

1.A Sets, Relations, Graphs, and Functions

Set *a collection of objects(element)*

Let A be a set. If a is the elements in A, we write $a \in A$.

How to specify sets

1. *to enumerate all of the elements*
2. *to state the **properties** that characterizes the elements.*

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

$p(x)$ is a **predicate**

$p(x)$ is either **true** or **false** depending on x

$$A = \{x \in U \mid p(x)\}$$

$A \subseteq U$, U is the **universe of discourse**

$x \in U$ U is the **type** of x in A

$p(x)$ **attribute** of x

3. *automata, grammars, programs*

Three cases for two sets A and B

Case 1. subset

$$A \subseteq B \text{ or } B \subseteq A$$

$$\Leftrightarrow A - B = \emptyset \text{ or } B - A = \emptyset$$

$$\Leftrightarrow A \cap \bar{B} = \emptyset \text{ or } B \cap \bar{A} = \emptyset$$

Case 2. disjoint

$$A \cap B = \emptyset$$

Case 3. in general (neither subset nor disjoint)

$$\text{not}(A \subseteq B \text{ or } B \subseteq A) \text{ and not } (A \cap B = \emptyset)$$

$$\Leftrightarrow A \not\subseteq B \text{ and } B \not\subseteq A \text{ and } A \cap B \neq \emptyset.$$

$$\Leftrightarrow A \cap \bar{B} \neq \emptyset \text{ and } \bar{A} \cap B \neq \emptyset \text{ and } A \cap B \neq \emptyset.$$

Venn diagram

$$\bar{A} \cap \bar{B} ? = \emptyset$$

Cartesian product of two sets, A and B

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

$(a, b) \in A \times B$ **ordered pair.**

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

Binary relation R from A to B .

$$R \subseteq A \times B. \quad a \in A, b \in B, (a, b) \in R \text{ or } a R b.$$

Product of two relations R and S where $R \subseteq A \times B$ and $S \subseteq B \times C$.

$$R \cdot S = \{(a, c) \mid (a, b) \in R, (b, c) \in S\}$$

Binary relation R on A $R \subseteq A \times A$.

$$\text{Identity relation } R \text{ on } A \quad id_A = \{(a, a) \mid a \in A\}$$

$$\forall R \subseteq A \times A, R \cdot id_A = id_A \cdot R = R$$

Inverse of a relation R , $R^{-1} = \{(b, a) \mid (a, b) \in R\}$

Repeated product of binary relations.

Let $R \subseteq A \times A$. We define

$$R^2 = R \cdot R, \quad R^3 = R \cdot R \cdot R, \quad \dots \quad R^n = R \cdot R \cdot \dots \cdot R, \text{ and}$$

$R = R^1$. Then

$$R^n R^m = R^{n+m}, \text{ for } (\forall n, m \in \mathbb{N}), n, m \geq 1.$$

$R^0 = ?$ If we define $R^0 = id_A$,

$$R^n R^m = R^{n+m}, \text{ for } n, m \geq 0.$$

Another (**recursive**) definition for **repeated product** of binary relations

$$R^0 = id_A. \quad \text{basis}$$

$$R^n = R \cdot R^{n-1}, n \geq 1. \quad \text{recursion}$$

$$\text{ex) } R^3 = R \cdot R^2 = R \cdot R \cdot R^1 = R \cdot R \cdot R \cdot R^0 = R \cdot R \cdot R \cdot id_A = R \cdot R \cdot R$$

Some properties of the binary relations

R is *reflexive*, if $\forall a \in A, a R a$.

$$id_A \subseteq R$$

R is *symmetric*, if $a R b$ implies $b R a$.

$$R = R^{-1}$$

R is *transitive*, if $a R b$ and $b R c$ implies $a R c$.

$$R \cdot R \subseteq R$$

R is *irreflexive*, if $\forall a \in A, a \not R a$.

$$R \cap id_A = \emptyset$$

R is *asymmetric*, if $a R b$ implies $b \not R a$.

$$R \cap R^{-1} = \emptyset$$

R is *asymmetric* $\Rightarrow R$ is *irreflexive*.

