Chapter 2 Basic Structures: Sets, and Functions

Discrete Mathematics and Its Applications
Zhejiang University/CS/Course/Xiaogang Jin
E-Mail: xiaogangj@cise.zju.edu.cn

2.1 Sets

□ INTRODUCTION

- **G. Cantor** (1845-1918) German Mathematician
  - 1895 founder of set theory (Naive set theory)
  - Set: a basic (undefined) concept
  - Discover that the set of real numbers is uncountable.

- **H. Poincaré** France Mathematician

- **B. Russell** (1872-1970) English Philosopher
  - Nobel Prize for literature(1950), two times imprisoned
  - His most famous work "**Principia Mathematica**" (written with A. N. Whitehead)
  - 1902 Russell Paradox

In a town, the barber shaves all and only those who do not shave themselves.
Question: does the barber shave himself?

Let $P(x) = x \notin x$ and $B = \{x \mid x \notin x\}$, $B \in B$ — true or false?

$$B \in B \Rightarrow B \notin B$$
$$B \notin B \Rightarrow B \in B$$

— Contradiction!

SETS AND SUBSETS

Set

- Set: The object in a *set* are called the elements, or members, of the set. A set is said to contain its elements.

- The ways of describing sets:
  - List
  - Predicate(stating the properties)

    Let $P(x)$ be a predicate, $\{x \mid P(x)\}$: the set of all x, such that $P(x)$ is true.
  - Venn Diagram

- Properties of sets:
  - Order of elements does not matter.
  - Repetition of elements does not matter.
  - Certainty

- Infinite and Finite Set

– Cardinality of set S ($|S|$) is the number of elements in S.

Infinite Countable (e.g., natural numbers, integers)

Uncountable (e.g., real numbers)*[Later $\cdots$]*

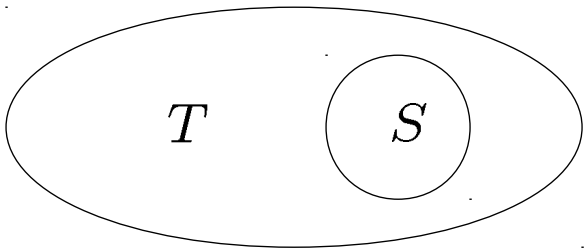
Example: We introduce several sets and their notations that will throughout this book.

$a)$ $\mathbb{Z}^+ = \{x \mid x \text{ is a positive integer}\}$
$b)$ $\mathbb{N} = \{x \mid x \text{ is a positive integer or zero}\}$
$c)$ $\mathbb{Z} = \{x \mid x \text{ is an integer}\}$
$d)$ $\mathbb{R} = \{x \mid x \text{ is a real number}\}$
$e)$ The set that has no elements is denoted by the symbol $\emptyset$ and is called empty(null) set.

Subsets

- Subsets and proper subsets
  - Subset notation: $\subseteq$

    $S \subseteq T \Leftrightarrow (\forall x \in S \Rightarrow x \in T)$
  - Proper Subset: $\subset$



  - Empty set $\emptyset$ and Universal set U:

For any set A,

$$A \subseteq A, \qquad \emptyset \subseteq A \subseteq U$$

Example: Determine whether each of the following statements is true or false.

1) $\emptyset \subseteq \emptyset$

2) $\emptyset \in \emptyset$

3) $\emptyset \subseteq \{\emptyset\}$

4) $\emptyset \in \{\emptyset\}$

2.2 Set Operations

SET OPERATIONS

If A and B are two sets, then we can define the following operations on sets:

- *Union*

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

- *Intersection*

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

Sets A, B are called *disjoint*, if $A \cap B = \emptyset$.

– *Difference*

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

If A, B disjoint, then $A - B = A$.

