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

2.1 Sets

Def. *1 A **set** is an **unordered**(distinguished) **collection** of **objects**.*

*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*"

*An **ordered**(undistinguished) **collection** of **objects**.*

ordered pair, triple, quadruple, …, n-tuple

Two ways to define sets

i) To ***enumerate*** *the elements*(원소나열법)

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

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

ii) to specify ***condition*** *with* ***predicate***(조건제시법)

$P = \{x | p(x)\}$

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

truth set of predicate p(x)

$P \subseteq U$.

iii) to write a program(?)

CS322

Def. *2 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: $\{\} = \varnothing \neq \{\varnothing\}$.

Def. *3 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* $A \subseteq B$.

$$A \subseteq B \equiv (^{\forall}x \in A) \Rightarrow (^{\exists}x \in B)$$

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)* $A \neq B (\Leftrightarrow \neg(A = B))$.

$$A \subset B \equiv (A \subseteq B) \wedge (A \neq B)$$

New Definition for Equality of sets

Def. *2.1 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 ***proove*** $A = B$

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

ii) $\forall x \in B \Rightarrow x \in A)$ $\quad$ $B \subseteq A$.

Theorem *1 For any set S,*

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

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

Def. *4 Let S be a set. If there are* ***exactly*** *n elements in S where n is a non-negetive integer, we say that S is* ***finite*** *set and that n is the* ***cardinality*** *of the set S, and denoted as |S|(or #(S)).*

Def. *5 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

Def. *6 Given a set S, the power set of S, denoted by P(S) or 2^S, is set of all subsets of S.*

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

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

Cartesian Products

Def. *8 Let A and B be sets. The* **Cartesian product** *of set A and B, denoted by A × B, is set of* ***all*** **ordered pairs***(a, b), where …*

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

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

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

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

Note that $(a, b) \neq (b, a)$ *but* $\{a, b\} = \{b, a\}$.

Def. *9 The Cartesian product of the sets* $A_1, A_2, \ldots, A_n$, *denoted by*

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

Def. *7 The* **ordered n-tuple** $(a_1, a_2, \ldots, a_n)$ *is …*

$(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \ldots \times A_n$.

2.2 Set Operations

Def. *1* ***Union***

$A \cup B = \{x | x \in A \vee x \in B\} = \{x | x \in A \text{ or } x \in B\}$.

Def. *2* ***Intersection***

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

Def. *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

Def. *4* ***Difference***

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

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

Def. *5 Let U be a* ***universe****. The* ***complement*** *of the set A, denoted A, is called the complement of A with respect to(w.r.t.) U is …*

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

Compare *the* ***Venn diagrams*** *for $\cap$, $\cup$, and $\overline{\ }$ in* ***set operations***

with the ***truth tables*** *for $\wedge$, $\vee$, and $\neg$ in* ***propositional logic****.*

Set Identities Table 1 in p. 132

1. **Identity laws** $A \cup \varnothing = A$ $A \cap U = A$
2. **Domination laws** $A \cup U = U$ $A \cap \varnothing = \varnothing$
3. **Idempotent laws** $A \cup A = A$ $A \cap A = A$
4. **Double Complement law** $\overline{(\tilde{A})} = A$
5. **Commutative laws** $A \cup B = B \cup A$ $A \cap B = B \cap A$
6. **Associate laws** $A \cup (B \cup C) = (A \cup B) \cup C$
   $A \cap (B \cap C) = (A \cap B) \cap C$
7. **Distributive laws** $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
8. **De Morgan's laws** $\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$
9. **Absortion laws** $A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$
10. **Complement laws** $A \cup \overline{A} = U$ $A \cap \overline{A} = \varnothing$
11. $U/\varnothing$ **laws** $\overline{U} = \varnothing$ $\overline{\varnothing} = U$

Compare with the <u>Table 6</u>(logical equivalence) of Section 1.2 p. 25

$(\{\mathbf{T}, \mathbf{F}\}, \neg, \vee, \wedge)$ *vs* $(\{U, \emptyset\}, \overline{\ }, \cup, \cap)$

propositional logic and set algebra are ***isomorphic***

$(\{\mathbf{T}, \mathbf{F}\}, \Rightarrow)$ *and complete lattice*

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) $\overline{A} \cap \overline{B}$

