Discrete Mathematics

Dr. Mohamed Marey

Chapter 2

2. 1 Basic structures

- Sets
- Functions
- Sequences
- Sums

Sets

- Used to group objects together
- Objects of a set often have similar properties
  - all students enrolled at UC Merced
  - all students currently taking discrete mathematics
- 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

Notation

- $a \in A: a \text{ is an elemnet of the set } A. \; a \notin A: \text{otherwise}$
- The set of all vowels in the English alphabet can be written as V={a, e, i, o, u}
- The set of odd positive integers less than 10 can be expressed by O={1, 3, 5, 7, 9}
- Nothing prevents a set from having seemingly unrelated elements, {a, 2, Fred, New Jersey}
- The set of positive integers <100: {1,2,3,…, 99}

Notation

- **Set builder**: characterize the elements by stating the property or properties
- The set O of all odd positive integers < 10:

  O={x|x is an odd positive integer < 10}

  or specify as

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

- The set of positive rational numbers

$$Q^{+} = \{x \in R \mid x = p/q \text{ for some positive integers } p \text{ and } q\}$$

Notation

$N = \{1,2,3,\ldots\}$ the set of natural numbers

$Z = \{\ldots, -2, -1, 0, 1, \ldots\}$ the set of integers

$Z^{+} = \{1,2,3,\ldots\}$ the set of positive integers

$\mathrm{Q} = \{p/q \mid p \in Z, q \in Z, \text{and } q \neq 0\}$ the set of rational numbers

R, the set of real numbers

- The set {N, Z, Q, R} is a set containing four elements, each of which is a set

Sets and operations

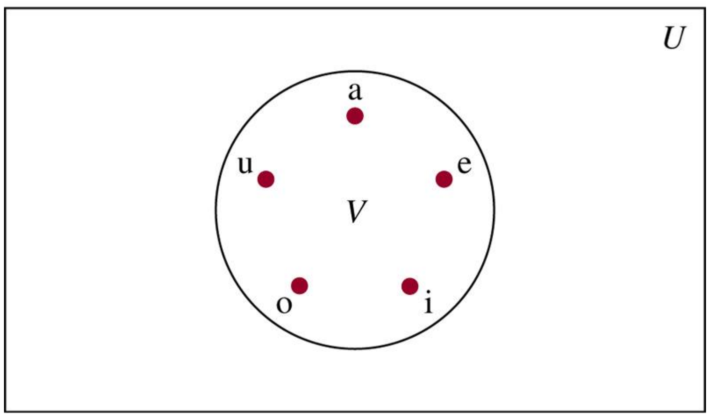
- A **datatype** or **type** is the name of a set,
- Together with a set of operations that can be performed on objects from that set
- **Boolean**: the name of the set {0,1} together with operations on one or more elements of this set such as AND, OR, and NOT

Sets

- Two sets are equal **if and only if** they have the same elements
- That is if A and B are sets, then A and B are equal if and only if $\forall x(x \in A \leftrightarrow x \in B)$. We write A=B if A and B are equal sets
- The sets {1, 3, 5} and {3, 5, 1} are equal
- The sets {1, 3, 3, 3, 5, 5, 5, 5} is the same as {1, 3, 5} because the have the same elements

Venn diagram

- Rectangle: **Universal** set that contains all the objects
- Circle: sets
  - U: 26 letters of English alphabet
  - V: a set of vowels in the English alphabet



Empty set and singleton

- **Empty (null)** set: denoted by {} or Ø
- The set of positive integers that are greater than their squares is the null set
- **Singleton**: A set with one element
- A common mistake is to confuse Ø with {Ø}

Subset

- The set A is a subset of B **if and only if** every element of A is also an element of B
- Denote by $A \subseteq B$
- We see $A \subseteq B$ if and only if $\forall x(x \in A \rightarrow x \in B)$

Empty set and the set S itself

- Theorem: or every set S
  - (i) $\emptyset \subseteq S$, and
  - (ii) $S \subseteq S$
- Let S be a set, to show $\emptyset \subseteq S$, we need to show $\forall x(x \in \emptyset \rightarrow x \in S)$ is true.
- But $x \in \emptyset$ is always false, and thus the conditional statement is always true
- (ii) is left as an exercise

Proper subset

- A is a **proper subset** of B: Emphasize that A is a subset of B but that $A \neq B$, and write it as $A \subset B$

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A)$$

- One way to show that two sets have the same elements is to show that each set is a subset of the other, i.e., if $A \subseteq B$ and $B \subseteq A$, then $A = B$

$$\forall x(x \in A \leftrightarrow x \in B)$$

Sets have other sets as members

- $A=\{\emptyset, \{a\}, \{b\}, \{a,b\}\}$
- $B=\{x|x$ is a subset of the set $\{a, b\}\}$
- Note that $A=B$ and $\{a\} \in A$ but $a \notin A$
- Sets are used extensively in computing problem

Cardinality

- Let S be a set. If there are exactly n distinct elements in S where n is a non-negative integer
- S is a **finite** set
- $|S|=n$, n is the **cardinality** of S
  - Let A be the set of odd positive integers < 10, $|A|=5$
  - Let S be the set of letters in English alphabet, $|S|=26$
  - The null set has no elements, thus $|\emptyset|=0$

Infinite set and power set

- A set is said to be infinite if it is not finite
  - The set of positive integers is infinite
- 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 P(S)
- The power set of {0,1,2}
  - $P(\{0,1,2\})=\{\emptyset,\{0\},\{1\},\{2\},\{0,1\},\{1,2\},\{0,2\},\{0,1,2\}\}$
  - Note the empty set and set itself are members of this set of subsets

Example

- What is the power set of the empty set?
  - $P(\emptyset)=\{\emptyset\}$
- The set $\{\emptyset\}$ has exactly two subsets, i.e., $\emptyset$, and the set $\{\emptyset\}$. Thus $P(\{\emptyset\})=\{\emptyset, \{\emptyset\}\}$
- If a set has n elements, then its power set has 2^n elements

Cartesian product

- Sets are unordered
- 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, and a_n as its n^{th} element
- $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$

  if and only if $a_i = b_i$ for $i = 1, 2, .., n$

Ordered pairs

- 2-tupels are called ordered pairs
- (a, b) and (c, d) are equal if and only if a=c and b=d
- Note that (a, b) and (b, a) are not equal unless a=b

Cartesian product

- The **Cartesian product** of sets A and B, denoted by A x B, is the set of all ordered pairs (a,b), where a ∈ A and b ∈ B

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

- A: students of UC Merced, B: all courses offered at UC Merced
- A x B consists of all ordered pairs of (a, b), i.e., all possible enrollments of students at UC Merced

Example

- A={1, 2}, B={a, b, c}, What is A x B?
  - A x B = {(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)}
- A subset R of the Cartesian product A x B is called a **relation**
- A={a, b, c} and B={0, 1, 2, 3}, R={(a, 0), (a, 1), (a,3), (b, 1), (b, 2), (c, 0), (c,3)} is a relation from A to B
- A x B $\neq$ B x A
  - B x A = {(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)}

Cartesian product: general case

- Cartesian product of A_1, A_2, …, A_n, is denoted by A_1 x A_2 x … x A_n is the set of ordered n-tuples (a_1, a_2, …, a_n) where ai belongs to A_i for i=1, 2, …, n

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

- A={0,1}, B={1,2}, C={0,1,2}

  A x B x 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}}

Using set notation with quantifiers

- $\forall x \in S(P(x))$ denotes the universal quantification P(x) over all elements in the set S
- Shorthand for $\forall x(x \in S \to (P(x))$
- $\exists x S(P(x))$ is shorthand for $\exists x(x \in S \wedge P(x))$
- What do they mean? $\forall x \in R(x^2 \geq 0), \exists x \in Z(x^2 = 1)$
  - The square of every real number is non-negative
  - There is an integer whose square is 1

Truth sets of quantifiers

- Predicate P, and a domain D, the truth set of P is the set of elements x in D for which P(x) is true, denote by $\{x \in D | P(x)\}$
- $P(x)$ is $|x|=1$, $Q(x)$ is $x^2=2$, and $R(x)$ is $|x|=x$ and the domain is the set of integers
  - Truth set of P, $\{x \in Z \,|\, |x|=1\}$, i.e., the truth set of P is $\{-1,1\}$
  - Truth set of Q, $\{x \in Z \,|\, x^2=2\}$, i.e., the truth set is $\emptyset$
  - Truth set of R, $\{x \in Z \,|\, |x|=x\}$, i.e., the truth set is N

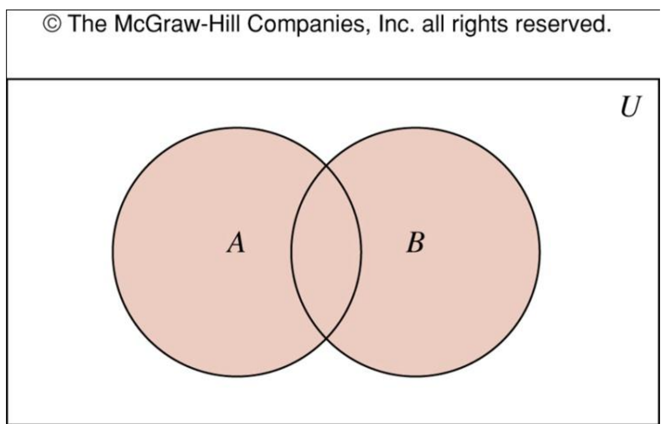
Example

- $\forall x P(x)$ is true over the domain U if and only if truth set of P is the set U
- $\exists x P(x)$ is true over the domain U if and only if truth set of P is non-empty

