Introduction to Mathematical Logic

For CS Students

CS104/CS108

Yida TAO (陶伊达)

2024 年 2 月 28 日

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

translate concept into concrete language

What is Set?

A Set (集合) is a collection of objects

- A = Students in our class
- B = $\{1, 5, 10, 20\}$
- $\mathbb{Z}$ = Integers

Elements of Sets

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

- A = Students in our class: Tom $\in$ A
- B = $\{1, 5, 10, 20\}$: $1 \in B$, $30 \notin B$
- $\mathbb{Z}$ = Integers: $1 \in \mathbb{Z}$, $\pi \notin \mathbb{Z}$

Intension & Extension

set 有 2类

decide concept

- Intension (内涵): The intension of a set is its description or defining properties, i.e., what is true about members of a set. (对概念的定义)
- Extension (外延): The extension of a set is its members or contents. (概念所代表的对象)

don't care property
list them all

Intension & Extension

$\mathbb{P}$ = Prime numbers

- **Intension** of $\mathbb{P}$: any natural number greater than 1 that is not a product of two smaller natural numbers.
- **Extension** of $\mathbb{P}$: $2, 3, 5, 7, 11, 13, 17, 19, \ldots\ldots$

describe the property

表示

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

$\{x \mid \varphi(x)\}$

Think:

even number

- What's the set $\{x \mid x \in \mathbb{Z}$ and x is divisible by 2$\}$
- What's the set $\{x \mid x \neq x\}$? ϕ empty set
- What's the set $\{X \mid X \notin X\}$?

set is an element of the set

罗素悖论

Axiom of Extension

1 Set

外延原理

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: $\{0\}$

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

$\{0\}$

Order & Repetition Don't Matter

无关

- $\{a\} = \{a,a\}$
- $\{a,b\} = \{b,a\} = \{a,b,b\} = \{a,b,b,a\}$
- $\{a,b,c\} = \{c,b,a\} = \{b,c,b,a\}$

Subset 子集

- 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 | x is human}
  - {x | x is a prime number} $\not\subseteq$ {x | x is an odd number}
  - {< 孟子， 孟母 >， < 曹植， 曹操 >} $\subseteq$ {<x, y> | x is y's son}
- 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)

“子集”的集合

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., $\mathcal{P}(A)$.

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

Set Operations

1 Set

- $A \cup B$ 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: $\{x \mid x \in A \ and \ x \notin B\}$

$\in A$ and $\notin B$

Set Properties

- $A \subseteq B$ iff. $A \cap B = A$
- $A \subseteq B$ iff. $A \cup B = B$

Table of Contents

2 Relation

Why do we need relation?

2 Relation

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

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

Only capture elements with same property

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

自定义的关系

Why do we need relation?

2 Relation

Suppose that we have a phone book listing 1000 names in alphabetical order along with addresses and phone numbers.

Let T be the set containing these names, addresses, and phone numbers.

As a set, T is a collection of 3000 elements having no particular order or other relationships.

As a database, our phone book is more than merely a set with 3000 entries. The database is a structure: a set together with certain relations.

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

n元组

n-tuple 相等
①个数等
②每个对应相等

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 tuple has properties that distinguish it from a set:

- A tuple may contain multiple instances of the same element, e.g., $\langle 1, 2, 2, 3 \rangle \neq \langle 1, 2, 3 \rangle$

  $\{1,2,2,3\} = \{1,2,3\}$ set 相同
- 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.

Binary Relation

Intuitively, a binary relation from a set X to a set Y is a set of ordered pairs <x, y> where x is an element of X and y is an element of Y.

全部组合

$A \times B$ denotes the Cartesian product (笛卡尔积) of set A and B: $\{\langle x, y\rangle \mid x \in A \text{ and } y \in B\}$ (the set of all ordered pairs where x is in A and y is in B.)

A binary relation R over sets X and Y is a subset of Cartesian product $A \times B$, denoted as $R \subseteq A \times B$.

is also a set

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 on the set $\{$x | x is human$\}$
- $\{\langle x, y \rangle \mid x$ is y's spouse$\}$ is a binary relation on 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 $A_1 = A_2 = ... = A_n = A$. 都是A集合的元素

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

binary → n-ary

n-ary relation

2 Relation

Example: recall the phone book database that contains 1000 entries T. N is a set of names in T; P is a set of phone numbers in T; A is a set of addresses in T.