Compare with the truth table in the ***logic***

2^n *regions in the Ven diagram for n sets*

Four cases for relations on two set in the Venn Diagram

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

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

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

iv) *otherwise* ***incomparable***

Generalized Union and Intersections

Definition 6 Generalized Union

$A_1 \cup A_2 \cup \ldots \cup A_n = \cup_{i=1}^{n} A_i = \cup_{i \in N_n} A_i$ *where* $N_n = \{1, 2, \ldots, n\}$.

Definition 7 Generalized Intersection

$A_1 \cap A_2 \cap \ldots \cap A_n = \cap_{i=1}^{n} A_i. = \cap_{i \in N_n} A_i$ *where* $N_n = \{1, 2, \ldots, n\}$.

*Note that ∪ and ∩ are **associative** and n-ary operator.*

2.3 Functions

Def. *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 → B, if f is a function from A to B.

***total**: for **all** elements of A(domain)*

***unique**: exactly one elements of B(codomain)*

$\forall a \in A: \exists^1 b \in B \ .\ni.\ f(a) = b.$

$|A| <^? |B|.$

*A **function** can be considered as a **set** of pairs!(Remember the **graph**)*

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

*Let f: A → A, then f is called a function **on** A.*

Def. *2 Let $f: A \rightarrow B$.*

*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**).*

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

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

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

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

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

$\subseteq B$.

The range of f is $f(A) \subseteq B$.

How many different functions $f: A \rightarrow B$?

One-to-One and Onto function

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

$\forall a \in A\ \forall b \in A, [(f(a)=f(b)) \rightarrow (a=b)]$ *or logically equivalent*

$\forall a \in A\ \forall b \in A, [(a \neq b) \rightarrow (f(a) \neq f(b))]$.

A injective function is called ***injection****.*

$|A| \leq |B|$.

Def. *6 Let f: $A \rightarrow B$ and $(A, \leq)$ and $(B, \leq)$ are* ***posets****(See 9.6),*

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***

Def. *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**.*

$|A| \geq |B|$.

Def. *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)**.*

$|A| = |B|$.

Def. *9 Let $f: A \to B$ and f be **one-to-one** and **onto (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 $f(a) = b$.

Def. *10 Let g: A → B and f: B → C. The composition of f and g, denoted by f ∘ g: A → C, is defined by*

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

Def. *11 Let f: A → B. The* ***graph*** *of the function f is defined by*

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

Def. *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)*

Def. *13* ***partial function*** *f: A ↦ B.*

$\forall a \in A$: $\exists 1 b \in B$.э. *f(a) = b. in* ***Definition*** *1. But*

$\exists a \in A$: .э. *f(a) is undifined.*

~~total~~ *and* ***uniqueness***

Identity function(relation) *on A*

Let f: A → A. Then

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

$f \circ \iota_A = \iota_A \circ f = f$. ***Identity function*** *w.r.t function composition.*

2.4 Sequences and Summations

Def. 1 sequence (수열) $\{a_n\}$

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

Def. *2* ***Geometic sequence(progression;*** 등비수열 *)*

$\{g_n\} = g(n) = ar^n$.

Def. *3* ***Arithmetic sequence(progression;*** 등차수열 *)*

$\{b_n\} = b(n) = a + nd$.

Ex. 4 string: *Let* $s: \{1, 2, \ldots, n\} \to V = \{a, b, \ldots, z\}$.

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

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

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

s is the ***string***(vocabulary sequence 문자열) *over V of length n.*

Recurrence Relation(점화식)

Def. 4 Let $a: N \rightarrow \mathbf{R}$ and $f: \mathbf{R}^n \rightarrow \mathbf{R}$. We define $a: N \rightarrow \mathbf{R}$ by

$a_n = f(a_0, a_1, \ldots, a_{n-1})$ with definitions of $a_0, a_1, \ldots,$ and a_{n-1}.

