14 λD 中的数字与算术
Numbers and arithmetic in λD

读书笔记

许博

1 用于自然数的皮亚诺公理

皮亚诺假设存在一个集合 $\mathbb{N}$，一个特定的成员 0，以及一个由 $\mathbb{N}$ 到 $\mathbb{N}$ 的后继函数 s。所以在 $\mathbb{N}$ 中，我们有成员 0，$s(0)$，$s(s(0))$ 等，表示 0，1，2 等。

之后，皮亚诺通过添加公理，使得这些形式化的数字行为符合预期。为了保证函数 s 一定产生新的数字，皮亚诺添加了两条公理：

$ax\text{-}nat_1$: $\forall_{x\in\mathbb{N}}(s(x) \neq 0)$

$ax\text{-}nat_2$: $\forall_{x,y\in\mathbb{N}}(s(x) = s(y) \Rightarrow x = y)$

公理 $ax\text{-}nat_2$ 表示 s 是一个单射的函数，而 $ax\text{-}nat_1$ 隐含了 s 不是满射的。这两条公理决定了不同层数 s 的自然数不相同。

除此之外，皮亚诺还添加了另一条公理，以通过数学归纳法确定所有自然数的性质：

$ax\text{-}nat_3$: $(P0 \wedge \forall x : \mathbb{N}.(Px \Rightarrow P(sx))) \Rightarrow \forall x : \mathbb{N}.Px$

引理 1.1 对于所有 $n \in \mathbb{N} : n = 0 \vee \exists_{m\in\mathbb{N}}(n = s(m))$

2 以公理方式引入整数

整数的公理化假设存在一个 $\mathbb{Z}$，一个特定的成员 0，以及一个由 $\mathbb{Z}$ 到 $\mathbb{Z}$ 的后继函数 s。包含如下公理：

$$
\begin{array}{lll}
(1) & \mathbb{Z} := \perp\!\!\!\perp : *_s \\
(2) & 0 := \perp\!\!\!\perp : \mathbb{Z} \\
(3) & s := \perp\!\!\!\perp : \mathbb{Z} \to \mathbb{Z} \\
(4) & \textit{ax-int}_1 := \perp\!\!\!\perp : \textit{bijective}(\mathbb{Z}, \mathbb{Z}, s) \\
(5) & \textit{inj-suc} := \ldots \texttt{ use } \wedge\textit{-el}_1 \ldots : \textit{injective}(\mathbb{Z}, \mathbb{Z}, s) \\
(6) & \textit{surj-suc} := \ldots \texttt{ use } \wedge\textit{-el}_2 \ldots : \textit{surjective}(\mathbb{Z}, \mathbb{Z}, s) \\
 & \boxed{y : \mathbb{Z}} \\
(7) & \quad a_7(y) := \textit{surj-suc}\ y : \exists^{\geq 1} x : \mathbb{Z} . (s\, x =_{\mathbb{Z}} y) \\
 & \quad \boxed{x_1, x_2 : \mathbb{Z} \mid u : s\, x_1 =_{\mathbb{Z}} y \mid v : s\, x_2 =_{\mathbb{Z}} y} \\
(8) & \quad\quad a_8(\ldots) := \textit{eq-sym}(\mathbb{Z}, s\, x_2, y, v) : y =_{\mathbb{Z}} s\, x_2 \\
(9) & \quad\quad a_9(\ldots) := \textit{eq-trans}(\mathbb{Z}, s\, x_1, y, s\, x_2, u, a_8(\ldots)) : s\, x_1 =_{\mathbb{Z}} s\, x_2 \\
(10) & \quad\quad a_{10}(\ldots) := \textit{inj-suc}\, x_1\, x_2\, a_9(\ldots) : x_1 =_{\mathbb{Z}} x_2 \\
(11) & \quad a_{11}(y) := \ldots \texttt{ use } \Rightarrow\textit{-in} \texttt{ and } \forall\textit{-in} \ldots : \exists^{\leq 1} x : \mathbb{Z} . (s\, x =_{\mathbb{Z}} y) \\
(12) & \quad a_{12}(y) := \ldots \texttt{ use } \wedge\textit{-in} \texttt{ on } a_7(y) \texttt{ and } a_{11}(y) \ldots : \\
 & \quad\quad\quad \exists^1 x : \mathbb{Z} . (s\, x =_{\mathbb{Z}} y) \\
(13) & a_{13} := \ldots \texttt{ use } \forall\textit{-in} \ldots : \forall y : \mathbb{Z} . \exists^1 x : \mathbb{Z} . (s\, x =_{\mathbb{Z}} y) \\
(14) & p := \lambda y : \mathbb{Z} . \iota(\mathbb{Z}, \lambda x : \mathbb{Z} . (s\, x =_{\mathbb{Z}} y), a_{12}(y)) : \mathbb{Z} \to \mathbb{Z} \\
 & \boxed{y : \mathbb{Z}} \\
(15) & \quad \textit{s-p-ann}(y) := \iota\textit{-prop}(\mathbb{Z}, \lambda x : \mathbb{Z} . (sx =_{\mathbb{Z}} y), a_{12}(y)) : s(p\, y) =_{\mathbb{Z}} y \\
(16) & \quad a_{16}(y) := \textit{s-p-ann}(s\, y) : s(p(s\, y)) =_{\mathbb{Z}} s\, y \\
(17) & \quad \textit{p-s-ann}(y) := \textit{inj-suc}\, (p(s\, y))\, y\, a_{16}(y) : p(s\, y) =_{\mathbb{Z}} y
\end{array}
$$

