Introduction to Mathematical Logic

For CS Students

CS104

Yida TAO (陶伊达)

2025 年 2 月 27 日

Before we dive into propositional logic and first-order logic, let's briefly discuss the prerequisite knowledge: set, relation, function, and mathematical proof.

Table of Contents

What is Set?

A Set (集合) is a collection of objects

- S: students in our class
- E: even numbers
- $\mathbb{N}$: natural numbers

Elements of Sets

An object in the set is called element of the set (集合的元素)

- S: students in our class: Tom $\in$ S
- E: even numbers: $2 \in E$, $3 \notin E$
- $\mathbb{N}$: natural numbers: $1 \in \mathbb{N}$, $\pi \notin \mathbb{N}$

Set cardinality: the number of elements in a set, denoted as $|A|$.

How do we formally (precisely) define a set?

Defining a Set

A set can be defined by:

- Extension (外延): define by listing all elements
- Intension (内涵): define by common characteristics

Example: E = Even numbers

- **Extension** of E: $2, 4, 6, 8, 10, \ldots\ldots$
- **Intension** of E: any number that is divisible by 2

Defining a Set

What about these infinite set?

- The set of valid algebra expressions over variables x, y, z? (e.g., $x + y - z$)
- The set of valid Java programs?

Definition

1 Set

If $\varphi(x)$ represents a property (common characteristics), then $\{x \mid \varphi(x)\}$ denotes the set of all elements that have this property.

What's the set R?

- $R = \{x \mid x \neq x\}$?
- $R = \{X \mid X \notin X\}$?

Definition

Axiom of Extension

The two sets A and B are equal ($A = B$) if and only if A and B have the same members.

Example: A and B are the same set:

- $A = \{x \in \mathbb{R} : x + y = y\}$ for every real number y
- $B = \{x \in \mathbb{R} : x \times z = x\}$ for every real number z

Order doesn't matter: $\{a, b, c\} = \{c, b, a\}$

Subset

- A set A is a subset of a set B if all elements of A are also elements of B.
- Formally, $A \subseteq B$ iff for any x, if $x \in A$, then $x \in B$.
  - $\{$Aristotle, Russell$\} \subseteq \{x \mid \text{x is human}\}$
  - $\{x \mid \text{x is a prime number}\} \not\subseteq \{x \mid \text{x is an odd number}\}$
- For any set A, we have $\varnothing \subseteq A$ and $A \subseteq A$.

Proper Subset (真子集)

- If $A \subseteq B$ and $A \neq B$ (i.e. there exists at least one element of B which is not an element of A), then A is a proper (or strict) subset of B, denoted by $A \subset B$.
- $\varnothing$ (empty set, or $\{\}$) is a proper subset of any set except itself.

Power Set (幂集)

If A is a set, then $\{X \mid X \subseteq A\}$ is the power set of A (the set of all subsets of A), i.e., $\mathcal{P}(A)$.

- $\mathcal{P}(\{a, b, c\}) =?$
- $\mathcal{P}(\varnothing) =?$
- $\mathcal{P}(\{\varnothing\}) =?$

- $A \cup B$ denotes the union (并集) of set A and B: $\{x \mid x \in A \ or \ x \in B\}$
- $A \cap B$ denotes the intersection (交集) of set A and B: $\{x \mid x \in A \ and \ x \in B\}$
- $A - B$ denotes the difference (差集) of set A and B: $\{x \mid x \in A \ and \ x \notin B\}$

Set Operations

W is a collection of set.

$\bigcap W \stackrel{\text{def}}{=} \{x \mid \forall B \in W, x \in B\}$.

Let $W = \{(-r, r) \mid r > 0, r \in \mathbb{R}\}$.

What is $\bigcap W$?

Table of Contents

2 Relation

Why do we need relation?

Which **structure** can we build with a **set** of bricks?

- A wall
- A tower
- A bridge
- ......

Depending on the **relations** of bricks, the structure is different.

Why do we need relation?

Mathematical structures are defined with sets, plus various relations (e.g., $<$) and functions (e.g., $+$).

- $(\mathbb{N}, <) : 0 < 1 < 2 < 3 < \ldots$
- $(\mathbb{N}, \prec) : \ldots \prec 6 \prec 4 \prec 2 \prec 0 \prec 1 \prec \ldots$

Both structures are constructed with set $\mathbb{N}$, but they are different structures (e.g., the first structure has a minimum element while the second doesn't)

n-tuples (有序 n 元组)

In mathematics, a *tuple* is a finite sequence or ordered list of numbers.