$a(n) = f(a(0), a(1), \ldots, a(n-1))$ with definitions of $a(0), \ldots, a(n-1)$.

Def. 5 Fibonacci sequence

$f_n = f_{n-1} + f_{n-1}$ with $f_0 = 0$ and $f_1 = 1$

Special Integer Sequences

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

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

See Table 1 in p. 162

Summations

See Theorem 1 and Table 2 in p. 166

2.5 Cardinality of Sets

Def. *1 A set S if* ***finite*** *with cardinality $n \in \mathbf{N}$, written $|A| = n$,*
if there is a bijection from the set {0, 1, …, n-1} to S.
A set is ***infinite*** *otherwise.*

Def. *2 The sets A and B have the same* ***cardinality****, if and only if,*
there is a bijection(one-to-one correspondence) from A to B.

Thm. *3.0 Let A and B are sets.*
$|A| \leq |B|$, *if there is a* ***injection(one-to-one)*** *$f: A \to B$.*
$|A| \geq |B|$, *if there is a* ***surjection*** *f(****onto****): $A \to B$.*
$|A| = |B|$, *if there is a* ***bijection*** *f:(****one-to-one*** $\wedge$ ***onto****) $A \leftrightarrow B$.*

Def. *3.1 Let A and B are sets. We say the* ***cardinalities*** *of A and B are same,* $|A| = |B|$*, if there is a* ***bijection*** $f: A \leftrightarrow B$.

Extended Set Equivalence

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

written $A \cong_f B$ *or* $A \cong B$ *for short.*

If f is a ***bijection*** *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 from A and f, and identify A from B and f^{-1} *(vice versa)*

Set Isomorphim *includes* ***Set Equivalence***

$\{0, 1, \ldots, n\text{-}1\} \cong_f \{1, 2, \ldots, n\}$ *What is f?*

$\{0, 1, \ldots, n\text{-}1\} = \{0, 1, \ldots, n\text{-}1\}$ *and* $\{0, 1, \ldots, n\text{-}1\} \cong_f \{0, 1, \ldots, n\text{-}1\}$ *f?*

Countable Sets

Def. *4 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).* $|S| = \aleph_0$.

$\mathbf{N} \supset \mathbf{N}^+$ *but* $|\mathbf{N}| = |\mathbf{N}^+| = \aleph_0$.

$\mathbf{N} \cong_f \mathbf{N}^+$ *What is the natural number,* $\mathbf{N}$ *or* $\mathbf{N}^+$*?*

$\mathbf{I} \supset \mathbf{N}$ *but* $|\mathbf{I}| = |\mathbf{N}| = \aleph_0$. *What is the* ***bijection****?*

$\mathbf{Q} \supset \mathbf{N}$ *but* $|\mathbf{Q}| = |\mathbf{N}| = \aleph_0$. *See example 4*

But!

$\mathbf{R} \supset \mathbf{N}$ *but* $|\mathbf{R}| > |\mathbf{N}| = \aleph_0$. *See example 5*

Uncountable Sets

Cantor Diagonal Argument*(1874, 1891)*

Consider $f:\mathbf{N} \to \{0, 1\}$ *or* $f = \{0, 1\}^{\mathbf{N}}$.

f is an ***infinite binary*** *string*

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

Power set *of natural numbers*

Assume $|2^{\mathbf{N}}| = |\mathbf{N}|$. *Then we can* ***enumerate***(번호매김 ; countable)

binary strings B_i *for* $i \in \mathbf{N}$.

$B_0 = (b_{00}, b_{01}, \ldots, b_{0n}, \ldots)$

$B_1 = (b_{10}, b_{11}, \ldots, b_{1m}, \ldots)$

…

$B_n = (b_{n0}, b_{n1}, \ldots, b_{nn}, \ldots)$

…

Define ***complement*** *of a binary string* $B = (b_0, b_1, \ldots, b_n, \ldots)$,

$\overline{B} = (\overline{b}_0, \overline{b}_1, \ldots, \overline{b}_n, \ldots)$ *where for* $i \in \mathbf{N}$,

$\overline{b}_i = 0$, *if* $b_i = 1$ *and* $\overline{b}_i = 1$, *if* $b_i = 0$.

