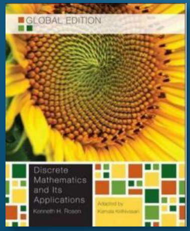
Basic Structures: Functions, Sequences, and Cardinality

Chapter 2



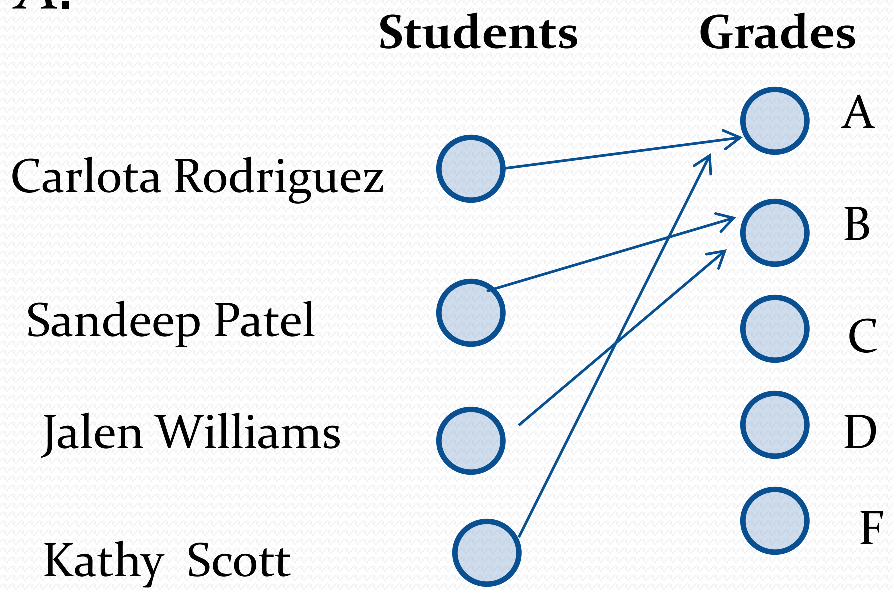
- Taken from the instructor's resource of *Discrete Mathematics and Its Applications*, 7/e
- Edited by Shin Hong hongshin@handong.edu

Functions

Let A and B be nonempty sets.

A *function* f from A to B, denoted $f: A \rightarrow B$ is an assignment of each element of A to exactly one element of B. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A.

- Functions are sometimes called *mappings* or *transformations*.



Functions

- A function f: $A \to B$ can also be defined as a subset of $A \times B$ (a relation). This subset is restricted to be a relation where no two elements of the relation have the same first element.
- Specifically, a function f from A to B contains one, and only one ordered pair (a, b) for every element $a \in A$.

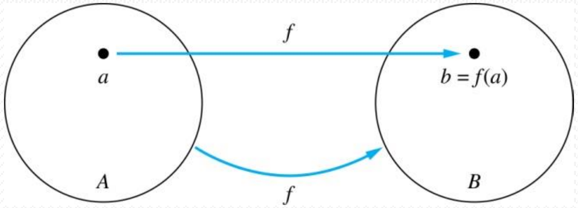
$$\forall x[x \in A \to \exists y[y \in B \land (x, y) \in f]]$$

and

$$\forall x, y_1, y_2[[(x, y_1) \in f \land (x, y_2)] \to y_1 = y_2]$$

Functions

Given a function f: $A \rightarrow B$:



- We say f *maps* A to B *or*

  f is a *mapping* from A to B.
- A is called the *domain* of f.
- B is called the *codomain* of f.
- If $f(a) = b$,
  - then b is called the *image* of a under f.
  - a is called the *preimage* of b.