2.2 Set operations

- **Union**: the set that contains those elements that are either in A or in B, or in both

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$



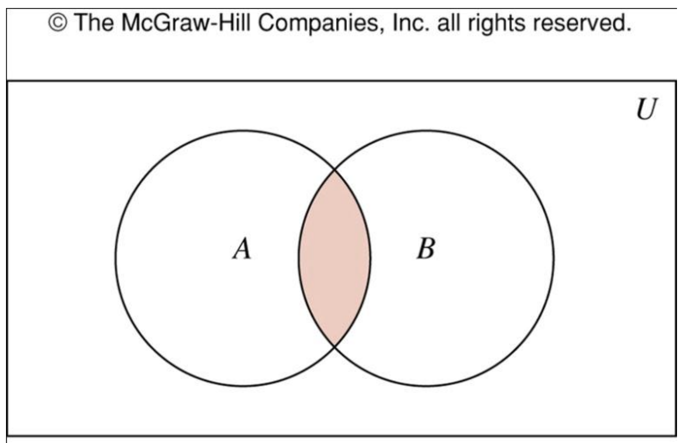
A *B* is shaded.

- A={1,3,5}, B={1,2,3}, AUB={1,2,3,5}

Intersection

- **Intersection**: the set containing the elements in both A and B

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

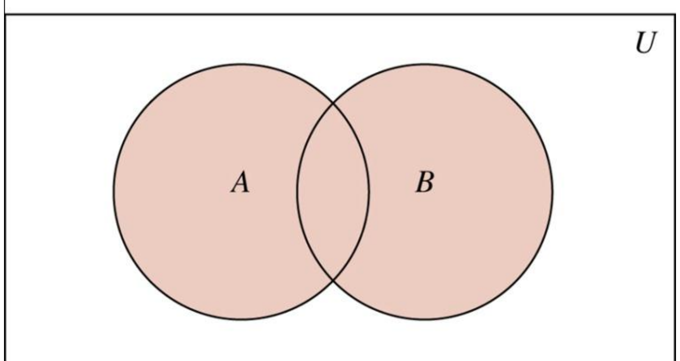


A *B* is shaded.

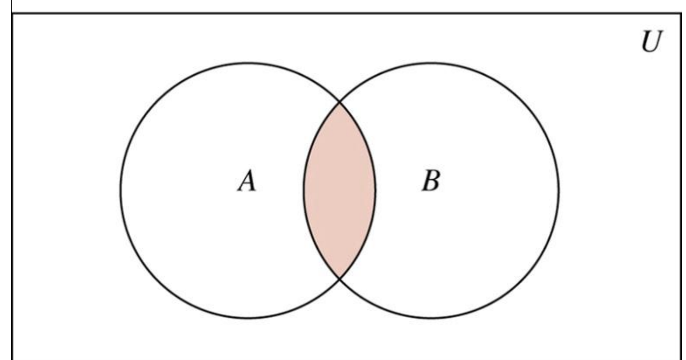
- A={1,3,5}, B={1,2,3}, A∩B={1,3}

Disjoint set

- Two sets are **disjoint** if their intersection is ∅
- A={1,3}, B={2,4}, A and B are disjoint
- Cardinality: $|A \cup B| = |A| + |B| - |A \cap B|$



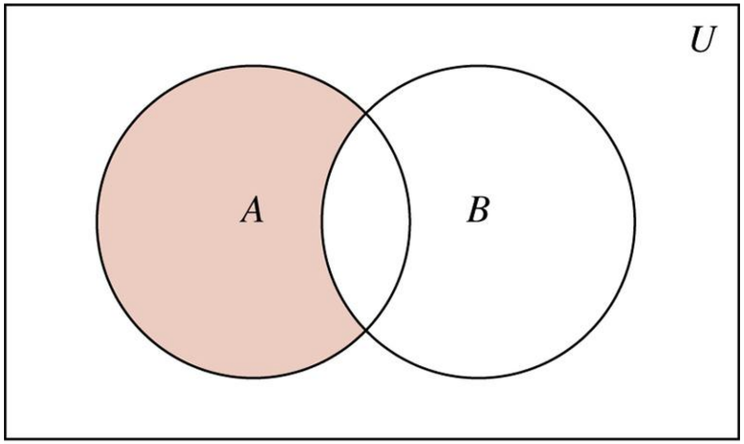
A *B* is shaded.



A *B* is shaded.

Difference and complement

- A-B: the set containing those elements in A but not in B $A - B = \{x \mid x \in A \wedge x \notin B\}$

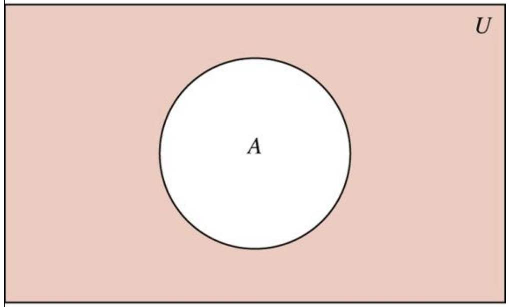


$A - B$ is shaded.

- A={1,3,5},B={1,2,3}, A-B={5}

Complement

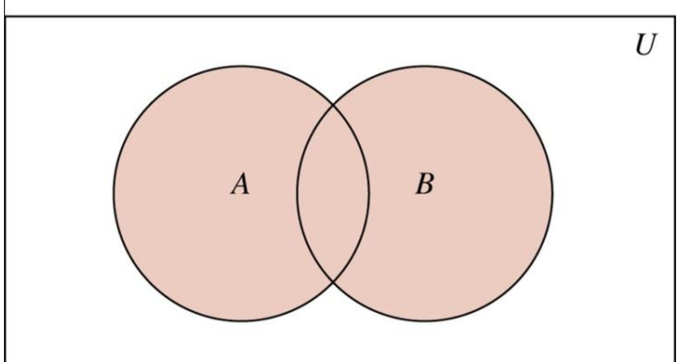
- Once the universal set U is specified, the complement of a set can be defined
- **Complement** of A: $\overline{A} = \{x \mid x \notin A\}, \overline{A} = U - A$
- A-B is also called the complement of B with respect to A



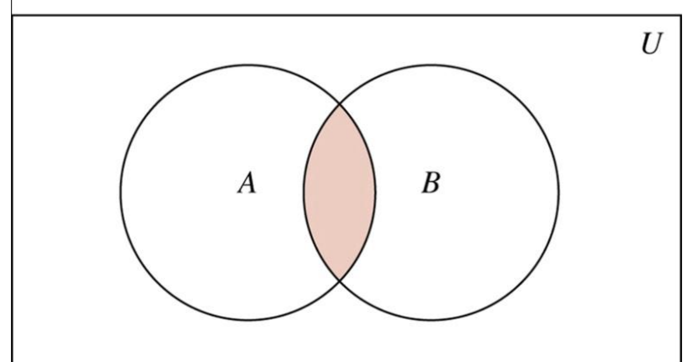
$\overline{A}$ is shaded.

Example

- A is the set of positive integers > 10 and the universal set is the set of all positive integers, then $\overline{A} = \{x \mid x \leq 10\} = \{1,2,3,4,5,6,7,8,9,10\}$
- A-B is also called the complement of B with respect to A



$A \quad B$ is shaded.



$A \quad B$ is shaded.

Set identities

TABLE 1 Set Identities.

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

Example

- Prove $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- Will show that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$ and $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$
- (→): Suppose that $x \in \overline{A \cap B}$, by definition of complement and use De Morgan's law

$$\neg(x \in A \wedge x \in B)$$

$$\equiv (\neg(x \in A)) \vee (\neg(x \in B))$$

$$\equiv (x \notin A) \vee (x \notin B)$$

- By definition of complement $x \in \overline{A}$ or $x \in \overline{B}$
- By definition of union $x \in \overline{A} \cup \in \overline{B}$

Example

- (←): Suppose that $x \in \overline{A} \cup \overline{B}$
- By definition of union $x \in \overline{A} \vee x \in \overline{B}$
- By definition of complement $x \notin A \vee x \notin B$
- Thus $\neg(x \in A) \vee \neg(x \in B)$
- By De Morgan's law: $$\neg(x \in A) \vee \neg(x \in B)$$ $$\equiv \neg(x \in A \wedge x \in B)$$ $$\equiv \neg(x \in (A \cap B))$$
- By definition of complement, $x \in \overline{A \cap B}$

Builder notation

- Prove it with builder notation

$$
\begin{aligned}
\overline{A \cap B} &= \{x \mid x \notin A \cap B\} \quad \text{(def of complement)} \\
&= \{x \mid \neg(x \in (A \cap B))\} \quad \text{(def of not belong to)} \\
&= \{\mathrm{x} \mid \neg(x \in A \wedge x \in B)\} \quad \text{(def of intersection)} \\
&= \{x \mid \neg(x \in A) \vee \neg(x \in B)\} \quad \text{(De Morgan's law)} \\
&= \{x \mid x \notin A \vee x \notin B\} \quad \text{(def of not belong to)} \\
&= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} \quad \text{(def of complement)} \\
&= \{x \mid x \in \overline{A} \cup \overline{B}\} \quad \text{(def of union)} \\
&= \overline{A} \cup \overline{B}
\end{aligned}
$$

Example

- Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- (→): Suppose that $x \in A \cap (B \cup C)$ then $x \in A$ and $x \in B \cup C$. By definition of union, it follows that $x \in A$, and ($x \in B$ or $x \in C$). Consequently, $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$
- By definition of intersection, it follows $x \in A \cap B$ or $x \in A \cap C$
- By definition of union, $x \in (A \cap B) \cup (A \cap C)$

Example

- $(\leftarrow)$: Suppose that $x \in (A \cap B) \cup (A \cap C)$
- By definition of union, $x \in A \cap B$ or $x \in A \cap C$
- By definition of intersection, $x \in A$ and $x \in B$, or $x \in A$ and $x \in C$
- From this, we see $x \in A$, and $x \in B$ or $x \in C$
- By definition of union, $x \in A$ and $x \in B \cup C$
- By definition of intersection, $x \in A \cap (B \cup C)$

Membership table

TABLE 2 A Membership Table for the Distributive Property.

