λD 中的数学：初次尝试

Mathematics in λD: A First Attempt

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：$\forall x, y \in S,\ x \leq y \Rightarrow y \leq x \Rightarrow x =_S y$
3. 传递性：$\forall x, y, z \in S,\ x \leq y \Rightarrow y \leq z \Rightarrow x \leq z$

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

$$\boxed{S : *_s}$$

$$\boxed{m_1, m_2 : S}$$

$$\boxed{u \ : \ \forall n : S \, . \, (m_1 \leq n)}$$

$$\boxed{v \ : \ \forall n : S \, . \, (m_2 \leq n)}$$

(1) $a_1(S, m_1, m_2, u, v) \ := \ t_1 \ : \ m_1 \leq m_2$

(2) $a_2(S, m_1, m_2, u, v) \ := \ t_2 \ : \ m_2 \leq m_1$

(3) $a_3(S, m_1, m_2, u, v) \ := \ t_3 \ : \ m_1 = m_2$

$$\boxed{w \ : \ S \textit{ has a least element}}$$

(4) $a_4(S, w) \ := \ t_4 \ : \ \textit{the least element is unique}$

目录

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：$\Pi P : S \to *_p . (Px \Leftrightarrow Py)$

相等的自反性

$S : *_s$

$x : S$

$y : S$

(1) $eq(S,x,y) \ := \ \Pi P : S \to *_p . \ (P\,x \Leftrightarrow P\,y) \ : \ *_p$

$P \ : \ S \to *_p$

(2) $a_2(S,x,P) \ := \ \ldots ? \ldots \ : \ P\,x \Leftrightarrow P\,x$

(3) $eq\text{-}refl(S,x) \ := \ \lambda P : S \to *_p . \ a_2(S,x,P) \ : \ eq(S,x,x)$

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

$S : *_s$

$P : S \to *_p$

$x, y : S$

$u \ : \ x =_S y$

(1) $a_1(S,P,x,y,u) \ := \ u\,P \ : \ P\,x \Leftrightarrow P\,y$

(2) $a_2(S,P,x,y,u) \ := \ \Leftrightarrow\text{-}el_1(P\,x, P\,y, a_1(S,P,x,y,u)) \ : \ P\,x \Rightarrow P\,y$

$v : P\,x$

(3) $eq\text{-}subs(S,P,x,y,u,v) \ := \ a_2(S,P,x,y,u)\ v \ : P\,y$

相等的一致性

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

谓词为 $\lambda z : S . Q(fz)$，由替换性

$$
\begin{array}{ll}
 & S, T : *_s \\
 & \quad f : S \to T \\
 & \quad\quad x, y : S \\
 & \quad\quad\quad u : x =_S y \\
 & \quad\quad\quad\quad Q : T \to *_p \\
 & \quad\quad\quad\quad\quad v : Q(f\,x) \\
(1) & \quad\quad\quad\quad\quad a_1^\dagger := \textit{eq-subs}(S, \lambda z : S . Q(f\,z), x, y, u, v) \; : \; Q(f\,y) \\
(2) & \quad\quad\quad\quad a_2 := \lambda v : Q(f\,x) . a_1 \; : \; Q(f\,x) \Rightarrow Q(f\,y) \\
(3) & \quad\quad\quad a_3 := \lambda Q : T \to *_p . a_2 \; : \; \Pi Q : T \to *_p . (Q(f\,x) \Rightarrow Q(f\,y)) \\
(4) & \quad\quad\quad \textit{eq-cong}_1(S, T, f, x, y, u) := a_3 \; : \; f\,x =_T f\,y
\end{array}
$$

†*parameters suppressed*

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

$$
\begin{array}{ll}
 & S, T : *_s \\
 & \quad f : S \to T \\
 & \quad\quad x : S \\
(1) & \quad\quad Q_1(S, T, f, x) := \lambda z : S . (f\,x =_T f\,z) \; : \; S \to *_p \\
 & \quad\quad\quad y : S \\
 & \quad\quad\quad\quad u : x =_S y \\
(2) & \quad\quad\quad\quad \textit{eq-cong}_2(S, T, f, x, y, u) := \\
 & \quad\quad\quad\quad\quad \textit{eq-subs}(S, Q_1(S, T, f, x), x, y, u, \textit{eq-refl}(T, f\,x)) \; : \; f\,x =_T f\,y
\end{array}
$$

