《软件分析与验证》

一阶理论

贺飞
清华大学软件学院

2022 年 3 月 13 日

- **语法**：一阶逻辑公式的构成
  - 符号集：逻辑符号、非逻辑符号
  - 构造规则：项、原子公式、文字、合式公式
- **语义**：一阶逻辑公式的含义
  - 解释 + 变量赋值：项求值和公式求值
  - 可满足式、有效式
  - 语义蕴涵
- **相继式演算系统** $\mathcal{S}_{FOL}$：证明一阶逻辑有效式
  - 推理规则
  - 可靠、完备、半可判定

表达能力与可判定性

命题逻辑可判定，但表达能力不够; 一阶逻辑的表达能力足够，但却不可判定

- 能否在表达能力与可判定性之间达成平衡?

程序操作的对象通常是一些结构，如整数、数组、列表等

- 能否针对这些结构定制对应的形式系统?

一阶理论:

- 表达能力比一阶逻辑弱
- 许多一阶理论是可判定的

目录

定义

定义

一阶理论（*first-order theory*）$\mathcal{T}$ 可表示为二元组 $(\Sigma, \mathcal{A})$，其中：

- Σ 是一个非逻辑符号集，称为签名（*signature*）；
- $\mathcal{A}$ 是一组定义在 Σ 上的闭公式，称为公理集（*axiom*）。

Σ-公式（也称 $\mathcal{T}$-公式）：只由逻辑符号（包括变元符号、逻辑联结词符号和量词符号等）和 Σ 中非逻辑符号组成的一阶逻辑公式。

一阶理论是一阶逻辑的受限形式，其中：

- Σ 定义了理论中允许出现的非逻辑符号（一阶逻辑允许任意非逻辑符号）
- $\mathcal{A}$ 定义了这些非逻辑符号的含义

- $\mathcal{T}$-解释（$\mathcal{T}$-interpretation）：满足 $\mathcal{T}$ 中所有公理的解释 $\mathcal{M}$，即 $\forall A \in \mathcal{A}.\, [\![A]\!]_{\mathcal{M}} = \mathit{true}$。
- $\mathcal{T}$-可满足式（$\mathcal{T}$-satisfaction）：存在一个 $\mathcal{T}$-解释 $\mathcal{M}$ 和一个赋值 ρ，使得 $[\![\varphi]\!]_{\mathcal{M},\rho}$ 为真。
- $\mathcal{T}$-有效式（$\mathcal{T}$-validity）：对任意 $\mathcal{T}$-解释 $\mathcal{M}$ 和任意赋值 ρ，$[\![\varphi]\!]_{\mathcal{M},\rho}$ 都为真，常记作 $\mathcal{T} \models \varphi$。
- $\mathcal{T}$-语义蕴含（$\mathcal{T}$-entailment）：φ $\mathcal{T}$-语义蕴含 ψ，或称 ψ 是 φ 在理论 $\mathcal{T}$ 下的逻辑推论，当且仅当 $\varphi \to \psi$ 是 $\mathcal{T}$-有效式。

可判定性（*decidability*）：如果存在一个算法，对任意给定的 Σ-公式，能够在有限时间内正确地判定出该公式是否是 $\mathcal{T}$-有效式，就称该理论是可判定的。

一阶理论的片段（*fragment*）：对 Σ-公式语法引入一定的限制，如不允许量词出现。

许多不可判定一阶理论的片段是可判定的 。

等式理论

定义

等式理论（*theory of equality*）$\mathcal{T}_E$ 由以下两部分构成：

- 签名 Σ_E：$\{=, a, b, c, \ldots, f, g, h, \ldots, p, q, r, \ldots\}$
  - 引入了一个特殊的二元谓词符号“=”
  - 对其他常数、函数和谓词符号的使用没有限制
- 公理集 $\mathcal{A}_E$，定义“=”的含义

例

$\mathcal{T}_E$ 公式实例：

- $\forall x, y.\ (x = y \to y = x)$
- $a = b \wedge b = c \to g(f(a), b) = g(f(c), a)$

“=” 的含义由 $\mathcal{A}_E$ 中的公理定义：

1. 自反性：$\forall x.\ x = x$
2. 对称性：$\forall x, y.\ (x = y \rightarrow y = x)$
3. 传递性：$\forall x, y, z.\ (x = y \wedge y = z \rightarrow x = z)$
4. 函数同余：$\forall \mathbf{x}, \mathbf{y}.\ ((\bigvee_{i=1}^{n} x_i = y_i) \rightarrow f(\mathbf{x}) = f(\mathbf{y}))$
5. 谓词同余：$\forall \mathbf{x}, \mathbf{y}.\ ((\bigvee_{i=1}^{n} x_i = y_i) \rightarrow p(\mathbf{x}) \leftrightarrow p(\mathbf{y}))$

