2 Basic Structures:Sets, Functions, Sequences, and Sums

2.1 Sets

***Definition** 1 A **set** is an unordered **collection** of **objects**.*

Cantor's naive set theory

Russel's paradox

$S = \{x | x \notin x\}$

$S \in S$ *iff* $S \notin S$. **contradictory**

Self denial is a contrdiction

How about the set

$\overline{S} = \{x | x \in x\}$

Halting problem

Is there a program that reads program and data, and

decides whether the program with the data will ***halt or not****?*

In Chap. 3.1

Some similar examples in the world

A barber who shave everybody who can not shave himself.

Shall the barber shave himself?

An adjective is heterological, if the adjective does not posses

the property it describes.(monosyllabic, polysyllabic)

Is the adjective "heterological" ***heterological****?*

How about "homolicical"?

There is a sign that "It is written by me(liar)".

Did you(liar) write it?

Contradiction ***denial of self recursion****!*

Definition *2 An object in a set is called* ***element*** *or* ***member*** *of the set. A set is said to contain its elements.*

$a \in A$ "*a is an element of the set A*"

$a \notin A$ "*a is* ***not*** *an element of the set A*"

Two ways of to define sets

i) To enumerate the elements

$A = \{a_1, a_2, \ldots, a_n\}$ *finite*

$A = \{a_1, a_2, \ldots\}$ *infinite*

ii) to specify condition with predicate

$A = \{x \mid P(x)\}$

$A = \{x \in U \mid P(x)\}$ *U:* ***universe****(domain) of discourse*

iii) to write a program(?)

CS322

Some important sets in discrete mathematics

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

Definition *3 Two sets are* ***equal*** *if and only if they have* ***same elements***.

$A = B$ *"Two set A and B are equal"*

$\{\}, \varnothing$ ***empty set*** *"a set that has no elements"*

note: $\{\} = \varnothing \neq \{\varnothing\}$.

Definition *4 The set A is said to* ***subset*** *of B, if and only if, every elements of A is also an elements of B, and denoted as* $A \subseteq B$.

$A \subseteq B \Leftrightarrow \forall x \in A \Rightarrow x \in B$

For two sets A and B, write $A \subset B$ and say that A is a proper subset of B, if and only if, $A \subseteq B$ and(but) $A \neq B$($\Leftrightarrow \neg(A = B)$).

$$A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B$$

New Definition for Equality of sets

***Definition** 3.1 Two sets A and B are **equal** if and only if A is a subset of B and B is a subset of A(vice versa).*

$$A = B, \quad \equiv A \subseteq B \wedge B \subseteq A$$
$$\equiv (\forall x \in A \Rightarrow x \in B) \wedge (\forall x \in B \Rightarrow x \in A)$$
$$\equiv \forall x \in A \Leftrightarrow x \in B$$

Two prove A = B

i) $\forall x \in A \Rightarrow x \in B)$ $A \subseteq B$, *and*
$\forall x \in B \Rightarrow x \in A)$ $B \subseteq A$.

ii) Venn Diagram

with n set variables, 2^n membership regions
similar to truth table in logic

***Theorem** 1 For any set S,*

(i) $\varnothing \subseteq S$ (ii) $S \subseteq S$.

(i) $\forall S(\varnothing \subseteq S)$ (ii) $\forall S(S \subseteq S)$

***Definition** 5 Let S be a set. If there are **exactly** n elements in S where n is a nonnegetive integer, we say that S is **finite** set and that n is the **cardinality** of the set S, and denoted as $|S|$.*

***Definition** 6 A set is said to be **finite**, if the cardinality of set is finite. A set is said to be **infinite** if it is not finite.*

The Power Set

***Definition** 7 Given a set S, the power set of S, denoted by P(S) or 2^S, is set of all subsets of S.*

$$P(S) = 2^S \equiv \{A | A \subseteq S\}$$

$$|P(S)| = |2^S| = 2^{|S|}.$$

Cartesian Products

Definition *9 Let A and B be sets. The* **Cartesian product** *of set A and B, denoted by* $A \times B$, *is …*

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

$|A \times B| = |A| \times |B|$

Definition *10 The Cartesian product of the sets* $A_1, A_2, \ldots, A_n$, *denoted by*

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

Definition *8 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, …,* a_n *as its n-th element.*

$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$, *iff,* $a_i = b_i$ *for* $i = 1, 2, \ldots, n$.

