第 9 章　哥德尔第一不完全性定理

我们现在考察语言 $\mathcal{L}_{ar}=\{0,\mathsf{S},+,\cdot\}$ 并且研究初等数论的标准模型 $\mathfrak{N}=(\mathbb{N},0,S,+,\cdot)$。同时具有加法和乘法的模型与前面的普莱斯伯格算术 $(\mathbb{N},0,S,+)$ 和司寇伦的乘法模型 $(\mathbb{N},0,\times)$ 大不相同。我们本章的目标是下列三大定理：塔尔斯基不可定义定理，哥德尔的第一不完全性定理和丘奇的不可判定性定理。

需要的主要三个步骤为：可表示性，语法的算术化和不动点引理。我们下面分别讨论。

第 1 节　可表示性

9.1.1　罗宾逊算术 Q

粗略地说，研究“可表示性”就是研究什么样的标准自然数上的关系可以用形式语言 $\mathcal{L}_{ar}$ 中的公式表示或表达出来。我们的目标是先确定“表示”的精确定义，然后证明所有递归关系都是在选定的算术系统内“可表示的”。自然，算术系统越强，所能证明的命题就越多。因此，为了获得最强烈的反差，我们选取一个非常弱的（可以说是最弱的）系统 Q，称为罗宾逊[1] 算术。其它的选择还有 PA^-（差不多是 PA 除掉归纳法）和 PA；或者为了编码的方便，也有把指数函数添到语言之中并添加适当的关于指数运算的公理；当然还可以选择集合论的语言和 ZFC 公理或适当的片断。

罗宾逊算术理论 Q 的公理有如下 7 条:

Q1　$\forall x\ \mathsf{S}x\not\approx 0$。

Q2　$\forall x\forall y\ (\mathsf{S}x\approx\mathsf{S}y\to x\approx y)$。

Q3　$\forall x\ (x\not\approx 0\to\exists y\ x\approx\mathsf{S}y)$。

Q4　$\forall x\ (x+0\approx x)$。

Q5　$\forall x\forall y\ (x+\mathsf{S}y\approx\mathsf{S}(x+y))$。

[1]罗宾逊，Raphael Robinson （1911 - 1995），美国数学家。

Q6　$\forall x\,(x\cdot \mathsf{0}\approx \mathsf{0})$。

Q7　$\forall x\forall y\,(x\cdot \mathsf{S}y\approx x\cdot y+x)$。

显然，标准自然数模型 $\mathfrak{N}$ 是 Q 的一个模型。但是 Q 还有很多其它模型。

例 9.1. 考察结构 $\mathfrak{M}=(\mathbb{N}\cup\{\infty\},0,S,+,\cdot)$，其中函数 S、$+$ 和 $\cdot$ 为通常的后继、加法和乘法依照如下方式扩张到新元素 ∞ 上：

(1) $S(\infty)=\infty$；

(2) $n+\infty=\infty+n=\infty+\infty=\infty$（对所有的 $n\in\mathbb{N}$）；

(3) $\infty\cdot 0=0\cdot\infty=0$ 并且 $n\cdot\infty=\infty\cdot n=\infty\cdot\infty=\infty$（对所有的 $n\in\mathbb{N}$ 且 $n\neq 0$）。

则结构 $\mathfrak{M}\models \mathsf{Q}$。（练习）

引理 9.1.　*(a)* $\mathsf{Q}\nvdash \forall x\,\mathsf{S}x\not\approx x$。

(b) 对每一个标准自然数 $n\in\mathbb{N}$，$\mathsf{Q}\vdash \mathsf{Sn}\not\approx \mathsf{n}$，其中 n 代表 $\mathsf{S}^n\mathsf{0}$。

证明: 根据 $S(\infty)=\infty$ 在例 9.1 中的模型 $\mathfrak{M}$ 上成立，我们立刻得到 (a)。

断言 (b) 则是通过（外面的）对标准自然数 $n\in\mathbb{N}$ 作归纳而得到的。

当 $n=0$ 时，$\mathsf{Q}\vdash \mathsf{S0}\not\approx \mathsf{0}$，这是根据 (Q1)。

假定 $\mathsf{Q}\vdash \mathsf{Sn}\not\approx \mathsf{n}$。则根据 (Q2) 的逆否命题，我们立刻有 $\mathsf{Q}\vdash \mathsf{S(n+1)}\not\approx \mathsf{n+1}$。　□