– *Complement*

Let U be the universal set.

$$\bar{A} = U - A$$

– *Symmetric Difference*

$$A \oplus B = (A - B) \cup (B - A)$$

SET IDENTITIES

Identity laws	$A \cup \emptyset = A \qquad A \cap U = A$
Domination laws	$A \cup U = U \qquad A \cap \emptyset = \emptyset$
Idempotent laws	$A \cup A = A \qquad A \cap A = A$
Complementation law	$\overline{\overline{A}} = A$
Commutative laws	$A \cup B = B \cup A \qquad A \cap B = B \cap A$
Associative laws	$A \cup (B \cup C) = (A \cup B) \cup C$
	$A \cap (B \cap C) = (A \cap B) \cap C$
Distributive laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Laws of excluded middle	$A \cap \overline{A} = \emptyset \qquad A \cup \overline{A} = U$
Absorption laws	$A \cap (A \cup B) = A$
De Morgan's laws	$\overline{A \cup B} = \overline{A} \cap \overline{B} \qquad \overline{A \cap B} = \overline{A} \cup \overline{B}$

Still more laws:

$A \oplus B = B \oplus A$

$(A \oplus A) = \emptyset$

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

- By using that each set is a subset of the other.
- By using logical equivalences.

Example: Let A, B, and C be sets. Prove that

1) $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap \overline{A}$.

2) If $A \oplus B = A \oplus C$ then $B = C$.

Solution: 2)

$$\begin{aligned} B &= \emptyset \oplus B = (A \oplus A) \oplus B \\ &= A \oplus (A \oplus B) = A \oplus (A \oplus C) \\ &= (A \oplus A) \oplus C \ = \emptyset \oplus C = C \end{aligned}$$

THE POWER SET AND CARTESIAN PRODUCTS

The Power Set

Definition: Given a set S, the *power set* of S is the set of all subsets of the set S. The power set of S is denoted by $P(S)$ or 2^S.

$$2^S = \{T \mid T \subseteq S\}$$

Example: 1) What is the power set of the set $\{a, b, c\}$? 2) What is the power set of the empty set? What is the power set of the set $\{\emptyset\}$?

Remark: If a set has n elements, then its power set has 2^n elements.

Cartesian Products

- The ordered n-tuple

Definition: The *ordered n-tuple* $(a_1, a_2, \cdots, a_n)$ 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.

- $(a_1, \cdots, a_n) = (b_1, \cdots, b_n) \Leftrightarrow a_i = b_i$ for $i = 1, \cdots n$.
- In particular, 2-tuples are called *ordered pairs*
  $(a, b) = (c, d) \Leftrightarrow a = c$ and $b = d$.

- Cartesian Products

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

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

– $A^2 = A \times A$ (the Cartesian square of A)

– If A and B finite, $A \times B$ finite. IF A has m elements and B has n elements, then $A \times B$ has $m \cdot n$ elements.

– If A infinite and B non-empty, $A \times B$, $B \times A$ infinite.

Properties of Cartesian Products:

(1) $A \times \emptyset = \emptyset \times B = \emptyset$

(2) In general, $A \times B \neq B \times A$

(3) In general, $(A \times B) \times C \neq A \times (B \times C)$
but $=$ hold if we identify $((a, b), c)$ and $(a, (b, c))$.

(4) $\times$ disturbs over $\cup$ and $\cap$:

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

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

– $A^n = A \times A \times \cdots \times A$ (n times)

Example: Let A, B, C and D be sets. Determine whether each of the following statements is true or false.

1) If $A \times B \subseteq C \times D$, then $A \subseteq C$ and $B \subseteq D$.
2) If $A \subseteq C$ and $B \subseteq D$, then $A \times B \subseteq C \times D$.
3) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$.
4) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$.

$A = D = \emptyset;\ B = C = \{1\}$

2.3 Cardinality of Finite and Infinite Sets

□ COUNTING FINITE SETS

- **Cardinality:** The size of a set S,denoted by $|S|$.

- **Principle of Inclusion-exclusion**: Let A and B are two finite sets, then

$$|A \cup B| = |A| + |B| - |A \cap B|$$

The principle of inclusion-exclusion can be extended to three or more sets.

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i \ne j \le n} |A_i \cap A_j| + \cdots + (-1)^{n-1} |\cap_{i=1}^{n} A_i|$$

Example: How many bit strings of length eight either start with a 1 bit or end with the two bits 00?

Solution:

First, constructing a bit string of length eight beginning with a 1 bit can be done in $2^7 = 128$ ways.

Second, constructing a bit string of length eight ending with two bits 00 can be done in $2^6 = 64$ ways.

Third, constructing a bit string of length eight beginning with a 1 bit and ending with two bits 00 can be done in $2^5 = 32$ ways.