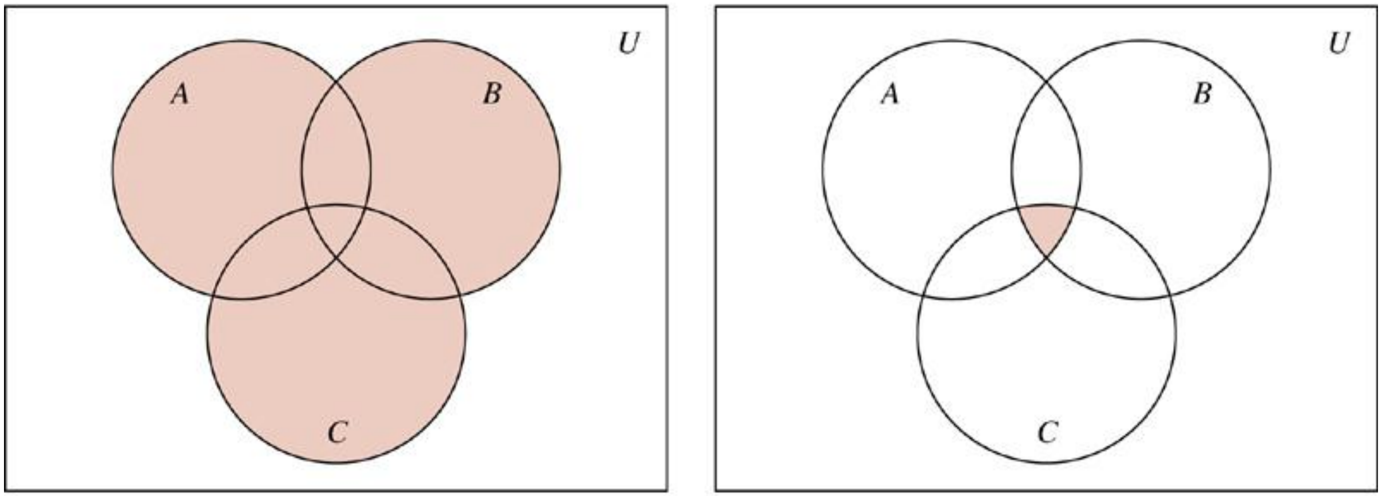
A	B	C	$B \cup C$	$A \cap (B \cup C)$	$A \cap B$	$A \cap C$	$(A \cap B) \cup (A \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1
1	0	1	1	1	0	1	1
1	0	0	0	0	0	0	0
0	1	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Example

- Show that $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$

$$
\begin{aligned}
\overline{A \cup (B \cap C)} &= \overline{A} \cap \overline{B \cap C} \quad \text{(De Morgan's law)} \\
&= \overline{A} \cap (\overline{B} \cup \overline{C}) \quad \text{(De Morgan's law)} \\
&= (\overline{B} \cup \overline{C}) \cap \overline{A} \quad \text{(commutative law)} \\
&= (\overline{C} \cup \overline{B}) \cap \overline{A} \quad \text{(commutative law)}
\end{aligned}
$$

Generalized union and intersection



(a) $A \cup B \cup C$ is shaded.   (b) $A \cap B \cap C$ is shaded.

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

General case

- Union: $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$
- Intersection $A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$
- Union: $A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots = \bigcup_{i=1}^{\infty} A_i$
- Intersection: $A_1 \cap A_2 \cap \cdots \cap A_n \cap \cdots = \bigcap_{i=1}^{\infty} A_i$
- Suppose A_i={1, 2, 3,…, i} for i=1,2,3,…

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

$$\bigcap_{i=1}^{\infty} A_i = \bigcap_{i=1}^{\infty} \{1,2,3,\ldots,i\} = \{1\}$$

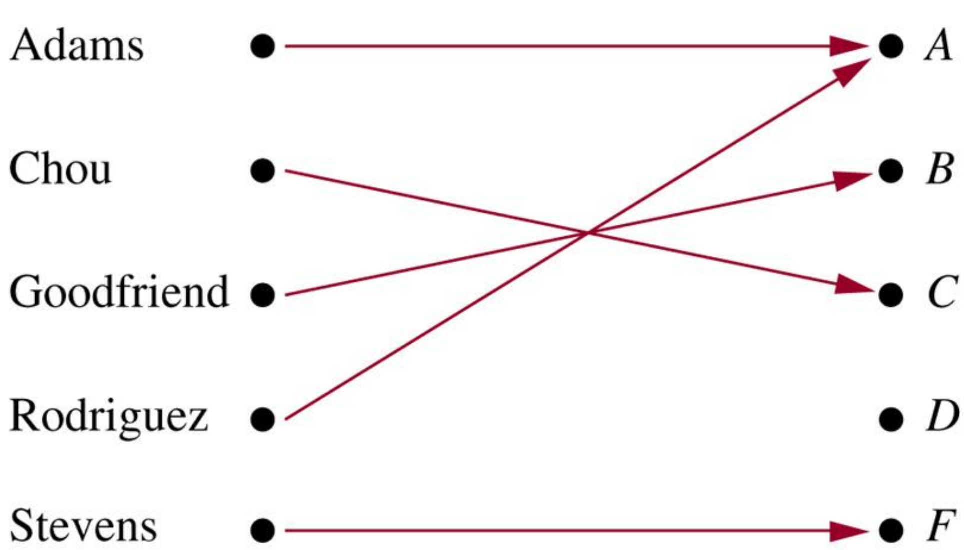
Computer representation of sets

- U={1,2,3,4,5,6,7,8,9,10}
- A={1,3,5,7,9} (odd integer ≤10),B={1,2,3,4,5} (integer ≤5)
- Represent A and B as 1010101010, and 1111100000
- Complement of A: 0101010101
- A⋂B: 1010101010^1111100000=1010100000

which corresponds to {1,3,5}

2.3 Functions

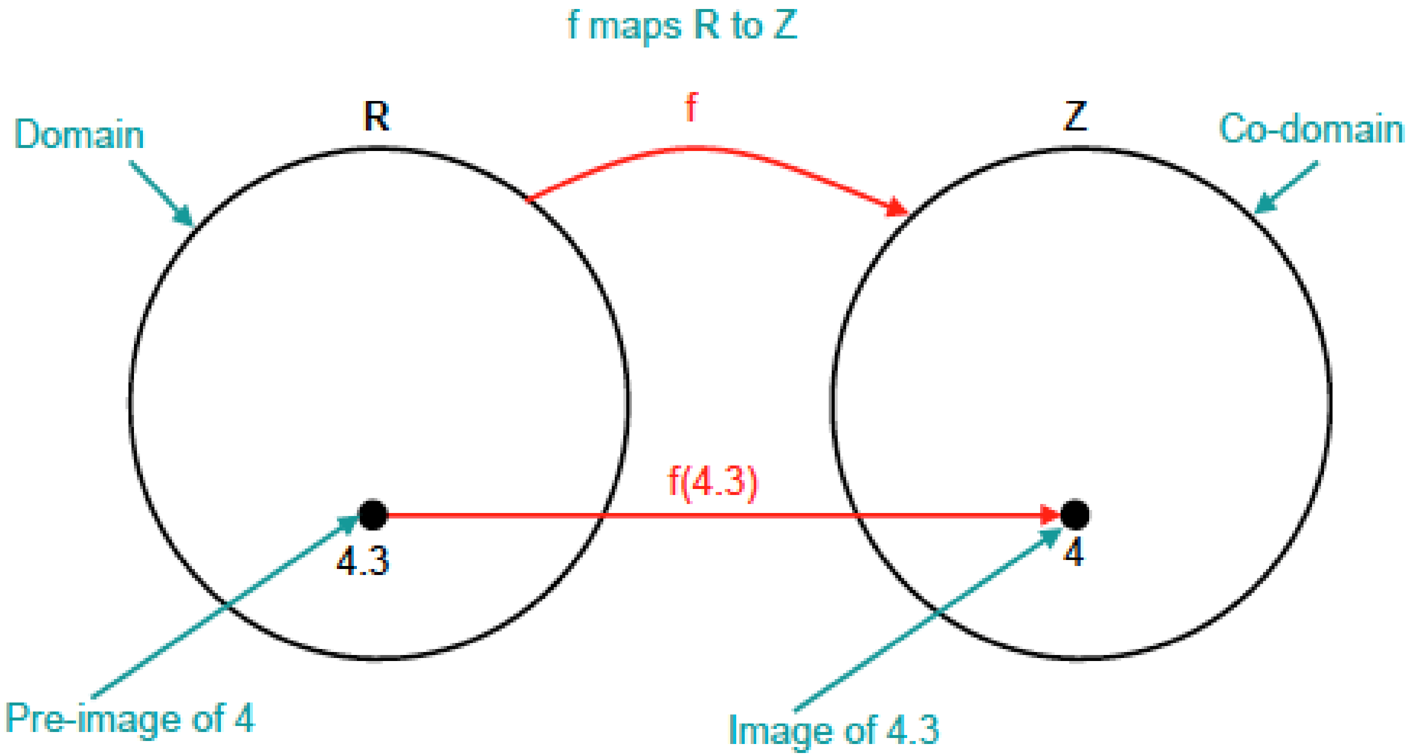
- Assign each element of a set to a particular element of a second set