R is *antisymmetric*, if $a R b$ and $a \neq b$ implies $b \not R a$. $R \cap R^{-1} \subseteq id_A$

R is *asymmetric* $\Rightarrow R$ is *antisymmetric*.

A *directed graph* $G = (V, E)$ is

V : a set of *vertices*,

$E \subseteq V \times V$: a set of *edges*,

E : a *binary relation* on V

Let $\mathbb{P} = \{\text{reflexive, symmetric, transitive}\}$ and R' be the \mathbb{P} -closure of R .

i) R' is \mathbb{P} .

ii) $R \subseteq R'$.

iii) R' is the **smallest** set among satisfying i) and ii).

$\Leftrightarrow \forall R''$ satisfying i) and ii), $R' \subseteq R''$.

reflexive closure of R , $R' = R \cup id_A$.

symmetric closure of R , $R'' = R \cup R^{-1}$.

transitive closure of R ,

$$R^+ = R^1 \cup R^2 \cup R^3 \cup \dots = \bigcup_{i \in N_1} R^i \text{ where } N_1 = \{1, 2, 3, \dots\}.$$

reflexive-transitive closure of R ,

$$R^* = R^0 \cup R^1 \cup R^2 \cup R^3 \cup \dots = \bigcup_{i \in N_0} R^i \text{ where } N_0 = \{0, 1, 2, \dots\}.$$

What is the **reflexive-symmetric-transitive closure** of R ?

A binary relation R is **equivalence**,

if R is **reflexive**, **symmetric**, and **transitive**.

A binary relation R is **(ir)reflexive partial order**,

if R is **(ir)reflexive**, **antisymmetric**, and **transitive**.

Let $R \subseteq A \times A$ be an **equivalence**,

$[a]_R = \{b \in A \mid a R b\}$ **equivalence class**,

if $a R b$, $[a]_R = [b]_R$.

$\{[a]_R \mid a \in A\}$ **equivalence partition**.

$\cup_{a \in A} [a]_R = A$, if $a R b$. $[a]_R \cap [b]_R = \emptyset$.

Power set of a set A ,

$P(A) = 2^A = \{B \mid B \subseteq A\}$ $B \subseteq A \Leftrightarrow B \in 2^A$.

$|2^A| = 2^{|A|}$.

Let A be a set and \oplus be a binary operation on A .

$$\oplus: A \times A \rightarrow A.$$

- i) $\forall a, b \in A, a \oplus b \in A.$ **closed** **algebraic system**
- ii) $\forall a, b, c \in A, a \oplus (b \oplus c) = (a \oplus b) \oplus c$ **associative** **semi-group**
binary operation \Rightarrow n-ary operation
- iii) $\exists e \in A .\exists. \forall a \in A, e \oplus a = a \oplus e = a$ **identity** **monoid**

Let (A, \oplus, e) and $(B, \otimes, \varepsilon)$ be two monoids.

- If
- i) $h: A \rightarrow B$ is a onto function, $|A| \geq |B|$
- ii) $h(a \oplus b) = h(a) \otimes h(b)$, and *preserve operation*
- iii) $h(e) = \varepsilon.$ *preserve identity*

Then h is called a **homomorphism**, and the monoid $(B, \otimes, \varepsilon)$ is called a **homomorphic** to the monoid (A, \oplus, e) w.r.t. h .

(A, \oplus, e) is called **concretization** of $(B, \otimes, \varepsilon)$ and

$(B, \otimes, \varepsilon)$ is called **abstract interpretation** of (A, \oplus, e) .

If h is one-to-one and onto, h is called **isomorphism**.

Let \leq be a partial order on A . $\leq \subseteq A \times A$

Then (A, \leq) is called as partially ordered set or **poset** for short.