Questions

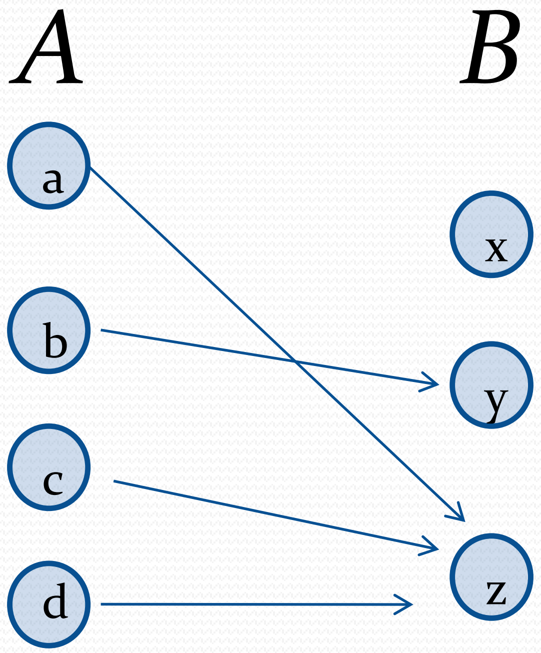
$f(\mathrm{a}) = ?$ z

The image of d is ? z

The domain of f is ? A

The codomain of f is ? B

The preimage of y is ? b



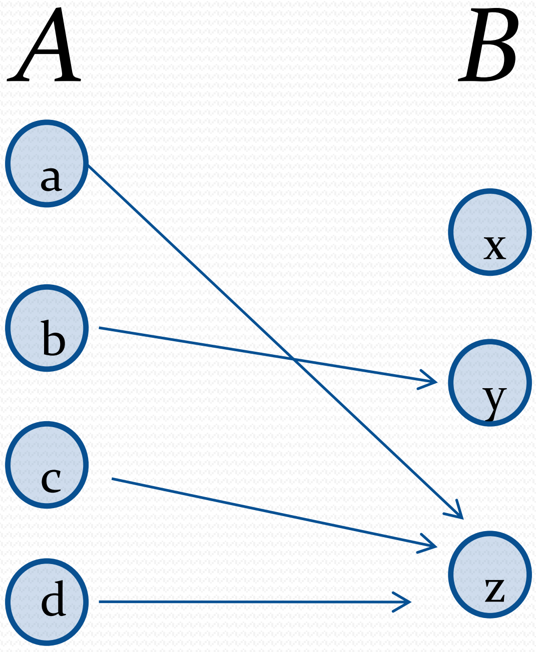
Question on Functions and Sets

- If $f : A \rightarrow B$ and S is a subset of A, then

$$f(S) = \{f(s) | s \in S\}$$

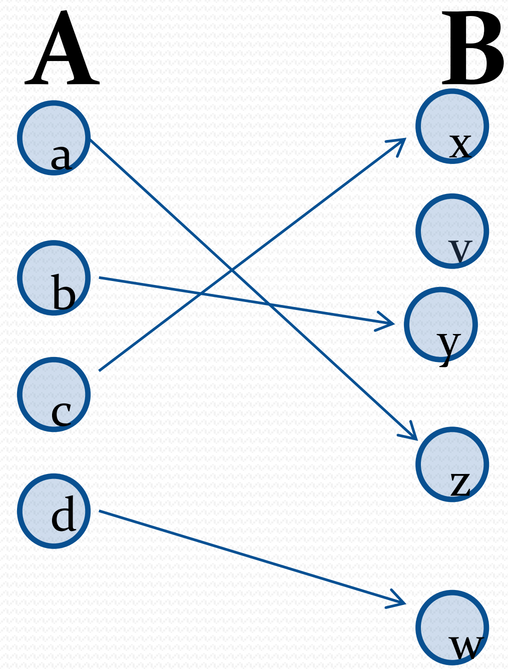
f {a,b,c,} is ? {y,z}

f {c,d} is ? {z}



Injections

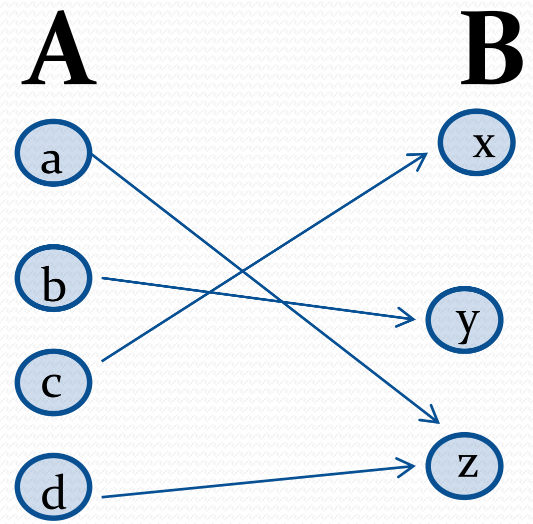
Definition: A function f is said to be *one-to-one* , or *injective*, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. A function is said to be an *injection* if it is one-to-one.



Surjections

A function $f : A \to B$ is called *onto* or *surjective* iff for every element $b \in B$ there is an element $a \in A$ such that $f(a) = b$.

A function *f* is called a *surjection* if it is **onto**.



Example

Example 1: for $f : \{a,b,c,d\} \rightarrow \{1,2,3\}$, $f(a) = 3$, $f(b) = 2$, $f(c) = 1$, and $f(d) = 3$. Is f an onto function?

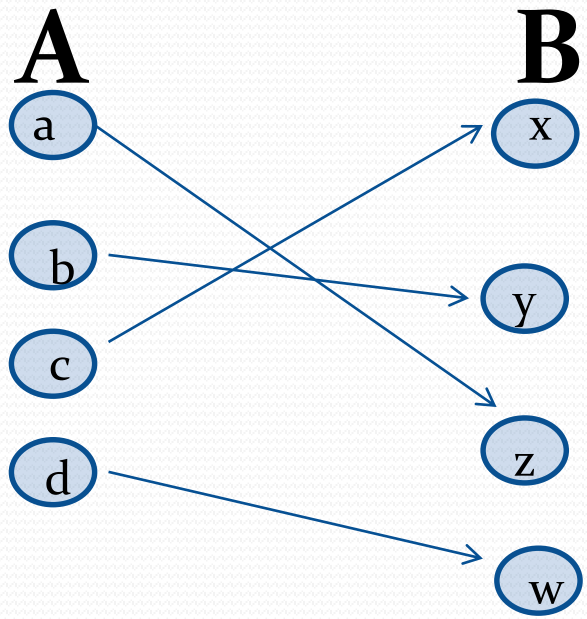
Solution: Yes, f is onto since all three elements of the codomain are images of elements in the domain.

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

Solution: No, f is not onto because there is no integer x with $x^2 = -1$, for example.