Function

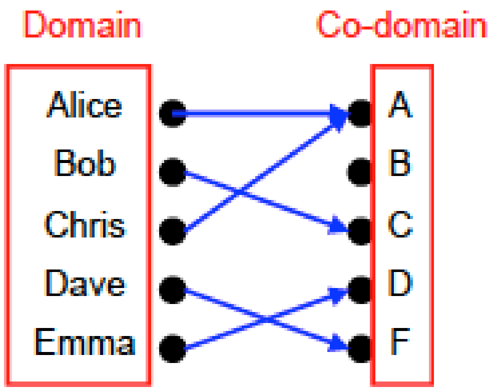
- A **function** f from A to B, $f:A \rightarrow B$, is an assignment of **exactly one** element of B to each element of A
- $f(a)=b$ if b is the unique element of B assigned by the function f to the element a
- Sometimes also called **mapping** or **transformation**

Terminology

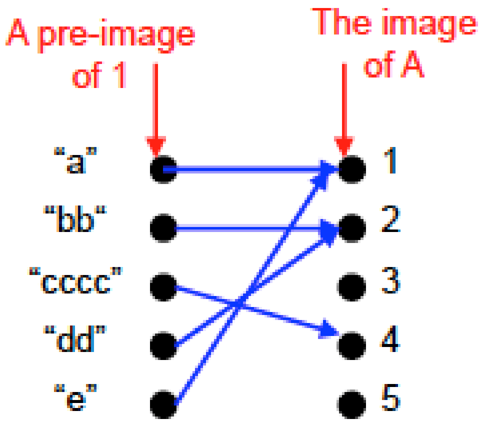


Example of the floor function

Examples



A class grade function



A string length function

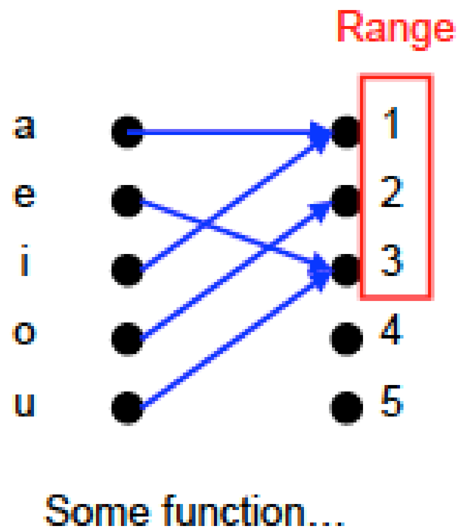
Exercises

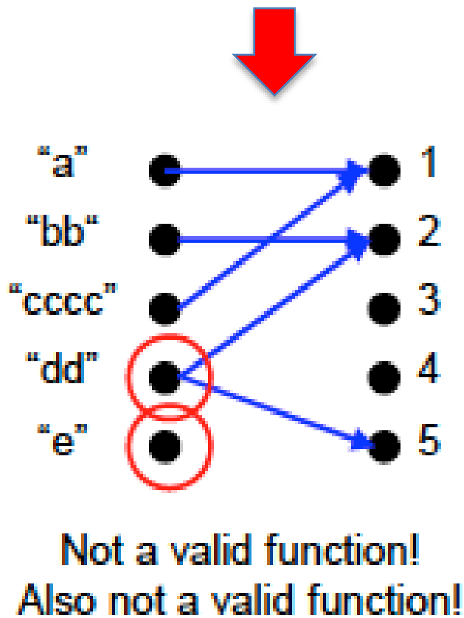
Why is f not a function from R to R if

(a) $f(x) = 1/x$

(b) $f(x) = x^{1/2}$

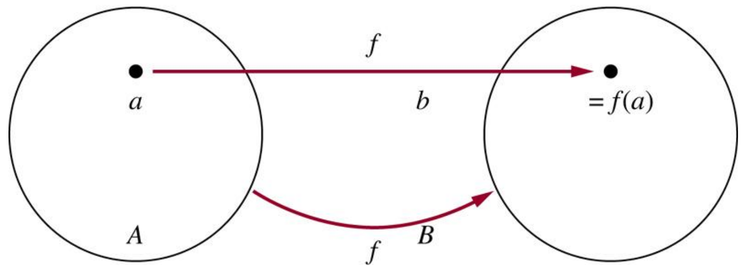
More examples





What is the difference between co-domain and range?

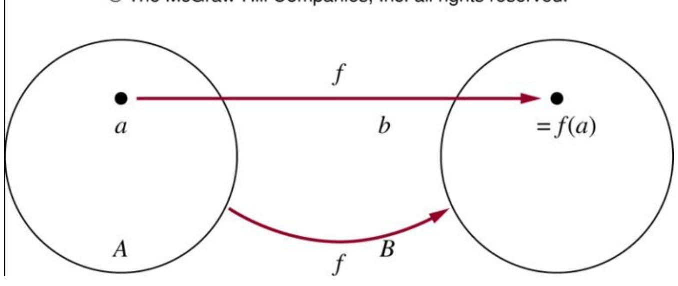
Function and relation



- f:A→B can be defined in terms of a relation from A to B
- Recall a **relation** from A to B is just a subset of A x B
- **A relation from A to B that contains one, and only one, ordered pair (a,b) for every element a ∈ A, defines a function f from A to B**
- f(a)=b where (a,b) is the unique ordered pair in the relation

Domain and range

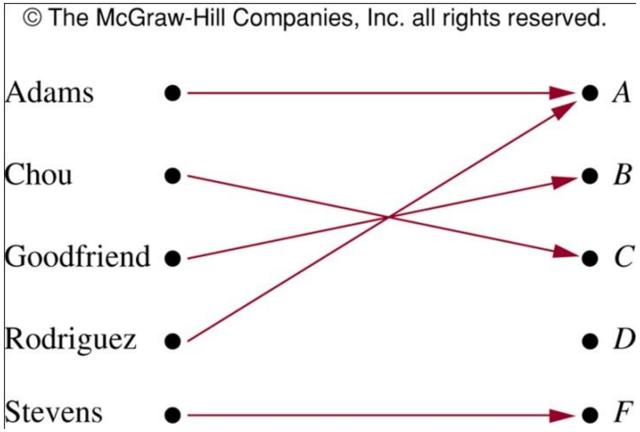
- If f is a function from A to B
  - A is the **domain** of f
  - B is the **codomain** of f
  - f(a)=b, b is the **image** of a and a is **preimage** of b
  - **Range** of f: set of all images of element of A
  - f **maps** A to B



Function

- Specify a function by
  - Domain
  - Codomain
  - Mapping of elements
- Two functions are equal if they have
  - Same domain, codomain, mapping of elements

Example



- G: function that assigns a grade to a student, e.g., G(Adams)=A
- Domain of G: {Adams, Chou, Goodfriend, Rodriguez, Stevens}
- Codomain of G: {A, B, C, D, F}
- Range of G is: {A, B, C, F}

Example

- Let R be the relation consisting of (Abdul, 22), (Brenda, 24), (Carla, 21), (Desire, 22), (Eddie, 24) and (Felicia, 22)
- f: f(Abdul)=22, f(Brenda)=24, f(Carla)=21, f(Desire)=22, f(Eddie)=24, and f(Felicia)=22
- Domain: {Abdul, Brenda, Carla, Desire, Eddie, Felicia}
- Codomain: set of positive integers
- Range: {21, 22, 24}

Example

- f: assigns the last two bits of a bit string of length 2 or greater to that string, e.g., f(11010)=10
- Domain: all bit strings of length 2 or greater
- Codomain: {00, 01, 10, 11}
- Range: {00, 01, 10, 11}

Example

- f: Z → Z, assigns the square of an integer to its integer, $f(x)=x^2$
- Domain: the set of all integers
- Codomain: set of all integers
- Range: all integers that are perfect squares, i.e., {0, 1, 4, 9, ...}

