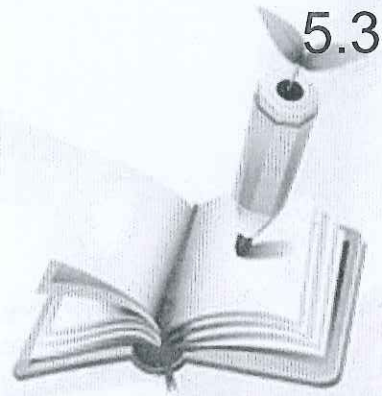
Chapter 5: Sequences, Mathematical Induction and Recursion

5.3 Mathematical Induction II



Example 1 – Proving a Divisibility Property

Proposition 5.3.1

For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3. → $3 \mid 2^{2n} - 1$ is $P(n)$

Proof (by mathematical induction) $n \geq 0 = P(0) = P(0)$

Identify the property $P(n)$. $P(0) = 3 \mid 2^0 - 1 = 3 \mid 0$ ✓

$2^{2n} - 1$ is divisible by 3 for all integers $n \geq 0 \leftarrow p(n)$

Base step: Show that $P(0)$ is true:

To establish $P(0)$, we must show that

$2^{2 \cdot 0} - 1$ is divisible by 3. $\leftarrow P(0)$

But $2^{2 \cdot 0} - 1 = 2^0 - 1 = 1 - 1 = 0$

and 0 is divisible by 3 because $0 = 3 \cdot 0$. Hence $P(0)$ is true.

Example 1 – Proving a Divisibility Property

Inductive step: Show that for all integers $k \geq 0$, if $P(k)$ is true then $P(k+1)$ is also true:

Let k be any integer with $k \geq 0$, and suppose that

$2^{2k} - 1$ is divisible by 3. $\leftarrow P(k)$ inductive hypothesis

now make $n = k$
$\therefore P(n) = P(k)$
$\therefore 2^{2k} - 1 = 3K \quad (k \in \mathbb{Z})$

By definition of divisibility, this means that

$2^{2k} - 1 = 3r$ for some integer r.

[We must show that P(k + 1) is true. That is:] We must show that

$2^{2(k+1)} - 1$ is divisible by 3. $\leftarrow P(k+1)$

Example 1 – Proving a Divisibility Property

But
$$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\ &= 2^{2k} \cdot 2^2 - 1 && \text{by the laws of exponents} \\ &= 2^{2k} \cdot 4 - 1 \\ &= 2^{2k}(3+1) - 1 \\ &= 2^{2k} \cdot 3 + (2^{2k} - 1) && \text{by the laws of algebra} \\ &= 2^{2k} \cdot 3 + 3r && \text{by inductive hypothesis} \\ &= 3(2^{2k} + r) && \text{by factoring out the 3.} \end{aligned}$$

$3K$

But $2^{2k} + r$ is an integer because it is a sum of products of integers, and so, by definition of divisibility, $2^{2(k+1)} - 1$ is divisible by 3 *[as was to be shown]*.

[Since we have proved the basis step and the inductive step, we conclude that the proposition is true.]

$P(k)\ 5^k + 9 < 6^k$

$P(k+1)\ 5^{k+1} + 9 < 6^{k+1}$

$5^{k+1} + 9 <? 6 \cdot 5^k + 54 < 6^{k+1}$

LHS of $P(k+1)$: $5 \cdot 5^k < 6 \cdot 5^k$

$9 < 54$

$\therefore 5^{k+1} + 9 < 6 \cdot 5^k + 54 < 6^{k+1}$

OR

$5^{k+1} + 9 <? 6^{k+1}$

$= 5 \cdot 5^k + 9$

$< 5 \cdot 5^k + 45 \quad (9 < 45)$

$= 5 \cdot (5^k + 9)$

$< 5 \cdot 6^k$

$< 6 \cdot 6^k$

Example 2 – Proving an Inequality

Proposition 5.3.2

For all integers $n \geq 3$, $2n + 1 < 2^n$.

Proof (by mathematical induction):

Let the property $P(n)$ be the inequality

$$2n + 1 < 2^n. \qquad \leftarrow P(n)$$

Base step: Show that $P(3)$ is true.

To establish $P(3)$, we must show that

Step 1 : $2 \cdot 3 + 1 < 2^3$. $\qquad \leftarrow P(3)$

But

$$2 \cdot 3 + 1 = 7 \quad \text{and} \quad 2^3 = 8 \quad \text{and} \quad 7 < 8.$$

Hence $P(3)$ is true.

Example 2 – Proving an Inequality

Show that for all integers $k \geq 3$, if $P(k)$ is true then $P(k + 1)$ is true:

Suppose that k is any integer with $k \geq 3$ such that

Step 2: $2k + 1 < 2^k$. $\qquad \leftarrow P(k)$ inductive hypothesis Assume true

[We must show that P(k + 1) is true. That is:] We must show that

Step 3 : $2(k + 1) + 1 < 2^{(k+1)}$. Prove

Or, equivalently,

$$2k + 3 < 2^{(k+1)}. \qquad \leftarrow P(k + 1)$$

But

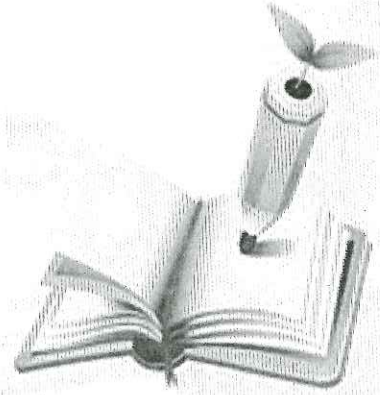
$$\begin{aligned} 2k + 3 &= (2k + 1) + 2 && \text{by algebra} \\ &< 2^k + 2^k && \text{because } 2k + 1 < 2^k \text{ by the inductive hypothesis and because } 2 < 2^k \text{ for all integers } k \geq 2 \\ \bullet\ 2k + 3 &< 2 \cdot 2^k = 2^{k+1} && \text{by the laws of exponents.} \end{aligned}$$

[This is what we needed to show.]

[Since we have proved the basis step and the inductive step, we conclude that the proposition is true.]

Chapter 5: Sequences, Mathematical Induction and Recursion

5.6 Defining Sequences Recursively



Defining Sequences Recursively

A sequence can be defined in a variety of different ways.

- The first few terms: $a_m, a_{m+1}, a_{m+2}, \cdots$, e.g., {3, 5, 7, ...}
- Each term is given by an explicit formula

$$a_n = \frac{(-1)^n}{n+1} \quad \text{for all integers } n \geq 0.$$

- Recursion
  - Recurrent relation: a formula that defines each later term a_k in the sequence by reference to earlier terms $a_{k-i}, a_{k-i+1}, \cdots a_{k-1}$.
  - Initial conditions: one or more initial values for the sequence $a_0, a_1, \cdots a_{i-1}$.

Example 1 – Computing Terms of a Recursively Defined Sequence

Define a sequence $c_0, c_1, c_2, \cdots$ recursively as follows: For all integers $k \geq 2$,

(1) $c_k = c_{k-1} + kc_{k-2} + 1$ recurrence relation

(2) $c_0 = 1$ and $c_1 = 2$ initial conditions.

Find c_2, c_3, and c_4.

Example 1 – Computing Terms of a Recursively Defined Sequence

Solution:

$c_2 = c_1 + 2c_0 + 1$ by substituting $k = 2$ into (1)

$= 2 + 2 \cdot 1 + 1$ since $c_1 = 2$ and $c_0 = 1$ by (2)

(3) • $c_2 = 5$

$c_3 = c_2 + 3c_1 + 1$ by substituting $k = 3$ into (1)

$= 5 + 3 \cdot 2 + 1$ since $c_2 = 5$ by (3) and $c_1 = 2$ by (2)

(4) • $c_3 = 12$

$c_4 = c_3 + 4c_2 + 1$ by substituting $k = 4$ into (1)

$= 12 + 4 \cdot 5 + 1$ since $c_3 = 12$ by (4) and $c_2 = 5$ by (3)

(5) • $c_4 = 33$

Example 4 – Showing That a Sequence Given by an Explicit Formula Satisfies a Certain Recurrence Relation

For each integer $n \geq 1$,

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

a. Find C_1, C_2, and C_3.

b. Show that this sequence satisfies the recurrence relation $C_k = \frac{4k-2}{k+1}C_{k-1}$ for all integers $k \geq 2$.

Example 4 – Solution

a. $C_1 = \frac{1}{2}\binom{2}{1} = \frac{1}{2}\cdot 2 = 1, \quad C_2 = \frac{1}{3}\binom{4}{2} = \frac{1}{3}\cdot 6 = 2,$

$C_3 = \frac{1}{4}\binom{6}{3} = \frac{1}{4}\cdot 20 = 5$

$$C_k = \frac{4k-2}{k+1}C_{k-1}$$

b. To obtain the kth and $(k-1)$st terms of the sequence, just substitute k and $k-1$ in place of n in the explicit formula for $C_1, C_2, C_3 \cdots$

$$C_k = \frac{1}{k+1}\binom{2k}{k} = \frac{1}{k+1}\cdot\frac{(2k)!}{(k)!\,(k)!}$$

$$C_{k-1} = \frac{1}{(k-1)+1}\binom{2(k-1)}{k-1} = \frac{1}{k}\binom{2k-2}{k-1} = C_{k-1}$$

$$= \frac{1}{k}\cdot\frac{(2k-2)!}{(k-1)!\,(2k-2-(k-1))!} = \frac{1}{k}\cdot\frac{(2k-2)!}{(k-1)!\,(k-1)!}$$

Example 4 – Solution

$$C_k = \frac{1}{k+1} \cdot \frac{(2k)!}{(k)!\,(k)!}$$

For each integer $k \geq 2$,

$$\frac{4k-2}{k+1} C_{k-1} = \frac{4k-2}{k+1}\left[\frac{1}{k}\binom{2k-2}{k-1}\right] \quad \text{by substituting}$$

$$= \frac{2(2k-1)}{(k+1)} \cdot \frac{1}{k} \cdot \frac{(2k-2)!}{(k-1)!\,(k-1)!} \quad \text{by the formula for } n \text{ choose } r$$

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

$$= \frac{1}{(k+1)} \cdot \frac{(2k)!}{k!\,k!}$$

$$= \frac{1}{(k+1)} \cdot \binom{2k}{k} \quad \text{by the formula for } n \text{ choose } r$$

$$= C_k$$

Fibonacci Numbers

A single pair of rabbits (male and female) is born at the beginning of a year. Assume the following conditions:

- Rabbit pairs are not fertile during their first month of life but thereafter give birth to one new male/female pair at the end of every month.
- No rabbits die.

How many rabbits will there be at the end of the year?

Fibonacci Numbers

For each integer $n \geq 1$, let

F_n: the number of rabbit pairs alive at the end of month n

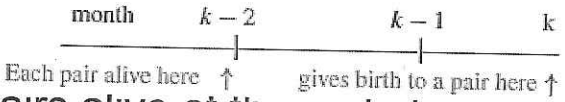
F_0: the initial number of rabbit pairs with $F_0 = 1$.

Because the first pair of rabbits is not fertile until the second month $F_1 = 1$.

pair of rabbits month 1 = 1
month 2 = 2
month 3 = 3
month 4 = 5
month 5 = 8

The crucial observation is that

- The number of rabbit pairs born at the end of month k is the same as the number of pairs alive at the end of month $k - 2$.



The number of rabbit pairs alive at the end of month k equals the ones alive at the end of month $k - 1$ plus the pairs newly born at the end of the month. Thus,

For all $k \geq 2$, $F_k = F_{k-1} + F_{k-2}$

$F_{2-1} + F_{2-2} = F_1 + F_0$

Fibonacci Numbers

The complete specification of the Fibonacci sequence is:

For all integers $k \geq 2$,

(1) $F_k = F_{k-1} + F_{k-2}$ recurrence relation

(2) $F_0 = 1, \quad F_1 = 1$ initial conditions.

Compute F_2, F_3, and so forth through F_{12}:

(3) $F_2 = F_1 + F_0 = 1 + 1 = 2$ by (1) and (2)

(4) $F_3 = F_2 + F_1 = 2 + 1 = 3$ by (1), (2) and (3)

(5) $F_4 = F_3 + F_2 = 3 + 2 = 5$ by (1), (3) and (4)

(6) $F_5 = F_4 + F_3 = 5 + 3 = 8$ by (1), (4) and (5)

(7) $F_6 = F_5 + F_4 = 8 + 5 = 13$ by (1), (5) and (6)

(8) $F_7 = F_6 + F_5 = 13 + 8 = 21$ by (1), (6) and (7)

(9) $F_8 = F_7 + F_6 = 21 + 13 = 34$ by (1), (7) and (8)

(10) $F_9 = F_8 + F_7 = 34 + 21 = 55$ by (1), (8) and (9)

(11) $F_{10} = F_9 + F_8 = 55 + 34 = 89$ by (1), (9) and (10)

(12) $F_{11} = F_{10} + F_9 = 89 + 55 = 144$ by (1), (10) and (11)

(13) $F_{12} = F_{11} + F_{10} = 144 + 89 = 233$ by (1), (11) and (12)

Fibonacci Numbers - Exercise

Prove that $F_{k+1}^2 - F_k^2 = F_{k-1}F_{k+2}$, for all integers $k \geq 1$.

Hint:

LHS $F_{k+1}^2 - F_k^2 = (F_k + F_{k-1})^2 - F_k^2$

$= F_k^2 + 2F_kF_{k-1} + F_{k-1}^2 - F_k^2$

$= 2F_kF_{k-1} + F_{k-1}^2$ LHS

RHS $F_{k-1}F_{k+2} = F_{k-1}(F_{k+1} + F_k)$

$= F_{k-1}((F_k + F_{k-1}) + F_k)$

$= F_{k-1}(2F_k + F_{k-1})$

$= 2F_kF_{k-1} + F_{k-1}^2$ RHS

Compound Interest

A_0: the initial amount in the account.

$A_k = A_{k-1}(1 + r)$, where r is the interest rate

A_n: the amount in the account at the end of year n.

