Discrete Mathematics (for Computer Science)

Final Session

TA

2021-12-24

INSTITUTE OF PARALLEL AND DISTRIBUTED SYSTEMS

范围1: 期末考试（闭卷）

- **逻辑1, 2, 4, 5章**
  - 不包括存在型前束范式
- **集合论9, 10, 11.1,11.2章节**

- **一切以课本为准，不要使用DPLL等课本上没有的技术**

范围2: quiz（开卷）

- **形式化验证**
  - DPLL, convert program into SAT
  - Lazy SMT, EUF, symbolic execution
  - Hoare triple, Hoare inference rules, loop invariant(quiz会给出invariant), weakest precondition
  - 不考WFF的自动识别, strongest postcondition

- **自动机和图灵机**
  - DFA, Turing machine basics, the language of Turing machine
  - 不考Turing machine variants, undecidability

Set theory

- **Definition & Representation**
- **Operations**
- **Set identities**
- **Cardinality of finite set**
- **ZF Axiom System**

Definition of Set

- **A Set is an unordered collection of distinct objects, which may be anything (including other sets).**
  - Unorder(无序性） Distinction(特异性) and Deterministic（确定性）
  - Enumerate（外延表示法） or set-builder notation（内涵表示法）

$$\{2,3,5,7,11,\dots\} = \{x \mid x\ is\ a\ prime\ number\}$$

$\mathbb{N}$:All the natural number:$0, 1, 2, 3, \dots$

$\mathbb{Z}$:All the integer:$\dots, -2, -1, 0, 1, 2, \dots$

$\mathbb{Q}$:All the rational number

$\mathbb{R}$:All the real number

$\mathbb{C}$:All the complex number

$\varnothing$:Empty set, contains nothing.$\{\}$

U:The universal set, contains all the objects under *consideration*

Relations Between Sets

- $A = B \Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$
- $A \subseteq B \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$
- $A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$

Set Operation

- $A \cup B = \{x | x \in A \vee x \in B\}$
- $A \cap B = \{x | x \in A \wedge x \in B\}$
- $A - B = \{x | x \in A \wedge x \notin B\}$
- $-A \text{ or } \bar{A} = \{x | x \in U \wedge x \notin A\}$
- $A \bigoplus B = \{x | x \in A \mathbin{\overline{\vee}} x \in B\} = (A - B) \cup (B - A)$

Set Operation

- $\bigcup A = \{x | (\exists z)(z \in A \land x \in z)\}$
- $\bigcap A = \{x | (\forall z)(z \in A \rightarrow x \in z)\}$
- $\mathrm{P}(A) = \{x | x \subseteq A\}$
- $\mathrm{A} \times B = \{< \mathrm{x}, \mathrm{y} > | x \in A \land y \in B\}$

Set Identities（集合恒等式）

Identity laws (同一律)

$$A \cap U = A$$
$$A \cup \varnothing = A$$

Commutative laws (交换律)

$$A \cup B = B \cup A$$
$$A \cap B = B \cap A$$

Domination laws (零律)

$$A \cup U = U$$
$$A \cap \varnothing = \varnothing$$

Associative laws (结合律)

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

Idempotent laws (幂等律)

$$A \cup A = A$$
$$A \cap A = A$$

Distributive laws (分配律)

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

Set Identities

Complementation law (双补律)

$$\overline{(\overline{A})} = A$$

Complement laws (补余律)

$$A \cup \overline{A} = U$$
$$A \cap \overline{A} = \varnothing$$

Absorption laws (吸收律)

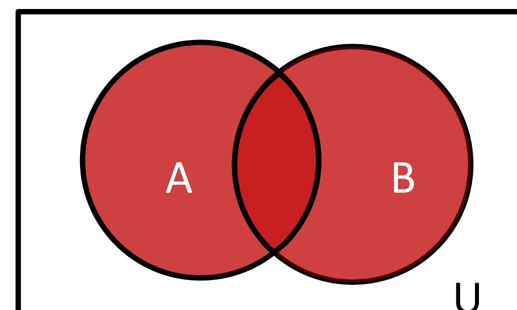
$$A \cup (A \cap B) = A$$
$$A \cap (A \cup B) = A$$

De Morgan's laws (摩根律)