Example

- In programming languages
  - int floor(float x){…}
    - Domain: the set of real numbers
    - Codomain: the set of integers

Functions

- Two real-valued functions with the same domain can be added and multiplied
- Let f_1 and f_2 be functions from A to **R**, then f_1+f_2, and f_1f_2 are also functions from A to **R** defined by
  - $(f_1+f_2)(x)= f_1(x)+f_2(x)$
  - $(f_1f_2)(x)= f_1(x)\ f_2(x)$
- Note that the functions f_1+f_2 and f_1f_2 at x are defined in terms f_1 and f_2 at x

Example

- $f_1(x) = x^2$ and $f_2(x) = x - x^2$
  - $(f_1+f_2)(x)=f_1(x)+f_2(x)=x^2+x-x^2=x$
  - $(f_1f_2)(x)=f_1(x)f_2(x)=x^2(x-x^2)=x^3-x^4$

Function and subset

- When f is a function from A to B ($f:A \rightarrow B$), the image of a subset of A can also be defined
- Let S be a subset of A, the image of S under function f is the subset of B that consists of the images of the elements of S
- Denote the image of S by f(S)

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

$$\text{or } \{f(s) \mid s \in S\} \text{ as shorthand}$$

- f(S) denotes a set, not the value of function f

One-to-one function

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

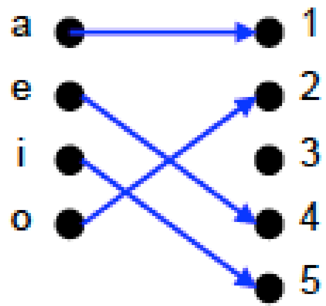
$$\forall a \forall b (f(a) = f(b) \rightarrow a = b)$$

- Using contrapositive of the implication in the definition (p→q ≡ q whenever p)
- A function f is one-to-one if and only if f(a)≠f(b) whenever a≠b $\forall a \forall b (a \neq b \rightarrow f(a) \neq f(b))$
- Every element of B is the image of a unique element of A

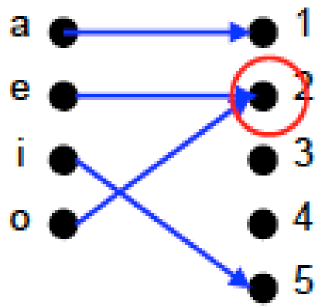
One-to-one functions

A function is one-to-one if each element in the co-domain has a unique pre-image

– Meaning no 2 values map to the same result



A one-to-one function

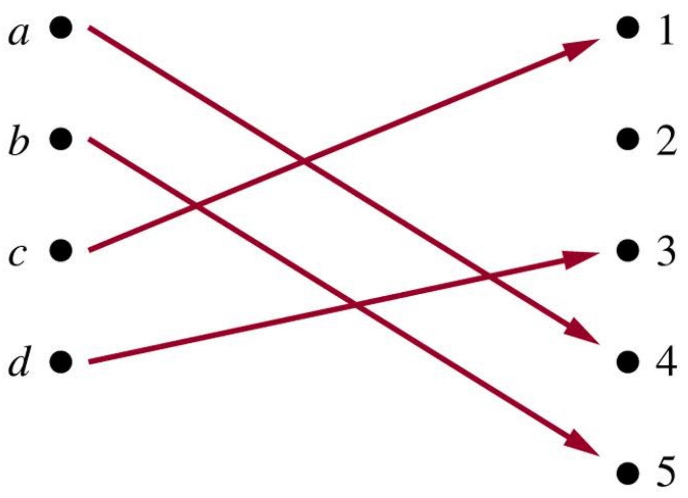


A function that is not one-to-one

injective or one-to-one

Example

- f maps {a,b,c,d} to {1,2,3,4,5} with f(a)=4, f(b)=5, f(c)=1, f(d)=3
- Is f an one-to-one function?



Example

- Let $f(x)=x^2$, from the set of integers to the set of integers. Is it one-to-one?
- $f(1)=1$, $f(-1)=1$, $f(1)=f(-1)$ but $1 \neq -1$
- However, $f(x)=x^2$ is one-to-one for Z^+
- Determine $f(x)=x+1$ from real numbers to itself is one-to-one or not
- It is one-to-one. To show this, note that $x+1 \neq y+1$ when $x \neq y$

Increasing/decreasing functions

- Increasing (decreasing): if $f(x) \le f(y)$ ($f(x) \ge f(y)$), whenever $x<y$ and x, y are in the domain of f

$$\forall x \forall y (x < y \to f(x) \le f(y))$$

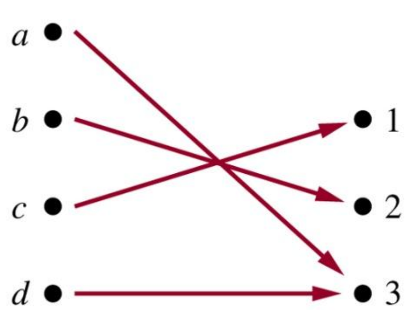
- Strictly increasing (decreasing): if $f(x)<f(y)$ ($f(x) > f(y)$) whenever $x<y$, and x, y are in the domain of f
- A function that is either strictly increasing or decreasing must be one-to-one

Onto functions

- **Onto**: A function from A to B is onto or **surjective**, if and only if for every element b ∈ B there is an element a ∈ A with f(a)=b

$$\forall y \exists x (f(x) = y), \text{where } x \text{ is in the domain and } y \text{ is the codomain}$$

- Every element of B is the image of some element in A

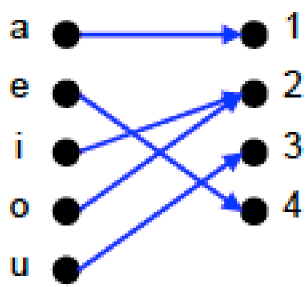


f maps from {a, b, c, d} to {1, 2, 3}, is f onto?

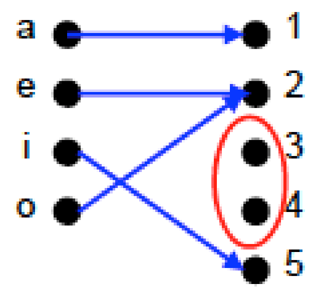
Onto Functions

A function is onto if each element in the co-domain is an image of some pre-image

- Meaning all elements in the right are mapped to



An onto function



A function that is not onto

surjective = onto.

Example

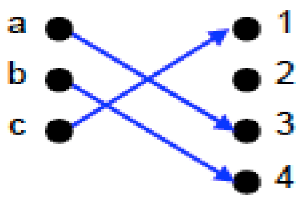
- Is $f(x)=x^2$ from the set of integers to the set of integers onto?
  - $f(x)=-1$?
- Is $f(x)=x+1$ from the set of integers to the set of integers onto?
  - It is onto, as for each integer y there is an integer x such that $f(x)=y$
  - To see this, $f(x)=y$ iff $x+1=y$, which holds if and only if $x=y-1$

One-to-one correspondence

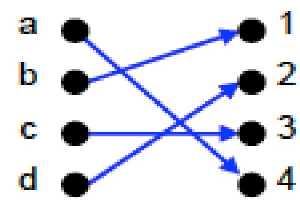
- The function f is a **one-and-one correspondence**, or **bijective**, if it is both one-to-one and onto
- Let f be the function from {a, b, c, d} to {1, 2, 3, 4} with f(a)=4, f(b)=2, f(c)=1, and f(d)=3, is f bijective?
  - It is one-to-one as no two values in the domain are assigned the same function value
  - It is onto as all four elements of the codomain are images of elements in the domain

Example

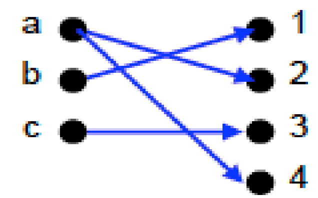
- Are the following functions onto, one-to-one, both, or neither?



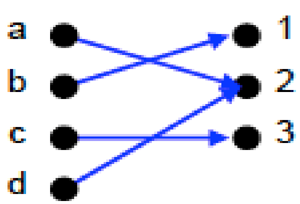
1-to-1, not onto



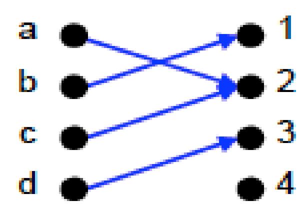
Both 1-to-1 and onto



Not a valid function



Onto, not 1-to-1



Neither 1-to-1 nor onto

1-to-1 and onto function are called bijective.