Bijections

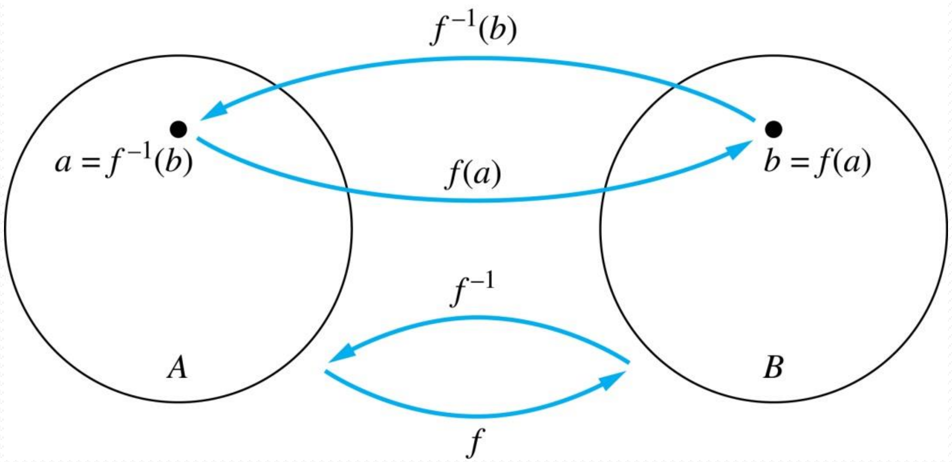
A function f is a ***one-to-one correspondence***, or a *bijection*, if it is both one-to-one and onto (surjective and injective).



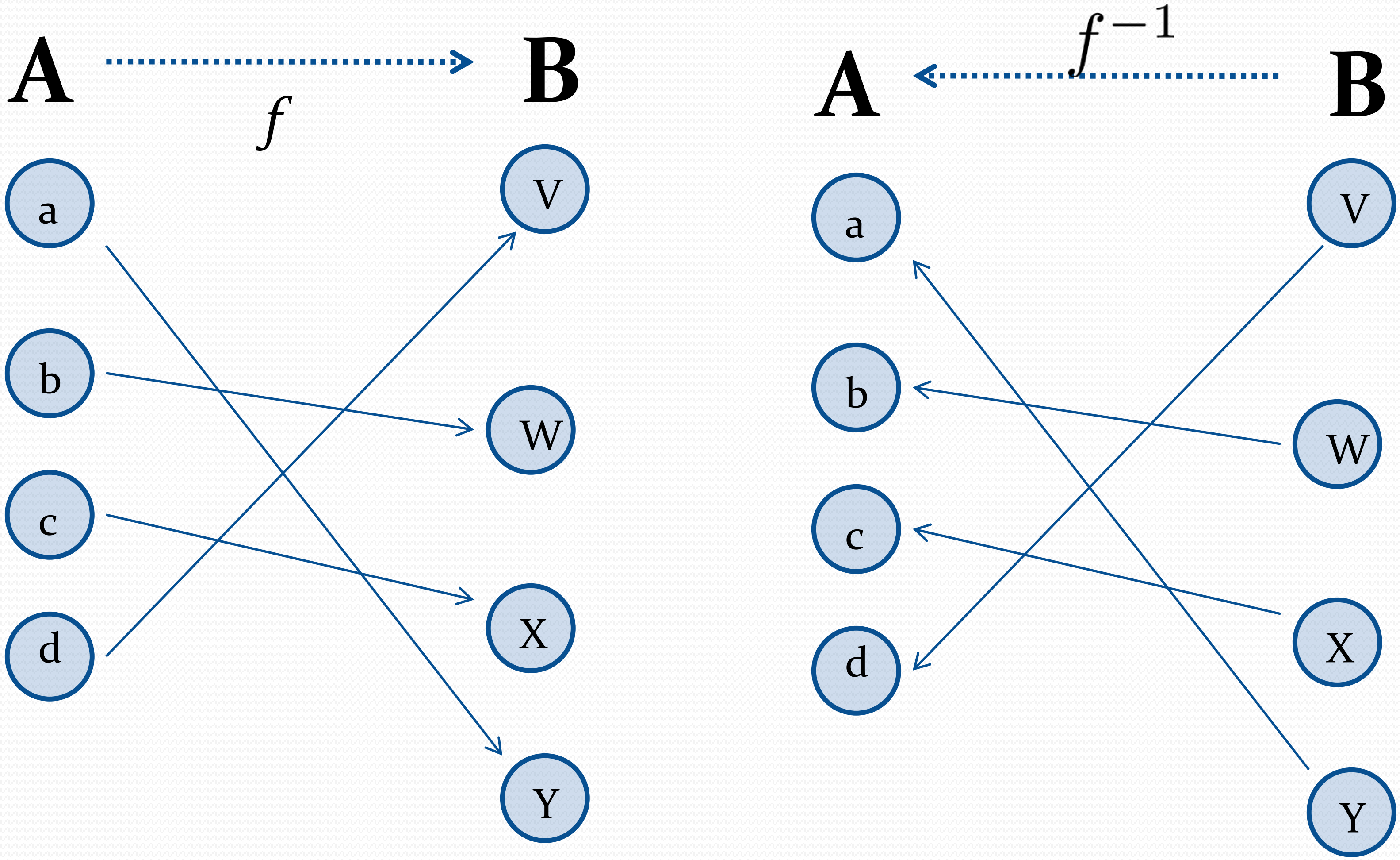
Inverse Functions

Definition: Let *f* be a bijection from *A* to *B*. Then the *inverse* of *f*, denoted f^{-1}, is the function from *B* to *A* defined as $f^{-1}(y) = x \text{ iff } f(x) = y$

No inverse exists unless *f* is a bijection. Why?



Inverse Functions



Questions

Example 2: Let f: **Z** → **Z** be such that $f(x) = x + 1$. Is f invertible, and if so, what is its inverse?