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

Cardinality of finite set

- The cardinality of a set is the number of elements it contains.
- If $|A|$ is a set, we denote its cardinality by writing $|A|$ or $card(A)$
- Only finite set’ s cardinality is a specific number
- $|A_1 \cup A_2| \leq |A_1| + |A_2|$
- $|A_1 \cap A_2| \leq \min(|A_1|, |A_2|)$
- $|A_1 - A_2| \geq |A_1| - |A_2|$
- $|A_1 \oplus A_2| = |A_1| + |A_2| - 2|A_1 \cap A_2|$
- $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$
- $|\mathcal{P}(A)| = 2^n = 2^{|A|}$



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

Principle of Inclusion and Exclusion(容斥定理)

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{n-1} |A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n|$$

n=2: $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

n=3: $|A_1 \cup A_2 \cup A_3| =$

$$|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

ZF Axiom System

- ZF.1 Axiom of extensionality（外延公理）
- ZF.2 Axiom of the empty set （空集合存在公理）
- ZF.3 Axiom of pairing （无序对集合存在公理）
- ZF.4 Axiom of union （并集合公理）
- ZF.5 Subset axiom schema(子集公理模式)
- ZF.6 Axiom of power set （幂集合公理）
- ZF.7 Axiom of regularity (正则公理)
- ZF.8 Axiom of infinity（无穷公理）
- ZF.9 Axiom of replacement （替换公理）
- ZF.10 Axiom of choice（选择公理）

Binary Relations

- **Binary Relation Basics**
- **Equivalence Relation and Partitions**
  – Reflexivity, Symmetry and Transitivity.
- **Compatible Relation and Covers**
  – Reflexivity and Symmetry
- **Partial Order Relation**
  – Reflexivity, Anti-symmetry and Transitivity
- **Closure**

Binary Relation

- a binary relation(二元关系) from $\boldsymbol{A}$ to $\boldsymbol{B}$ is a set $\boldsymbol{R}$ of **ordered pairs**, where the first element of each ordered pair comes from $\boldsymbol{A}$ and the second element comes from $\boldsymbol{B}$.
  - domain(定义域), range(值域), field(域)
- Representation:
  - Relation Matrix(关系矩阵), Digraphs(关系图)

Special Relations

- For any set $\boldsymbol{A}$, there are three kinds of special relations.
  - The identity relation （恒等关系）：
$$\boldsymbol{I_A} = \{\langle \boldsymbol{x}, \boldsymbol{x} \rangle | \boldsymbol{x} \in \boldsymbol{A}\}$$
  - The universal relation （全域关系）：
$$\boldsymbol{E_A} = \{\langle \boldsymbol{x}, \boldsymbol{y} \rangle | \boldsymbol{x} \in \boldsymbol{A} \wedge \boldsymbol{y} \in \boldsymbol{A}\}$$
  - The empty relation （空关系）：
$$\boldsymbol{N_A} = \emptyset$$
- For arbitrary elements $\boldsymbol{x} \in \boldsymbol{A}$ and $\boldsymbol{y} \in \boldsymbol{A}$:
  - xN_Ay holds never
  - xE_Ay holds always
  - xI_Ay holds if and only if $x = y$

Inverse of Relations （关系的逆）

Defination

Let R be a relation from a set A to a set B.The inverse relation of R, denoted by R^{-1}, is the set of ordered pairs $\{\langle b,a\rangle | \langle a,b\rangle \in R\}$ from B to A

Let $A = \{a,b,c\}$, a relation on A, $R = \{\langle a,b\rangle, \langle a,c\rangle, \langle b,a\rangle, \langle c,b\rangle\}$, then:

$$R^{-1} = \{\langle b,a\rangle, \langle c,a\rangle, \langle a,b\rangle, \langle b,c\rangle\}$$

Composite of Relations （关系的合成）

Definition

Let R be a relation from A to B, and S be a relation from B to C. The composite of R and S, donate as $S \circ R$, is:

$$S \circ R = \{\langle x, y\rangle | (\exists z)(\langle x, z\rangle \in R \wedge \langle z, y\rangle \in S)\}$$

Let $A = \{1, 2, 3\}$,two relations on A,
$R = \{\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$,$S = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 3, 1\rangle, \langle 3, 3\rangle\}$

