

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：

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

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

公理 $ax-nat_2$ 表示 s 是一个单射的函数，而 $ax-nat_1$ 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：

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

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：

- (1) $\mathbb{Z} := \perp : *_s$
 - (2) $0 := \perp : \mathbb{Z}$
 - (3) $s := \perp : \mathbb{Z} \rightarrow \mathbb{Z}$
 - (4) $ax-int_1 := \perp : bijective(\mathbb{Z}, \mathbb{Z}, s)$
 - (5) $inj-suc := \dots \text{ use } \wedge-el_1 \dots : injective(\mathbb{Z}, \mathbb{Z}, s)$
 - (6) $surj-suc := \dots \text{ use } \wedge-el_2 \dots : surjective(\mathbb{Z}, \mathbb{Z}, s)$
- | | | | | | |
|---|---|---|--|------------------|---|
| $y : \mathbb{Z}$ | <ol style="list-style-type: none"> (7) $a_7(y) := surj-suc\ y : \exists^{\geq 1} x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ <table border="0" style="margin-left: 20px;"> <tr> <td style="border: 1px solid black; padding: 2px; display: inline-block;">$x_1, x_2 : \mathbb{Z} \mid u : sx_1 =_{\mathbb{Z}} y \mid v : sx_2 =_{\mathbb{Z}} y$</td> <td style="vertical-align: middle;"> <ol style="list-style-type: none"> (8) $a_8(\dots) := eq-sym(\mathbb{Z}, sx_2, y, v) : y =_{\mathbb{Z}} sx_2$ (9) $a_9(\dots) := eq-trans(\mathbb{Z}, sx_1, y, sx_2, u, a_8(\dots)) : sx_1 =_{\mathbb{Z}} sx_2$ (10) $a_{10}(\dots) := inj-suc\ x_1\ x_2\ a_9(\dots) : x_1 =_{\mathbb{Z}} x_2$ (11) $a_{11}(y) := \dots \text{ use } \Rightarrow-in \text{ and } \forall-in \dots : \exists^{\leq 1} x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ (12) $a_{12}(y) := \dots \text{ use } \wedge-in \text{ on } a_7(y) \text{ and } a_{11}(y) \dots :$
 $\exists^1 x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ </td> </tr> </table> <ol style="list-style-type: none"> (13) $a_{13} := \dots \text{ use } \forall-in \dots : \forall y : \mathbb{Z}. \exists^1 x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ (14) $p := \lambda y : \mathbb{Z}. \iota(\mathbb{Z}, \lambda x : \mathbb{Z}. (sx =_{\mathbb{Z}} y), a_{12}(y)) : \mathbb{Z} \rightarrow \mathbb{Z}$ <table border="0" style="margin-left: 20px;"> <tr> <td style="border: 1px solid black; padding: 2px; display: inline-block;">$y : \mathbb{Z}$</td> <td style="vertical-align: middle;"> <ol style="list-style-type: none"> (15) $s-p-ann(y) := \iota-prop(\mathbb{Z}, \lambda x : \mathbb{Z}. (sx =_{\mathbb{Z}} y), a_{12}(y)) : s(py) =_{\mathbb{Z}} y$ (16) $a_{16}(y) := s-p-ann(sy) : s(p(sy)) =_{\mathbb{Z}} sy$ (17) $p-s-ann(y) := inj-suc\ (p(sy))\ y\ a_{16}(y) : p(sy) =_{\mathbb{Z}} y$ </td> </tr> </table> | $x_1, x_2 : \mathbb{Z} \mid u : sx_1 =_{\mathbb{Z}} y \mid v : sx_2 =_{\mathbb{Z}} y$ | <ol style="list-style-type: none"> (8) $a_8(\dots) := eq-sym(\mathbb{Z}, sx_2, y, v) : y =_{\mathbb{Z}} sx_2$ (9) $a_9(\dots) := eq-trans(\mathbb{Z}, sx_1, y, sx_2, u, a_8(\dots)) : sx_1 =_{\mathbb{Z}} sx_2$ (10) $a_{10}(\dots) := inj-suc\ x_1\ x_2\ a_9(\dots) : x_1 =_{\mathbb{Z}} x_2$ (11) $a_{11}(y) := \dots \text{ use } \Rightarrow-in \text{ and } \forall-in \dots : \exists^{\leq 1} x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ (12) $a_{12}(y) := \dots \text{ use } \wedge-in \text{ on } a_7(y) \text{ and } a_{11}(y) \dots :$
 $\exists^1 x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ | $y : \mathbb{Z}$ | <ol style="list-style-type: none"> (15) $s-p-ann(y) := \iota-prop(\mathbb{Z}, \lambda x : \mathbb{Z}. (sx =_{\mathbb{Z}} y), a_{12}(y)) : s(py) =_{\mathbb{Z}} y$ (16) $a_{16}(y) := s-p-ann(sy) : s(p(sy)) =_{\mathbb{Z}} sy$ (17) $p-s-ann(y) := inj-suc\ (p(sy))\ y\ a_{16}(y) : p(sy) =_{\mathbb{Z}} y$ |
| $x_1, x_2 : \mathbb{Z} \mid u : sx_1 =_{\mathbb{Z}} y \mid v : sx_2 =_{\mathbb{Z}} y$ | <ol style="list-style-type: none"> (8) $a_8(\dots) := eq-sym(\mathbb{Z}, sx_2, y, v) : y =_{\mathbb{Z}} sx_2$ (9) $a_9(\dots) := eq-trans(\mathbb{Z}, sx_1, y, sx_2, u, a_8(\dots)) : sx_1 =_{\mathbb{Z}} sx_2$ (10) $a_{10}(\dots) := inj-suc\ x_1\ x_2\ a_9(\dots) : x_1 =_{\mathbb{Z}} x_2$ (11) $a_{11}(y) := \dots \text{ use } \Rightarrow-in \text{ and } \forall-in \dots : \exists^{\leq 1} x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ (12) $a_{12}(y) := \dots \text{ use } \wedge-in \text{ on } a_7(y) \text{ and } a_{11}(y) \dots :$
 $\exists^1 x : \mathbb{Z}. (sx =_{\mathbb{Z}} y)$ | | | | |
| $y : \mathbb{Z}$ | <ol style="list-style-type: none"> (15) $s-p-ann(y) := \iota-prop(\mathbb{Z}, \lambda x : \mathbb{Z}. (sx =_{\mathbb{Z}} y), a_{12}(y)) : s(py) =_{\mathbb{Z}} y$ (16) $a_{16}(y) := s-p-ann(sy) : s(p(sy)) =_{\mathbb{Z}} sy$ (17) $p-s-ann(y) := inj-suc\ (p(sy))\ y\ a_{16}(y) : p(sy) =_{\mathbb{Z}} y$ | | | | |