An *n-tuple* is a tuple of n elements, where n is a non-negative integer.

Properties of n-tuples

A tuple has properties that distinguish it from a set:

- A tuple may contain multiple instances of the same element, e.g., $\langle 1, 2, 2, 3 \rangle \neq \langle 1, 2, 3 \rangle$
- Tuple elements are ordered, e.g., $\langle 1, 2, 3 \rangle \neq \langle 3, 2, 1 \rangle$
- A tuple has a finite number of elements while a set may not.

The general rule for the identity of two n-tuples:

$$\langle x_1, x_2, \ldots, x_m \rangle = \langle y_1, y_2, \ldots, y_n \rangle \text{ iff } m = n \text{ and } x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$$

$A \times B$ denotes the Cartesian product (笛卡尔积) of set A and B (the set of all ordered pairs where x is in A and y is in B.)

$$A \times B = \{\langle x, y \rangle \mid x \in A \text{ and } y \in B\}$$

A binary relation R over sets X and Y is a subset of Cartesian product $A \times B$, denoted as $R \subseteq A \times B$.
Intuitively, a binary relation from a set X to a set Y is a set of ordered pairs $\langle x, y \rangle$ where x is an element of X and y is an element of Y.

Binary Relation

The statement $\langle x, y \rangle \in R$ reads "x is R-related to y", and is denoted by $R(x, y)$ or xRy.

When $X = Y$, we call a relation R from X to Y a (binary) relation over X.
(R 是 X 中的一个二元关系).

Examples

- $\{\langle x, y \rangle \mid x$ is y's father$\}$ is a binary relation over the set $\{$x | x is human$\}$
- $\{\langle x, y \rangle \mid x$ is y's spouse$\}$ is a binary relation over the set $\{$x | x is married$\}$
- $<$ is a binary relation over $\mathbb{N}, \mathbb{Z}, \mathbb{R}$

n-ary relation

Cartesian product of sets $A_1, A_2, ..., A_n (n \geq 1)$:

$$A_1 \times A_2 \times ... \times A_n = \{\langle x_1, x_2, ..., x_n \rangle \mid x_1 \in A_1, x_2 \in A_2, ..., x_n \in A_n\}$$

Denoted as A^n if $A_1 = A_2 = ... = A_n = A$.

If $R \subseteq A^n$, R is denoted as an *n-ary* relation over A.

Which n-ary relations do we have in a scenario of course enrollment?

1. **Unary relation** $(n = 1)$
A unary relation involves only one entity type, can be viewed as an adjective describing the elements of the set (i.e., the property of elements).
   - $\mathit{EnrolledStudent}(\mathit{StudentID})$: The set of students who are currently enrolled.
   - $\mathit{ActiveCourse}(\mathit{CourseID})$: The set of courses that are currently being offered.

Which n-ary relations do we have in a scenario of course enrollment?

2. **Binary relation** ($n = 2$)
   - $Enrollment(StudentID, CourseID)$
   - $Prerequisite(CourseID1, CourseID2)$
   - $Teaches(ProfessorID, CourseID)$
3. **Ternary relation** ($n = 3$)
   - $ProjectGroup(StudentID, CourseID, GroupID)$: Represents that a student is part of a specific project group within a course.

Equivalence Relation

Let R be a binary relation on a set A.

- R is **reflexive**(自反) if for all $x \in A$, xRx.
- R is **symmetric**(对称) if for all $x, y \in A$, if xRy, then yRx.
- R is **transitive**(传递) if for all $x, y, z \in A$, if xRy and yRz, then xRz.

R is an equivalence relation (等价关系) on A if A is nonempty and R is reflexive, symmetric and transitive.

Equivalence Relation

- "=" is an equivalence relation on $\mathbb{N}$
- $\{\langle x, y\rangle \mid$ x and y have the same birthday$\}$ is an equivalence relation on $\{x \mid x$ is human$\}$.
- $\{\langle x, y\rangle \mid$ x is parallel to y$\}$ is an equivalence relation on the set of lines in a plane.

Equivalence Class

Given an equivalence relation R over a set A, for any $x \in A$, the equivalence class(等价类) of x is the set

$$[x]_R = \{y \in A \mid xRy\}$$

$[x]_R$ is the set of all elements of A that are equivalent to x.

Equivalence Class

Key properties:

- Every element belongs to exactly one equivalence class.
- Different equivalence classes are disjoint.
- The set of all equivalence classes forms a partition of A (集合的划分).

