

λD 中的数学

Mathematics in λD

报告人：许博

期望证明的引理

偏序关系

令 \leq 是集合 S 上的一个偏序关系, 则 \leq 满足:

1. 自反性: $\forall x \in S, x \leq x$
2. 反对称性: $\forall x, y \in S, x \leq y \Rightarrow y \leq x$
3. 传递性: $\forall x, y, z \in S, (x \leq y \wedge y \leq z) \Rightarrow x \leq z$

定义 12.1.1 (最小元)

令 S 是一个集合, 以及 \leq 是一个在 S 上的二元关系. 对 $m \in S$, 如果 $\forall n \in S (m \leq n)$, 则 m 是 S 中的一个最小元。

引理 12.1.2 (最小元唯一)

令 S 是一个由关系 \leq 偏序的集合. 若 S 关于 \leq 有一个最小元, 则这个最小元唯一。

期望的证明

非形式化证明

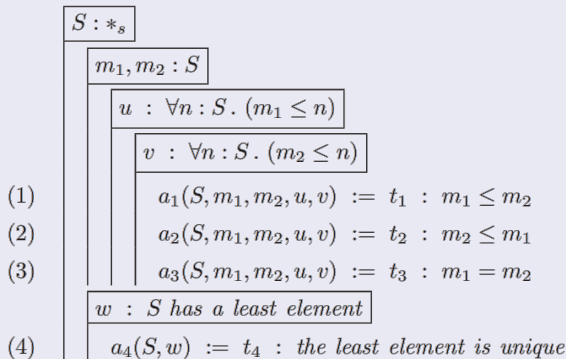
假设 m_1 和 m_2 是 S 的成员并且两者都是最小元。

则 $\forall n \in S (m_1 \leq n)$ 且 $\forall n \in S (m_2 \leq n)$ 。

特别地, $m_1 \leq m_2$ 且 $m_2 \leq m_1$, 由 \leq 的反对称性可得, $m_1 = m_2$ 。

因此, 如果 S 具有一个最小元, 则这个元素唯一。

尝试在 λD 中形式化证明



目录

1 相等

2 序

3 唯一存在

莱布尼兹相等

如果两个对象在所有可能的环境中都是不可区分的，则这两个对象是相等的。
形式化为： $\prod P : S \rightarrow *_{\mathcal{P}}. (Px \Leftrightarrow Py)$

相等的自反性

- | | |
|-----|---|
| | $S : *_{\mathcal{S}}$ |
| | $x : S$ |
| | $y : S$ |
| (1) | $eq(S, x, y) := \prod P : S \rightarrow *_{\mathcal{P}}. (Px \Leftrightarrow Py) : *_{\mathcal{P}}$ |
| | $P : S \rightarrow *_{\mathcal{P}}$ |
| (2) | $a_2(S, x, P) := \dots? \dots : Px \Leftrightarrow Px$ |
| (3) | $eq-refl(S, x) := \lambda P : S \rightarrow *_{\mathcal{P}}. a_2(S, x, P) : eq(S, x, x)$ |

相等的替换性

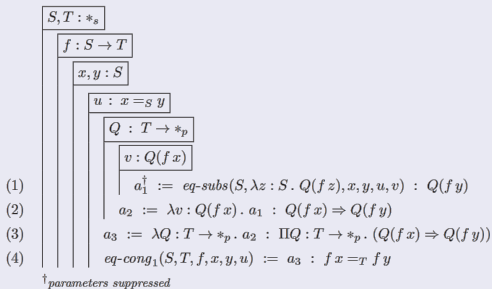
对于所有在 S 上的谓词 P ，如果 $x =_S y$ 且 Px 成立，则 Py 也成立