$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \equiv (a_1 = b_1) \wedge (a_2 = b_2) \wedge \ldots \wedge (a_n = b_n)$.

We call **ordered pair**, *for 2-tuples.*

The ordered pairs $(a, b) = (c, d)$, *iff,* $a = c \wedge b = d$.

Note that $(a, b) \neq (b, a)$

If $R \subseteq A \times B$, *the R is called a* ***relation*** *from A to B.(Chap. 8)*

$A \times B \neq B \times A$.

We write a R b, if $(a, b) \in R$.

Two aspects of the relation

i) subset of $A \times B$, $(a, b) \in R$.

$R \subseteq A \times B$

ii) infix binary boolean operation, $a\ R\ b$,

$R: A \times B \rightarrow \{\mathbf{T}, \mathbf{F}\}$

2.2 Set Operations

Definition 1 Union

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

Definition 2 Intersection

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

Definition 3 *Two sets A and B are called* ***disjoint****, iff, their intersection …*

$$A \cap B = \varnothing.$$

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

principles of set of inclusion-exclusion

Definition 4 Difference

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

Let domain of discourse for sets be U, U is called ***universe*** *of the set.*

Definition *5 Let U be a* ***universe****. The* ***complement*** *of the set A, denoted* $\overline{A}$*, is called the complement of A with respect to(w.r.t.) U is …*

$$\overline{A} = U - A = \{x | \, x \in U \wedge x \notin A\} = \{x \in U | \, x \notin A\}$$

Four regions in the Venn diagram for two sets A and B.

i) $A \cap B$ *ii)* $\overline{A} \cap B$ *iii)* $A \cap \overline{B}$ *iv)* $\overline{A} \cap \overline{B}$

membership table

Four cases for relations on two set in the Venn Diagram

i) $(A \cap \overline{B} = \varnothing) \wedge (\overline{A} \cap B = \varnothing)$ $\equiv A = B,$ ***equal***

ii) $(A \cap \overline{B} = \varnothing)$ *or* $(\overline{A} \cap B = \varnothing)$ $\equiv A \subseteq B$ *or* $B \subseteq A,$ ***subset***

iii) $(A \cap B = \varnothing)$ $\equiv A \cap B = \varnothing,$ ***disjoint***

iv) otherwise ***incomparable***

Set Identities

$A \cup \varnothing = A$	$A \cap U = A$	*Identity laws*
$A \cup U = U$	$A \cap \varnothing = \varnothing$	*Domination laws*
$A \cup A = A$	$A \cap A = A$	*Idempotent laws*
$\overline{(A)} = A$		*Double complement 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 ...*
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	*distributive ...*
$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	*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*

See Table 6(logical equivalence) of Section 1.2

($\{\mathbf{T}, \mathbf{F}\}, \neg, \vee, \wedge$) vs ($\{U, \varnothing\}, \bar{}\,, \cup, \cap$)

propositional logic and boolean algebra are ***isomorphic***

complete lattice

Generalized Union and Intersections

Definition 6

$$A_1 \cup A_2 \cup \ldots \cup A_n = \cup_{i=1}^{n} A_i.$$

Definition 7

$$A_1 \cap A_2 \cap \ldots \cap A_n = \cap_{i=1}^{n} A_i.$$

*Note that $\cup$ and $\cap$ are **associative** and n-ary operator.*

2.3 Functions

Definition 1 Let A and B be nonempty sets.

A **function**(**mapping**, **transformation**) f from A to B is

an assignment of exactly **one** element of B to **each**(**all**) element of A.

We write $f(a) = b$, if b is the unique element of B assigned to a of A.

We write $f: A \to B$.

total: to all elements of A(domain)

unique: exactly one elements of B(codomain)

$f: A \to B$ is a relation from A to B, $f \subseteq A \times B$.

If $f(a)=b$, we write $(a, b) \in f$ or $(a, f(a)) \in f$.

$f = \{(a, f(a)) | \ ^{\forall}a \in A\}$

$B^A = \{f: A \to B\}$

$|B^A| = |B|^{|A|}$

Let $f: A \to A$, then f is called a function on A.

