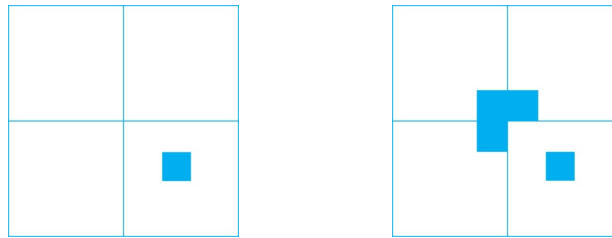
Remove a square from one of the four $2^k \times 2^k$ checkerboards. By the inductive hypothesis, this board can be tiled. Also by the inductive hypothesis, the other three boards can be tiled with the square from the corner of the center of the original board removed. We can then cover the three adjacent squares with a triominoe.

Hence, the entire $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed can be tiled using right triominoes.

Guidelines: **Mathematical Induction Proofs**

Template for Proofs by Mathematical Induction

1. Express the statement that is to be proved in the form "for all $n \geq b$, $P(n)$" for a fixed integer b.

2. Write out the words "Basis Step" or "step 1". Then show that $P(b)$ is true, taking care that the correct value of b is used. This completes the first part of the proof.

3. Write out the words "Inductive Step."

4. State and clearly identify, the inductive hypothesis, in the form "assume that $P(k)$ is true for an arbitrary fixed integer $k \geq b$."

5. State what needs to be proved under the assumption that the inductive hypothesis is true. That is, write out what $P(k+1)$ says.

6. Prove the statement $P(k+1)$ making use the assumption $P(k)$. Be sure that your proof is valid for all integers k with $k \geq b$, taking care that the proof works for small values of k, including $k = b$

7. Clearly identify the conclusion of the inductive step, such as by saying "this completes the inductive step."

8. After completing the basis step and the inductive step. State the conclusion, namely that by mathematical induction, $P(n)$ is true for all integers n with $n \geq b$.

Exercises   *Section* **3.1 – Mathematical Induction**

1. Prove that $1^2 + 3^2 + 5^2 + \cdots + (2n+1)^2 = \frac{1}{3}(n+1)(2n+1)(2n+3)$ whenever n is a nonnegative integer.

2. Prove that $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$ whenever n is a positive integer.

3. Prove that $3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = \frac{3}{4}\left(5^{n+1} - 1\right)$ whenever n is a nonnegative integer.

4. Prove that $2 - 2 \cdot 7 + 2 \cdot 7^2 - \cdots + 2 \cdot (-7)^n = \frac{1 - (-7)^{n+1}}{4}$ whenever n is a nonnegative integer.

5. Find a formula for the sum of the first n even positive integers. Prove the formula.

6. *a)* Find a formula for $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)}$ by examining the values of this expression for

    values of this expression for small values of n.
    b) Prove the formula.

7. Prove that $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$ whenever n is a positive integer.

8. Prove that for very positive integer n, $\displaystyle\sum_{k=1}^{n} k 2^k = (n-1)2^{n+1} + 2$.

9. Prove that for very positive integer n, $1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{1}{3}n(n+1)(n+2)$.

10. Prove that for very positive integer n,
    $$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2) = \frac{1}{4}n(n+1)(n+2)(n+3)$$

11. Let $P(n)$ be the statement that $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}$ where n is an integer greater than 1.

    a) Show is the statement $P(2)$?

    b) Show that $P(2)$ is true, completing the basis step of the proof.

    c) What is the inductive hypothesis?
    d) What do you need to prove in the inductive step?
    e) Complete the inductive step.
    f) Explain why these steps show that this inequality is true whenever n is an integer greater than 1.

12. Prove that $3^n < n!$ if n is an integer greater than 6.

13. Prove that $2^n > n^2$ if n is an integer greater than 4.

14. Prove that for every positive integer n, $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > 2\left(\sqrt{n+1} - 1\right)$.

15. Use mathematical induction to prove that 2 divides $n^2 + n$ whenever n is a positive integer.

16. Use mathematical induction to prove that 3 divides $n^3 + 2n$ whenever n is a positive integer.

17. Use mathematical induction to prove that 5 divides $n^5 - n$ whenever n is a positive integer.

18. Use mathematical induction to prove that $n^2 - 1$ is divisible by 8 whenever n is an odd positive integer.

19. Use mathematical induction to prove that 21 divides $4^{n+1} + 5^{2n-1}$ whenever n is a positive integer.

(20 – 50) Prove that the statement is true by the mathematical induction

20. $1 + 2 \cdot 2 + 3 \cdot 2^2 + \ldots + n \cdot 2^{n-1} = 1 + (n-1) \cdot 2^n$

21. $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

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

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

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

25. $\frac{4}{5} + \frac{4}{5^2} + \frac{4}{5^3} + \cdots + \frac{4}{5^n} = 1 - \frac{1}{5^n}$

26. $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$

27. $3 + 3^2 + 3^3 + \ldots + 3^n = \frac{3}{2}\left(3^n - 1\right)$

28. $x^{2n} + x^{2n-1}y + \cdots + xy^{2n-1} + y^{2n} = \frac{x^{2n+1} - y^{2n+1}}{x - y}$

29. $5 \cdot 6 + 5 \cdot 6^2 + 5 \cdot 6^3 + \cdots + 5 \cdot 6^n = 6\left(6^n - 1\right)$

30. $7 \cdot 8 + 7 \cdot 8^2 + 7 \cdot 8^3 + \cdots + 7 \cdot 8^n = 8\left(8^n - 1\right)$

31. $3 + 6 + 9 + \cdots + 3n = \frac{3n(n+1)}{2}$

32. $5 + 10 + 15 + \cdots + 5n = \dfrac{5n(n+1)}{2}$

33. $1 + 3 + 5 + \cdots + (2n-1) = n^2$

34. $4 + 7 + 10 + \cdots + (3n+1) = \dfrac{n(3n+5)}{2}$

35. $2 + 4 + 6 + \cdots + 2(n-1) + 2n = n(n+1)$

36. $1 + (1+2) + (1+2+3) + \cdots + (1+2+\cdots+n) = \dfrac{n(n+1)(n+2)}{6} = \displaystyle\sum_{k=1}^{n}\left(\sum_{i=1}^{k} i\right)$

37. $1 + 2 + 3 + \cdots + n < \dfrac{(2n+3)^2}{7}$

38. $\dfrac{1}{2n} \le \dfrac{1 \cdot 3 \cdot 5 \cdots (2n-3) \cdot (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n-2) \cdot (2n)}$

39. $\dfrac{2n+1}{2n+2} \le \dfrac{\sqrt{n+1}}{\sqrt{n+2}}$

40. $n! < n^n \quad for \quad n > 1$

41. For every positive integer n.　　$n < 2^n$

42. For every positive integer n.　　3 is a factor of $n^3 - n + 3$

43. For every positive integer n.　　4 is a factor of $5^n - 1$

44. $\left(a^m\right)^n = a^{mn}$ (a and m are constant)

45. $2^n > 2n \quad if \quad n \ge 3$

46. If $0 < a < 1$, then $a^n < a^{n-1}$

47. If $n \ge 4$, then $n! > 2^n$

48. $3^n > 2n+1 \quad if \quad n \ge 2$

49. $2^n > n^2 \quad for \quad n > 4$

50. $4^n > n^4 \quad for \quad n \ge 5$

51. A pile of n rings, each smaller than the one below it, is on a peg on board. Two other pegs are attached to the board. In the game called the Tower of Hanoi puzzle, all the rings must be moved, one at a time, to a different peg with no ring ever placed on top of a smaller ring. Find the least number of moves that would be required. Prove your result by mathematical induction.
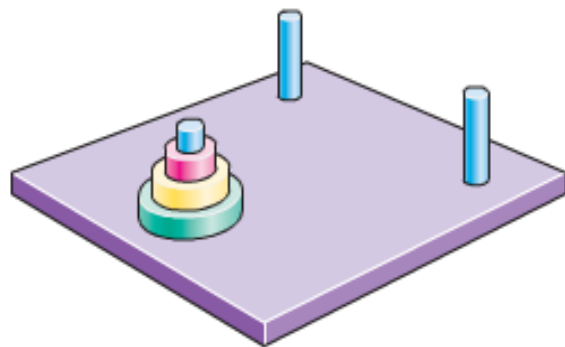
Section 3.2 − Recursive Definitions and Structural Induction

Recursive Algorithms

Definition

A **recursive** or **inductive** *definition* of a function consists of two steps.

1. **BASIS STEP**: Specify the value of the function at zero.
2. **RECURSIVE STEP**: Give a rule for finding its value at an integer from its values at smaller integers.

Example

Suppose f is defined by:
$$f(0) = 3$$
$$f(n+1) = 2f(n) + 3$$
Find $f(1), f(2), f(3), f(4)$

Solution

$f(1) = 2f(0) + 3 = 2{\cdot}3 + 3 = 9$
$f(2) = 2f(1) + 3 = 2{\cdot}9 + 3 = 21$
$f(3) = 2f(2) + 3 = 2{\cdot}21 + 3 = 45$
$f(4) = 2f(3) + 3 = 2{\cdot}45 + 3 = 93$

Example

Give a recursive definition of the factorial function $n!$

Solution

$f(0) = 1$
$f(n + 1) = (n + 1){\cdot} f(n)$
These 2 equations define $n!$

Example

Give a recursive definition of a^n, where a is a nonzero real number and n is a nonnegative integer.

Solution

$$a^0 = 1$$
$$a^{n+1} = a \cdot a^n \text{ for } n = 0, 1, 2, 3, \ldots.$$
These 2 equations define a^n for all nonnegative integers n.

Example

Give a recursive definition of: $\displaystyle\sum_{k=0}^{n} a_k$

<u>*Solution*</u>

The first part of the definition is $\displaystyle\sum_{k=0}^{0} a_k = a_0$

The second part is $\displaystyle\sum_{k=0}^{n+1} a_k = \left(\sum_{k=0}^{n} a_k\right) + a_{n+1}$

Fibonacci Numbers

Example

The Fibonacci numbers are defined as follows:

$f_0 = 0$

$f_1 = 1$

$f_n = f_{n-1} + f_{n-2}$

Find f_2, f_3, f_4, f_5

<u>*Solution*</u>

$f_2 = f_1 + f_0 = 1 + 0 \underline{= 1|}$

$f_3 = f_2 + f_1 = 1 + 1 \underline{= 2|}$

$f_4 = f_3 + f_2 = 2 + 1 \underline{= 3|}$

$f_5 = f_4 + f_3 = 3 + 2 \underline{= 5|}$

Example

Show that whenever $n \geq 3$, $f_n = \alpha^{n-2}$, where $\alpha = \dfrac{1+\sqrt{5}}{2}$

<u>*Solution*</u>

Basis Step: $n = 3$, $\alpha < 2 = f_3$

$$n = 4, \ \alpha^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} < 3 = f_4$$

146

Inductive Step: Assume that P_k holds $f_k = \alpha^{k-2}$

We need to prove that P_{k+1} is true, that is $f_{k+1} = \alpha^{(k+1)-2} = \alpha^{k-1}$ is also true.

$$\alpha^{k-1} = \alpha^2 \cdot \alpha^{k-3} \qquad\qquad \alpha^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{3+\sqrt{5}}{2} = \frac{2+1+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2} = 1 + \alpha$$

$$= (\alpha + 1) \cdot \alpha^{k-3}$$

$$= \alpha^{k-2} + \alpha^{k-3}$$

By the inductive hypothesis, we have $f_k > \alpha^{k-2}$ $f_{k-1} > \alpha^{k-3}$

Therefore. $f_{k+1} = f_k + f_{k-1} > \alpha^{k-2} + \alpha^{k-3} = \alpha^{k-1}$

Hence, P_{k+1} is true. This completes the proof.

Lamé's Theorem

Let a and b be positive integers with $a \geq b$. Then the number of divisions used by the Euclidian algorithm to find $\gcd(a, b)$ is less than or equal to five times the number of decimal digits in b.

Proof

When we use the Euclidian algorithm to find $\gcd(a, b)$ with $a \geq b$,

n divisions are used to obtain $\left(with\ a = r_0,\ b = r_1\right)$:

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 \leq r_1$$
$$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 \leq r_1$$
$$\vdots \quad \vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n \leq r_{n-1}$$
$$r_{n-1} = r_n q_n$$

Since each quotient $q_1, q_2, \ldots, q_{n-1}$ is at least 1 and $q_n \geq 2$:

$$r_n \geq 1 = f_2$$
$$r_{n-1} \geq 2 r_n \geq 2 f_2 = f_3$$
$$r_{n-2} \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4$$
$$\vdots \quad \vdots$$
$$r_2 \geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n$$
$$b = r_1 \geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}$$

It follows that if n divisions are used by the Euclidian algorithm to find $\gcd(a, b)$ with $a \geq b$, then

$b \geq f_{n+1}$. $f_{n+1} \geq \alpha^{n-1}$, for $n > 2$, where $\alpha = \dfrac{1+\sqrt{5}}{2}$. Therefore, $b > \alpha^{n-1}$.

Because $\log \alpha \approx 0.208 > \dfrac{1}{5}$, $\log b > (n-1)\log \alpha > \dfrac{n-1}{5}$. Hence, $n - 1 < 5 \cdot \log b$

Suppose that b has k decimal digits. Then $b < 10^k$ and $\log b < k$. It follows that $n - 1 < 5k$ and since k is an integer, $n \leq 5k$.

As a consequence of Lamé's Theorem, $O(\log b)$ divisions are used by the Euclidian algorithm to find $\gcd(a, b)$ whenever $a > b$.

Recursively Defined Sets and Structures

Recursive definitions of sets have two parts:

- The *basis step* specifies an initial collection of elements.
- The *recursive step* gives the rules for forming new elements in the set from those already known to be in the set.

Sometimes the recursive definition has an *exclusion rule*, which specifies that the set contains nothing other than those elements specified in the basis step and generated by applications of the rules in the recursive step.

We will always assume that the exclusion rule holds, even if it is not explicitly mentioned.

We will later develop a form of induction, called *structural induction*, to prove results about recursively defined sets.

Example

Consider the subset S of the set of integers recursively defined by

> *Basis step*: $3 \in S$.
> *Recursive step*: If $x \in S$ and $y \in S$, then $x + y$ is in S.
>
> > Initially 3 is in S, then $3 + 3 = 6$, then $3 + 6 = 9$, etc.

Example

Consider the subset **N** of the set of natural numbers recursively defined by

> *Basis step*: $0 \in \mathbf{N}$.
> *Recursive step*: If n is in **N**, then $n + 1$ is in **N**.
>
> > Initially 0 is in S, then $0 + 1 = 1$, then $1 + 1 = 2$, etc.

Strings

Definition

The set Σ^* of *strings* over the alphabet Σ:

Basis step: $\lambda \in \Sigma^*$ (λ is the empty string)

Recursive step: If $w \in \Sigma^*$ and $x \in \Sigma$, then $wx \in \Sigma^*$.

Example

If $\Sigma = \{0,1\}$, the strings in in Σ^* are the set of all bit strings, $\lambda, 0, 1, 00, 01, 10, 11$, etc.

Example

If $\Sigma = \{a,b\}$, show that *aab* is in Σ^*.

Since $\lambda \in \Sigma^*$ and $a \in \Sigma$, $a \in \Sigma^*$.

Since $a \in \Sigma^*$ and $a \in \Sigma$, $aa \in \Sigma^*$.

Since $aa \in \Sigma^*$ and $b \in \Sigma$, $aab \in \Sigma^*$.

String Concatenation

Definition

Two strings can be combined via the operation of *concatenation*. Let Σ be a set of symbols and Σ^* be the set of strings formed from the symbols in Σ. We can define the concatenation of two strings, denoted by $\cdot$, recursively as follows.

Basis step: If $w \in \Sigma^*$, then $w \cdot \lambda = w$.

Recursive step: If $w_1 \in \Sigma^*$ and $w_2 \in \Sigma^*$ and $x \in \Sigma$, then $w_1 \cdot \left(w_2 x \right) = \left(w_1 \cdot w_2 \right) x$.

- ✓ Often $w_1 \cdot w_2$ is written as $w_1 w_2$.
- ✓ If $w_1 = abra$ and $w_2 = cadabra$, the concatenation $w_1 w_2 = abracadabra$.

Length of a String

Example

Give a recursive definition of $l(w)$, the length of the string w.

Solution

The length of a string can be recursively defined by:

$l(w) = 0$;

$l(wx) = l(w) + 1$ if $w \in \Sigma^*$ and $x \in \Sigma$.

Well-Formed Formulae in Propositional Logic

Definition

The set of *well-formed formulae* in propositional logic involving **T**, **F**, propositional variables, and operators from the set $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$.

Basis step: **T**, **F**, and s, where s is a propositional variable, are well-formed formulae.

Recursive step: If E and F are well formed formulae, then $(\neg E)$, $(E \wedge F)$, $(E \vee F)$, $(E \rightarrow F)$, $(E \leftrightarrow F)$, are well-formed formulae.

Examples

$((p \vee q) \rightarrow (q \wedge \textbf{F}))$ is a well-formed formula.
$pq \wedge$ is not a well formed formula.

Rooted Trees

Definition

The set of *rooted trees,* where a rooted tree consists of a set of vertices containing a distinguished vertex called the *root*, and edges connecting these vertices, can be defined recursively by these steps:

Basis step: A single vertex r is a rooted tree.

Recursive step: Suppose that T_1, T_2, …, T_n are disjoint rooted trees with roots r_1, r_2, …, r_n, respectively. Then the graph formed by starting with a root r, which is not in any of the rooted trees T_1, T_2, …, T_n, and adding an edge from r to each of the vertices r_1, r_2, …, r_n, is also a rooted tree.
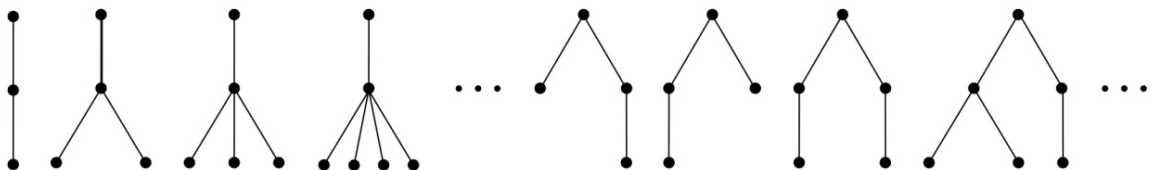
Definition

The set of **extended binary trees** can be defined recursively by these steps:
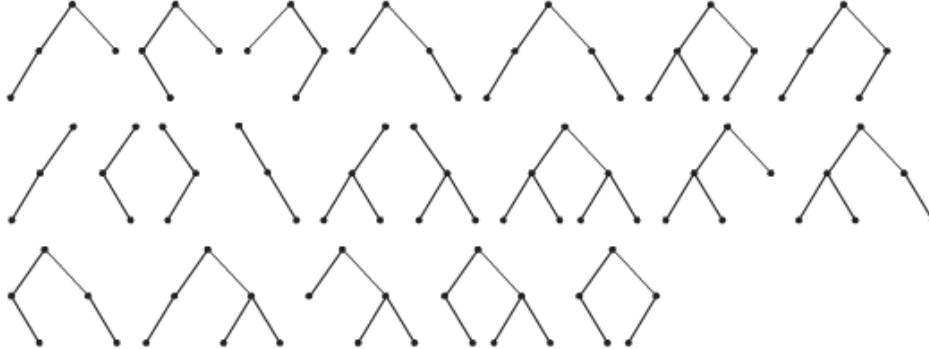
Basis step: The empty set is an extended binary tree.

Recursive step: If T_1 and T_2 are disjoint extended binary trees, there is an extended binary tree, denoted by $T_1 \cdot T_2$, consisting of a root r together with edges connecting the root to each of the roots of the left subtree T_1 and the right subtree T_2 when these trees are nonempty.

Extended Binary Trees

Definition

The set of **full binary trees** can be defined recursively by these steps:

Basis step: There is a full binary tree consisting only of a single vertex r.

Recursive step: If T_1 and T_2 are disjoint full binary trees, there is a full binary tree, denoted by $T_1 \cdot T_2$, consisting of a root r together with edges connecting the root to each of the roots of the left subtree T_1 and the right subtree T_2.
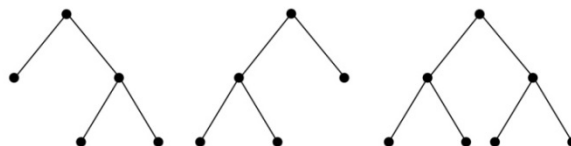
Full Binary Trees

152

Structural Induction

Example

Show that the set S defined by specifying that $3 \in S$ and that if $x \in S$ and $y \in S$, then $x + y$ is in S, is the set of all positive integers that are multiples of 3.

Solution

Let A be the set of all positive integers divisible by 3.

To prove that $A = S$, show that A is a subset of S and S is a subset of A.

$A \subset S$: Let P(n) be the statement that $3n$ belongs to S.

Basis step: $3 \cdot 1 = 3 \in S$, by the first part of recursive definition.

Inductive step: Assume P(k) is true. By the second part of the recursive definition, if $3k \in S$, then since $3 \in S$, $3k + 3 = 3(k + 1) \in S$. Hence, P($k + 1$) is true.

$S \subset A$:

Basis step: $3 \in S$ by the first part of recursive definition, and $3 = 3 \cdot 1$.

Inductive step: The second part of the recursive definition adds $x + y$ to S, if both x and y are in S. If x and y are both in A, then both x and y are divisible by 3. It follows that $x + y$ is divisible by 3.

Full Binary Trees

Definition

The *height $h(T)$* of a full binary tree T is defined recursively as follows:

Basis step: The height of a full binary tree T consisting of only a root r is $h(T) = 0$.

Recursive step: If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 T_2$ has height

$$h(T) = 1 + \max\left(h(T_1), h(T_2)\right).$$

The number of vertices $n(T)$ of a full binary tree T satisfies the following recursive formula:

Basis step: The number of vertices of a full binary tree T consisting of only a root r is $n(T) = 1$.

Recursive step: If T_1 and T_2 are full binary trees, then the full binary tree $T = T_1 T_2$ has the number of vertices $n(T) = 1 + n(T_1) + n(T_2)$.

Theorem

If T is a full binary tree, then $n(T) \le 2^{h(T)+1} - 1$

Proof

Use structural induction.

Basis step: The result holds for a full binary tree consisting only of a root, $n(T) = 1$ and $h(T) = 0$.

Hence, $n(T) = 1 \le 2^{0+1} - 1 = 1$.

Recursive step: Assume $n(T_1) \le 2^{h(T_1)+1} - 1$ and also $n(T_2) \le 2^{h(T_2)+1} - 1$ whenever T_1 and T_2 are

full binary trees.

$$n(T) = 1 + n(T_1) + n(T_2) \qquad \text{\textit{(by recursive formula of n(T))}}$$

$$\le 1 + \left(2^{h(T_1)+1} - 1\right) + \left(2^{h(T_2)+1} - 1\right) \qquad \text{\textit{(by inductive hypothesis)}}$$

$$\le 2 \cdot \max\left(2^{h(T_1)+1}, 2^{h(T_2)+1}\right) - 1$$

$$= 2 \cdot 2^{\max(h(T_1)+1,\ h(T_2))+1} - 1 \qquad \left(\max\left(2^x, 2^y\right) = 2^{\max(x,y)}\right)$$

$$= 2 \cdot 2^{h(t)} - 1 \qquad \text{\textit{(by recursive definition of h(T))}}$$

$$= 2^{h(t)+1} - 1$$

Exercises   *Section* **3.2 – Recursive Definitions and Structural Induction**

1. Find $f(1), f(2), f(3)$, and $f(4)$ if $f(n)$ is defined recursively by $f(0)=1$ and for $n = 0, 1, 2,...$

   a) $f(n+1) = f(n) + 2$

   b) $f(n+1) = 3f(n)$

   c) $f(n+1) = 2^{f(n)}$

   d) $f(n+1) = f(n)^2 + f(n) + 1$

2. Find $f(1), f(2), f(3)$, $f(4)$ and $f(5)$ if $f(n)$ is defined recursively by $f(0)=3$ and for $n = 0, 1, 2,...$

   a) $f(n+1) = -2f(n)$

   b) $f(n+1) = 3f(n) + 7$

   c) $f(n+1) = 3^{f(n)/3}$

   d) $f(n+1) = f(n)^2 - 2f(n) - 2$

3. Find $f(2), f(3)$, $f(4)$ and $f(5)$ if $f(n)$ is defined recursively by $f(0) = f(1) = 1$ and for $n = 1, 2,...$

   a) $f(n+1) = f(n) - f(n-1)$

   b) $f(n+1) = f(n)f(n-1)$

   c) $f(n+1) = f(n)^2 + f(n-1)^3$

   d) $f(n+1) = f(n) / f(n-1)$

4. Determine whether each of these proposed definitions is a valid recursive definition of a function f from the set of nonnegative integers to the set of integers. If f is well defined, fund a formula for $f(n)$ when n is nonnegative integer and prove that your formula is valid.

   a) $f(0) = 0,\ f(n) = 2f(n-2)\ \ for\ \ n \geq 1$

   b) $f(0) = 1,\ f(n) = -f(n-1)\ \ for\ \ n \geq 1$

   c) $f(0) = 1,\ f(n) = f(n-1) - 1\ \ for\ \ n \geq 1$

   d) $f(0) = 2,\ f(1) = 3,\ f(n) = f(n-1) - 1\ \ for\ \ n \geq 2$

   e) $f(0) = 1,\ f(1) = 2,\ f(n) = 2f(n-2)\ \ for\ \ n \geq 2$

   f) $f(0) = 1,\ f(1) = 0,\ f(2) = 2, f(n) = 2f(n-3)\ \ for\ \ n \geq 3$

   g) $f(0) = 0,\ f(1) = 1,\ f(n) = 2f(n+1)\ \ for\ \ n \geq 2$

   h) $f(0) = 0,\ f(1) = 1,\ f(n) = 2f(n-1)\ \ for\ \ n \geq 2$

   i) $f(0) = 2,\ f(n) = f(n-1)$ if n is odd and $n \geq 1$ and $f(n) = 2f(n-2)$ if n is even and $n \geq 2$

   j) $f(0) = 1,\ f(n) = 3f(n-1)$ if n is odd and $n \geq 1$ and $f(n) = 9f(n-2)$ if n is even and $n \geq 2$

5. Give a recursive definition of the sequence $\{a_n\}$, $n = 1, 2, 3,\ldots$ if

a) $a_n = 6n$

b) $a_n = 2n + 1$

c) $a_n = 10^n$

d) $a_n = 5$

e) $a_n = 4n - 2$

f) $a_n = 1 + (-1)^n$

g) $a_n = n(n+1)$

h) $a_n = n^2$

6. Prove that $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$ when n is a positive integer and f_n is the nth Fibonacci number.

7. Prove that $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$ when n is a positive integer and f_n is the nth Fibonacci number.