相等的对称性

$\boxed{S : *_s}$

$\boxed{x : S}$

(1) $Q_2(S,x) := \lambda z : S \,.\, (z =_S x) \;:\; S \to *_p$

(2) $a_2(S,x) := \textit{eq-refl}(S,x) \;:\; x =_S x$

$\boxed{y : S}$

$\boxed{u \;:\; x =_S y}$

(3) $\textit{eq-sym}(S,x,y,u) :=$

$\textit{eq-subs}(S,\, Q_2(S,x)\,, x, y, u,\, a_2(S,x)) \;:$

$y =_S x$

(4) $a_4(S) := \lambda x, y : S \,.\, \lambda u : (x =_S y) \,.\, \textit{eq-sym}(S,x,y,u) \;:$

$\forall x, y : S \,.\, (x =_S y \Rightarrow y =_S x)$

相等的传递性

$\boxed{S : *_s}$

$\boxed{x : S}$

(1) $Q_3(S,x) := \lambda w : S \,.\, (x =_S w) \;:\; S \to *_p$

$\boxed{y, z : S}$

$\boxed{u \;:\; x =_S y}$

$\boxed{v \;:\; y =_S z}$

(2) $\textit{eq-trans}(S,x,y,z,u,v) :=$

$\textit{eq-subs}(S,\, Q_3(S,x)\,, y, z, v, u) \;:\; x =_S z$

(3) $a_3(S) := \lambda x, y, z : S \,.\, \lambda u : (x =_S y) \,.\, \lambda v : (y =_S z) \,.\, \textit{eq-trans}(S,x,y,z,u,v) \;:$

$\forall x, y, z : S \,.\, (x =_S y \;\Rightarrow\; y =_S z \;\Rightarrow\; x =_S z)$

形式化定义“偏序”

$$
\begin{array}{ll}
 & \boxed{S : *_s} \\
 & \quad \boxed{\leq : S \to S \to *_p} \\
 & \quad\quad \texttt{Notation}: \ x \leq_S y \ \texttt{for} \ \leq x\, y \ (\text{on } S) \\
(1) & \quad\quad \mathit{refl}(S, \leq) \ := \ \forall x : S \,.\, (x \leq_S x) \ : \ *_p \\
(2) & \quad\quad \mathit{trans}(S, \leq) \ := \\
 & \quad\quad\quad \forall x : S \,.\, \forall y : S \,.\, \forall z : S \,.\, (x \leq_S y \Rightarrow y \leq_S z \Rightarrow x \leq_S z) : *_p \\
(3) & \quad\quad \mathit{pre\text{-}ord}(S, \leq) \ := \ \mathit{refl}(S, \leq) \wedge \mathit{trans}(S, \leq) \ : \ *_p \\
(4) & \quad\quad \mathit{antisymm}(S, \leq) \ := \ \forall x : S \,.\, \forall y : S \,.\, (x \leq_S y \Rightarrow y \leq_S x \Rightarrow x =_S y) \ : \ *_p \\
(5) & \quad\quad \mathit{part\text{-}ord}(S, \leq) \ := \ \mathit{pre\text{-}ord}(S, \leq) \wedge \mathit{antisymm}(S, \leq) \ : \ *_p
\end{array}
$$

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

(a) $\boxed{S : *_s}$

(b) $\boxed{\leq : S \to S \to *_p}$

(c) $\boxed{r : \textit{part-ord}(S, \leq)}$

(d) $\boxed{m_1, m_2 : S}$

(e) $\boxed{u : \forall n : S\,.\,(m_1 \leq_S n) \mid v : \forall n : S\,.\,(m_2 \leq_S n)}$

(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) $a_3 := r : \underline{\textit{pre-ord}(S, \leq) \wedge \textit{antisymm}(S, \leq)}$

(4) $a_4 := \wedge\text{-}el_2(\textit{pre-ord}(S, \leq), \textit{antisymm}(S, \leq), a_3) :$
$\underline{\textit{antisymm}(S, \leq)}$

(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) $a_9(S, \leq, r) := \lambda m_1, m_2 : S\,.\,\lambda u : \ldots\,.\,\lambda v : \ldots\,.\,a_8 :$
$\underline{\forall m_1, m_2 : S\,.\,((\forall n : S\,.\,(m_1 \leq_S n)) \Rightarrow (\forall n : S\,.\,(m_2 \leq_S n)) \Rightarrow}$
$\underline{m_1 =_S m_2)}$