Then $S \circ R = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 1, 3\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle\}$

Power of Relations （关系的幂）

- For a relation R on set A, $n \in \mathbb{N}$, the nth power of R, donated by R^n, is :
  - $R^0 = I_A$
  - $R^{n+1} = R^n \circ R$
- $R = \{\langle a, b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, d\rangle\}$
  - $R^0 = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, \langle d, d\rangle\}$
  - $R^1 = R = \{\langle a, b\rangle, \langle b, a\rangle, \langle b, c\rangle, \langle c, d\rangle\}$
  - $R^2 = R^4 = \{\langle a, a\rangle, \langle a, c\rangle, \langle b, b\rangle, (b, d)\}$
  - $R^3 = R^5 = \{\langle a, b\rangle, \langle a, d\rangle, \langle b, a\rangle, \langle b, c\rangle\}$

Reflexivity(自反性)

- Some relations always hold from any element to itself.
- Examples:
  - $\boldsymbol{x} = \boldsymbol{x}$ for any x
  - $\boldsymbol{A} \subseteq \boldsymbol{A}$ for any set A
  - $\boldsymbol{x} \geq \boldsymbol{x}$ for any x
- Relations of this sort are called reflexive.

R on A is reflexive $\Leftrightarrow (\forall \boldsymbol{a})(\boldsymbol{a} \in \boldsymbol{A} \rightarrow \boldsymbol{aRa})$

Symmetry(对称性)

- In some relations, the relative order of the objects doesn't matter.
- Examples:
  - If $x = y$ then $y = x$
  - If $x \equiv_k y$ then $y \equiv_k x$
- These relations are called symmetric.

$$R \text{ on } A \text{ is symmetric} \Leftrightarrow$$
$$(\forall a)(\forall b)((a \in A \wedge b \in A \wedge aRb) \rightarrow bRa)$$

Anti-symmetry(反对称性)

- Some relation is symmetric only in its diagonal.
- Examples:
  - If $\boldsymbol{x} \le \boldsymbol{y}$ and $\boldsymbol{y} \le \boldsymbol{x}$,then $\boldsymbol{x} = \boldsymbol{y}$
  - If $\boldsymbol{A} \subseteq \boldsymbol{B}$ and $\boldsymbol{B} \subseteq \boldsymbol{A}$, then $\boldsymbol{A} = \boldsymbol{B}$
- Relations of this sort are called antisymmetric.

$$\boldsymbol{R} \text{ on } \boldsymbol{A} \text{ is antisymmetric} \Leftrightarrow$$
$$(\forall \boldsymbol{a})(\forall \boldsymbol{b})((\boldsymbol{a} \in \boldsymbol{A} \wedge \boldsymbol{b} \in \boldsymbol{A} \wedge \boldsymbol{aRb} \wedge \boldsymbol{bRa}) \to \boldsymbol{a} = \boldsymbol{b})$$

Transitivity(传递性)

- Many relations can be chained together.
- Examples:
  - If $x = y$ and $y = z$ then $x = z$
  - If $P \subseteq Q$ and $Q \subseteq S$, then $P \subseteq S$
  - If $x \equiv_k y$ and $y \equiv_k z$, then $x \equiv_k z$
- These relations are called transitive.

$$R \text{ on } A \text{ is transitive} \Leftrightarrow$$
$$(\forall a)(\forall b)(\forall c)\big((a \in A \wedge b \in A \wedge c \in A \wedge aRb \wedge bRc) \rightarrow aRc\big)$$

Equivalence Relations(等价关系)

- An **equivalence relation** is a relation that is **reflexive, symmetric and transitive**.
- Some examples:
  - $x = y$
  - $x \equiv_k y$
  - x has the same color with y
  - x has the same shape with y

Partitions(划分)

- A **partition of a set** is a way of splitting the set into **disjoint, nonempty subsets** so that every element belongs to exactly one subset.
- Intuitively, a partition of a set breaks the set apart into smaller pieces.