- | | |
|-----|--|
| | $S : *_{\mathcal{S}}$ |
| | $P : S \rightarrow *_{\mathcal{P}}$ |
| | $x, y : S$ |
| | $u : x =_S y$ |
| (1) | $a_1(S, P, x, y, u) := uP : Px \Leftrightarrow Py$ |
| (2) | $a_2(S, P, x, y, u) := \Leftrightarrow-el_1(Px, Py, a_1(S, P, x, y, u)) : Px \Rightarrow Py$ |
| | $v : Px$ |
| (3) | $eq-subst(S, P, x, y, u, v) := a_2(S, P, x, y, u) v : Py$ |

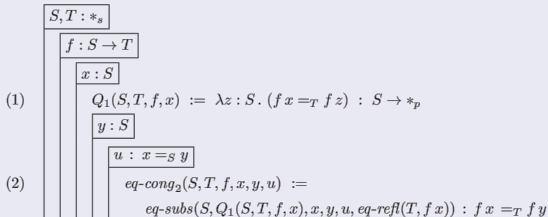
相等的一致性

对于所有的函数 $f: S \rightarrow T$ 以及 $x, y: S$, 如果 $x =_S y$, 则 $fx =_T fy$
 展开为: $fx =_T fy$ 为 $\Pi Q: T \rightarrow *_p. (Q(fx) \Leftrightarrow Q(fy))$

谓词为 $\lambda z: S. Q(fz)$, 由替换性



谓词为 $\lambda z: S. (fx =_T fz)$, 由自反性及替换性



相等的对称性

$S : *_s$
 $x : S$
 (1) $Q_2(S, x) := \lambda z : S. (z =_S x) : S \rightarrow *_p$
 (2) $a_2(S, x) := eq-refl(S, x) : x =_S x$
 $y : S$
 $u : x =_S y$
 (3) $eq-sym(S, x, y, u) :=$
 $eq-subst(S, Q_2(S, x), x, y, u, a_2(S, x)) :$
 $y =_S x$
 (4) $a_4(S) := \lambda x, y : S. \lambda u : (x =_S y). eq-sym(S, x, y, u) :$
 $\forall x, y : S. (x =_S y \Rightarrow y =_S x)$

相等的传递性

$S : *_s$
 $x : S$
 (1) $Q_3(S, x) := \lambda w : S. (x =_S w) : S \rightarrow *_p$
 $y, z : S$
 $u : x =_S y$
 $v : y =_S z$
 (2) $eq-trans(S, x, y, z, u, v) :=$
 $eq-subst(S, Q_3(S, x), y, z, v, u) : x =_S z$
 (3) $a_3(S) := \lambda x, y, z : S. \lambda u : (x =_S y). \lambda v : (y =_S z). eq-trans(S, x, y, z, u, v) :$
 $\forall x, y, z : S. (x =_S y \Rightarrow y =_S z \Rightarrow x =_S z)$

形式化定义 “偏序”

 $S : *_s$ $\leq : S \rightarrow S \rightarrow *_p$

Notation: $x \leq_S y$ for $\leq x y$ (on S)

$$(1) \quad \text{refl}(S, \leq) := \forall x : S. (x \leq_S x) : *_p$$

$$(2) \quad \text{trans}(S, \leq) := \\ \forall x : S. \forall y : S. \forall z : S. (x \leq_S y \Rightarrow y \leq_S z \Rightarrow x \leq_S z) : *_p$$

$$(3) \quad \text{pre-ord}(S, \leq) := \text{refl}(S, \leq) \wedge \text{trans}(S, \leq) : *_p$$

$$(4) \quad \text{antisymm}(S, \leq) := \forall x : S. \forall y : S. (x \leq_S y \Rightarrow y \leq_S x \Rightarrow x =_S y) : *_p$$

$$(5) \quad \text{part-ord}(S, \leq) := \text{pre-ord}(S, \leq) \wedge \text{antisymm}(S, \leq) : *_p$$