8. Give a recursive definition of
a) The set of odd positive integers
b) The set of positive integers powers of 3
c) The set of polynomial with integer coefficients
d) The set of even integers
e) The set of positive integers congruent to 2 modulo 3.
f) The set of positive integers not divisible by 5

9. Let S be the subset of the set of ordered pairs of integers defined recursively by
Basis step: $(0, 0) \in S$.
Recursive step: If $(a, b) \in S$, then $(a + 2, b + 3) \in S$ and $(a + 3, b + 2) \in S$

a) List the elements of S produced by the first five applications of the recursive definition.
b) Use strong induction on the number of applications of the recursive step of the definition to show that $5 | a + b$ when $(a, b) \in S$.
c) Use structural induction to show that $5 | a + b$ when $(a, b) \in S$.

10. Let S be the subset of the set of ordered pairs of integers defined recursively by
Basis step: $(0, 0) \in S$.
Recursive step: If $(a, b) \in S$, then $(a, b + 1) \in S$, $(a + 1, b + 1) \in S$ and $(a + 2, b + 1) \in S$

a) List the elements of S produced by the first five applications of the recursive definition.
b) Use strong induction on the number of applications of the recursive step of the definition to show that $a \leq 2b$ whenever $(a, b) \in S$.
c) Use structural induction to show that $a \leq 2b$ whenever $(a, b) \in S$.

Section 3.3 − **The Basics of Counting**

Basic Counting Principle

The Product Rule

A procedure can be broken down into a sequence of two tasks. There are n_1 ways to do the first task and n_2 ways to do the second task. Then there are $n_1 \cdot n_2$ ways to do the procedure

Example

How many bit strings of length seven are there?

Solution

    Since each of the seven bits is either a 0 or a 1, the answer is $2^7 = 128$.

Example

A new company with just two employees rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?

Solution

    The procedure of assigning offices to these 2 employees consists of assigning an office to one employee, which can be done in 12 ways, then assigning an office to the second different from the office assigned to the first, which can be done in 11 ways.

    By the product rule, there are $12 \cdot 11 = 132 \;\; ways$ to assign offices to these 2 employees.

Example

There are 32 microcomputers in a computer center. Each microcomputer has 24 ports. How many different ports to a computer in the center are there?

Solution

    $32 \cdot 24 = 768 \;\; ports$

Example

How many different license plates can be made if each plate contains a sequence of three uppercase English letters followed by three digits?

Solution

    By the product rule, there are $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 17{,}576{,}000$ different possible license plates.

Counting Functions

    26 choices for each letter   10 choices for each digit

Example

How many functions are there from a set with *m* elements to a set with *n* elements?

Solution

Since a function represents a choice of one of the *n* elements of the codomain for each of the *m* elements in the domain, the product rule tells us that there are $n \cdot n \cdots n = n^m$ such functions.

Counting One-to-One Functions

Example

How many one-to-one functions are there from a set with *m* elements to one with *n* elements?

Solution

Suppose the elements in the domain are a_1, a_2, ..., a_m. There are *n* ways to choose the value of a_1 and $n - 1$ ways to choose a_2, etc. The product rule tells us that there are

$n(n-1)(n-2) \cdots (n-m+1)$ such functions.

Counting Subsets of a Finite Set

Example

Use the product rule to show that the number of different subsets of a finite set *S* is $2^{|S|}$.

Solution

When the elements of S are listed in an arbitrary order, there is a one-to-one correspondence between subsets of *S* and bit strings of length |*S*|. When the *i*th element is in the subset, the bit string has a 1 in the *i*th position and a 0 otherwise. By the product rule, there are $2^{|S|}$ such bit strings, and therefore $2^{|S|}$ subsets.

Product Rule in Terms of Sets

* If A_1, A_2, ..., A_m are finite sets, then the number of elements in the Cartesian product of these sets is the product of the number of elements of each set.
* The task of choosing an element in the Cartesian product $A_1 \times A_2 \times \ldots \times A_m$ is done by choosing an element in A_1, an element in A_2, ...and an element in A_m.
* By the product rule, it follows that: $\left| A_1 \times A_2 \times \ldots \times A_m \right| = \left| A_1 \right| \cdot \left| A_2 \right| \cdot \cdots \cdot \left| A_m \right|$

Basic Counting Principles

Definition: *The Sum Rule*

If a task can be done either in one of n_1 ways or in one of n_2 ways to do the second task, where none of the set of n_1 ways is the same as any of the n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Example

The mathematics department must choose either a student or a faculty member as a representative for a university committee. How many choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student.

Solution

By the sum rule it follows that there are 37 + 83 = **120** possible ways to pick a representative.

Example

A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

Solution

Since no project is on more than one list, by the sum rule there are 23 + 15 + 19 = **57** ways to choose a project.

The Sum Rule in terms of sets

The sum rule can be phrased in terms of sets.

$|A \cup B| = |A| + |B|$ as long as A and B are disjoint sets.

Or more generally, $\left| A_1 \cup A_2 \cup \ldots \cup A_m \right| = \left| A_1 \right| + \left| A_2 \right| + \ldots + \left| A_m \right|$ when $A_i \cup A_j = \varnothing$ for all i, j.

Example

Suppose statement labels in a programming language can be either a single letter or a letter followed by a digit. Find the number of possible labels.

Solution

Use the product rule. $26 + 26 \cdot 10 = \textbf{286}$

Subtraction Rule

Definition

If a task can be done either in one of n_1 ways or in one of n_2 ways, then the total number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.

Also known as, the *principle of inclusion-exclusion*: $|A \cup B| = |A| + |B| - |A \cap B|$

Example

How many bit strings of length eight either start with a 1 bit or end with the two bits 00?

Solution

Use the subtraction rule.

- Number of bit strings of length eight that start with a 1 bit: $2^7 = 128$
- Number of bit strings of length eight that start with bits 00: $2^6 = 64$
- Number of bit strings of length eight that start with a 1 bit and end with bits 00 : $2^5 = 32$

Hence, the number is $128 + 64 - 32 = 160$.
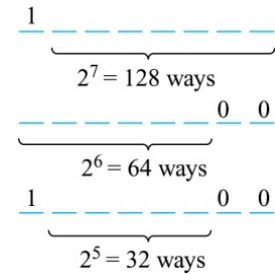
Example

A computer company receives 350 applications from computer graduates for a job planning a line of new Web servers. Suppose that 220 of these applicants majored in computer science, 147 majored in business, and 51 majored both in computer science and in business. How many of these applicants majored neither in computer science nor in business?

Solution

Let A: majored in computer science
B: majored in business

$$|A \cup B| = |A| + |B| - |A \cap B|$$
$$= 220 + 147 - 51$$
$$= 316$$

$350 - 316 = 34$

We conclude that 34 of the applicants majored neither in computer science nor in business

Division Rule

Definition

There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.

✓ Restated in terms of sets: If the finite set A is the union of n pairwise disjoint subsets each with d elements, then $n = |A|/d$.

✓ In terms of functions: If f is a function from A to B, where both are finite sets, and for every value $y \in$ B there are exactly d values $x \in A$ such that $f(x) = y$, then $|B| = |A|/d$.

Example

How many ways are there to seat four people around a circular table, where two seatings are considered the same when each person has the same left and right neighbor?

Solution

Number the seats around the table from 1 to 4 proceeding clockwise.

There are four ways to select the person for seat 1, 3 for seat 2, 2, for seat 3, and one way for seat 4. Thus there are 4! = 24 ways to order the four people.

But since two seatings are the same when each person has the same left and right neighbor, for every choice for seat 1, we get the same seating.

Therefore, by the division rule, there are 24/4 = 6 different seating arrangements.

Definition

We can solve many counting problems through the use of *tree diagrams*, where a branch represents a possible choice and the leaves represent possible outcomes.

Example

How many bit strings of length four do not have two consecutive 1s?
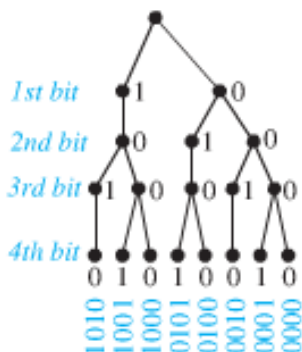
There are eight bits strings of length ***four*** without two consecutive 1s

Example

Suppose that "I Love Discrete Math" T-shirts come in five different sizes: S,M,L,XL, and XXL. Each size comes in four colors (white, red, green, and black), except XL, which comes only in red, green, and black, and XXL, which comes only in green and black. What is the minimum number of stores that the campus book store needs to stock to have one of each size and color available?

Solution
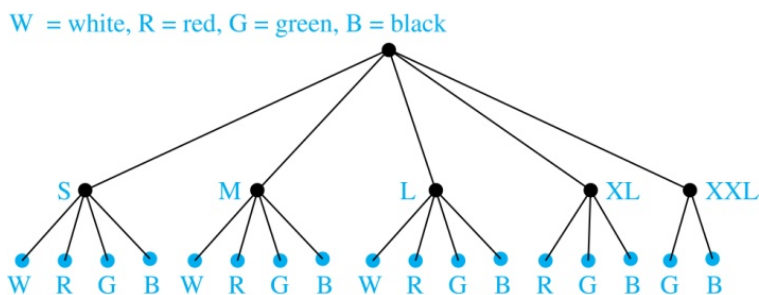
The store must stock **17** T-shirts.

Exercises   *Section* 3.3 − The Basics of Counting

1. There are 18 mathematics majors and 325 computer science majors at a college
    a) In how many ways can two representatives be picked so that one is a mathematics major and the other is a computer science major?
    b)   In how many ways can one representative be picked who either a mathematics major or a computer science major?

2. An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?

3. A multiple-choice test contains 10 questions. There are four possible answers for each question
    a) In how many ways can a student answer the questions on the test if the student answers every question?
    b)   In how many ways can a student answer the questions on the test if the student can leave answers blank?

4. A particular brand of shirt comes in 12 colors, has a male version and a female version, and comes in three sizes for each sex. How many different types of the shirts are made?

5. How many different three-letter initials can people have?

6. How many different three-letter initials with none of the letters repeated can people have?

7. How many different three-letter initials are there, that begin with an A?

8. How many bit strings are there of length eight?

9. How many bit strings of length ten both begin and end with a 1?

10. How many bit strings of length n, where n is a positive integer, start and end with 1s?

11. How many strings are there of lowercase letters of length four or less, not counting the empty string?

12. How many strings are there of four lowercase letters that have the letter x in them?

13. How many positive integers between 50 and 100

    a) Are divisible by 7? Which integers are these
    b) Are divisible by 11? Which integers are these
    c) Are divisible by 7 and 11? Which integers are these

14. How many positive integers less than 100

    a) Are divisible by 7?
    b) Are divisible by 7 but not by 11?
    c) Are divisible by both 7 and 11?
    d) Are divisible by either 7 or 11?
    e) Are divisible by exactly one of 7 and 11?
    f) Are divisible by neither 7 nor 11?

15. How many positive integers less than 1000

    g) Are divisible by 7?
    h) Are divisible by 7 but not by 11?
    i) Are divisible by both 7 and 11?
    j) Are divisible by either 7 or 11?
    k) Are divisible by exactly one of 7 and 11?
    l) Are divisible by neither 7 nor 11?
    m) have distinct digits?
    n) have distinct digits and are even?

16. A committee is formed consisting of one representative from each of the 50 states in the United States, where the representative from a state is either the governor or one of the two senators from that state. How many ways are there to form this committee?

17. How many license plates can be made using either three digits followed by three uppercase English letters or three uppercase English letters followed by three digits?

18. How many license plates can be made using either two uppercase English letters followed by four digits or two digits followed by four uppercase English letters?

19. How many license plates can be made using either three uppercase English letters followed by three digits or four uppercase English letters followed by two digits?

20. How many strings of eight English letter are there
    a) that contain no vowels, if letters can be repeated?
    b) that contain no vowels, if letters cannot be repeated?
    c) that start with a vowel, if letters can be repeated?
    d) that start with a vowel, if letters cannot be repeated?
    e) That contain at least one vowel, if letters can be repeated?
    f) That contain at least one vowel, if letters cannot be repeated?

21. How many ways are there to seat four of a group of ten people around a circular table where two seatings are considered the same when everyone has the same immediate left and immediate right neighbor?

22. In how many ways can a photographer at a wedding arrange 6 people in a row from a group of 10 people, where the bride and the groom are among these 10 people, if
    a) The bride must be in the picture?
    b) Both the bride and groom must be in the picture?
    c) Exactly one of the bride and the groom is in the picture?

23. How many different types of homes are available if a builder offers a choice of 6 basic plans, 3 roof styles, and 2 exterior finishes?

24. A menu offers a choice of 3 salads, 8 main dishes, and 7 desserts. How many different meals consisting of one salad, one main dish, and one dessert are possible?

25. A couple has narrowed down the choice of a name for their new baby to 4 first names and 5 middle names. How many different first- and middle-name arrangements are possible?

26. An automobile manufacturer produces 8 models, each available in 7 different exterior colors, with 4 different upholstery fabrics and 5 interior colors. How many varieties of automobile are available?

27. A biologist is attempting to classify 52,000 species of insects by assigning 3 initials to each species. Is it possible to classify all the species in this way? If not, how many initials should be used?

28. How many 4-letter code words are possible using the first 10 letters of the alphabet under:
   a) No letter can be repeated
   b) Letters can be repeated
   c) Adjacent can't be alike

29. How many 3 letters license plate without repeats

30. How many ways can 2 coins turn up heads, H, or tails, T – if the combined outcome (H, T) is to be distinguished from the outcome (T, H)?

31. How many 2-letter code words can be formed from the first 3 letters of the alphabet if no letter can be used more than once?

32. A coin is tossed with possible outcomes heads, H, or tails, T. Then a single die is tossed with possible outcomes 1, 2, 3, 4, 5, or 6. How many combined outcomes are there?

33. In how many ways can 3 coins turn up heads, H, or tails, T – if combined outcomes such as (H,T,H), (H, H, T), and (T, H, H) are to be considered different?

34. An entertainment guide recommends 6 restaurants and 3 plays that appeal to a couple.

   a) If the couple goes to dinner or to a play, how many selections are possible?
   b) If the couple goes to dinner and then to a play, how many combined selections are possible?

Section 3.4 − **Permutations and Combinations**

Permutation

A permutation of a set of distinct objects is an arrangement of the objects is a *specific Order Without* repetition. An ordered arrangement of *r* elements of a set is called an *r -permutation*.

Theorem

If *n* is a positive integer and *r* is an integer with $1 \le r \le n$, then there are

$$P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$$

r –permutation of a set with *n* distinct elements.

Proof

Use the product rule. The first element can be chosen in *n* ways. The second in *n* − 1 ways, and so on until there are $(n - (r - 1))$ ways to choose the last element.

Corollary

If *n* and *r* are integers with $1 \le r \le n$, then

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

Example

In mid 2007, eight candidates sought the Democratic nomination for president. In how many ways could voters rank their first, second, and third choices?

Solution

$P_{8,3} = 336$ 　　　　　　　　　　　　　　 *8 Math* → *Prob* → (nPr) 3

```
8 nPr 3
              336
■
```
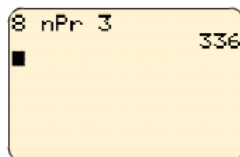
Example

How many ways are there to select a first-prize winner, a second prize winner, and a third-prize winner from 100 different people who have entered a contest?

Solution

$$P(100,3) = 100 \cdot 99 \cdot 98 = 970,200$$

Example

Suppose that there are eight runners in a race. The winner receives a gold medal, the second-place finisher receives a silver medal, and the third-place finisher receives a bronze medal. How many different ways are there to award these medals, if all possible outcomes of the race can occur and there are no ties?

Solution

There are: $P(8,3) = 8 \cdot 7 \cdot 6 = 336 \ \textit{ways}$

Example

Suppose that a saleswoman has to visit eight different cities. She must begin her trip in a specified city, but she can visit the other seven cities in any order she wishes. How many possible orders can the saleswoman use when visiting these cities?

Solution

The first city is chosen, and the rest are ordered arbitrarily. Hence the orders are:

$$7! = 5040$$

If she wants to find the tour with the shortest path that visits all the cities, she must consider 5040 paths!

Example

How many permutations of the letters *ABCDEFGH* contain the string *ABC* ?

Solution

We solve this problem by counting the permutations of six objects, *ABC, D, E, F, G,* and *H.*

$$6! = 720$$

Combination

Definition

An *r-combination* of elements of a set is an unordered selection of r elements from the set. Thus, an r-combination is simply a subset of the set with r elements

Combination of a set of n distinct objects taken r @ a time ***without*** repetition is an r element subset of the set of n objects.

The arrangement of the elements *doesn't matter*.

$$C_{n,r} = \binom{n}{r} = \frac{P_{n,r}}{r!} = \frac{n!}{r!(n-r)!}$$

n Math $\rightarrow$ Prob $\rightarrow$ $3(nCr)$ r

Example

Let S be the set $\{a, b, c, d\}$. Then $\{a, c, d\}$ is a 3-combination from S. It is the same as $\{d, c, a\}$ since the order listed does not matter.

Solution

$C(4,2) = 6$ because the 2-combinations of $\{a, b, c, d\}$ are the six subsets $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$, and $\{c, d\}$.

Theorem

The number of *r*-combinations of a set with n elements, where $n \geq r \geq 0$, equals

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

Proof

By the product rule $P(n, r) = C(n, r) \cdot P(r, r)$. Therefore,

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

Example

How many poker hands of five cards can be dealt from a standard deck of 52 cards? Also, how many ways are there to select 47 cards from a deck of 52 cards?

Solution

Since the order in which the cards are dealt does not matter, the number of five card hands is:

$$C(52, 5) = \frac{52!}{5!(52-5)!} = 2,598,960$$

168

Corollary

Let n and r be nonnegative integers with $r \le n$. Then $C(n, r) = C(n, n - r)$.

Proof

From Theorem 2, it follows that $C(n, r) = \dfrac{n!}{r!(n-r)!}$

and $C(n, n-r) = \dfrac{n!}{(n-r)!\left[n-(n-r)!\right]} = \dfrac{n!}{(n-r)!r!}$

Hence, $C(n, r) = C(n, n - r)$.

Definition

A *combinatorial proof* of an identity is a proof that uses one of the following methods.

➢ A *double counting proof* uses counting arguments to prove that both sides of an identity count the same objects, but in different ways.
➢ A *bijective proof* shows that there is a bijection between the sets of objects counted by the two sides of the identity.

Example

How many ways are there to select five players from a 10-member tennis team to make a trip to a match at another school?

Solution

The number of combinations is $C(10, 5) = \dfrac{10!}{5!(10-5)!} = 252$

Example

A group of 30 people have been trained as astronauts to go on the first mission to Mars. How many ways are there to select a crew of six people to go on this mission?

Solution

The number of possible crews is $C(30, 6) = \dfrac{30!}{6!24!} = 593,775$

Example

How many bits strings of length n contain exactly r 1s?

Solution

The positions of r 1s in a bit string of length n form an r-combination of the set $\{1,2,3,\ldots,n\}$. There are $C(n, r)$.

169

Example

Suppose that there are 9 faculty members in the mathematics department and 11 in the computer science department. How many ways are there to select a committee to develop a discrete mathematics course at a school if the committee is to consist of three faculty member from the mathematics department and four from the computer science department?

Solution

$$C(9,\ 3) \cdot C(11,\ 4) = \frac{9!}{3!6!} \cdot \frac{11!}{4!7!}$$

$$= 27,720$$

Exercises   *Section* **3.4 – Permutations and Combinations**

1. Decide whether the situation involves *permutations* or *combinations*
   a) A batting order for 9 players for a baseball game
   b) An arrangement of 8 people for a picture
   c) A committee of 7 delegates chosen from a class of 30 students to bring a petition to the administration
   d) A selection of a chairman and a secretary from a committee of 14 people
   e) A sample of 5 items taken from 71 items on an assembly line
   f) A blend of 3 spices taken from 7 spices on a spice rack
   g) From the 7 male and 10 female sales representatives for an insurance company, team of 8 will be selected to attend a national conference on insurance fraud.
   h) Marbles are being drawn without replacement from a bag containing 15 marbles.
   i) The new university president named 3 new officers a vice-president of finance, a vice-president of academic affairs, and a vice-president of student affairs.
   j) A student checked out 4 novels from the library to read over the holiday.
   k) A father ordered an ice cream cone (chocolate, vanilla, or strawberry) for each of his 4 children.

2. How many different permutations are the of the set $\{a, b, c, d, e, f, g\}$?

3. How many permutations of $\{a, b, c, d, e, f, g\}$ end with a?

4. Find the number of 5-permutations of a set with nine elements

5. In how many different orders can five runners finish a race if no ties are allowed?

6. A coin flipped eight times where each flip comes up either heads or tails. How many possible outcomes
   a) Are there in total?
   b) Contain exactly three heads?
   c) Contain at least three heads?
   d) Contain the same number of heads and tails?

7. A coin flipped 10 times where each flip comes up either heads or tails. How many possible outcomes
   a) Are there in total?
   b) Contain exactly two heads?
   c) Contain at least three heads?
   d) Contain the same number of heads and tails?

8. How many bit strings of length 12 contain
   a) Exactly three 1s?
   b) At most three 1s?
   c) At least three 1s?
   d) An equal number of 0s and 1s?

9. A group contains *n* men and *n* women. How many ways are there to arrange these people in a row if the men and women alternate?

10. In how many ways can a set of two positive integers less than 100 be chosen?

11. In how many ways can a set of five letters be selected from the English alphabet?

12. How many subsets with an odd number of elements does a set with 10 elements have?

13. How many subsets with more than two elements does a set with 100 elements have?

14. How many ways are there for eight men and five women to stand in a line so that no two women stand next to each other?

15. How many ways are there for six men and 10 women to stand in a line so that no two men stand next to each other?

16. A professor writes 40 discrete mathematics true/false questions. Of the statements in these questions. 17 are true. If the questions can be positioned in any order, how many different answer keys are possible?

17. Thirteen people on a softball team show up for a game.
    a) How many ways are there to choose 10 players to take the field?
    b) How many ways are there to assign the 10 positions by selecting players from the 13 people who show up?
    c) Of the 13 people who show up, there are three women. How many ways are there to choose 10 players to take the field if at least one of these players must be a woman?

18. A club has 25 members
    a) How many ways are there to choose four members of the club to serve on an executive committee?
    b) How many ways are there to choose a president, vice president, secretary, and treasurer of the club, where no person can hold more than one office?

19. How many 4-permutations of the positive integers not exceeding 100 contain three consecutive integers, k, $k + 1$, $k + 2$, in the order
    a) Where these consecutive integers can perhaps be separated by other integers in the permutation?
    b) Where they are in consecutive positions in the permutation?

20. The English alphabet contains 21 constants and five vowels. How many strings of six lowercase letters of the English alphabet contain
    a) Exactly one vowel?
    b) Exactly two vowels?
    c) At least one vowel?
    d) At least two vowels?

21. Suppose that a department contains 10 men and 15 women. How many ways are there to form a committee with six members if it must have
    a) The same number of men and women?
    b) More women than men?

22. How many bit strings contain exactly eight 0s and 10 1s if every 0 must be immediately followed by a 1?

23. How many bit strings contain exactly five 0s and 14 1s if every 0 must be immediately followed by two 1s?

24. A concert to raise money for an economics prize is to consist of 5 works; 2 overtures, 2 sonatas, and a piano concerto.
    a) In how many ways can the program be arranged?
    b) In how many ways can the program be arranged if an overture must come first?

25. A zydeco band from Louisiana will play 5 traditional and 3 original Cajun compositions at a concert. In how many ways can they arrange the program if
    a) The begin with a traditional piece?
    b) An original piece will be played last?

26. In an election with 3 candidates for one office and 6 candidates for another office, how many different ballots may be printed?

27. A business school gives courses in typing, shorthand, transcription, business English, technical writing, and accounting. In how many ways can a student arrange a schedule if 3 courses are taken? assume that the order in which courses are schedules matters.

28. If your college offers 400 courses, 25 of which are in mathematics, and your counselor arranges your schedule of 4 courses by random selection, how many schedules are possible that do not include a math course? Assume that the order in which courses are scheduled matters.

29. A baseball team has 19 players. How many 9-player batting orders are possible?

30. A chapter of union Local 715 has 35 members. In how many different ways can the chapter select a president, a vice-president, a treasurer, and a secretary?

31. An economics club has 31 members.
    a) If a committee of 4 is to be selected, in how many ways can the selection be made?
    b) In how many ways can a committee of at least 1 and at most 3 be selected?

32. In a club with 9 male and 11 female members, how many 5-member committees can be chosen that have
    a) All men?
    b) All women?
    c) 3 men and 2 women?

33. In a club with 9 male and 11 female members, how many 5-member committees can be selected that have

    a) At least 4 women?

    b) No more than 2 men?

34. In a game of musical chairs, 12 children will sit in 11 chairs arranged in a row (one will be left out). In how many ways can this happen, if we count rearrangements of the children in the chairs as different outcomes?

35. A group of 3 students is to be selected from a group of 14 students to take part in a class in cell biology.

    a) In how many ways can this be done?

    b) In how many ways can the group who will not take part be chosen?

36. Marbles are being drawn without replacement from a bag containing 16 marbles.

    a) How many samples of 2 marbles can be drawn?

    b) How many samples of 2 marbles can be drawn?

    c) If the bag contains 3 yellow, 4 white, and 9 blue marbles, how many samples of 2 marbles can be drawn in which both marbles are blue?

37. A bag contains 5 black, 1 red, and 3 yellow jelly beans; you take 3 at random. How many samples are possible in which the jelly beans are

    a) All black?

    b) All red?

    c) All yellow?

    d) 2 black and 1 red?

    e) 2 black and 1 yellow?

    f) 2 yellow and 1 black?

    g) 2 red and 1 yellow?

Section 3.5 – Applications of Recurrence Relations

Modeling with Recurrence Relations

Definition

A *recurrence relation* for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely, a_0, a_1, …, a_{n-1}, for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer

Example

A young pair of rabbits (one of each gender) is placed on an island. A pair of rabbits does not breed until they are 2 months old. After they are 2 months old, each pair of rabbits produces another pair each month. Find a recurrence relation for the number of pairs of rabbits on the island after n months, assuming that rabbits never die.

Reproducing pairs (at least two months old)	Young pairs (less than two months old)	Month	Reproducing pairs	Young pairs	Total pairs
		1	0	1	1
		2	0	1	1
		3	1	1	2
		4	1	2	3
		5	2	3	5
		6	3	5	8

Modeling the Population Growth of Rabbits on an Island

Solution

Let f_n be the number of pairs of rabbits after n months.

- There are is $f_1 = 1$ pairs of rabbits on the island at the end of the first month.
- We also have $f_2 = 1$ because the pair does not breed during the first month.
- To find the number of pairs on the island after n months, add the number on the island after the previous month, f_{n-1}, and the number of newborn pairs, which equals f_{n-2}, because each newborn pair comes from a pair at least two months old.

Consequently the sequence $\{f_n\}$ satisfies the recurrence relation $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$ with the initial conditions $f_1 = 1$ and $f_2 = 1$.

The number of pairs of rabbits on the island after n months is given by the nth Fibonacci number.

The Tower of Hanoi

In the late nineteenth century, the French mathematician Édouard Lucas invented a puzzle, called the Tower of Hanoi, consisting of three pegs on a board with disks of different sizes. Initially all of the disks are on the first peg in order of size, with the largest on the bottom

Rules: You are allowed to move the disks one at a time from one peg to another as long as a larger disk is never placed on a smaller.

Goal: Using allowable moves, end up with all the disks on the second peg in order of size with largest on the bottom.