Quotient Set(商集)

- Given an equivalence relation $\boldsymbol{R}$ over a set $\boldsymbol{A}$, the quotient set of $\boldsymbol{A}$ is set of all the disjoint equivalence classes of $\boldsymbol{A}$, donated by $\boldsymbol{A}/\boldsymbol{R}$**:**

$$\boldsymbol{A}/\boldsymbol{R} = \{\boldsymbol{y}|(\exists\boldsymbol{x})(\boldsymbol{x} \in \boldsymbol{A} \wedge \boldsymbol{y} = [\boldsymbol{x}]_{\boldsymbol{R}})\}$$

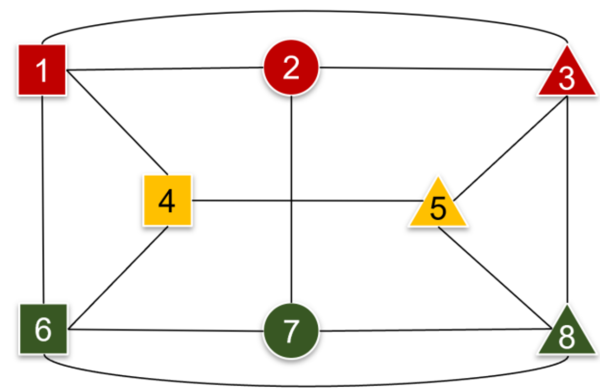
- For $\boldsymbol{R} = \{\langle x, y\rangle | x \equiv_3 y\}$ on set $\boldsymbol{A} = \{1,2,3 \dots 8\}$
  - $\boldsymbol{A}/\boldsymbol{R} = \{[1]_{\boldsymbol{R}}, [2]_{\boldsymbol{R}}, [3]_{\boldsymbol{R}}\} = \{\{1,4,7\}, \{2,5,8\}, \{3,6\}\}$

Compatible Relations (相容关系)

- An **compatible relation** is a relation that is **reflexive and symmetric**.
- Some examples:
  - x has at least one same letter with y
  - $x \cap y \neq \emptyset$
  - x has same color or same shape with y

Maximal Compatible Class(极大相容类)

- Given a compatible relation A, C is called **compatible class (相容类)** if:
  - $C \subseteq A$
  - $(x \in A) \wedge (\forall y)((y \in C) \rightarrow xRy)$
- A compatible class C is called **maximal compatible class** if C is not the subset of any compatible class, donate by C_R.



Covers(覆盖)

- A **cover of a set** is a way of splitting the set into **nonempty subsets** so that every element belongs to at least one subset.
- Intuitively, a cover contains pieces that cover every element of a set.
- **A partition is a cover, but a cover is not a partition.**

Compatible Relation and Covers

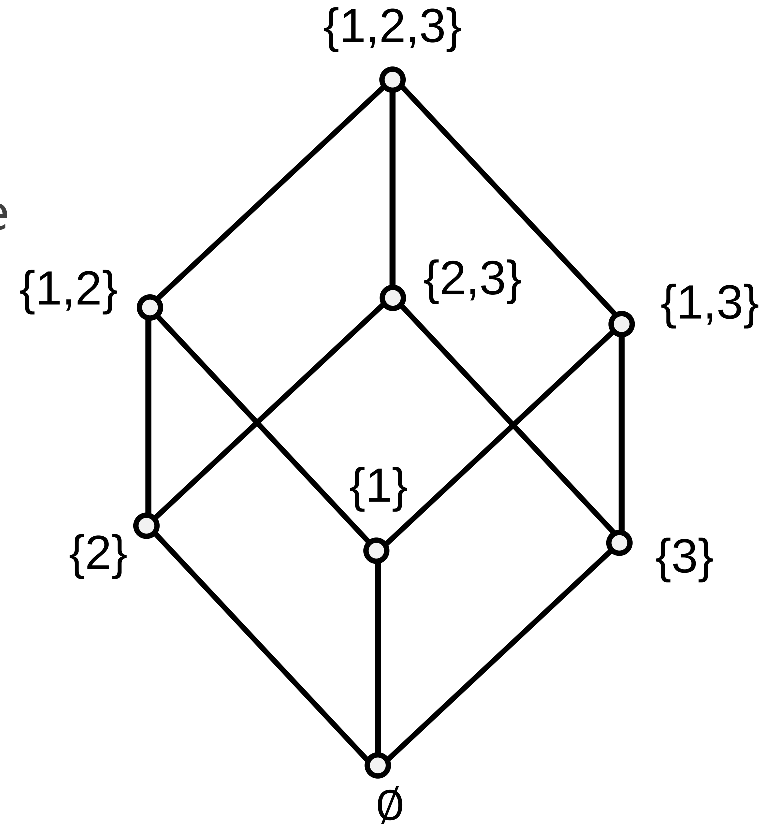
- Given a compatible relation $\boldsymbol{R}$ on a set $\boldsymbol{A}$, the set of all maximal compatible classes is a cover of $\boldsymbol{A}$, called the complete cover (完全覆盖) of $\boldsymbol{A}$, donate by $\boldsymbol{C_R(A)}$.
  - $C_R(A)$ is unique.
- A compatible relation of $\boldsymbol{A}$ can generate a complete cover of $\boldsymbol{A}$
- A cover of $\boldsymbol{A}$ can generate a compatible relation of $\boldsymbol{A}$
- Two different covers can generate the same compatible relation.