注： 引理 9.1 虽然很短，但包含的信息对本节的理解是至关重要的。

- 首先它表明了标准和非标准自然数的区别。每一个标准自然数 $n\in\mathbb{N}$ 都在我们的语言内有一个“名字”，即*数码* n。这个数码 n 是算术语言中的项 $\mathsf{S}^n\mathsf{0}$，它是语言内与“外面的”自然数 n 的对应物。而非标准数则都是“无名鼠辈”，似乎飘忽不定。
- 考察断言 (b) 对所有 $n\in\mathbb{N}$，$\mathsf{Q}\vdash \mathsf{n}\not\approx \mathsf{Sn}$。注意这里实际上是一族证明，而不是一个证明。当自然数 n 越来越大时，Q 对 $\mathsf{n}\not\approx \mathsf{Sn}$ 的证明也越来越长。而断言 (a) 则不然，它否证的是一个适用于所有数的一致的[2]证明。
- 最后，请大家注意我们在“外部的”证明（如证明 (b) 时可以用归纳法）和系统 Q 内证明（Q 中显然没有归纳法）的区别。

我们再看 Q 的一些其它的简单事实。在本节中，我们用“$\vdash$”来表达“$\mathsf{Q}\vdash$”；并且将 $x\leq y$ 定义成 $\exists z(x+z\approx y)$。

[2]这里的一致指的是数学中常用的一致性，即 uniformity，与无矛盾性无关。

引理 9.2. 对所有 $m, n \in \mathbb{N}$，我们有

(1) $\vdash \forall x(\mathsf{S}x + \mathsf{n} \approx x + \mathsf{Sn})$。

(2) $\vdash \mathsf{m} + \mathsf{n} \approx \mathsf{S}^{m+n}\mathsf{0}$ 并且 $\vdash \mathsf{m} \cdot \mathsf{n} \approx \mathsf{S}^{m \cdot n}\mathsf{0}$。

(3) 如果 $n \neq m$ 则 $\vdash \mathsf{n} \not\approx \mathsf{m}$。

(4) 如果 $m \leq n$ 则 $\vdash \mathsf{m} \leq \mathsf{n}$。

(5) 如果 $m \not\leq n$ 则 $\vdash \mathsf{m} \not\leq \mathsf{n}$。

(6) $\vdash \forall x(x \leq \mathsf{n} \leftrightarrow x \approx \mathsf{0} \vee \cdots \vee x \approx \mathsf{n})$。

(7) $\vdash \forall x(x \leq \mathsf{n} \vee \mathsf{n} \leq x)$。

证明: 见习题。 □

引理 9.2 告诉我们一些有关 Q 模型的事实，后面我们会用到。令 $\mathfrak{M}$ 为任意一个 Q 的模型。

- 由引理 9.2 (2) 和 (3) 我们有：函数 $n \mapsto \mathsf{n}^{\mathfrak{M}}$ 是从标准模型 $\mathfrak{N}$ 到模型 $\mathfrak{M}$ 的一个嵌入。因此，我们可以不失一般性地假设 $\mathfrak{N} \subseteq \mathfrak{M}$。
- 还有 (6) 告诉我们：如果 $b \in \mathfrak{N}$ 并且 $a \leq^{\mathfrak{M}} b$，则 $a \in \mathfrak{N}$。换句话说，$\mathfrak{M}$ 中所有的新元素都是缀在 $\mathfrak{N}$ 后面的；表述这种情形的术语为 $\mathfrak{M}$ 是 $\mathfrak{N}$ 的一个*尾节扩张*。

9.1.2 可表示性

令 T 为一个包含 Q 的理论。在下面的讨论中，如果不加说明，则可隐含地假定理论 T 为 Q。

定义 9.1. 我们称一个自然数上的 k-元关系 P 为在 T 中*数码逐点可表示的*[3] 或简称为*可表示的*，如果存在一个公式 $\rho(\vec{x})$，称为 P 的一个*表示公式*，使得

$$\begin{aligned} (n_1, n_2, \cdots, n_k) \in P \quad &\Rightarrow \quad T \vdash \rho(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_k); \text{ 并且} \\ (n_1, n_2, \cdots, n_k) \notin P \quad &\Rightarrow \quad T \vdash \neg\rho(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_k)。 \end{aligned}$$