Examples:

- “being born in the same year” on the set of human beings
- “has the same suit/rank” on the set of standard 52 cards
- “has the same number of vertices” on the set of polygons.

Equivalence Class

Example: Define a relation R “congruence modulo 4” (模 4 同余) on $\mathbb{Z}$:

$$aRb \Leftrightarrow a \equiv b \pmod{4}$$

Find the equivalence classes of R.

Two integers will be related by R if they have the same remainder after dividing by 4. The possible remainders are $0, 1, 2, 3$. So the equivalence classes are:

$$
\begin{aligned}
[0]_R &= \{n \in \mathbb{Z} \mid n \bmod 4 = 0\} = 4\mathbb{Z} \\
[1]_R &= \{n \in \mathbb{Z} \mid n \bmod 4 = 1\} = 4\mathbb{Z} + 1 \\
[2]_R &= \{n \in \mathbb{Z} \mid n \bmod 4 = 2\} = 4\mathbb{Z} + 2 \\
[3]_R &= \{n \in \mathbb{Z} \mid n \bmod 4 = 3\} = 4\mathbb{Z} + 3
\end{aligned}
$$

Every integer belongs to exactly one of these four sets, which are disjoint. They form a partition of $\mathbb{Z}$: $\mathbb{Z} = [0]_R \cup [1]_R \cup [2]_R \cup [3]_R$.

Partial Order Relation (偏序关系)

- A binary relation R on a set A is antisymmetric (反对称的) if for all $x, y \in A$, if xRy and yRx, then $x = y$.
- A binary relation R on a set A is a partial order (偏序关系) if R is reflexive, antisymmetric, and transitive.
- For $x \in A$, if there doesn't exist another $y \in A$ such that yRx, then x is the minimal element (极小元) of this partial order.
- For $x \in A$, if there doesn't exist another $y \in A$ such that xRy, then x is the maximal element (极大元) of this partial order.

Examples:

- The relation $\leq$ is a partial order on $\mathbb{N}$. 0 is the minimal element, no maximal element.
- The binary relation "x is divisible by y" on the set of positive integers is a partial order. It has no minimal elements, and 1 is a maximal element.
- $\subseteq$ is a partial order on $\mathcal{P}(\mathbb{N})$, $\varnothing$ is the minimal element, $\mathbb{N}$ is the maximal element.

Total Order Relation (全序关系)

Formally, a partial order relation R on a set A is a total order (linear order), if for any $x, y \in A$, either xRy or yRx.

Intuitively, a total order or linear order is a partial order in which **any two elements are comparable**.

Total Order Relation

Are these partial order relations also total order relations?

- The relation $\leq$ is a partial order on $\mathbb{N}$. 0 is the minimal element, no maximal element.
- The binary relation "x is divisible by y" on the set of positive integers is a partial order. It has no minimal elements, and 1 is a maximal element.
- $\subseteq$ is a partial order on $\mathcal{P}(\mathbb{N})$, $\varnothing$ is the minimal element, $\mathbb{N}$ is the maximal element.

Table of Contents

Why Functions?

A binary relation typically allows “one-to-many” relations. For example, for the $<$ relation on $\mathbb{R}$, 0 is related to all positive real numbers。

However, this “one-to-many” situation must be excluded in many cases:

- x’s mother is y.
- x and x^2.
- Computer keyboard input and screen output.

Definition

A function from a set X to a set Y is a binary relation R between X and Y that satisfies the two following conditions:

- For any $x \in X$, there exists $y \in Y$ such that xRy.
- If $y, z \in Y$ such that xRy and xRz, then $y = z$.

A function from a set X to a set Y assigns to each element of X exactly one element of Y.

We typically use f, g, h to represent functions. The notation

$$f : A \to B$$

expresses that f is a function from set A to a subset of set B.

- The *domain* (定义域) of f: the set of input values
- The *codomain*（陪域、上域）of f: the set of **possible** output values
- The *range* (值域) of f: the set of **actual** output values, i.e., a subset of the B
- We typically use $f(x) = y$ to denote $\langle x, y \rangle \in f$.