Therefore, the number of bit strings of length eight either start with a 1 bit or and with the two bits 00 is equals to $128 + 64 - 32 = 160$.

□ CARDINALITY OF INFINITE SETS

• Two sets **have the same cardinality (equinumerous)** iff there is an one-to-one correspondence from A to B, i.e. $|A| = |B|$.

Example: Let $N_1 = \{1, 3, 5, \cdots, \}$, then $|\mathbb{N}| = |N_1|$ and where the one-to-one correspondence is $f(n) = 2n - 1$.

Example: Let $S = \{x | x \in (0, 1) \text{ and } x \in \mathbb{R}\}$, then S and $\mathbb{R}$ have the same cardinality.

– the one-to-one correspondence is $f(x) = \tan(\pi(x - \frac{1}{2}))$

or $f(x) = \text{ctan}\pi x$

Remark:

1) Two sets have the same cardinality is a equivalence relation.

2) Two sets have the same cardinality, but the one-to-one correspondence may be not unique.

3) A set and its proper set have the same cardinality iff it is infinite set.

Hilbert Hotel:

Let a hotel have a denumerable set of rooms numbered 1, 2, 3, $\cdots$.

– Any finite number n of guests can be accommodated without evicting the current guests by moving the current guests from room i to room $n + i$.

– A denumerable number of guests can be similarly accommodated by moving the existing guests from i to $2i$, freeing up a denumerable number of rooms.

- Infinite sets are divided into two types:

– countable (denumerable) set

A set that is either finite or has the same cardinality as the set of natural numbers $\mathbb{N}$, $\aleph_0$ is called countable.

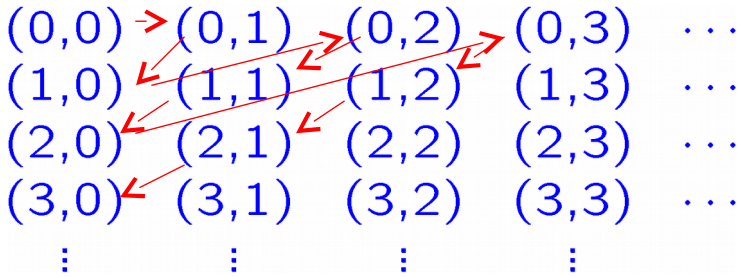
– uncountable set

- Some special infinite sets:

1) The set of integers is countable, or $|\mathbb{N}| = |\mathbb{Z}|$.

2) The set of rational numbers is countable,or $|\mathbb{N}| = |\mathbb{Q}|$.

3) The set $\mathbb{N} \times \mathbb{N}$ is denumerable.



- Properties of the countable sets:

  1) No infinite set has a smaller cardinality than a denumerable set (or, none is smaller than the set of natural numbers).

  2) The union of two countable sets is countable.

  3) The union of finite number of countable sets is countable.

  4) The union of a countable number of countable sets is countable .

Theorem: The cardinality of the power set of an arbitrary set has a greater cardinality than the original arbitrary set, or $|2^A| > |A|$.

Theorem: The set of real numbers is uncountable, or $|R| = \aleph > \aleph_0$.

Proof: (1) $|(0,1)| = |\mathbb{R}|$ $\Leftarrow \tau(x) = \tan(x - \frac{1}{2})\pi$

(2) $(0,1)$ is uncountable.

$(0,1)$ is uncountable

If (0,1) is denumerable, all the number between 0 and 1 can be listed:

$$\begin{array}{ll} 0 & 0.a_{00}a_{01}a_{02}\cdots \\ 1 & 0.a_{10}a_{11}a_{12}\cdots \\ 2 & 0.a_{20}a_{21}a_{22}\cdots \\ & \cdots\cdots \end{array}$$

where $a_{ij} \in \{0,1,2,3,4,5,6,7,8,9\}$.

Now we construct a new decimal fraction

$$b = 0.b_0b_1b_2b_3\cdots$$

where $b_i = 2$, if $a_{ii} = 1$ and $b_i = 1$ if $a_{ii} \neq 1$.

$b \in (0,1)$ $\quad$ b not in the list $\quad$ – Contradiction!

