Theory of Programming Languages
程序设计语言理论

张昱

Department of Computer Science and Technology
University of Science and Technology of China

September, 2008

第2章　断言与规则

2.1　归纳定义 [PFPL, 1]

2.2　假言断言 [PFPL, 2]

2.3　参数化断言 [PFPL, 3]

2.1 归纳定义-1

❖ 断言(Judgement, assertion) [PFPL, 1]

例如，n nat　　n是自然数

$a=b$ nat　　a nat、b nat且a和b相等

❖ 推理规则(Inference Rules)

例如，

$$\frac{}{\texttt{zero}\ \mathrm{nat}} \qquad \frac{a\ \mathrm{nat}}{\texttt{succ}(a)\ \mathrm{nat}} \tag{1.2}$$

$$\frac{}{\texttt{zero} = \texttt{zero}\ \mathrm{nat}} \qquad \frac{a = b\ \mathrm{nat}}{\texttt{succ}(a) = \texttt{succ}(b)\ \mathrm{nat}} \tag{1.4}$$

2.1 归纳定义-2

❖ 归纳定义(Inductive Definition)

➢ 由一组形如 $\dfrac{J_1 \cdots J_k}{J}$ 的推理规则组成

❖ 推导(Derivations)

➢ 一个断言的推导由一组规则组成，它从公理(axioms)开始，结束于该断言。

➢ 推导可以用树来描述

如果 $\dfrac{J_1 \cdots J_k}{J}$ 是推理规则，$\nabla_1, \cdots, \nabla_k$ 是其前提的推导，则 $\dfrac{\nabla_1 \cdots \nabla_k}{J}$ 是其结论的一个推导.

2.1 归纳定义-3

❖ 推导(Derivations)

➢ 例如

$$\dfrac{\dfrac{\dfrac{}{\mathtt{zero}\ \mathrm{nat}}}{\mathtt{succ}(\mathtt{zero})\ \mathrm{nat}}}{\dfrac{\mathtt{succ}(\mathtt{succ}(\mathtt{zero}))\ \mathrm{nat}}{\mathtt{succ}(\mathtt{succ}(\mathtt{succ}(\mathtt{zero})))\ \mathrm{nat}}}$$

底

顶

➢ **正向推导(自底向上构造):** 公理→...(规则)...→结论

➢ **逆向推导(自顶向下构造):** 结论→...(规则)...→公理

——目标制导的

2.1 归纳定义-4

- 规则归纳(Rule Induction)
  - P(J)：表示性质P在断言J 可推导时是成立的。
  - 如果P封闭于定义J的规则之下，则P对所有可推导的断言J是满足的。
  - 对于每一规则 $\dfrac{J_1 \cdots J_k}{J}$

    有：如果P(J_1),…, P(J_k)，则P(J).---归纳步

    P(J_1),…, P(J_k) ---归纳假设
  - 规则归纳原理：要证明P(a nat)对所有a nat成立，则只要证明:

    1) P(zero nat)

    2) 假设P(a nat)成立，则P(succ(a) nat)成立

2.1 归纳定义-5

❖ 迭代归纳定义(Iterated Induction Definitions)

➢ 一个归纳定义建立在另一个归纳定义之上

$$\frac{}{\texttt{nil}\ \text{list}} \qquad \frac{a\ \text{nat} \quad b\ \text{list}}{\texttt{cons}(a;b)\ \text{list}} \qquad \textbf{(1.8)}$$

归纳原理

要证明**P(a list)**对所有**a list**成立，则只要证明:

1) **P(nil list).**

2) 假设**P(b list)**成立且**a nat**，则**P(cons(a;b) list)**成立.

2.1 归纳定义-6

- 联立归纳定义(Simultaneous Induction Definitions)
  - 同时定义两个或多个断言

$$\frac{}{\texttt{zero even}} \qquad \frac{a \text{ odd}}{\texttt{succ}(a) \text{ even}} \qquad \frac{a \text{ even}}{\texttt{succ}(a) \text{ odd}} \tag{1.9}$$

归纳原理

要证明P(a even)对所有a even成立以及P(a odd)对所有a odd成立，则只要证明：

1) **P(zero even)**
2) **如果P(a odd)，则P(succ(a) even)成立**
3) **如果P(a even)，则P(succ(a) odd)成立**