† *parameters suppressed*

形式化“最小元”定义

$$\begin{array}{ll} \text{(a)} & \boxed{S : *_s \mid \ \leq : S \to S \to *_p \mid m : S} \\ \text{(1)} & \quad Least(S, \leq, m) \ := \ \forall n : S \, . \, (m \leq n) \ : \ *_p \end{array}$$

形式化“至少存在一个”，“至多存在一个”以及“只存在一个”

$$\boxed{S : *_s}$$

$$\boxed{P : S \to *_p}$$

$$\begin{array}{ll} (1) & \exists(S, P) \ := \ \Pi A : *_p \, . \, ((\forall x : S \, . \, (P\, x \Rightarrow A)) \Rightarrow A) \ : \ *_p \\ (2) & \exists^{\geq 1}(S, P) \ := \ \exists(S, P) \ : \ *_p \\ (3) & \exists^{\leq 1}(S, P) \ := \ \forall y, z : S \, . \, (P\, y \Rightarrow P\, z \Rightarrow (y =_S z)) \ : \ *_p \\ (4) & \exists^{1}(S, P) \ := \ \exists^{\geq 1}(S, P) \wedge \exists^{\leq 1}(S, P) \ : \ *_p \end{array}$$

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) $a_{10} := a_{9[Fig.\ 12.9]} : \exists^{\leq 1} x : S\ .\ Least(S, \leq, x)$

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

(11) $a_{11}(S, \leq, r, w) := \wedge\text{-}in(\exists^{\geq 1} \ldots, \exists^{\leq 1} \ldots, w, a_{10}) :$

$\exists^1 x : S\ .\ Least(S, \leq, x)$

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

$\boxed{S : *_s}$

$\quad \boxed{P : S \to *_p}$

$\quad\quad \boxed{u : (\exists^1 x : S \,.\, P\,x)}$

(1) $\quad\quad\quad \iota(S,P,u) \;:=\; \perp\!\!\!\perp \;:\; S$

$\quad\quad\quad \texttt{Notation}: \; \iota^{u}_{x:S}(P\,x)$ for $\iota(S,P,u)$

(2) $\quad\quad\quad \iota\text{-}prop(S,P,u) \;:=\; \perp\!\!\!\perp \;:\; P\,(\iota^{u}_{x:S}(P\,x))$

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 $\exists^1_{x\in S}(P(x))$，则 $\forall_{z\in S}(P(z)) \Rightarrow (z =_S \iota_{x\in S}(P(x)))$

(a) $\boxed{S : *_s \mid P : S \to *_p \mid u : (\exists^1 x : S \,.\, P\,x)}$

(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) $\boxed{z : S \mid v : P\,z}$

(4) $a_4 := a_3\ z\ (\iota^u_{x:S}(P\,x))\ v\ \iota\text{-}prop(S, P, u) : z =_S \iota^u_{x:S}(P\,x)$

(5) $a_5(S, P, u) := \lambda z : S \,.\, \lambda v : P\,z \,.\, a_4 : \forall z : S \,.\, (P\,z \Rightarrow (z =_S \iota^u_{x:S}(P\,x)))$

† *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*

$$a_{11} : \exists^1 x : S.Least(S, \leq, x)$$
$$a_5 : \forall z : S.(Pz \Rightarrow (z =_S \iota^u_{x:S}(Px)))$$

证明

(a) $S : *_s \mid \leq : S \to S \to *_p \mid r : part\text{-}ord(S, \leq)$

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

(1) $Min(S, \leq, r, w) :=$
$\iota(S, \lambda m : S \,.\, Least(S, \leq, m), a_{11\,[Fig.\ 12.15]}(S, \leq, r, w)) : S$

(2) $a_2(S, \leq, r, w) :=$
$a_{5\,[Fig.\ 12.17]}(S, \lambda m : S \,.\, Least(S, \leq, m), a_{11\,[Fig.\ 12.15]}(S, \leq, r, w)) :$
$\forall x : S \,.\, (Least(S, \leq, x) \Rightarrow (x =_S Min(S, \leq, r, w)))$