Example

When a professor reports the final letter grades for the students in her class, we can regard this as a function g:

- Domain: the set of students in the class
- Codomain: $\{A, B, C, D, F\}$
- Range: $\{A, B, C\}$

n-ary function

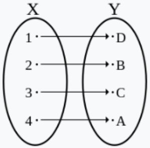
3 Function

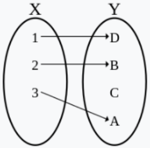
- If the domain of f is the Cartesian product $A_1 \times A_2 \times ... \times A_n (n \geq 1)$, then f is called an *n-ary* function.
- An *n-ary* function maps ordered n-tuples from its domain to elements in its codomain.
- $f : A^n \to A$ is called an *n-ary* function in A.
- For example, the addition function $+$ from $\mathbb{N}^2$ to $\mathbb{N}$ is a binary function. Its domain is $\mathbb{N}^2$, its codomain is $\mathbb{N}$.

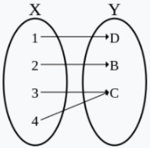
Injective, Surjective, and Bijective Functions

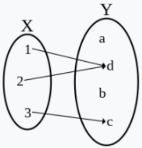
Given a function $f : X \to Y$:

- Injective (one-to-one, 单射): if each element of the codomain is mapped to by *at most* one element of the domain, i.e., for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$.
- Surjective (onto, 满射): if each element of the codomain is mapped to by *at least* one element of the domain, i.e., for any $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- Bijective (one-to-one correspondence, 双射): if **each element** of the codomain is mapped to by *exactly one* element of the domain. That is, the function is both injective and surjective.

<table>
<tr><th></th><th>surjective</th><th>non-surjective</th></tr>
<tr><td>injective</td><td>

bijective</td><td>

injective-only</td></tr>
<tr><td>non-injective</td><td>

surjective-only</td><td>

general</td></tr>
</table>

Injective, Surjective, and Bijective Functions

Is the following function one-to-one? onto? bijective?

- X and Y are set of human beings. The function $f : X \to Y$ is defined as: $f = \{\langle x, y\rangle \mid y \text{ is the mother of } x\}$
- The function $f : \mathbb{N} \to \mathbb{N}$ is defined as $f(x) = x^2$.

Inductive Definition

How do we formally define $\mathbb{N} = \{0, 1, 2, ...\}$?

Inductive Definition

The set $\mathbb{N}$ of natural numbers is inductively defined (归纳定义) by the following rules:

(i) $0 \in \mathbb{N}$

(ii) For any n, if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$

(iii) Only n generated by (finite iterations of) (i) and (ii), $n \in \mathbb{N}$

The above definition can be equivalently stated as follows:

$\mathbb{N}$ is the smallest inductive subset of S that satisfies conditions (i) and (ii):

(i) $0 \in S$

(ii) For any n, if $n \in S$, then $n + 1 \in S$

An inductive definition always implies that we are looking for the smallest set such that the given rules hold.

Proof by Induction (归纳证明)

Let P be a property, and $P(x)$ denotes that x has property P.

For a set defined inductively, to prove that all its elements have a property P, one can use the **proof by induction** method.

- Base case: We need to show that $P(n)$ is true for the smallest possible value of n, e.g., $P(n_0)$ is true.
- Induction Hypothesis: Assume that the statement $P(k)$ is true for any positive integer $k \geq n_0$.
- Inductive Step: Show that the statement $P(k+1)$ is true.

Example: proof by induction

Prove $2^n > n + 4$ for $n \geq 3, n \in \mathbb{N}$.

Define the function for computing Fibonacci sequence:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots\ldots$$

Recursive Definition

A recursive definition (递归定义) of a function f, defines a value of function at some natural number n in terms of the function's value at some previous point(s).

For example, let g, h be known functions on $\mathbb{N}$, which define a function f on $\mathbb{N}$:

$$\begin{cases} f(0) = g(0), \\ f(n') = h(f(n)). \end{cases}$$

For any $n \in \mathbb{N}$, the value of $f(n)$ can be computed from the above definition using $f(0), f(1), \ldots, f(n-1)$, and this type of definition is referred to as **recursive definition**.

Proof by Contradiction

- Prove that $\sqrt{2}$ is irrational (无理数).
- Prove that there are infinitely many prime numbers.

Readings

Optional

- TextD: Chapter 1.1. Mathematical Proof
- TextI: Preliminaries
- TextH: Chapter Zero
- Text1: 绪论、第一章
- Text2: 第一、二章
- Text3: 引言、第一章

Assignments
Coursework

- Assignment 1 released. Check Blackboard for details.
- The assignment can be either handwritten or completed using software (recommended but not required: LaTeX).
- Assignment should be submitted as **pdf** to Blackboard (for handwritten assignments, you may scan it or take a **clear** photo of it then upload).

Introduction to Mathematical Logic

Thank you for listening!
Any questions?