证明 $x \leq y \wedge y \leq x \Rightarrow x = y$

(a)	$S : *_s$
(b)	$\leq : S \rightarrow S \rightarrow *_p$
(c)	$r : \text{part-ord}(S, \leq)$
(d)	$m_1, m_2 : S$
(e)	$u : \forall n : S. (m_1 \leq_S n) \mid v : \forall n : S. (m_2 \leq_S n)$
(1)	$a_1^\dagger := u m_2 : \underline{m_1 \leq_S m_2}$
(2)	$a_2 := v m_1 : \underline{m_2 \leq_S m_1}$
(3)	$a_3 := r : \underline{\text{pre-ord}(S, \leq) \wedge \text{antisymm}(S, \leq)}$
(4)	$a_4 := \wedge\text{-el}_2(\text{pre-ord}(S, \leq), \text{antisymm}(S, \leq), a_3) : \underline{\text{antisymm}(S, \leq)}$
(5)	$a_5 := a_4 : \underline{\forall x : S. \forall y : S. (x \leq_S y \Rightarrow y \leq_S x \Rightarrow x =_S y)}$
(6)	$a_6 := a_5 m_1 m_2 : \underline{m_1 \leq_S m_2 \Rightarrow m_2 \leq_S m_1 \Rightarrow m_1 =_S m_2}$
(7)	$a_7 := a_6 a_1 : \underline{m_2 \leq_S m_1 \Rightarrow m_1 =_S m_2}$
(8)	$a_8 := a_7 a_2 : \underline{m_1 =_S m_2}$
(9)	$a_9(S, \leq, r) := \lambda m_1, m_2 : S. \lambda u : \dots \lambda v : \dots a_8 : \underline{\forall m_1, m_2 : S. ((\forall n : S. (m_1 \leq_S n)) \Rightarrow (\forall n : S. (m_2 \leq_S n)) \Rightarrow m_1 =_S m_2)}$

[†]parameters suppressed

形式化 “最小元” 定义

$$\begin{array}{l}
 \text{(a)} \quad \boxed{S : *_{\mathcal{S}} \mid \leq : S \rightarrow S \rightarrow *_{\mathcal{P}} \mid m : S} \\
 \text{(1)} \quad \boxed{Least(S, \leq, m) := \forall n : S. (m \leq n) : *_{\mathcal{P}}}
 \end{array}$$

形式化 “至少存在一个”, “至多存在一个” 以及 “只存在一个”

$$\begin{array}{l}
 \boxed{S : *_{\mathcal{S}}} \\
 \boxed{P : S \rightarrow *_{\mathcal{P}}} \\
 \text{(1)} \quad \exists(S, P) := \Pi A : *_{\mathcal{P}}. ((\forall x : S. (P x \Rightarrow A)) \Rightarrow A) : *_{\mathcal{P}} \\
 \text{(2)} \quad \exists^{\geq 1}(S, P) := \exists(S, P) : *_{\mathcal{P}} \\
 \text{(3)} \quad \exists^{\leq 1}(S, P) := \forall y, z : S. (P y \Rightarrow P z \Rightarrow (y =_S z)) : *_{\mathcal{P}} \\
 \text{(4)} \quad \exists^1(S, P) := \exists^{\geq 1}(S, P) \wedge \exists^{\leq 1}(S, P) : *_{\mathcal{P}}
 \end{array}$$

证明仅存在一个最小元

$$a_9 : \forall m_1, m_2 : S. ((\forall n : S. (m_1 \leq_S n)) \Rightarrow (\forall n : S. (m_2 \leq_S n))) \Rightarrow m_1 =_S m_2$$

$$\vdots$$

$$(10) \quad a_{10} := a_9[Fig. 12.9] : \exists^{\leq 1} x : S. Least(S, \leq, x)$$

$$(d) \quad \boxed{w : \exists^{\geq 1} x : S. Least(S, \leq, x)}$$

$$(11) \quad \boxed{\begin{aligned} a_{11}(S, \leq, r, w) &:= \wedge\text{-in}(\exists^{\geq 1} \dots, \exists^{\leq 1} \dots, w, a_{10}) : \\ &\quad \exists^1 x : S. Least(S, \leq, x) \end{aligned}}$$

