Formal Methods（形式化方法）

Lecture 13. More about Logic

智能与计算学部 章衡

2021年上学期

Outline

Example

Each even number greater than 2 equals to the sum of two primes.

- E: the set of all even numbers
- P: the set of all primes
- $x + y$: $x + y$ is the sum of x and y
- $x = y$: x equals to y
- $x > y$: x is greater than y
- $\forall x$: for all x we have that $\cdots$
- $\exists x$: there is some x such that $\cdots$
- $\forall x : E \bullet (x > 2 \rightarrow \exists y : P \bullet \exists z : P \bullet x = y + z)$

- m-ary predicates: propositions with m parameters
  - E, P: unary predicates; $=$, $>$: binary predicates
- m-ary functions
  - $+$: a binary function
- universal quantifier $\forall$, existential quantifier $\exists$
- constants,variables

Terms (项)

Definition (Term)

Terms are precisely those expressions which can be obtained by finitely many applications of the following rules:

1. Variables and constants are terms.
2. If $t_1, \ldots, t_m$ are terms and f an m-ary function for some $m \geq 0$, then $f(t_1, \ldots, t_m)$ is also a term.

Example

Let x, y be variables, c a constant, g a unary function, and f a binary function. Is $f(f(x, c), g(y))$ a term?

- x, y, c
- $f(x, c), g(y)$
- $f(f(x, c), g(y))$

Formulas (公式)

Definition (Formula)

First-order formulas (or simply, formulas) are those expressions obtained by finitely many applications of the following rules:

1. If $t_1, \ldots, t_m$ are terms and P an m-ary predicate, then $P(t_1, \ldots, t_m)$ and $(t_1 = t_2)$ are formulas;such formulas are called atomic formulas.
2. If φ and ψ are formulas, then $(\neg\varphi)$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \Rightarrow \psi)$, $(\varphi \Leftrightarrow \psi)$ are formulas.
3. If φ is a formula, x a variable, and S a unary predicate, then $\forall x : S \bullet \varphi$ and $\exists x : S \bullet \varphi$ are formulas; in both formulas, φ is called the scope of quantifiers $\forall x : S$ and $\exists x : S$, respectively.

Example

Let P be a unary predicate, and T be a binary predicate. Is $\exists x : P \bullet \exists y : P \bullet (R(x, y) \wedge \forall y : P \bullet T(x, y))$ a formula?

$$T(x, y)$$

$$\forall y : P \bullet T(x, y)$$

$$(R(x, y) \wedge \forall y : P \bullet T(x, y))$$

$$\exists y : Q \bullet (R(x, y) \wedge \forall y : P \bullet T(x, y))$$

$$\exists x : P \bullet \exists y : Q \bullet (R(x, y) \wedge \forall y : P \bullet T(x, y))$$

Sentences (语句)

Definition (Free occurrence and free variable)

An occurrence of a variable x is called free w.r.t. some formula φ if it is not quantified in φ, i.e., not in the scope of any quantifier in φ. A variable x is called free w.r.t. φ if there is at least one free occurrence of x in φ.

Example

$$
\begin{array}{rcl}
T(x, y) & : & x, y \\
\forall y : P \bullet T(x, y) & : & x \\
(R(x, y) \wedge \forall y : P \bullet T(x, y)) & : & x, y \\
\exists y : Q \bullet (R(x, y) \wedge \forall y : P \bullet T(x, y)) & : & x \\
\exists x : P \bullet \exists y : Q \bullet (R(x, y) \wedge \forall y : P \bullet T(x, y)) & : & \text{no free variable}
\end{array}
$$

Definition (Sentence)

Every sentence is a formula without free variable.

Informal semantics

1. $P(t_1, \ldots, t_m)$: the relation (represented by P) holds for the tuple of objects (represented by) $t_1, \ldots, t_m$;
2. $(t_1 = t_2)$: the objects (represented by) t_1 and t_2 are the same;
3. $(\neg\varphi)$: the property (represented by) φ does not hold;
4. $(\varphi \wedge \psi)$: both properties (represented by) φ and ψ hold;
5. $(\varphi \vee \psi)$: either the property (represented by) φ or the property (represented by) ψ holds;
6. $(\varphi \Rightarrow \psi)$: if the property (represented by) φ holds, then the property (represented by) ψ also holds;
7. $(\varphi \Leftrightarrow \psi)$: the property (represented by) φ holds if, and only if the property (represented by) ψ holds;
8. $\forall x : S \bullet \varphi$: for every object x, if x in S then the property (represented by) φ holds;
9. $\exists x : S \bullet \varphi$: there is some object x such that x in S and the property (represented by) φ holds.