Let (A, \leq) be a poset. We define binary operator on A ,

$$\vee, \wedge : A \times A \rightarrow 2^A$$

$$a \vee b = \min \{c \in A \mid a \leq c \text{ and } b \leq c\} \quad \text{least upper bound}$$

$$a \wedge b = \max \{c \in A \mid c \leq a \text{ and } c \leq b\}. \quad \text{greatest lower bound}$$

If a **unique** lub and a **unique** glb,

$$\vee, \wedge : A \times A \rightarrow A. \quad (A, \leq) \text{ is called as a } \mathbf{lattice} \text{ and}$$

(A, \vee, \wedge) is called a **algebra** induced by the lattice (A, \leq) .

Boolean algebra, $(\{f, t\}, \vee, \wedge)$, is induced by the lattice $(\{f, t\}, \{f \leq t\})$.

Let A be a sets. Then

Set algebra on A , $(2^A, \cup, \cap)$, is induced by the lattice $(2^A, \subseteq)$.

Singleton set algebra, $(2^{\{a\}}, \cup, \cap)$, is **isomorphic** to

boolean algebra, $(\{f, t\}, \vee, \wedge)$ with respect to **bijection** g .

What is the **bijective** function g ?

A binary **relation** from A to B is said to be a **function** from A to B , if

- | | |
|--|---------------|
| 1) $\forall a \in A, \exists (a, b) \in f,$ | total |
| 2) $\forall a \in A, \exists_1(a, b) \in f.$ | unique |

$f: A \rightarrow B$ $(a, b) \in f$ or $a f b$ or $f(a) = b$ or $f a = b.$

Relation revisited

i) $R \subseteq A \times B.$ *set of pairs*

ii) $R: A \rightarrow 2^B$ *set valued function*

$R(a) = \{b_1, b_2, \dots, b_n\},$ iff $(a, b_1), (a, b_2), \dots, (a, b_n) \in R.$

$\forall a \in A, \exists_1\{b_1, b_2, \dots, b_n\} \subseteq B$ or $\exists_1\{b_1, b_2, \dots, b_n\} \in 2^B.$

$\therefore R: A \rightarrow 2^B.$

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

$R(a, b) = \text{true},$ iff $(a, b) \in R.$

1.B Strings and languages, revisited.

Concatenation of strings, revisited

$$\therefore \Sigma^* \times \Sigma^* \rightarrow \Sigma^* .$$

a function from two strings to a string
a binary operation on strings

$$(1) \forall x, y \in \Sigma^*, xy \in \Sigma^* .$$

closed

$$(2) \exists x, y \in \Sigma^*, xy \neq yx$$

noncommutative

$$(3) \forall x, y, z \in \Sigma^*, x(yz) = (xy)z$$

associative

$$(4) \forall x \in \Sigma^*, \varepsilon x = x\varepsilon = x$$

ε is the identity element

$\therefore (\Sigma^*, \cdot, \varepsilon)$ is a noncommutative monoid.

Another (*recursive*) definition of Σ^* .

basis $\varepsilon \in \Sigma^*$ and $\forall a \in \Sigma, a \in \Sigma^*$.

recursion 1 If $x, y \in \Sigma^*$, then $xy \in \Sigma^*$.

recursion 2 If $x \in \Sigma^*$ and $a \in \Sigma$, then $xa \in \Sigma^*$.

Extend the domain and range of the concatenation from strings to languages (set of strings)

$$\therefore 2^{\Sigma^*} \times 2^{\Sigma^*} \rightarrow 2^{\Sigma^*}.$$

Let $L, S \subseteq \Sigma^*$ (or $L, S \in 2^{\Sigma^*}$). Then we define

$$LS = \{xy \mid x \in L, y \in S\}$$

$$|LS| \leq |L| \times |S|$$

$(2^{\Sigma^*}, \cdot, \{\varepsilon\})$ is a (induced) noncommutative **monoid**.

power of an alphabet revisited

$$\Sigma^0 = \{\varepsilon\} \quad \text{basis}$$

$$\Sigma^n = \Sigma\Sigma^{n-1} \text{ for } n \geq 1 \quad \text{recursion}$$

$$|\Sigma^n| = |\Sigma|^n.$$

We can **extend** to the power of languages

$$L^0 = \{\varepsilon\} \quad \text{basis}$$

$$L^n = LL^{n-1} \text{ for } n \geq 1 \quad \text{recursion}$$

$$|L^n| \leq |L|^n.$$

$$L^* = L^0 \cup L^1 \cup L^2 \cup \dots = \bigcup_{i \in N_0} L^i.$$

$$L^+ = L^1 \cup L^2 \cup L^3 \cup \dots = \bigcup_{i \in N_1} L^i.$$

For any $L \subseteq \Sigma^*$, $L^* \subseteq \Sigma^*$.