- Unary relation: each of N,P,A (a "unary relation" should be viewed as a predicate or an adjective describing elements of the set.) 一元一般就是property
- Binary relation: x and y are elements of N (i.e., names), $x < y$ means that x precedes y alphabetically, which is a binary relation on T.
- Ternary relation: $\{$ <Amy Angels, 35 Mediterranean Ave, 224-1357 >, < Barbara Braves, 221 Atlantic Ave, 301-1734 >, < Charles Cubs, 312 Baltic Ave, 223-9876 > $\}$, is a 3-ary (ternary) relation over T.

Equivalence Relation

① R_1 : is taller than

R_2 : has the same score

Let R be a binary relation on a set A.

Alice R Alice

- R is **reflexive**(自反) if for all x∈A, xRx.

  R_1 不自反 R_2 reflective

- R is **symmetric**(对称) if for all x, y∈A, if xRy, then yRx.
- R is **transitive**(传递) if for all x, y, z∈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

2 Relation

- ”=” is an equivalence relation on $\mathbb{N}$。
- $\{$ <x,y> | x and y are contemporaries$\}$ is an equivalence relation on $\{$x | x is human$\}$.
- $\{$<x,y> | 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 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.

$[x]_R$ 在 R 关系下与 x 等价的所有元素的集合

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

Equivalence Class

Theorem: If R is an equivalence relation over A, then every $a \in A$ belongs to exactly one equivalence class. ①属于唯一类

Theorem: Given an equivalence relation on set A, the collection of equivalence classes forms a partition (划分) of set A. ②按类划分

Examples of equivalence relation.

- ”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 on $\mathbb{Z}$ by:

$[x]_R \{y \in \mathbb{N} \mid yRx\}$

$$aRb \Leftrightarrow a \bmod 4 = b \bmod 4$$

Find the equivalence classes of R.

governed by relation

4 "=" 16

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:

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

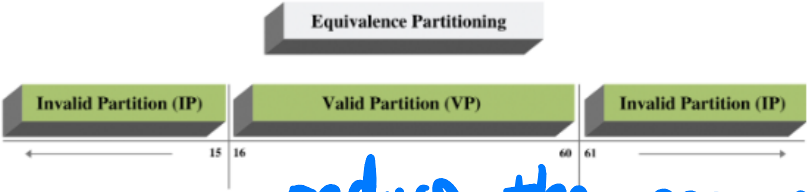
Every integer belongs to exactly one of these four sets: $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$. These four sets are disjoint. Hence $\{[0], [1], [2], [3]\}$ is a partition of $\mathbb{Z}$.

解体的

Equivalence Class

Applications in CS: Equivalence partitioning or equivalence class partitioning is a software testing technique that divides the input data of a software unit into partitions of equivalent data from which test cases can be derived.

E.g., a gym APP requires user ages between 16 to 60. How do you test the age input?



reduce the resources

Partial Order Relation (偏序关系)

xRy and yRx unless x=y

- A binary relation R on a set A is antisymmetric (反对称的) if for all x, y ∈ 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.

一定有 xRy

- 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.

一定有 yRx

- 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.

在左为"小"
在右为"大"

Partial Order Relation

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)

任何两元素都可以用R描述

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. ✗ 不是任2个元素能比
- $\subseteq$ is a partial order on $\mathcal{P}(\mathbb{N})$, $\varnothing$ is the minimal element, $\mathbb{N}$ is the maximal element. ✗

$\{3,1\} \not\subseteq \{4,2\}$
且 $\{4,2\} \not\subseteq \{3,1\}$

同(2)

得有至少一个成立 xRy / yRx

Applications in CS

2 Relation

Consider a program P as a set of variables.

The relation ”value of variable x depends on the value of variable y” is a partial order on P.

Statements that don’t have such dependency can be swapped without affecting the program execution outcome, which is widely adopted in compiler optimization.

没有依赖关系的语句可交换

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. 一对一匹配的关系
- 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:

one - to - one mapping

- 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.

Definition

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

$$f : A \rightarrow B$$

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** ouput values, i.e., a subset of the B
- We typically use $f(x) = y$ to denote $\langle x, y\rangle \in f$.

是f的元素

relation 这么写 (但一般不用)

Example

3 Function

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: $\{A, B, C\}$ 实际范围

n-ary function

- If the domain of f is the Cartesian product $A_1 \times A_2 \times \ldots \times A_n (n \geq 1)$, 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 $\mathbb{N}$.