Peg 1   Peg 2   Peg 3
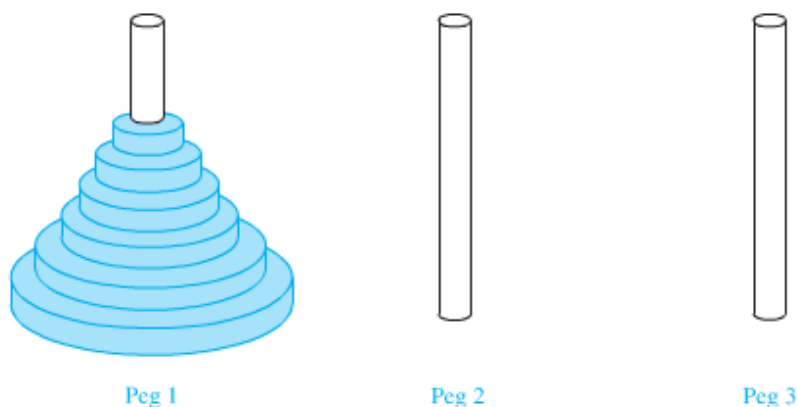
Solution

Let $\{H_n\}$ denote the number of moves needed to solve the Tower of Hanoi Puzzle with n disks. Set up a recurrence relation for the sequence $\{H_n\}$. Begin with n disks on peg 1. We can transfer the top $n-1$ disks, following the rules of the puzzle, to peg 3 using H_{n-1} moves.

First, we use 1 move to transfer the largest disk to the second peg. Then we transfer the $n-1$ disks from peg 3 to peg 2 using H_{n-1} additional moves. This cannot be done in fewer steps. Hence,

$$H_n = 2H_{n-1} + 1$$

The initial condition is $H_1 = 1$ since a single disk can be transferred from peg 1 to peg 2 in one move.

Peg 1   Peg 2   Peg 3
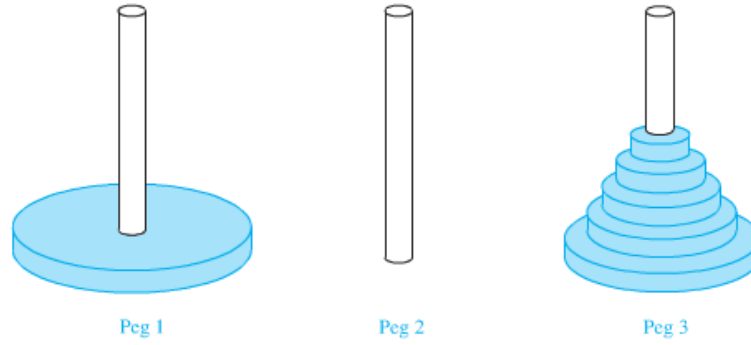
We can use an iterative approach to solve this recurrence relation by repeatedly expressing H_n in terms of the previous terms of the sequence.

$$
\begin{aligned}
H_n &= 2H_{n-1} + 1 \\
&= 2\left(2H_{n-2} + 1\right) + 1 \\
&= 2^2 H_{n-2} + 2 + 1 \\
&= 2^2\left(2H_{n-3} + 1\right) + 2 + 1 \\
&= 2^3 H_{n-3} + 2^2 + 2 + 1 \\
&\ \ \vdots \qquad \vdots \\
&= 2^{n-1} H_1 + 2^{n-2} + 2^{n-3} + \cdots + 2 + 1 \qquad \textit{since } H_1 = 1 \\
&= 2^{n-1} + 2^{n-2} + 2^{n-3} + \cdots + 2 + 1 \\
&\qquad\qquad\qquad \textit{Using the formula for the sum of the terms of geometric series} \\
&= 2^n - 1
\end{aligned}
$$

There was a myth created with the puzzle. Monks in a tower in Hanoi are transferring 64 gold disks from one peg to another following the rules of the puzzle. They move one disk each day. When the puzzle is finished, the world will end.

Using this formula for the 64 gold disks of the myth,

$2^{64} - 1 = 18{,}446{,}\ 744{,}073{,}\ 709{,}551{,}615$ days are needed to solve the puzzle, which is more than 500 billion years.

Reve's puzzle (proposed in 1907 by Henry Dudeney) is similar but has 4 pegs. There is a well-known unsettled conjecture for the minimum number of moves needed to solve this puzzle.

Example

Find a recurrence relation and give initial conditions for the number of bit strings of length n without two consecutive 0s. How many such bit strings are there of length five?

Solution

Let a_n denote the number of bit strings of length n without two consecutive 0s. To obtain a recurrence relation for $\{a_n\}$ note that the number of bit strings of length n that do not have two consecutive 0s is the number of bit strings ending with a 0 plus the number of such bit strings ending with a 1.

Now assume that $n \geq 3$.

The bit strings of length n ending with 1 without two consecutive 0s are the bit strings of length $n-1$ with no two consecutive 0s with a 1 at the end. Hence, there are a_{n-1} such bit strings.

The bit strings of length n ending with 0 without two consecutive 0s are the bit strings of length $n-2$ with no two consecutive 0s with 10 at the end. Hence, there are a_{n-2} such bit strings.

We conclude that $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$.

The initial conditions are:

$a_1 = 2$, since both the bit strings 0 and 1 do not have consecutive 0s.

$a_2 = 3$, since the bit strings 01, 10, and 11 do not have consecutive 0s, while 00 does.

To obtain a_5, we use the recurrence relation three times to find that:

$a_3 = a_2 + a_1 = 3 + 2 = 5$

$a_4 = a_3 + a_2 = 5 + 3 = 8$

$a_5 = a_4 + a_3 = 8 + 5 = 13$

Number of bit strings
of length n with no
two consecutive 0s:

End with a 1: | Any bit string of length $n-1$ with no two consecutive 0s | 1 a_{n-1}

End with a 0: | Any bit string of length $n-2$ with no two consecutive 0s | 1 0 $\underline{a_{n-2}}$

Total: $a_n = a_{n-1} + a_{n-2}$

Example

A computer system considers a string of decimal digits a valid codeword if it contains an even number of 0 digits. For instance, 1230407869 is valid, whereas 1230407869 is not valid. Let a_0 be the number of valid n-digit codewords. Find a recurrence relation for a_n.

Solution

Note that $a_1 = 9$ because there are 10 one-digit strings, and only one, namely the string 0, is not valid.

A recurrence relation can be derived for this sequence by considering how a valid n-digit string can be obtained from strings of $n - 1$ digits. There are two ways to form a valid string with n digits from a string with one fewer digit.

1. A valid string with n digits can be obtained by appending a valid string of $n - 1$ digits with a digit other than 0. This appending can be done in 9 ways. Hence, a valid string with n digits can be formed in this manner in $9a_{n-1}$ ways.

2. A valid string with n digits can be obtained by appending a 0 to a string of length $n - 1$ that is not valid. The number of ways that this can be done equals the number of invalid $(n - 1)$-digit strings. Because there are 10^{n-1} strings of length $n - 1$, and a_{n-1} are valid, there are $10^{n-1} - a_{n-1}$ valid n–digit strings obtained by appending an invalid string of length $n - 1$ with a 0.

   Because all valid strings of length n are produced in one of these two ways, it follows that there are

   $$a_n = 9a_{n-1} + \left(10^{n-1} - a_{n-1}\right)$$

   $$= 8a_{n-1} + 10^{n-1}$$

   Valid strings of length n.

Example

Find a recurrence relation for C_n, the number of ways to parenthesize the product of $n + 1$ numbers, $x_0 \cdot x_1 \cdot x_2 \cdots x_n$, to specify the order of multiplication. For example, $C_3 = 5$, since all the possible ways to parenthesize 4 numbers are

$$\left(\left(x_0 \cdot x_1\right) \cdot x_2\right) \cdot x_3 \qquad \left(x_0 \cdot \left(x_1 \cdot x_2\right)\right) \cdot x_3 \qquad \left(x_0 \cdot x_1\right) \cdot \left(x_2 \cdot x_3\right)$$

$$x_0 \cdot \left(\left(x_1 \cdot x_2\right) \cdot x_3\right) \qquad x_0 \cdot \left(x_1 \cdot \left(x_2 \cdot x_3\right)\right)$$

Solution

Note that however parentheses are inserted in $x_0 \cdot x_1 \cdot x_2 \cdots x_n$, one "$\cdot$" operator remains outside all parentheses. This final operator appears between two of the $n + 1$ numbers, say x_k and x_{k+1}. Since there are C_k ways to insert parentheses in the product $x_0 \cdot x_1 \cdot x_2 \cdots x_k$ and C_{n-k-1} ways to insert parentheses in the product $x_{k+1} \cdot x_{k+2} \cdots x_n$, we have

$$C_n = C_0 C_{n-1} + C_1 C_{n-2} + \cdots + C_{n-2} C_1 + C_{n-1} C_0$$

$$= \sum_{k=0}^{n-1} C_k C_{n-k-1}$$

The initial conditions are $C_0 = C_1 = 1$.

Exercises   *Section* 3.5 − **Applications of Recurrence Relations**

1.   *a*) Find a recurrence relation for the number of permutation of a set with n elements
       b) Use the recurrence relation to find the number of permutations of a set with n elements using iteration.

2.   A vending machine dispensing books of stamps accepts only one-dollar coins, $1 bills, and $5 bills.
       a) Find a recurrence relation for the number of ways to deposit n dollars in the vending machine, where the order in which the coins and bills are deposited matter.
       b) What are the initial conditions?
       c) How many ways are there to deposit $10 for a book of stamps?

3.   *a*) Find a recurrence relation for the number of bit strings of length n that contain three consecutive 0s.
       b) What are the initial conditions?
       c) How many bit strings of length seven contain three consecutive 0s?

4.   *a*) Find a recurrence relation for the number of bit strings of length n that do not contain three consecutive 0s.
       b) What are the initial conditions?
       c) How many bit strings of length seven do not contain three consecutive 0s?

5.   *a*) Find a recurrence relation for the number of ways to climb n stairs if the person climbing the stairs can take one stair or two stairs at a time.
       b) What are the initial conditions?
       c) In how many can this person climb a flight of eight stairs

Section 3.6 – Solving Linear Recurrence Relations

Definition

A *linear homogeneous recurrence relation of degree k with constant coefficients* is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

Where $c_1, c_2, \cdots, c_k$ are real numbers, and $c_k \neq 0$

✓ It is *linear* because the right-hand side is a sum of the previous terms of the sequence each multiplied by a function of *n*.

✓ It is *homogeneous* because no terms occur that are not multiples of the $a_j s$. Each coefficient is a constant.

✓ The *degree* is *k* because a_n is expressed in terms of the previous *k* terms of the sequence.

Solving Linear Homogeneous Recurrence Relations

The basic approach is to look for solutions of the form $a_n = r^n$, where *r* is a constant.

Note that $a_n = r^n$ is a solution to the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ if and only if $r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k}$.

Algebraic manipulation yields the *characteristic equation*:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_{k-1} r^{n-k} = 0$$

The sequence $\{a_n\}$ with $a_n = r^n$ is a solution if and only if *r* is a solution to the characteristic equation.

The solutions to the characteristic equation are called the *characteristic roots* of the recurrence relation. The roots are used to give an explicit formula for all the solutions of the recurrence relation.

Theorem

Let c_1 and c_2 be real numbers. Suppose that $r^2 - c_1 r - c_2 = 0$ has two distinct roots r_1 and r_2. Then the sequence $\{a_n\}$ is a solution to the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ if and only if for $n = 0$, 1, 2, ... , where α_1 and α_2 are constants.

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

This shows that the sequence $\{a_n\}$ with $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ is a solution of the recurrence relation.

Example

What is the solution to the recurrence relation $a_n = a_{n-1} + 2a_{n-2}$ with $a_0 = 2$ and $a_1 = 7$?

Solution

The characteristic equation is $r^2 - r - 2 = 0$.

Its roots are $r = 2$ and $r = -1$. Therefore, $\{a_n\}$ is a solution to the recurrence relation if and only if $a_n = \alpha_1 2^n + \alpha_2 (-1)^n$, for some constants α_1 and α_2.

To find the constants α_1 and α_2, note that

$$a_0 = \alpha_1 + \alpha_2 = 2$$
$$a_1 = 2\alpha_1 - \alpha_2 = 7.$$

Solving these equations, we find that $\alpha_1 = 3$ and $\alpha_2 = -1$.

Hence, the solution is the sequence $\{a_n\}$ with $\underline{a_n = 3 \cdot 2^n - (-1)^n}$

An Explicit Formula for the Fibonacci Numbers

Example

We can use Theorem to find an explicit formula for the Fibonacci numbers. The sequence of Fibonacci numbers satisfies the recurrence relation $f_n = f_{n-1} + f_{n-2}$ with the initial conditions: $f_0 = 0$ and $f_1 = 1$.

Solution

The roots of the characteristic equation $r^2 - r - 1 = 0$ are $r_{1,2} = \dfrac{1 \pm \sqrt{5}}{2}$

Therefore, from the theorem it follows that the Fibonacci numbers are given by

$$f_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Using the initial conditions $f_0 = 0$ and $f_1 = 1$, we have

$$f_0 = \alpha_1 + \alpha_2 = 0$$
$$f_1 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right) + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right) = 1$$

The solution to these simultaneous equations for α_1 and α_2 is $\alpha_1 = \dfrac{1}{\sqrt{5}}$ and $\alpha_2 = -\dfrac{1}{\sqrt{5}}$

Consequently, the Fibonacci numbers are given by

$$\underline{f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n}$$

Theorem

Let c_1 and c_2 be real numbers with $c_2 \neq 0$. Suppose that $r^2 - c_1 r - c_2 = 0$ has one repeated root r_0.

Then the sequence $\{a_n\}$ is a solution to the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ iff

$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$ for $n = 0,1,2,\ldots$, where α_1 and α_2 are constants.

Example

What is the solution to the recurrence relation $a_n = 6a_{n-1} - 9a_{n-2}$ with $a_0 = 1$ and $a_1 = 6$?

Solution

The characteristic equation is $r^2 - 6r + 9 = 0$.

The only root is $r = 3$. Therefore, $\{a_n\}$ is a solution to the recurrence relation if and only if

$a_n = \alpha_1 3^n + \alpha_2 n (3)^n$ where α_1 and α_2 are constants.

$$\begin{cases} a_0 = 1 = \alpha_1 \\ a_1 = 6 = \alpha_1 \cdot 3 + \alpha_2 \cdot 3 \end{cases} \rightarrow \quad \alpha_1 = 1 \ and \ \alpha_2 = 1$$

Hence, $a_n = 3^n + n(3)^n \ \underline{= (n+1)3^n}$.

Theorem

Let $c_1, c_2, \ldots, c_k$ be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$$

has k distinct roots $r_1, r_2, \ldots, r_k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

$$iff \quad a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

for $n = 0, 1, 2, \ldots$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are constants.

Example

Find the solution to the recurrence relation $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ with $a_0 = 2$, $a_1 = 5$ and $a_2 = 15$?

Solution

The characteristic equation is $r^3 - 6r^2 + 11r - 6 = 0$.

The characteristic roots are $r = 1, \ 2, \ 3$.

The solutions to the recurrence relation are of the form $a_n = \alpha_1 \cdot 1^n + \alpha_2 \cdot 2^n + \alpha_2 \cdot 3^n$ where α_1, α_2 and α_3 are constants.

$$\begin{cases} a_0 = 2 = \alpha_1 + \alpha_2 + \alpha_3 \\ a_1 = 5 = \alpha_1 + \alpha_2 \cdot 2 + \alpha_3 \cdot 3 \\ a_2 = 15 = \alpha_1 + \alpha_2 \cdot 4 + \alpha_3 \cdot 9 \end{cases} \rightarrow \alpha_1 = 1 \ \alpha_2 = -1 \ \text{and} \ \alpha_3 = 2$$

$$\underline{a_n = 1 - 2^n + 2 \cdot 3^n}$$

Theorem

Let c_1, c_2, ..., c_k be real numbers. Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$$

has t distinct roots r_1, r_2, ..., r_k with multiplicities m_1, m_2, ..., m_k respectively so that $m_i \geq 1$ for $i = 0, 1, 2, ..., t$ and $m_1 + m_2 + \cdots + m_t = k$ Then a sequence $\{a_n\}$ is a solution of the recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

iff
$$a_n = \left(\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1} \cdot n^{m_1-1}\right) r_1^n$$
$$+ \left(\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{2,m_2-1} \cdot n^{m_2-1}\right) r_2^n$$
$$+ \cdots + \left(\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1} \cdot n^{m_t-1}\right) r_t^n$$

for $n = 0, 1, 2, \ldots$, where $\alpha_{i,j}$ are constants for $1 \leq i \leq t$ and $0 \leq j \leq m_{i-1}$.

Example

Suppose that the roots of the characteristic equation of a linear homogeneous recurrence relation are 2, 2, 2, 5, 5, and 9 (that is, there are three roots, the root 2 with multiplicity three, the root 5 with multiplicity two, and the root 9 with multiplicity one). What is the form of the general solution?

Solution

The general form of the solution is:

$$\left(\alpha_{1,0} + \alpha_{1,1} n + \alpha_{1,2} \cdot n^2\right) 2^n + \left(\alpha_{2,0} + \alpha_{2,1} n\right) 5^n + \alpha_{3,0} 9^n$$

Example

Find the solution to the recurrence relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$

with $a_0 = 1$, $a_1 = -2$ and $a_2 = -1$?

Solution

The characteristic equation is $r^3 + 3r^2 + 3r + 1 = 0$.

The characteristic root is a single root $r = -1$ of multiplicity three.

The solutions to the recurrence relation are of the form

$a_n = \left(\alpha_{1,0} + \alpha_{1,1} \cdot n + \alpha_{1,2} \cdot n^2\right) \cdot (-1)^n$ where α_1, α_2 and α_3 are constants.

$$\begin{cases} a_0 = 1 = \alpha_{1,0} \\ a_1 = -2 = -\alpha_{1,0} - \alpha_{1,1} - \alpha_{1,2} \\ a_2 = -1 = \alpha_{1,0} + 2\alpha_{1,1} + 4\alpha_{1,2} \end{cases} \rightarrow \alpha_{1,0} = 1 \quad \alpha_{1,1} = 3 \quad and \quad \alpha_{1,2} = -2$$

$$\underline{a_n = \left(1 + 3n - 2n^2\right) \cdot (-1)^n}$$

Linear Nonhomogeneous Recurrence Relations with Constant Coefficients

Definition

A *linear nonhomogeneous recurrence relation with constant coefficients* is a recurrence relation of the form:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)$$

where c_1, c_2, ..., c_k are real numbers, and $F(n)$ is a function not identically zero depending only on n.

The recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

is called the **associated homogeneous recurrence relation**.

➢ The following are linear nonhomogeneous recurrence relations with constant coefficients:

$$a_n = a_{n-1} + 2^n$$

$$a_n = a_{n-1} + a_{n-2} + n^2 + n + 1$$

$$a_n = 3a_{n-1} + n3^n$$

$$a_n = a_{n-1} + a_{n-2} + a_{n-3} + n!$$

where the following are the associated linear homogeneous recurrence relations, respectively:

$$a_n = a_{n-1}$$

$$a_n = a_{n-1} + a_{n-2}$$
$$a_n = 3a_{n-1}$$
$$a_n = a_{n-1} + a_{n-2} + a_{n-3}$$

Theorem

If $\left\{a_n^{(p)}\right\}$ is a particular solution of the nonhomogeneous linear recurrence relation with constant

coefficients

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n)$$

then every solution is of the form $\left\{a_n^{(p)} + a_n^{(k)}\right\}$, where $\left\{a_n^{(k)}\right\}$ is a solution of the associated

homogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

Example

Find all solutions of the recurrence relation $a_n = 3a_{n-1} + 2n$. What is the solution with $a_1 = 3$?

Solution

The associated linear homogeneous equation is $a_n = 3a_{n-1}$.

Its solutions are $a_n^{(k)} = \alpha 3^n$, where α is a constant.

Because $F(n) = 2n$ is a polynomial in n of degree one.

Let the linear function $p_n = cn + d$ be such a solution

Then $a_n = 3a_{n-1} + 2n$ becomes $cn + d = 3(c(n-1) + d) + 2n$.

$\Rightarrow (2 + 2c)n + (2d - 3c) = 0.$

It follows that $cn + d$ is a solution if and only if $2 + 2c = 0$ and $2d - 3c = 0$.

Therefore, $cn + d$ is a solution if and only if $c = -1$ and $d = -3/2$.

Consequently, $a_n^{(p)} = -n - \dfrac{3}{2}$ is a particular solution.

By Theorem, all solutions are of the form $a_n = a_n^{(p)} + a_n^{(k)} = -n - \dfrac{3}{2} + \alpha 3^n$, where α is a constant.

$a_1 = 3$, let $n = 1$. Then $3 = -1 - \dfrac{3}{2} + 3\alpha \;\to\; 3\alpha = 3 + \dfrac{5}{2} \Rightarrow \boxed{\alpha = \dfrac{11}{6}}$.

Hence, the solution is $\underline{a_n = -n - \dfrac{3}{2} + \dfrac{11}{6} 3^n}$.

Example

Find all solutions of the recurrence relation $a_n = 5a_{n-1} - 6a_{n-2} + 7^n$.

Solution

The linear nonhomogeneous equation is $a_n = 5a_{n-1} - 6a_{n-2}$.

Its solutions are $a_n^{(k)} = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n$, where α_1 and α_2 are constants

The trial solution is $a_n^{(p)} = C \cdot 7^n$

$$C \cdot 7^n = 5C \cdot 7^{n-1} - 6C \cdot 7^{n-2} + 7^n$$

$$C \cdot 7^n = 7^{n-2}(35C - 6C + 49)$$

$$C \cdot 7^2 = 29C + 49$$
$$49C - 29C = 49$$
$$20C = 49$$
$$C = \frac{49}{20}$$

Hence, $a_n^{(p)} = \frac{49}{20} \cdot 7^n$

Hence, the solution is $\underline{a_n = \alpha_1 \cdot 3^n + \alpha_2 \cdot 2^n + \frac{49}{20} \cdot 7^n}$.

Exercises   *Section* 3.6 − **Solving Linear Recurrence Relations**

1.   Determine which of these are linear homogeneous recurrence relations with constant coefficients. Also find the degree of those that are

     a) $a_n = 3a_{n-1} + 4a_{n-2} + 5a_{n-3}$

     b) $a_n = 2na_{n-1} + a_{n-2}$

     c) $a_n = a_{n-1} + a_{n-4}$

     d) $a_n = a_{n-1} + 2$

     e) $a_n = a_{n-1}^2 + a_{n-2}$

     f) $a_n = a_{n-2}$

     g) $a_n = a_{n-1} + n$

     h) $a_n = 3a_{n-2}$

     i) $a_n = 3$

     j) $a_n = a_{n-1}^2$

     k) $a_n = a_{n-1} + 2a_{n-3}$

     l) $a_n = \dfrac{a_{n-1}}{n}$

2.   Solve these recurrence relations together with the initial conditions given

     a) $a_n = 2a_{n-1}$ for $n \geq 1,\ a_0 = 3$

     b) $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2,\ a_0 = 1,\ a_1 = 0$

     c) $a_n = 4a_{n-1} - 4a_{n-2}$ for $n \geq 2,\ a_0 = 6,\ a_1 = 8$

     d) $a_n = 4a_{n-2}$ for $n \geq 2,\ a_0 = 0,\ a_1 = 4$

     e) $a_n = \dfrac{a_{n-2}}{4}$ for $n \geq 2,\ a_0 = 1,\ a_1 = 0$

     f) $a_n = a_{n-1} + 6a_{n-2}$ for $n \geq 2,\ a_0 = 3,\ a_1 = 6$

     g) $a_n = 7a_{n-1} - 10a_{n-2}$ for $n \geq 2,\ a_0 = 2,\ a_1 = 1$

     h) $a_n = -6a_{n-1} - 9a_{n-2}$ for $n \geq 2,\ a_0 = 3,\ a_1 = -3$

     i) $a_{n+2} = -4a_{n-1} + 5a_n$ for $n \geq 0,\ a_0 = 2,\ a_1 = 8$

3.   How many different messages can be transmitted in *n* microseconds using three different signals if one signal requires 1 microsecond for transmittal, the other two signals require 2 microseconds each for transmittal, and a signal in a message is followed immediately by the next signal?

4. In how many ways can a $2 \times n$ rectangular checkerboard be tiled using 1×2 and 2×2 pieces?

5. Find the solution to $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$ *for* $n \geq 3$, $a_0 = 3$, $a_1 = 6$ *and* $a_2 = 0$

6. Find the solution to $a_n = 7a_{n-2} + 6a_{n-3}$ *with* $a_0 = 9$, $a_1 = 10$ *and* $a_2 = 32$

7. Find the solution to $a_n = 5a_{n-2} - 4a_{n-4}$ *with* $a_0 = 3$, $a_1 = 2$, $a_2 = 6$ *and* $a_3 = 8$

8. Find the recurrence relation $a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3}$ *with* $a_0 = -5$, $a_1 = 4$ *and* $a_2 = 88$

9. Find the recurrence relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ *with* $a_0 = 5$, $a_1 = -9$ *and* $a_2 = 15$

10. Find the general form of the solutions of the recurrence relation $a_n = 8a_{n-2} - 16a_{n-4}$

11. What is the general form of the solutions of a linear homogeneous recurrence relation if its characteristic equation has roots 1, 1, 1, 1, –2, –2, –2, 3, 3, –4?

12. What is the general form of the solutions of a linear homogeneous recurrence relation if its characteristic equation has roots –1, –1, –1, 2, 2, 5, 5, 7?

Lecture Four

Section 4.1 – Relations and Their Properties

Definition

Let A and B be sets. A binary relation from A to B is a subset of $A \times B$

A binary relation from A to B is a set R of ordered pairs where the first element of each ordered pair comes from A and the second element comes from B. We use the notation $a\,R\,b$ to denote that $(a, b) \in R$ and $a \not R b$ to denote that $(a, b) \notin R$. Moreover, when (a, b) belongs to R, a is said to be related to b by R.

Example

Let $A = \{0, 1, 2\}$ and $B = \{a, b\}$. Then $\{(0, a), (0, b), (1, a), (2, b)\}$ is a relation from A to B.

This means, for instance, that $0\,R\,a$ but the $1 \not R b$.

Relations can be represented graphically, as shown below, using arrows to represent ordered pairs.
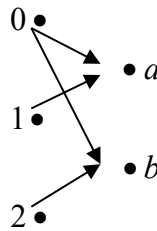
Another way to represent this relation is to use a table.

R	a	b
0	x	x
1	x	
2		x

Relations on a Set
Definition

A **relation** on a set A is a relation from A to A. and it's a subset of $A \times A$

Example

Let A = {1, 2, 3, 4} which ordered pairs are the relation $R = \{(a, b) \mid a \text{ divides } b\}$?