$A_1 = A_0(1 + r)$

$A_2 = A_1(1 + r)$

$\vdots$

$A_{n-1} = A_{n-2}(1 + r)$

$A_n = A_{n-1}(1 + r)$

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

Recursive Definitions of Sum and Product

• Definition

Given numbers $a_1, a_2, \ldots, a_n$, where n is a positive integer, the **summation from $i = 1$ to n of the a_i**, denoted $\sum_{i=1}^{n} a_i$, is defined as follows:

$$\sum_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n, \quad \text{if } n > 1.$$

The **product from $i = 1$ to n of the a_i**, denoted $\prod_{i=1}^{n} a_i$, is defined by

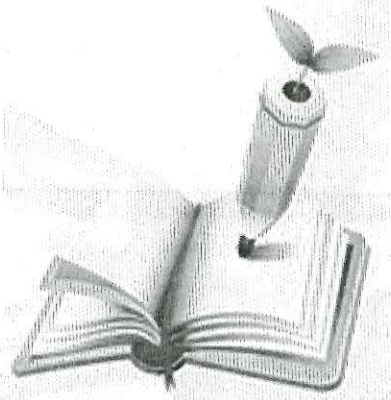
$$\prod_{i=1}^{1} a_i = a_1 \quad \text{and} \quad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) \cdot a_n, \quad \text{if } n > 1.$$

- The effect of these definitions is to specify an order in which sums and products of more than two numbers are computed. For example,

$$\sum_{i=1}^{4} a_i = \left(\sum_{i=1}^{3} a_i\right) + a_4 = \left(\left(\sum_{i=1}^{2} a_i\right) + a_3\right) + a_4 = ((a_1 + a_2) + a_3) + a_4.$$

Chapter 5: Sequences, Mathematical Induction and Recursion

5.7 Solving Recurrence Relations by Iteration



The Method of Iteration

The most basic method for finding an explicit formula for a recursively defined sequence is **iteration**.

Iteration works as follows:

- Given a sequence $a_0, a_1, a_2, \cdots$ defined by a recurrence relation and initial conditions
- Start from the initial conditions, calculate successive terms of the sequence until you see a pattern developing.
- At that point you guess an explicit formula.

Example 1 – Finding an Explicit Formula

Let $a_0, a_1, a_2, \cdots$ be the sequence defined recursively as follows: For all integers $k \geq 1$,

(1) $a_k = a_{k-1} + 2$ recurrence relation

(2) $a_0 = 1$ initial condition.

Use iteration to guess an explicit formula for the sequence.

Solution:

We know that to say

$$a_k = a_{k-1} + 2 \quad \text{for all integers } k \geq 1$$

Means

$$a_{\square} = a_{\square - 1} + 2$$ no matter what positive integer is placed into the box $\square$.

In particular, $a_1 = a_0 + 2$, $a_2 = a_1 + 2$, $a_3 = a_2 + 2$, and so forth.

Example 1 – Finding an Explicit Formula

Here's how the process works for the given sequence:

$a_0 = 1$ — the initial condition

$a_1 = a_0 + 2 = 1 + 2$ — by substitution

$a_2 = a_1 + 2 = (1 + 2) + 2 = 1 + 2 + 2$ — eliminate parentheses

$a_3 = a_2 + 2 = (1 + 2 + 2) + 2 = 1 + 2 + 2 + 2$ — eliminate parentheses again; write $3 \cdot 2$ instead of $2 + 2 + 2$?

$a_4 = a_3 + 2 = (1 + 2 + 2 + 2) + 2 = 1 + 2 + 2 + 2 + 2$ — eliminate parentheses again; definitely write $4 \cdot 2$ instead of $2 + 2 + 2 + 2$—the length of the string of 2's is getting out of hand.

Example 1 – Finding an Explicit Formula

Since it appears helpful to use the shorthand $k \cdot 2$ in place of $2 + 2 + \cdots + 2$ (k times), we do so, starting again from a_0.

$a_0 = 1 = 1 + 0 \cdot 2$ — the initial condition

$a_1 = a_0 + 2 = 1 + 2 = 1 + 1 \cdot 2$ — by substitution

$a_2 = a_1 + 2 = (1 + 2) + 2 = 1 + 2 \cdot 2$

$a_3 = a_2 + 2 = (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$

$a_4 = a_3 + 2 = (1 + 3 \cdot 2) + 2 = 1 + 4 \cdot 2$ — At this point it certainly seems likely that the general pattern is $1 + n \cdot 2$; check whether the next calculation supports this.

$a_5 = a_4 + 2 = (1 + 4 \cdot 2) + 2 = 1 + 5 \cdot 2$ — It does! So go ahead and write an answer. It's only a guess, after all.

$\vdots$

Example 1 – Finding an Explicit Formula

Guess: $a_n = 1 + n \cdot 2 = 1 + 2n$ P(n)

The answer obtained for this problem is just a guess. To be sure of the correctness of this guess, you will need to check it by mathematical induction.

Checking the Correctness of a Formula by Mathematical Induction

- It is all too easy to make a mistake and come up with the wrong formula.
- That is why it is important to confirm your calculations by checking the correctness of your formula.
- The most common way to do this is to use mathematical induction.

Example 1 – Finding an Explicit Formula

Let the property $p(n)$ be the equation

$$a_n = 1 + 2n \quad (n \geq 0) \qquad \leftarrow \quad p(n)$$

We must show that $p(n)$ is true for all integers $n \geq 0$.

Show that p(0) is true. To establish p(0), we must show that $a_0 = 1 + 2 * 0$. Step 1: p(0)

But

$$a_0 = 1$$

$$1 + 2 * 0 = 1$$

Hence, p(1) is true.

Example 1 – Finding an Explicit Formula

Step 2: **Show that for all integers $k \geq 0$, if $p(k)$ is true, then $p(k+1)$ is also true:**

[*Suppose that $p(k)$ is true for a particular but arbitrarily chosen integer $k \geq 0$.* That is:]

$$a_k = 1 + 2k$$

[*We must show that $p(k+1)$ is true.* That is:] we must show

$$a_{k+1} = 1 + 2(k+1)$$

But

$$\begin{aligned} a_{k+1} &= a_k + 2 && \text{By recurrence relation} \\ &= 1 + 2k + 2 && \text{By inductive hypothesis} \\ &= 1 + 2(k+1) && \text{By recurrence relation} \end{aligned}$$

which is the right-hand side of the equation. [*as was to be shown.*]

[*Since we have proved the basis step and the inductive step, we conclude that the formula holds for all terms of the sequence.*]

$P(k+1) = 2k+3$, $a_k = a_{k-1} + 2$, $a_{k+1} = a_k + 2$ → $a_{k+1} = (1+2k)+2$, $a_{k+1} = 2k+3$ True

Arithmetic Sequences

A sequence like the one in Example 1, in which each term equals the previous term plus a fixed constant, is called an arithmetic sequence.

• Definition

A sequence $a_0, a_1, a_2, \ldots$ is called an **arithmetic sequence** if, and only if, there is a constant d such that

$$a_k = a_{k-1} + d \quad \text{for all integers } k \geq 1.$$

It follows that,

$$a_n = a_0 + dn \quad \text{for all integers } n \geq 0.$$

Geometric Sequences

Let r be a fixed nonzero constant, and suppose a sequence $a_0, a_1, a_2, \cdots$ is defined recursively as follows:

$$a_k = ra_{k-1} \quad \text{for all integers } k \geq 1,$$
$$a_0 = a.$$

Use iteration to guess an explicit formula for this sequence.

• Definition

A sequence $a_0, a_1, a_2, \ldots$ is called a **geometric sequence** if, and only if, there is a constant r such that

$$a_k = ra_{k-1} \quad \text{for all integers } k \geq 1.$$

It follows that,

$$a_n = a_0 r^n \quad \text{for all integers } n \geq 0.$$

Using Formulas to Simplify Solutions Obtained by Iteration

Explicit formulas obtained by iteration can often be simplified by using formulas.

Theorem 5.2.2 Sum of the First n Integers

For all integers $n \geq 1$,

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

memorize

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

memorize

Theorem 5.2.3 Sum of a Geometric Sequence

For any real number r except 1, and any integer $n \geq 0$,

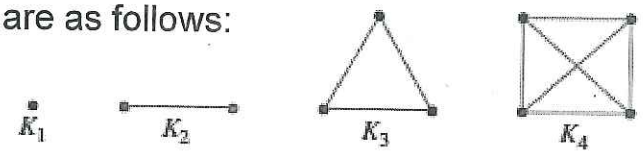
$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

memorize

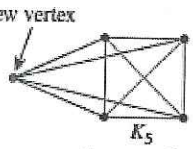
$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Example 6 – Using the Formula for the Sum of the First n Positive Integers

- Let K_n be the picture obtained by drawing n dots called *vertices,* and joining each pair of vertices by a line segment, called an *edge*.
- Then K_1, K_2, K_3, and K_4 are as follows:



- Observe that K_5 may be obtained from K_4 by adding one vertex and drawing edges between this new vertex and all the vertices of K_4 (the old vertices), because each pair of old vertices is already joined by an edge, and adding the new edges joins each pair of vertices consisting of an old one and the new one.



- Thus the number of edges of K_5 = 4 + the number of edges of K_4.

Example 6 – Using the Formula for the Sum of the First n Positive Integers

By the same reasoning, for all integers $k \geq 2$, the number of edges of K_l is $l - 1$ more than the number of edges of K_{l-1}. That is, if for each integer $n \geq 1$

$$s_n = \text{the number of edges of } K_n,$$

then

$$s_k = s_{k-1} + (k - 1) \qquad \text{for all integers } k \geq 2.$$

Note that s_1, is the number of edges in K_1, which is 0, and use iteration to find an explicit formula for $s_1, s_2, s_3, \cdots$.

$\sum_{K=1}^{n}\left(\sum_{J=1}^{K} 1\right) = \frac{n(n+1)}{2}$ or Combination method $1 \leq j \leq k \leq n$ (choose 2)

$\therefore \binom{2+n-1}{2}$

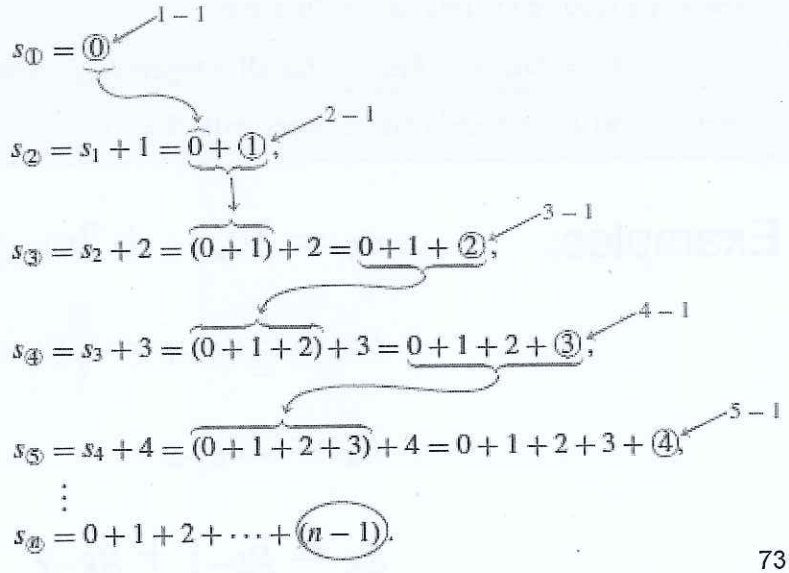
~~Example 6 – Using the Formula for the Sum of the First n Positive Integers~~

Solution: Because

$$s_k = s_{k-1} + (k - 1) \qquad \text{for all integers } k \geq 2$$

and

then, in particular,



Guess:

Example 6 – Using the Formula for the Sum of the First n Positive Integers

By Theorem 5.2.2.

$$0 + 1 + 2 + 3 + \cdots + (n - 1) = \frac{n(n-1)}{2}$$

Hence,

$$s_n = \frac{n(n-1)}{2}$$

Second-Order Linear Homogeneous Recurrence Relations with Constant Coefficients

• Definition

A **second-order linear homogeneous recurrence relation with constant coefficients** is a recurrence relation of the form

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{for all integers } k \geq \text{some fixed integer,}$$

where A and B are fixed real numbers with $B \neq 0$. Previous 2 terms

Examples:

$$a_k = 3a_{k-1} + 2a_{k-2}$$

$$c_k = \frac{1}{2}c_{k-1} - \frac{3}{7}c_{k-2}$$

$$e_k = 2e_{k-2}$$

$$g_k = g_{k-1} + g_{k-2}$$

The Distinct-Roots Case

Lemma 5.8.1

Let A and B be real numbers. A recurrence relation of the form

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{for all integers } k \geq 2 \qquad 5.8.1$$

is satisfied by the sequence

$$1, t, t^2, t^3, \ldots, t^n, \ldots,$$

where t is a nonzero real number, if, and only if, t satisfies the equation

$$t^2 - At - B = 0 \qquad 5.8.2$$

Equation (5.8.2) is called the *characteristic equation* of the recurrence relation.

$t_k = At^{k-1} + Bt^{k-2}$

Example 2 – Using the Characteristic Equation to Find Solutions to a Recurrence Relation

Consider the recurrence relation that specifies that the kth term of a sequence equals the sum of the $(k-1)$st term plus twice the $(k-2)$nd term. That is,

$$a_k = a_{k-1} + 2a_{k-2} \quad \text{for all integers } k \geq 2. \qquad 5.8.3$$

Find all sequences that satisfy relation (5.8.3) and have the form

$$1, t, t^2, t^3, \ldots, t^n, \ldots,$$

where t is nonzero.

Example 2 – Solution

By Lemma 5.8.1, relation (5.8.3) is satisfied by a sequence $1, t, t^2, t^3, \ldots, t^n, \ldots$ if, and only if, t satisfies the characteristic equation

$$t^2 - t - 2 = 0.$$

Since

$$t^2 - t - 2 = (t-2)(t+1),$$

the only possible values of t are 2 and –1.
It follows that the sequences

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \quad \text{and} \quad 1, -1, (-1)^2, (-1)^3, \ldots, (-1)^n, \ldots.$$

are both solutions for relation (5.8.3) and there are no other solutions of this form.

