12 λD 中的数学：第一个尝试

Mathematics in λD: a first attempt

读书笔记

许博

1 疑问

1. P260, Remark 12.2.1 中，为何定义 $\Pi P : S \to *_p.(Px \Rightarrow Py)$ 也可以表示 $x = y$?

2 先举个例子

第十一章中，我们在 λD 中表示了逻辑。在本章中，将转向数学（mathematics）。尽管逻辑的推导框架对数学至关重要，因为逻辑包含了推理的原则，但是数学本身要比单纯的逻辑多的多。

本章以一个关于偏序集合的例子开始，即证明在这样的集合中只存在至多一个最小元。一个在集合 S 上的关系 R 如果满足自反性，反对称性和传递性，则这个关系是偏序的。

Definition 12.1.1 Let S be a set and $\leq$ a binary relation on S. Then $m \in S$ is a *least element* of S with respect to $\leq$ if $\forall_{n \in S}(m \leq n)$.

Lemma 12.1.2 *Let S be a set, partially ordered by $\leq$. Assume that S has a least element with respect to $\leq$. Then this least element is unique.*

Proof Assume that m_1 and m_2 are elements of S and that both are *least* elements. Then $\forall_{n \in S}(m_1 \leq n)$ and $\forall_{n \in S}(m_2 \leq n)$. In particular, $m_1 \leq m_2$ and $m_2 \leq m_1$. Hence, $m_1 = m_2$, by antisymmetry of $\leq$. It follows that, if S has a least element, then this element is unique. □

在 λD 中形式化这个证明：

$S : *_s$

$m_1, m_2 : S$

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

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

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

$w \ : \ S \ has \ a \ least \ element$

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

Figure 12.1 A first attempt of proving Lemma 12.1.2 in λD

注意到其中存在的几个问题。有一些可以以直观的方式解决：
- 符号 '≤' 表示在 S 上的一个任意的偏序关系。这些隐含的假设会在章节 12.4 中明确的表示。
- 全称量词 ∀ 在 λD 中被编码为 Π。
- 解决未知项 t_1 和 t_2 代表什么：应是 ∀-消去规则的实例，所以令 $t_1 \equiv \forall\text{-}el(S, \lambda x : S.m_1 \leq x, u, m_2)$ 以及 $t_2 \equiv \forall\text{-}el(S, \lambda y : S.m_2 \leq y, v, m_1)$，或者简单地令 $t_1 \equiv um_2$ 以及 $t_2 \equiv vm_1$。

剩下的问题似乎更加重要：
Q1 符号 '=' 表示了基本的相等关系，作为数学中许多领域的基础，但尚未是我们系统的一部分，如何补足这点？
Q2 行 (3) 中 t_3 代表什么？
Q3 如何表达 S 拥有一个最小元？
Q4 如何表达最小元的唯一性？
Q5 如何证明最小元的唯一性，也即 t_4 是什么？

3 相等

相等显然是两个参数之间的关系：对于一对元素 x 和 y，有命题 $x = y$。又因为在类型理论中，每个元素都应具有一个类型；所以假设 S 是 x 和 y 的类型。故我们可以将相等看作是在 S 上的二元谓词。写作 $x =_S y$ 以表示 S 中的 x 和 y 相等。

所以，相等是一个参数化的二元关系：对每一个类型 S，有一个相等关

系 $=_S: S \to S \to *$，作用于类型为 S 的项。

现在，核心问题是：S 中的元素 x 和 y“相等”意味着什么？德国数学家莱布尼兹（G.W. Leibniz，1646-1716）给出的一个富有哲学的答案是，如果两个对象在所有可能的环境中都是不可分辨的，则这两个对象是相等的。可以更简洁地表示为：“对任意在 S 上的谓词 P，Px 的有效性等价于 Py 的有效性”，也即，对于给定的 P，要么 Px 和 Py 都成立，要么两者都不成立。在这种情况下，没有可能分辨 x 和 y，故两者相等。

莱布尼兹对于相等的看法可以作为描述性定义在 λD 中进行形式化，形式化地定义 $eq(S,x,y)$ 表示 S 中的元素 x 和 y 的相等，为

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

甚至更为简单的定义也可以，即：

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

使用图 12.2 显示这个被定义的相等时一个满足自反性的关系。使用名字 $eq\text{-}refl(S,x)$ 表示自反性的证明。

$S : *_s$

$x : S$

$y : S$

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

$P \;:\; S \to *_p$

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

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

Figure 12.2 Definition of equality, and the reflexivity property for equality

需要注意的是，我们得到的是相等的二阶定义，因为 Π 抽象的谓词 $P : S \to * : \Box$ 是二阶的，所以公式中的 Π 是一个二阶全称量词。

在图 12.2 中的推导中存在一个空，即行 (2) 中，$Px \Leftrightarrow Px$ 的证明，有两种方式解决：

(1) 特定的方法（ad-hoc approach）：也即找到 $Px \Leftrightarrow Px$ 的成员，使用表达式 $\Leftrightarrow -in(Px, Px, \lambda u : Px.u, \lambda u : Px.u)$ 即可。