例 9.2. *(1)* 自然数上的等同关系 $\{(n, n) : n \in \mathbb{N}\}$ 被公式 $x \approx y$ 所表示：显然，$m = n$ 蕴涵 $\vdash \mathsf{m} \approx \mathsf{n}$，并且根据引理 9.2 *(3)*，$m \neq n$ 蕴涵 $\vdash \mathsf{m} \not\approx \mathsf{n}$。

(2) 类似地，引理 9.2 *(4)* 和 *(5)* 告诉我们关系 $\leq$ 可以被公式 $x \leq y$ 表示。

[3] 数码逐点可表示的，numeralwise representable；可表示的，representable。

我们看一些可表示性的简单性质：

- 如果 P 是可表示的，则 P 是递归的。

  证明：对给定的自然数组 $\vec{n}$，递归地枚举所有 Q（或任何递归的公理系统 T）中的证明序列，直到 $\rho(\vec{\mathsf{n}})$ 或 $\neg\rho(\vec{\mathsf{n}})$ 的证明出现。如果是前者，则 $P(\vec{n})$ 成立；后者，则 $P(\vec{n})$ 不成立。可表示性告诉我们该证明一定会出现。 □

- 可表示的关系在布尔运算下是封闭的。

  证明：假设 P 和 Q 分别由公式 ρ_1 和 ρ_2 表示。则 $P\cup Q$、$P\cap Q$ 和 $\mathbb{N}^k\setminus P$ 分别由公式 $\rho_1\vee\rho_2$、$\rho_1\wedge\rho_2$ 和 $\neg\rho_1$ 来表示。 □

- 如果 P 在 Q 中被公式 ρ 表示，则 P 在 Q 的任何相容扩张（例如，PA 或 $\mathrm{Th}(\mathfrak{N})$）中都被 ρ 表示。

- P 在 $\mathrm{Th}(\mathfrak{N})$ 中被 ρ 表示当且仅当 P 在结构 $\mathfrak{N}$ 中被 ρ 定义。

  证明：练习。 □

定理 9.1 (Q 的 Σ_1-完备性)**.** 对任一 Σ_1-闭语句 τ，我们有

$$\mathfrak{N}\models\tau \quad \text{当且仅当} \quad \mathsf{Q}\vdash\tau。$$

注：

- 我们称一个 $\mathcal{L}_{ar}$ 中的公式为 Δ_0 的，如果它只包含有界量词。我们称一个形如 $\exists x_1\cdots\exists x_n\,\theta$ 的公式为 Σ_1 的，其中 θ 是 Δ_0 的。一个 Σ_1 公式的否定总是逻辑等价于一个形如 $\forall x_1\cdots\forall x_n\theta$ 的公式，我们称这样的公式是 Π_1 的。而如果一个公式机即等价于一个 Σ_1 公式又等价于一个 Π_1 公式，我们就称之为 Δ_1 的。

- 引理 9.1 告诉我们对 Π_1-闭语句，如 $\forall x(\mathsf{S}x\not\approx x)$，我们则没有这种完备性。

证明：由于“$\Leftarrow$”立刻可以从 $\mathfrak{N}$ 是 Q 的一个模型导出，我们下面证明另一个方向“$\Rightarrow$”。

断言. 对任何 Δ_0-闭语句 σ，对任何 Q 的模型 $\mathfrak{M}$，我们有 $\mathfrak{M}\models\sigma$ 当且仅当 $\mathfrak{N}\models\sigma$。

断言的证明. 我们对 σ 进行归纳。首先注意：对任何一个闭项 t（即，t 中不含自由变元），我们有 $t^{\mathfrak{N}}=t^{\mathfrak{M}}$。因此断言对任何的原子闭公式成立。不难证明对于不含量词（无论有界或无界的）的闭语句 τ 断言也成立。

给定任意的形如 $(\forall x\le t)\theta(x)$ 的闭公式 σ，其中 t 是一个闭项，并假定 $\mathfrak{N}\models(\forall x\le t)\theta(x)$。则对所有的 $a\le^{\mathfrak{N}}t^{\mathfrak{N}}$，都有 $\mathfrak{N}\models\theta(\mathsf{a})$。移到模型 $\mathfrak{M}$ 中来讨论，我们有 $t^{\mathfrak{M}}=$