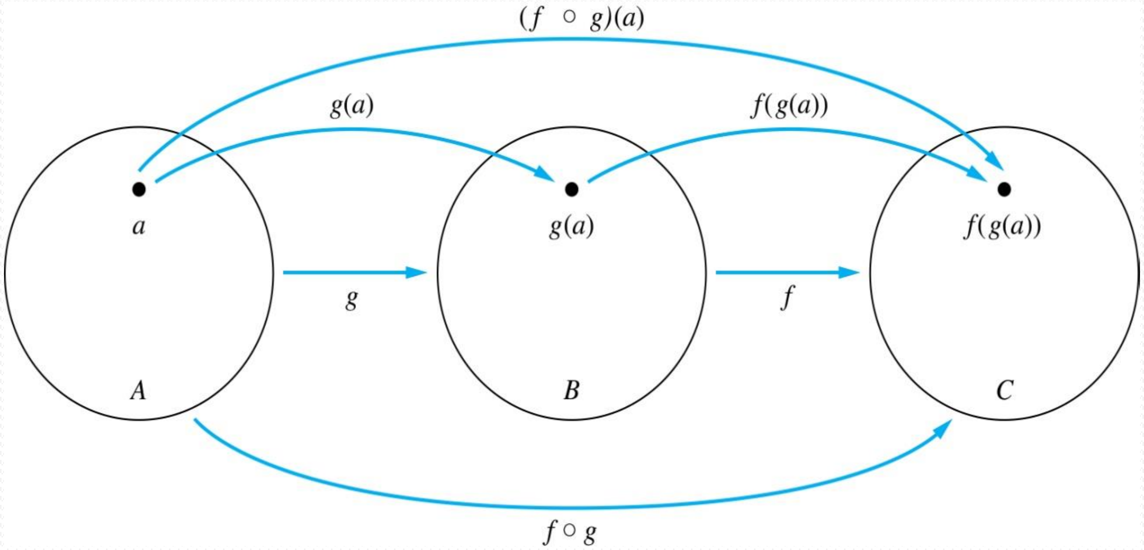
Solution: The function f is invertible because it is a one-to-one correspondence. The inverse function f^{-1} reverses the correspondence so $f^{-1}(x) = y - 1$.

Example 3: Let f: **R** → **R** be such that $f(x) = x^2$. Is f invertible, and if so, what is its inverse?

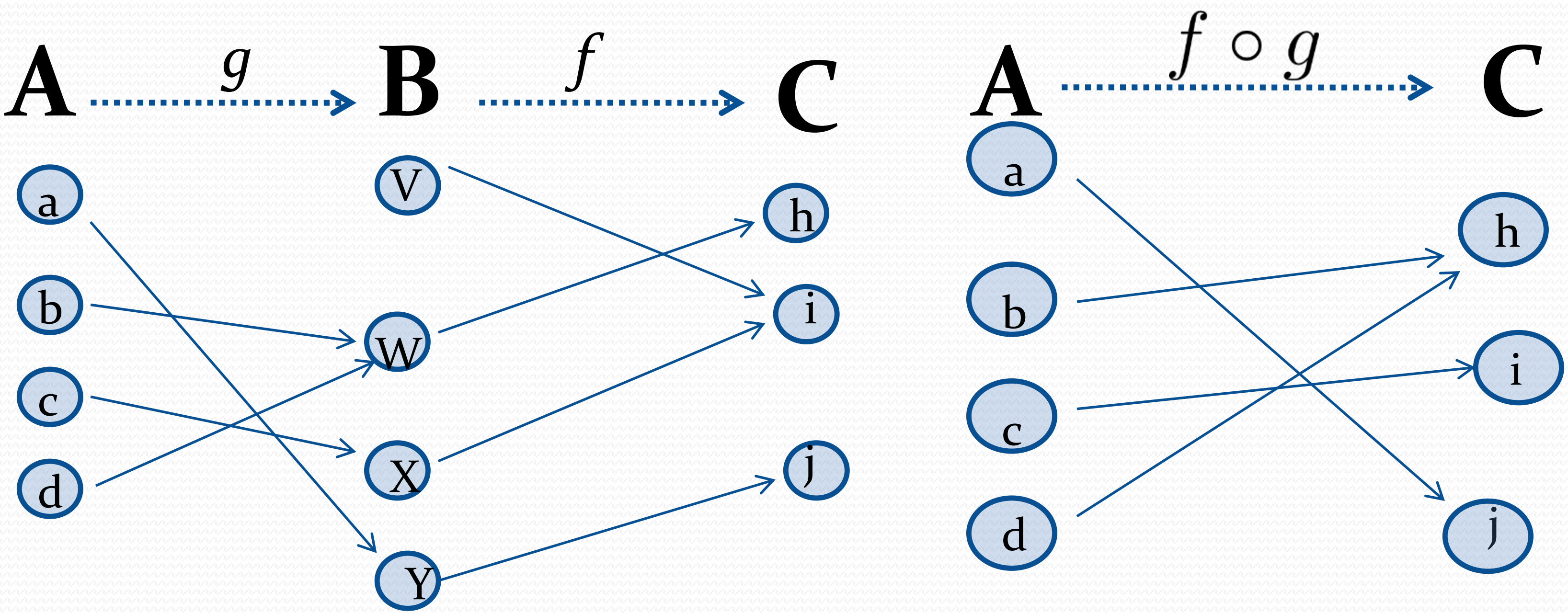
Solution: The function f is not invertible because it is neither one-to-one nor onto .