(2) 通用方法：首先证明一个引理，即 $A \Leftarrow A$ 对于任意的 $A : *_p$ 都成立，命名这个证明为 $\Leftrightarrow -refl(A)$，然后使用表达式 $\Leftrightarrow -refl(Px)$ 填空即可。

为便于阅读，使用记号 $x =_S y$ 表示 $eq(S,x,y)$。

而相等还满足替代性（substitutivity），也即“对所有在 S 上的谓词 P，

如果 $x =_S y$ 且 Px 成立，则 Py" 也成立，则当在任意命题中出现的 t_1 以及 $t_1 =_S t_2$，使用 t_2 替换 t_1 不影响命题的真值。

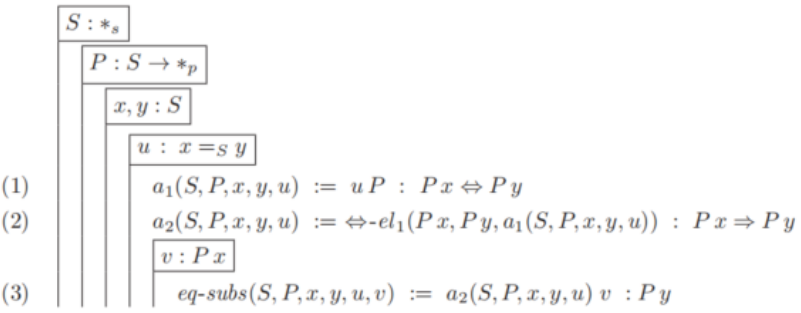

Figure 12.4 Substitutivity as property of equality

4 相等的一致性

一致性与替代性相似，但一致性关注以集合而非命题作为域的函数。一致性即“对所有的函数 $f : S \to T$ 且 $x, y : S$，如果 $x =_S y$，则 $fx =_T fy$”。

我们将使用 $x =_S y$ 推导结果 $fx =_T fy$，因此需要找到一个合适的谓词。首先展开目标 $fx =_T fy$ 为 $\Pi Q : T \to *_p.(Q(fx) \Leftrightarrow Q(fy))$。

第一种方式，令谓词为 $\lambda z : S.Q(fz)$，由替代性可以得到 $Q(fy)$，证明过程如下：

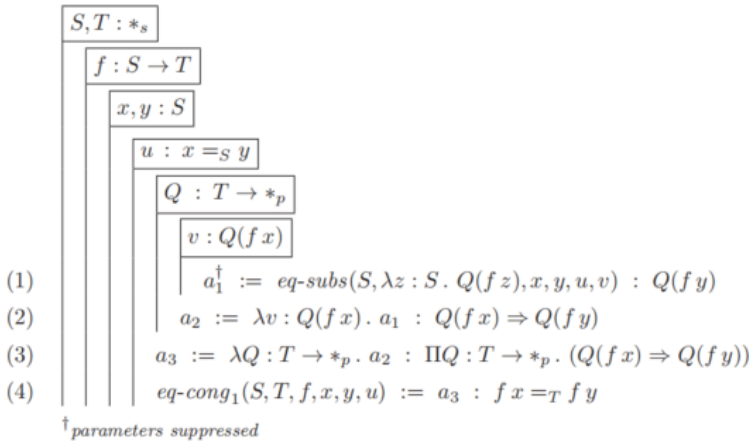

Figure 12.5 First proof of the congruence property for equality

第二种方式，令谓词为 $\lambda z : S.(fx =_T fz)$，由自反性可以得到 $fx =_T fx$，

再由替代性可以得到 $fx =_T fy$，需要注意的是，第一个 x 是抽象中的自由变量，证明过程如下：

$S, T : *_s$

$f : S \to T$

$x : S$

(1) $Q_1(S,T,f,x) := \lambda z : S\,.\,(f\,x =_T f\,z) : S \to *_p$

$y : S$

$u : x =_S y$

(2) $eq\text{-}cong_2(S,T,f,x,y,u) :=$

$eq\text{-}subs(S, Q_1(S,T,f,x), x, y, u, eq\text{-}refl(T, f\,x)) : f\,x =_T f\,y$

Figure 12.6 Second proof of the congruence property for equality

5 序，Orders

在知道如何编码“相等”后，还需要知道引理 12.1.2 的证明中起到重要作用的其它关系，也即符号 ‘$\leq$’ 表示的序关系。与 ‘$=$’ 相似，$\leq : S \to S \to *_p$，为了便于阅读，我们使用 $x \leq_S y$ 表示在集合 S 中的元素 x 和 y 上应用关系 $\leq$。形式化定义“偏序”（即偏序关系所具有的类型）：