2.1 归纳定义-7

❖ 用规则定义函数

- 以下规则定义加法断言 $\mathrm{sum}(a,b,c)$

$$\frac{b\ \mathrm{nat}}{\mathrm{sum}(\mathtt{zero},b,b)} \qquad \frac{\mathrm{sum}(a,b,c)}{\mathrm{sum}(\mathtt{succ}(a),b,\mathtt{succ}(c))} \tag{1.10}$$

定理(PFPL Theorem 1.4)：对于所有的a nat和b nat，存在唯一的c nat使得sum(a,b,c)。

证明：证明分解为

- **(Existence,存在性)如果a nat和b nat，则存在c nat使得sum(a,b,c)。**
- **(Uniqueness,唯一性)如果a nat，b nat，c nat，c' nat，sum(a,b,c)，sum(a,b,c')，则c = c' nat。**

2.1 归纳定义-8

(Existence,存在性)如果a nat和b nat，则存在c nat使得 sum(a,b,c)。

假设P(a nat)表示命题：如果b nat则存在c nat使得sum(a,b,c).现在根据规则(1.2)归纳证明如果a nat，则P(a nat):

1. 证明P(zero nat): 假设b nat并且让c为b，由规则(1.10)可得 sum(zero,b,c).
2. 证明假设P(a nat)，则P(succ(a) nat): 即假设如果b nat则存在c nat使得sum(a,b,c)，现证明如果b' nat则存在c' nat使得 sum(succ(a),b,c').
   假设b' nat ，由归纳假设，存在c nat使得sum(a,b',c). 取 c'=succ(c)，应用规则(1.10)可得sum(succ(a),b',c').

2.1 归纳定义-9

(Uniqueness,唯一性)如果a nat, b nat, c nat, c' nat, sum(a,b,c), sum(a,b,c'), 则c = c' nat。

根据规则(1.10)归纳证明如果sum(a,b,c_1), 则如果sum(a,b,c_2), 那么c_1 = c_2.

1. 假设a=zero且c_1 = b, 对b归纳证明如果sum(zero,b,c_2), 则c_2是b.由(PFPL Lemma1.1),得b=b nat.
2. 假设a=succ(a')且c_1 = succ(c_1'), 其中sum(a',b,c_1'). 对b归纳证明可得如果sum(a,b,c_2), 则c_2 = succ(c_2') nat, sum(a',b,c_2') b.由外层归纳假设c_1' = c_2' nat, 故有c_1 = c_2 nat.

2.1 归纳定义-10

❖ 用规则定义函数

- 以下规则定义加法断言 $\mathrm{sum}(a,b,c)$

$$\frac{b\ \mathrm{nat}}{\mathrm{sum}(\mathtt{zero},b,b,)} \qquad \frac{\mathrm{sum}(a,b,c)}{\mathrm{sum}(\mathtt{succ}(a),b,\mathtt{succ}(c))} \qquad \textbf{(1.10)}$$

- **模式(mode)**：以加法断言为例
  - 模式 $(\forall,\forall,\exists)$: 对于所有的a nat和所有的b nat,存在c nat使得sum(a,b,c).
  - "和唯一"$(\forall,\forall,\exists!)$：对于所有的a nat和所有的b nat，存在唯一的c nat使得sum(a,b,c)。 **sum是其两个参数的全函数**
  - "如果存在则和唯一"$(\forall,\forall,\exists^{\leq 1})$：对于所有的a nat和所有的b nat，最多存在唯一的c nat使得sum(a,b,c)。 **sum是其参数的部分函数**

一般地，全称量化参数视为断言的输入，存在量化参数视为输出.

2.1 归纳定义-11

- 用规则定义函数
  - **模式(mode)**：以加法断言为例
    - “如果存在则和唯一” $(\forall, \forall, \exists^{\leq 1})$：对于<u>所有</u>的**a nat**和<u>所有</u>的**b nat**，<u>最多存在唯一</u>的**c nat**使得**sum(a,b,c)**。 **sum是其参数的部分函数**

    一般地，全称量化参数视为断言的输入，存在量化参数视为输出.