- Continuum Hypothesis(CH)

$|\mathbb{N}| = \aleph_0 \qquad |\mathbb{R}| = \aleph_1 \qquad \aleph_0 < \aleph_1$

$\exists?\ w$ such that $\aleph_0 < w < \aleph_1$

- **Cantor** formulated CH, and spent the last years of his career unsuccessfully trying to prove it. His failure obsessed him and caused recurring bouts of serious depression.

- To prove or disprove CH was the first problem on **David Hilbert**'s famous 1900 list of important unsolved problems in mathematics.

• Similarly, attempts to prove or disprove CH, or to prove it undecidable, consumed most of **Kurt Gödel**'s 36 years at the Institute for Advanced Study. But he did produce an important partial proof. In 1938, Gödel showed that CH cannot be disproved from the axioms of Zermelo-Fraenkel (ZF) set theory.

• In 1963 **Paul Cohen** showed that CH cannot be proved from the ZF axioms.

• Together, Gödel and Cohen's results show that CH is independent of the ZF axioms: neither it nor its negation can be derived from them. Among other things, this means that CH is undecidable in ZF. After Euclid's parallel postulate, CH was the first major conjecture to be proved undecidable by standard mathematics.

2.4 Functions

INTRODUCTION

Definition: Let A and B be to B:

- $\forall x \in A \exists b \in B$ s.t. $f(a) = b$
- b unique

$$f : A \to B \Leftrightarrow \forall a \in A \; \exists! b \in B : f(a) = b$$

— f *maps* A to B

- A is the domain of f, Dom $f = A$
- B is the codomain of f , Codom $f = B$
- $f(a) = b$, $a \in A$, $b \in B$

  b is the image of a, a is a pre-image of b
- The range of f is the set:

$$\text{Range}(f) = \{b \in B \mid \exists a \in A, f(a) = b\}$$

Discrete Mathematics and Its Applications
Zhejiang University/CS/Course/Xiaogang Jin
E-Mail: xiaogangj@cise.zju.edu.cn

ONE-TO-ONE AND ONTO FUNCTIONS

Definition: Let f be a function from A to B :

- one-to-one function:(injective)(单射)
  $\forall a, b \in A \wedge a \neq b \Rightarrow f(a) \neq f(b)$
- onto function:(surjective)(满射)
  $\forall b \in B \ \exists a \in A$ such that $f(a) = b$
- bijection function:(one-to-one correspondence)(双射或一一映射)
  one-to-one + onto

INVERSE AND COMPOSITION OF FUNCTIONS

Definition: Let f be a one-to-one correspondence from A to B. The inverse function of f $f^{-1} : B \to A$

$$\forall a \in A, b \in B \ (f(a) = b) \Leftrightarrow (f^{-1}(b) = a)$$

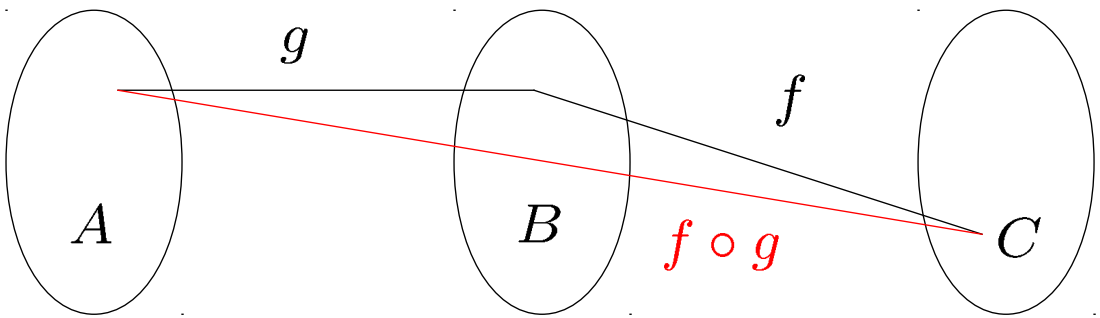
Remark:

- A one-to-one correspondence is called *invertible*.
- A function is not invertible if it is not a one-to-one correspondence, since the inverse of such a function does not exist.

Definition: Let $g : A \to B$ and $f : B \to C$ are two functions.

The composition of the functions f and g, $f \circ g : A \to C$

$$\forall a \in A,\ (f \circ g)(a) = f(g(a)).$$



SOME IMPORTANT FUNCTIONS

Definition:

- The floor functions $\lfloor x \rfloor$ assigns the real number x the largest integer that is less than or equal to x.
- The ceiling function $\lceil x \rceil$ assigns to the real number x the smallest integer that is greater than or equal to x.