Definition (Logical consequence (逻辑推论), informal definition)

Suppose $\Sigma = \{\varphi_1, \ldots, \varphi_n\}$, and $\varphi_1, \ldots, \varphi_n, \psi$ are sentences. We call ψ a logical consequence of Σ, denoted $\Sigma \models \psi$ (or $\varphi_1, \ldots, \varphi_n \models \psi$), if the property $\varphi_1 \wedge \cdots \wedge \varphi_n \Rightarrow \psi$ holds.In this case, we say that ψ is derivable from Σ.

We say that φ is logically equivalent to ψ, denoted $\varphi \equiv \psi$, if we have both $\varphi \models \psi$ and $\psi \models \varphi$.

Conventions

- $\exists x : S \bullet (\varphi \land \psi)$ may be rewritten as $\exists x : S \mid \varphi \bullet \psi$
- $\forall x : S \bullet (\varphi \Rightarrow \psi)$ may be rewritten as $\forall x : S \mid \varphi \bullet \psi$
- $\exists x_1 : S \bullet \cdots \bullet \exists x_n : S \bullet \varphi$ may be rewritten as $\exists x_1, \ldots, x_n : S \bullet \varphi$
- $\forall x_1 : S \bullet \cdots \bullet \exists x_n : S \bullet \varphi$ may be rewritten as $\forall x_1, \ldots, x_n : S \bullet \varphi$

Example

- $\forall x : E \bullet (x > 2 \Rightarrow \exists y : P \bullet \exists z : P \bullet x = y + z)$:

$$\forall x : E \mid x > 2 \bullet \exists y, z : P \bullet x = y + z$$

Built-in predicates, functions and constants

- Built-in predicates: $\mathbb{N}, \mathbb{Z}, <, \leq, >, \geq, \in, \subseteq, \subset, \ldots$
- Built-in functions: $+, -, *, /, \ldots$
- Built-in constants: $0, 1, 2, \ldots$

Exercise

Ex. 1

Let us consider a directed graph G. Suppose V is a unary predicate intended to define the set of vertices in G, and E is a binary predicate intended to define the set of edges in G. Please use a first-order sentence to describe the following property:

The indegree of G is not greater than 3.

Ex. 2

Let P be a unary predicate. Please use a first-order sentence to assert that

P consists of the set of all primes.

Note that the bulit-in functions $+, -, *, /$ and predicates $=, >, \geq, <, \leq$ are allowed.

Outline

Deductive system (演绎系统)

- Deductive systems provide a syntactic way to prove $\Sigma \models \psi$.
- A deductive system consists of the finite set of inference rules of the following form:

Definition (Inference rule (推理规则))

Every inference rule is of the following form:

$$\frac{\Sigma_1 \models \varphi_1 \cdots \Sigma_n \models \varphi_n}{\Sigma \models \psi} \text{ [name] <condition of application>}$$

Inference rules (1)

Reference and monotonicity

$$\frac{}{\varphi \vDash \varphi} \quad [\text{ref}] \qquad \frac{\Sigma \vDash \varphi}{\Sigma, \Gamma \vDash \varphi} \quad [+]$$

$\neg$

$$\frac{\Sigma, \neg\varphi \vDash \psi \quad \Sigma, \neg\varphi \vDash \neg\psi}{\Sigma \vDash \varphi} \quad [\neg -]$$

Inference rules (2)

$\wedge$

$$\frac{\Sigma \models \varphi \wedge \psi}{\Sigma \models \varphi} \quad [\wedge-_1] \qquad \frac{\Sigma \models \varphi \wedge \psi}{\Sigma \models \psi} \quad [\wedge-_2]$$

$$\frac{\Sigma \models \varphi \quad \Sigma \models \psi}{\Sigma \models \varphi \wedge \psi} \quad [\wedge+]$$

$\vee$

$$\frac{\Sigma, \varphi \models \chi \quad \Sigma, \psi \models \chi}{\Sigma, \varphi \vee \psi \models \chi} \quad [\vee-]$$

$$\frac{\Sigma \models \varphi}{\Sigma \models \varphi \vee \psi} \quad [\vee+_1] \qquad \frac{\Sigma \models \varphi}{\Sigma \models \psi \vee \varphi} \quad [\vee+_2]$$

Inference rules (3)

$\Rightarrow$

$$\frac{\Sigma \models \varphi \Rightarrow \psi \quad \Sigma \models \varphi}{\Sigma \models \psi} \quad [\Rightarrow -] \qquad \frac{\Sigma, \varphi \models \psi}{\Sigma \models \varphi \Rightarrow \psi} \quad [\Rightarrow +]$$