    通常将输出放在输入之后，但是也可以不这样做。例如，
    - “如果存在则和唯一” $(\forall, \exists^{\leq 1}, \forall)$：对于<u>所有</u>的**a nat**和<u>所有</u>的**c nat**，<u>最多存在唯一</u>的**b nat**使得**sum(a,b,c)**。

      自然数的加法有一个（部分）逆函数，即减法。

2.2 假言断言-1

- 直言断言(Categorical judgements)
  - 是关于论域中目标的无条件断言
- 假言断言(Hypothetical judgements) [PFPL, 2]
  - 有一个或多个引起结果(consequent)的假设(hypotheses, assumptions),
  - 可推导的(derivability)断言 $J \vdash K$
    - 对于给定的一组定义直言断言的规则集，上述可推导的断言中，J和K是直言断言，并且在规则集上扩展增加J为新公理可以推导出K.
    - 迭代形式: $J_1 \vdash J_2 \vdash \cdots J_n \vdash K$
      可简写为 $J_1, \cdots, J_n \vdash K$

2.2 假言断言-2

- 可推导的(derivability)断言 $J \vdash K$

  一般用 Γ代表断言的有限序列，则 $\Gamma \vdash K$ 表示K可由 Γ 推导出.

- 推理规则与可推导的断言之间联系紧密

  如果 $\dfrac{J_1 \cdots J_k}{J}$ 是一条基本规则，则断言 $J_1, \cdots, J_n \vdash J$

  是有效的.

  如果 $J_1, \cdots, J_n \vdash J$ 是有效的，则以假设J_i为公理可以推导得到J.

  J的推理规则本质上是一个复合的推理规则，其中J_i为前提，J为结论.

2.2 假言断言-3

[PFPL, 2.1] **Derivability judgements & Inference rules**

$$\frac{J_1 \cdots J_k}{J}$$ **is derivable iff** $J_1, \cdots, J_n \vdash J$

Structural Properties

- **Reflexivity** For every judgement **J**, $\Gamma, J \vdash J$
- **Weakening** If $\Gamma \vdash J$, then $\Gamma, K \vdash J$
- **Exchange** If $\Gamma_1, J_1, J_2, \Gamma_2 \vdash J$, then $\Gamma_1, J_2, J_1, \Gamma_2 \vdash J$
- **Contraction** If $\Gamma, J, J \vdash K$, then $\Gamma, J \vdash K$
- **Transitivity** If $\Gamma, K \vdash J$ and $\Gamma \vdash K$, then $\Gamma \vdash J$

2.2 假言断言-4

- 可接受的(admissibility)断言 $J \models K$

  对于给定的规则集，如果J可从该规则集中推导出，则K 可从规则集中推导出.

[PFPL, 2.2] **Admissibility judgements & Inference rules**

$$\frac{J_1 \cdots J_k}{J} \quad \text{is admissible iff} \quad J_1, \cdots, J_n \models J$$

例如 $\mathrm{succ}(a)\ \mathrm{nat} \models a\ \mathrm{nat}$ **(2.9)**

$$\frac{\mathrm{succ}(a)\ \mathrm{nat}}{a\ \mathrm{nat}}$$ **(2.10)**

是可接受的，但不是可导出的

$\mathrm{succ}(a)\ \mathrm{nat} \not\vdash a\ \mathrm{nat}$ **(2.11)**

可接受的断言具有与可推导的断言相同的结构性质。

2.2 假言断言-5

❖ 条件归纳定义

➢ 由一组形如

$$\frac{\Gamma\Gamma_1 \vdash J_1 \quad \cdots \quad \Gamma\Gamma_n \vdash J_n}{\Gamma \vdash J} \qquad (2.13)$$

的**条件规则**组成.称 Γ 为规则的**全局假设**, Γ_i 为规则的第**i**个前提的**局部假设**.

➢ 若所给的条件规则对全局上下文的选择无限制，则该规则是纯的(**pure**)，可以将全局上下文隐含起来，即

$$\frac{\Gamma_1 \vdash J_1 \quad \cdots \quad \Gamma_n \vdash J_n}{J} \qquad (2.14)$$

2.2 假言断言-6

❖ 条件归纳定义

- 有时有必要限制一个推理规则的全局上下文，使得该规则仅当全局上下文满足指定副条件(side condition)时应用.这样的规则是不纯的(impure).
  这时不能隐含全局上下文。

$$\frac{\Gamma\Gamma_1 \vdash J_1 \quad \cdots \quad \Gamma\Gamma_n \vdash J_n \quad S(\Gamma)}{\Gamma \vdash J} \quad (2.15)$$

S(Γ)是全局上下文上的副条件

2.2 假言断言-7

❖ 条件归纳定义

➢ 以下性质对任何条件归纳定义是可接受的(admissible):

$$\frac{}{\Gamma, J \vdash J} \qquad \frac{\Gamma \vdash J}{\Gamma, K \vdash J} \qquad \frac{\Gamma \vdash K \quad \Gamma, K \vdash J}{\Gamma \vdash J} \qquad \textbf{(2.16)}$$

归纳原理

➢ 为证明对所有的 $\Gamma \vdash J$，$\mathcal{P}(\Gamma \vdash J)$

则需要对每一规则 $\dfrac{\Gamma\Gamma_1 \vdash J_1 \quad \cdots \quad \Gamma\Gamma_n \vdash J_n}{\Gamma \vdash J}$

必须证明：如果 $\mathcal{P}(\Gamma\Gamma_1 \vdash J_1), \cdots, \mathcal{P}(\Gamma\Gamma_n \vdash J_n)$

则 $\mathcal{P}(\Gamma \vdash J)$.