Note that these sequences can be rewritten more simply as

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \text{ and } 1, -1, 1, -1, \ldots, (-1)^n, \ldots.$$

The Distinct-Roots Case

Lemma 5.8.2

If $r_0, r_1, r_2, \ldots$ and $s_0, s_1, s_2, \ldots$ are sequences that satisfy the same second-order linear homogeneous recurrence relation with constant coefficients, and if C and D are *any* numbers, then the sequence $a_0, a_1, a_2, \ldots$ defined by the formula

$$a_n = Cr_n + Ds_n \quad \text{for all integers } n \geq 0$$

also satisfies the same recurrence relation.

Given a second-order linear homogeneous recurrence relation with constant coefficients, if the characteristic equation has two distinct roots, then Lemmas 5.8.1 and 5.8.2 can be used together to find a particular sequence that satisfies both the recurrence relation and two specific initial conditions.

Example 3 – Finding the Linear Combination That Satisfies the Initial Conditions

Find a sequence that satisfies the recurrence relation of Example 2,

$$a_k = a_{k-1} + 2a_{k-2} \quad \text{for all integers } k \geq 2, \qquad 5.8.3$$

and that also satisfies the initial conditions

$$a_0 = 1 \text{ and } a_1 = 8.$$

$t^2 = 1 \cdot t + 2$

$t^2 - t - 2 = 0$

$(t-2)(t+1) = 0$

Solution:

Example 2, the sequences

$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots$ and $1, -1, 1, -1, \ldots, (-1)^n, \ldots$

both satisfy relation (5.8.3) (though neither satisfies the given initial conditions).

Example 3 – Solution

By Lemma 5.8.2, therefore, any sequence $a_0, a_1, a_2, \ldots$ that satisfies an explicit formula of the form

$$a_n = C \cdot 2^n + D(-1)^n \qquad 5.8.6$$

where C and D are numbers, also satisfies relation (5.8.3).

You can find C and D so that $a_0, a_1, a_2, \ldots$ satisfies the specified initial conditions by substituting $n = 0$ and $n = 1$ into equation (5.8.6) and solving for C and D:

Plug in

$$\begin{aligned} a_0 = 1 &= C \cdot 2^0 + D(-1)^0, \\ a_1 = 8 &= C \cdot 2^1 + D(-1)^1. \end{aligned} \quad \Longrightarrow \quad \begin{aligned} C &= 3. \\ D &= -2. \end{aligned}$$

Get C & D

now sub in

It follows that the sequence $a_0, a_1, a_2, \ldots$ given by

$$a_n = 3 \cdot 2^n + (-2)(-1)^n = 3 \cdot 2^n - 2(-1)^n,$$

for integers $n \geq 0$, satisfies both the recurrence relation and the given initial conditions.

The Distinct-Roots Case

The techniques of Examples 2 and 3 can be used to find an explicit formula for *any* sequence that satisfies:

- A second-order linear homogeneous recurrence relation with constant coefficients
- The characteristic equation has distinct roots
- The first two terms of the sequence are known.

The Distinct-Roots Case

Theorem 5.8.3 Distinct-Roots Theorem

Suppose a sequence $a_0, a_1, a_2, \ldots$ satisfies a recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2} \qquad 5.8.1$$

for some real numbers A and B with $B \neq 0$ and all integers $k \geq 2$. If the characteristic equation

$$t^2 - At - B = 0 \qquad 5.8.2$$

has two distinct roots r and s, then $a_0, a_1, a_2, \ldots$ is given by the explicit formula

$$a_n = Cr^n + Ds^n,$$

where C and D are the numbers whose values are determined by the values a_0 and a_1.

Example 4 – A Formula for the Fibonacci Sequence

The Fibonacci sequence $F_0, F_1, F_2, \ldots$ satisfies the recurrence relation

$$F_k = F_{k-1} + F_{k-2} \qquad \text{for all integers } k \geq 2$$

with initial conditions

$$F_0 = F_1 = 1.$$

Find an explicit formula for this sequence.

Example 4 – A Formula for the Fibonacci Sequence

- Characteristic equation:

$$t^2 - t - 1 = 0$$

(1) Step

$$\Rightarrow \quad t = \frac{1 \pm \sqrt{1 - 4(-1)}}{2} = \begin{cases} \frac{1+\sqrt{5}}{2} = r \\ \frac{1-\sqrt{5}}{2} = s \end{cases}$$

(2) Step

It follows from the distinct-roots theorem that the Fibonacci sequence is given by the explicit formula

$$F_n = C\left(\frac{1+\sqrt{5}}{2}\right)^n + D\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \text{for all integers } n \geq 0, \qquad 5.8.7$$

(3) Step

where C and D are the numbers whose values are determined by the fact that $F_0 = F_1 = 1$.

Example 4 – A Formula for the Fibonacci Sequence

To find C and D, write

now Solve @ F_0 & F_1

$$F_0 = 1 = C\left(\frac{1+\sqrt{5}}{2}\right)^0 + D\left(\frac{1-\sqrt{5}}{2}\right)^0 = C \cdot 1 + D \cdot 1 = C + D$$

and

$$F_1 = 1 = C\left(\frac{1+\sqrt{5}}{2}\right)^1 + D\left(\frac{1-\sqrt{5}}{2}\right)^1 = C\left(\frac{1+\sqrt{5}}{2}\right) + D\left(\frac{1-\sqrt{5}}{2}\right)$$

$$\Rightarrow \quad C = \frac{1+\sqrt{5}}{2\sqrt{5}} \quad \text{and} \quad D = \frac{-(1-\sqrt{5})}{2\sqrt{5}}.$$

$$F_n = \left(\frac{1+\sqrt{5}}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{-(1-\sqrt{5})}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n,$$

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \qquad 5.8.8$$

The Single-Root Case

Lemma 5.8.4

Let A and B be real numbers and suppose the characteristic equation

$$t^2 - At - B = 0$$

has a single root r. Then the sequences $1, r^1, r^2, r^3, \ldots, r^n, \ldots$ and $0, r, 2r^2, 3r^3, \ldots, nr^n, \ldots$ both satisfy the recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for all integers $k \geq 2$.

The Single-Root Case

Theorem 5.8.5 Single-Root Theorem

Suppose a sequence $a_0, a_1, a_2, \ldots$ satisfies a recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for some real numbers A and B with $B \neq 0$ and for all integers $k \geq 2$. If the characteristic equation $t^2 - At - B = 0$ has a single (real) root r, then $a_0, a_1, a_2, \ldots$ is given by the explicit formula

$$a_n = Cr^n + Dnr^n,$$

where C and D are the real numbers whose values are determined by the values of a_0 and any other known value of the sequence.

Example 5 – Single-Root Case

Suppose a sequence $b_0, b_1, b_2, \ldots$ satisfies the recurrence relation

$$b_k = 4b_{k-1} - 4b_{k-2} \quad \text{for all integers } k \geq 2, \qquad 5.8.11$$

with initial conditions

$$b_0 = 1 \quad \text{and} \quad b_1 = 3.$$

Find an explicit formula for $b_0, b_1, b_2, \ldots$.

$t^2 = 4t - 4 \rightarrow t^2 - 4t + 4 = 0 \longrightarrow (t-2)^2 = 0$

$2^n, \; n2^n$

$a_n = C2^n + D \cdot n \cdot 2^n$

Solve for C & D

Example 5 – Solution

The characteristic equation

$$t^2 - 4t + 4 = 0 \quad (1)$$

has the unique root $r = 2$. → (2)

It follows from the single-root theorem that $b_0, b_1, b_2, \ldots$ is given by the explicit formula

$$b_k = 4b_{k-1} - 4b_{k-2} \quad \text{for all integers } k \geq 2, \qquad 5.8.11$$

where C and D are the real numbers whose values are determined by the fact that $b_0 = 1$ and $b_1 = 3$.

To find C and D, write (3)

$$b_0 = 1 = C \cdot 2^0 + D \cdot 0 \cdot 2^0 = C$$

and

$$b_1 = 3 = C \cdot 2^1 + D \cdot 1 \cdot 2^1 = 2C + 2D.$$

⟹ C = 1 and D = 1/2

Answer ⟹ $b_n = 2^n + \frac{1}{2}n2^n = 2^n\left(1 + \frac{n}{2}\right)$ for all integers $n \geq 0$.

Started @ 2

Chapter 5 Exam

1. Induction
2. Iteration - Show pattern Ex: $h_0 = 1$, $h_k = 2^k - h_{k-1}$ $(k \geq 1)$
3. r-Combination Ex: $\binom{n}{r+1} = \frac{n-r}{r+1}\binom{n}{r}$
4. Second-Order
5. ~~Nested Loops~~ Counting Algorithm
   Ex: K=1 to n, J=1 to K, i=1 to j
6. Loop Invariant

$h_0 = 1$
$h_1 = 2^1 - h_0 = 2^1 - 1$
$h_2 = 2^2 - h_1 = 2^2 - 2^1 + 1$
$h_3 = 2^3 - h_2 = 2^3 - 2^2 + 2^1 - 1$
$h_4 = 2^4 - h_3 = 2^4 - 2^3 + 2^2 - 2^1 + 1$
h_n

//

Change base $h_0 = (-2)^0$
$h_1 = -(-2)^1 - (-2)^0$
$h_2 = (-2)^2 + (-2)^1 + (-2)^0$
$h_3 = -(-2)^3 - (-2)^2 - (-2)^1 - (-2)^0$
$h_4 = (-2)^4 + (-2)^3 + (-2)^2 + (-2)^1 + (-2)^0$

notice h_1 & h_3 have negatives

$\therefore h_3 = (-1)[(-2)^3 + (-2)^2 + (-2)^1 + (-2)^0]$

$\therefore h_n = \sum_{i=0}^{n} (-1)^n (-2)^i$

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

from $\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$

SECTION 5.5

Application: Correctness of Algorithms

Application: Correctness of Algorithms

- Each program is designed to do a specific task.
- A program is correct if it produces correct output for any input.
- Most computer programmers write their programs using a combination of logical analysis and trial and error.
  - To get a program to run, the programmer must first fix all syntax errors.
  - When the syntax errors have been removed, however, the program may still contain logical errors that prevent it from producing correct output.
- Frequently, programs are tested using sets of sample data for which the correct output is known in advance.
  - The sample data are deliberately chosen to test the correctness of the program under extreme circumstances.
  - But for most programs the number of possible sets of input data is either infinite or unmanageably large, and so no amount of program testing can give perfect confidence that the program will be correct for all possible sets of legal input data.

Assertions

Consider an algorithm that is designed to produce a certain final state from a certain initial state. Both the initial and final states can be expressed as predicates involving the input and output variables.

Often the predicate describing the initial state is called the **pre-condition for the algorithm**, and the predicate describing the final state is called the **post-condition for the algorithm**.

Example 1 – *Algorithm Pre-Conditions and Post-Conditions*

Here are pre- and post-conditions for some typical algorithms.

a. Algorithm to compute a product of nonnegative integers

Pre-condition: The input variables m and n are nonnegative integers.

Post-condition: The output variable p equals mn.

Example 1 – *Algorithm Pre-Conditions and Post-Conditions* cont'd

b. Algorithm to find quotient and remainder of the division of one positive integer by another

Pre-condition: The input variables a and b are positive integers.

Post-condition: The output variables q and r are integers such that $a = bq + r$ *and* $0 \leq r < b$.

Example 1 – *Algorithm Pre-Conditions and Post-Conditions* cont'd

c. Algorithm to sort a one-dimensional array of real numbers

Pre-condition: The input variable $A[1], A[2], \ldots, A[n]$ is a one-dimensional array of real numbers.

Post-condition: The output variable $B[1], B[2], \ldots, B[n]$ is a one-dimensional array of real numbers with same elements as $A[1], A[2], \ldots, A[n]$ but with the property that $B[i] \leq B[j]$ whenever $i \leq j$.

Loop Invariants

The method of loop invariants is used to prove correctness of a loop with respect to certain pre- and post-conditions. It is based on the principle of mathematical induction.

Suppose that an algorithm contains a **while** loop and that entry to this loop is restricted by a condition *G*, called the **guard**.

Suppose also that assertions describing the current states of algorithm variables have been placed immediately preceding and immediately following the loop.

Loop Invariants

The assertion just preceding the loop is called the **pre-condition for the loop** and the one just following is called the **post-condition for the loop**. The annotated loop has the following appearance:

[*Pre-condition for the loop*]

while (*G*)

[*Statements in the body of the loop. None contain branching statements that lead outside the loop.*]

end while

[*Post-condition for the loop*]

Loop Invariants

• Definition

A loop is defined as **correct with respect to its pre- and post-conditions** if, and only if, whenever the algorithm variables satisfy the pre-condition for the loop and the loop terminates after a finite number of steps, the algorithm variables satisfy the post-condition for the loop.

Establishing the correctness of a loop uses the concept of loop invariant.

A **loop invariant** is a predicate with domain a set of integers, which satisfies the condition: For each iteration of the loop, if the predicate is true before the iteration, then it is true after the iteration.

Loop Invariants

The following theorem, called the *loop invariant theorem*, formalizes these ideas.

Theorem 5.5.1 Loop Invariant Theorem

Let a **while** loop with guard G be given, together with pre- and post-conditions that are predicates in the algorithm variables. Also let a predicate $I(n)$, called the **loop invariant,** be given. If the following four properties are true, then the loop is correct with respect to its pre- and post-conditions.

I. **Basis Property:** The pre-condition for the loop implies that $I(0)$ is true before the first iteration of the loop.

II. **Inductive Property:** For all integers $k \geq 0$, if the guard G and the loop invariant $I(k)$ are both true before an iteration of the loop, then $I(k+1)$ is true after iteration of the loop.

III. **Eventual Falsity of Guard:** After a finite number of iterations of the loop, the guard G becomes false.

IV. **Correctness of the Post-Condition:** If N is the least number of iterations after which G is false and $I(N)$ is true, then the values of the algorithm variables will be as specified in the post-condition of the loop.

Example 2 – *Correctness of a Loop to Compute a Product*

The following loop is designed to compute the product *mx* for a nonnegative integer *m* and a real number *x*, without using a built-in multiplication operation. Prior to the loop, variables *i* and *product* have been introduced and given initial values *i* = 0 and *product* = 0.