公理 $ax{-}int_1$ 表示 s 是一个双射函数：单射以及满射。由满射性可得，对于所有 $y \in \mathbb{Z}$，存在一个 $x \in \mathbb{Z}$，使得 $s(x) = y$。由单射性可得，y 确定时，满足 $s(x) = y$ 的 x 是唯一的。

行 (14) 中定义的 p，$p(y)$ 表示 y 的前驱，也即 $s(x) = y$ 中的 x，可以发现，p 是 s 的逆函数。

除了上图中出现的公理 $ax{-}int_1$，还有公理 $ax{-}int_2$，也即用于整数的归纳法，与自然数的版本相比较，在增加了前驱方向的归纳：

$$
\begin{array}{l}
\boxed{P : \mathbb{Z} \to *_p} \\
\quad \textit{ax-int}_2(P) := \perp\!\!\!\perp : \\
\quad\quad [P\, 0 \wedge \forall x : \mathbb{Z} . (P\, x \Rightarrow (P(s\, x) \wedge P(p\, x)))] \Rightarrow \forall x : \mathbb{Z} . P\, x
\end{array}
$$

Figure 14.4 The induction axiom for integer numbers

此时我们可以将从 0“向上”的整数，也即自然数，作为 $\mathbb{Z}$ 的一个子集

$\mathbb{N}$：

$$
\begin{array}{ll}
 & \boxed{P : \mathbb{Z} \to *_p} \\
(1) & \quad nat\text{-}cond(P) \ := \ P\,0 \wedge \forall x : \mathbb{Z}.\,(P\,x \Rightarrow P(s\,x)) \ : \ *_p \\
(2) & \mathbb{N} \ := \ \lambda x : \mathbb{Z}.\,\Pi P : \mathbb{Z} \to *_p\,.\,(nat\text{-}cond(P) \Rightarrow P\,x) \ : \ \mathbb{Z} \to *_p \\
(3) & zero\text{-}prop \ := \ \ldots \ [Exerc.\ 14.2(a)] \ \ldots \ : \ 0 \,\varepsilon\, \mathbb{N} \\
(4) & clos\text{-}prop \ := \ \ldots \ [Exerc.\ 14.2(b)] \ \ldots \ : \ \forall x : \mathbb{Z}.\,(x \,\varepsilon\, \mathbb{N} \Rightarrow s\,x \,\varepsilon\, \mathbb{N}) \\
(5) & a_5 \ := \ \ldots \ \texttt{use} \ \wedge\text{-}in \ \ldots \ : \ nat\text{-}cond(\mathbb{N}) \\
(6) & nat\text{-}smallest \ := \ \ldots \ [Exerc.\ 14.3] \ \ldots \ : \\
 & \qquad \Pi Q : \mathbb{Z} \to *_p\,.\,(nat\text{-}cond(Q) \Rightarrow (\mathbb{N} \subseteq Q))
\end{array}
$$