Composition

- **Definition**: Let *f*: *B* → *C*, *g*: *A* → *B*. The *composition of f with g*, denoted $f \circ g$ is the function from *A* to *C* defined by $$f \circ g(x) = f(g(x))$$



Composition



Composition

Example 1: If $f(x) = x^2$ and $g(x) = 2x + 1$, then

$$f(g(x)) = (2x+1)^2$$

and

$$g(f(x)) = 2x^2 + 1$$

Composition Questions

Example 2: Let g be the function from the set $\{a,b,c\}$ to itself such that $g(a) = b$, $g(b) = c$, and $g(c) = a$. Let f be the function from the set $\{a,b,c\}$ to the set $\{1,2,3\}$ such that $f(a) = 3$, $f(b) = 2$, and $f(c) = 1$.

What is the composition of f and g, and what is the composition of g and f.

Solution: The composition $f \circ g$ is defined by

$f \circ g\ (a) = f(g(a)) = f(b) = 2.$

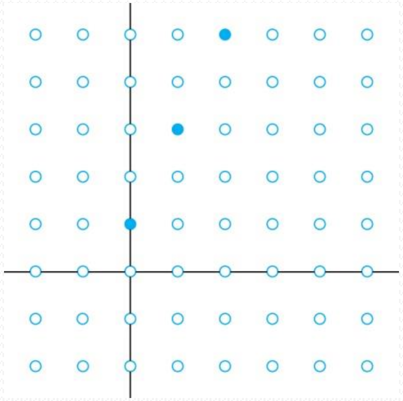
$f \circ g\ (b) = f(g(b)) = f(c) = 1.$

$f \circ g\ (c) = f(g(c)) = f(a) = 3.$

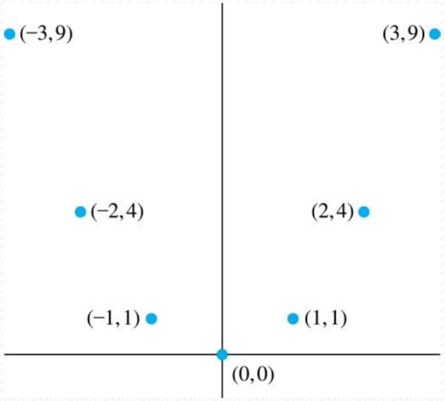
Note that $g \circ f$ is not defined, because the range of f is not a subset of the domain of g.

Graphs of Functions

- Let f be a function from the set A to the set B. The *graph* of the function f is the set of ordered pairs $\{(a,b) \mid a \in A \text{ and } f(a) = b\}$.



Graph of $f(n) = 2n + 1$ from Z to Z



Graph of $f(x) = x^2$ from Z to Z

Partial Functions

A *partial function* f from a set A to a set B, *denoted* $f: A \multimap$
$\longrightarrow B$

is an assignment to each element a in a subset of A, called the *domain of definition* of f, of a unique element b in B.

- f is *undefined* for elements in A that are not in the domain of definition of f.
- When the domain of definition of f equals A, we say that f is a *total function*.

Example: f: $\mathbf{Z} \rightarrow \mathbf{R}$ where $f(n) = \sqrt{n}$ is a partial function because of nonnegative integers; f is undefined for negative integers.

Sequences

A *sequence* is a function from a subset of the integers (usually either the set {0, 1, 2, 3, 4, …..} or {1, 2, 3, 4, ….}) to a set *S*.

- The notation a_n is used to denote the image of the integer *n*. We can think of a_n as the equivalent of *f(n)* where *f* is a function from {0,1,2,…..} to *S*. We call a_n a *term* of the sequence.

Sequences

Example: Consider the sequence $\{a_n\}$ where

$$a_n = \frac{1}{n} \qquad \{a_n\} = \{a_1, a_2, a_3, \ldots\}$$

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4} \ldots$$

Geometric Progression

Definition: A *geometric progression* is a sequence of the form: $a, ar, ar^2, \ldots, ar^n, \ldots$

where the *initial term a* and the *common ratio r* are real numbers.

Examples:

1. Let $a = 1$ and $r = -1$. Then:

$$\{b_n\} = \{b_0, b_1, b_2, b_3, b_4, \ldots\} = \{1, -1, 1, -1, 1, \ldots\}$$

2. Let $a = 2$ and $r = 5$. Then:

$$\{c_n\} = \{c_0, c_1, c_2, c_3, c_4, \ldots\} = \{2, 10, 50, 250, 1250, \ldots\}$$

3. Let $a = 6$ and $r = 1/3$. Then:

$$\{d_n\} = \{d_0, d_1, d_2, d_3, d_4, \ldots\} = \{6, 2, \frac{2}{3}, \frac{2}{9}, \frac{2}{27}, \ldots\}$$

Arithmetic Progression

Definition: A *arithmetic progression* is a sequence of the form: $a, a+d, a+2d, \ldots, a+nd, \ldots$

where the *initial term a* and the *common difference d* are real numbers.

Examples:

1. Let $a = -1$ and $d = 4$:

$$\{s_n\} = \{s_0, s_1, s_2, s_3, s_4, \ldots\} = \{-1, 3, 7, 11, 15, \ldots\}$$

2. Let $a = 7$ and $d = -3$:

$$\{t_n\} = \{t_0, t_1, t_2, t_3, t_4, \ldots\} = \{7, 4, 1, -2, -5, \ldots\}$$

3. Let $a = 1$ and d = 2:

$$\{u_n\} = \{u_0, u_1, u_2, u_3, u_4, \ldots\} = \{1, 3, 5, 7, 9, \ldots\}$$

Strings

Definition: A *string* is a finite sequence of characters from a finite set (an alphabet).