11

Identity Function

Identity function:

It is one-to-one and onto

$$\iota_A : A \to A, \iota_A(x) = x, \forall x \in A$$

A function such that the image and the pre-image are ALWAYS equal

f(x) = 1*x

f(x) = x + 0

The domain and the co-domain must be the same set

2.3 Inverse function

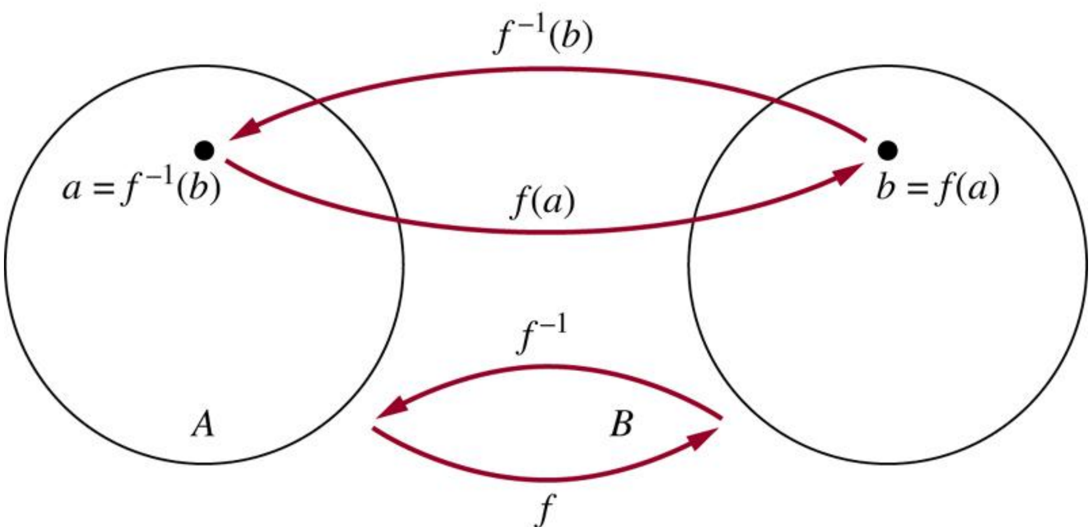
- Consider a one-to-one correspondence f from A to B
- Since f is onto, every element of B is the image of some element in A
- Since f is one-to-one, every element of B is the image of a unique element of A
- Thus, we can define a new function from B to A that reverses the correspondence given by f

Inverse function

- Let f be a one-to-one correspondence from the set A to the set B
- The **inverse function** of f is the function that assigns an element b belonging to B the unique element a in A such that f(a)=b
- Denoted by f^{-1}, hence $f^{-1}(b)=a$ when $f(a)=b$
- Note f^{-1} is not the same as $1/f$

One-to-one correspondence and inverse function

- If a function f is not one-to-one correspondence, cannot define an inverse function of f



- A one-to-one correspondence is called **invertible**

Example

- f is a function from {a, b, c} to {1, 2, 3} with f(a)=2, f(b)=3, f(c)=1. Is it invertible? What is it its inverse?
- Let f: Z→Z such that f(x)=x+1, Is f invertible? If so, what is its inverse?

  $y=x+1$, $x=y-1$, $f^{-1}(y)=y-1$
- Let f: R→R with $f(x)=x^2$, Is it invertible?
  - Since f(2)=f(-2)=4, f is not one-to-one, and so not invertible

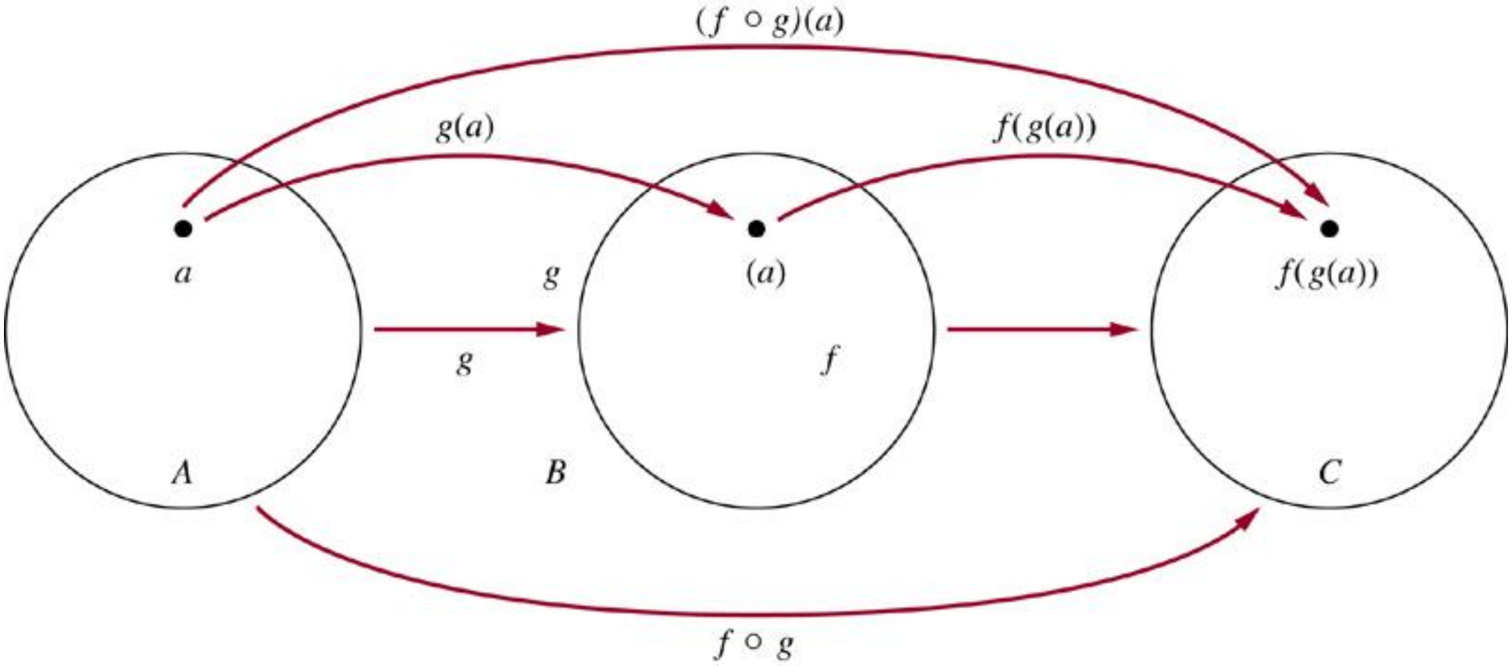
Example

- Sometimes we restrict the domain or the codomain of a function or both, to have an invertible function
- The function $f(x)=x^2$, from R^+ to R^+ is
  - one-to-one : If $f(x)=f(y)$, then $x^2=y^2$, then $x+y=0$ or $x-y=0$, so $x=-y$ or $x=y$
  - onto: $y= x^2$, every non-negative real number has a square root
  - inverse function: $f^{-1}(y)=\sqrt{y}$

Composition of functions

- Let g be a function from A to B and f be a function from B to C, the composition of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(a)=f(g(a))$
  - First apply g to a to obtain g(a)
  - Then apply f to g(a) to obtain $(f \circ g)(a)=f(g(a))$

Composition of functions



- Note $f \circ g$ cannot be defined unless

  the range of g is a subset of the domain of f

Example

- g: {a, b, c} → {a, b, c}, g(a)=b, g(b)=c, g(c)=a, and f:{a,b,c} →{1,2,3}, f(a)=3, f(b)=2, f(c)=1. What are $f \circ g$ and $g \circ f$?
- $(f \circ g)(a)=f(g(a))=f(b)=2$, $(f \circ g)(b)=f(g(b))=f(c)=1$, $(f \circ g)(c)=f(a)=3$
- $(g \circ f)(a)=g(f(a))=g(3)$ not defined. $g \circ f$ is not defined

Example

- $f(x)=2x+3$, $g(x)=3x+2$. What are $f \circ g$ and $g \circ f$?
- $(f \circ g)(x)=f(g(x))=f(3x+2)=2(3x+2)+3=6x+7$
- $(g \circ f)(x)=g(f(x))=g(2x+3)=3(2x+3)+2=6x+11$
- Note that $f \circ g$ and $g \circ f$ are defined in this example, but they are not equal
- The commutative law does not hold for composition of functions

$f \circ f^{-1}$

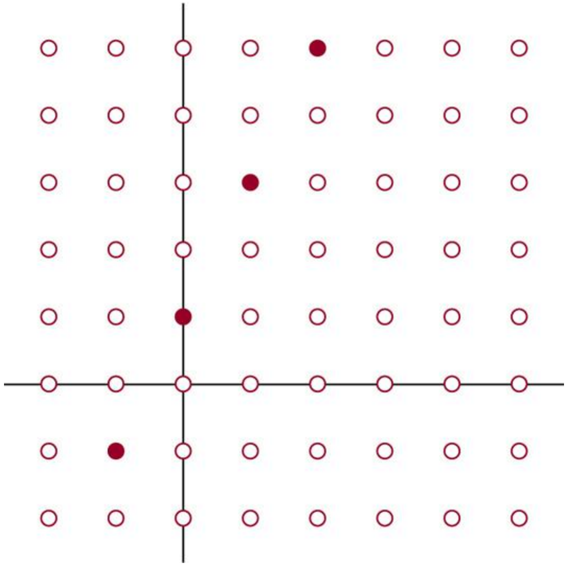
- $f \circ f^{-1}$ form an identity function in any order
- Let $f: A \rightarrow B$ with $f(a)=b$
- Suppose f is one-to-one correspondence from A to B
- Then f^{-1} is one-to-one correspondence from B to A
- The inverse function reverses the correspondence of f, so $f^{-1}(b)=a$ when $f(a)=b$, and $f(a)=b$ when $f^{-1}(b)=a$
- $(f^{-1} \circ f)(a)=f^{-1}(f(a))=f^{-1}(b)=a$, and
- $(f \circ f^{-1})(b)=f(f^{-1})(b))=f(a)=b$