Figure 14.5 The natural numbers as a subset of $\mathbb{Z}$

其中 $nat{-}cond(P)$ 表示 P 满足自然数的归纳法的谓词，也即覆盖了所有的自然数，可以看到，如果一个整数 x 对于任意满足 $nat{-}cond$ 的谓词 P，都有 Px 成立，则 x 是一个自然数。而满足 $nat{-}cond$ 的谓词并不一定只作用于自然数，所以 $nat{-}smallest$ 表示了 $\mathbb{N}$ 是这些子集中的最小子集。

但目前仍存在一个问题，整数集合 $\mathbb{Z}$ 不能保证其的左右是无限的，比如对于集合 $\{a,b,c,d\}$，令 $a=0$，有 $s(a)=b, s(b)=c, s(c)=d, s(d)=a$，$s$ 同样是双射的，并且适用于归纳法。解决方式是添加一个公理，以确保 0 的前驱不是自然数：

$ax{-}int_3 := \perp\!\!\!\perp : \neg(p0 \;\varepsilon\; \mathbb{N})$

至此我们拥有了整数，自然数，以及负数。

3 ‘新’$\mathbb{N}$ 的基本性质

在 ‘新’ 的 $\mathbb{N}$ 中，之前的皮亚诺公理依然成立。对于自然数的数学归纳法，需要重新表述为：$(P0 \wedge \forall x : \mathbb{Z}.(x \,\varepsilon\, \mathbb{N} \Rightarrow (Px \Rightarrow P(sx)))) \Rightarrow \forall x : \mathbb{Z}.(x \,\varepsilon\, \mathbb{N} \Rightarrow Px)$。

引理 3.1 $\forall x : \mathbb{Z}.(x \;\varepsilon\; \mathbb{N} \Rightarrow (x =_{\mathbb{Z}} 0 \vee px \;\varepsilon\; \mathbb{N}))$

(1) *nat-split* := ... : $\forall x : \mathbb{Z} \,.\, (x \;\varepsilon\; \mathbb{N} \Rightarrow (x =_{\mathbb{Z}} 0 \vee p\, x \;\varepsilon\; \mathbb{N}))$

(2) *nat-split-alt* := ... : $\forall x : \mathbb{Z} \,.\, (\neg(x \;\varepsilon\; \mathbb{N}) \vee x =_{\mathbb{Z}} 0 \vee p\, x \;\varepsilon\; \mathbb{N})$

$\boxed{x : \mathbb{Z}}$

(3) $pos(x) := p\, x \;\varepsilon\; \mathbb{N}$

(4) $neg(x) := \neg(x \;\varepsilon\; \mathbb{N})$

(5) *trip* := *nat-split-alt* : $\forall x : \mathbb{Z} \,.\, (neg(x) \vee x =_{\mathbb{Z}} 0 \vee pos(x))$

Figure 14.9 Positive and negative numbers, and the tripartition property

Lemma 14.3.2 *(a)* $\forall x : \mathbb{Z} \,.\, (pos(s\, x) \Leftrightarrow x \;\varepsilon\; \mathbb{N})$,
(b) $\forall x : \mathbb{Z} \,.\, (pos(s\, x) \Leftrightarrow (x =_{\mathbb{Z}} 0 \vee pos(x)))$,
(c) $\forall x : \mathbb{Z} \,.\, (neg(p\, x) \Leftrightarrow (x =_{\mathbb{Z}} 0 \vee neg(x)))$.

Lemma 14.3.3 *(a)* $\forall x : \mathbb{Z} \,.\, (pos(x) \Leftrightarrow x \neq_{\mathbb{Z}} 0 \wedge \neg neg(x))$,
(b) $\forall x : \mathbb{Z} \,.\, (neg(x) \Leftrightarrow x \neq_{\mathbb{Z}} 0 \wedge \neg pos(x))$,
(c) $\forall x : \mathbb{Z} \,.\, (x =_{\mathbb{Z}} 0 \Leftrightarrow \neg pos(x) \wedge \neg neg(x))$.