Solution

R = {(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)}
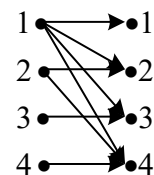
Example

Consider these relations on the set of integers:

$$R_1 = \{(a, b) \mid a \leq b\}$$
$$R_2 = \{(a, b) \mid a > b\}$$
$$R_3 = \{(a, b) \mid a = b \text{ or } a = -b\}$$
$$R_4 = \{(a, b) \mid a = b\}$$
$$R_5 = \{(a, b) \mid a = b + 1\}$$
$$R_6 = \{(a, b) \mid a + b \leq 3\}$$

Which of these relations contain each of the pairs $(1, 1)$, $(1, 2)$, $(2, 1)$, $(1, -1)$, and $(2, 2)$?

Solution

$(1, 1) \rightarrow R_1, R_3, R_4, \text{ and } R_6$

$(1, 2) \rightarrow R_1 \text{ and } R_6$

$(2, 1) \rightarrow R_2, R_5, \text{ and } R_6$

$(1, -1) \rightarrow R_2, R_3, \text{ and } R_6$

$(2, 2) \rightarrow R_1, R_3, \text{ and } R_4$

Example

How many relations are there on a set with n elements?

Solution

A relation on a set A is a subset of $A \times A$. Because $A \times A$ has n^2 elements when A has n elements, and a set with m elements has 2^m subsets, there are 2^{n^2} subset of $A \times A$.

Thus there are 2^{n^2} relations on a set with n elements.

Properties of Relations

Reflexive

Definition

A relation R on a set A is called ***reflexive*** if $(a, a) \in R$ for every element $a \in A$

Example

Consider the following relations on $\{1, 2, 3, 4\}$:

$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$

$R_2 = \{(1, 1), (1, 2), (2, 1)\}$

$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$

$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$

$R_6 = \{(3, 4)\}$

Which of these relations are ***reflexive***?

Solution

The relations R_3 and R_5 are reflexive because they contain all pairs of the form (a, a), namely, $(1, 1), (2, 2), (3, 3),$ and $(4, 4)$.

$R_1, R_2, R_4,$ *and* R_6 are not reflexive because $(3, 3)$ is not in any of these relations.

Example

Is the "divides" relation on the set of positive integers reflexive?

Solution

Because $a | a$ whenever a is a positive integer, the "divides" relation is reflexive.

(0 is doesn't divide 0)

Symmetric

Definition

A relation R on a set A is called **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.

$$\forall a \forall b \left((a, b) \in R \rightarrow (b, a) \in R \right)$$

A relation R on a set A such that for all $a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ is called **antisymmetric**.

$$\forall a \forall b \left(\left((a, b) \in R \wedge (b, a) \in R \right) \rightarrow (a = b) \right)$$

Example

Is the "divides" relation on the set of positive integers symmetric? Is it antisymmetric?

Solution

It is antisymmetric because $1 | 2$ bur $2 \nmid 1$

Example

Consider the following relations on $\{1, 2, 3, 4\}$:

$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$

$R_2 = \{(1, 1), (1, 2), (2, 1)\}$

$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$

$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$

$R_6 = \{(3, 4)\}$

Which of these relations are symmetric and which are antisymmetric?

Solution

The relations R_2 and R_3 are symmetric because in each case (b, a) belongs to the relation whenever (a, b) does. $(1, 2)$ *and* $(2, 1)$ in R_2 $(1, 2), (2, 1), (1, 4)$ *and* $(4, 1)$ in R_3.

The relations R_1, R_4, R_5 and R_6 are antisymmetric because for each relations there is no pair of elements a and b with $a \neq b$ such that both (a, b) and (b, a) belong to the relation.

Transitive

Definition

A relation **R** on a set **A** is called ***transitive*** if whenever $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$, for all $a, b, c \in A$

$$\forall a \forall b \forall c \big(\big((a, b) \in R \wedge (b, c) \in R \big) \rightarrow (a, c) \in R \big)$$

Example

Consider the following relations on $\{1, 2, 3, 4\}$:

$R_1 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$

$R_2 = \{(1, 1), (1, 2), (2, 1)\}$

$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$

$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$

$R_6 = \{(3, 4)\}$

Which of these relations are transitive?

Solution

The relations R_4 and R_5 are transitive because in each of these relations case that is (a, b) and (b, c) belong to this relation then (a, c) also does.
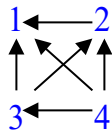
For R_4 | For R_5
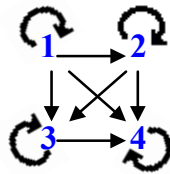
The relation R_1 is not transitive because $(3, 4)$ *and* $(4, 1)$ belong to R_1 but not $(3, 1)$

The relation R_2 is not transitive because $(2, 1)$ *and* $(1, 2)$ belong to R_2 but not $(2, 2)$

The relation R_3 is not transitive because $(4, 1)$ *and* $(1, 2)$ belong to R_3 but not $(4, 2)$

Example

Consider these relations on the set of integers:

$R_1 = \{(a, b) \mid a \le b\}$ $\qquad\qquad$ $R_2 = \{(a, b) \mid a > b\}$

$R_3 = \{(a, b) \mid a = b \text{ or } a = -b\}$ $\qquad$ $R_4 = \{(a, b) \mid a = b\}$

$R_5 = \{(a, b) \mid a = b+1\}$ $\qquad\qquad$ $R_6 = \{(a, b) \mid a+b \le 3\}$

Which of these relations contain each of the pairs $(1, 1)$, $(1, 2)$, $(2, 1)$, $(1, -1)$, and $(2, 2)$?

Solution

The relations R_1, R_2, R_3 and R_4 are transitive.

R_1 is transitive because $a \le b$ and $b \le c$ imply that $a \le c$

R_2 is transitive because $a > b$ and $b > c$ imply that $a > c$

R_3 is transitive because $a = \pm b$ and $b = \pm c$ imply that $a = \pm c$

R_4 is transitive because $a = b$ and $b = c$ imply that $a = c$

The relations R_5 and R_6 are not transitive.

R_5 is not transitive because $a = b+1$ and $b = c+1$ imply that $a = (c+1)+1 = c+2 \ne c+1$

R_6 is not transitive because $2+1 \le 3$ and $1+2 \le 3$ imply that $2+2 \nleq 3$

Example

Is the "divides" relation on the set of positive integers transitive?

Solution

Suppose a divides b and b divides c. Then there are positive integers m and n such that $b = ma$ and $c = nb$. Hence $c = n(ma) = (nm)a$, so a divides c.

Therefore this relation is transitive.

Combining Relations

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

The relations $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ and $R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$

$R_1 \cup R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\}$

$R_1 \cap R_2 = \{(1, 1)\}$

$R_1 - R_2 = \{(2, 2), (3, 3)\}$

$R_2 - R_1 = \{(1, 2), (1, 3), (1, 4)\}$

Example

Let R_1 be the "less than" relation on the set of real numbers and let R_2 be the "greater than" relation on the set of real numbers, that is $R_1 = \{(x,y)|x < y\}$ and $R_2 = \{(x,y)|x > y\}$.

What are $R_1 \cup R_2$, $R_1 \cap R_2$, $R_1 - R_2$, $R_2 - R_1$, and $R_1 \oplus R_2$?

Solution

$(x,y) \in R_1 \cup R_2$ if and only if $(x,y) \in R_1$ or $(x,y) \in R_2$. That implies $(x, y) \in R_1 \cup R_2$ iff $x < y$ or $x > y$. Since $x < y$ or $x > y$ means that, that follows that $R_1 \cup R_2 = \{(x, y)| x \neq y\}$.

$R_1 \cap R_2 = \emptyset$, since it is impossible for a pair (x, y) to belong to both R_1 and R_2 because $x < y$ and $x > y$.

$R_1 - R_2 = R_1$, since $R_1 \cap R_2 = \emptyset$

$R_2 - R_1 = R_2$, since $R_1 \cap R_2 = \emptyset$

$R_1 \oplus R_2 = R_1 \cup R_2 - R_1 \cap R_2 = \{(x, y)| x \neq y\}$

Definition

Let R be a relation from a set A to a set B and S a relation from B to a set C. The composite of R and A is the relation consisting of ordered pairs (a, c), where $a \in A, c \in C$, and for which there exists an element $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$. We denote the composite of R and S by $S \circ R$.

Example

What is the composite of the relation R and S, where
R is the relation from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$ with $R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$.
S is the relation from $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$ with $S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$.

Solution

$$
\begin{array}{ccc}
R & S & S \circ R \\
(1,1) & (1,0) & \rightarrow & (1,0) \\
(1,4) & (4,1) & \rightarrow & (1,1) \\
(2,3) & (3,1) & \rightarrow & (2,1) \\
(2,3) & (3,2) & \rightarrow & (2,2) \\
(3,1) & (1,0) & \rightarrow & (3,0) \\
(3,4) & (4,1) & \rightarrow & (3,1)
\end{array}
$$

$S \circ R = \{(1,0), (1,1), (2,1), (2,2), (3,0), (3,1)\}$

Definition

Let R be a relation on the set A. Then powers R^n, $n = 1, 2, 3, \ldots$ are defined recursively by

$$R^1 = R \quad and \quad R^{n+1} = R^n \circ R$$

Example

Let $R = \{(1, 1), (2, 1), (3, 2), (4, 3)\}$. Find the powers R^n, $n = 2, 3, 4, \ldots$

Solution

$$R^2 = R \circ R = \{(1, 1), (2, 1), (3, 1), (4, 2)\}$$
$$R^3 = R^2 \circ R = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$$
$$R^4 = R^3 \circ R = \{(1, 1), (2, 1), (3, 1), (4, 1)\}$$

From that, it follows that $R^n = R^3$ for $n = 5, 6, 7, \ldots$.

Theorem

The relation on a set A is transitive **iff** $R^n \subseteq R$ for $n = 1, 2, 3, \ldots$.

Proof

Suppose that $R^n \subseteq R$ for $n = 1, 2, 3, \ldots$. In particular, $R^2 \subseteq R$. If $(a, b) \in R$ and $(b, c) \in R$, then by definition of composite, $(a, c) \in R^2$. Because $R^2 \subseteq R$, this means that $(a, c) \in R$. Hence, R is transitive.

Using mathematical induction to prove the only if part of the theorem

Assume that $R^n \subseteq R$ where n is a positive integer. This is the inductive hypothesis.

To complete the inductive step we must show that this implies that R^{n+1} is also a subset of R.

Assume that $(a, b) \in R^{n+1}$, then because $R^{n+1} = R^n \circ R$, there is an element x with $x \in A$ such that $(a, x) \in R$ and $(x, b) \in R^n$. The inductive hypothesis, namely, that $R^n \subseteq R$, implies that $(x, b) \in R$

Furthermore, because R is transitive, and $(a, x) \in R$ and $(x, b) \in R$, it follows that $(a, b) \in R$.

This shows that $R^n \subseteq R$.

Exercises   *Section* **4.1 – Relations and Their Properties**

1. List the ordered pairs in the relation R from $A = \{0, 1, 2, 3, 4\}$ to $B = \{0, 1, 2, 3\}$ where $(a, b) \in R$ if and only if

    a) $a = b$ *b)* $a + b = 4$ *c)* $a > b$

    d) $a \mid b$ *e)* $gcd(a,b) = 1$ *f)* $lcm(a,b) = 2$

2. *a)* List all the ordered pairs in the relation $R = \{(a, b) \mid a \ divides \ b\}$ on the set $\{1, 2, 3, 4, 5, 6\}$

    b) Display this relation graphically.

    c) Display this relation in tabular form.

3. For each of these relations on the set $\{1, 2, 3, 4\}$, decide whether it is reflexive, symmetric, antisymmetric and transitive

    a) $\{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$
    b) $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$
    c) $\{(2, 4), (4, 2)\}$
    d) $\{(1, 2), (2, 3), (3, 4)\}$
    e) $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$
    f) $\{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$

4. Determine whether the relation R on the set of all people is reflexive, symmetric, antisymmetric, and/or transitive, where $(a, b) \in R$ if and only if

    a) a is taller than b.
    b) a and b were born on the same day
    c) a has the same first name as b.
    d) a and b have a common grandparent.

5. Determine whether the relation **R** on the set of all **real numbers** is reflexive, symmetric, antisymmetric, and/or transitive, where $(x, y) \in$ **R** if and only if

    a) $x + y = 0$ *b)* $x = \pm y$ *c)* $x - y$ is a rational number   *d)* $x = 2y$
    e) $xy \geq 0$ *f)* $xy = 0$ *g)* $x = 1$ *h)* $x = 1 \ or \ y = 1$

6. Determine whether the relation R on the set of all **integers numbers** is reflexive, symmetric, antisymmetric, and/or transitive, where $(x, y) \in R$ if and only if

    a) $x \neq y$ *b)* $xy \geq 1$ *c)* $x = y + 1 \ or \ x = y - 1$ *d)* $x \equiv y (\boldsymbol{mod} \ 7)$
    e) x *is a multiple of* y *f)* $x = y^2$ *g)* $x \geq y^2$

7. Show that the relation $R = \varnothing$ on nonempty set S is symmetric and transitive, but not reflexive.

8. Show that the relation $R = \varnothing$ on nonempty set $S = \varnothing$ is reflexive, symmetric and transitive.

9. Give an example of a relation on a set that is
   a) both symmetric and antisymmetric
   b) neither symmetric nor antisymmetric

10. A relation R is called **asymmetric** if $(a, b) \in R$ implies that $(b, a) \notin R$. Explore the notion of an asymmetric relation to the following
    a) $\{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$
    b) $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$
    c) $\{(2, 4), (4, 2)\}$
    d) $\{(1, 2), (2, 3), (3, 4)\}$
    e) $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$
    f) $\{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$
    g) a is taller than b.
    h) a and b were born on the same day
    i) a has the same first name as b.
    j) a and b have a common grandparent.

11. Let R be the relation $R = \{(a, b)| \ a < b\}$ on the set of integers. Find
    a) R^{-1} b) $\overline{R}$

12. Let R be the relation $R = \{(a, b)| \ a \ divides \ b\}$ on the set of positive integers. Find
    a) R^{-1} b) $\overline{R}$

13. Let R be the relation on the set of all states in the U.S. consisting of pairs (a, b) where state a borders state b. Find
    a) R^{-1} b) $\overline{R}$

14. Let $R_1 = \{(1, 2), (2, 3), (3, 4)\}$ and

    $R_2 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3), (3, 4)\}$ be relation from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$. Find
    a) $R_1 \cup R_2$ b) $R_1 \cap R_2$ c) $R_1 - R_2$ d) $R_2 - R_1$

15. Let the relation R = $\{(1, 2), (1, 3), (2, 3), (2, 4), (3, 1)\}$ and the relation S = $\{(2, 1), (3, 1), (3, 2), (4, 2)\}$. Find $S \circ R$

16. $R_1 = \{(a,b) \in \mathbf{R}^2 | a > b\}$ $R_3 = \{(a,b) \in \mathbf{R}^2 | a < b\}$ $R_5 = \{(a,b) \in \mathbf{R}^2 | a = b\}$

    $R_2 = \{(a,b) \in \mathbf{R}^2 | a \geq b\}$ $R_4 = \{(a,b) \in \mathbf{R}^2 | a \leq b\}$ $R_6 = \{(a,b) \in \mathbf{R}^2 | a \neq b\}$

    Find the following:

    a) $R_1 \cup R_3$ b) $R_1 \cup R_5$ c) $R_2 \cap R_4$ d) $R_3 \cap R_5$ e) $R_1 - R_2$

200

f) $R_2 - R_1$ *g*) $R_1 \oplus R_3$ *h*) $R_2 \oplus R_4$ *i*) $R_1 \circ R_1$ *j*) $R_1 \circ R_2$

k) $R_1 \circ R_3$ *l*) $R_1 \circ R_4$ *m*) $R_1 \circ R_5$ *n*) $R_1 \circ R_6$ *o*) $R_2 \circ R_3$

17. Let R_1 *and* R_2 be the "*divides*" and "*is a multiple of*" relations on the set of all positive integers, respectively. That is $R_1 = \{(a,b) \mid a \text{ divides } b\}$ and $R_2 = \{(a,b) \mid a \text{ is a multiple of } b\}$

Find the following:

a) $R_1 \cup R_2$ *b*) $R_1 \cap R_2$ *c*) $R_1 - R_2$ *d*) $R_2 - R_1$ *e*) $R_1 \oplus R_2$

Section 4.2 – Representing Relations

Representing Relations Using Matrices

A relation between finite sets can be represented using a zero-one matrix. Suppose that R is a relation from $A = \{a_1, a_2, a_3, \ldots, a_m\}$ to $B = \{b_1, b_2, b_3, \ldots, b_n\}$. The relation R can be represented by the matrix $M_a = \{m_{ij}\}$ where

$$m_{ij} = \begin{cases} 1 \text{ if } \left(a_i, b_j\right) \in R \\ 0 \text{ if } \left(a_i, b_j\right) \notin R \end{cases}$$

Example

Suppose that A = {1, 2, 3} and B = {1, 2}. Let R the relation from A to B containing (a, b) if $a \in A$, $b \in B$, and $a > b$. What is the matrix representing R is $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, and $b_1 = 1$, $b_2 = 2$?

Solution

$$R = \{(2, 1), (3, 1), (3, 2)\} \qquad M_R = \begin{bmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Example

Let $A = \{a_1, a_2, a_3\}$ and $B = \{b_1, b_2, b_3, b_4, b_5\}$. Which ordered pairs are in the relation R represented by the matrix

$$M_R = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix} ?$$

Solution

$$R = \left\{\left(a_1, b_2\right), \left(a_2, b_1\right), \left(a_2, b_3\right), \left(a_2, b_4\right), \left(a_3, b_1\right), \left(a_3, b_3\right), \left(a_3, b_5\right)\right\}$$

A relation R on A is ***reflexive*** if $(a, a) \in R$ whenever $a \in A$

$$M_R = \left(M_R\right)^t \qquad \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

A relation R on A is ***symmetric***

$$\begin{bmatrix} \diagdown & 1 \\ 1 & \diagdown & 0 \\ & 0 & \diagdown \end{bmatrix}$$
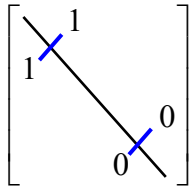
A relation R on A is ***antisymmetric*** iff $(a, b) \in R$ and $(b, a) \in R \implies a = b$

$$\begin{bmatrix} \diagdown & 1 \\ 0 & \diagdown & 0 \\ & 0 & \diagdown \\ & & 1 \end{bmatrix}$$
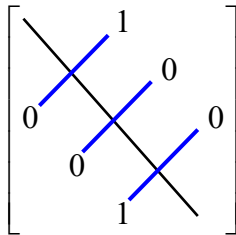
Example

Suppose that the relation R on the set is represented by the matrix

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Is R reflexive, symmetric, and/or antisymmetric?

Solution

   Because the diagonal elements are equal to 1, R is reflexive.
   M_R is symmetric and it is not antisymmetric.

Relations Using Diagraphs

Definition

A directed ***graph***, or ***diagraph***, consists of a set V of ***vertices*** (or *nodes*) together with a set E ordered pairs of elements of V called ***edges*** (or *arcs*). The vertex a is called the ***initial*** vertex of the edge (a, b), and the vertex b is called the ***terminal*** vertex of this edge.

Example

Draw the directed graph with vertices *a, b, c,* and *d,* and edges (*a, b*), (*a, d*), (*b, b*), (*b, d*), (*c, a*), (*c, b*), and (*d, b*)

Solution
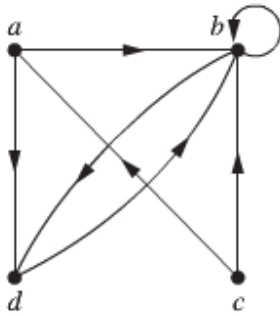
Example

Draw the directed graph of the relation $R = \{(1, 1), (1, 3), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (4, 1)\}$ on the set $\{1, 2, 3, 4\}$

Solution
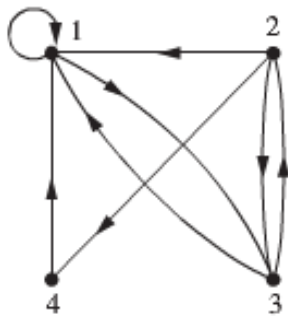
Example

What are the ordered pairs in the relation *R* represented by the directed graph shown below
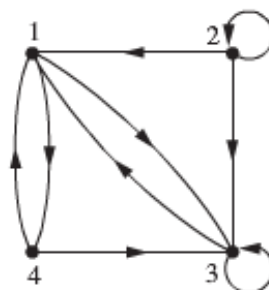
Solution

$R = \{(1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (3, 1), (3, 3), (4, 1), (4, 3)\}$

Exercises   *Section* 4.2 – **Representing Relations**

1. Represent each of these relations on {1, 2, 3} with a matrix (with the elements of this set listed in increasing order). Then draw the directed graphs representing each relation
   a) {(1, 1), (1, 2), (1, 3)}
   b) {(1, 2), (2, 1), (2, 2), (3, 3)}
   c) {(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)}
   d) {(1, 3), (3, 1)}

2. Represent each of these relations on {1, 2, 3, 4} with a matrix (with the elements of this set listed in increasing order). Then draw the directed graphs representing each relation
   a) {(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)}
   b) {(1, 1), (1, 4), (2, 2), (3, 3), (4, 1)}
   c) { (1, 2), (1, 3), (1, 4), (2, 1), (2, 3), (2, 4), (3, 1), (3, 2), (3, 4), (4, 1), (4, 2), (4, 3)}
   d) {(2, 4), (3, 1), (3, 2), (3, 4)}

3. List the ordered pairs in the relations on {1, 2, 3} corresponding to these matrices (where the rows and columns correspond to the integers listed in increasing order). Then draw the directed graphs representing each relation

   $$a) \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \qquad b) \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad c) \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

4. List the ordered pairs in the relations on {1, 2, 3, 4} corresponding to these matrices (where the rows and columns correspond to the integers listed in increasing order). Then draw the directed graphs representing each relation

   $$a) \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \qquad b) \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad c) \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

5. Let R be the relation represented by the matrix

   $$M_R = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

   Find: a) R^2 b) R^3 c) R^4

6. Draw the directed graph that represents the relation {(a, a), (a, b), (b, c), (c, b), (c, d), (d, a), (d, b)}

7. Determine whether the relations represented by the directed graphs are reflexive, irreflexive, symmetric, antisymmetric, and/or transitive

a)
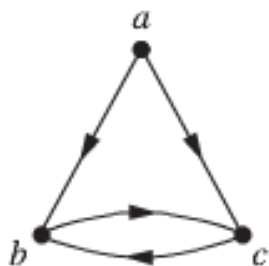
b)
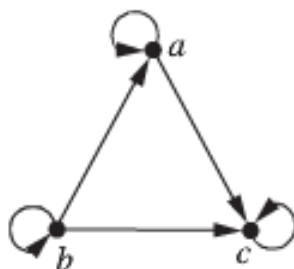
c)
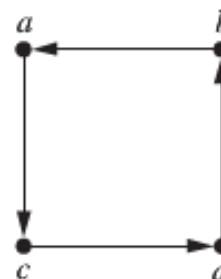
d)
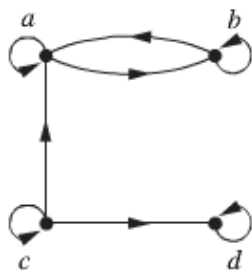
e)
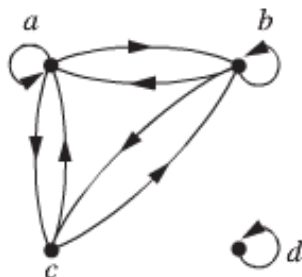
f)

Section 4.3 – Closures of Relations

Closures

The **reflexive closure** of R can be formed by adding to R all pairs of the form (a, a) with $a \in A$, not already in R.

The reflexive closure of R equals $R \cup \Delta$ where

$\Delta = \{(a,a) \mid a \in A\}$ is the **diagonal relation** on A.

Example

What is the reflexive closure of the relation $R = \{(a,b) \mid a < b\}$ on the set of integers?

Solution

The reflexive closure of R is the relation

$$R \cup \Delta = \{(a,b) \mid a < b\} \cup \{(a,a) \mid a \in \mathbb{Z}\}$$
$$= \{(a,b) \mid a \le b\}$$

Example

What is the symmetric closure of the relation $R = \{(a,b) \mid a > b\}$ on the set of positive integers?

Solution

The symmetric closure of R is the relation

$$R \cup R^{-1} = \{(a,b) \mid a > b\} \cup \{(b,a) \mid a > b\}$$
$$= \{(a,b) \mid a \ne b\}$$

Path in Directed Graphs

Definition

A path from a to b in the directed graph G is a sequence of edges (x_0, x_1), (x_1, x_2), (x_2, x_3),

..., (x_{n-1}, x_n) in G, where n is nonnegative integer, and $x_0 = a$ and $x_n = b$, that is, a sequence of edges where the terminal vertex of an edge is the same as the initial vertex in the next edge in the path. The path is denoted by x_0, x_1, x_2, ..., x_{n-1}, x_n and has length n. We view the empty set of edges as a path of length zero from a to a. A path of length $n \ge 1$ that begins and ends at the same vertex is called a **circuit** or **cycle**.

Example

Which of the following are paths in the directed graph: *a, b, e, d; a, e, c, d, b; b ,a, c, b, a, a, b; d, c; c, b, a; e, b, a, b, a, b, e?*

What are the lengths of those that are paths?

Which of the paths in this list are circuits?
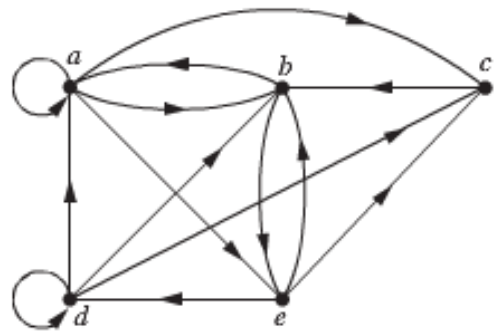
Solution

Each of (a, b), (b, e), and (e, d) is an edge a, b, e, d is a path of length 3

(c, d) is not an edge, therefore a, e, c, d, b is not a path

b ,a, c, b, a, a, b is a path of length 6

d, c is a path of length 1

c, b, a is a path of length 2

e, b, a, b, a, b, e is a path of length 6

The 2 paths b, a, c, b, a, a, b and e, b, a, b, a, b, e are circuits because they begin and end the same vertex.

The paths $a, b, e, d; c, b, a;$ and d, c are not circuits

Theorem

Let R be a relation on a set A. There is a path of length n, where n is a positive integer, from a to b if and only if $(a,b) \in R^n$

Proof

Using mathematical induction

There is a path from a to b of length one if and only if $(a,b) \in R$, which is true when $n = 1$.

Assume that the theorem is true for a positive integer n.

We need to prove that there is a path of length $n + 1$ from a to b if and only if $c \in A$ such there is a path of length 1 from a to c, so $(a,c) \in R$, and path of length n from c to b $(c,b) \in R^n$.

Consequently, by the inductive hypothesis, there is a path of length $n + 1$ from a to b if and only if there is an element c with $(a,c) \in R$ and $(c,b) \in R^n$. But there is such an element iff $(a,b) \in R^{n+1}$.

Therefore, there is a path of length $n + 1$ from a to b iff $(a,b) \in R^{n+1}$. This completes the proof.

Transitive Closures

Definition

Let R be a relation on a set A. The ***connectivity relation*** R^* consists of the pairs (a, b) such that there is a path of length at least one from a to b in R.