$\varepsilon \notin \Sigma^+$, but $\varepsilon \in L^+$, only if $\varepsilon \in L$.

String, revisited

Let x be a string over Σ . Then we write $x \in \Sigma^$.*

Let $|x| = n (n \geq 0)$. Then

$$x = a_1 a_2 \dots a_n \in \Sigma^n \text{ or } \Sigma^* \text{ (if } n=0, x = a_1 a_2 \dots a_n = \varepsilon)$$

$$\text{where } 1 \leq \forall i \leq n, a_i \in \Sigma.$$

Consider a function $x: \{1, 2, \dots, n\} \rightarrow \Sigma$.

$$1 \leq \forall i \leq n, \text{ if } x(i) = a_i, \text{ we can write } x = (a_1, a_2, \dots, a_n)$$

$$a_1 a_2 \dots a_n \leftrightarrow^{1:1} (a_1, a_2, \dots, a_n)$$

The strings over Σ of length $n (\Sigma^n)$,

is isomorphic to the functions from $\{1, 2, \dots, n\}$ to Σ w.r.t. f .

Let $B^A = \{f \mid f: A \rightarrow B\}$. Then $|B^A| = |B|^{|A|}$.

$$|\Sigma^n| = |\Sigma^{\{1, 2, \dots, n\}}| = |\Sigma|^n.$$

Let $x = a_1a_2 \dots a_n$ be a string of length n and $k \geq 0$.

$x^R = a_na_{n-1} \dots a_2a_1$. **reversal** of x .

$k:x = a_1a_2 \dots a_k$, if $k \leq n$; **prefix** of x with length k .
= x , otherwise.

$x:k = (k:x^R)^R$. **suffix** of x with length k .

1.C Set isomorphism and infinite sets

If there exists a **bijection** (, onto 1-1) f from A to B ,
 two sets A and B have same **cardinality**, written $|A| = |B|$, and
 two sets A and B are said to be **isomorphic** w.r.t. f , $A \cong_f B$.

function f is **onto** (surjection; correspondence), if

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

$$|A| \geq |B|$$

f^{-1} is **total** but **not** unique function.

function f is **one-to-one** (injection), if

$$\forall a_1, a_2 \in A, a_1 \neq a_2 \text{ implies } f(a_1) \neq f(a_2).$$

$$\text{if } \exists b \in B . \exists. f(a) = b, \exists_1 a \in A.$$

$$|A| \leq |B|$$

f^{-1} is **unique** but **not** total function.

function f is **one-to-one and onto (bijection)**.

$$\forall b \in B, \exists a \in A .\exists. f(a) = b. \wedge \forall a_1, a_2 \in A, a_1 \neq a_2 \text{ implies } f(a_1) \neq f(a_2).$$

$$\forall b \in B, \text{ if } \exists_1 a \in A .\exists. f(a) = b.$$

$$|A| = |B|$$

f^{-1} is a **function**.

Let f be a bijective (1-1 and onto) function from A to B .

$$f: A \leftrightarrow B.$$

f is a function from A to B , and

f^{-1} is a function from B to A .

$$\forall a \in A, \exists_1 f(a) \in B \wedge \forall b \in B, \exists_1 f^{-1}(b) \in A.$$

The set A and B are **isomorphic** w.r.t. f , $A \cong_f B$.

Two sets A and B has same **cardinality**, if there is a bijective function between them.