在上面的两个同余公理中，f 和 p 可替换为任何函数或谓词，因此称这两个公理为公理模式（*axiom scheme*）。

例

$$\forall x_1, x_2, y_1, y_2.(x_1 = y_1 \wedge x_2 = y_2 \rightarrow f_2(x_1, x_2) = f_2(y_1, y_2))$$

是函数同余公理模式在符号 f_2 上的一个实例。

为简化讨论，应用以下规则消去 $\mathcal{T}_E$ 公式中除“=”以外的其他谓词符号：

1. 对应于每一个谓词符号 p，引入一个新的函数符号 f_p；
2. 引入一个新的常元符号 $\bullet$；
3. 把每一处 $p(t_1, \ldots, t_n)$ 的出现替换为 $f_p(t_1, \ldots, t_n) = \bullet$。

应用上述规则的结果称等式和未解释函数理论（*theory of equality and uninterpreted functions, EUF*）：

- 唯一的谓词符号为“=”
- 所有原子公式均为等式或不等式

例

$$x = y \to (p(x) \leftrightarrow p(y))$$

变换后:

$$x = y \to ((f_p(x) = \bullet) \leftrightarrow (f_p(y) = \bullet))$$

例

$$p(x) \wedge q(x, y) \wedge q(y, z) \to \neg q(x, z)$$

变换后:

$$(f_p(x) = \bullet \wedge f_q(x, y) = \bullet \wedge f_q(y, z) = \bullet) \to f_q(x, z) \neq \bullet$$

$\mathcal{T}_E$ 是可判定的吗?

- 答案是否定的。
- $\mathcal{T}_E$ 允许任何常元、函数和谓词符号出现，可以编码任何一阶逻辑公式 φ:
  - 将 φ 中的 "=" 替换为一个新的谓词符号，得到 φ'
  - φ' 不含 "="
  - φ' 和 $\mathcal{T}_E$ 中的公理 $\mathcal{A}$ 无关
- $\mathcal{T}_E$ 的无量词片段是可判定的（且有研究价值）

算术理论

皮亚诺算术（Peano Arithmetic）$\mathcal{T}_{PA}$

签名 $\Sigma_{PA} = \{0, 1, +, \times, =\}$，其中

- 0 和 1 为常量；
- $+$ 和 $\times$ 为二元函数，$=$ 为二元谓词
- 除上述五个符号外，Σ_{PA} 不含其它非逻辑符号！

公理集 $\mathcal{A}_{PA}$ 赋予 $0, 1, +, \times, =$ 以含义

1. 有关**等式**的公理：自反、对称、传递、同余
2. **零元**：$\forall x.\ \neg(x + 1 = 0)$
3. **后继**：$\forall x, y.\ ((x + 1 = y + 1) \rightarrow x = y)$
4. **与 0 加法**：$\forall x.\ x + 0 = x$
5. **加法后继**：$\forall x, y.\ x + (y + 1) = (x + y) + 1$
6. **与 0 乘法**：$\forall x.\ x \times 0 = 0$
7. **乘法后继**：$\forall x, y.\ x \times (y + 1) = x \times y + x$
8. **归纳性**：$(F[0] \wedge \forall x.\ (F[x] \rightarrow F[x + 1])) \rightarrow \forall x.\ F[x]$

皮亚诺算术 $\mathcal{T}_{PA}$：解释

皮亚诺算术的预期解释（*intended interpretation*）:

- 论域: $\mathbb{N}$
- $\mathcal{I}[0], \mathcal{I}[1]$: $0_{\mathbb{N}}, 1_{\mathbb{N}} \in \mathbb{N}$
- $\mathcal{I}[+]$: $+_{\mathbb{N}}$，$\mathbb{N}$ 上的加法
- $\mathcal{I}[\times]$: $\times_{\mathbb{N}}$，$\mathbb{N}$ 上的乘法
- $\mathcal{I}[=]$: $=_{\mathbb{N}}$，$\mathbb{N}$ 上的相等关系

方便起见，记 $x \times y$ 为 xy

注意 $\mathcal{T}_{PA}$ 只有五个非逻辑符号。

如何在 $\mathcal{T}_{PA}$ 下表示 $3x + 5 = 2y$?

$$(1+1+1) \times x + 1 + 1 + 1 + 1 + 1 = (1+1) \times y$$

如何表示 $x > 5$?

$$\exists y.\ (\neg(y = 0) \land x = 5 + y)$$

如何表示 $x + 1 \leq y$?