$$f^{-1} \circ f = \iota_A,\ f \circ f^{-1} = \iota_B,\ \iota_A, \iota_B \text{ are identity functions of A and B}$$

$$(f^{-1})^{-1} = f$$

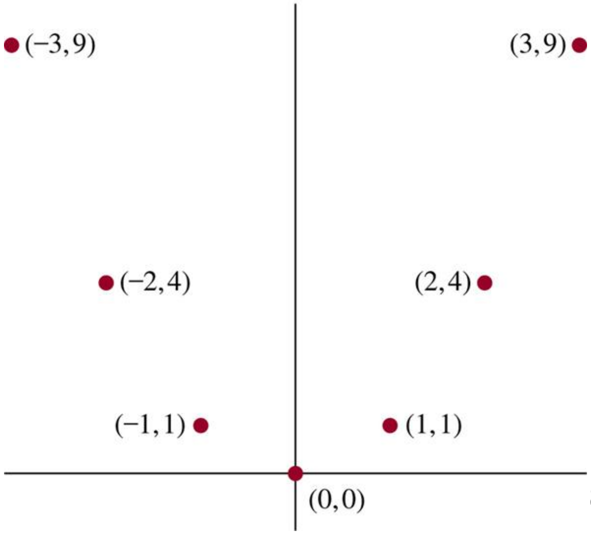
Graphs of functions

- Associate a set of pairs in A x B to each function from A to B
- The set of pairs is called the graph of the function: $\{(a,b)\,|\,a \in A,\ b \in B, \text{ and } f(a)=b\}$

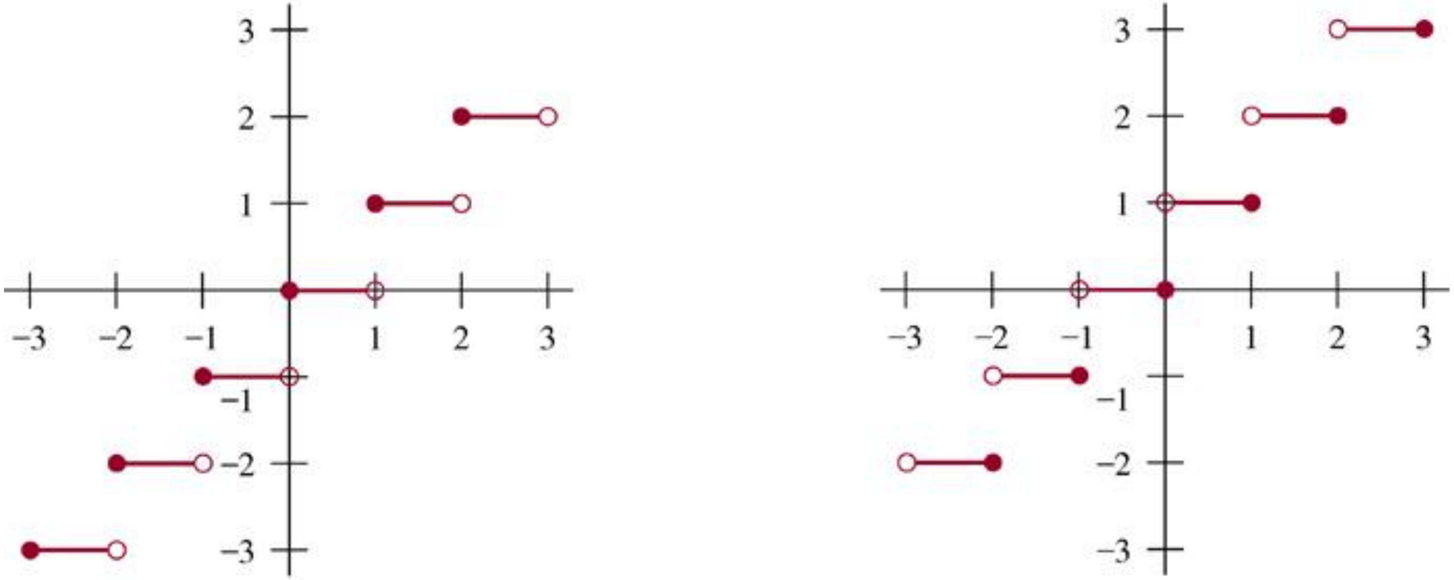


f(x)=2x+1

$f(x)=x^2$



Example



(a) $y = [x]$ (b) $y = [x]$

$$\text{floor}: y = \lfloor x \rfloor \qquad \text{ceiling}: y = \lceil x \rceil$$

2.4 Sequences

- Ordered list of elements
  - e.g., 1, 2, 3, 5, 8 is a sequence with 5 elements
  - 1, 3, 9, 27, 81, …, 30, …, is an infinite sequence
- **Sequence** $\{a_n\}$: a function from a subset of the set of integers (usually either the set of {0, 1, 2, …} or the set {1, 2, 3, …}) to a set S
- Use a_n to denote the image of the integer n
- Call a_n a **term** of the sequence

Sequences

- Example: $\{a_n\}$ where $a_n=1/n$
  - $a_1, a_2, a_3, a_4, \ldots$
  - 1, ½, 1/3, ¼,…
- When the elements of an infinite set can be listed, the set is called **countable**
- Will show that the set of positive rational numbers is countable, but the set of real numbers is not

Geometric progression

- **Geometric progression**: a sequence of the form

  $a, ar, ar^2, ar^3, \ldots, ar^n$

  where the initial term a and common ratio r are real numbers
- Can be written as $f(x)=a \cdot r^x$
- The sequences $\{b_n\}$ with $b_n=(-1)^n$, $\{c_n\}$ with $c_n=2*5^n$, $\{d_n\}$ with $d_n=6*(1/3)^n$ are geometric progression
  - b_n : 1, -1, 1, -1, 1, …
  - c_n: 2, 10, 50, 250, 1250, …
  - d_n: 6, 2, 2/3, 2/9, 2/27, …

Arithmetic progression

- **Arithmetic progression**: a sequence of the form

  a, a+d, a+2d, …, a+nd

  where the initial term a and the common difference d are real numbers
- Can be written as $f(x)=a+dx$
- $\{s_n\}$ with $s_n=-1+4n$, $\{t_n\}$ with $t_n=7-3n$
  - $\{s_n\}$: -1, 3, 7, 11, …
  - $\{t_n\}$: 7, 4, 1, 02, …

String

- Sequences of the form $a_1, a_2, \ldots, a_n$ are often used in computer science
- These finite sequences are also called **strings**
- The **length** of the string S is the number of terms
- The **empty string**, denoted by **λ**, is the string has no terms

Recurrence relation

- Express a_n in terms of one or more of the previous terms of the sequence
- Example: $a_n=a_{n-1}+3$ for $n=1,2,3,\ldots$ and $a_1=2$
  - $a_2=a_1+3=2+3=5$, $a_3=a_2+3=(2+3)+3=2+3x2=8$, $a_4=a_3+3=(2+3+3)+3=2+3+3+3=2+3x3=11$
  - $a_n=2+3(n-1)$
  - $a_n=a_{n-1}+3=(a_{n-2}+3)+3=a_{n-2}+3x2$
    $=(a_{n-3}+3)+3x2=a_{n-3}+3x3$
    $=a_2+3(n-2)=(a_1+3)+3(n-2)=2+3(n-1)$

Fibonacci sequence

- $f_0=0$, $f_1=1$, $f_n=f_{n-1}+f_{n-2}$, for n=2, 3, 4
  - $f_2=f_1+f_0=1+0=1$
  - $f_3=f_2+f_1=1+1=2$
  - $f_4=f_3+f_2=2+1=3$
  - $f_5=f_4+f_3=3+2=5$
  - $f_6=f_5+f_4=5+3=8$

Closed formula

- Determine whether the sequence $\{a_n\}$, $a_n=3n$ for every nonnegative integer n, is a solution of the recurrence relation $a_n=2a_{n-1}-a_{n-2}$ for n=2,3,4,
  – For n>=2, $a_n=2a_{n-1}-a_{n-2}=2(3(n-1))-3(n-2)=3n=a_n$
- Suppose $a_n=2^n$, Note that $a_0=1$, $a_1=2$, $a_2=4$, but $2a_1-a_0=2x2-1=3 \neq a_2$, thus $a_n=2^n$ is not a solution of the recurrence relation

Special integer sequences

- Finding some patterns among the terms
- Are terms obtained from previous terms
  - by adding the same amount or an amount depends on the position in the sequence?
  - by multiplying a particular amount?
  - By combining previous terms in a certain way?
  - In some cycle?

Example

- Find formulate for the sequences with the following 5 terms
  - 1, ½, ¼, 1/8, 1/16
  - 1, 3, 5, 7, 9
  - 1, -1, 1, -1, 1
- The first 10 terms: 1, 2, 2, 3, 3, 3, 4, 4, 4, 4
- The first 10 terms: 5, 11, 17, 23, 29, 35, 41, 47, 53, 59

Example

- Conjecture a simple formula for $\{a_n\}$ where the first 10 terms are 1, 7, 25, 79, 241, 727, 2185, 6559, 19681, 59047

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, . . .