$t^{\mathfrak{N}} \in \mathfrak{N}$。由于 $\mathfrak{M}$ 是 $\mathfrak{N}$ 的尾节扩张，任何 $a \leq^{\mathfrak{M}} t^{\mathfrak{M}}$ 都是属于 $\mathfrak{N}$ 的，所以根据归纳假定，$\mathfrak{M} \models \theta(\mathsf{a})$。所以 $\mathfrak{M} \models \sigma$。

同理，$\mathfrak{M} \models \sigma$ 也蕴涵 $\mathfrak{N} \models \sigma$，这就验证了断言。

注意：断言实际上是“Δ_0-完全性”的模型论表述。换句话说，断言告诉我们，对任何 Δ_0-闭语句 σ，$\mathfrak{N} \models \sigma$ 当且仅当 $\mathsf{Q} \vdash \sigma$。现在假定 $\mathfrak{N} \models \exists \vec{x}\, \sigma(\vec{x})$，其中 σ 为一个 Δ_0 公式。则对某个 $\vec{a} \in \mathfrak{N}^k$，我们有 $\mathfrak{N} \models \sigma(\vec{\mathsf{a}})$。根据断言，$\mathsf{Q} \vdash \theta(\vec{\mathsf{a}})$。所以 $\mathsf{Q} \vdash \exists \vec{x}\, \sigma(\vec{x})$。　□

下面的引理告诉我们如何处理约束量词。该引理我们以后会常常用到。

引理 9.3. 如果关系 $P \subseteq \mathbb{N}^{k+1}$ 被公式 $\rho(\vec{x}, y)$ 所表示，则关系 $(\exists c < b)P(\vec{a}, c)$ 和 $(\forall c < b)P(\vec{a}, c)$ 分别被 $(\exists z < y)\rho(\vec{x}, z)$ 和 $(\forall z < y)\rho(\vec{x}, z)$ 所表示。

证明：习题。　□

9.1.3　函数的可表示性

我们的目标是证明每个递归的关系都是可表示的（从而递归关系就是可表示关系）。由于递归关系是用递归函数来定义的，为此我们自然地想借助递归函数来达到我们的目标。为此，我们引入一个函数的可表示性概念。

定义 9.2. 我们称一个函数 $f : \mathbb{N}^k \to \mathbb{N}$ 为在 T 中**可表示的**，如果存在一个公式 $\varphi(x_1, \cdots, x_k, y)$ 使得对所有的 $(n_1, \cdots, n_k) \in \mathbb{N}^k$，我们有

$$\vdash_T \forall y[\varphi(\mathsf{n}_1, \cdots, \mathsf{n}_k, y) \leftrightarrow y = \mathsf{f}(\mathsf{n}_1, \cdots, \mathsf{n}_k)]。$$

在此情形下，我们也称 φ **作为一个函数表示** f。

我们常常把一个函数 $f(x)$ 与它的图像 $G_f = \{(x, y) : x = f(y)\}$ 等同起来（为简化讨论，我们假定 $k = 1$）。那么公式 φ 表示 G_f（作为一个二元关系）与公式 φ 表示 f（作为一个一元函数）有什么不同吗？首先，如果 $f(n) = m$，则 $(n, m) \in G_f$，我们作为关系要求 $\vdash_T \varphi(\mathsf{n}, \mathsf{m})$，而作为函数也要求（从右向左方向，当 $y = f(n)$ 时）$\vdash_T \varphi(\mathsf{n}, \mathsf{m})$，这一点双方是一样的。如果 $y \neq f(n)$ 时，作为关系表示 G_f 的 φ 仅仅能逐点地验证对每个 $m \neq f(n)$ 的标准自然数 m，$\vdash_T \neg\varphi(\mathsf{n}, \mathsf{m})$，而对作为函数表示 f 的 φ，我们要求的更多，我们要求它能有个相容的对 Π_1 语句的证明：$\vdash_T \forall y[y \neq \mathsf{f}(\mathsf{n}) \to \neg\varphi(\mathsf{n}, y)]$。如同前面引理 9.1 所告诉我们的，后者要强得多。