$$\exists z.\ x + 1 + z = y$$

$\mathcal{T}_{PA}$ 的语法糖:

- 任意自然数可以表示为多个 1 相加
- 关系式可以通过引入一个额外的自然数变量转换为等式
- 严格关系式再增加一个该额外变量不等于 0 的约束

皮亚诺算术 $\mathcal{T}_{PA}$：性质

- $\mathcal{T}_{PA}$ 是不可判定的
- $\mathcal{T}_{PA}$ 的无量词片段还是不可判定的
- 猜测：乘法会让推理异常复杂，应该尝试更简单的理论！

签名:

$$\Sigma_{\mathbb{N}} : \{0, 1, +, =\}$$

公理集 $\mathcal{A}_{\mathbb{N}}$:

1. 有关等式的公理：自反、对称、传递、同余
2. **零元**：$\forall x.\ \neg(x + 1 = 0)$
3. **后继**：$\forall x, y.\ ((x + 1 = y + 1) \rightarrow x = y)$
4. **与 0 加法**：$\forall x.\ x + 0 = x$
5. **加法后继**：$\forall x, y.\ x + (y + 1) = (x + y) + 1$
6. **归纳性**：$(F[0] \wedge (\forall x.\ F[x] \rightarrow F[x + 1])) \rightarrow \forall x.\ F[x]$

相比于 $\mathcal{T}_{PA}$，签名里少了乘号，公理集中少了有关乘号的两个公理。

- $\mathcal{T}_{\mathbb{N}}$ 是可判定的！（但相当困难：$O(2^{2^n})$）
- $\mathcal{T}_{\mathbb{N}}$ 允许量词消去：对任意 $\mathcal{T}_{\mathbb{N}}$ 公式 φ，存在一个等价的无量词公式 φ'
- $\mathcal{T}_{\mathbb{N}}$ 的无量词片段也是可判定的，且判定复杂度为 coNP-完全。

$\mathcal{T}_{\mathbb{N}}$ 可以表达任意整数的加、减、数乘和关系运算

- 任意整数可以表示为两个自然数相减
- 减法可以通过移位表示成加法
- 数乘可以表示成多次加法
- 关系式可以通过引入一个额外的自然数变量转换为等式
- 严格关系式再增加一个该额外变量不等于 0 的约束

例

考虑公式

$$\varphi_0: \quad \forall w, x.\ \exists y, z.\ x + 2y - z - 13 > -3w + 5$$

其中 $-$ 同一般减法，w, x, y, z 为 $\mathbb{Z}$ 中的整数

解

对 φ_0 中的每一个变量 v，引入新变量 v_p, v_n：

$$\begin{aligned}\varphi_1: \quad & \forall w_p, w_n, x_p, x_n.\ \exists y_p, y_n, z_p, z_n. \\ & (x_p - x_n) + 2(y_p - y_n) - (z_p - z_n) - 13 > -3(w_p - w_n) + 5\end{aligned}$$

$$\begin{aligned}\varphi_2: \quad & \forall w_p, w_n, x_p, x_n.\ \exists y_p, y_n, z_p, z_n.\ \exists u. \\ & \qquad (\neg(u = 0) \wedge x_p + y_p + y_p + z_n + w_p + w_p + w_p \\ & \qquad\quad = x_n + y_n + y_n + z_p + w_n + w_n + w_n + u \\ & \qquad\qquad + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \\ & \qquad\qquad\qquad + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1).\end{aligned}$$

线性整数算术理论（*theory of linear-integer arithmetic*）：

签名 $\Sigma_{\mathbb{Z}} = \{\ldots, -2, -1, 0, 1, 2, \ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots, +, -, =, >\}$,

- $-2, -1, 0, 1, 2, \ldots, +, -, =, >$ 的含义同普通算术
- $-3\cdot, -2\cdot, 2\cdot, 3\cdot$ 等为一元函数，表示数乘

可以证明：$\mathcal{T}_{\mathbb{Z}}$ 可归约到 $\mathcal{T}_{\mathbb{N}}$

- 其表达能力相同，故不再对 $\mathcal{T}_{\mathbb{Z}}$ 加以公理化
- $\mathcal{T}_{\mathbb{Z}}$ 使用起来更方便，比 $\mathcal{T}_{\mathbb{N}}$ 更常用

总结：一阶理论

一阶理论定义：

- 签名 Σ，公理集 $\mathcal{A}$

一些常见的一阶理论：

- $\mathcal{T}_E$, $\mathcal{T}_{PA}$, $\mathcal{T}_{\mathbb{N}}$, $\mathcal{T}_{\mathbb{Z}}$

下节课内容

- 程序语义

谢谢！