$\Leftrightarrow$

$$\frac{\Sigma \models \varphi \Leftrightarrow \psi \quad \Sigma \models \varphi}{\Sigma \models \psi} \quad [\Leftrightarrow -_1] \qquad \frac{\Sigma \models \varphi \Leftrightarrow \psi \quad \Sigma \models \psi}{\Sigma \models \varphi} \quad [\Leftrightarrow -_2]$$

$$\frac{\Sigma, \varphi \models \psi \quad \Sigma, \psi \models \varphi}{\Sigma \models \varphi \Leftrightarrow \psi} \quad [\Leftrightarrow +]$$

Formal proof

Definition (Formal proof)

Let Σ be a set of formulas, φ a formula. We say that $\Sigma \models \varphi$ is formally provable if there is a finite sequence of the form

$$\Sigma_1 \models \varphi_1, \Sigma_2 \models \varphi_2, \ldots, \Sigma_n \models \varphi_n \tag{1}$$

such that(1) for $k = 1, \ldots, n, \ \Sigma_k \models \varphi_k$ is obtained from

$$\Sigma_1 \models \varphi_1, \ldots, \Sigma_{k-1} \models \varphi_{k-1}$$

by some inference rule presented previously,(2) $\Sigma_n = \Sigma$and (3)$\varphi_n = \varphi$. In this case, the above sequence is called a formal proof of $\Sigma \models \varphi$.

Example

Below is a formal proof of $\varphi \wedge \psi \models \varphi$:

(1) $\varphi \wedge \psi \models \varphi \wedge \psi$ [ref]

(2) $\varphi \wedge \psi \models \varphi$ [$\wedge -_1$], (1)

Rule $\in$

Example

Please prove the following by deductive system: If $\varphi \in \Sigma$ then $\Sigma \vDash \varphi$.

Proof.

Suppose $\varphi \in \Sigma$, and let $\Sigma_0 == \Sigma \setminus \{\varphi\}$.Then the following is a formal proof of $\Sigma_0, \varphi \vDash \varphi$.

(1)	$\varphi \vDash \varphi$	[ref]
(2)	$\Sigma_0, \varphi \vDash \varphi$	[+], (1)

We thus have that $\Sigma \vDash \varphi$. $\square$

Rule $\in$

$$\frac{}{\Sigma \vDash \varphi} \quad [\in] \quad <\varphi \in \Sigma>$$

Transitivity of inference

Rule of transitivity

$$\frac{\Sigma \models \varphi_1 \quad \cdots \quad \Sigma \models \varphi_n \quad \varphi_1, \ldots, \varphi_n \models \psi}{\Sigma \models \psi} \quad \text{[trans]}$$

Proof (by deductive system).

(1)	$\varphi_1, \ldots, \varphi_n \models \psi$	Assumption
(2)	$\varphi_1, \ldots, \varphi_{n-1} \models \varphi_n \Rightarrow \psi$	$[\Rightarrow +]$, (1)
	$\vdots$	
(n+1)	$\models (\varphi_1 \Rightarrow \cdots (\varphi_{n-1} \Rightarrow (\varphi_n \Rightarrow \psi)) \cdots)$	$[\Rightarrow -]$, (n)
(n+2)	$\Sigma \models (\varphi_1 \Rightarrow \cdots (\varphi_{n-1} \Rightarrow (\varphi_n \Rightarrow \psi)) \cdots)$	$[+]$, (n+1)
(n+3)	$\Sigma \models \varphi_1$	Assumption
(n+4)	$\Sigma \models (\varphi_2 \Rightarrow \cdots (\varphi_{n-1} \Rightarrow (\varphi_n \Rightarrow \psi)) \cdots)$	$[\Rightarrow -]$, (n+1)
	$\vdots$	
(m-2)	$\Sigma \models \varphi_n \Rightarrow \psi$	$[\Rightarrow -]$, (n+1)
(m-1)	$\Sigma \models \varphi_n$	Assumption
(m)	$\Sigma \models \psi$	$[\Rightarrow -]$, (m-2), (m-1) $\square$

Example 1

Example

Please give a formal proof of $\neg\varphi \Rightarrow \psi \vDash \neg\psi \Rightarrow \varphi$.

Proof.