*A set is said to be **countable (enumerable, (finite or infinite))**, if it has the same cardinality with a subset of \mathbb{N} , and **uncountable (infinite)**, otherwise.*

*A set is **countably infinite**, if it has the same cardinality with \mathbb{N} . the cardinality of \mathbb{N} is denoted as \aleph , $|\mathbb{N}| = \aleph$.*

*Let A be **countable**. Then we can **enumerate** the set in **numeric order**.*

$A = \{a_0, a_1, \dots, a_n\}$ ***finite** for some $n \geq 0$.*

$A = \{a_0, a_1, \dots \}$ ***infinite(countable, enumerable)***

Consider

$$N_1 = \{1, 2, 3, \dots\}$$

$$|N_1| = |\mathbb{N}| = \aleph, \text{ but } N_1 \subset \mathbb{N}.$$

$$E = \{e \in \mathbb{N} \mid e = 2i, i \in \mathbb{N}\}$$

$$|E| = |\mathbb{N}| = \aleph, \text{ but } E \subset \mathbb{N}.$$

$$I = \mathbb{N} \cup \{-i \mid i \in \mathbb{N}\}$$

$$|I| = |\mathbb{N}| = \aleph, \text{ but } \mathbb{N} \subset I.$$

$$Q = \mathbb{N} \times \mathbb{N}$$

$$|Q| = |\mathbb{N}| = \aleph.$$

enumerate $(i, j) \in \mathbb{N} \times \mathbb{N}$ in (natural) numeric order

$$\mathbb{N} \times \mathbb{N} = \{(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), (3, 0), (2, 1), \dots\}$$

$$f(i, j) = 1 + 2 + 3 + \dots + (i+j) + j \qquad f(0, 0) = 0$$

$$= (i+j)(i+j+1)/2 + j$$

$f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ is one-to-one and onto

$$\therefore |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \aleph.$$

Prove $|\Sigma^*| = \aleph$.

Proof Canonical(lexicographical) order for Σ^* .

in order of size and if same size, alphabetic order.

Let $|\Sigma| = k$. Then we can alphabetic order $\Sigma = \{a_0, a_1, \dots, a_{k-1}\}$,

and we can order $x \in \Sigma^*$ where $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \dots = \bigcup_{i \in \mathbb{N}_0} \Sigma^i$.

$\Sigma^* = \{\underline{\varepsilon}, \underline{a_0}, \underline{a_1}, \dots, \underline{a_{k-1}}, \underline{a_0a_0}, \underline{a_0a_1}, \dots, \underline{a_0a_{k-1}}, \underline{a_1a_0}, \dots, \underline{a_{k-1}a_{k-1}}, \underline{a_0a_0a_0}, \dots, \underline{a_{k-1}a_{k-1}a_{k-1}}, \dots\}$

If $x = a_1a_2 \dots a_n$, the order of x , $f(x)$, is n -digit k -ary number plus base.

$$\begin{aligned} f(x) &= k^0 + k^1 \dots + k^{n-1} + a_1k^{n-1} + a_2k^{n-2} + \dots + a_nk^0 \\ &= (k^n - 1)/(k-1) + a_1k^{n-1} + a_2k^{n-2} + \dots + a_nk^0. \end{aligned}$$

We enumerate $x = a_1a_2 \dots a_n \in \Sigma^*$ in numeric order

$\therefore f: \Sigma^* \rightarrow \mathbb{N}$ is one-to-one onto. Q.E.D.

Consider $\{0, 1\}^{\mathbb{N}}$: **infinite binary strings** (See pp.12)

and $2^{\mathbb{N}}$: **power set of natural numbers** (Note that $2^A = \{B \mid B \subseteq A\}$)

Cantor's diagonal argument

Assume $2^{\mathbb{N}}$ is countable.