2.3 参数化断言-1

参数化断言(Parametric judgements) [PFPL, 3]

- 允许用一组有限参数集扩展对象的域
- 推导模式(derivation scheme)：包含指定参数的推导

❖ 参数化(Parameterization)

- 设$\mathcal{X}$是一组有限的参数集合，$\mathcal{J}$ 是一个假言或直言断言. 参数化断言 $\mathcal{X}\mid\mathcal{J}$ 示断言 在$\mathcal{J}$参数 下$\mathcal{X}$是满足的.
- 参数化断言的证明由断言$\mathcal{J}$(其中$\mathcal{X}$里的参数可以用作对象)的参数化推导或推导模式$\nabla_{\mathcal{X}}$组成.
- 例如， $x \mid x \text{ nat} \vdash \mathtt{succ}(\mathtt{succ}(x)) \text{ nat}$ **(3.1)**

2.3 参数化断言-2

[PFPL, 3.2] Structural Properties

- **Proliferation** If $\mathcal{X}|\mathcal{J}$ and $x \notin \mathcal{X}$, then $\mathcal{X}, x|\mathcal{J}$.
- **Swapping** If $\mathcal{X}_1, x_1, x_2, \mathcal{X}_2|\mathcal{J}$ then $\mathcal{X}_1, x_2, x_1, \mathcal{X}_2|\mathcal{J}$
- **Duplication** If $\mathcal{X}, x, x|\mathcal{J}$, then $\mathcal{X}, x|\mathcal{J}$
- **Renaming** If $\mathcal{X}, x|\mathcal{J}_x$, then $\mathcal{X}, y|\mathcal{J}_y$, provided that $y \notin \mathcal{X}$.

2.3 参数化断言-3

❖ 参数化归纳定义(Parametric Inductive Definitions)

➢ 由一组形如 $$\frac{\mathcal{X}\mathcal{X}_1|\Gamma\Gamma_1 \vdash J_1 \quad \cdots \quad \mathcal{X}\mathcal{X}_n|\Gamma\Gamma_n \vdash J_n}{\mathcal{X}|\Gamma \vdash J} \quad (3.5)$$
的参数化规则组成.称 $\mathcal{X}$ 为规则的全局参数，$\mathcal{X}_i$ 为规则第i个前提的新的局部参数(fresh local parameters).

➢ Freshness：将局部参数与全局参数分离开来以避免它们之间的冲突.

➢ 全局上下文 $\mathcal{X}|\Gamma$，第i个前提的局部上下文 $\mathcal{X}_i|\Gamma_i$

2.3 参数化断言-4

❖ 参数化归纳定义(Parametric Inductive Definitions)

➢ Pure paremetric rule

$$\frac{\mathcal{X}_1|\Gamma_1 \vdash J_1 \quad \cdots \quad \mathcal{X}_n|\Gamma_n \vdash J_n}{J} \qquad (3.6)$$

归纳原理

➢ 为证明对所有的$\mathcal{X}|\Gamma \vdash J$，$\mathcal{P}(\mathcal{X}|\Gamma \vdash J)$

则需要对每一规则 $\dfrac{\mathcal{X}\mathcal{X}_1|\Gamma\Gamma_1 \vdash J_1 \quad \cdots \quad \mathcal{X}\mathcal{X}_n|\Gamma\Gamma_n \vdash J_n}{\mathcal{X}|\Gamma \vdash J}$

必须证明如果 $\mathcal{P}(\mathcal{X}\mathcal{X}_1\Gamma\Gamma_1 \vdash J_1), \cdots, \mathcal{P}(\mathcal{X}\mathcal{X}_n|\Gamma\Gamma_n \vdash J_n)$

则 $\mathcal{P}(\mathcal{X}|\Gamma \vdash J)$.

Homework

1. [PFPL, 1] 1.9 Exercises 1.
2. [PFPL, 1] 1.9 Exercises 2.

Thanks!