[Pre-condition: m is a nonnegative integer, x is a real number, $i = 0$, and $product = 0$.]

while $(i \neq m)$

1. $product := product + x$
2. $i := i + 1$

end while

[Post-condition: $product = mx$]

Example 2 – *Correctness of a Loop to Compute a Product* cont'd

Let the loop invariant be

$$I(n)\text{: } i = n \quad \text{and} \quad product = nx$$

→ constant

The guard condition *G* of the **while** loop is

$$G\text{: } i \neq m$$

Use the loop invariant theorem to prove that the **while** loop is correct with respect to the given pre- and post-conditions.

Example 2 – *Solution*

I. Basis Property: *[I(0) is true before the first iteration of the loop.]*

$I(0)$ is "$i = 0$ and *product* $= 0 \cdot x$", which is true before the first iteration of the loop because $0 \cdot x = 0$.

II. Inductive Property: *[If $G \wedge I(k)$ is true before a loop iteration (where $k \geq 0$), then $I(k + 1)$ is true after the loop iteration.]*

Example 2 – *Solution* cont'd

Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. Then as execution reaches the top of the loop, $i \neq m$, *product* $= kx$, and $i = k$.

Since $i \neq m$, the guard is passed and statement 1 is executed. Before execution of statement 1,

$$\text{product}_{\text{old}} = kx.$$

Thus execution of statement 1 has the following effect:

$$\text{product}_{\text{new}} = \text{product}_{\text{old}} + x = kx + x = (k + 1)x.$$

Example 2 – *Solution*

cont'd

Similarly, before statement 2 is executed,

$$i_{\text{old}} = k,$$

so after execution of statement 2,

$$i_{\text{new}} = i_{\text{old}} + 1 = k + 1.$$

Hence after the loop iteration, the statement $I(k + 1)$, namely, ($i = k + 1$ and *product* = $(k + 1)x$), is true. This is what we needed to show.

Statement 1 & Statement 2 proved K+1 inductive step ✓

Example 2 – *Solution*

cont'd

III. Eventual Falsity of Guard: *[After a finite number of iterations of the loop, G becomes false.]*

The guard G is the condition $i \neq m$, and m is a nonnegative integer.

By I and II, it is known that

for all integers $n \geq 0$, if the loop is iterated n times, then $i = n$ and product = nx.

So after m iterations of the loop, $i = m$.

Thus G becomes false after m iterations of the loop. ✓

Example 2 – *Solution* cont'd

IV. Correctness of the Post-Condition: *[If N is the least number of iterations after which G is false and I(N) is true, then the value of the algorithm variables will be as specified in the post-condition of the loop.]*

According to the post-condition, the value of *product* after execution of the loop should be *mx*.

But if *G* becomes false after *N* iterations, $i = m$. And if *I*(*N*) is true, $i = N$ and $product = Nx$.

Since both conditions (*G* false and *I*(*N*) true) are satisfied, $m = i = N$ and $product = mx$ as required.

Correctness of the Euclidean Theorem

The crucial loop, annotated with pre- and post-conditions, is the following:

[Pre-condition: A and B are integers with $A > B \geq 0, a = A, b = B, r = B$.*]*

while $(b \neq 0)$

1. $r := a \bmod b$
2. $a := b$
3. $b := r$

end while

[Post-condition: $a = \gcd(A, B)$*]*

$gcd(A,B) = gcd(B,r)$

Correctness of the Euclidean Theorem

Proof:

To prove the correctness of the loop, let the invariant be

$$I(n)\text{: } \gcd(a, b) = \gcd(A, B) \quad \text{and} \quad 0 \leq b < a.$$

The guard of the **while** loop is

$$G\text{: } b \neq 0.$$

Correctness of the Euclidean Theorem

I. Basis Property: *[I(0) is true before the first iteration of the loop.]*

I(0) is

$$\gcd(A, B) = \gcd(a, b) \quad \text{and} \quad 0 \leq b < a.$$

According to the pre-condition,

$$a = A, \quad b = B, \quad r = B, \quad \text{and} \quad 0 \leq B < A.$$

Hence gcd(*A*, *B*) = gcd(*a*, *b*). Since $0 \leq B < A$, $b = B$, and $a = A$ then $0 \leq b < a$. Hence *I*(0) is true.

Correctness of the Euclidean Theorem

II. Inductive Property: *[If $G \wedge I(k)$ is true before an iteration of the loop (where $k \geq 0$), then $I(k+1)$ is true after iteration of the loop.]*

$I(k)$: $\gcd(a,b) = \gcd(A,B)$, $0 \leq b < a$

Suppose k is a nonnegative integer such that $G \wedge I(k)$ is true before an iteration of the loop. *[We must show that $I(k+1)$ is true after iteration of the loop.]* Since G is true, $b_{\text{old}} \neq 0$ and the loop is entered. And since $I(k)$ is true, immediately before statement 1 is executed,

$$\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(A, B) \quad \text{and} \quad 0 \leq b_{\text{old}} < a_{\text{old}}. \qquad 5.5.5$$

Correctness of the Euclidean Theorem

After execution of statement 1,

$$r_{\text{new}} = a_{\text{old}} \bmod b_{\text{old}}.$$

Thus, by the quotient-remainder theorem,

$$a_{\text{old}} = b_{\text{old}} \cdot q + r_{\text{new}} \quad \text{for some integer } q$$

and r_{new} has the property that

$$0 \leq r_{\text{new}} < b_{\text{old}}. \qquad 5.5.6$$

By Lemma 4.8.2,

$$\gcd(a_{\text{old}}, b_{\text{old}}) = \gcd(b_{\text{old}}, r_{\text{new}}).$$

So by the equation of (5.5.5),

$$\gcd(b_{\text{old}}, r_{\text{new}}) = \gcd(A, B). \qquad 5.5.7$$

Stmt1: $r_{new} = a_{old} \bmod b_{old}$

Stmt2: $a_{new} = b_{old}$

Stmt3: $b_{new} = r_{new} = a_{old} \bmod b_{old}$

$\gcd(a,b) = \gcd(b_{old}, r)$

$= \gcd(b_{old}, a_{old} \bmod b_{old})$

Correctness of the Euclidean Theorem

When statements 2 and 3 are executed,

$$a_{\text{new}} = b_{\text{old}} \quad \text{and} \quad b_{\text{new}} = r_{\text{new}}. \qquad 5.5.8$$

Substituting equations (5.5.8) into equation (5.5.7) yields

$$\gcd(a_{\text{new}}, b_{\text{new}}) = \gcd(A, B). \qquad 5.5.9$$

And substituting the values from the equations in (5.5.8) into inequality (5.5.6) gives

$$0 \leq b_{\text{new}} < a_{\text{new}}. \qquad 5.5.10$$

Hence after the iteration of the loop, by equation (5.5.9) and inequality (5.5.10),

$$\gcd(a, b) = \gcd(A, B) \quad \text{and} \quad 0 \leq b < a,$$

which is $I(k + 1)$. *[This is what we needed to show.]*

Eventually $\gcd(a_{new}, b_{new}) = \gcd(b, r) = \gcd(a, 0)$

break loop

Correctness of the Euclidean Theorem

III. Eventual Falsity of the Guard: *[After a finite number of iterations of the loop, G becomes false.]*

- Each value of b obtained by repeated iteration of the loop is nonnegative and less than the previous value of b.
- Thus, by the well-ordering principle, there is a least value b_{min}. The fact is that $b_{\text{min}} = 0$
- Since $b_{\text{min}} = 0$, the guard is false immediately following the loop iteration in which b_{min} is calculated.

- **well-ordering principle** states that every non-empty set of positive integers contains a least element

Correctness of the Euclidean Theorem

IV. Correctness of the Post-Condition: *[If N is the least number of iterations after which G is false and I(N) is true, then the values of the algorithm variables will be as specified in the post-condition.]*

Suppose that for some nonnegative integer *N*, *G* is false and *I(N)* is true. *[We must show the truth of the post- condition: a = gcd(A, B).]* Since G is false, *b* = 0, and since *I*(*N*) is true,

$$\gcd(a, b) = \gcd(A, B). \qquad 5.5.11$$

Correctness of the Euclidean Theorem

Substituting *b* = 0 into equation (5.5.11) gives

$$\gcd(a, 0) = \gcd(A, B).$$

But by Lemma 4.8.1,

$$\gcd(a, 0) = a.$$

Hence *a* = gcd*(A, B) [as was to be shown].*

$$c_k = 4c_{k-1} + 5$$

$$c_3 = 4c_2 + 5 = 4^3 \times 2 + 4^2 \times 5 + 4 \times 5 + 5$$

$$c_3 = 4^3 \times 2 + 5(4^2 + 4^1 + 1)$$

$$c_n = 4^n \times 2 + 5(4^{n-1} + 4^{n-2} + \dots 4^2 + 4^1 + 4^0)$$

$$c_n = 4^n \times 2 + 5 \sum_{i=0}^{n-1} 4^i$$

$$c_n = 4^n \times 2 + 5\left(\frac{4^{n-1+1} - 1}{4-1}\right)$$

$$\boxed{c_n = 4^n \times 2 + 5\left(\frac{4^n - 1}{3}\right)}$$

11

$I(n)$: $i = n+1$, $Sum = A[1] + \dots + A[n+1]$

$n=0$? (1) $I(0)$: $i=1$, $Sum = A[1]$ → program initialized properly

(2) $G \wedge I(k) \rightarrow I(k+1)$

before loop $I(k)$: $i_{old} = k+1$, $sum_{old} = A[1] + \dots + A[k+1]$

Statement 1: $i_{new} = i_{old} + 1 = k+1+1 = k+2$

Statement 2: $Sum_{new} = Sum_{old} + A[i] = \overbrace{A[1] + \dots + A[k+1]}^{old} + \overbrace{A[k+2]}^{A[i]}$

Check $I(k+1)$: $I(n)$, $n = k+1$, $I(k+1)$: $i = k+1+1$, $i = k+2$

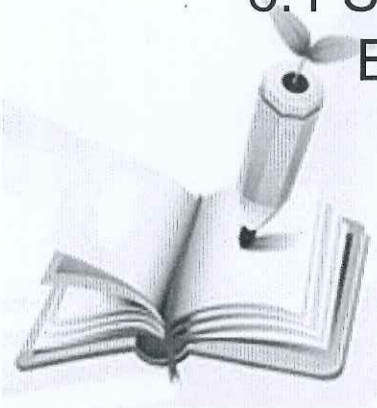
↳ $Sum = A[1] + \dots + A[k+1+1] = A[1] + \dots A[k+2]$

Program matches theory of $I(n)$. $i = k+2$, $sum = \dots + A[k+2]$

(3/4) After N rounds we reach last iteration where G is true & $I(N)$ true. At $I(N+1)$ G is now false. Now $i = m$ & $i = N+2$ therefore $m = N+2$. Sum currently holds $A[1] + \dots A[N+2]$ After replacement we have $Sum = A[1] + \dots A[m]$

Chapter 6: Set Theory

6.1 Set Theory: Definition and the Element Method of Proof



Sets

- A set is an **unordered** collection of objects. The objects in a set are called the elements, or members of the set.
- A set is said to contain its elements.

  $A = \{a_1, a_2, \ldots, a_n\}$ "A contains $a_1, a_2, \ldots, a_n$"
- $a \in A$ "a is an element of A" "a is a member of A"
- $a \notin A$ "a is not an element of A"

Examples:

- **Vowels in the English alphabet**

  V = { a, e, i, o, u }
- **First seven prime numbers.**

  X = { 2, 3, 5, 7, 11, 13, 17 }

Important Sets in Discrete Math

- $\mathrm{N} = \{0, 1, 2, 3, \ldots\}$, the set of natural numbers
- $\mathrm{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of all integers
- $Z^+ = \{1, 2, 3, \ldots\}$, the set of positive integers
- $\mathrm{Q} = \{p/q \mid p \in \mathrm{Z}, q \in \mathrm{Z}, and\ q \neq 0\}$, the set of all rational numbers
- R, the set of all real numbers
- R^+, the set of positive real numbers
- C, the set of complex numbers.

Set Cardinality

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

Examples

- Let A be the set of odd positive integers less than 10. Then $|A| = 5$.
- Let S be the set of letters in the English alphabet. Then $|S| = 26$.
- $|\emptyset| = 0$.
- $|\{\emptyset\}| = 1$

Representing Sets

Representing a set by:

1) Set-roster notation: Listing (enumerating) all the members of the set.

Example:

- Let $A = \{1,2,3\}$, $B = \{3,1,2\}$, and $C = \{1,1,2,3,3,3\}$.
  - A, B, and C have exactly the same three elements: 1, 2, and 3. therefore, A, B, and C are simply different ways to represent the same set.
- $\{0\} \neq 0$: $\{0\}$ is a set with one element, namely 0; 0 is just the symbol that represents the number zero.
- The set $\{1, \{1\}\}$ has two elements: 1 and the set whose only element is 1.
- For each nonnegative integer n, let $U_n = \{n, -n\}$. Find U_1, U_2 and U_0.
  - $U_1 = \{1, -1\}$, $U_2 = \{2, -2\}$, $U_0 = \{0, -0\} = \{0\}$.

Representing Sets (cont')

Representing a set by:

1) Set-roster notation: Listing (enumerating) all the members of the set.
2) Set builder notation: defining a set by property $\{x \in S | P(x)\}$.
   - Set builder notation: let S be a set and let $P(x)$ be a property that elements of S may or may not satisfy.
   - $\{x \in S | P(x)\}$ formulates a new set to be the set of all element x in S such that P(x) is true.

$$\{x \in S | P(x)\}$$

the set of all ↗ ↖ such that

Using the Set-Builder Notation

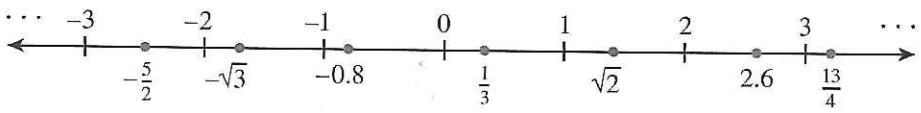
Example: Given that R denotes the set of all real numbers, Z is the set of all integers, Z^+ is the set of all positive integers, describe each of the following sets.

- $\{x \in R | -2 < x < 5\}$: open interval of real numbers between -2 and 5. → builder notation
- $\{x \in Z | -2 < x < 5\}$: open interval of all integers between -2 and 5. it is equal to the set $\{-1,0,1,2,3,4\}$. set-roster notation
- $\{x \in Z^+ | -2 < x < 5\}$: open interval of all positive integers between -2 and 5. it is equal to the set $\{1,2,3,4\}$.