我们举一个具体的例子：令 $T = \mathsf{Q}$。对于零函数 $Z(x) = 0$ 的图像 $G_Z = \{(x, 0) : x \in \mathbb{N}\}$ 来说，它被公式 $\varphi(x, y) :=_{df} \ y + y \approx y$ 作为一个关系表示（练习）；但由于 Q 不能证明 $\forall y(y + y \approx y \to y \approx 0)$（练习），所以，$\varphi(x, y)$ 并不作为一个函数表示零函数。

从这段讨论我们可以得出，如果公式 φ 表示 f（作为一个一元函数），则公式 φ 也表示 G_f（作为一个二元关系）。但反过来则不一定。关于函数可表示性的问题，我们等一下在推论 9.1 中会有更明确的结论。

引理 9.4. 令 t 为语言 $\mathcal{L}_{ar}$ 中的一个项，其中出现的变元都包含在 $x_1, x_2, \cdots, x_k$ 当中。则它诱导出的 k-元函数 $f_t(n_1, n_2, \cdots, n_k) = t(n_1, n_2, \cdots, n_k)$ 是可表示的。特别地，后继函数、常数函数、加法、乘法和投射函数都是可表示的。

证明: 令 $\varphi(x_1, x_2, \cdots, x_k, y)$ 为 $y \approx t(x_1, x_2, \cdots, x_k)$。则对任何的 $n_1, n_2, \cdots, n_k \in \mathbb{N}$ 显然有

$$\vdash_T \forall y\ [y \approx t(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_k) \leftrightarrow y \approx \mathsf{f_t}(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_k)]$$

因为 $\vdash_T\ t(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_k) \approx \mathsf{f_t}(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_k)$（这可以从引理 9.2，加上对 t 归纳来证明）。 □

定理 9.2. 可表示函数构成的类对复合运算封闭，即，假定函数 $h_1(x_1, x_2, \cdots, x_n)$、$h_2(x_1, x_2, \cdots, x_n)$、$\cdots$、$h_r(x_1, x_2, \cdots, x_n)$ 和函数 $g(y_1, y_2, \cdots, y_r)$ 都是可表示的，则复合函数 $f = g(h_1, h_2, \cdots, h_r)$ 也是。

证明: 我们用向量符号 $\vec{x}$ 表示 $(x_1, x_2, \cdots, x_n)$。固定公式 $\theta_i(\vec{x}, y_i)$（作为函数）分别表示 $h_i(\vec{x})$ $(1 \le i \le r)$，和公式 $\psi(y_1, y_2, \cdots, y_r, z)$（作为函数）表示 $g(y_1, y_2, \cdots, y_r)$。对 $1 \le i \le r$，$\vec{m} \in \mathbb{N}^n$ 我们有

$$\vdash_T \forall y_i[\theta_i(\vec{\mathsf{m}}, y_i) \leftrightarrow y_i \approx \mathsf{h}_i(\vec{\mathsf{m}})], \tag{9.1}$$

并且对 $n_1, n_2, \cdots, n_r \in \mathbb{N}$，我们有

$$\vdash_T \quad \forall z[\psi(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_r, z) \leftrightarrow z \approx \mathsf{g}(\mathsf{n}_1, \mathsf{n}_2, \cdots, \mathsf{n}_r)]。 \tag{9.2}$$

令 $\varphi(\vec{x}, z)$ 为公式

$$\forall y_1 \cdots \forall y_r[(\bigwedge_{i=1}^{r} \theta_i(\vec{x}, y_i)) \to \psi(y_1, \cdots, y_r, z)]。$$

我们证明：对任何 $\vec{m} \in \mathbb{N}^n$，

$$\vdash_T \forall z(\varphi(\vec{\mathsf{m}}, z) \leftrightarrow z \approx \mathsf{f}(\vec{\mathsf{m}}))。$$

先看从右向左的方向，我们要证：$\vdash_T \varphi(\vec{\mathsf{m}}, \mathsf{f}(\vec{\mathsf{m}}))$，即

$$\vdash_T \forall y_1 \cdots \forall y_r[(\bigwedge_{i=1}^{r} \theta_i(\vec{\mathsf{m}}, y_i)) \to \psi(y_1, \cdots, y_r, \mathsf{f}(\vec{\mathsf{m}}))]。$$

根据一阶逻辑，我们只要证

$$\bigwedge_{i=1}^{r} \theta_i(\vec{\mathsf{m}}, y_i) \vdash_T \psi(y_1, \cdots, y_r, \mathsf{f}(\vec{\mathsf{m}}))。$$