We can **enumerate** $|2^{\mathbb{N}}|$ subsets of \mathbb{N} , in numeric order as follows,

$2^{\mathbb{N}} = \{a_0, a_1, \dots, a_i, \dots\}$ where

$$\forall i \in \mathbb{N}, a_i \leftrightarrow (b_{i0}, b_{i1}, \dots, b_{ij}, \dots) \in 2^{\mathbb{N}}$$

$$\forall j \in \mathbb{N}, \text{ if } b_{ij} = 1 \text{ then } j \in a_i \in 2^{\mathbb{N}},$$

$$\text{ if } b_{ij} = 0 \text{ then } j \notin a_i \in 2^{\mathbb{N}}.$$

\therefore Power set of $\mathbb{N} \leftrightarrow$ infinite binary string

Power set of integers and infinite binary strings are isomorphic.

$$\therefore |2^{\mathbb{N}}| = |\{0, 1\}^{\mathbb{N}}|.$$

Consider $a \leftrightarrow (\bar{b}_0, \bar{b}_1, \dots, \bar{b}_i, \dots)$ where $\forall i \in \mathbb{N}$, $\bar{b}_i = 1$, if $b_{ii} = 0$,
 $\bar{b}_i = 0$, if $b_{ii} = 1$.

Since $\forall i \in \mathbb{N}$, $\bar{b}_i \neq b_{ii}$, $\therefore \forall i \in \mathbb{N}$, $a \neq a_i$.
 $\therefore a \notin \{a_0, a_1, \dots, a_i, \dots\}$.

But $a \in 2^{\mathbb{N}}$ by the **definition** of power set.

$a \notin \{a_0, a_1, \dots, a_i, \dots\}$ but $a \in 2^{\mathbb{N}}$.

\therefore **Contradiction!!!**

We fail to enumerate $2^{\mathbb{N}} = \{a_0, a_1, \dots, a_i, \dots\}$ in numeric order!

\therefore **We conclude that $|2^{\mathbb{N}}| > |\{a_0, a_1, \dots, a_i, \dots\}| = \aleph$.**

$2^{\mathbb{N}}$ is uncountable.

$\{0, 1\}^*$ vs $\{0, 1\}^{\mathbb{N}}$.

$\{0, 1\}^*$: *all(countably infinite union of finite binary strings*

$$= \{0, 1\}^0 \cup \{0, 1\}^1 \cup \{0, 1\}^2 \cup \{0, 1\}^3 \cup \dots$$

$$= \{\varepsilon\} \cup \{0, 1\} \cup \{00, 01, 10, 11\} \cup \{000, \dots, 111\} \cup \dots$$

$$= \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \dots, 111, \dots\}$$

$\{0, 1\}^{\mathbb{N}}$: *all(uncountably infinite union of) infinite binary strings*

$$= \{000\dots000\dots, \quad \leftrightarrow \{\}$$

$$100\dots000\dots, \quad \leftrightarrow \{0\}$$

$$010\dots000\dots, \quad \leftrightarrow \{1\}$$

$$110\dots000\dots, \quad \leftrightarrow \{0, 1\}$$

...

$$111\dots111\dots\} \quad \leftrightarrow \{0, 1, 2, \dots\} = \mathbb{N}$$

$$|\{0, 1\}^{\mathbb{N}}| = |2^{\mathbb{N}}| > |\{0, 1\}^*| = \aleph.$$

Cantor's diagonal argument

Complement of diagonal element

Russel's paradox

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

$$x \in S, \text{ iff } x \notin x.$$

*But $S \in S$, iff $S \notin S$. **contradictory!***

Halting problem

$H(P)$: if halt(P, P) then loop forever

*elses not halt(P, P) then stop **fi***

What happens if $H(H)$ stops or loops forever?

Denial of self recursion

Σ^ is countable.*

strings are countable

But is 2^{Σ^} uncountable.*

languages are uncountable

class of languages

N. Chomsky

Finite(countable)

Countably infinite

*natural numbers, integers, rational numbers,
finite strings ...*

Uncountable

Cantor's diagonal argument

*power set of natural numbers
infinite strings
real numbers*

Some informal descriptions on countable and uncountable infiniteness

$\aleph \pm k = \aleph$ $\aleph \times k = \aleph$ ***countable***

$\aleph \times \aleph = \aleph$ $\aleph^k = \aleph$ ***countable***

But $k \times k \times \dots = k^{\aleph} > \aleph$ ***uncountable*** ($k \geq 2$)