Representing Sets (cont')

Representing a set by:

1) Set-roster notation: Listing (enumerating) all the members of the set.
2) Set builder notation: defining a set by property $\{x \in S | P(x)\}$.
3) Ellipses (⋯, read as "and so forth") can be used when the general pattern of the elements is obvious.
   Example: a set of integers between 1 and 100: A= {1,2,3 …, 100}
4) Representing real numbers with a picture.
   - The number 0 corresponds to a middle point, called the *origin*.
   - A unit of distance is marked off, and each point to the right of the origin corresponds to a positive real number found by computing its distance from the origin.



Subsets

- $A \subseteq B$ means that "for all elements x, if $x \in A$ then $x \in B$"

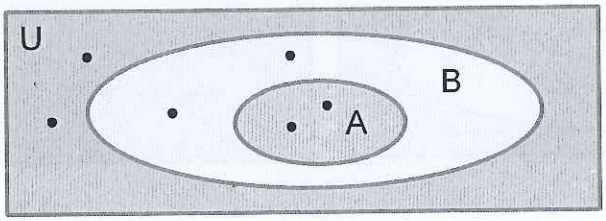
$$A \subseteq B \Leftrightarrow \forall x(x \in A \rightarrow x \in B).$$

- The negation:

$A \not\subseteq B$: there is at least one element x such that $x \in A$ and $x \notin B$.

$$A \not\subseteq B \Leftrightarrow \exists x(x \in A \wedge x \notin B)$$

- A is a proper subset of B $A \subset B \Leftrightarrow$
  1) $A \subseteq B$, and
  2) there is at least one element in B that is not in A.



9

Example 1 – Testing Whether One Set Is a Subset of Another

Let $A = \{1\}$ and $B = \{1, \{1\}\}$.

a. Is $A \subseteq B$?

b. If so, is A a proper subset of B?

Solution:

a. Because $A = \{1\}$, A has only one element, namely the symbol 1. This element is also one of the elements in set B . Hence every element in A is in B, and so $A \subseteq B$.

b. B has two distinct elements, the symbol 1 and the set {1} whose only element is 1. Since $1 \neq \{1\}$, the set {1} is not an element of A, and so there is an element of B that is not an element of A. Hence A is a proper subset of B.

10

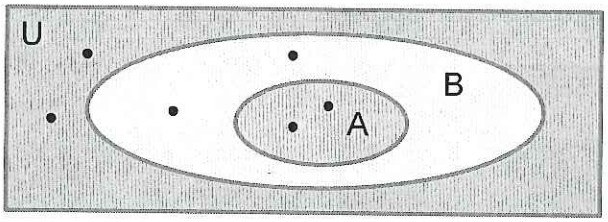
Subsets: Proof and Disproof

- To proof A is a subset of B $(A \subseteq B)$
  - Suppose x is a particular but arbitrarily chosen element of A $(x \in A)$, and show that x is an element of B $(x \in B)$

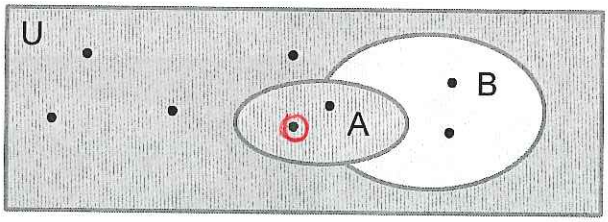
$$A \subseteq B \quad \Leftrightarrow \quad \forall x, \text{if } x \in A \text{ then } x \in B$$

- To proof A is NOT a subset of B $(A \not\subseteq B)$
  - Find a single $x \in A$ such that $x \notin B$.

$$A \not\subseteq B \quad \Leftrightarrow \quad \exists x, \text{such that } x \in A \text{ and } x \notin B$$



$A \subseteq B$



$A \not\subseteq B$

Example – Proving and Disproving Subset Relations

Define sets A and B as follows:

$$A = \{m \in \mathbf{Z} \mid m = 6r + 12 \text{ for some } r \in \mathbf{Z}\}$$
$$B = \{n \in \mathbf{Z} \mid n = 3s \text{ for some } s \in \mathbf{Z}\}.$$

a. Outline a proof that $A \subseteq B$.

b. Prove that $A \subseteq B$.

c. Disprove that $B \subseteq A$.

Example – Solution

a. Proof Outline:

Suppose x is a particular but arbitrarily chosen element of A.

.
.
.

Therefore, x is an element of B.

b. Proof:

Suppose x is a particular but arbitrarily chosen element of A.

[We must show that $x \in B$. By definition of B, this means we must show that $x = 3 \cdot (\text{some integer})$.]

By definition of A, there is an integer r such that

$$x = 6r + 12 = 3(2r + 4) = 3s \longrightarrow \therefore x \text{ also} \in B$$

where $s = 2r + 4$. s is an integer because products and sums of integers are integers.

Thus, by definition of B, x is an element of B,

Example – Solution

cont'd

c. To disprove that $B \subseteq A$, you must find an element of B that is not an element of A.

$B \not\subseteq A \quad \Leftrightarrow \quad \exists x$, such that $x \in B$ and $x \notin A$

Let $x = 3$, then $x \in B$ because $3 = 3 \cdot 1$, but $x \notin A$ because there is no integer r such that $3 = 6r + 12$.

$$\begin{aligned} & 6r + 12 = 3 && \text{by assumption} \\ \Rightarrow \quad & 2r + 4 = 1 && \text{by dividing both sides by 3} \\ \Rightarrow \quad & 2r = 3 && \text{by subtracting 4 from both sides} \\ \Rightarrow \quad & r = 3/2 && \text{by dividing both sides by 2,} \end{aligned}$$

but 3/2 is not an integer. Thus $3 \in B$ but $3 \notin A$, and so $B \not\subseteq A$

Set Equality

Definition: Given two sets A and B, A equals B, written $A = B$, if, and only if, every element of A is in B and every element of B is in A.

Symbolically:

$$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ and } B \subseteq A$$

Example 3 – Set Equality

Define sets A and B as follows:

$$A = \{m \in \mathbf{Z} \mid m = 2a \text{ for some integer } a\}$$
$$B = \{n \in \mathbf{Z} \mid n = 2b - 2 \text{ for some integer } b\}$$

Is $A = B$?

Solution:

Yes. To prove this, both subset relations $A \subseteq B$ and $B \subseteq A$ must be proved.

Example – Solution

cont'd

Part 1, Proof That $A \subseteq B$:

Suppose x is a particular but arbitrarily chosen element of A.

By definition of A, there is an integer a such that $x = 2a$.

$$x = 2a = 2a + 2 - 2 = 2(a + 1) - 2 = 2b - 2.$$ Satisfies B as well

where $b = a + 1$ is an integer since it is a sum of integers.

Thus, by definition of B, x is an element of B

Part 2, Proof That $B \subseteq A$:

Similarly we can prove that $B \subseteq A$. Hence $A = B$.

belongs to

Distinction between $\in$ and $\subseteq$

↳ Subset

Which of the following are true statements?

T a. $2 \in \{1,2,3\}$: true. 2 is an element of set $\{1,2,3\}$

F b. $\{2\} \in \{1,2,3\}$: false. 2 is not equal to $\{2\}$. The set $\{2\}$ is not an element of set $\{1,2,3\}$.

F c. $2 \subseteq \{1,2,3\}$: false. 2 is not a set. not a bag

T d. $\{2\} \subseteq \{1,2,3\}$: true. The set $\{2\}$ is a subset of $\{1,2,3\}$

F e. $\{2\} \subseteq \{\{1\},\{2\},\{3\}\}$: false. The set $\{\{1\},\{2\},\{3\}\}$ has three elements $\{1\}, \{2\}$ and $\{3\}$. The set $\{2\}$ is an element of the set $\{\{1\},\{2\},\{3\}\}$. Should be $\in$

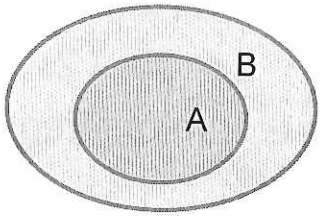
f. T $\{2\} \in \{\{1\},\{2\},\{3\}\}$: true. $\{2\}$ is an element of the set $\{\{1\},\{2\},\{3\}\}$.

To make true $\{\{2\}\} \subseteq \{\{1\},\{2\},\{3\}\}$ ✓

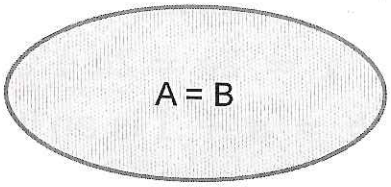
Also $\{2\} \in \{\{1\},\{2\},\{3\}\}$ ✓

Venn Diagrams

- Venn Diagrams can be used to represents the relationships between different sets.
- Venn Diagrams of $A \subseteq B$

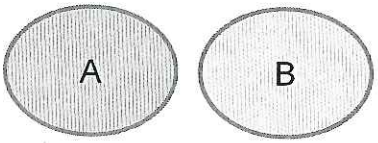


(a) $A \subseteq B$

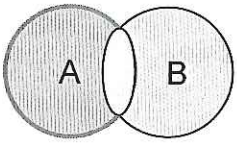


(b) $A = B$

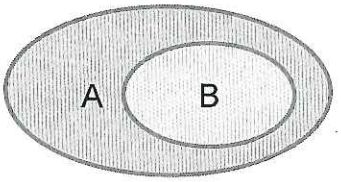
- Venn Diagrams of $A \nsubseteq B$



(a)



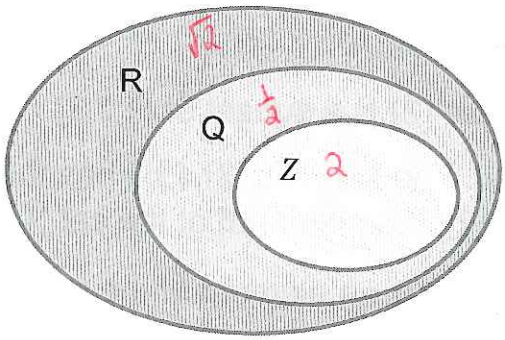
(b)



(c)

Relations among Sets of Numbers

- $\mathrm{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of all integers
- $\mathrm{Q} = \{p/q \mid p \in \mathrm{Z}, q \in \mathrm{Z}, and\ q \neq 0\}$, the set of all rational numbers
- R, the set of all real numbers

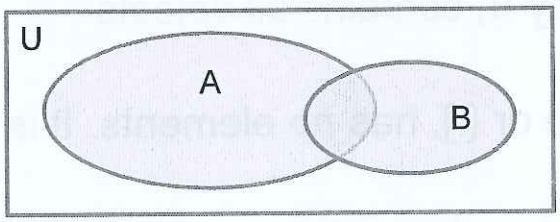


Operations on Sets

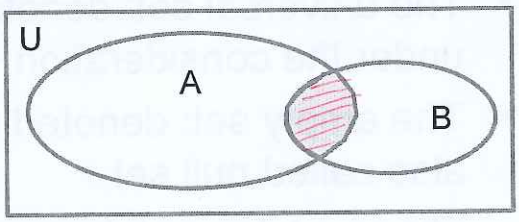
Let A and B be subsets of a universal set U.

1. The **union** of A and B, denoted $\boldsymbol{A \cup B}$, is the set of all elements that are in at least one of A *or* B.
$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$$
2. The **intersection** of A and B, denoted $\boldsymbol{A \cap B}$, is the set of all elements that are common to both A and B.
$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\},$$
3. The **difference** of B minus A (or **relative complement** of A in B), denoted $\boldsymbol{B - A}$, is the set of all elements that are in B and not A.
$$B - A = \{x \in U \mid x \in B \text{ and } x \notin A\},$$ in B but not in big A
4. The **complement** of A, denoted A^c, is the set of all elements in U that are not in A.
$$A^c = \{x \in U \mid x \notin A\}.$$ Like negation

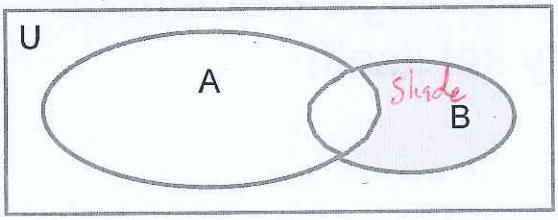
Venn Diagram Representations for Operations on Sets



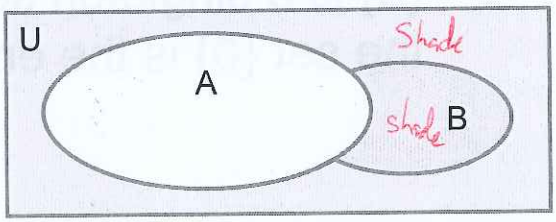
(a) Shaded region represents $A \cup B$.



(b) Shaded region represents $A \cap B$.



(c) Shaded region represents $B - A$.



(d) Shaded region represents A^c.

Notation for Subsets of Real Numbers

- Given real numbers a and b with $a \leq b$:

$$(a,b) = \{x \in R | a < x < b\} \quad [a,b] = \{x \in R | a \leq x \leq b\}$$
$$(a,b] = \{x \in R | a < x \leq b\} \quad [a,b) = \{x \in R | a \leq x < b\}$$

- The symbols ∞ and $-\infty$ are used to indicate intervals that are unbounded either on the right or on the left.

$$(a,\infty) = \{x \in R | x > a\} \quad [a,\infty) = \{x \in R | x \geq a\}$$
$$(-\infty,b) = \{x \in R | x < b\} \quad (-\infty,b] = \{x \in R | x \leq b\}$$

Special sets

- The universal set: denoted by U, contains all objects under the consideration.
- The empty set: denoted as $\emptyset$ or $\{\}$, has no elements. It is also called null set.
- The singleton set: has only one element.
  - $\{\emptyset\}$ is a singleton set. The single element of the set $\{\emptyset\}$ is the empty set itself!