Example

Let R be the relation on the set of all people in the world that contains (a, b) if a has met b. What is R^n, where n is a positive integer greater than one? What is R^*?

Solution

The relation R^* contain (a, b) if there is a person c such that $(a, c) \in R$ and , that is, if there is a person c such that a has met c and c has met b.

Similarly, R^n consists of those pairs (a, b) such that there are people $x_1, x_2, \ldots, x_{n-1}$ such that a has met x_1. x_1 has met $x_2, \ldots, x_{n-1}$ has met b.

The relation R^* contains (a, b) if there is a sequence of people, starting with a and ending with b, such that each person in the sequence has met next person in the sequence.

Example

Let R be the relation on the set of all states in U.S. that contains (a, b) if state a and state b have a common border. What is R^n, where n is a positive integer? What is R^*?

Solution

The relation R^n contain (a, b), where it is possible to go from state a to state b by crossing exactly n state borders. The relation R^* consists of the ordered pairs (a, b), where it is possible to go from state a to state b crossing as many borders as necessary.

The only ordered pairs not in R^* are those containing sates that are not connected to the continental U.S.

Theorem

The transitive closure of a relation R equals the connectivity relation R^*.

Lemma

Let A be a set with n elements, and let R be the relation on A. If there is a path of length at least one in R from a to b, then there is such a path with length not exceeding n. Moreover, when $a \neq b$, if there is a path of length at least one in R from a to b, then there is such a path with length not exceeding $n - 1$.
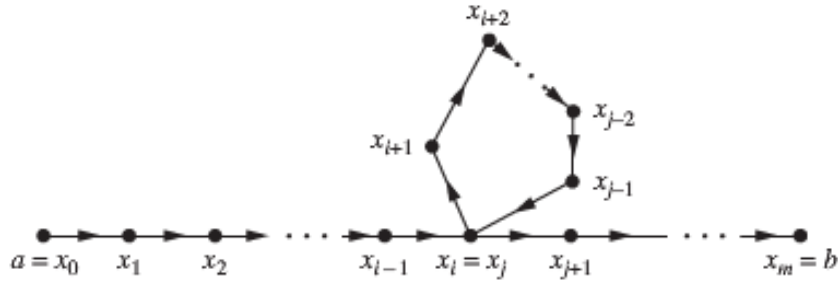
Proof

Suppose there is a path from a to b in R. Let m be the length of the shortest such path.

Suppose that x_0, x_1, x_2, ..., x_{m-1}, x_m, where $x_0 = a$ and $x_m = b$, is such a path.

Suppose that $a = b$ and that $m > n$, so that $m \geq n+1$.

By the pigeonhole principle, because there are n vertices in A, among m vertices x_0, x_1, ..., x_m, at least two are equal.

Suppose that $x_i = x_j$ with $0 \leq i < j \leq m-1$. Then the path contains a circuit from x_i to itself. This circuit can be deleted from the path from a to b, leaving a path, namely, x_0, x_1, ..., x_i, x_{j+1}, ..., x_m, from a to b of shorter length. Hence, the path of shortest length must have less than or equal to n.

Exercises   Section 4.3 – Closures of Relations

1. Let R be the relation on the set $\{0, 1, 2, 3\}$ containing the ordered pairs $(0, 1)$, $(1, 1)$, $(1, 2)$, $(2, 0)$, $(2, 2)$, and $(3, 0)$. Find the
    a) Reflexive closure of R.
    b) Symmetric closure of R.

2. Let R be the relation $\{(a, b) \mid a \neq b\}$ on the set of integers. What is the reflexive closure of R?

3. Let R be the relation $\{(a, b) \mid a \text{ divides } b\}$ on the set of integers. What is the symmetric closure of R?

4. How can the directed graph representing the reflexive closure of a relation on a finite set be constructed from the directed graph of the relation?

5. Draw the directed graph of the *reflexive*, *symmetric*, and *both reflexive and symmetric* closure of the relations with the directed graph shown

   a)   *b)*   *c)*
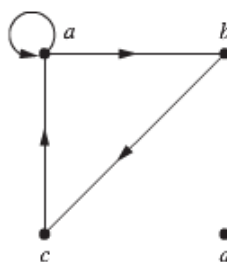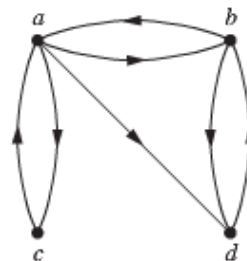
6. 1. Determine whether these sequences of vertices are paths in this directed graph
    a) a, b, c, e
    b) b, e, c, b, e
    c) a, a, b, e, d, e
    d) b, c, e, d, a, a, b
    e) b, c, c, b, e, d, e, d
    f) a, a, b, b, c, ,c, b, e, d
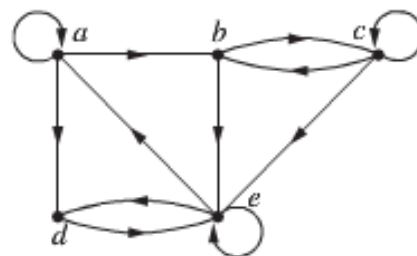
   2. Find all circuits of length three in the directed graph

7. Let R be the relation on the set $\{1, 2, 3, 4, 5\}$ containing the ordered pairs $(1, 3)$, $(2, 4)$, $(3, 1)$, $(3, 5)$, $(4, 3)$, $(5, 1)$, and $(5, 2)$. Find
    a) R^2 *b)* R^3 *c)* R^4 *d)* R^5 *e)* R^6 *f)* R^*

8. Let R be the relation on the pair (a, b) if a and b are cities such that there is a direct non-stop airline flight from a to b. When is (a, b) in
    a) R^2 *b)* R^3 *c)* R^*

9. Let R be the relation on the set of all students containing the ordered pair (a, b) if a and b are in at least one common class and $a \neq b$. When is (a, b) in

    a) R^2 *b*) R^3 *c*) R^*

10. Suppose that the relation R is reflexive. Show that R^* is reflexive.

11. Suppose that the relation R is symmetric. Show that R^* is symmetric.

12. Suppose that the relation R is irreflexive. Is the relation R^2 necessarily irreflexive.

Section 4.4 – Equivalence Relations

Definition

A relation on a set A is called an ***equivalence relation*** if it is reflexive, symmetric, and transitive.

Definition

Two elements a and b that related by an equivalence relation are called ***equivalent***. The notation $a \sim b$ is often used to denotes that a and b are equivalent elements with respect to a particular equivalence relation.

Example

Let R be the relation on the set of integers such that aRb if and only if $a = b$ or $a = -b$. It follows that R is an equivalence relation.

Example

Let R be the relation on the set of real numbers such that aRb if and only if $a - b$ is an integer . Is R an equivalence relation?

Solution

Because $a - a = 0$ is an integer for all real numbers a, aRa for all real numbers a. Hence, R is reflexive

Suppose that aRb, then $a - b$ is an integer, so $b - a$ and $b - c$ are integers.

Therefore, $a - c = (a - b) + (b - c)$ is also an integer. Hence, aRc.

Thus, R is transitive. Consequently, R is an equivalence relation.

Example

Let m be an integer with $m > 1$. Show that the relation $R = \{(a, b) \mid a \equiv b \pmod{m}\}$ is an equivalence relation on the set of integers.

Solution

$a \equiv b \pmod{m}$ *iff* m divides $a - b$.

Since $0 = 0 \cdot m$ then $a - a = 0$ is divisible by m. Hence, $a \equiv a \pmod{m}$, so congruence modulo m is reflexive.

Suppose that $a \equiv b \pmod{m}$, then $a - b$ is divisible by m, so $a - b = km$, where k is an integer. It follows that $b - a = (-k)m$, so $b \equiv a \pmod{m}$. Hence, congruence modulo m is symmetric.

Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then m divides both $a - b$ and $b - c$. so $a - b = km$ and $b - c = lm$, where k and l are integers. It follows that $a - c = (a - b) + (b - c) = km + lm = (k + l)m$, so $a \equiv c \pmod{m}$. Hence, congruence modulo m is transitive.

The congruence modulo m is an equivalence relation.

Example

Let n be a positive integer and S a set of strings. Suppose that R_n is the relation on S such that $s\ R_n\ t$ if and only if $s = t$, or both s and t have at least n characters and the first n characters of s and t are the same. That is, a string of fewer than n characters is related only to itself; a string s with at least n characters is related to a string t if and only if t has at least n characters and t begins with the n characters at the start of s. For example, let $n = 3$ and let S be the set of all bit strings. Then $s\ R_3\ t$ either when $s = t$ or both s and t are bit strings of length 3 or more that begin with the same three bits. For instant, $01\ R_3\ 01$ and $00111\ R_3\ 00101$ but $01\not R_3\ 010$ and $01011\not R_3\ 01110$

Show that every set S of strings and every positive integer n, R_n is an equivalence relation on S.

Solution

The relation R_n is reflexive because $s = s$, so that $s\ R_n\ s$ whenever s is a string in S.

If $s\ R_n\ t$, then either $s = t$ or s and t are both at least n characters long that begin with same n characters. This means that $t\ R_n\ s$. Therefore, R_n is symmetric.

Suppose that $s\ R_n\ t$ and $t\ R_n\ u$. Then either $s = t$ or s and t are both at least n characters long s and t begin with same n characters, and either $t = u$ or t and u are both at least n characters long t and u begin with same n characters. From this, we can deduce that either $s = u$ or s and u are both at least n characters long s and u begin with same n characters.
Because s, t and u are all at least n characters long s and u begin with same n characters as t does. Therefore, R_n is transitive.

It follows that R_n is an equivalence relation.

Example

Let R be the relation on the set of real numbers such that $x\ R\ y$ if and only if x and y are real numbers that differ by less than 1, that is $|x - y| < 1$. Show that R is not an equivalence relation.

Solution

Let $x = 2.5$, $y = 1.8$, and $z = 1.1$, so that
$|x - y| = |2.5 - 1.8| = .7 < 1$ and $|y - z| = |1.8 - 1.1| = .7 < 1$
But $|x - z| = |2.5 - 1.1| = 1.4 > 1$. That is $2.5 R\ 1.8$, $1.8 R\ 1.1$, but $2.5 \not R\ 1.1$

Equivalence Classes

Definition

Let R be an equivalent relation on a set A. The set of all elements that are related to an element a of A is called the ***equivalence class*** of a. The equivalence class of a with respect to R is denoted by $[a]_R$. When only one relation is under consideration, we can delete the subscript R and write $[a]$ for this equivalence class.

$$[a]_R = \{s \mid (a,\, s) \in R\}$$

$b \in [a]_R$, then b called a ***representative*** of this equivalence class.

Example

Let R be the relation on the set of integers such that aRb if and only if $a = b$ or $a = -b$. What is the equivalence class for this relation?

Solution

Because an integer is equivalent to itself and its negative in this equivalence relation, it follows that $[a] = \{-a,\, a\}$. This set contains two distinct integers unless $a = 0$.

For instance, $[7] = \{-7,\, 7\}$, $[5] = \{-5,\, 5\}$, and $[0] = \{0\}$

Example

What is the equivalence class of 0 and 1 for congruence modulo 4?

Solution

The equivalence class of 0 contains all integers a such that $a \equiv 0 \,(\mathbf{mod}\ 4)$. The integers in this class are those divisible by 4, Hence, the equivalence class of 0 for this relation is

$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$

The equivalence class of 1 contains all integers a such that $a \equiv 1 \,(\mathbf{mod}\ 4)$. The integers in this class are those that have a remainder of 1 when divided by 4, Hence, the equivalence class of 1 for this relation is

$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

Example

What is the equivalence class of the string 0111 with respect to the equivalence relation R_3 on the set of all bit strings?

Recall that $s\ R_3 t$ if and only if s and t are bit strings with $s = t$ or s and t are strings of at least three bits that start with the same three bits.

Solution

The bit strings equivalent to 0111 are the bit strings with at least three bits that begin with 011. These are the bit strings 011, 0110, 0111, 01100, 01101, 01110, 01111, and so on …

$$[011]_{R_3} = \{011,\ 0110,\ 0111,\ 01100,\ 01101,\ 01110,\ 01111,\ …\}$$

Equivalence Classes and Partitions

Theorem

Let R be an equivalence relation on a set A. These statements for elements a and b of A are equivalent:

$(i)\ aRb \qquad (ii)\ [a]=[b] \qquad (iii)\ [a]\cap[b]\neq\varnothing$
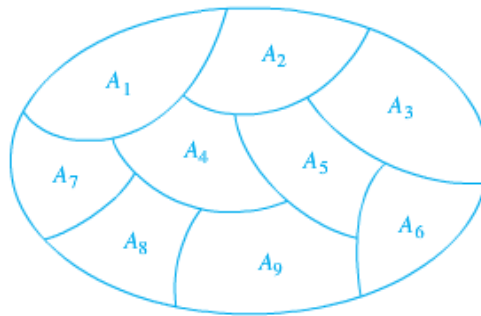
$$\bigcup_{i\in I} A_i = S$$

Example

Suppose that $S = \{1, 2, 3, 4, 5, 6\}$.

The collection of sets $A_1 = \{1,\ 2,\ 3\}$, $A_2 = \{4,\ 5\}$, and $A_3 = \{6\}$ forms a partition of S. Because these sets are disjoint and their union is S.

Theorem

Let R be an equivalent relation on a set S. Then the equivalence classes of R form a partition of S, Conversely, given a partition $\{A_i \mid i \in I\}$ of the set S, there is an equivalence relation R that has the sets A_i, $i \in I$, as its equivalence classes.

Example

List the ordered pairs in the equivalence relation R produced by the partition $A_1 = \{1, 2, 3\}$, $A_2 = \{4, 5\}$, and $A_3 = \{6\}$ of $S = \{1, 2, 3, 4, 5, 6\}$.

Solution

The subsets in the partition are the equivalence classes of R. The pair $(a, b) \in R$ if and only if a and b are in the same subset of the partition.

The pairs (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), and (3, 3) belong to R because $A_1 = \{1, 2, 3\}$ is an equivalence class.

The pairs (4, 4), (4, 5), (5, 4), and (5, 5) belong to R because $A_2 = \{4, 5\}$ is an equivalence class.

The pair (6, 6) belong to R because $A_3 = \{6\}$ is an equivalence class

Example

What are the sets in the partition of the integers arising from congruence modulo 4?

Solution

$$[0]_4 = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$$
$$[1]_4 = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$$
$$[2]_4 = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$$
$$[3]_4 = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$$

Exercises *Section* **4.4 – Equivalence Relations**

1. Which of these relations on {0, 1, 2, 3} are equivalence relations?
    Determine the properties of an equivalence relation that the others lack.
    What are the equivalence classes of the equivalence relations?
    a) {(0, 0), (1, 1), (2, 2), (3, 3)}
    b) {(0, 0), (0, 2), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)}
    c) {(0, 0), (1, 1), (1, 2), (2, 1), (3, 2), (3, 3)}
    d) {(0, 0), (1, 1), (1, 3), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)}
    e) {(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)}

2. Which of these relations on the set of all people are equivalence relations?
    Determine the properties of an equivalence relation that the others lack.
    What are the equivalence classes of the equivalence relations?
    a) $\{(a, b)\,|\,a$ *and* b *are the same age*$\}$

    b) $\{(a, b)\,|\,a$ *and* b *have the same parents*$\}$

    c) $\{(a, b)\,|\,a$ *and* b *share a common parent*$\}$

    d) $\{(a, b)\,|\,a$ *and* b *have met*$\}$

    e) $\{(a, b)\,|\,a$ *and* b *speak a common language*$\}$

3. Which of these relations on the set of all functions from $\mathbb{Z}$ to $\mathbb{Z}$ are equivalence relations?
    Determine the properties of an equivalence relation that the others lack.
    What are the equivalence classes of the equivalence relations?
    a) $\{(f, g)\,|\,f(1) = g(1)\}$
    b) $\{(f, g)\,|\,f(0) = g(0) \ or \ f(1) = g(1)\}$
    c) $\{(f, g)\,|\,f(x) - g(x) = 1 \ for \ all \ x \in \mathbb{Z}\}$
    d) $\{(f, g)\,|\ for \ some \ C \in \mathbb{Z}, \ for \ all \ x \in \mathbb{Z}, \ f(x) - g(x) = C\}$
    e) $\{(f, g)\,|\,f(0) = g(1) \ or \ f(1) = g(0)\}$

4. Define three equivalence relations on the set of students in your discrete mathematics class different from the relations discussed in the text. Determine the equivalence classes for each of these equivalence relations.

5. Define three equivalence relations on the set of buildings on a college campus. Determine the equivalence classes for each of these equivalence relations.

6. Let R be the relation on the set of all sets of real numbers such that $S\,R\,T$ if and only if S and T have the same cardinality. Show that R is an equivalence relation. What are the equivalence classes of the sets {0, 1, 2} and $\mathbf{Z}$?

7. Suppose that A is a nonempty set, and f is a function that has A as its domain. Let R be the relation on A consisting of all ordered pairs (x, y) such that $f(x) = f(y)$

    a) Show that R is an equivalence relation on A.

    b) What are the equivalence classes of R?

8. Suppose that A is a nonempty set, and R is an equivalence relation on A. Show that there is a function f with A as its domain such that $(x, y) \in R$ if and only if $f(x) = f(y)$

9. Determine whether the relation with the directed graph shown is an equivalence relation
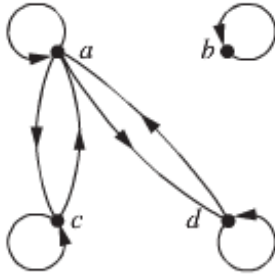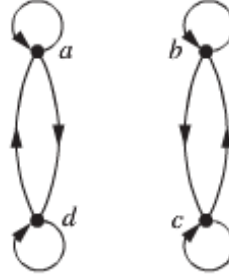
a)   *b)*   *c)*
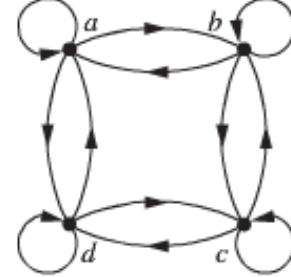
10. Which of these collections of subsets are partitions of $\{1, 2, 3, 4, 5, 6\}$

    a) $\{1, 2\}, \{2, 3, 4\}, \{4, 5, 6\}$

    b) $\{1\}, \{2, 3, 6\}, \{4\}, \{5\}$

    c) $\{2, 4, 6\}, \{1, 3, 5\}$

    d) $\{1, 4, 5\}, \{2, 6\}$

11. Which of these collections of subsets are partitions of $\{-3, -2, -1, 0, 1, 2, 3\}$

    a) $\{-3, -1, 1, 3\}, \{-2, 0, 2\}$

    b) $\{-3, -2, -1, 0\}, \{0, 1, 2, 3\}$

    c) $\{-3, 3\}, \{-2, 2\}, \{-1, 1\}, \{0\}$

    d) $\{-3, -2, 2, 3\}, \{-1, 1\}$

Section 4.5 – **Partial Orderings**

Definition

A relation R on set S is called a partial ordering or partial order if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a partially ordered set, or poset, and is denoted by (S, R). Members of S are called elements of the poset.

Example

Show that the "greater than or equal" relation $(\geq)$ is a partial ordering on the set of integers

Solution

Because $a \geq a$ for every integer a, $\geq$ is reflexive.
If $a \geq b$ and $b \geq a$, then $a = b$. Hence, $\geq$ is symmetric.
If $a \geq b$ and $b \geq c$ imply that $a \geq c$. Hence, $\geq$ is transitive.
It follows that $(\geq)$ is a partial ordering on the set of integers and $(\mathbb{Z}, \geq)$ is a poset.

Example

Show that the inclusion relation $\subseteq$ is a partial ordering on the power set of a set S.

Solution

Because $A \subseteq A$ whenever is a subset of S. $\subseteq$ is reflexive.
It is antisymmetric because $A \subseteq B$ and $B \subseteq A$ imply that $A = B$
$A \subseteq B$ and $B \subseteq C$ imply that $A \subseteq C$, Hence $\subseteq$ is transitive.
Hence, $\subseteq$ is a partial ordering on $P(S)$ and $\left(P(S), \subseteq \right)$ is a poset.

Example

Let R be the relation on the set of people such that xRy if x and y are people and x is older than y. Show that is not a partial ordering,

Solution

R is not reflexive, because no person is older than herself or himself $x\cancel{R}x$
R is antisymmetric because if a person x is older than y, then y is not older than x. That is xRy, then $y\cancel{R}x$.
The relation is transitive because a person x is older than y, then y is older than z, then x is older than z.
R is not a partial ordering.

Definition

The elements a and b of poset $(S, \preceq)$ are called comparable if either $a \preceq b$ or $b \preceq a$. When a and b are elements of S such that neither $a \preceq b$ nor $b \preceq a$, a and b are called incomparable.

Example

In the poset $(\mathbb{Z}, \mid)$ are the integers 3 and 9 comparable? Are 5 and 7 comparable?

Solution

   The integers 3 and 9 are comparable, because 3 | 9.

   The integers 5 and 7 are *incomparable*, because $5 \nmid 7$ and $7 \nmid 5$

Definition

If $(S, \preceq)$ is a poset and every two elements of S are comparable, S is called a ***totally ordered*** or ***linearly ordered*** set, and $\preceq$ is called a ***total order*** or a ***linear order***. A totally ordered set is also called a ***chain***.

Example

The poset $(\mathbb{Z}, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever a and b are integers.

Example

The poset $\left(\mathbb{Z}^+, \mid \right)$ is not totally ordered, because it contains elements that are incomparable, such as 5 and 7.

Definition

If $(S, \preceq)$ is well-ordered set if it is a poset such that $\preceq$ is a total ordering and every nonempty subset of S has a least element.

Example

The set of ordered pairs of positive integers, $\mathbb{Z}^+ \times \mathbb{Z}^+$, with $\left(a_1, a_2 \right) \preceq \left(b_1, b_2 \right)$ if $a_1 < b_1$, or if $a_1 = b_1$ and $a_2 < b_2$ (Lexicographic ordering), is a well-ordered set.

The set **Z**, with the usual $\leq$ ordering, is not well-ordered because the set of negative integers, which is a subset of **Z**, has no least element.

Theorem – **The Principle of Well-Ordered Induction**

Suppose that S is a well-ordered set. Then $P(x)$ is true for all $x \in S$, if

Inductive Step: For every $y \in S$, if $P(x)$ is true for all $x \in S$ with $x \prec y$, then $P(y)$ is true.

Proof

Suppose it is not the case that $P(x)$ is true for all $x \in S$. Then there is an element $y \in S$ such that, $P(y)$ is false.

Consequently, the set $A = \{x \in S \mid P(x) \text{ is false}\}$ is nonempty. Because S is well ordered, A has a least element a. By the choice of a as a least element of A, we know that $P(x)$ is true for all with $x \prec a$. This implies by the inductive step $P(a)$ is true. This contradiction shows that $P(x)$ must be true for all $x \in S$.

Example

Determine whether $(3,\ 5) \prec (4,\ 8)$, whether $(3,\ 8) \prec (4,\ 5)$, and whether $(4,\ 9) \prec (4,\ 11)$ in the poset $(\mathbb{Z} \times \mathbb{Z},\ \preceq)$, where $\preceq$ is the lexicographic ordering constructed from the usual $\leq$ relation on $\mathbb{Z}$.

Solution

Because $3 < 4$, it follows that $(3,\ 5) \prec (4,\ 8)$ and that $(3,\ 8) \prec (4,\ 5)$. We have $(4,\ 9) \prec (4,\ 11)$, because the first entries of $(4,\ 9)$ and $(4,\ 11)$ are the same but $9 < 11$.

Maximal and Minimal Elements

An element of a poset is called maximal if it is not less than any element of the poset. That is, a is *maximal* in the poset $(S,\ \preceq)$ if there is no element $b \in S$ such that $a \prec b$.

Similarly, an element of a poset is called minimal if it is not greater than any element of the poset. That is, a is *minimal* in the poset $(S,\ \preceq)$ if there is no element $b \in S$ such that $b \prec a$.

Maximal and minimal elements are easy to spot using a *Hasse* diagram. They are the "top" and "bottom" elements in the diagram.

Sometimes there is an element in a poset that is greater than every other element. Such that an element is called the greatest element. That is, a s the *greatest element* of the poset $(S,\ \preceq)$

Example

Which elements of the poset ({2, 4, 5, 10, 12, 20, 25},, |) are maximal, and which are minimal?

Solution

From the Hasse diagram, the poset shows that the maximal elements are 12, 20, and 25
The minimal elements are 2 and 5.
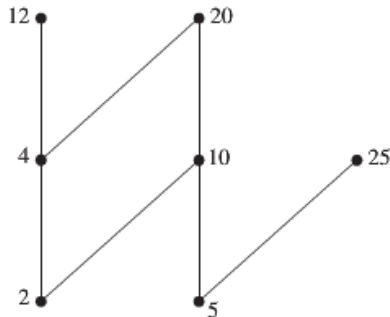
Hasse Diagram

Example

Determine whether the posets represented by each of the Hasse diagrams in figure below have greatest element and a least element.

(a)   (b)   (c)   (d)
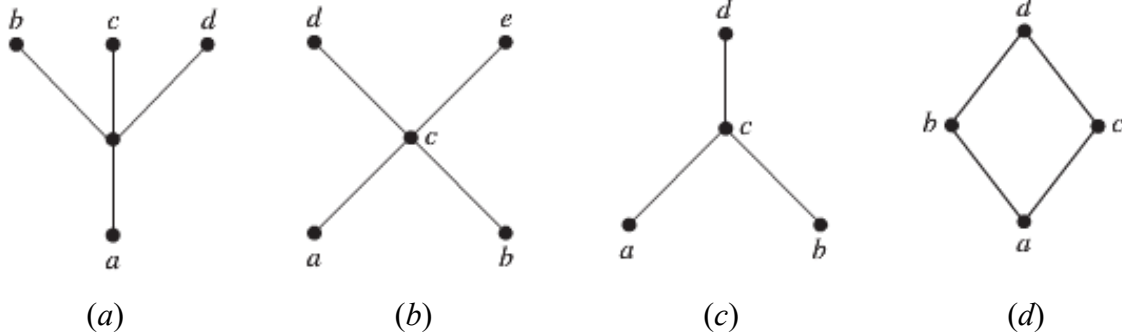
Solution

The least element of the poset with Hasse diagram (a) is a. This poset has no greatest element.
The poset with Hasse diagram (b) has neither a least nor a greatest element.
The poset with Hasse diagram (c) has no least element. Its greatest element is d.
The poset with Hasse diagram (d) has least element a and greatest element d.

Example

Let S be a set. Determine whether there is a greatest element and a least element in the poset $(P(S), \subseteq)$

Solution

The least element is the empty set, because $\varnothing \subseteq T$ for any subset T of S.
The greatest element in this poset, because $T \subseteq S$ whenever T is a subset of S.

Example

Find the lower and upper bounds of the subsets {a, b, c}, {j, h}, and
{a, c, d, f} in the poset with the Hasse diagram shown in the figure.