Summations

- The sum of terms: a_m, a_{m+1}, ..., a_n from $\{a_n\}$

$$\sum_{j=m}^{n} a_j,\ \sum\nolimits_{j=m}^{n} a_j,\ \text{or} \sum\nolimits_{m\le j\le n} a_j$$

  that represents $a_m + a_{m+1} + \ldots + a_n$

  – Here j is the index of summation (can be replaced arbitrarily by i or k)

  – The index runs from the lower limit m to upper limit n

  – The usual laws for arithmetic applies

$$\sum\nolimits_{j=1}^{n}(ax_j + by_j) = a\sum\nolimits_{j=1}^{n} x_j + b\sum\nolimits_{j=1}^{n} y_j \text{ where } a, b \text{ are real numbers}$$

Example

- Express the sum of the first 100 terms of the sequence $\{a_n\}$ where a_n=1/n, n=1, 2, 3, …

$$\sum_{j=1}^{100} \frac{1}{j}$$

- What is the value of $\sum_{k=1}^{5} k^2$

$$\sum_{k=1}^{5} k^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 1 + 4 + 9 + 16 + 25 = 55$$

- What is the value of $\sum_{k=4}^{8} (-1)^k$

$$\sum_{k=4}^{8} (-1)^k = (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8 = 1 + (-1) + 1 + (-1) + 1 = 1$$

- Shift index:

$$\sum_{j=1}^{5} j^2 = \sum_{k=0}^{4} (k+1)^2 \text{ by setting } j = k+1, \text{ or } k = j-1$$

Geometric series

- **Geometric series**: sums of geometric progressions

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

$$\begin{aligned}
S &= \sum_{j=0}^{n} ar^j \\
rS &= \sum_{j=0}^{n} ar^{j+1} \\
&= \sum_{k=1}^{n+1} ar^k \\
&= \sum_{k=0}^{n} ar^k + (ar^{n+1} - a) \\
&= S + (ar^{n+1} - a) \\
S &= \frac{ar^{n+1} - a}{r-1}
\end{aligned}$$

Double summations

- Often used in programs

$$\sum_{i=1}^{4}\sum_{j=1}^{3} ij = \sum_{i=1}^{4}(i + 2i + 3i)$$

$$= \sum_{i=1}^{4} 6i = 6 + 12 + 18 + 24 = 60$$

- Can also write summation to add values of a function of a set

$$\sum_{s \in S} f(s)$$

$$\sum_{s \in \{0,2,4\}} s = \sum 0 + 2 + 4 = 6$$

TABLE 2 Some Useful Summation Formulae.

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

Example

- Find $\sum_{k=50}^{100} k^2$

$$\sum_{k=50}^{100} k^2 = \sum_{k=1}^{100} k^2 - \sum_{k=1}^{49} k^2 = \frac{100\cdot 101\cdot 201}{6} - \frac{49\cdot 50\cdot 99}{6} = 338350 - 40425 = 297925$$

- Let x be a real number with |x|<1, Find $\sum_{n=0}^{\infty} x^n$

$$\sum_{j=0}^{n} ar^j = \begin{cases} \dfrac{ar^{n+1}-a}{r-1} & \text{if } r \neq 1 \\ (n+1)a & \text{if } r = 1 \end{cases}, \quad \sum_{n=0}^{k} x^n = \frac{x^{k+1}-1}{x-1}, \quad \sum_{n=0}^{\infty} x^n = \lim_{k\to\infty} \frac{x^{k+1}-1}{x-1} = \frac{-1}{x-1} = \frac{1}{1-x}$$

- Differentiating both sides of $\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$

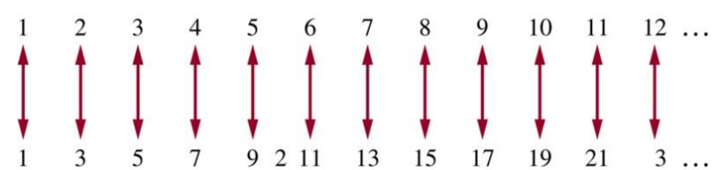
$$\sum_{k=0}^{\infty} kx^{k-1} = \frac{1}{(1-x)^2}$$

2.5 Cardinality

- The sets A and B have the same cardinality, |A|=|B|, if and only if there is a one-to-one correspondence from A to B
- **Countable**: A set that is *either* **finite** *or* has the same cardinality as the set of **positive integers**
- A set that is not countable is called **uncountable**
- When an infinite set S is countable, we denote the cardinality of S by $\mathbb{N}_0$, i.e., $|S| = \mathbb{N}_0$

Example

- Is the set of odd positive integers countable?
  - f(n)=2n-1 from Z^+ to the set of odd positive integers
  - One-to-one: suppose that f(n)=f(m) then 2n-1=2m-1, so n=m
  - Onto: suppose t is an odd positive integer, then t is 1 less than an even integer 2k where k is a natural number. Hence t=2k-1=f(k)



Infinite set

- An infinite set is countable if and only if it is possible to **<u>list</u>** the elements of the set in a sequence
- The reason being that a one-to-one correspondence f from the set of **positive integers** to a set S can be expressed by

$a_1, a_2, \ldots, a_n, \ldots$ where $a_1=f(1), a_2=f(2), \ldots a_n=f(n)$

- For instance, the set of odd integers, $a_n=2n-1$

Example

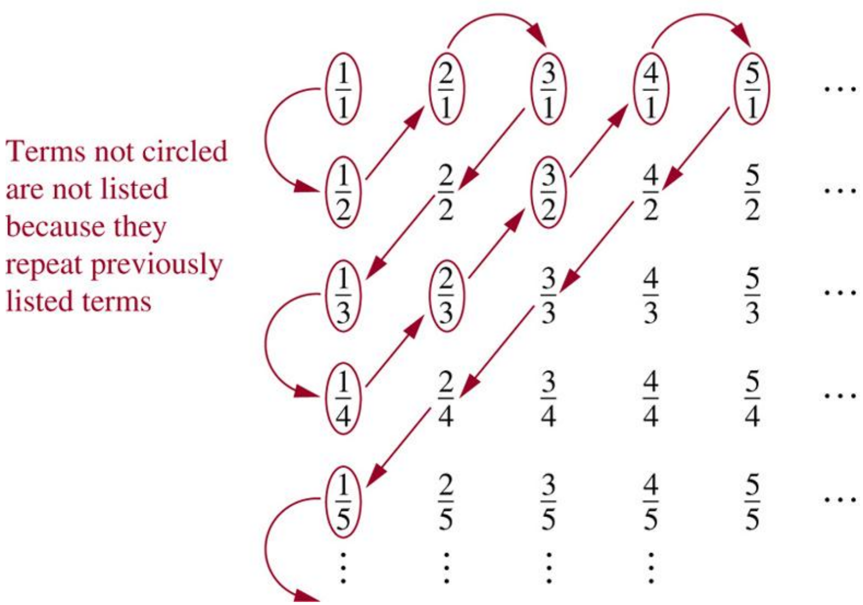
- Show the set of all integers is countable
- We can list all integers in a sequence by 0, 1, -1, 2, -2, …
- Or $f(n)=n/2$ when n is even and $f(n)=-(n-1)/2$ when n is odd (n=1, 2, 3, …)

Example

- Is the set of positive rational numbers countable?
- Every positive rational number is p/q
- First consider p+q=2, then p+q=3, p+q=4, …

1, ½, 2,3,1/3,
¼, 2/3, 3/2, 4, 5,…

Because all positive rational numbers are listed once, the set is countable



Example

- Is the set of real numbers uncountable?
- Proof by contradiction
- Suppose the set is countable, then the subset of all real numbers that fall between 0 and 1 would be countable (as any subset of a countable set is also countable)
- The real numbers can then be listed in some order, say, r_1, r_2, r_3, …

Example

- So

$$r_1 = 0.d_{11}d_{12}d_{13}d_{14}\cdots, \text{ where } d_{ij} \in \{0,1,2,3,4,5,6,7,8,9\}$$
$$r_2 = 0.d_{21}d_{22}d_{23}d_{24}\cdots$$
$$r_3 = 0.d_{31}d_{32}d_{33}d_{34}\cdots$$
$$r_4 = 0.d_{41}d_{42}d_{43}d_{44}\cdots$$
$$r = 0.23794101\ldots\text{(for example)}$$

- Form a new real number with

$$r = 0.d_1d_2d_3d_4\cdots$$
$$d_i = \begin{cases} 4 & \text{if } d_{ii} \neq 4 \\ 5 & \text{if } d_{ii} = 4 \end{cases}$$
$$r_1 = 0.23794102\cdots$$
$$r_2 = 0.44590138\cdots$$
$$r_3 = 0.09118764\cdots$$
$$r_4 = 0.80553900\cdots$$
$$r = 0.4544\ldots$$

- Every real number has a unique decimal expansion
- The real number r is not equal to r_1, r_2, … as its decimal expansion of r_i in the i-th place differs from others
- So there is a real number between 0 and 1 that is not in the list
- So the assumption that all real numbers can between 0 and 1 can be listed must be false
- So all the real numbers between 0 and 1 cannot be listed
- The set of real numbers between 0 and 1 is uncountable