4 整数加法

为了计算形式化的数字，形式化算术运算。首先是加法，通过如下形式的递归定义：

(i) $m + 0 = m$，

(ii) $m + s(n) = s(m + n)$。

可以发现 m 没有变动，递归基于第二个操作数，因此可以重新表述为：

(i) $+_m(0) = m$，

(ii) $+_m(s(n)) = s(+_m(n))$。

而对于操作数是负数的情况，可以由 (ii) 推导得到，因此，对于整数而言，这两个定义足够。

用于整数的良构递归定义：

Theorem 14.4.3 *(Recursion Theorem for $\mathbb{Z}$)*
Let A be a type, $a : A$ and let $f_1, f_2 : A \to A$.
Then there exists exactly one function $g : \mathbb{Z} \to A$ such that

– $g\, 0 =_A a$,
– $g(s\, x) =_A f_1(g\, x)$ *if* $x : \mathbb{Z}$ *and* $pos(s\, x)$,
– $g(p\, x) =_A f_2(g\, x)$ *if* $x : \mathbb{Z}$ *and* $neg(p\, x)$.

对于一个能够终止的作用于整数集合的递归定义，存在一个唯一的函数 g 满足。形式化为：

$\boxed{A : *_s \mid a : A \mid f_1, f_2 : A \to A}$

$$
\begin{array}{l}
\textit{spec-rec-th}(A, a, f_1, f_2) \;:=\; \ldots \;: \\
\qquad \exists^1 g : \mathbb{Z} \to A\,.\,[\,g\,0 =_A a \wedge \\
\qquad\qquad\qquad \forall x : \mathbb{Z}\,.\,[\,(\textit{pos}(s\,x) \Rightarrow (g(s\,x) =_A f_1(g\,x))) \wedge \\
\qquad\qquad\qquad\qquad (\textit{neg}(p\,x) \Rightarrow (g(p\,x) =_A f_2(g\,x)))\,]\,]
\end{array}
$$

Figure 14.10 The Recursion Theorem for $\mathbb{Z}$ in λD

而如果给定的函数 f 是一个双射函数，则可以定义良构递归为：

Theorem 14.4.5 *(Recursion Theorem for $\mathbb{Z}$, with bijection)*
Let A be a type, $a : A$ and $f : A \to A$, a bijection.
Then there exists exactly one function $g : \mathbb{Z} \to A$ such that

- $g\,0 =_A a$,
- $g(s\,x) =_A f(g\,x)$ *for all* $x : \mathbb{Z}$.

在 λD 中形式化 $+_m$ 以及 $+$：

(1) $a_1 \;:=\; \textit{ax-int}_1 \;:\; \textit{bijective}(\mathbb{Z}, \mathbb{Z}, s)$

$\boxed{m : \mathbb{Z}}$

(2) $\textit{rec-add-prop}(m) \;:=\; \lambda g : \mathbb{Z} \to \mathbb{Z}\,.\,(g\,0 =_{\mathbb{Z}} m \wedge \forall x : \mathbb{Z}\,.\,(g(s\,x) =_{\mathbb{Z}} s(g\,x))) \;:$
$\qquad (\mathbb{Z} \to \mathbb{Z}) \to *_p$

(3) $\textit{rec-add-lem}(m) \;:=\;$ ... `use Theorem 14.4.5` ... $:$
$\qquad \exists^1 g : \mathbb{Z} \to \mathbb{Z}\,.\,(\textit{rec-add-prop}(m)\;g)$

(4) $\textit{plus}(m) \;:=\; \iota(\mathbb{Z} \to \mathbb{Z}, \textit{rec-add-prop}(m), \textit{rec-add-lem}(m)) \;:\; \mathbb{Z} \to \mathbb{Z}$

`Notation :` $+_m$ `for` $\textit{plus}(m)$

Figure 14.11 Addition $+_m : \mathbb{Z} \to \mathbb{Z}$ in λD

(1) $+ \;:=\; \lambda x : \mathbb{Z}\,.\,\lambda y : \mathbb{Z}\,.\,(+_x\, y) \;:\; \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}$

`Notation :` $x + y$ `for` $+\,x\,y$

$\boxed{x : \mathbb{Z}}$

(2) $\textit{plus-i}(x) \;:=\; \ldots \;:\; x + 0 =_{\mathbb{Z}} x$

$\boxed{y : \mathbb{Z}}$

(3) $\textit{plus-ii}(x, y) \;:=\; \ldots \;:\; x + s\,y =_{\mathbb{Z}} s(x + y)$

(4) $\textit{plus-iii}(x, y) \;:=\; \ldots \;:\; x + p\,y =_{\mathbb{Z}} p(x + y)$

Figure 14.12 Properties of addition in $\mathbb{Z}$, formalised in λD