描述符 ι

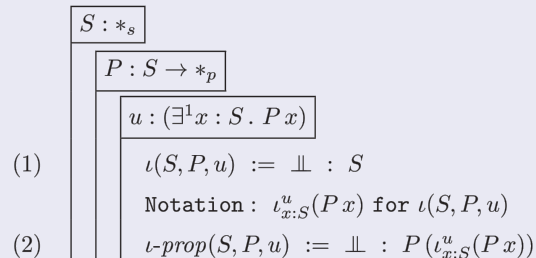
a minimum, the minimum

传统数学中，通过一个名字代表一个最小元，比如说 S 关于 \leq 的 *the minimum*。需要注意的是，如果唯一性未证明，则只能说 *a minimum*

使用描述符 ι 命名唯一存在的元素：

$\iota_{x \in S}(P(x))$ 表示 S 中唯一具有满足 $P(x)$ 的成员 x 。因此，集合 S 中关于关系 \leq 的 *the minimum* 是 $\iota_{s \in S}(Least(S, \leq, m))$ 。

定义描述符 ι



应用描述符 ι 的一个例子

引理 12.7.1

令 S 是一个集合, P 是 S 上的一个谓词, 假设 $\exists_{x \in S}^1(P(x))$, 则
 $\forall_{z \in S}(P(z)) \Rightarrow (z =_S \iota_{x \in S}(P(x)))$

- (a) $S : *_s \mid P : S \rightarrow *_p \mid u : (\exists^1 x : S . P x)$
- (1) $a_1^\dagger := u : (\exists^{\geq 1} x : S . P x \wedge \exists^{\leq 1} x : S . P x)$
- (2) $a_2 := \wedge\text{-el}_2(\exists^{\geq 1} x : S . P x, \exists^{\leq 1} x : S . P x, u) : \exists^{\leq 1} x : S . P x$
- (3) $a_3 := a_2 : \forall x, y : S . (P x \Rightarrow P y \Rightarrow (x =_S y))$
- (b) $z : S \mid v : P z$
- (4) $a_4 := a_3 z (\iota_{x:S}^u(P x)) v \iota\text{-prop}(S, P, u) : z =_S \iota_{x:S}^u(P x)$
- (5) $a_5(S, P, u) := \lambda z : S . \lambda v : P z . a_4 : \forall z : S . (P z \Rightarrow (z =_S \iota_{x:S}^u(P x)))$

† parameters suppressed

使用 ι 重新表述并证明引理 12.1.2

引理 12.1.2 (最小元唯一)

令 S 是一个由关系 \leq 偏序的集合。若 S 关于 \leq 有一个最小元, 则这个最小元唯一。

重新表述

令 \leq 是集合 S 上的偏序关系; 如果 S 有最小元 x , 则 x 是 S 中关于 \leq 的 *the minimum*

$$a_{11} : \exists^1 x : S. \text{Least}(S, \leq, x)$$

$$a_5 : \forall z : S. (Pz \Rightarrow (z =_S \iota_{x.S}^u(Px)))$$

证明

- | | |
|-----|--|
| (a) | $S : *_s \mid \leq : S \rightarrow S \rightarrow *_p \mid r : \text{part-ord}(S, \leq)$ |
| (b) | $w : \exists^{\geq 1} x : S. \text{Least}(S, \leq, x)$ |
| (1) | $\text{Min}(S, \leq, r, w) :=$ $\iota(S, \lambda m : S. \text{Least}(S, \leq, m), a_{11}[\text{Fig. 12.15}](S, \leq, r, w)) : S$ |
| (2) | $a_2(S, \leq, r, w) :=$ $a_5[\text{Fig. 12.17}](S, \lambda m : S. \text{Least}(S, \leq, m), a_{11}[\text{Fig. 12.15}](S, \leq, r, w)) :$ $\forall x : S. (\text{Least}(S, \leq, x) \Rightarrow (x =_S \text{Min}(S, \leq, r, w)))$ |