Partial-order Relation(偏序关系)

- An **partial-order relation** is a relation that is **reflexive, anti-symmetric and transitive**.
- Some example:
  - $x \leq y$
  - $x \subseteq y$
  - x can be divided by y (on $\mathbb{N}^+$)
- A set $\boldsymbol{A}$ together with a partial ordering $\boldsymbol{R}$ is called a partially ordered set, or poset(偏序集), and is denoted by $\langle \boldsymbol{A}, \boldsymbol{R} \rangle$.
  - $\langle \mathbb{N}, \leq \rangle$,$\langle \mathcal{P}(A), \subseteq \rangle$ are both poset.

Hasse Diagram(哈斯图)

- For poset $\langle A, \leq \rangle$:
  - Every vertex is an element
  - If $x \leq y \wedge x \neq y$, then vertex y is above vertex x
  - If $\langle x, y \rangle \in cov(A)$, then there's an undirected edge between x and y



Quasi-order Relation(拟序关系)

- An **quasi-order relation, or strict order relation** is a relation that is **anti-reflexive, transitive**.
- Some example:
  - $x < y$
  - $x \subset y$
  - x is taller than y

Maximal(最大) and Maximum(极大) Elements

- For a poset $\langle A, \leq \rangle$, and $B \subseteq A$:
  - If there exists $y \in B$ such that $\forall x \in B$, $x \leq y$, we call y the **maximum** elements(最大元) of B

$$y\ is\ maximum \Leftrightarrow y \in B \wedge (\forall x)(x \in B \rightarrow x \leq y)$$

  - If there exists $y \in B$ such that $\forall x \in B$, if $y \leq x$, then $x = y$. We call y the **maximal** elements(极大元) of B

$$y\ is\ maximal \Leftrightarrow y \in B \wedge (\forall x)((x \in B \wedge y \leq x) \rightarrow x = y)$$

Minimum(最小) and Minimal(极小) Elements

- For a poset $\langle A, \leq \rangle$, and $B \subseteq A$:
  - If there exists $x \in B$ such that $\forall y \in B$, $x \leq y$, we call x the **minimum** elements(最小元) of B

$$x\ is\ minimum \Leftrightarrow x \in B \wedge (\forall y)(y \in B \rightarrow x \leq y)$$

  - If there exists $x \in B$ such that $\forall y \in B$, if $y \leq x$, then $x = y$. We call x the **minimal** elements(极小元) of B

$$x\ is\ minimal \Leftrightarrow x \in B \wedge (\forall y)((y \in B \wedge y \leq x) \rightarrow x = y)$$

Upper Bound(上界) and Supremum(上确界)

- For a poset $\langle \boldsymbol{A}, \leq \rangle$, and $\boldsymbol{B} \subseteq \boldsymbol{A}$:
  - If there exists $\boldsymbol{y} \in \boldsymbol{A}$ such that $\forall \boldsymbol{x} \in \boldsymbol{B}$, $\boldsymbol{x} \leq \boldsymbol{y}$, we call $\boldsymbol{y}$ the **upper bound（上界）** of $\boldsymbol{B}$

    $$\boldsymbol{y\ is\ upper\ bound} \Leftrightarrow \boldsymbol{y} \in \boldsymbol{A} \wedge (\forall \boldsymbol{x})(\boldsymbol{x} \in \boldsymbol{B} \rightarrow \boldsymbol{x} \leq \boldsymbol{y})$$

  - Let $\boldsymbol{C} = \{\boldsymbol{y} |\ \boldsymbol{y}\ is\ the\ upper\ bound\ of\ \boldsymbol{B}\}$, then the minimum elements in $\boldsymbol{C}$ is the **supremum（上确界）** of $\boldsymbol{B}$.