(1)	$\neg\varphi \Rightarrow \psi, \neg\psi, \neg\varphi \vDash \neg\varphi \Rightarrow \psi$	$[\in]$
(2)	$\neg\varphi \Rightarrow \psi, \neg\psi, \neg\varphi \vDash \neg\varphi$	$[\in]$
(3)	$\neg\varphi \Rightarrow \psi, \neg\psi, \neg\varphi \vDash \psi$	$[\Rightarrow -]$, (1),(2)
(4)	$\neg\varphi \Rightarrow \psi, \neg\psi, \neg\varphi \vDash \neg\psi$	$[\in]$
(5)	$\neg\varphi \Rightarrow \psi, \neg\psi \vDash \varphi$	$[\neg -]$, (3), (4)
(6)	$\neg\varphi \Rightarrow \psi \vDash \neg\psi \Rightarrow \varphi$	$[\Rightarrow +]$, (5)

$\square$

Example 2

Example

Please give a formal proof of $\varphi \Rightarrow \psi, \psi \Rightarrow \chi \vDash \varphi \Rightarrow \chi$.

Proof.

(1)	$\varphi \Rightarrow \psi, \psi \Rightarrow \chi, \varphi \vDash \varphi \Rightarrow \psi$	$[\in]$
(2)	$\varphi \Rightarrow \psi, \psi \Rightarrow \chi, \varphi \vDash \varphi$	$[\in]$
(3)	$\varphi \Rightarrow \psi, \psi \Rightarrow \chi, \varphi \vDash \psi$	$[\Rightarrow -]$, (1), (2)
(4)	$\varphi \Rightarrow \psi, \psi \Rightarrow \chi, \varphi \vDash \psi \Rightarrow \chi$	$[\in]$
(5)	$\varphi \Rightarrow \psi, \psi \Rightarrow \chi, \varphi \vDash \chi$	$[\Rightarrow -]$, (4), (3)
(6)	$\varphi \Rightarrow \psi, \psi \Rightarrow \chi \vDash \varphi \Rightarrow \chi$	$[\Rightarrow +]$, (5)

$\square$

Exercise

Ex. 3

Please prove the following by deductive system:

1. $(\varphi \land \psi) \lor (\varphi \land \chi) \vDash \varphi \land (\psi \lor \chi)$。
2. If Σ is finite, and we have both $\Sigma, \varphi \vDash \psi$ and $\Sigma, \varphi \vDash \neg\psi$, then we also have $\Sigma \vDash \neg\varphi$.

First-order inference rules (1)

$\forall$

$$\frac{\Sigma \models \forall x : S \bullet \varphi}{\Sigma \models t \in S \Rightarrow \varphi[t/x]} \quad [\forall-]$$

$$\frac{\Sigma \models x \in S \Rightarrow \varphi}{\Sigma \models \forall x : S \bullet \varphi} \quad [\forall+] \quad \text{<x has no free occurrence in } \Sigma\text{>}$$

where $\varphi[t/x]$ denote the formula obtained from φ by substituting t for all occurrences of x.

$\exists$

$$\frac{\Sigma, x \in S, \varphi \models \psi}{\Sigma, \exists x : S \bullet \varphi \models \psi} \quad [\exists-] \quad \text{<x has no free occurrence in } \Sigma \text{ and } \psi\text{>}$$

$$\frac{\Sigma \models t \in S \wedge \varphi(t)}{\Sigma \models \exists x : S \bullet \varphi(x)} \quad [\exists+]$$

where $\varphi(x)$ is obtained from $\varphi(t)$ by substituting x for some occurrences of t.

First-order inference rules (2)

=

$$\frac{\Sigma \vDash \varphi(t) \quad \Sigma \vDash t = t'}{\Sigma \vDash \varphi(t')} \quad [=-]$$

$$\frac{}{\vDash x = x} \quad [=+]$$

where $\varphi(t')$ is obtained from $\varphi(t)$ by substituting t' for some occurrences of t.

Example 3

Example

Prove the following by deductive systems: $\forall x : S \bullet \forall y : T \bullet \varphi(x, y) \equiv \forall y : T \bullet \forall x : S \bullet \varphi(x, y)$.

Proof.

Due to the symmetry, only prove $\forall x : S \bullet \forall y : T \bullet \varphi(x, y) \vDash \forall y : T \bullet \forall x : S \bullet \varphi(x, y)$.