- Sequences of characters or bits are important in computer science.
- The *empty string* is represented by λ.
- The string *abcde* has *length* 5.

Recurrence Relations

A *recurrence relation* for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms (e.g., a_0, a_1, a_{n-1}) for all integers n

- A sequence is called a *solution* of a recurrence relation if its terms satisfy the recurrence relation.
- The *initial conditions* for a sequence specify the terms that precede the first term where the recurrence relation takes effect.

Fibonacci Sequence

Definition: Define the *Fibonacci sequence*, $f_0, f_1, f_2, \ldots,$ by:

- Initial Conditions: $f_0 = 0$, $f_1 = 1$
- Recurrence Relation: $f_n = f_{n-1} + f_{n-2}$

Example: Find f_2, f_3, f_4, f_5 and f_6 .

Answer:

$$
\begin{aligned}
f_2 &= f_1 + f_0 = 1 + 0 = 1, \\
f_3 &= f_2 + f_1 = 1 + 1 = 2, \\
f_4 &= f_3 + f_2 = 2 + 1 = 3, \\
f_5 &= f_4 + f_3 = 3 + 2 = 5, \\
f_6 &= f_5 + f_4 = 5 + 3 = 8.
\end{aligned}
$$

Questions about Recurrence Relations

Example 1: Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + 3$ for $n = 1,2,3,4,\ldots.$ and suppose that $a_0 = 2$. What are a_1, a_2 and a_3?

[Here $a_o = 2$ is the initial condition.]

Solution: We see from the recurrence relation that

$$a_1 = a_o + 3 = 2 + 3 = 5$$

$$a_2 = 5 + 3 = 8$$

$$a_3 = 8 + 3 = 11$$

Questions about Recurrence Relations

Example 2: Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} - a_{n-2}$ for $n = 2,3,4,\ldots.$ and suppose that $a_0 = 3$ and $a_1 = 5$. What are a_2 and a_3?

[Here the initial conditions are $a_0 = 3$ and $a_1 = 5$.]

Solution: We see from the recurrence relation that

$$a_2 = a_1 - a_0 = 5 - 3 = 2$$

$$a_3 = a_2 - a_1 = 2 - 5 = -3$$

Solving Recurrence Relations

- Finding a formula for the nth term of the sequence generated by a recurrence relation is called *solving the recurrence relation*.

- Such a formula is called a *closed formula*.

- Various methods for solving recurrence relations will be covered in Chapter 8 where recurrence relations will be studied in greater depth.

Ex. Financial Application

Suppose that a person deposits $10,000.00 in a savings account at a bank yielding 11% per year with interest compounded annually. How much will be in the account after 30 years?

Let P_n denote the amount in the account after 30 years. P_n satisfies the following recurrence relation:

$$P_n = P_{n-1} + 0.11P_{n-1} = (1.11)\, P_{n-1}$$

with the initial condition $P_0 = 10{,}000$

Financial Application

$$P_n = P_{n-1} + 0.11P_{n-1} = (1.11)\,P_{n-1}$$

with the initial condition $P_0 = 10{,}000$

Solution: Forward Substitution

$P_1 = (1.11)P_0$

$P_2 = (1.11)P_1 = (1.11)^2P_0$

$P_3 = (1.11)P_2 = (1.11)^3P_0$

$\vdots$

$P_n = (1.11)P_{n-1} = (1.11)^n\mathrm{P}_0 = (1.11)^n\, 10{,}000$

$P_n = (1.11)^n\, 10{,}000$ (Can prove by induction, covered in Chapter 5)

$P_{30} = (1.11)^{30}\, 10{,}000 = \$228{,}992.97$

Useful Sequences

TABLE 1 **Some Useful Sequences.**

nth Term	*First 10 Terms*
n^2	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, ...
n^3	1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, ...
n^4	1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, ...
2^n	2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, ...
3^n	3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, ...
$n!$	1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, ...
f_n	1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ...

Summations

- Sum of the terms $a_m, a_{m+1}, \ldots, a_n$
  from the sequence $\{a_n\}$
- The notation:

$$\sum_{j=m}^{n} a_j \quad \textstyle\sum_{j=m}^{n} a_j \quad \textstyle\sum_{m \leq j \leq n} a_j$$

  represents

$$a_m + a_{m+1} + \cdots + a_n$$

- The variable *j* is called the *index of summation*. It runs through all the integers starting with its *lower limit m* and ending with its *upper limit n*.

Summations

- More generally for a set *S*:

$$\sum_{j \in S} a_j$$

- **Examples**:

$$r^0 + r^1 + r^2 + r^3 + \cdots + r^n = \sum_{0}^{n} r^j$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots = \sum_{1}^{\infty} \frac{1}{i}$$

$$\text{If } S = \{2, 5, 7, 10\} \text{ then } \sum_{j \in S} a_j = a_2 + a_5 + a_7 + a_{10}$$

Product Notation (*optional*)

- Product of the terms $a_m, a_{m+1}, \ldots, a_n$ from the sequence $\{a_n\}$

- The notation:

$$\prod_{j=m}^{n} a_j \qquad \textstyle\prod_{j=m}^{n} a_j \qquad \prod_{m\le j\le n} a_j$$

represents

$$a_m \times a_{m+1} \times \cdots \times a_n$$

Geometric Series

Sums of terms of geometric progressions

$$\sum_{j=0}^{n} ar^j = \begin{cases} \frac{ar^{n+1}-a}{r-1} & r \neq 1 \\ (n+1)a & r = 1 \end{cases}$$