定义域2元　　上域

在N中

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

上域

- Injective (one-to-one, 单射或一一映射): 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 $x_1 = x_2$.

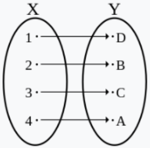
  → 可以没有能对应的

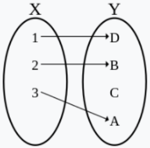
  至少一个对应的x

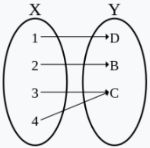
- Surjective (onto, 满射): if each element of the codomain is mapped to by *at least* one element of the domain, i.e., for any $y \in Y$, there exists $x \in X$ such that $f(x) = y$.
- Bijective (双射): if **each element** of the codomain is mapped to by *exactly one* element of the domain. That is, the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

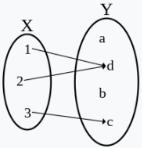
Injective, Surjective, and Bijective Functions

3 Function

<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>

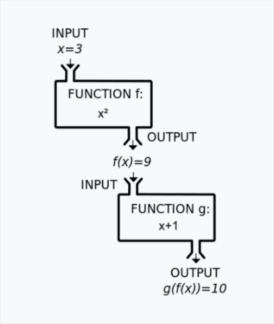
general</td></tr>
</table>

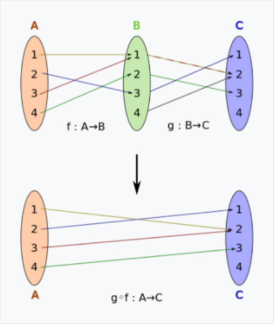
Is the following function one-to-one? onto? bijective?

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

no

Given $f : X \to Y,\ g : Y \to Z$. The *composite function* is denoted $g \circ f : X \to Z$, defined by $(g \circ f)(x) = g(f(x))$ for all x in X.





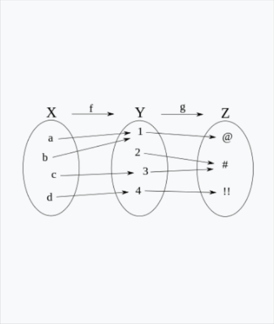


Table of Contents

4 Mathematical Definitions & Proof

Inductive Definition

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

Inductive Definition

The set $\mathbb{N}$ of natural numbers is inductively defined 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), $n \in \mathbb{N}$

只能由 (i)(ii) 创造

Inductive Definition

与前页中(iii)等价

The above definition can be equivalently stated as follows: $\mathbb{N}$ is the smallest inductive subset of S that satisfies conditions (i) and (ii):

排除其他元素

(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.

Inductive Definition

归纳定义集

Examples of inductively defined sets:

- The set of strings with alphabet Σ (later)
- Logical formulae (later)
- BNF notation: a notation used to describe the syntax of programming languages or other formal languages. (you'll learn this in the compiler course)

Proof by Induction (归纳证明)

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

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

指后一个

- (i) $P(0)$;
- (ii) For any $n \in \mathbb{N}$, if $P(n)$, then $P(n')$ (n' is the successor of n)

Then, for any $n \in \mathbb{N}$, $P(n)$.

模板 Template for proof by induction

4 Mathematical Definitions & Proof

最小值正确

- 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

4 Mathematical Definitions & Proof

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

Base case: $n=3$ $\quad 2^3 > 3+4$

Induction hypothesis: assume $2^n > n+4$

Inductive step: $2 \times 2^n > 2(n+4) > n+5$

$2^{n+1} > n+1+4$

$\begin{cases} P(3) \checkmark \\ P(n) \to P(n+1) \end{cases}$

Recursive Definition (递归定义)

A recursive definition 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**.

Example: Recursive Definition

4 Mathematical Definitions & Proof

$$f(n) = \begin{cases} 0 & n=1 \\ 1 & n=2 \\ f(n-1)+f(n-2) & n\geq 3 \end{cases}$$

Define the function for computing Fibonacci sequence:

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

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
- TextI: Preliminaries
- TextH: Chapter Zero
- Text1: 绪论、第一章
- Text2: 第一、二章
- Text3: 引言、第一章

Introduction to Mathematical Logic

Thank you for listening!
Any questions?