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：

$P : \mathbb{Z} \rightarrow *_p$	$ax-int_2(P) := \perp :$ $[P\ 0 \wedge \forall x : \mathbb{Z}. (Px \Rightarrow (P(sx) \wedge P(px)))] \Rightarrow \forall x : \mathbb{Z}. Px$
----------------------------------	--

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} :

- | | |
|--|----------------------------------|
| | $P : \mathbb{Z} \rightarrow *_p$ |
|--|----------------------------------|
- (1) $\text{nat-cond}(P) := P\,0 \wedge \forall x : \mathbb{Z}. (P\,x \Rightarrow P(s\,x)) : *_p$
 - (2) $\mathbb{N} := \lambda x : \mathbb{Z}. \Pi P : \mathbb{Z} \rightarrow *_p. (\text{nat-cond}(P) \Rightarrow P\,x) : \mathbb{Z} \rightarrow *_p$
 - (3) $\text{zero-prop} := \dots [\text{Exerc. 14.2}(a)] \dots : 0 \in \mathbb{N}$
 - (4) $\text{clos-prop} := \dots [\text{Exerc. 14.2}(b)] \dots : \forall x : \mathbb{Z}. (x \in \mathbb{N} \Rightarrow s\,x \in \mathbb{N})$
 - (5) $a_5 := \dots \text{use } \wedge\text{-in } \dots : \text{nat-cond}(\mathbb{N})$
 - (6) $\text{nat-smallest} := \dots [\text{Exerc. 14.3}] \dots :$
 $\Pi Q : \mathbb{Z} \rightarrow *_p. (\text{nat-cond}(Q) \Rightarrow (\mathbb{N} \subseteq Q))$

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

其中 $\text{nat-cond}(P)$ 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 $P\,x$ 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：

$$ax\text{-int}_3 := \perp\!\!\!\perp : \neg(p\,0 \in \mathbb{N})$$

至此我们拥有了整数，自然数，以及负数。