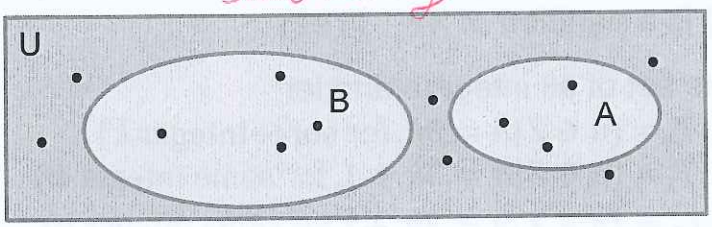
Disjoint Sets

- Two sets are called disjoint **if, and only if**, they have no elements in common.
- Alternate: A and B are disjoint **if and only if**

$$A \cap B = \emptyset$$

- Example: Sets $\{1, 3, 5, 7, 9\}$ and $\{2, 4, 6, 8, 10\}$ are disjoint.

Share nothing



Mutually Disjoint

- Sets $A_1, A_2, A_3 \cdots$ are mutually disjoint (or pairwise disjoint or non-overlapping) if, and only if, no two sets A_i and A_j with distinct subscripts have any elements in common.
- More precisely, for all i, $j = 1,2,3, \cdots$

$$A_i \cap A_j = \emptyset \quad \text{whenever } i \neq j$$

Exercises:

a. Sets $A_1 = \{3, 5\}$, $A_2 = \{1, 4, 6\}$ and $A_3 = \{2\}$ are mutually disjoint?
   - yes

b. Sets $B_1 = \{2, 4, 6\}$, $B_2 = \{3, 7\}$ and $B_3 = \{4, 5\}$ are mutually disjoint?
   - No.

Partitions of Sets

Ex: Quotient remainder theorem

A finite or infinite collection of nonempty sets $\{A_1, A_2, A_3 \cdots\}$ is a partition of a set A if, and only if,

- A is the union of all A_i
- The sets $A_1, A_2, A_3 \cdots$ are mutually disjoint.

Exercises:

a. Let $A = \{1, 2, 3, 4, 5, 6\}$, $A_1 = \{1, 2\}$, $A_2 = \{3, 4\}$ and $A_3 = \{5, 6\}$. Is $\{A_1, A_2, A_3\}$ is a partition of A? (Yes)

b. Let Z be the set of all integers and let

$$T_0 = \{n \in Z | n = 3k, \text{for some integer } k\}$$
$$T_1 = \{n \in Z | n = 3k + 1, \text{for some integer } k\}$$
$$T_2 = \{n \in Z | n = 3k, +2 \text{ for some integer } k\}$$

Is $\{T_0, T_1, T_2\}$ a partition of Z? (Yes)

Power Sets

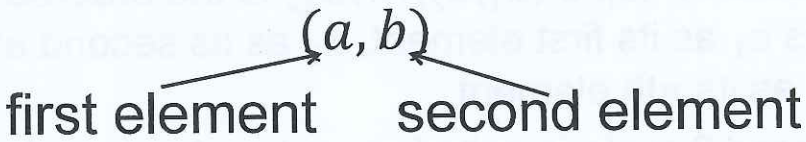
- Given a set S, the *power set* of S is the set of all subsets of the set S. The power set of S is denoted by $\mathcal{P}(S)$.

Examples:

- What is the power set of the set {0, 1, 2}?
  - $\mathcal{P}(\{0, 1, 2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$.
  - $|\mathcal{P}(\{1,2,3\}| = 8$ → cardinality of this Power set $2^n = 2^3 = 8$
- What is the power set of ∅?
  - $\mathcal{P}(\emptyset) = \{\emptyset\}$; $|\mathcal{P}(\emptyset)| = 1$
- What is the power set of the set {∅}?
  - $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$; $|\mathcal{P}(\{\emptyset\})| = 2$
- If S is a set with $|S| = n$ then $|P(S)| = 2^n$.

Ordered Pair

- Given elements a and b the symbol (a, b) denotes the ordered pair:



- Two ordered pairs (a, b) and (c, d) are equal if, and only if, $a = c$ and $b = d$.

$(a, b) = (c, d)$ means that $a = c$ and $b = d$

Ordered Pair - Exercise

- Is (1,2) = (2,1)?
  - No. By definition of equality of ordered pairs,
    $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$
- Is $\left(3, \frac{5}{10}\right) = (\sqrt{9}, \frac{1}{2})$?
  - Yes. $3 = \sqrt{9}$ and $\frac{5}{10} = \frac{1}{2}$
- What is the first element of (1,1)?
  - The first and second elements of (1,1) are both 1.

Ordered n-tuple

- Sets are used to represent unordered collections.
- **Ordered-n tuples** are used to represent an ordered collection.
- The ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has a_1 as its first element, a_2 as its second element, $\cdots$, and a_n as its nth element.
- An ordered 2-tuple is called an ordered pair and an ordered 3-tuple is called an ordered triple.
- Two n-tuples are equal if and only if their corresponding elements are equal.

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Leftrightarrow a_1{=}b_1 \wedge a_2{=}b_2 \wedge \cdots \wedge a_n{=}b_n$$

- In particular, $(a, b) = (c, d) \Leftrightarrow a = c \text{ and } b = d$

Cartesian Product

- The Cartesian product of two sets A and B, denoted by $A \times B$ and read "A cross B", is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

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

$$|A_1 \times A_2 \cdots \times A_n| = |A_1| * |A_2| * \cdots * |A_n|$$

Example:

- What is $A \times B \times C$ 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)}

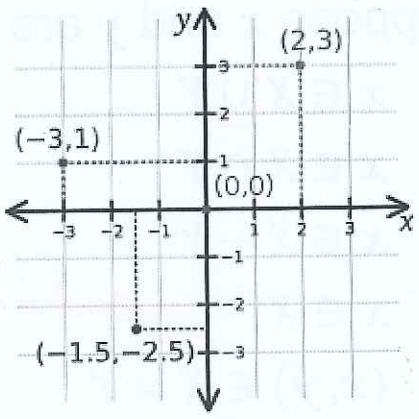
Cartesian Product - Exercise

Let $A = \{1, 2, 3\}$ and $B = \{u, v\}$.

- Find $A \times B$
  - $A \times B = \{(1, u), (1, v), (2, u), (2, v), (3, u), (3, v)\}$
- Find $\mathrm{B} \times A$
  - $B \times A = \{(u, 1), (u, 2), (u, 3), (v, 1), (v, 2), (v, 3)\}$
- Find $\mathrm{B} \times B$
  - $B \times B = \{(u, u), (u, v), (v, u), (v, v)\}$
- Let R denote the set of all real numbers. Describe $\mathrm{R} \times R$
  - $\mathrm{R} \times R$ is the set of all ordered pairs (x, y) where both x and y are real numbers.

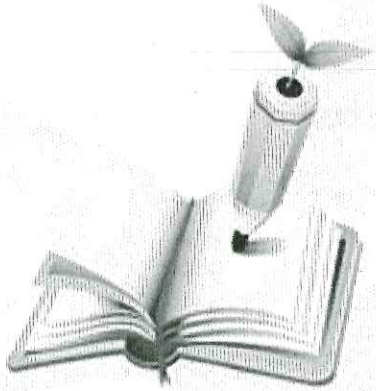
The Cartesian Plane

- $R \times R$: the set of all ordered pairs (x, y) where both x and y are real numbers.
- The Cartesian plane: horizontal and vertical axes are drawn on a plane, each pair (x, y) in $R \times R$ corresponds to a unique point in the plane.



Chapter 6: Set Theory

6.2 Properties of Set



Procedural Versions of Set Definitions

Let X and Y be subsets of a universal set U and suppose x and y are elements of U.

1. $x \in X \cup Y \iff x \in X$ or $x \in Y$
2. $x \in X \cap Y \iff x \in X$ and $x \in Y$
3. $x \in X - Y \iff x \in X$ and $x \notin Y$
4. $x \in X^c \iff x \notin X$ → complement of X
5. $(x, y) \in X \times Y \iff x \in X$ and $y \in Y$

Set Identities

- An identity is an equation that is universally true for all elements in some set.

Let all sets referred to below subsets of a universal set U.

1. Commutative laws: for all sets A and B
   (a) $A \cup B = B \cup A$ and (b) $A \cap B = B \cap A$
2. Associative laws: for all sets A, B and C
   (a) $A \cup (B \cup C) = (A \cup B) \cup C$ and
   (b) $A \cap (B \cap C) = (A \cap B) \cap C$
3. Distributive laws: for all sets A, B and C
   (a) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
   (b) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4. Identity laws: for all sets A,
   (a) $A \cup \emptyset = A$ and (b) $A \cap U = A$
5. Complement law: for all sets A
   (a) $A \cup A^c = U$ and (b) $A \cap A^c = \emptyset$

Set Identities (cont')

6. Double Complement law: for all sets A
   $(A^c)^c = A$
7. Idempotent laws: for all sets A
   (a) $A \cup A = A$ and (b) $A \cap A = A$
8. Universal bound laws: for all sets A
   (a) $A \cup U = U$ and (b) $A \cap \emptyset = \emptyset$
9. De Morgan's law: for all sets A and B
   (a) $(A \cap B)^c = A^c \cup B^c$ and (b) $(A \cup B)^c = A^c \cap B^c$
10. Absorption law: for all sets A and B
    (a) $A \cup (A \cap B) = A$ and (b) $A \cap (A \cup B) = A$
11. Complements of U and $\emptyset$:
    (a) $U^c = \emptyset$ and (b) $\emptyset^c = U$
12. Set Difference Laws: for all sets A and B
    $A - B = A \cap B^c$

Element Argument: The Basic Method for Proving that One Set Is a Subset of Another

- Let set X and Y be given, to prove that $X \subseteq Y$

1. Suppose that x is a particular but arbitrarily chosen element of X,
2. Show that x is an element of Y.

Proving Set Identities

Basic Method for Proving That Sets are Equal

Let sets X and Y be given. To prove that $X = Y$:
1. Prove that $X \subseteq Y$
2. Prove that $Y \subseteq X$

Proving a Distributive Law: for all sets A, B and C,

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

Proof idea:

Suppose A, B and C are arbitrarily chosen sets.

1. Show $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$
   Equivalent to: $\forall x$, if $x \in A \cup (B \cap C)$ then $x \in (A \cup B) \cap (A \cup C)$.
2. Show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.
   Equivalent to: $\forall x$, if $x \in (A \cup B) \cap (A \cup C)$ then $x \in A \cup (B \cap C)$.

Proving A Distributive Law

Theorem 6.2.2(3)(a) A Distributive Law for Sets
For all sets A, B and C,

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

Proof:
Suppose A, B and C are arbitrarily chosen sets.

Proof that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$***:***
Suppose $x \in A \cup (B \cap C)$. By definition of union, $x \in A$ or $x \in B \cap C$.

OR

Case 1 ($x \in A$): Since $x \in A$, then by definition of union $x \in A \cup B$ and $x \in A \cup C$. Hence by definition of intersection, $x \in (A \cup B) \cap (A \cup C)$.

Case 2 ($x \in B \cap C$): Since $x \in B \cap C$, then by definition of intersection $x \in B$ and $x \in C$. Since $x \in B$, $x \in A \cup B$ by definition of union. Similarly, since $x \in C$, $x \in A \cup C$ by definition of union. Hence $x \in (A \cup B) \cap (A \cup C)$ by definition of intersection.

In both cases, $x \in (A \cup B) \cap (A \cup C)$. Hence $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ by definition of subset.

Proving A Distributive Law (cont')

Theorem 6.2.2(3)(a) A Distributive Law for Sets
For all sets A, B and C,

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

Proof (cont'):
Proof that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$**:**
Suppose $x \in (A \cup B) \cap (A \cup C)$. By definition of intersection, $x \in A \cup B$ and $x \in A \cup C$. Consider the two cases $x \in A$ and $x \notin A$.

Case 1 ($x \in A$): Since $x \in A$, we can immediately conclude that $x \in A \cup (B \cap C)$ by definition of union.

Case 2 ($x \notin A$): Since $x \in A \cup B$, x is in at least one of A or B. But x is not in A; hence x is in B. Similarly, since $x \in A \cup C$, x is in at least one of A or C. But x is not in A; hence x is in C. We have shown that both $x \in B$ and $x \in C$, and so by definition of intersection, $x \in B \cap C$. It follows by definition of union that $x \in A \cup (B \cap C)$.

In both cases $x \in A \cup (B \cap C)$. Hence, by definition of subset, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Conclusion: Since both subset relations have been proved, it follows by definition of set equality that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof of a De Morgan's Law for Sets

Theorem 6.2.2(9)(a) A De Morgan's Law for Sets
For all sets A, B and C, $(A \cup B)^c = A^c \cap B^c$

Proof:
Suppose A and B are arbitrarily chosen sets.

Proof that $(\mathbf{A \cup B})^{\mathbf{c}} \subseteq \mathbf{A^c \cap B^c}$:
Suppose $x \in (A \cup B)^c$. [*We must show that* $x \in A^c \cap B^c$].

- By definition of complement, $x \notin A \cup B$, which means "it is false that (x is in A or x is in B)."
- By De Morgan's laws of logic, this implies that "x is not in A and x is not in B", symbolically, $x \notin A$ and $x \notin B$. Hence, by the definition of complement, $x \in A^c$ and $x \in B^c$.
- It follows that $x \in A^c \cap B^c$ by the definition of intersection [as was to be shown.]

So, by the definition of subset, $(A \cup B)^c \subseteq A^c \cap B^c$.

Proof of a De Morgan's Law for Sets (cont')

Theorem 6.2.2(9)(a) A De Morgan's Law for Sets
For all sets A, B and C, $(A \cup B)^c = A^c \cap B^c$

Proof (cont'):
Suppose A and B are arbitrarily chosen sets.

Proof that $\mathbf{A^c \cap B^c} \subseteq (\mathbf{A \cup B})^{\mathbf{c}}$:
Suppose $x \in \mathbf{A^c \cap B^c}$. [*We must show that* $(\mathbf{A \cup B})^{\mathbf{c}}$].

- By definition of intersection, $x \in \mathbf{A^c}$ and $x \in \boldsymbol{B^c}$.
- By definition of complement, $x \notin \boldsymbol{A}$ and $x \notin \boldsymbol{B}$. In other words, x is not in A and x is not in B.
- By De Morgan's laws of logic, this implies that "it is false that x is in A or x is in B", which can be written as $x \notin A \cup B$ by the definition of union.
- Hence, by the definition of complement, $x \in (\mathbf{A \cup B})^{\mathbf{c}}$[as was to be shown.]