Definition *2 Let $f: A \to B$.*

*A is a **domain** of f, B is a **codomain(range)** of f.*

*If $f(a)=b$, b is the **image** of a and a is the **preimage** of b.*

*Two functions f and g are said to be **equal**, if $f = g$.(**set equivalence**).*

Definition *3 Let $f_1, f_2: A \to \mathbf{R}$. $f_1+f_2, f_1 f_2: A \to \mathbf{R}$ is defined by*

$(f_1+f_2)(x) = f_1(x) + f_2(x)$ *and* $f_1 f_2(x) = f_1(x)f_2(x)$.

Definition *4 Let $f: A \to B$ and $S \subseteq A$. Then the imange of S under f is*

$f(S) = \{t \in B | \exists s \in S\ (t = f(s)\}$ *or*

$= \{f(s) \in B | \forall s \in S\}$ *for short.*

The range of f is f(A).

One-to-One and Onto function

Definition 5 Let $f: A \to B$. f is **one-to-one**(1:1) or **injective**, iff

$\forall a \in A \forall b \in A(a \neq b \to f(a) \neq f(b))$, or logically equivalent

$\forall a \in A \forall b \in A(f(a) = f(b) \to a = b)$.

A injective function is called **injection**.

Definition 6 Let $f: A \to B$ and $(A, \leq)$ and $(B, \leq)$ are **posets**(See 8.6),

if $x, y \in A$ and $x < y$, $f(x) \leq f(y)$, f is called **increasing** and

$f(x) < f(y)$, f is called **strictly increasing**

$f(x) \geq f(y)$, f is called **decreasing**

$f(x) > f(y)$, f is called **strictly decreasing**

Definition 7 Let $f: A \to B$. f is **onto** or **surjective**, iff

$\forall b \in B \exists a \in A(f(a) = b)$, or $f(A) = B$.

A surjective function is called **surjection** or **correspondence**.

Definition *8 Let* $f: A \to B$. *f is* ***one-to-one correspondence*** *or* ***one-to-one onto*** *or* ***bijective****, if f is both* ***one-to-one(injective)*** *and* ***onto(surjective)****.*

Theorem *1 Let A and B are sets.*

$|A| \leq |B|$, *if there is a* ***injection*** $f: A \to B$.

$|A| \geq |B|$, *if there is a* ***surjection*** $f: A \to B$.

$|A| = |B|$, *if there is a* ***bijection*** $f: A \to B$.

Definition *9 Let* $f: A \to B$ *and f be* ***one-to-one(injective)*** *and* ***onto(surjective) (bijective)****. The* ***inverse*** *of f also is a* ***function****,*

denoted $f^{-1}: B \to A$, *is defined by*

$f^{-1} = \{(b, a) | \ a \in A, f(a) = b \in B\}$ *or*

$f^{-1}(b) = a$ *when* $f(a) = b$.

Extension of Set Equivalence and Cardinality Revisited

Definition *5.1 Let A and B are sets. We say the* ***cardinalities*** *of A and B are same,* $|A| = |B|$, *if there is a* ***bijection*** $f: A \leftrightarrow B$.

We say that two sets A and B are ***isomorphic*** *with respect to f,* $A \cong_f B$.

If f is a ***bicection*** *from A to B and vice versa:* $f: A \leftrightarrow B$.

$\forall a \in A\ \exists^1 f(a) \in B$ and $\forall b \in B\ \exists^1 f^{-1}(b) \in A$.

We can identify B with A and f, and identify A with B and f^{-1} *(vice versa)*

Set Isomorphim

Extended Set Equivalence

Definition *10 Let $g: A \to B$ and $f: B \to C$. The composition of f and g, denoted by $f \circ g: A \to C$, is defined by*

$(f \circ g)(a) = f(g(a))$ *or* $f \circ g = \{(a, c) | f(a) = b, g(b) = c\}$.

Identity function(relation) *on A*

$\iota_A = \{(a, a) | a \in A\}$ or $\forall a \in A\ \iota_A(a) = a$.

Let $f: A \to A$. Then

$f \circ \iota_A = \iota_A \circ f = f$.

Definition *11 Let $f: A \to B$. The* ***graph*** *of the function f is defined by*

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

Definition *12 The* ***floor*** *and* ***ceiling*** *function: $\lfloor \cdot \rfloor \lceil \cdot \rceil : \mathbf{R} \to \mathbf{Z}$,*

$\lfloor x \rfloor = n \in \mathbf{Z}$, *n is the* ***largest integer*** *such that $n \le x$.(floor)*

$\lceil x \rceil = n \in \mathbf{Z}$, *n is the* ***smallest integer*** *such that $n \ge x$.(ceiling)*

***Three** face of the relation R form A to B: $R \supseteq A \times B$.*

*i) R is a sub**set of pairs***

$R \supseteq A \times B$, $(a, b) \in R$ *where* $a \in A$ *and* $b \in B$.