Consider an ***infinite diagonal*** *binary string* $B_d = (b_{00}, b_{11}, \ldots, b_{nn}, \ldots)$
and its ***complement*** $\overline{B}_d = (\overline{b}_{00}, \overline{b}_{11}, \ldots, \overline{b}_{nn}, \ldots)$

$\forall n \in \mathbf{N}, \overline{B}_d \neq B_n$. *But* $\overline{B}_d \in 2^{\mathbf{N}}$.($\overline{B}_d$ *is an infinite binary string)*

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

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

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

Note that core of the proof is

complement *of* ***diagonal(denial*** *of* ***self recursion)***

in ***infinite*** *string*

Halting problem

Is there a program that reads program as a 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****!*

***<u>Russel's paradox</u>*(1901, 1911)**

Assume a set R is defined as $R = \{x| \; x \notin R\}$.

Consider x as R itself, Then $R \in R$ *iff* $R \notin R$. ***contradictory***

$\therefore$ *R is undefined!*

Self denial is a contrdiction

How about the set?

$\overline{R} = \{x| \; x \in R\}$

<u>Gödel's Incompleteness Theorem(1931)</u>

Hilbert's 2nd problem(*23 problems; 1929*)

Is there a

Any logic cannot be both consistent and complete.

proof

$\mathbf{G}(p\text{: Theorem}) \equiv$ *Gödel number of the theorem p*

$F(x\text{: Gödel number}) \equiv$

$\quad \textbf{if } \exists p\text{: Theorem(Proof) for } x \rightarrow \mathbf{T}$

$\quad\ \mid\ \nexists p\text{: Theorem(Proof) for } x \rightarrow \mathbf{F}\ \textbf{fi}$

$Bew(y\text{: Gödel number}) \equiv$

$\quad \textbf{if } \exists p\text{: } F(\mathbf{G}(p)) \rightarrow \mathbf{T} \mid \nexists p\text{: } F(\mathbf{G}(p)) \rightarrow \mathbf{F}\ \textbf{fi}$

$\overline{Bew}(y\text{: Gödel number}) \equiv$

$\quad \textbf{if } \exists p\text{: } F(\mathbf{G}(p)) \rightarrow \mathbf{F} \mid \nexists p\text{: } F(\mathbf{G}(p)) \rightarrow \mathbf{T}\ \textbf{fi}$

$$\overline{Bew}(\mathbf{G}(\overline{Bew})) \Leftrightarrow \exists p\text{: } F(\mathbf{G}((\overline{Bew}))$$

$$\Leftrightarrow \nexists p\text{: } F(\mathbf{G}(\overline{Bew}))$$

Contradiction!

Thm. 2 *If A and B are* ***countable*** *sets, then* $A \cup B$ *is also* ***countable***.

proof *Without loss of generality, we can assume A and B are* ***disjoint***.

If there are not, we can replace B by B – A because

$A \cap (B - A) = \varnothing$ *and* $A \cup (B - A) = A \cup B$. *(Venn diagram)*

case i) A and B are both ***finite***. $|A| + |B|$ *is finite and* ***countable***.

case ii) A ***countable*** *and B is* ***finite***.

$A \cup B = b_1, b_2, \ldots, b_m, a_1, a_2, \ldots, a_n, \ldots$ *is* ***countable***.

case iii) Both A and B are ***countable***.

$A \cup B = a_1, b_1, a_2, b_2, \ldots, a_n, b_m, \ldots$ *is* ***countable***.

Theorem 3 *Let A and B are sets with* $|A| \le |B|$ *and* $|B| \le |A|$. *Then* $|A| = |B|$.

In other words,

$\exists f: A \rightarrow B$ *is a 1-1 and* ($\exists g: B \rightarrow A$ *is*) *1-1.*

Definition 5 *Let S be a set. Then* $f: N \rightarrow S$

2.6 Matrices