So, by the definition of subset,$\mathbf{A^c \cap B^c} \subseteq (\mathbf{A \cup B})^{\mathbf{c}}$.

Conclusion: since both set containments have been proved, by the definition of set equality $(A \cup B)^c = A^c \cap B^c$.

Intersection and Union with a Subset

Theorem 6.2.3 Intersection and Union with a Subset
For any sets A and B, if $A \subseteq B$, then
(a) $A \cap B = A$ and (b) $A \cup B = B$.

Proof:

Part (a):
Suppose A and B are sets with $A \subseteq B$. To show part (a) we must show both that $A \cap B \subseteq A$ and that $A \subseteq A \cap B$. We already know that $A \cap B \subseteq A$ by the inclusion of intersection property.

To show that $A \subseteq A \cap B$, let $x \in A$. *[We must show that $x \in A \cap B$.]* Since $A \subseteq B$, then $x \in B$ also. Hence

$$x \in A \text{ and } x \in B,$$

and thus $x \in A \cap B$ by definition of intersection *[as was to be shown]*.

Proof:
Part (b): The proof of part (b) is left as an exercise.

The Empty Set

- The empty set: denoted as ∅ or { }, has no elements. It is also called null set.

Theorem 6.2.4 A Set with No Elements Is a Subset of Every Set

If E is a set with no elements and A is any set, then $E \subseteq A$.

Corollary 6.2.5 Uniqueness of the Empty Set

There is only one set with no elements.

Element Method for Proving a Set Equals the Empty Set

To prove that a set X is equal to the empty set ∅, prove that X has no elements. To do this, suppose X has an element and derive a contradiction.

Proving a Set Equal the Empty Set

Example: Prove that for any set A, $A \cap \emptyset = \emptyset$.

Solution: Let A be a *[particular, but arbitrarily chosen]* set. To show that $A \cap \emptyset = \emptyset$, it suffices to show that $A \cap \emptyset$ has no elements.

Suppose there is an element x such that $x \in A \cap \emptyset$. Then, by definition of intersection, $x \in A$ and $x \in \emptyset$. In particular, $x \in \emptyset$. But this is impossible since $\emptyset$ has no elements.

[This contradiction shows that the supposition that there is an element x in $A \cap \emptyset$ is false. So $A \cap \emptyset$ has no elements, as was to be shown.]

Thus $A \cap \emptyset = \emptyset$.

A Proof for a Conditional Statement

Proposition 6.2.6:

For all sets A, B and C, if $A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \emptyset$.

Proof:

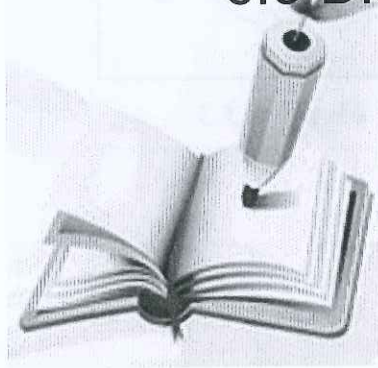
Suppose A, B and C, are any sets such that $A \subseteq B$ and $B \subseteq C^c$. We must show that $A \cap C = \emptyset$.

- Suppose not. That is, suppose there is an element x in $A \cap C$.
- By definition of intersection, $x \in A$ and $x \in C$. Then, since $A \subseteq B$, $x \in B$ by definition of subset.
- Also, since $B \subseteq C^c$, then $x \in C^c$ by definition of subset again.
- It follows by definition of complement that $x \notin C$.
- Thus $x \in C$ and $x \notin C$, which is a contradiction.

So the supposition that there is an element x in $A \cap C$ is false, and thus $A \cap C = \emptyset$ *[as was to be shown]*.

Chapter 6: Set Theory

6.3 Disproofs, and Algebraic Proofs



Disproof a Set Identity with a Counterexample

- Is the following set property true?

  For all sets A, B and C, $(A - B) \cup (B - C) = A - C$

$(A-B) \cup (B-C)$ $\qquad$ $A-C$

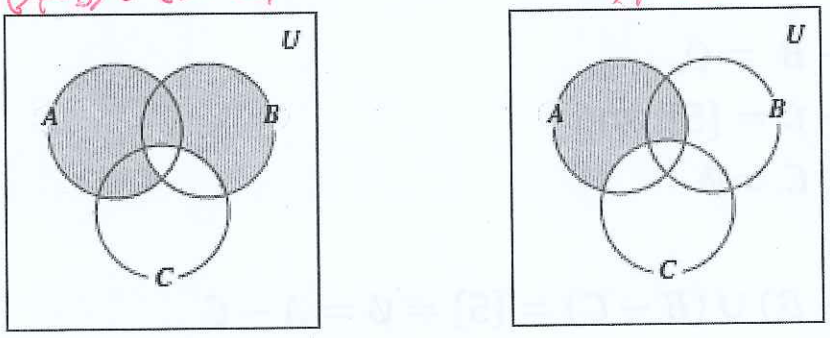


Figure 6.3.2

Disproof a Set Identity with a Counterexample

- Counterexample 1:

  Let $A = \{1,2,4,5\}$, $B = \{2,3,5,6\}$ and $C = \{4,5,6,7\}$

  Then,

  $A - B = \{1,4\}$, ?

  $B - C = \{2,3\}$, and

  $A - C = \{1,2\}$

  Hence,

  $(A - B) \cup (B - C) = \{1,2,3,4\}$

  $\neq A - C$

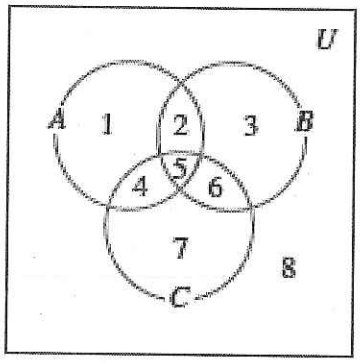


Figure 6.3.3

Disproof a Set Identity with a Counterexample

- Counterexample 2:

  Let $A = \emptyset$, $B = \{5\}$ and $C = \emptyset$

  Then,

  $A - B = \emptyset$,

  $B - C = \{5\}$, and

  $A - C = \emptyset$

  Hence,

  $(A - B) \cup (B - C) = \{5\} \neq \emptyset = A - C$

Disproof a Set Identity with a Counterexample

- Counterexample 3:

  Let $A = \{1\}$, $B = \emptyset$ and $C = \{1\}$

  Then,

  $A - B = \{1\}$,

  $B - C = \emptyset$, and

  $A - C = \emptyset$

  Hence,

  $(A - B) \cup (B - C) = \{1\} \neq \emptyset = A - C$

The Number of Subsets of a Set

Theorem 6.3.1

For all integers $n \geq 0$, if a set X has n elements, then $\mathscr{P}(X)$ has 2^n elements.

Proof (by mathematical induction):

Let the property $P(n)$ be the sentence

Any set with n elements has 2^n subsets. $\leftarrow P(n)$

Show that $P(0)$ is true:

To establish $P(0)$, we must show that

Any set with 0 elements has 2^0 subsets. $\leftarrow P(0)$

But the only set with zero elements is the empty set, and the only subset of the empty set is itself.

Thus a set with zero elements has one subset. Since $1 = 2^0$, we have that $P(0)$ is true.

The Number of Subsets of a Set

Show that for all integers $k \geq 0$, if $P(k)$ is true then $P(k+1)$ is also true: *[Suppose that $P(k)$ is true for a particular but arbitrarily chosen integer $k \geq 0$. That is:]*

Suppose that k is any integer with $k \geq 0$ such that

Any set with k elements has 2^k subsets. ← $P(k)$ inductive hypothesis

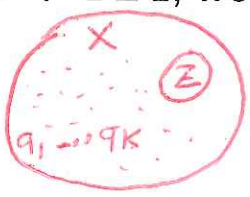
[We must show that $P(k+1)$ is true. That is:]

We must show that

Any set with $k+1$ elements has 2^{k+1} subsets. ← $P(k+1)$

The Number of Subsets of a Set

Let X be a set with $k+1$ elements. Since $k+1 \geq 1$, we may pick an element z in X.



$\{z\}$ = 1 element
$\{X\}$ = k element
$X = 2^k$
$Z = 2^1$

- Any subset of X either contains z or not.
- Any subset of X that does not contain z is a subset of $X - \{z\}$.
- Any subset A of $X - \{z\}$ can be matched up with a subset B, equal to $A \cup \{z\}$, of X that contains z.

Consequently, there are as many subsets of X that contain z as do not, and thus there are twice as many subsets of X as there are subsets of $X - \{z\}$.

The Number of Subsets of a Set

But $X - \{z\}$ has k elements, and so

$$\text{the number of subsets of } X - \{z\} = 2^k \qquad \text{by inductive hypothesis.}$$

Therefore,

$$\begin{aligned}\text{the number of subsets of } X &= 2 \cdot (\text{the number of subsets of } X - \{z\}) \\ &= 2 \cdot (2^k) && \text{by substitution} \\ &= 2^{k+1} && \text{by basic algebra.}\end{aligned}$$

[This is what was to be shown.]
[Since we have proved both the basis step and the inductive step, we conclude that the theorem is true.]

"Algebraic" Proofs of Set Identities

Construct an algebraic proof Set Difference Property,

$$(A \cup B) - C = (A - C) \cup (B - C).$$

Solution:

$$\begin{aligned}(A \cup B) - C &= (A \cup B) \cap C^c && \text{by the set difference law} \\ &= C^c \cap (A \cup B) && \text{by the commutative law for } \cap \\ &= (C^c \cap A) \cup (C^c \cap B) && \text{by the distributive law} \\ &= (A \cap C^c) \cup (B \cap C^c) && \text{by the commutative law for } \cap \\ &= (A - C) \cup (B - C) && \text{by the set difference law.}\end{aligned}$$

Deriving a Set Identity Using Properties of ∅

Construct an algebraic proof that for all sets A and B,

$$A - (A \cap B) = A - B.$$

Solution:

$$\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^c && \text{by the set difference law} \\
&= A \cap (A^c \cup B^c) && \text{by De Morgan's laws} \\
&= (A \cap A^c) \cup (A \cap B^c) && \text{by the distributive law} \\
&= \emptyset \cup (A \cap B^c) && \text{by the complement law} \\
&= (A \cap B^c) \cup \emptyset && \text{by the commutative law} \\
&= A \cap B^c && \text{by the Identity law for } \cup \\
&= A - B && \text{by the set difference law}
\end{aligned}$$

Cartesian Product

- The Cartesian product of two sets A and B, denoted by $A \times B$ and read "A cross B", is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

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

$$|A_1 \times A_2 \cdots \times A_n| = |A_1| * |A_2| * \cdots * |A_n|$$

Example:

- What is $A \times B \times C$ 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)}

Relation

- Let A and B be sets. A relation R from *A to B* is a subset of Cartesian product $A \times B$,

$$R \subseteq A \times B$$

- $R \subseteq A \times B$ means R is a set of ordered pairs of the form (a, b) where $a \in A$ and $b \in B$.
- The set A is called the domain of R and the set B is called its co-domain.
- Given an ordered pair (x, y) in $A \times B$, $x\ R\ y$ if and only if $(x, y) \in R$.
- Notation:
  - $x\ R\ y$ denotes x is related to y by R, means that $(x, y) \in R$
  - $x \not R\ y$ denotes x is not related to y by R, means that $(x, y) \notin R$

Relation - Exercise

- Let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$ and define a relation R from A to B as follows: Given any $(x, y) \in A \times B$,

$$(x, y) \in R \text{ means that } \frac{x+y}{2} \text{ is an integer.}$$

a. State explicitly which ordered pairs are in $A \times B$ and which are in R.

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

2) Examine each ordered pair in $A \times B$ to see whether its elements satisfy the defining condition for R:

$(1,1) \in R$, $(1,2) \notin R$, $(1,3) \in R$, $(2,1) \notin R$, $(2,2) \in R$, $(2,3) \notin R$

Thus, $R = \{(1,1), (1,3), (2,2)\}$

b. Is $1\ R\ 3$? Yes

c. Is $2\ R\ 3$? No

d. Is $2\ R\ 2$? Yes

e. What are the domain and co-domain of R?

➢ The domain of R is $A = \{1, 2\}$ and the co-domain is $B = \{1, 2, 3\}$

Arrow Diagram of a Relation

Suppose R is a relation from a set A to a set B. The arrow diagram for R is obtained as follows:

- Represent the elements of A as points in one region and the elements of B as points in another region.
- For each x in A and y in B, drawn an arrow from x to y if, and only if, x is related to y by R. Symbolically:

Drawn an arrow from x to y

If, and only if, $x\ R\ y$

If, and only if, $(x, y) \in R$.

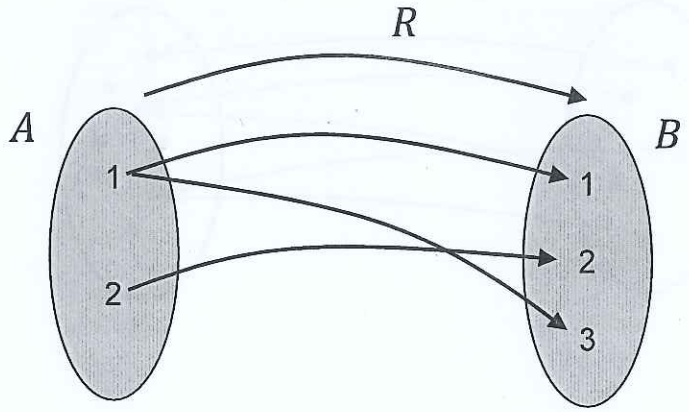
$R = \{(1,1), (1,3), (2,2)\}$

Arrow Diagram of a Relation

Let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$ and define a relation R from A to B as follows: Given any $(x, y) \in A \times B$,

$(x, y) \in R$ means that $\frac{x+y}{2}$ is an integer.

$R = \{(1,1), (1,3), (2,2)\}$.