$S : *_s$

$\leq : S \to S \to *_p$

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

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

(2) $trans(S, \leq) :=$

$\forall x : S\,.\,\forall y : S\,.\,\forall z : S\,.\,(x \leq_S y \Rightarrow y \leq_S z \Rightarrow x \leq_S z) : *_p$

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

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

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

Figure 12.7 Definitions regarding partial orders

可以看到 $\leq$ 是具有自反性，传递性和反对称性的关系。

现在可以证明由 $x \leq y \wedge y \leq x \Rightarrow x = y$，也即图 12.1 中的 t_3：

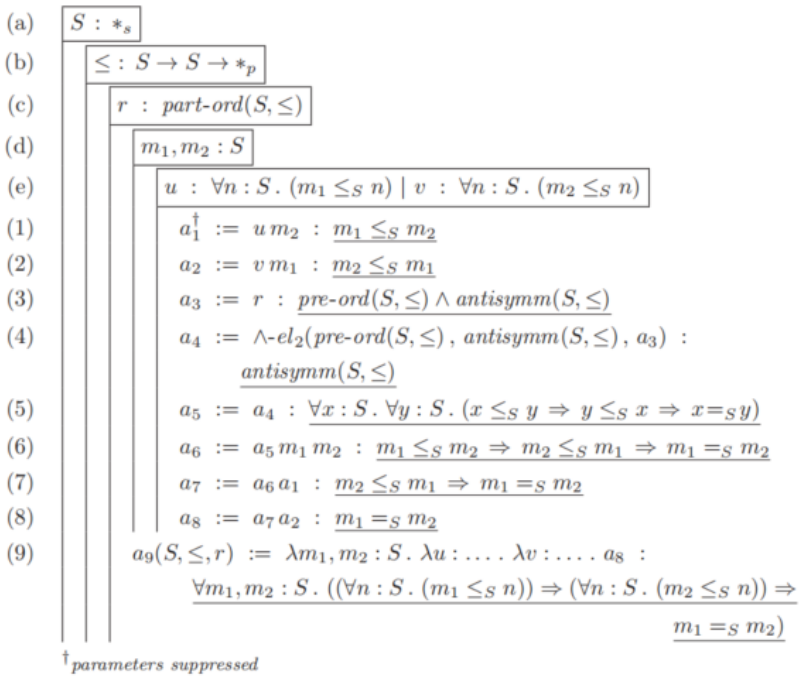

Figure 12.9 A formal proof of the first part of Lemma 12.1.2 in λD

可以看到，证明主要依赖于偏序关系的反对称性。

6 关于序的证明

除了已经证明过的相等的自反性以及替代性外，还有对称性和传递性。

对称性的证明使用了自反性和替代性：

$S : *_s$

$x : S$

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

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

$y : S$

$u \;:\; x =_S y$

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

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

Figure 12.10 Symmetry of equality follows from reflexivity and substitutivity

传递性的证明使用了替代性：

$S : *_s$

$x : S$

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

$y, z : S$

$u \;:\; x =_S y$

$v \;:\; y =_S z$

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

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

Figure 12.12 Transitivity of equality follows from substitutivity

7 唯一存在

引理 12.1.2 的证明中的大部分我们已经成功翻译，但是证明中的最后一个语句，这个引理本身以及相关联的定义 12.1.1，尚未翻译到 λD。

首先形式化描述“最小元”定义：

(a) $S : *_s \mid \leq : S \to S \to *_p \mid m : S$

(1) $\textit{Least}(S, \leq, m) \;:=\; \forall n : S\,.\,(m \leq n) \;:\; *_p$

Figure 12.13 A formal version of Definition 12.1.1

使用以大写 L 开头的名字 $Least$ 表示最小元，而后边的章中，会使用 $least$ 表示 S 中一个子集的一个最小元。

接下来的问题是如何表示存在的唯一性？首先，我们已经拥有了存在量词，显然存在量词表示存在至少一个，因此，我们可以写作 $\exists^{\geq 1}$ 而非只是 $\exists$。相对应的，我们可以通过 $\exists^{\leq 1}$ 表示存在至多一个，形式化的表示为 $\forall y, z : S.(P(y) \Rightarrow P(z) \Rightarrow y =_S z)$，也即不存在两个不同的元素满足谓词 P，若两个元素同时满足谓词，则这两个元素相等。此时可以通过两者合取表示仅存在一个元素满足谓词 P：

$S : *_s$

$P : S \to *_p$

(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) $\exists^{1}(S,P) := \exists^{\geq 1}(S,P) \wedge \exists^{\leq 1}(S,P) : *_p$

Figure 12.14 Various existential quantifiers

可观察到图 12.9 中的 a_9 的类型正是至多存在一个最小元。因此，现在我们可以完成证明：

$\vdots$

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

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

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

Figure 12.15 A completed formal version of Lemma 12.1.2 and its proof

$a_1 1$ 为“仅存在一个最小元”的证明。