Lower Bound(下界) and Infimum(下确界)

- For a poset $\langle \boldsymbol{A}, \leq \rangle$, and $\boldsymbol{B} \subseteq \boldsymbol{A}$:
  - If there exists $\boldsymbol{x} \in \boldsymbol{A}$ such that $\forall \boldsymbol{y} \in \boldsymbol{B}$, $\boldsymbol{x} \leq \boldsymbol{y}$, we call $\boldsymbol{x}$ the **lower bound（下界）** of $\boldsymbol{B}$

$$\boldsymbol{x\ is\ lower\ bound} \Leftrightarrow \boldsymbol{x} \in \boldsymbol{A} \wedge (\forall \boldsymbol{y})(\boldsymbol{y} \in \boldsymbol{B} \rightarrow \boldsymbol{x} \leq \boldsymbol{y})$$

  - Let $\boldsymbol{C} = \{\boldsymbol{x} |\ \boldsymbol{x}\ is\ the\ lower\ bound\ of\ \boldsymbol{B}\}$, then the maximum elements in C is the **infimum（下确界）** of $\boldsymbol{B}$.

Total Order Relation(全序关系)

- For a poset $\langle \boldsymbol{A}, \leq \rangle$:
  - For any $\boldsymbol{x} \in \boldsymbol{A}$ and $\boldsymbol{y} \in \boldsymbol{A}$, if $\boldsymbol{x} \leq \boldsymbol{y}$ **or** $\boldsymbol{y} \leq \boldsymbol{x}$ **,** then we call $\boldsymbol{x}$ and $\boldsymbol{y}$ are comparable.
  - If for any $\boldsymbol{x} \in \boldsymbol{A}$ and $\boldsymbol{y} \in \boldsymbol{A}$, we have x and y are comparable, then we called $\leq$ is a **total order relation** on $\boldsymbol{A}$, $\langle \boldsymbol{A}, \leq \rangle$ is a total order set.
- $\langle \mathbb{N}, \leq \rangle$ is a total order set
- For a non-empty set $\boldsymbol{A}$, $\langle \boldsymbol{\mathcal{P}}(\boldsymbol{A}), \subseteq \rangle$ is not a total order set.

Chain(链) and Anti-chain(反链)

- For a poset $\langle A, \leq \rangle$, $B \subseteq A$:
  - For any $x \in B$ and $y \in B$, if x and y are **comparable**, we call B is a **chain** on A, $|B|$ is the length of this chain.
  - For any $x \in B$ and $y \in B$, if x and y are **not comparable**, we call B is an **anti-chain** on A, $|B|$ is the length of this anti-chain.

Well Order Relation(良序关系)

- For a poset $\langle A, \leq \rangle$, if any non-empty subset of A has the minimal elements（极小元）, then we call $\leq$ is a **well order relation**, $\langle A, \leq \rangle$ is a well order set.
- $\langle \mathbb{N}, \leq \rangle$ is a well order set. $\langle \mathbb{Z}, \leq \rangle$ is not a well order set.

Closure(闭包)

- 自反闭包，对称闭包，传递闭包
- For a relation $\boldsymbol{R}$ on non-empty set $\boldsymbol{A}$, if there are another relation R' such that:
  - $\boldsymbol{R}'$ is **reflexive (symmetric, transitive)**
  - $\boldsymbol{R} \subseteq \boldsymbol{R}'$.
  - For any **reflexive (symmetric, transitive)** relation R'' on $\boldsymbol{A}$, $\boldsymbol{R} \subseteq \boldsymbol{R}'' \to \boldsymbol{R}' \subseteq \boldsymbol{R}''$.
- We call that $\boldsymbol{R}'$ is the **reflexive (symmetric, transitive)** closure of $\boldsymbol{R}$, donated by $\boldsymbol{r(R)}$ **(** $\boldsymbol{s(R)}$ **,** $\boldsymbol{t(R)}$ **)**