Solution

The upper bounds of {a, b, c} are e, f, j and h and its only lower bound is a.
There is no upper bounds of {j, h}, and its lower bounds are a, b, c, d, e,
and f.
The upper bounds of {a, c, d, f} are f, h, and j, and its lower bound is a.
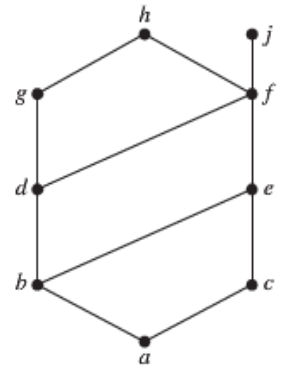
Lattices

A partially ordered set in which every pair of elements has both a least upper bound and a greatest lower
bound is called a **lattice**. Lattices have many special properties.

Example

Determine whether the posets represented by each of the Hasse diagrams are lattices
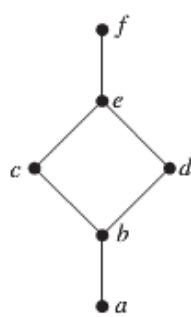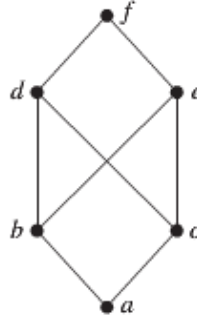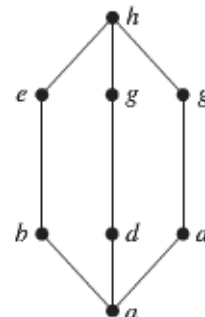
<div style="text-align:center">(a)   (b)   (c)</div>

Solution

The posets represented by the Hasse diagrams in (**a**) and (**c**) are both lattices because in each poset
every pair of elements has both a least upper bound and a greatest lower bound.
On the other hand, the poset with the Hasse diagram shown in (**b**) is not a lattice, because the elements
b and c have no least upper bound. Each of the elements d, e, and f is an upper bound, but none of
these 3 elements precedes the other two with respect to the ordering of this poset.

Example

Is the poset $\left(\mathbb{Z}^+, \mid \right)$ a lattice?

Solution

Let a and b be two positive integers, The least upper bound and greatest lower bound of these 2
integers are the least common multiple and the greatest common divisor of these integers,
respectively, as the reader should verify. It follows that this is a lattice.

Example

Determine whether the posets $(\{1, 2, 3, 4, 5\}, |)$ and $(\{1, 2, 4, 8, 16\}, |)$ are lattices

Solution

Because 2 and 3 have no upper bound in $(\{1, 2, 3, 4, 5\}, |)$, they are certainly do not have a least upper bound. Hence, the first poset is not a lattice.

Every elements of the second poset have both a least upper bound and a greatest lower bound. The least upper bound of 2 elements in this poset is the larger of the elements and the greatest lower bound of 2 elements is the smaller of the elements. Hence, the second poset is a lattice.

Example

Determine whether $(P(S), \subseteq)$ is a lattice where S is a set.

Solution

Let A and B be 2 subsets of S. The least upper bound and the greatest lower bound of A and B are $A \cup B$ and $A \cap B$, respectively.

Hence, $(P(S), \subseteq)$ is a lattice.

Exercises   *Section* 4.5 – **Partial Orderings**

1. Which of these relations on {0, 1, 2, 3} are partial orderings? Determine the properties of a partial
    ordering that the others lack.
    a) {(0, 0), (1, 1), (2, 2), (3, 3)}
    b) {(0, 0), (1, 1), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)}
    c) {(0, 0), (1, 1), (1, 2), (2, 2), (3, 3)}
    d) {(0, 0), (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)}
    e) {(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)}
    f) {(0, 0), (2, 2), (3, 3)}
    g) {(0, 0), (1, 1), (2, 0), (2, 2), (2, 3), (3, 3)}
    h) {(0, 0), (1, 1), (1, 2), (2, 2), (3, 1), (3, 3)}
    i) {(0, 0), (1, 1), (1, 2), (1, 3), (2, 0), (2, 2), (2, 3), (3, 0), (3, 3)}
    j) {(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3), (2, 0), (2, 2), (3, 3)}

2. Is (S, R) a poset If S is the set of all people in the world and $(a, b) \in R$, where a and b are people, if

    a) a is a taller than b?
    b) a is not taller than b?
    c) $a = b$ or a is an ancestor of b?
    d) a and b have a common friend?
    e) a is a shorter than b?
    f) a weighs more than b?
    g) $a = b$ or a is a descendant of b?
    h) a and b do not have a common friend?

3. Which of these are posets?
a) $(Z, =)$	b) $(Z, \neq)$	c) $(Z, \geq)$	d) $(Z, \nmid)$
e) $(R, =)$	f) $(R, <)$	g) $(R, \leq)$	h) $(R, \neq)$

4. Determine whether the relations represented by these zero-one matrices are partial orders

    a) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ b) $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ c) $\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ d) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$

    e) $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$ f) $\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

226

5. Determine whether the relation with the directed graph shown is a partial order.

a)
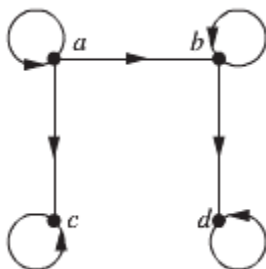
b)
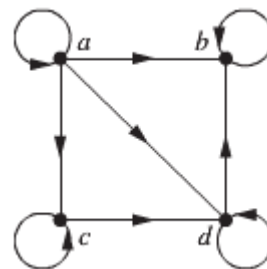
c)

6. Let (S, R) be a poset. Show that $\left(S, R^{-1}\right)$ is also a poset, where R^{-1} is the inverse of R. The poset $\left(S, R^{-1}\right)$ is called the dual of (S, R).

7. Draw the Hasse diagram for the "greater than or equal to" relation on $\{0, 1, 2, 3, 4, 5\}$

Section **4.6 – Graphs: Definitions and Basic Properties**

Definition

A graph $G = (V, E)$ consists of V, a nonempty set of vertices (or nodes) and E, a set of edges. Each edge has either one or two ***vertices*** (plural of ***vertex***) associated with it, called its ***endpoints***. An edge is said to connect its endpoints.

Visualize the graphs by using points to represent vertices and line segments, possibly curved, to represent edges, where the endpoints of a line segment representing an edge are the points representing the ***edge-endpoints***.
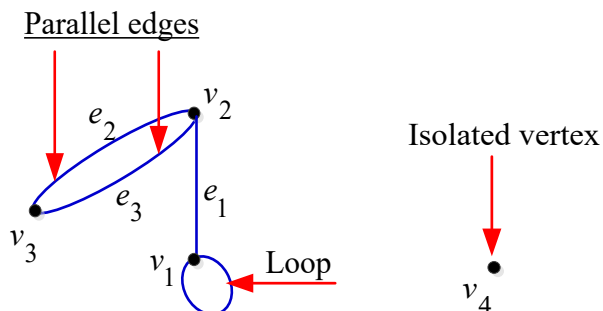
To model a computer network, we need graphs that have more than one edge connecting the same pair of vertices. Graphs that may have ***multiple edges*** connecting the same vertices are called ***multigraphs***. Sometimes a communications link connects a data center with itself, a feedback loop for diagnostic purposes. Such edges are called ***loops***.

Graphs that may include loops, and possibly multiple edges connecting the same pair of vertices or a vertex to itself, are sometimes called ***pseudographs***.

Sometimes we have a ***one-way*** communication link like
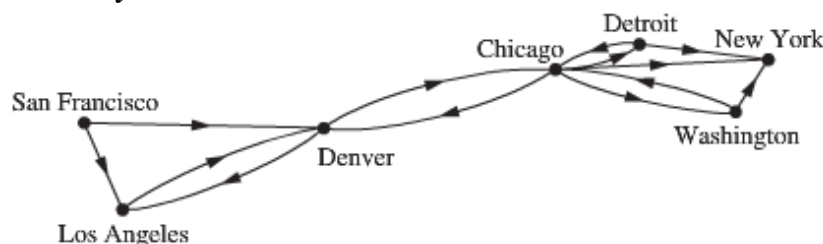
Basic Terminology

Definition

Two vertices u and v in an undirected graph G are called adjacent (or neighbors) in G if u and v are endpoints of an edge e of G. Such an edge e is called incident with the vertices u and v and e is said to connect u and v.

Graph Terminology			
Type	*Edges*	*Multiple Edges Allowed?*	*Loops Allowed?*
Simple graph	Undirected	No	No
Multigraph	Undirected	Yes	No
Pseudograph	Undirected	Yes	Yes
Simple directed graph	Directed	No	No
Directed multigraph	Directed	Yes	Yes
Mixed graph	Directed and undirected	Yes	Yes

Example

Consider the following graph:

a) Write the vertex set and the edge set, and give a table showing the edge-point function.

b) Find all edges that are incident on v_1, all vertices that are

   adjacent to v_1, all edges that are adjacent to e_1, all

   loops, all parallel edges, all vertices that are adjacent to themselves, and all isolated vertices.
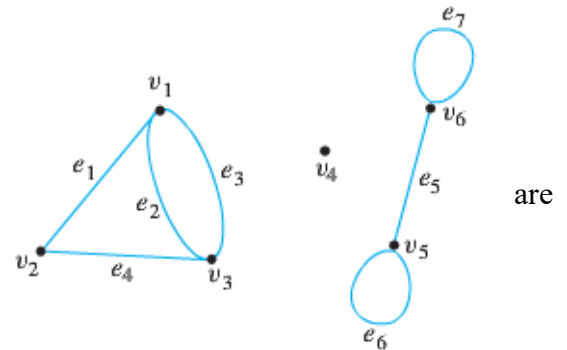
Solution

a) Vertex set = $\{v_1, v_2, v_3, v_4, v_5, v_6\}$

   Edge set = $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$

   Edge-point function:

Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_3\}$
e_3	$\{v_1, v_3\}$
e_4	$\{v_2, v_3\}$
e_5	$\{v_5, v_6\}$
e_6	$\{v_5\}$
e_7	$\{v_6\}$

b) $e_1, e_2,$ and e_3 are incident on v_1

   v_2 and v_3 are adjacent to v_1

   $e_2, e_3,$ and e_4 are adjacent to e_1

   e_6 and e_7 are loops.

e_2 and e_3 are parallel.

v_5 and v_6 are adjacent to themselves.

v_4 is an isolated vertex.

Example

Consider the two drawing shown below.
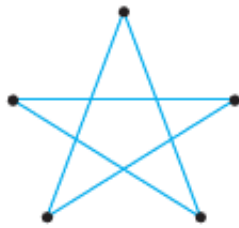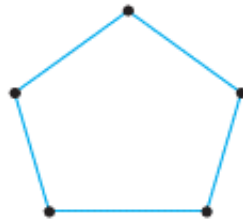
(a)   (b)

Label vertices and edges in such a way that both drawings represent the same graph

Solution
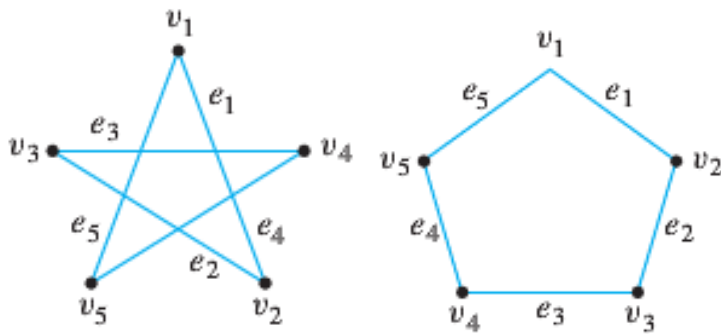
Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_3, v_4\}$
e_4	$\{v_4, v_5\}$
e_5	$\{v_5, v_1\}$

Definition

A **directed graph** (or **digraph**) (V, E) consists of a nonempty set of vertices V and a set of **directed edges** (or **arcs**) E. Each directed edge is associated with an ordered pair of vertices. The directed edge associated with the ordered pair (u, v) is said to *start* at u and *end* at v.
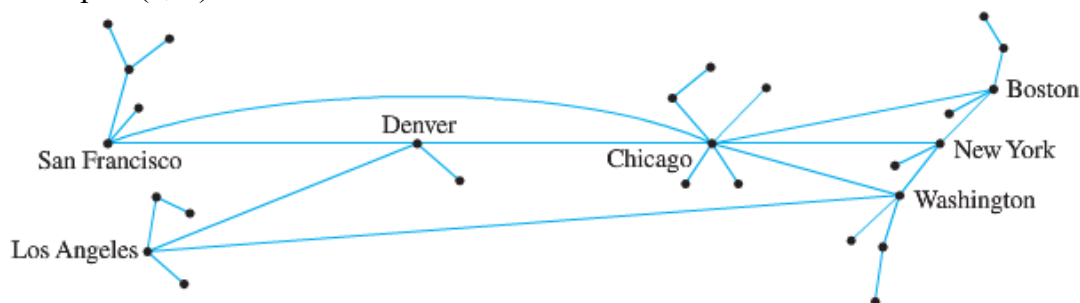
Special Graphs

Definition

A **simple graph** is a graph that does not have any loops or parallel edges. In a simple graph, an edge with endpoints v and w is denoted $\{u, v\}$

Example

Draw all simple graphs with the four vertices $\{u, v, w, x\}$ and two edges, one of which is $\{u, v\}$

Solution
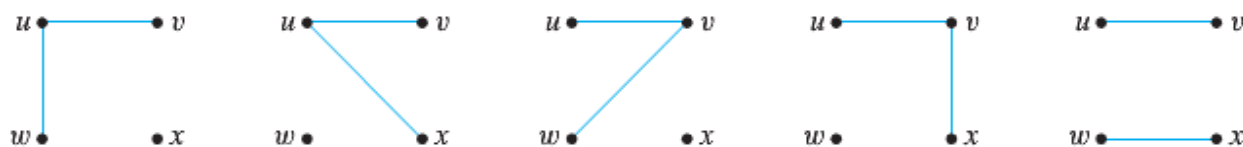
Definition

Let n be a positive integer. A **complete graph** on **n vertices**, denoted K_n is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.

The complete graphs $K_1, K_2, K_3, K_4,$ *and* K_5 can be drawn as follows

231
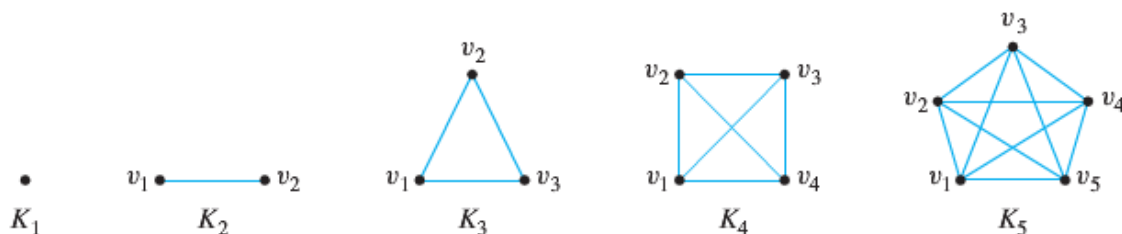
Definition

Let m and n be a positive integers. A ***complete bipartite graph*** on ***(m, n) vertices***, denoted $K_{m,n}$ is a simple graph with distinct vertices $v_1, v_2, \ldots, v_m$ and $w_1, w_2, \ldots, w_n$ that satisfies the following properties:

For all $i, k = 1, 2, \ldots, m$ and for all $j, l = 1, 2, \ldots, n$,

1. There is an edge from each vertex v_i to each vertex w_j

2. There is no edge from each vertex v_i to any other vertex v_k

3. There is no edge from each vertex w_j to any other vertex w_l

Example
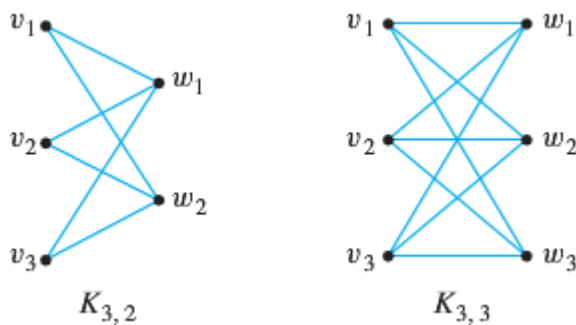
Definition

A graph H is said to be a subgraph of a graph if, and only if, every vertex in H is also a vertex in G, every edge in H is also an edge in G, and every edge in H has the same endpoints as it has in G.

Example

List all subgraphs of the graph G with vertex set $\{v_1, v_2\}$ and edge set $\{e_1, e_2, e_3\}$ where the endpoints of e_1 are v_1 and v_2, the endpoints of e_2 are v_1 and v_2 and e_3 is a loop at v_1.

Solution
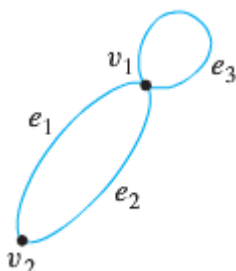
There are 11 subgraphs of G, which can be grouped according to those that do not have any edges, those that have one edge, those that have 2 edges, and those that have 3 edges.

232

1 2 3 4 5 6

7 8 9 10 11
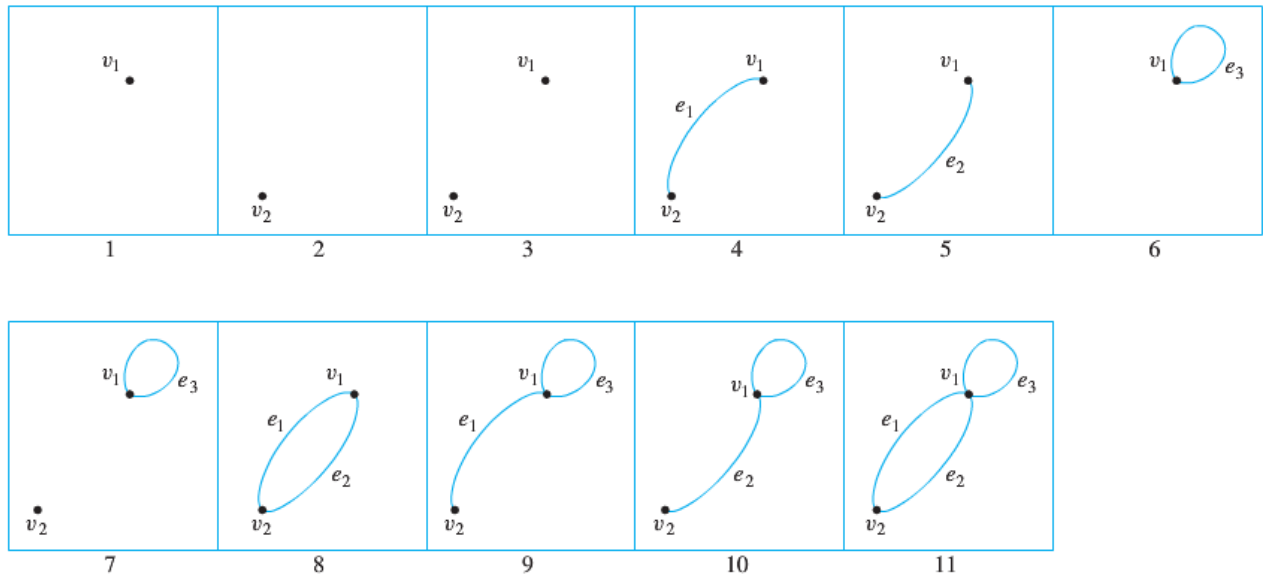
The concept of Degree

Definition

Let G be a graph and v a vertex of G. The ***degree of v***, denoted $\deg(v)$, equals the number of edges that are incident on v, with an edge that is a loop counted twice. The *total degree* of G is the sum of the degrees of all vertices of G.

The degree of this vertex equals 5.
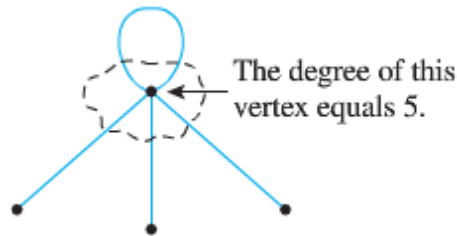
Example

Find the degree of each vertex of the graph G shown below. Then find the total degree of G.

Solution

$\deg(v_1) = 0$ since no edge is incident on v_1 $\left(v_1 \text{ is isolated}\right)$

$\deg(v_2) = 2$ since both e_1 and e_2 are incident on v_2

$\deg(v_3) = 4$ since both e_1 and e_2 are incident on v_3 and the loop e_3 is also incident on v_3

(contributes 2 to the degree of v_3)

Total degree of $G = \deg(v_1) + \deg(v_2) + \deg(v_3) = 0 + 2 + 4 = 6$

233
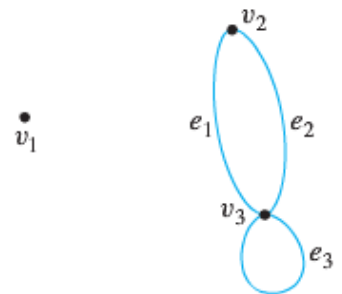
The Handshake *Theorem*

If G is any graph, then the sum of the degrees of all the vertices of G equals twice the number of edges of G. Specially, if the vertices of G are v_1, v_2, …, v_n, where n is a nonegative integer, then

$$\text{The total degree of } G = \deg(v_1) + \deg(v_2) + \ldots + \deg(v_n)$$
$$= 2 \cdot (\text{the number of edges of } G)$$

Corollary

The total degree of a graph is even.

Example

Draw a graph with the specified properties or show that no such graph exists.
- a) A graph with four vertices of degrees 1, 1, 2, and 3
- b) A graph with four vertices of degrees 1, 1, 3, and 3
- c) A simple graph with four vertices of degrees 1, 1, 2, and 3

Solution

- a) No such graph is possible. By Corollary, the total degree of a graph is even.
  But a graph with four vertices of degrees 1, 1, 2, and 3 would have a total degree of
  $1 + 1 + 2 + 3 = 7$ which is odd.
- b) Let G be any of the graphs shown below
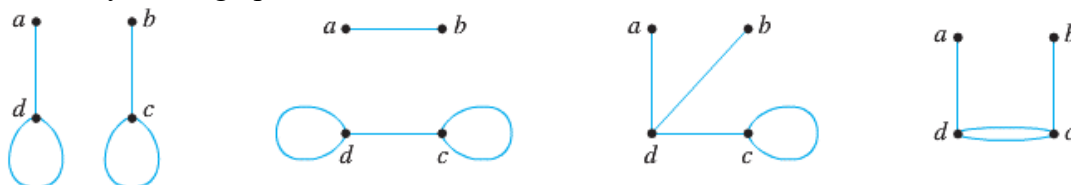
  In each case, no matter how the edges are labeled, $\deg(a) = \deg(b) = 1$ and $\deg(c) = \deg(d) = 3$
- c) There is no simple graph with four vertices of degrees 1, 1, 3, and 3.

Example

Is it possible in a group of 9 people for each to be friends with exactly five others?

Solution

Imagine constructing an "acquaintance graph" in which each of the nine people represented by a vertex and 2 vertices are joined by an edge if, and only if, the people they represent are friends. Suppose each of the people were friends with exactly five others. Then the degree of each of the 9 vertices of the graph would be 5, and so the total degree of the graph would be **45** (*odd*). Contradicts Corollary, which says that the total degree of a graph is even.
Therefore, the answer is no.

Example

A tournament where each team plays every other team exactly once and no ties are allowed is called a round-robin tournament. Such tournaments can be modeled using directed graphs where each team is represented by a vertex, Note that (a, b) is an edge if team a beats team b. This graph is a simple directed graph, containing no loops or multiple directed edges (because no 2 teams play each other more than once. Such a directed graph model is presented
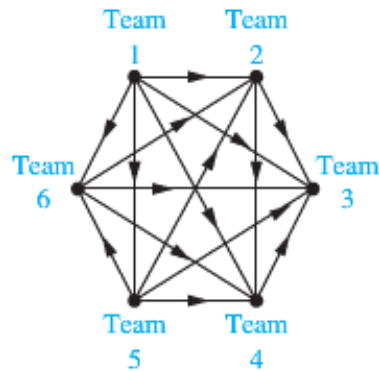
We see that team 1 is undefeated in this tournament, and Team 3 is winless.