(1)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), x \in S, y \in T \vDash \forall x : S \bullet \forall y : T \bullet \varphi(x, y)$	$[\in]$
(2)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), x \in S, y \in T \vDash x \in S \Rightarrow \forall y : T \bullet \varphi(x, y)$	$[\forall -]$, (1)
(3)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), x \in S, y \in T \vDash x \in S$	$[\in]$
(4)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), x \in S, y \in T \vDash \forall y : T \bullet \varphi(x, y)$	$[\Rightarrow -]$, (2), (3)
(5)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), x \in S, y \in T \vDash y \in T \Rightarrow \varphi(x, y)$	$[\forall -]$, (4)
(6)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), x \in S, y \in T \vDash y \in T$	$[\in]$
(7)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), x \in S, y \in T \vDash \varphi(x, y)$	$[\Rightarrow -]$, (5), (6)
(8)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), y \in T \vDash x \in S \Rightarrow \varphi(x, y)$	$[\Rightarrow +]$, (7)
(9)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y), y \in T \vDash \forall x : S \bullet \varphi(x, y)$	$[\forall +]$, (8)
(10)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y) \vDash y \in T \Rightarrow \forall x : S \bullet \varphi(x, y)$	$[\Rightarrow +]$, (9)
(11)	$\forall x : S \bullet \forall y : T \bullet \varphi(x, y) \vDash \forall y : T \bullet \forall x : S \bullet \varphi(x, y)$	$[\forall +]$, (10)

$\square$

Example 2

Example

Prove the following by deductive systems: $\neg\forall x : S \bullet \varphi(x) \equiv \exists x : S \bullet \neg\varphi(x)$.

Proof.

Only prove $\neg\forall x : S \bullet \varphi(x) \vDash \exists x : S \bullet \neg\varphi(x)$.

(1)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x), x \in S, \neg\varphi(x) \vDash x \in S$	$[\in]$
(2)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x), x \in S, \neg\varphi(x) \vDash \neg\varphi(x)$	$[\in]$
(3)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x), x \in S, \neg\varphi(x) \vDash x \in S \wedge \neg\varphi(x)$	$[\wedge+]$, (1), (2)
(4)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x), x \in S, \neg\varphi(x) \vDash \exists x : S \bullet \neg\varphi(x)$	$[\exists+]$, (3)
(5)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x), x \in S, \neg\varphi(x) \vDash \neg\exists x : S \bullet \neg\varphi(x)$	$[\in]$
(6)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x), x \in S \vDash \varphi(x)$	$[\neg-]$, (5)
(7)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x) \vDash x \in S \Rightarrow \varphi(x)$	$[\Rightarrow+]$, (6)
(8)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x) \vDash \forall x : S \bullet \varphi(x)$	$[\forall+]$, (7)
(9)	$\neg\forall x : S \bullet \varphi(x), \neg\exists x : S \bullet \neg\varphi(x) \vDash \neg\forall x : S \bullet \varphi(x)$	$[\in]$
(10)	$\neg\forall x : S \bullet \varphi(x) \vDash \exists x : S \bullet \neg\varphi(x)$	$[\neg-]$

$\square$

Example 3 (one-point rule)

Example (Prove the following property by deductive system)

- If $\Sigma \models \exists x : S \bullet (\varphi \wedge x = t)$ and x does not occur in t, then $\Sigma \models t \in S \wedge \varphi[t/x]$.

Proof.

(1)	$x \in S \wedge \varphi \wedge x = t \models x \in S \wedge \varphi \wedge x = t$	[ref]
(2)	$x \in S \wedge \varphi \wedge x = t \models x = t$	$[\wedge -_2]$, (1)
(3)	$x \in S \wedge \varphi \wedge x = t \models x \in S \wedge \varphi$	$[\wedge -_1]$, (1)
(4)	$x \in S \wedge \varphi \wedge x = t \models t \in S \wedge \varphi[t/x]$	$[= -]$, (3)
(5)	$\exists x : S \bullet (\varphi \wedge x = t) \models t \in S \wedge \varphi[t/x]$	$[\exists -]$, (4)
(6)	$\Sigma \models \exists x : S \bullet (\varphi \wedge x = t)$	Assumption
(7)	$\Sigma \models t \in S \wedge \varphi[t/x]$	[trans], (6), (5)

□

One-point rule (单点规则)

$$\frac{\Sigma \models \exists x : S \bullet (\varphi \wedge x = t)}{\Sigma \models t \in S \wedge \varphi[t/x]} \quad [\text{1-point}] \quad \langle x \text{ does not occur in } t \rangle$$

Assignments

Prove the following by deductive system:

1. $\models \varphi \vee \neg\varphi$ (i.e., $\emptyset \models \varphi \vee \neg\varphi$).
2. $\exists x : S \bullet \neg\varphi(x) \models \neg\forall x : S \bullet \varphi(x)$.
3. If x does not occur in ψ, then $\exists x : S \bullet (\varphi(x) \Rightarrow \psi) \models (\forall x : S \bullet \varphi(x)) \Rightarrow \psi$.