Constructing Closure

For a relation $\boldsymbol{R}$ on non-empty set $\boldsymbol{A}$, $\boldsymbol{r}(\boldsymbol{R}) = \boldsymbol{R} \cup \boldsymbol{R}^{\mathbf{0}}$

For a relation $\boldsymbol{R}$ on non-empty set $\boldsymbol{A}$, $\boldsymbol{s}(\boldsymbol{R}) = \boldsymbol{R} \cup \boldsymbol{R}^{-\mathbf{1}}$

For a relation $\boldsymbol{R}$ on non-empty set $\boldsymbol{A}$, $|\boldsymbol{A}| = n$,
$\boldsymbol{t}(\boldsymbol{R}) = \boldsymbol{R} \cup \boldsymbol{R}^{\mathbf{2}} \cdots \cup \boldsymbol{R}^{\boldsymbol{n}}$

Transitive Closure: Warshall Algorithm

- Warshall Algorithm is an efficient algorithm to calculate transitive closure

```
Warshall_Algorithm(M[1…n,1…n]):
  M⁰ ← M
  for i ← 1 to n:
    for j ← 1 to n:
      if Mⁱ⁻¹[j,i]==1:
        for k ← 1 to n:
          Mⁱ[j,k] = Mⁱ⁻¹[j,k]∨ Mⁱ⁻¹[i,k]
  return Mⁿ
```

Function

- **Definition and common functions**
- **Injective, surjective, bijective.**
- **Inverse of function.**

Function

- A relation f from set $\boldsymbol{A}$ to set $\boldsymbol{B}$ is called a function if:
  - For any $\boldsymbol{x} \in dom(f)$, there exists ***unique*** $\boldsymbol{y}$ such that $\boldsymbol{xfy}$
$$(\forall \boldsymbol{x})(\forall \boldsymbol{y_1})(\forall \boldsymbol{y_2})((\boldsymbol{xfy_1} \wedge \boldsymbol{xfy_2}) \rightarrow \boldsymbol{y_1} = \boldsymbol{y_2})$$
  - $dom(f) = \boldsymbol{A}$
$$(\forall \boldsymbol{x})(\boldsymbol{x} \in \boldsymbol{A} \rightarrow (\exists \boldsymbol{y})(\boldsymbol{y} \in \boldsymbol{B} \wedge \boldsymbol{xfy}))$$
- A function f from set $\boldsymbol{A}$ to set $\boldsymbol{B}$ is donated as $f\colon \boldsymbol{A} \rightarrow \boldsymbol{B}$.
- $\boldsymbol{xfy}$ writing as $f\colon \boldsymbol{x}| \rightarrow \boldsymbol{y}$ or $f(\boldsymbol{x}) = \boldsymbol{y}$

Function

- For relation $\boldsymbol{R}$ on $\boldsymbol{A}$, for a set $\boldsymbol{B}$
  - The **image** (象) of R on B , donate as $R[B]$ is:
    $$R[B] = \{y | \exists x(\langle x, y\rangle \in R \land x \in B)\}$$
- Similarly for a function $f: \boldsymbol{A} \to \boldsymbol{B}$, $\forall \boldsymbol{A_1} \subseteq \boldsymbol{A}$ we can define $f[A_1]$ to be the **image**(象) of A_1 on function f**.**
- $\forall B_1 \subseteq B$, $f^{-1}[B_1]$ is the **inverse image or preimage**(原象) of B_1 on f.

Injection(单射)

- $f: A \to B$ is an **injection** or **injective** if for any $x_1, x_2 \in A, x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

$$(\forall x_1)(\forall x_2)(x_1 \in A \wedge x_2 \in A \wedge x_1 \neq x_2 \to f(x_1) \neq f(x_2))$$

Different inputs has different outputs

- Or if $f(x_1) = f(x_2)$, then $x_1 = x_2$

$$(\forall x_1)(\forall x_2)(x_1 \in A \wedge x_2 \in A \wedge f(x_1) = f(x_2) \to x_1 = x_2)$$

Same outputs have the same input

Surjection(满射)