Exercises *Section* **4.6** − **Graphs: Definitions and Basic Properties**

1. Determine whether the graph shown has directed or undirected edges, whether it has multiple edges, and whether it has one or more loops.

a)
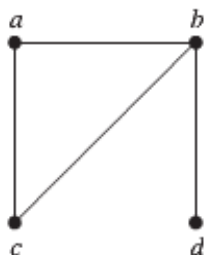
b)
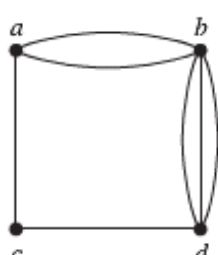
c)
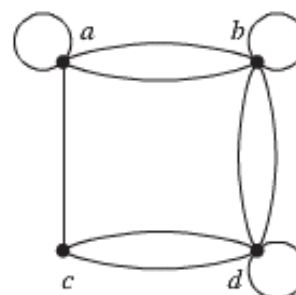
d)
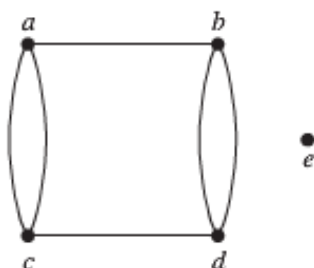
e)
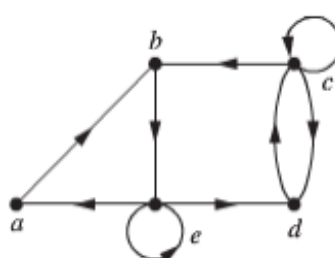
f)
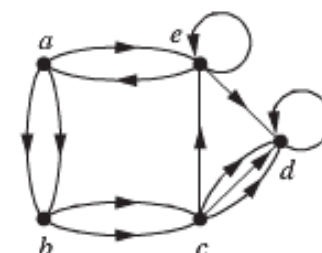
g)
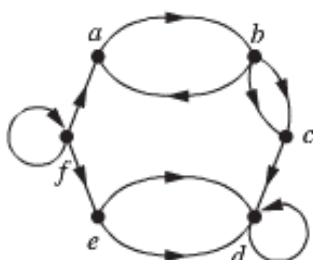
2. Define each graph formally by specifying its vertex set, its edge set, and a table giving the edge-endpoint function

a)
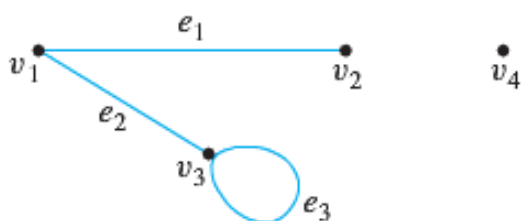
b)
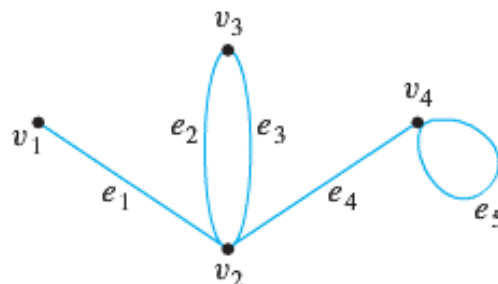
3. Graph G has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and edge set $\{e_1, e_2, e_3, e_4\}$, with edge-endpoint function as follow

Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_2\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_2\}$

4. Graph H has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and edge set $\{e_1, e_2, e_3, e_4\}$, with edge-endpoint function as follow

Edge	Endpoints
e_1	$\{v_1\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_1, v_5\}$

5. Show that the 2 drawings represent the same graph by labeling the vertices and edges of the right-hand drawing to correspond to those of the left-hand drawing.

   a)

   b)

   c)

237
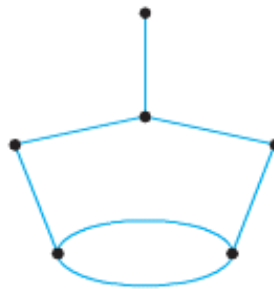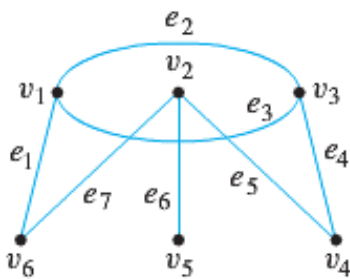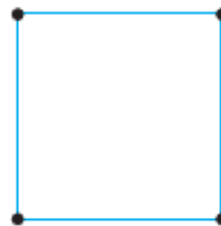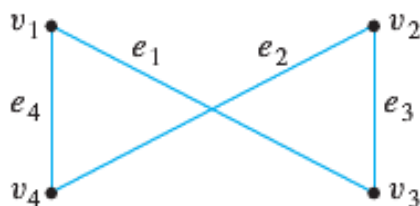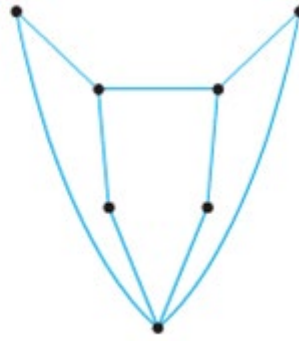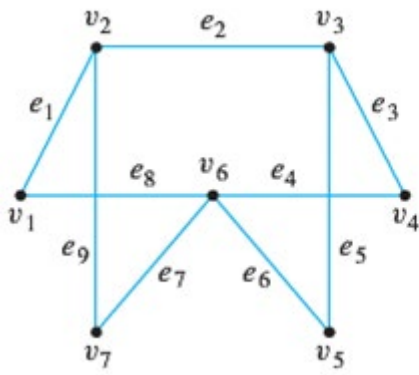
6. For each of the graphs

   i. Find all edges that are incident on v_1

   ii. Find all vertices that are adjacent to v_3

   iii. Find all edges that are adjacent to e_1

   iv. Find all loops
   v. Find all parallel edges
   vi. Find all isolated vertices
   vii. Find the degree of v_3

   viii. Find the total degree of the graph
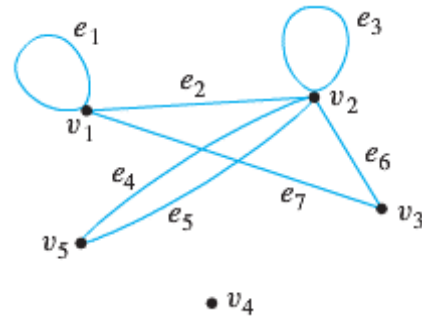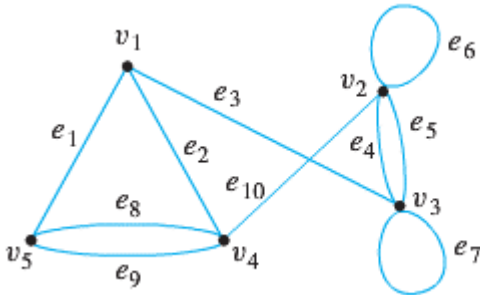
7. Let G be a simple graph. Show that the relation R on the set of vertices of G such that uRv if and only if there is an edge associated to $\{u, v\}$ is a symmetric, irreflexive relation on G.

8. Let G be an undirected graph with a loop at every vertex. Show that the relation R on the set of vertices of G such that uRv if and only if there is an edge associated to $\{u, v\}$ is a symmetric, reflexive relation on G.

9. Explain how graphs can be used to model electronic mail messages in a network. Should the edges be directed or undirected? Should multiple edges be allowed? Should loops be allowed? Describe a graph that models the electronic mail sent in a network in a particular week.

10. A bipartite graph G is a simple graph whose vertex set can be portioned into two disjoint nonempty subsets V_1 and V_2 such that vertices in V_1 may be connected to vertices in V_2, but no vertices in

V_1 are connected to other vertices in V_1 and no vertices in V_2 are connected to other vertices in V_2. For example, the graph G illustrated in (*i*) can be redrawn as shown in (*ii*). From the drawing in (*ii*), you can see that G is bipartite with mutually disjoint vertex set $V_1 = \{v_1, v_3, v_5\}$ and

$V_1 = \{v_2, v_4, v_6\}$

(*i*)

(*ii*)

a)

b)

c)

d)

e)

f)
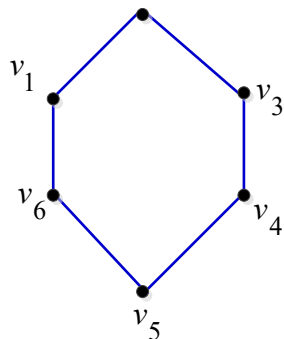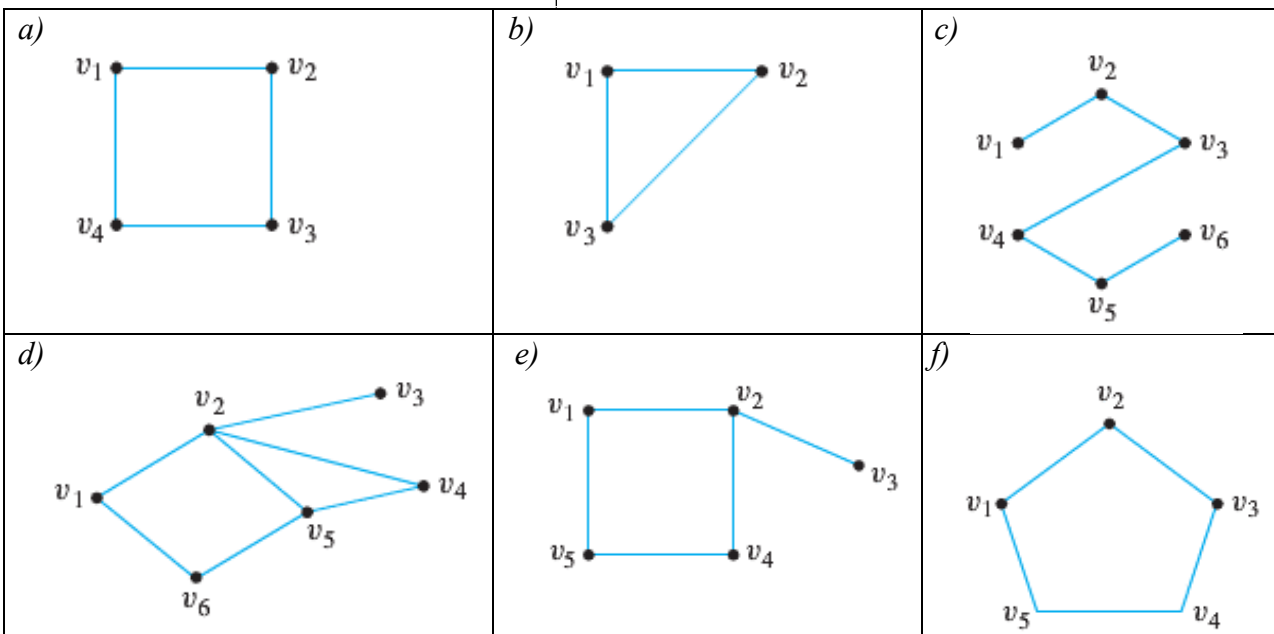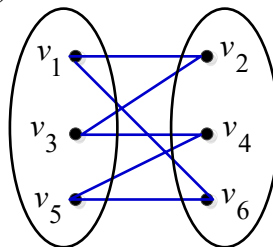
Section 4.7 – Representing Graphs and Graph Isomorphism

Sometimes, two graphs have exactly the same form, in the sense that there is a one-to-one correspondence between their vertex sets that preserves edges. In such case, we say that the two graphs are isomorphic.

Adjacency

Use the adjacency lists to describe the given graph
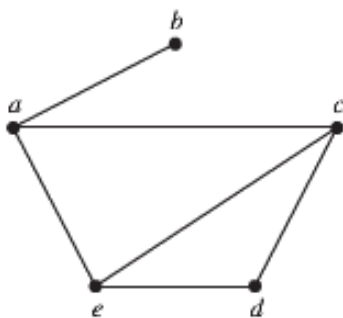
Adjacency List for a Simple Graph	
Vertex	*Adjacent Vertices*
a	b, c , e
b	a
c	a, d, e
d	c, e
e	a, c , d
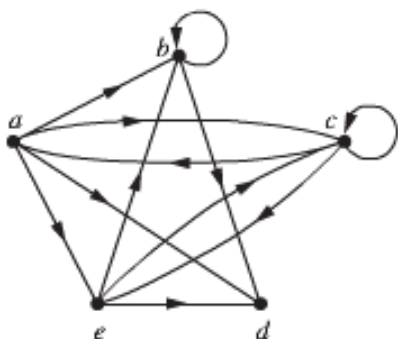
Adjacency List for a Directed Graph	
Initial Vertex	*Terminal Vertices*
a	b, c, d, e
b	b, d
c	a, c, e
d	
e	b, c , d

Adjacency Matrices

Suppose that $G = (V, E)$ is a simple graph where $|V| = n$. Suppose that the vertices of G are listed arbitrary as $v_1, v_2, \ldots, v_n$. The adjacency matrix A $\left(or\ A_G \right)$ of G, with respect to this listing of the vertices, is the $n \times n$ zero-one matrix with 1 as its $(i, j)th$ entry when v_i and v_j are adjacent, and 0 as its $(i, j)th$ entry when they are not adjacent.

$$a_{ij} = \begin{cases} 1 & if\ \{v_i, v_j\}\ is\ an\ edage\ of\ G \\ 0 & otherwise \end{cases}$$

Example

Draw a graph with the adjacency matrix

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$ with respect to the ordering of vertices *a, b, c, d.*

Solution

Example

Use an adjacency matrix to represent the pseudograph shown below.
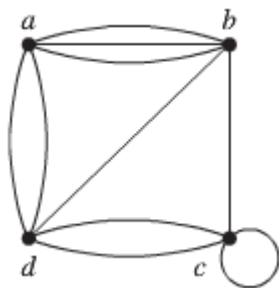
Solution

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

Incidence Matrices

Let $G = (V, E)$ be undirected graph. Suppose that $v_1, v_2, \ldots, v_n$ are the vertices and $e_1, e_2, \ldots, e_n$ are the edges of G. Then the incident matrix with respect to this ordering of V and E is the $n \times m$ matrix

$M = \begin{bmatrix} m_{ij} \end{bmatrix}$, where

$$m_{ij} = \begin{cases} 1 & \text{when edge } e_j \text{ is incident with } v_i \\ 0 & \text{otherwise} \end{cases}$$

Example

Represent the graph shown with an incidence matrix.

Solution

The incidence matrix is

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{cccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix} \end{array}$$
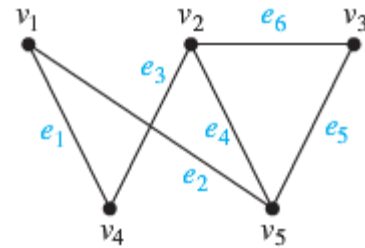
Example

Represent the graph shown below with an incidence matrix.
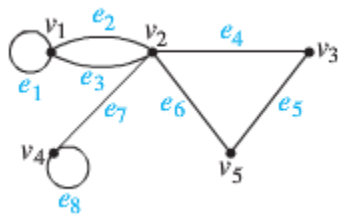
Solution

The incidence matrix is

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{array} \begin{array}{cccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 \\ \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Isomorphism of Graphs

Definition

The simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there exists a one-to-one and onto function f from V_1 to V_2 with the property that a and b are adjacent in G_1 if and only if $f(a)$ and $f(b)$ are adjacent in G_2, for all a and b in V_1. Such a function f is called an **isomorphism**. Two simple graphs that are not isomorphic are called **nonisomorphic**.

Example

Show that the graphs $G = (V, E)$ and $H = (V, E)$, displayed below are isomorphic
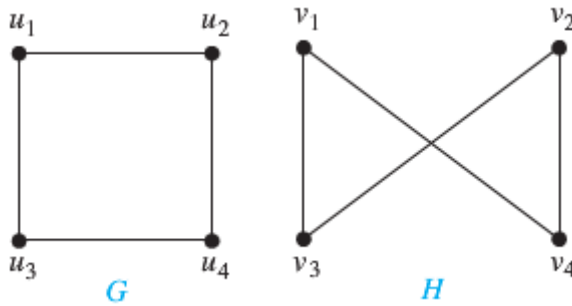
Solution

The function f with $f(u_1) = v_1$, $f(u_2) = v_2$, $f(u_3) = v_3$, and $f(u_4) = v_4$ is a one-to-one correspondence between V and W. To see that this correspondence preserves adjacency, note that adjacent vertices in G are u_1 *and* u_2, u_1 *and* u_3, u_2 *and* u_4, and u_3 *and* u_4, and each of the pairs

$f(u_1) = v_1$ and $f(u_2) = v_4$, $f(u_1) = v_1$ and $f(u_3) = v_3$, $f(u_2) = v_4$ and $f(u_4) = v_2$,

$f(u_3) = v_3$ and $f(u_4) = v_2$ consists of two adjacent vertices in H.

$\therefore$ If we flip v_2 & v_4, we end up the same graph.

Determining whether Two Simple Graphs are Isomorphic

Sometimes it is not hard to show that two graphs are not isomorphic. In Particular, we can show that two graphs are not isomorphic if we can find a property only one of the two graphs has, but that is preserved by isomorphism. A property preserved by isomorphism of graphs is called a ***graph invariant***.

Example

Show that the graphs shown below are not isomorphic
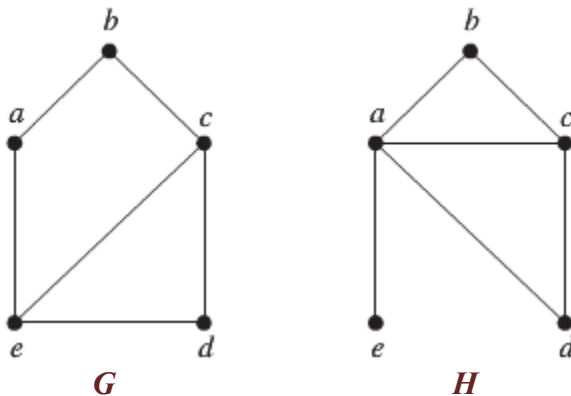
Solution

Both graphs *G* & *H* have 5 vertices and 6 edges.
H has a vertex of degree one, @ *e*, whereas *G* has no vertices of degree one.
It follows that *G* & *H* are not isomorphic.

Example

Determine whether the graphs shown below are isomorphic
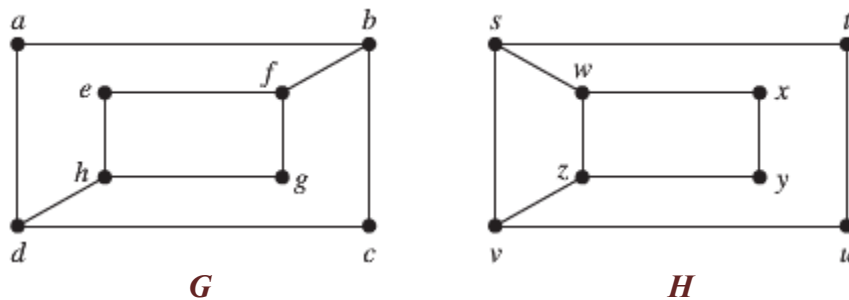
Solution

Both graphs *G* & *H* have 8 vertices and 10 edges.
Also both have 4 vertices of degree 2 and 4 vertices of degree 3.
$\deg(a) = 2$ in *G*, *a* must correspond to either *t, u ,x*, or *y* in *H*, because these are the vertices of degree 2 in *H*. However, each of these four vertices in *H* is adjacent to another vertex of degree 2 in *H*, which is not true for *a* in *G*. Therefore, *G* & *H* are not isomorphic.

Another way to see that G & H are not isomorphic is by checking the subgraphs of G & H shown below, they have a different shape.
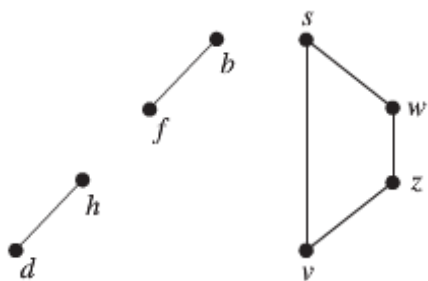
Example

Determine whether the graphs shown below are isomorphic

G	H
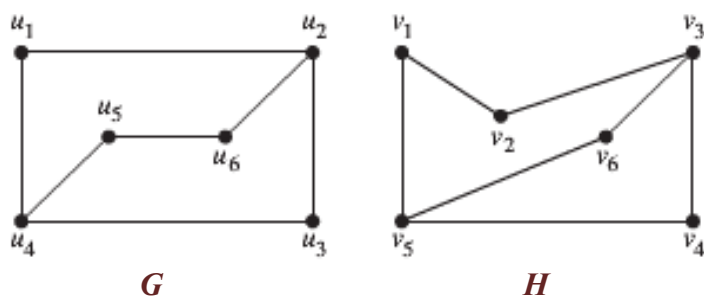
Solution

Both graphs G & H have 6 vertices and 7 edges.

Also both have 4 vertices of degree 2 and 2 vertices of degree 3.

From the subgraphs of G & H, all vertices of degree 2 and the edges connecting them are isomorphic.

$$u_1 \leftrightarrow v_6 \quad u_4 u_5 u_6 u_2 \leftrightarrow v_5 v_1 v_2 v_3$$

Exercises   *Section* 4.7 − **Representing Graphs and Graph Isomorphism**

Use the adjacency list to represent the given graph, then represent with an adjacency matrix

1.
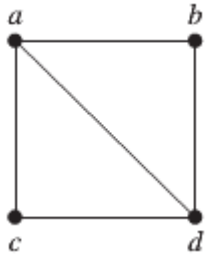
2.
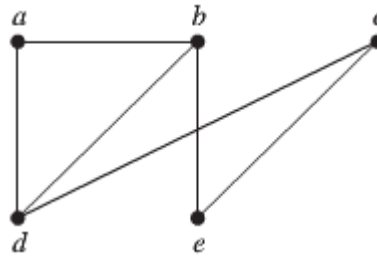
3.
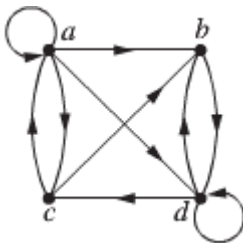
4.
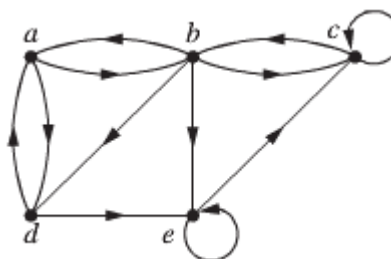
5.   Draw a graph with the given adjacency

a) $\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

b) $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

c) $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

6.   Represent the given graph using adjacency matrix

a)
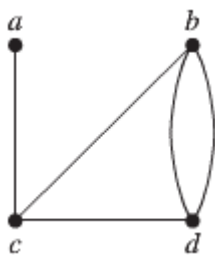
b)
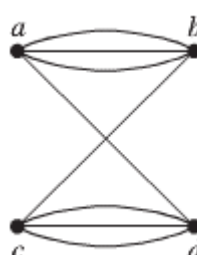
c)
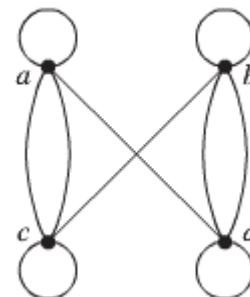
7.   Draw an undirected graph represented by the given adjacency

a) $\begin{bmatrix} 1 & 3 & 2 \\ 3 & 0 & 4 \\ 2 & 4 & 0 \end{bmatrix}$

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

c) $\begin{bmatrix} 0 & 1 & 3 & 0 & 4 \\ 1 & 2 & 1 & 3 & 0 \\ 3 & 1 & 1 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$

8. Find the adjacency matrix of the given directed multigraph with respect to the vertices listed in alphabetic order.

a)
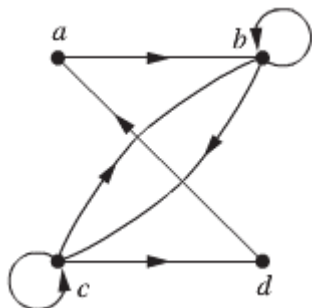
b)
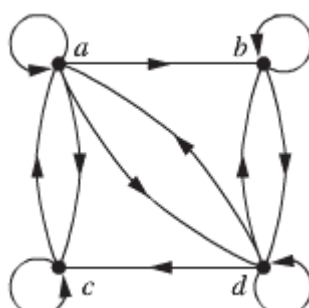
c)
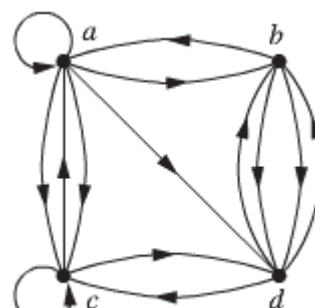
Determine whether the given pair of graphs is isomorphic. Exhibit an isomorphism or provide a rigorous argument that none exists.

9.
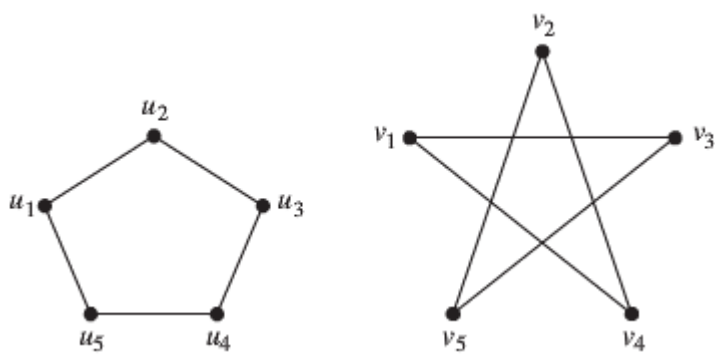
10.
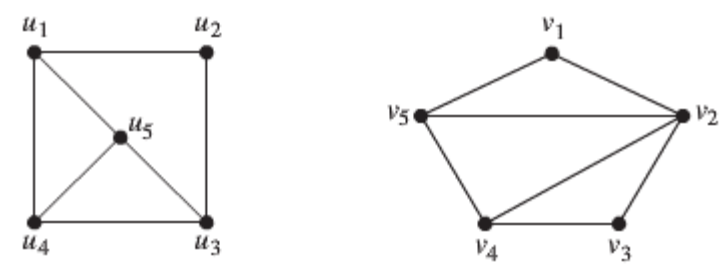
11.
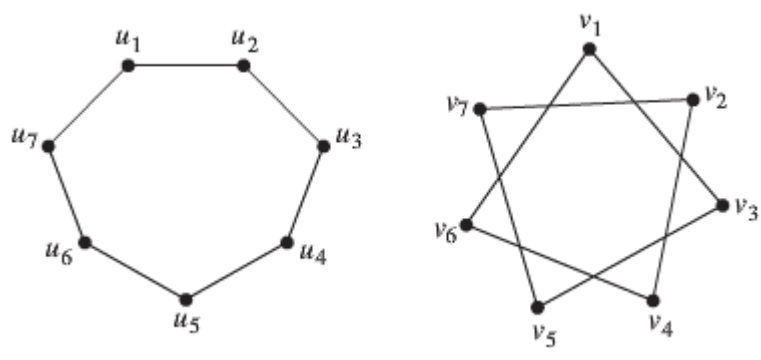
12.
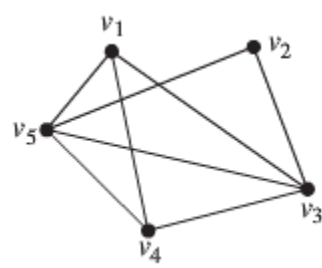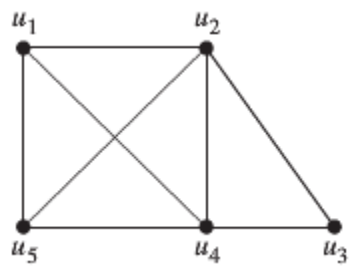
Section **4.8 − Connectivity**

Paths

A path is a sequence of edges that begins at a vertex of a graph and travels from vertex to vertex along edges of the graph.

Definitions

Let G be a graph, and let v and w be vertices in G.

A ***walk*** from v to w is a finite alternating sequence of adjacent vertices and edges of G. Thus a walk has the form

$$v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n$$

Where the v's represent vertices, the e's represents edges, $v_0 = v$, $v_n = w$ and for all $i = 1, 2, \ldots, n$, v_{i-1} *and* v_i are the endpoints of e_i. The trivial walk from v to v consists of the single vertex v.

A ***trail*** from v to w is a walk from v to w that does not contain a repeated edge.

A ***closed walk*** is a walk that starts and ends at the same vertex.

A ***circuit*** is a closed walk that contains at least one edge and does not contain a repeated edge.

A ***simple circuit*** is a circuit that does not any other repeated vertex except first and last.

	Repeated Edge?	**Repeated Vertex**	**Starts & Ends at Same Point?**	**Must Contain at Least One Edge?**
Walk	Allowed	Allowed	Allowed	No
Trail	No	Allowed	Allowed	No
Path	No	No	No	No
Closed Walk	Allowed	Allowed	Yes	Yes
Circuit	No	Allowed	Yes	Yes
Simple Circuit	No	First & last only	Yes	Yes

Notation for Walks
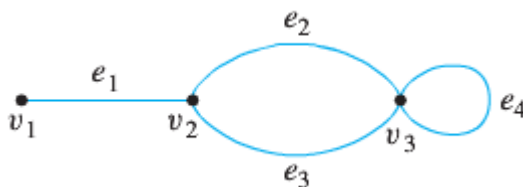
The notation $e_1 e_2 e_4 e_3$ refers unambiguous to the following walk: $v_1 e_1 v_2 e_2 e_4 v_3 e_3 v_2$. On the other hand, the notation e_1 is ambiguous if used to refer to a walk. It could mean either $v_1 e_1 v_1$ or $v_2 e_1 v_1$.