Proof: Let $S_n = \sum_{j=0}^{n} ar^j$

To compute S_n, first multiply both sides of the equality by r and then manipulate the resulting sum as follows:

$$rS_n = r\sum_{j=0}^{n} ar^j$$

$$= \sum_{j=0}^{n} ar^{j+1}$$

Continued on next slide →

Geometric Series

$$= \sum_{j=0}^{n} ar^{j+1}$$ From previous slide.

$$= \sum_{k=1}^{n+1} ar^{k}$$ Shifting the index of summation with $k = j + 1$.

$$= \left(\sum_{k=0}^{n} ar^{k}\right) + (ar^{n+1} - a)$$ Removing $k = n + 1$ term and adding $k = 0$ term.

$$= S_n + (ar^{n+1} - a)$$ Substituting S for summation formula

$$\therefore \quad rS_n = S_n + (ar^{n+1} - a)$$

$$S_n = \frac{ar^{n+1} - a}{r - 1}$$ if r $\neq$1

$$S_n = \sum_{j=0}^{n} ar^{j} = \sum_{j=0}^{n} a = (n+1)a$$ if r = 1

Some Useful Summation Formulae

TABLE 2 Some Useful Summation Formulae.

Sum	*Closed Form*
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x\rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x\rvert < 1$	$\frac{1}{(1-x)^2}$

Geometric Series: We just proved this.

Later we will prove some of these by induction.

Proof in text (requires calculus)

Cardinality

The *cardinality* of a set A is equal to the cardinality of a set B, denoted

$$|A| = |\mathrm{B}|,$$

if and only if there is a one-to-one correspondence from A to B.

If there is a one-to-one function (*i.e.*, an injection) from A to B, the cardinality of A is less than or the same as the cardinality of B and we write $|A| \leq |B|$.

Cardinality

A set S is finite with cardinality $n \in N$ if there is a bijection from the set $\{0, 1, \ldots, n-1\}$ to S.

A set is infinite if it is not finite.

Some facts which could easily be seen are:

1. If S' is infinite and is a subset of S, S is infinite.
2. Every subset of a finite set is finite.
3. If $f : S \to T$ be an injection and S is infinite, then T is infinite.
4. If S is an infinite set $\mathscr{P}(S)$ is infinite.
5. If S and T are infinite sets. $S \cup T$ is infinite.
6. If S is infinite and $T \neq \phi$, then $S \times T$ is infinite.
7. If S is infinite and $T \neq \phi$, the set of functions from T to S is infinite.

Countable Set

- A set is countable when
  - the set is finite, or
  - the set has the same cardinality as the set of positive integers.

- When an infinite set is countable (*countably infinite*) its cardinality is $\aleph_0$ (i.e., aleph null).

- A set that is not countable is *uncountable*.

Showing that a Set is Countable

- An infinite set is countable iff there is a way to list the elements of the set in a sequence with indexes of positive integers.
  - there must exist a function $f: N \to S = \{a_1, a_2, \ldots\}$ such that $a_1 = f(1),\ a_2 = f(2), \ldots,\ a_n = f(n), \ldots$

Showing that a Set is Countable

Ex. Show that the set of positive even integers E is countable.

Let $f(x) = 2x$.

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \ldots\ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 2 & 4 & 6 & 8 & 10 & 12 & \ldots\ldots \end{array}$$

Then f is a bijection from **N** to E since f is both one-to-one and onto. To show that it is one-to-one, suppose that $f(n) = f(m)$. Then $2n = 2m$, and so $n = m$. To see that it is onto, suppose that t is an even positive integer. Then $t = 2k$ for some positive integer k and $f(k) = t$.

Showing that a Set is Countable

Ex. Show that the set of integers **Z** is countable.

Z can be listed as a sequence:

$0, 1, -1, 2, -2, 3, -3, \ldots\ldots\ldots\ldots$

Or can define a bijection from **N** to **Z**:

- When n is even: $f(n) = n/2$
- When n is odd: $f(n) = -(n-1)/2$

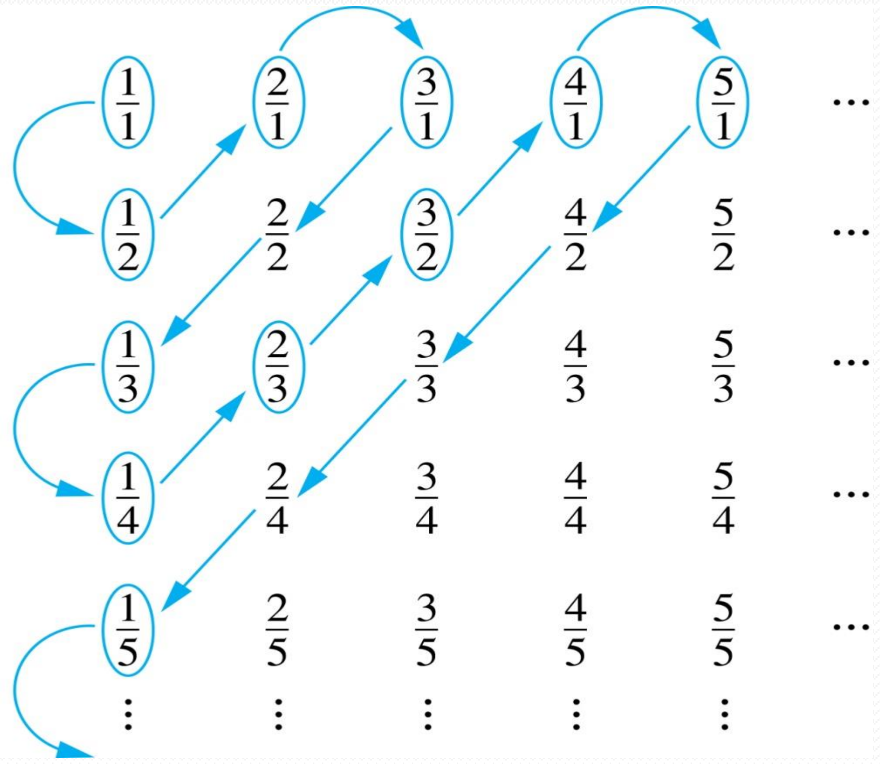
The Positive Rational Numbers are Countable