Functions

Definition: A function f from a set A to a set B, denoted as $f : A \to B$, is a relation with domain A and co-domain B that satisfies the following two properties:

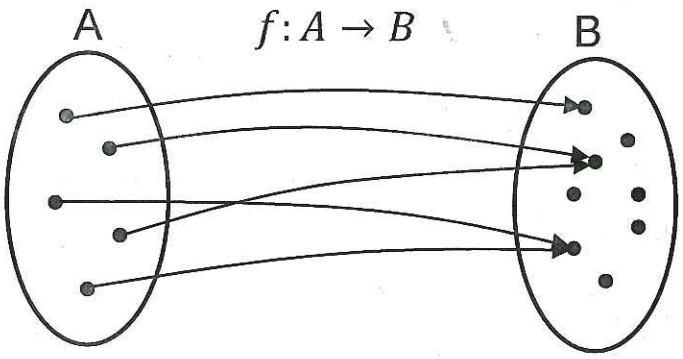
- For every element x in A, there is an element y in B such that $(x, y) \in f$ (there is at least one element of B that is related to x by f)
- For all elements x in A and y and z in B,

  If $(x, y) \in f$ and $(x, z) \in f$, then $y = z$.

  (there is at most one element of B that is related to x by f)

Functions

The Function $f : A \to B$ assigns exactly one element of B to each element of A.

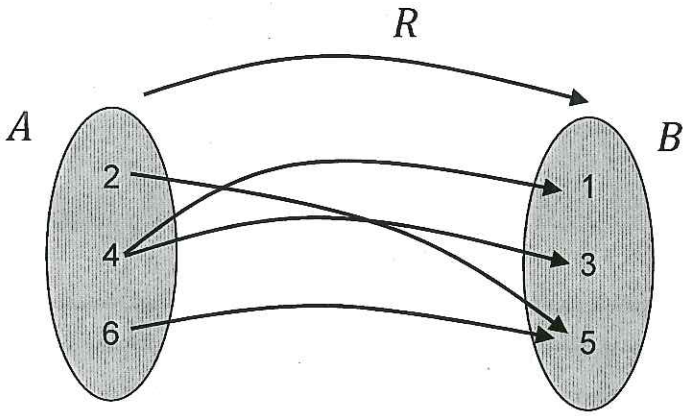


Functions – Exercise 1

Let $A = \{2, 4, 6\}$ and $B = \{1, 3, 5\}$. Which of the relations $R, S,$ and T defined below are functions from A to B?

a. $R = \{(2,5), (4,1), (4,3), (6,5)\}$

– No. The element 4 in A is mapped to two elements 1 and 3 in B.

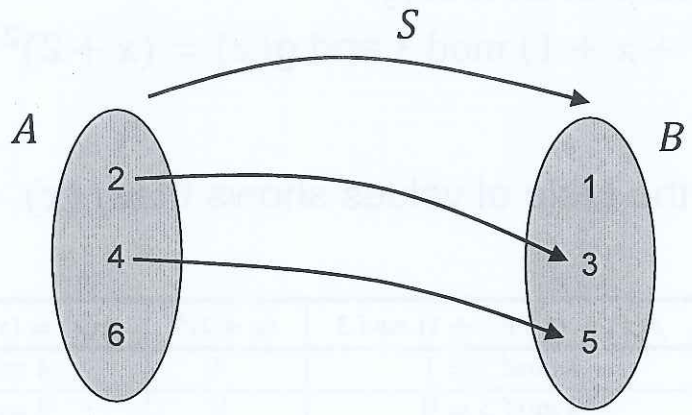


Functions – Exercise 1

Let $A = \{2, 4, 6\}$ and $B = \{1,\ 3, 5\}$. Which of the relations R, S, and T defined below are functions from A to B?

b. for all $(x, y) \in A \times B$, $(x, y) \in S$ means that $y = x + 1$

– No. The element 6 in A is not related to any element in B by S.

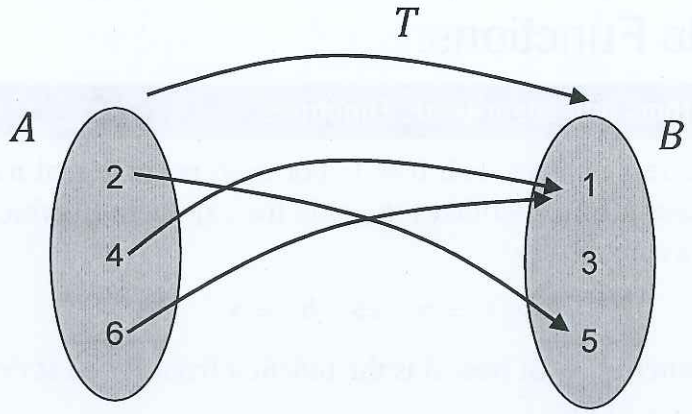


Functions – Exercise 1

Let $A = \{2, 4, 6\}$ and $B = \{1,\ 3, 5\}$. Which of the relations R, S, and T defined below are functions from A to B?

c. T is defined by the arrow diagram.

– Yes. $T(2) = 5, T(4) = 1, T(6) = 1$.



A Test for Function Equality

Theorem 7.1.1 A Test for Function Equality

If $F: X \to Y$ and $G: X \to Y$ are functions, then $F = G$ if, and only if, $F(x) = G(x)$ for all $x \in X$.

Example: Let $J_3 = \{0, 1, 2\}$, and define functions f and g from J_3 to J_3 as follows: For all x in J_3,

$$f(x) = (x^2 + x + 1) \bmod 3 \text{ and } g(x) = (x + 2)^2 \bmod 3$$

Does $f = g$?

Solution: Yes, the table of values shows that $f(x) = g(x)$ for all all x in J_3

x	$x^2 + x + 1$	$f(x) = (x^2 + x + 1)$ *mod* 3	$(x + 2)^2$	$g(x) = (x + 2)^2$ *mod* 3
0	1	1 *mod* 3 = 1	4	4 *mod* 3 = 1
1	3	3 *mod* 3 = 0	9	9 *mod* 3 = 0
2	7	7 *mod* 3 = 1	16	16 *mod* 3 = 1

Examples of Functions

- Identity function:

  Given a set X, define a function I_x from X to X by

  $$I_x(x) = x \text{ for all } x \text{ in } X.$$

  The function I_x is called the **identity function on X** because it sends each element of X to the element that is identical to it.

- Logarithmic Functions:

• Definition Logarithms and Logarithmic Functions

Let b be a positive real number with $b \neq 1$. For each positive real number x, the **logarithm with base b of x,** written $\log_b x$, is the exponent to which b must be raised to obtain x. Symbolically,

$$\log_b x = y \quad \Leftrightarrow \quad b^y = x.$$

The **logarithmic function with base b** is the function from $\mathbf{R}^+$ to $\mathbf{R}$ that takes each positive real number x to $\log_b x$.

Note: $b^{\log_b x} = x$, $\log_b b^m = m$

Boolean Functions

• Definition

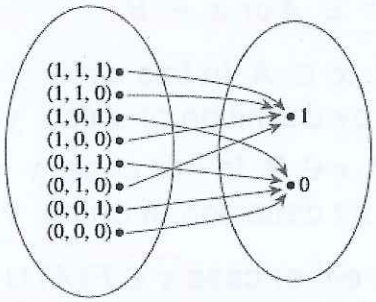
An **(n-place) Boolean function** f is a function whose domain is the set of all ordered n-tuples of 0's and 1's and whose co-domain is the set {0, 1}. More formally, the domain of a Boolean function can be described as the Cartesian product of n copies of the set {0, 1}, which is denoted $\{0, 1\}^n$. Thus f: $\{0, 1\}^n \rightarrow \{0, 1\}$.

Boolean function $f(x_1, x_2, \cdots, x_n)$:

- $x_1, x_2, \cdots, x_n$: Boolean variable {0,1}
- The output $f(x_1, x_2, \cdots, x_n) \in \{0,1\}$

Example: $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \bmod 2 = 3 \bmod 2$

Input			Output
x_1	x_2	x_3	$(x_1 + x_2 + x_3)\ mod\ 2$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0



Functions Acting on Sets

• Definition

If $f: X \rightarrow Y$ is a function and $A \subseteq X$ and $C \subseteq Y$, then

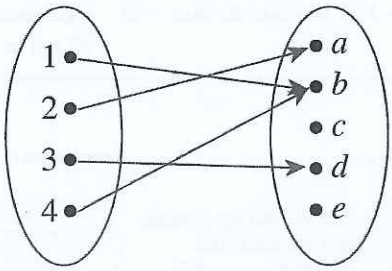
$$f(A) = \{y \in Y \mid y = f(x) \text{ for some } x \text{ in } A\}$$

and

$$f^{-1}(C) = \{x \in X \mid f(x) \in C\}.$$

$f(A)$ is called the **image of A**, and $f^{-1}(C)$ is called the **inverse image of C**.

Let $X = \{1, 2, 3, 4\}$ and $Y = \{a, b, c, d, e\}$, and define $F: X \rightarrow Y$ by the following arrow diagram. Let $A = \{1, 4\}$, $C = \{a, b\}$, and $D = \{c, e\}$. Find $F(A)$, $F(X)$, $F^{-1}(C)$, and $F^{-1}(D)$.



Solution: $F(A) = \{b\}$, $F(X) = \{a, b, d\}$, $F^{-1}(C) = \{1,2,4\}$, and $F^{-1}(D) = \emptyset$

Interactions of a Function with Union

Let X and Y be sets, let F be a function from X to Y, and let A and B be any subsets of X. Prove that

$$F(A \cup B) \subseteq F(A) \cup F(B).$$

Hint: y is any element in $F(A \cup B)$, then y is an element of $F(A \cup B)$.

Proof: Suppose $y \in F(A \cup B)$. *[We must show that $y \in F(A) \cup F(B)$.]*
By definition of function, $y = F(x)$ for some $x \in A \cup B$. By definition of union, $x \in A$ *or* $x \in B$. if $x \in A$ then $y \in F(A)$, if $x \in B$ then $y \in F(B)$

Case 1, $x \in A$: In this case, $y = F(x)$ for some x in A. Hence $y \in F(A)$, and so by definition of union, $y \in F(A) \cup F(B)$.

Case 2, $x \in B$: In this case, $y = F(x)$ for some x in B. Hence $y \in F(B)$, and so by definition of union, $y \in F(A) \cup F(B)$.

Thus in either case $y \in F(A) \cup F(B)$ *[as was to be shown].*

7.2 One-to-One Functions

• Definition

Let F be a function from a set X to a set Y. F is **one-to-one** (or **injective**) if, and only if, for all elements x_1 and x_2 in X,

$$\text{if } F(x_1) = F(x_2), \text{ then } x_1 = x_2,$$

or, equivalently,

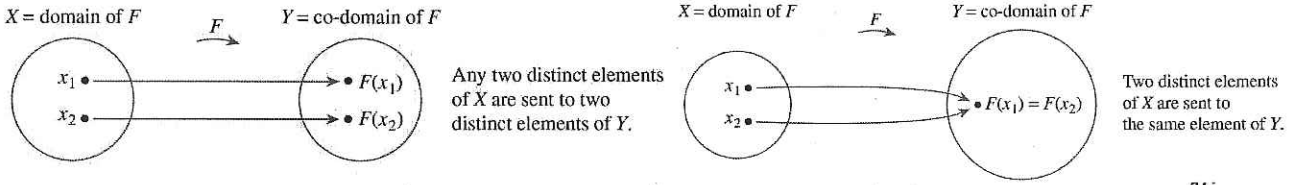
$$\text{if } x_1 \neq x_2, \text{ then } F(x_1) \neq F(x_2).$$

Symbolically,

$$F: X \to Y \text{ is one-to-one} \Leftrightarrow \forall x_1, x_2 \in X, \text{ if } F(x_1) = F(x_2) \text{ then } x_1 = x_2.$$

No multiple arrows in to right side

A function $F: X \to Y$ is *not* one-to-one $\Leftrightarrow$ $\exists$ elements x_1 and x_2 in X with $F(x_1) = F(x_2)$ and $x_1 \neq x_2$.



One-to-One Functions on Infinite Sets

Suppose f is a function defined on an infinite set X. By definition, f is one-to-one if, and only if, the following universal statement is true:

$$\forall x_1, x_2 \in X, \text{ if } f(x_1) = f(x_2) \text{ then } x_1 = x_2.$$

- To prove f is one-to-one:

  Use the method of direct proof: **Suppose** x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$ and **Show** that $x_1 = x_2$.

- To show that *f* is *not* one-to-one:

  Find elements x_1 and x_2 in X so that $f(x_1) = f(x_2)$ but $x_1 \neq x_2$.

Example 2 – Proving or Disproving That Functions Are One-to-One

Define $f : \boldsymbol{R} \to \boldsymbol{R}$ and g: $\boldsymbol{Z} \to \boldsymbol{Z}$ by the rules.

$$f(x) = 4x - 1 \text{ for all } x \in R$$

$4x_1 - 1 = 4x_2 - 1 \rightarrow 4x_1 = 4x_2 \rightarrow x_1 = x_1$ ✓ one to one

and

$$g(n) = n^2 \text{ for all } n \in Z$$

= No but it is for Z^+

a. Is f one-to-one? Prove or give a counterexample.

b. Is g one-to-one? Prove or give a counterexample.

Example 2 – Solution (a)

Answer to (a):

If the function $f: \mathbf{R} \to \mathbf{R}$ is defined by the rule $f(x) = 4x - 1$, for all real numbers x, then f is one-to-one.

Proof:

Suppose x_1 and x_2 are elements of X such that $f(x_1) = f(x_2)$. *[We must show that $x_1 = x_2$.]*

By definition of f,

$$4x_1 - 1 = 4x_2 - 1$$

Adding 1 to both sides gives

$$4x_1 = 4x_2$$

and dividing both sides by 4 gives

$$x_1 = x_2$$

which is what was to be shown.

Example 2 – Solution (b)

Answer to (b):

If the function $g: \mathbf{Z} \to \mathbf{Z}$ is defined by the rule $g(n) = n^2$, for all $n \in \mathbf{Z}$, then g is not one-to-one.

Counterexample:

Let $n_1 = 2$ and $n_2 = -2$. Then by definition of g,

$$g(n_1) = g(2) = 2^2 = 4 \quad \text{and also}$$
$$g(n_2) = g(-2) = (-2)^2 = 4.$$

Hence

$$g(n_1) = g(n_2) \quad \text{but} \quad n_1 \neq n_2,$$

and so g is not one-to-one.