The notation $v_2 v_3$ is ambiguous if used to refer to a walk. It could mean $v_2 e_2 v_3$ or $v_2 e_3 v_3$. On the other hand,
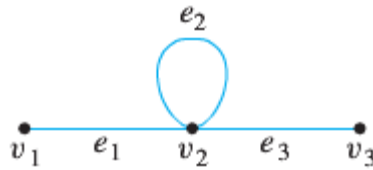
The notation $v_1v_2v_2v_3$ refers unambiguously to the walk $v_1e_1v_2e_2v_2e_3v_3$

Example

Determine which of the following walks are trails, paths, circuits, or simple circuits to the graph below.

a) $v_1e_1v_2e_3v_3e_4v_3e_5v_4$

b) $e_1e_3e_5e_5e_6$

c) $v_2v_3v_4v_5v_3v_6v_2$

d) $v_2v_3v_4v_5v_6v_2$

e) $v_1e_1v_2e_1v_1$

f) v_1
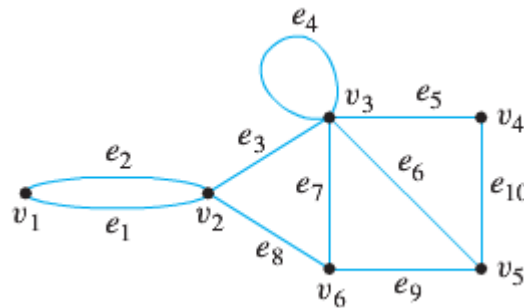
<u>Solution</u>

a) This walk has a repeated vertex but does not have a repeated edge, so it is a trail from v_1 to v_4 but not a path.

b) This is just a walk from v_1 to v_5. It is not a trail because it has a repeated edge.

c) This walk starts and ends at v_2, contains at least one edge, and does not have a repeated edge, so it is a circuit. Since the vertex v_3 is repeated in the middle, it is not a simple circuit.

d) This walk starts and ends at v_2, contains at least one edge, and does not have a repeated edge, and does not have a repeated vertex. Thus it is a simple circuit.

e) This is just a closed walk starting and ending at v_1. It is not a circuit because edge e_1 is repeated.

f) The first vertex of this walk is the same as its last vertex, but it does not contain an edge, and so it is not a circuit, It is a closed walk from v_1 to v_1. (It is also a trail from v_1 to v_1)

Example
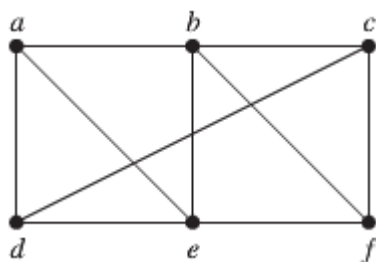
The given graph, *a, d, c, f, e* is a simple path of length 4, because {*a, d*}, {*d, c*}, {*c, f*}, and {*f, e*} are all edges. However, *d, e, c, a* is not a path, because {*e, c*} is not an edge.

Note that *b, c, f, e, b* is a circuit of length 4 because {*b, c*}, {*c, f*}, {*f, e*}, and {*e, b*} are edges, and this path begins and ends at *b*. The path *a, b, e, d, a, b*, which is of length 5, is not simple because it contains the edge {*a, b*} twice.

Connectedness

Definition

Let *G* be a graph. Two vertices *v* and *w* of *G* are ***connected*** if, and only if, there is a walk from *v* to *w*. The graph *G* is connected if, and only if, given any two vertices *v* and *w* in *G*, there is a walk from *v* to *w*. Symbolically,

$$G \text{ is connected} \iff \forall \text{ vertices } v, w \in V(G), \exists \text{ a walk from } v \text{ to } w.$$

Definition

An undirected graph is called ***connected*** if there is a path between every pair of distinct vertices of the graph. An undirected graph that is not *connected* is called ***disconnected***. We say that we *disconnect* a graph when we remove vertices or edges, or both, to produce a disconnected subgraph.

Example
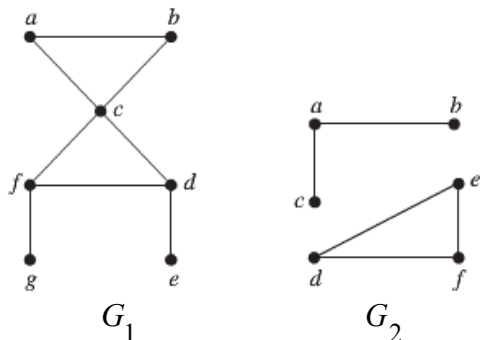
The graph G_1 is connected, because for every pair of distinct vertices there is a path between them.

However, the graph G_2 is not connected. For instance, there is no path in G_2 between vertices *a* and *b*.

Connected and Disconnected Graphs

Example

Which of the following graphs are connected?
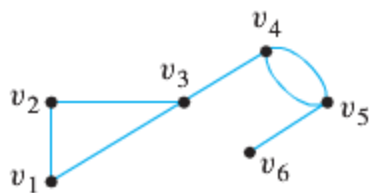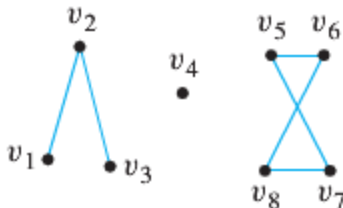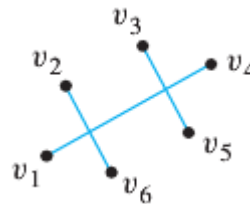
(a)   (b)   (c)

Solution

The graph represented in (a) is connected, whereas those of (b) and (c) are not.
To understand why (c) is not connected, two edges may cross at a point that is not a vertex.
Thus the graph in (c) can be drawn as follows:
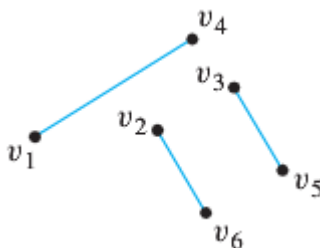
Theorem

There is a simple path between every pair distinct vertices of a connected undirected graph.

Proof

Let u and v be two distinct vertices of the connected undirected graph $G = (V, E)$. Because G is connected, there is at least one path between u and v. Let x_0, x_1, ..., x_n where $x_0 = u$ and $x_n = v$, be the vertex sequence of a path of least length. This path of least length is simple. To see this, suppose it is not simple. Then $x_i = x_j$ for some i and j with $0 \le i < j$. This means that there is a path from u to v of shorter length with vertex sequence x_0, x_1, ..., x_{i-1} x_j, ..., x_n obtained by deleting the edges corresponding to the vertex sequence x_i, ..., x_{j-1}

Definition

A graph H is a connected component of a graph G if, and only if,
- H is subgraph of G;
- H is connected; and
- No connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H.

Example

What are the connected components of the graph H shown below?
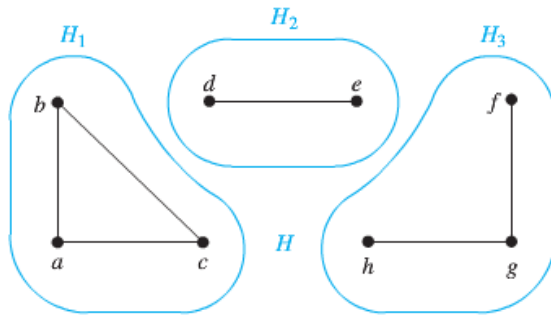
Solution

The graph H is the union of the three disjoint connected subgraphs H_1, H_2, *and* H_3. These three subgraphs are the connected components of H.

Example

Find all connected components of the following graph G.
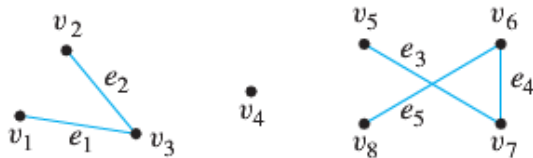
Solution

G has three connected components: H_1, H_2, *and* H_3 with vertex sets V_1, V_2, *and* V_3 and edges E_1, E_2, *and* E_3, where

$$V_1 = \{v_1, v_2, v_3\} \qquad E_1 = \{e_1, e_2\}$$

$$V_2 = \{v_4\} \qquad E_2 = \varnothing$$

$$V_3 = \{v_5, v_6, v_7, v_8\} \qquad E_3 = \{e_3, e_4, e_5\}$$

Example

Find the cut vertices and cut edges in the graph G.

G
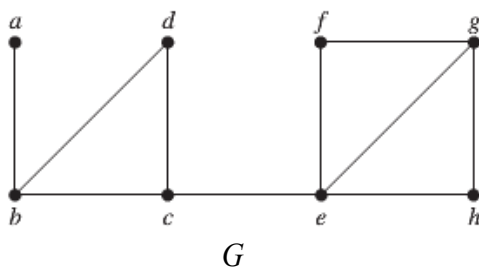
Solution

The cut vertices of G are b, c, and e. The removal of one of these vertices (and its adjacent edges) disconnects the graph. The cut edges are $\{a, b\}$ and $\{c, e\}$. Removing either one of these edges disconnects G.

Definition

A directed graph is weakly connected of there is a path between every two vertices in the underlying undirected graph.

Example

Are the directed graphs G and H shown below strongly connected? Are they weakly connected?

G   H
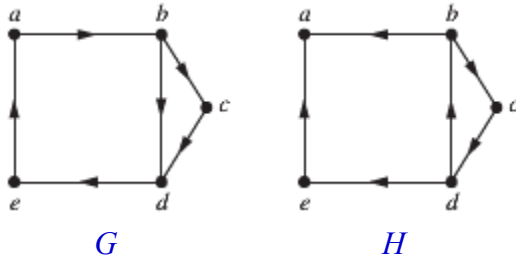
Solution

G is strongly connected because there is a path between any two vertices in this directed graph. Hence, G is also weakly connected.

The graph H is not strongly connected. There is no directed path from a to b in this graph. However, H is weakly connected, because there is a path between any 2 vertices in the underlying undirected graph of H.

Exercises   *Section* 4.8 – **Connectivity**

1. Does each of these lists of vertices form a path in the following graph? Which paths are simple? Which are circuits? Which are the lengths of those that are paths?
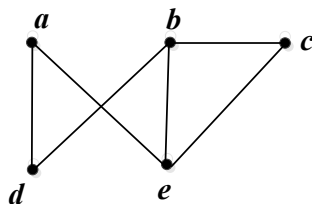
a) *a, e, b, c, b*   **b)** *a, e, a, d, b, c, a*   **c)** *e, b, a, d, b, e*   **d)** *c, b , d, a, e, c*

2. Does each of these lists of vertices form a path in the following graph? Which paths are simple? Which are circuits? Which are the lengths of those that are paths?
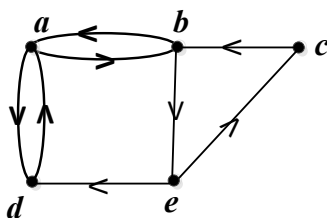
a) *a, b, e, c, b*   **b)** *a, d, a, d, a*   **c)** *a, d, b, e, a*   **d)** *a, b , e, c, b, d, a*

3. Determine whether of the following walks are trails, paths, circuits, or simple circuits or just walk to the graph below.
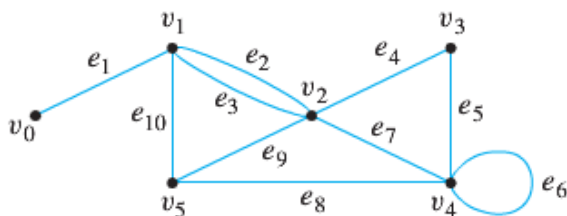
a) $v_0 e_1 v_1 e_{10} v_5 e_9 v_2 e_2 v_1$ **b)** $v_4 e_7 v_2 e_9 v_5 e_{10} v_1 e_3 v_2 e_9 v_5$ **c)** v_2

d) $v_5 v_2 v_3 v_4 v_4 v_5$ **e)** $v_2 v_3 v_4 v_5 v_2 v_4 v_3 v_2$ **f)** $e_5 e_8 e_{10} e_3$

4. Determine whether of the following walks are trails, paths, circuits, or simple circuits or just walk to the graph below.
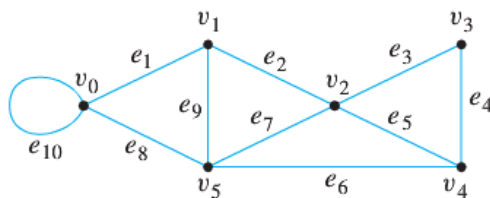
a) $v_1 e_2 v_2 e_3 v_3 e_4 v_4 e_5 v_2 e_2 v_1 e_1 v_0$ **b)** $v_2 v_3 v_4 v_5 v_2$ **c)** $v_4 v_2 v_3 v_4 v_5 v_2 v_4$

d) $v_2 v_1 v_5 v_2 v_3 v_4 v_2$ **e)** $v_0 v_5 v_2 v_3 v_4 v_2 v_1$ **f)** $v_5 v_4 v_2 v_1$

Section 4.9 – **Euler and Hamilton Paths**

The town of *Königsberg* was divided into 4 sections by the branches of the Pregel River. The town people took long walks through town. They wondered whether it was possible to start at some location in the town, travel across all the bridges once without crossing and bridge twice, and return to the starting point.
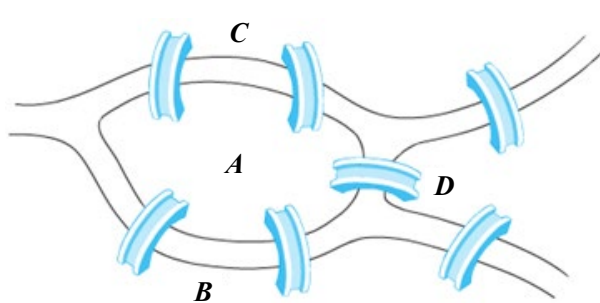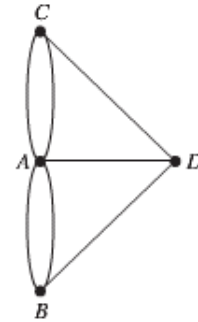
Königsberg Town   *Multigraph*

The Swiss mathematician Leonhard Euler solved this problem. His solution, published in 1736, may be the first use of graph theory. Euler studied this problem using the multigraph obtained when the four regions are represented by vertices and the bridges by edges.

Definition

Let G be a graph. An Euler Circuit for G is a circuit that contains every vertex and every edge of G. That is, an Euler circuit for G is a sequence of adjacent vertices and edges in G that has at least one edge, starts and ends at the same vertex, uses every vertex of G at least once, and uses every edge of G exactly once.

Theorem

A connected multigraph with at least two vertices has an Euler circuit if and only if each of its vertices has even degree.

Theorem

A connected multigraph has Euler path but not an Euler circuit if and only if it has exactly 2 vertices of odd degree.

Example

Which of the undirected graph have Euler circuit? Of those that do not, which have an Euler path?

G_1 G_2 G_3
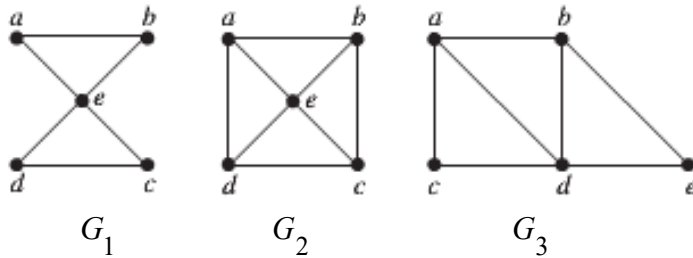
Solution

The graph G_1 has Euler circuit, for example, *a, e, c, d, e, b, a*.

G_2 & G_3 do not have Euler circuit. Because vertices *a, b, c, d* of G_2 & *a, b* of G_3 have degree 3

G_3 has an Euler path, *a, c, d, e, b, d, a, b*. G_2 does not have Euler path.

Example

Which of the undirected graph have Euler circuit? Of those that do not, which have an Euler path?

G_1 G_2 G_3
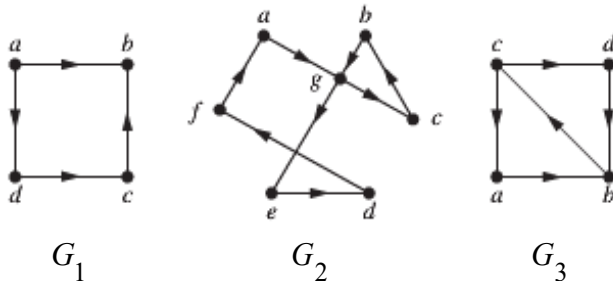
Solution

The graph G_2 has Euler circuit, for example, *a, g, c, b, g, e, d, f, a*.

G_1 & G_3 do not have Euler circuit. Because vertices *a, b, c, d* of G_1 have degree 1 (*odd*) & *c, b* of G_3 have degree 3

G_3 has an Euler path, *c, a, b, c, d, b*. but G_1 does not have Euler path.

Example

Show that the graph below does not have an Euler circuit

Solution

257
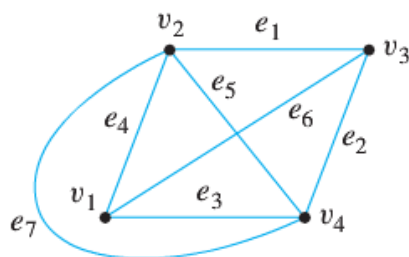
Vertices v_1 & v_3 both have degree 3, which is odd. Hence by the contrapositive form, this graph does not have an Euler circuit.

Definition

Let *G* be a graph, and let *v* and *w* be two distinct vertices of *G*. An Euler trail from *v* to *w* is a sequence of adjacent edges and vertices that starts at *v*, ends at *w*, passes through every vertex of *G* at least once, and traverses every edge of *G* exactly once.

Example

Many puzzles ask you to draw a picture in a continuous motion without lifting a pencil so that no part of the picture is retraced. We can solve such puzzles using Euler circuits and paths. For example, can Mohammed's scimitars, shown in Figure below, be drawn in this way, where the drawing begins and ends at the same point?
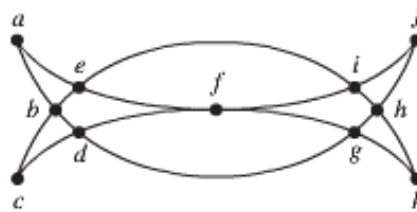
Solution

Let denote G for the graph. G has an Euler circuit, because all its vertices have even degree.
1. Form the circuit: *a, b, d, c, b, e, i, f, e, a*. We obtain the subgraph *H* by deleting the edges in this circuit and all vertices that become isolated when these edges are removed.
2. Form: *d, g, h, j, i, h, k, g, f, d* in H. After forming this circuit we have used all edges in G. Splicing this new circuit into the first circuit at the appropriate place produces the Euler circuit *a, b, d, g, h, j, i, h, k, g, f, d, c, b, e, i, f, e, a*. This circuit gives a way to draw the scimitars without lifting the pencil or retracting part of the picture.

Hamilton Path and Circuits

A simple path in a graph G that passes through every vertex exactly once is called a **Hamilton path**, and a simple circuit G in a graph G that passes through every vertex exactly once is called a *Hamilton circuit*. That is, the simple path $x_0, x_1, \ldots, x_{n-1}, x_n$ in the graph $G = (V, E)$ is a Hamilton path if

$V = \{x_0, x_1, \ldots, x_{n-1}, x_n\}$ and $x_i \neq x_j$ for $0 \leq i < j \leq n$, and the simple circuit

$x_0, x_1, \ldots, x_{n-1}, x_n, x_0$ (with $n > 0$) is a Hamilton circuit if $x_0, x_1, \ldots, x_{n-1}, x_n$ is a Hamilton path.
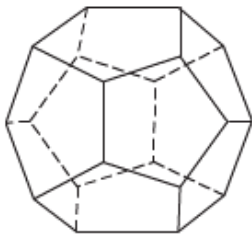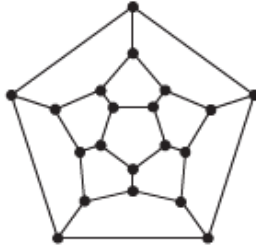
(a)   (b)

Hamilton's "A Voyage Round the World" Puzzle   *Solution to the "A Voyage Round the World" Puzzle*
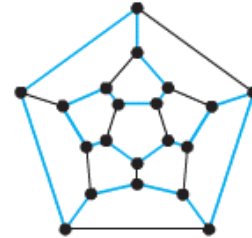
Example

Which of the simple given graphs have a Hamilton circuit or, if not, a Hamilton path?
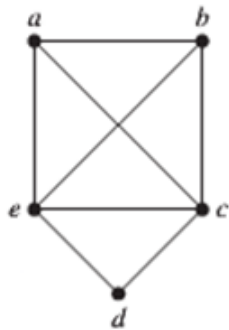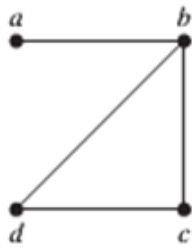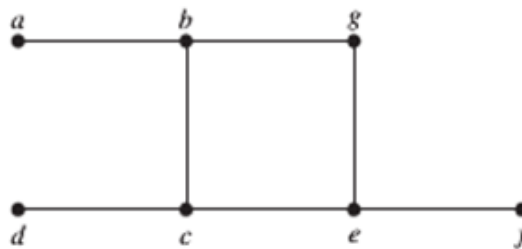
G_1 G_2 G_3

Solution

G_1 has a Hamilton circuit: *a, b, c, d, e, a*.

There is no Hamilton circuit in G_2, every vertex contain the edge *{a, b}* twice, but G_2 does have a Hamilton path, namely *a, b, c, d*.

G_3 has neither a Hamilton circuit nor a Hamilton path, because any path containing all vertices must contain one of the edges *{a, b}*, *{e, f}*, and *{c, d}* more than once.

Example

Show that K_n has a Hamilton circuit whenever $n \geq 3$.

<u>*Solution*</u>

We can form a Hamilton circuit in K_n beginning at any vertex. Such a circuit can be built by visiting vertices in any order we choose, as long as the path begins and ends at the same vertex and visits each other vertex exactly once. This is possible because there are edges in K_n between any two vertices.

Exercises   *Section* 4.9 − **Euler and Hamilton Paths**

Determine whether the given graph has an Euler circuit. Construct such a circuit when one exists. If no Euler circuit exists, determine whether the graph has an Euler path and construct such a path if one exists.

1.
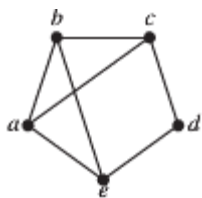
2.
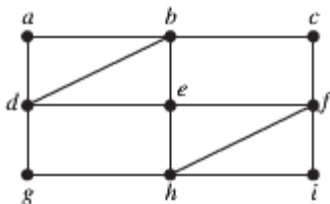
3.
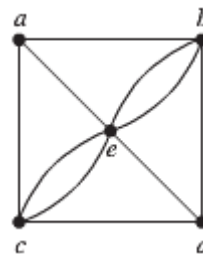
4.
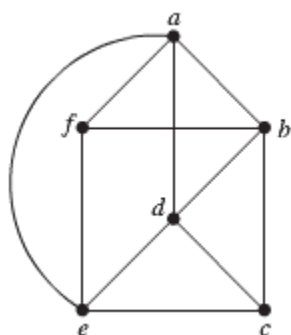
5.
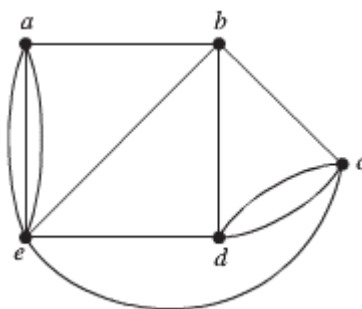
6.
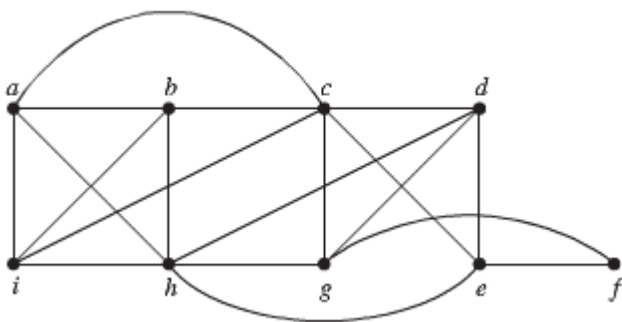
7.
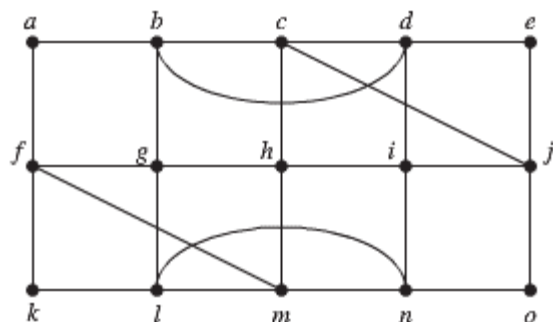
8. Can someone cross all the bridges shown in this map exactly once and return to the starting point?
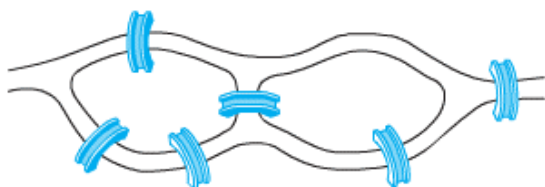
Determine whether the picture shown can be drawn with a pencil in a continuous motion without lifting the pencil or retracing part of the picture

9.

10.

11.
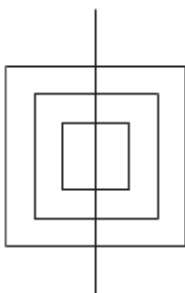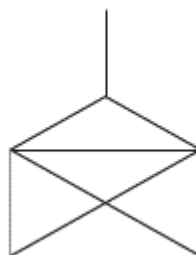
Determine whether the given graph has a Hamilton circuit. If it does, find such a circuit. If it does not, give an argument to show why no such circuit exists.
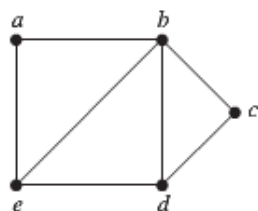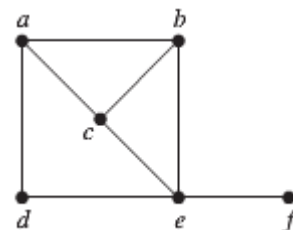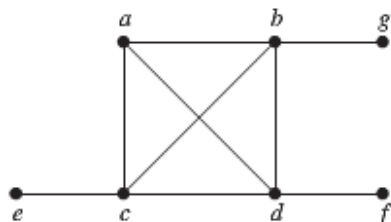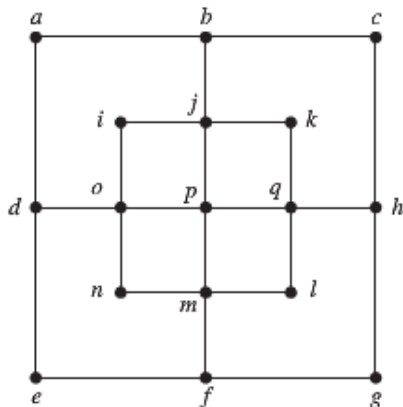
12.
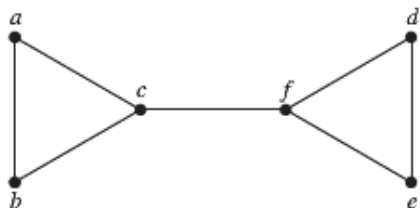
13.
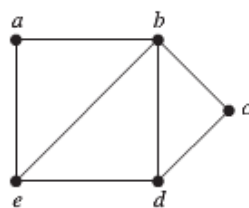
14.

15.

16.

17.

18. Imagine that the drawing below is a map showing 4 cities and the distances in kilometers between them. Suppose that a salesman must travel to each city exactly once, starting and ending in city A. Which route from city to city will minimize the total distance that must be traveled?