- Theorem. the set of all positive rational numbers is countable.

Constructing a sequence

List p/q with $p + q = 2$ first, and then list p/q with $p + q = 3$, and so on

1, ½, 2, 3, 1/3,1/4, 2/3, ….



Enumeration

- An enumeration of a set S is a surjective function f from an initial segment of N to S.
  - f is a string where every element appears at least once
  - f is an enumeration without repetitions if f is bijective
  - f is an enumeration with repetitions if it is not injective
- A set S is countable iff there is an enumeration of S
- **Example**
  - $S = \{\alpha, \beta, \gamma, \delta\}$
  - $<\alpha, \gamma, \beta, \beta, \delta, \alpha>$ is an enumeration with repetition.
  - $<\gamma, \alpha, \delta, \beta>$ is an enumeration without repetition.

Strings

The set of strings over a finite alphabet A is countably infinite.

Proof. Show that the strings can be listed in a sequence. First list

1. All the strings of length 0 in alphabetical order.
2. Then all the strings of length 1 in lexicographic (as in a dictionary) order.
3. Then all the strings of length 2 in lexicographic order.
4. And so on.

This implies a bijection from $\mathbf{N}$ to S and hence it is countably infinite.

Every Java programs is a string, thus countable

The set of all Java programs is countable.

- Proof

  Let S be the set of strings constructed from the characters which can appear in a Java program. Use the ordering from the previous example. Take each string in turn:

  - Feed the string into a Java compiler. (A Java compiler will determine if the input program is a syntactically correct Java program.)
  - If the compiler says YES, this is a syntactically correct Java program, we add the program to the list.
  - We move on to the next string.

  In this way we construct an implied bijection from **N** to the set of Java programs. Hence, the set of Java programs is countable.

Uncountable Set

- Theorem. the set of real numbers **R** is uncountable.
- Proof (proof by contradiction)
  - Suppose that **R** is countable.
  - Then, the set of all real numbers in [0, 1) is countable, and the elements can be listed with positive integer indexes as follow

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}\ \ldots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}\ \ldots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}\ \ldots \\ r_4 &= 0.d_{41}d_{42}d_{43}d_{44}\ \ldots \\ &\vdots \end{aligned} \qquad d_{ij} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

  - Let $r' = 0.d_1'\ d_2'\ d_3'$ ... such that $d_i' = 4$ iff $d_{ii} \neq 4$ and $d_i' = 5$ iff $d_{ii} = 4$
    Then, $\forall i \in N\ (r' \neq r_i)$.
    Consequently, this conclusion reaches to a contradiction.

Languages

Let Σ be a finite alphabet and Σ^* the set of all strings over Σ. Then $\mathscr{P}(\Sigma^*)$ is uncountable.

Proof using the Cantor's diagonalization

Let $<x_0, x_1, x_2, \ldots>$ be an enumeration of strings in Σ^* .

Suppose that $<A_0, A_1, \ldots>$ is an enumeration of $\mathscr{P}(\Sigma^*)$, s.t.

A_i represents a subset of strings Σ^* as a bit vector

$$
\begin{array}{c|cccc}
 & x_0 & x_1 & x_2 & \ldots \\
\hline
A_0 & a_{00} & a_{01} & a_{02} & \ldots \\
A_1 & a_{10} & a_{11} & a_{12} & \ldots \\
A_2 & a_{20} & a_{21} & a_{22} & \ldots \\
\vdots & \vdots & \vdots & \vdots &
\end{array}
$$

Cartinalities of the Uncountable

- A set S is of cardinality c if there is a bijection from the set of real numbers in [0, 1] to S.
  - c.f. the set of real numbers in [0, 1] is called a continuum
  - For a finite set A, $|A| < \aleph_0 < c$
  - For an infinite set A, $\aleph_0 \leq |A|$.
  - The continuum hypothesis states there is no set A s.t. $\aleph_0 < |A| < c$

- For a set A, $|S| < |\mathcal{P}(S)|$.
  - $\aleph_0 = |N| < |\mathcal{P}(N)| < |\mathcal{P}(\mathcal{P}(N))| < \cdots$

Computability

- A function is **computable** when there is a string of program source code to find the output of the function for each input
  - The set of computer programs is countable.
  - Thus, the set of computable functions is countable.

- The set of functions from $\boldsymbol{N}$ to $\boldsymbol{N}$ is uncountable. Thus, there is a function that is not computable (i.e., uncomputable)