Remark:

The floor function is often also called the **greatest integer function**. It is often denoted by $[x]$.

Properties of the Floor and Ceiling Functions

(1a) $\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$ where n is an integer

(1b) $\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$ where n is an integer

(1c) $\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$ where n is an integer

(1d) $\lceil x \rceil = n$ if and only if $x \leq n < x + 1$ where n is an integer

(2) $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$

(3a) $\lfloor -x \rfloor = -\lceil x \rceil$

(3b) $\lceil -x \rceil = -\lfloor x \rfloor$

(4a) $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ where m is an integer

(4b) $\lceil x + m \rceil = \lceil x \rceil + m$ where m is an integer

THE GROWTH OF FUNCTIONS

- BIG-O NOTATION

Definition: Let f and g be functions from the set of integers or the set of real numbers. We say that $f(x)$ is $\mathcal{O}(g(x))$ if there are constants C and k such that

$$|f(x)| \leq C|g(x)|$$

wherever $x > k$.

Remark: 1) $f(x)$ is $\mathcal{O}(g(x))$ can be denoted by $f(x) = \mathcal{O}(g(x))$.

2) A pair C, k that satisfies the definition is never unique.

3) If $f(x) = \mathcal{O}(g(x))$, and $|g(x)| \leq |h(x)|$ for sufficiently large values of x, then $f(x) = \mathcal{O}(h(x))$.

Example: Show that $f(x) = x^2 + 2x + 1$ is $\mathcal{O}(x^2)$.

Solution:

1) $0 \leq x^2 + 2x + 1 \leq x^2 + 2x^2 + x^2 = 4x^2$ where $x > 1$.

2) $0 \leq x^2 + 2x + 1 \leq x^2 + x^2 + x^2 = 3x^2$ where $x > 2$.

Note that in Example, $f(x) = x^2 + 2x + 1$ and $g(x) = x^2$, such that $f(x) = \mathcal{O}(g(x))$ and $g(x) = \mathcal{O}(f(x))$.

– functions $f(x)$ and $g(x)$ that satisfy both of these big-O relationships are of the **same order**.

Example: Show that $7x^2$ is $\mathcal{O}(x^3)$. Is it also true that x^3 is $\mathcal{O}(7x^2)$?

Theorem: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \cdots, a_n$ are real numbers. Then $f(x)$ is $\mathcal{O}(x^n)$.

Proof: Using the triangle inequality, if $x > 1$ we have

$$\begin{aligned}
|f(x)| &= |a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \\
&\leq |a_n|x^n + |a_{n-1}|x^{n-1} + \cdots + |a_1|x + |a_0| \\
&= x^n(|a_n| + |a_{n-1}|/x + \cdots + |a_1|/x^{n-1} + |a_0|/x^n) \\
&\leq x^n(|a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0|)
\end{aligned}$$

Then shows that

$$|f(x) \leq Cx^n$$

where $C = \sum_{k=0}^{n} |a_k|$ whenever $x > 1$. Hence $f(x)$ is $\mathcal{O}(x^n)$.

• BIG-OMEGA NOTATION AND BIG-THETA NOTATION

Definition: Let f and g be functions from the set of integers or the set of real numbers. We say that $f(x)$ is $\Omega(g(x))$ if there are constants C and k such that

$$|f(x)| \geq C|g(x)|$$

wherever $x > k$.

We say that $f(x)$ is $\Theta(g(x))$ if $f(x) = \mathcal{O}(g(x))$ and $f(x) = \Omega(g(x))$. We also say that $f(x)$ is of order $g(x)$.

Remark: $f(x) = \Theta(g(x))$ if we can find positive real numbers C_1 and C_2 and a positive number k such that

$$C_1|g(x) \leq |f(x)| \leq C_2|g(x)|$$

where $x \geq k$.

Theorem: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, where $a_0, a_1, \cdots, a_n$ are real numbers. Then $f(x)$ is of order x^n.

Homework 4:

6^{th} edition	5^{th} edition
P120 9 16 20	P85 9 13 16
P131 24 39	P94 16 32
P162 40 46	P237 36 P238 42