- $f: A \to B$ is a **surjection** or **surjective** if $ran(f) = B$, or for any $y \in B$, there exists $x \in \mathrm{A}$ such that $f(x) = B$

$$(\forall y)(\exists x)\big(y \in B \to (x \in A \land f(x) = y)\big)$$

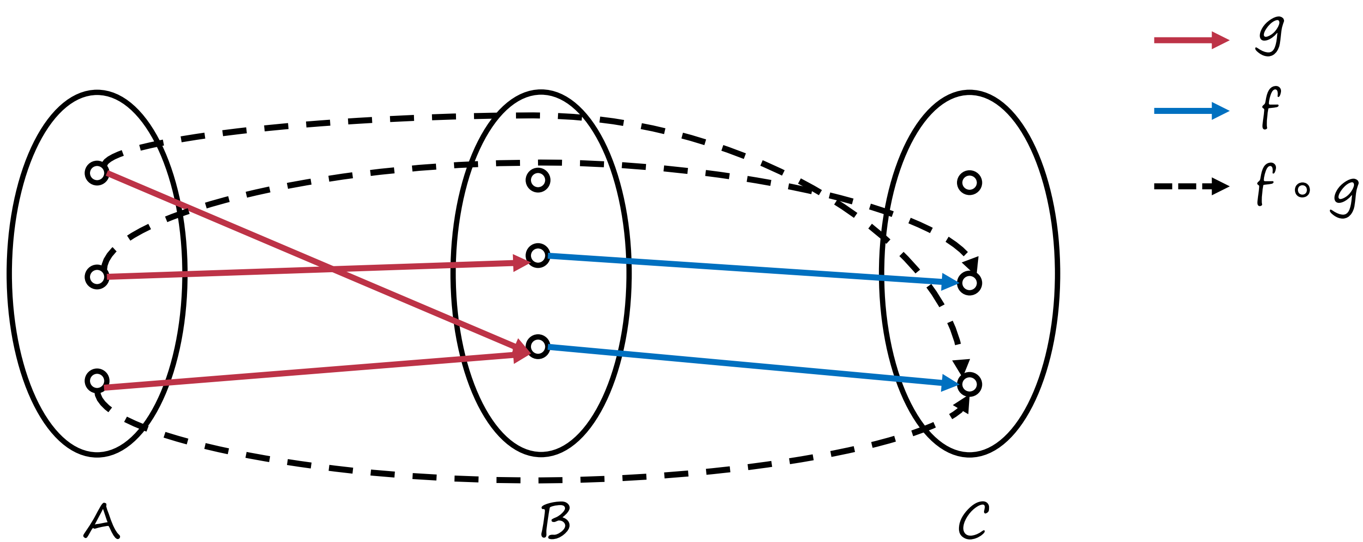
Every possible output has an input

Bijection(双射)

- $f: A \to B$ is a **bijection** or **bijective** if f is **both** injective and surjective.
- Bijections are sometimes called **one-to-one correspondences(一一对应)**.

Compose of Function

- Let $g: \boldsymbol{A} \to \boldsymbol{B}$, $f: \boldsymbol{B} \to \boldsymbol{C}$, then:
  - $f \circ g$ is a function $f \circ g: \boldsymbol{A} \to \boldsymbol{C}$
  - For any $x \in A$, $(f \circ g)(x) = f(g(x))$



Inverse of Function

- Let $f: \boldsymbol{A} \to \boldsymbol{B}$
  - The inverse (defined by relation) of f may not be a function
  - If the inverse of f is a function, we call f is **inversible** （可逆的）

$f: A \to B$, if there exists $g: B \to A$, such that $g \circ f = I_A$ and $f \circ g = I_B$, we call that f is **inversible**, and g is the **inverse function(反函数)** of f.

Some times g∘ f=I_A and f∘g=I_B may not hold simultaneously.

f is inversible if and only if f is bijective.

Left Inverse(左逆) and Right Inverse(右逆)

- Let $f: \boldsymbol{A} \to \boldsymbol{B}$, if there exists $g: \boldsymbol{B} \to \boldsymbol{A}$, such that
  - $g \circ f = I_A$, then we call g is the **left inverse** of f.
  - $f \circ g = I_B$, then we call g is the **right inverse** of f.