*ii) R is a **infix binary boolean(relational) operator***

$R: A \times B \rightarrow \{true, false\}$

$a \; R \; b$ *where* $a \in A$ *and* $b \in B$.

*iii) R is a **function** from A to* 2^B:

$R: A \rightarrow 2^B$.

$R(a) = \{b_1, b_2, \ldots, b_n\}$ *where* $a \in A$ *and* $\{b_1, b_2, \ldots, b_n\} \in 2^B$.

if $1 \leq {}^{\forall}i \leq n$, $(a, b_i) \in R$ *or* $a \; R \; b_i$. *for* $n \geq 0$,

if $n=0$, $R(a) = \{b_1, b_2, \ldots, b_n\} = \varnothing$.

Note that ${}^{\forall}a \in A$, ${}^{\exists}\{b_1, b_2, \ldots, b_n\} \in 2^B$ *is unique.*

***set valued** function.*

2.4 Sequences and Summations

Sequence $\{a_n\}$

a: $\mathbf{N} \rightarrow \mathbf{R}$. *We write* a_n *instead of* $a(n)$.

Let $s: \{1, 2, \ldots, n\} \rightarrow \{a, b, \ldots, z\}$.

We write $s = boy$ *or* $s = (b, o, y)$

instead of $s(1) = b$, $S(2) = o$, $s(3) = y$.

s is called the finite ***string*** *over V of length n.*

V is called the ***vocabulary(alphabet)*** *of string s.*

Some Useful Sequences

polynomial sequences	$n^2, n^3, n^4, \ldots$
exponential sequences	$2^n, 3^n, \ldots, n!$

Cardinality

Definition *4 The sets A and B have the same* ***cardinality****, if and only if, there is a one-to-one correspondence from A to B.*

Cardinality

Definition *5 A set is either* ***finite*** *or* ***same cardinality*** *with* $\mathbf{Z}^+$*(positive integers) is called* ***countable****. A set that is not countable is called* ***uncountable****. When an infinite set S is countable, we denote cardinality of S as* $\aleph_0$*(aleph null).* $|S| = \aleph_0$.

$\mathbf{Z}^+ \subset \mathbf{N}$	*but* $\|\mathbf{Z}^+\| = \|\mathbf{N}\| = \aleph_0$.	*See example 18*
$\mathbf{Z} \supset \mathbf{N}$	*but* $\|\mathbf{Z}\| = \|\mathbf{N}\| = \aleph_0$.	*???*
$\mathbf{Q} \supset \mathbf{N}$	*but* $\|\mathbf{Q}\| = \|\mathbf{N}\| = \aleph_0$.	*See example 20*
$\mathbf{R} \supset \mathbf{N}$	*but* $\|\mathbf{R}\| > \|\mathbf{N}\| = \aleph_0$.	*See example 21*

Cantor Diagonalization Argument*(1879)*

Consider f: $\mathbf{N} \rightarrow \{0, 1\}$

f is called ***infinite binary*** *string*

Consider the cardinality of $\{0, 1\}^{\mathbf{N}} \cong 2^{\mathbf{N}}$.

Assume $|2^{\mathbf{N}}| = \aleph_0$. *Then we can* ***enumerate*** *binary strings* B_i *for* $i \in \mathbf{N}$.

$B_0 = (b_{00}, b_{01}, b_{02}, \ldots)$

$B_1 = (b_{10}, b_{11}, b_{12}, \ldots)$

$B_2 = (b_{20}, b_{21}, b_{22}, \ldots)$

…

Consider a binary string $B = (b_0, b_1, b_2, \ldots)$

where $b_n = 0$ *if* $b_{nn} = 1$; $b_n = 1$, *if* $b_{nn} = 0$.

$\forall n \in \mathbf{N}\ B \neq B_n$. *But* $B \in 2^{\mathbf{N}}$.

$\therefore$ *The assumption* $|2^{\mathbf{N}}| = \aleph_0$ *was* ***wrong***.

$\therefore |2^{\mathbf{N}}| > \aleph_0$.

$2^{\mathbf{N}}$ *is* ***uncountable***.

Note that core of the proof is ***complement*** *of* ***diagonal(self denial)***