根据 (9.1) 的唯一性方向，我们有

$$\bigwedge_{i=1}^{r} \theta_i(\vec{\mathsf{m}}, y_i) \vdash_T \bigwedge_{i=1}^{r} (y_i \approx \mathsf{h}_i(\vec{\mathsf{m}})),$$

再在 (9.2) 中，将 n_i 用 $\mathsf{h}_i(\vec{\mathsf{m}})$ 替代，即可得到我们所要证的。

再看从左向右的方向，我们要证：$\vdash_T \forall z(\varphi(\vec{\mathsf{m}}, z) \to z \approx \mathsf{f}(\vec{\mathsf{m}}))$。仍根据一阶逻辑，我们只要证

$$\forall y_1 \cdots \forall y_r[(\bigwedge_{i=1}^{r} \theta_i(\vec{\mathsf{m}}, y_i)) \to \psi(y_1, \cdots, y_r, z)] \vdash_T z \approx \mathsf{f}(\vec{\mathsf{m}})。$$

根据 (9.1) 的从右向左方向，我们有 $\vdash_T \bigwedge_{i=1}^{r} \theta_i(\vec{\mathsf{m}}, \mathsf{h}_i(\vec{\mathsf{m}}))$；再根据假设，就得到 $\varphi(\vec{\mathsf{m}}, z) \vdash_T \psi(\mathsf{h}_1(\vec{\mathsf{m}}), \cdots, \mathsf{h}_r(\vec{\mathsf{m}}), z)$。再根据 (9.2) 中唯一性的方向，我们有

$$\varphi(\vec{\mathsf{m}}, z) \vdash_T z \approx \mathsf{g}(\mathsf{h}_1(\vec{\mathsf{m}}), \cdots, \mathsf{h}_r(\vec{\mathsf{m}}))。$$

因此，$\varphi(\vec{\mathsf{m}}, z) \vdash_T z \approx \mathsf{f}(\vec{\mathsf{m}})$。 □

注：

- 我们在证明中给出的公式 φ 是 Π_1-的（假定其它给定的公式都是 Δ_1- 的）。我们也可以用一个 Σ_1-公式 $\phi(\vec{x}, z)$ 来表示 f：

  $$\exists y_1 \exists y_2 \cdots \exists y_r[(\bigwedge_{i=1}^{r} \theta_i(\vec{x}, y_i)) \wedge \psi(y_1, \cdots, y_r, z)]。$$

  这对关心复杂性的读者也许是有用的。

- 我们给出详细证明的目的之一是说明引进“作为函数表示”这一概念的必要性。注意在上面的证明中，即使是较为简单的从右向左方向，也用到了唯一性。更进一步，我们可以举出具体反例说明仅用关系的可表示性是不够的（习题）。

我们下面处理正则极小算子。先证明一个有用的引理：

引理 9.5. 令公式 $\alpha(\vec{x}, y)$ 表示 $(k+1)$-元关系 $P \subseteq \mathbb{N}^{k+1}$。并假定 $\mathfrak{N} \models \forall \vec{a} \exists b\ P(\vec{a}, b)$。定义公式 $\varphi(\vec{x}, y)$ 为 $\alpha(\vec{x}, y) \wedge (\forall z < y) \neg \alpha(\vec{x}, z)$。则公式 $\varphi(\vec{x}, y)$（作为函数）表示函数 $f : \vec{a} \mapsto \mu b[P(\vec{a}, b)]$。

证明: 我们只证明唯一性的方向：$\vdash \varphi(\vec{\mathsf{a}}, y) \to y \approx \mathsf{f}(\vec{\mathsf{a}})$。

令 $b = f(\vec{a})$。则根据一阶逻辑 $\mathsf{b} < y \vdash (\exists z < y)\alpha(\vec{\mathsf{a}}, z)$。

另一方面，$y < \mathsf{b} \vdash \bigvee_{n<b} y \approx \mathsf{n}$，而根据 P 的可表示性 $\vdash \neg\alpha(\vec{\mathsf{a}}, y)$。

最后再利用引理 9.2 (7)：对任何 $b \in \mathbb{N}$，$\vdash \forall y(y \leq \mathsf{b} \vee \mathsf{b} \leq y)$，我们就得到

$$\vdash \varphi(\vec{\mathsf{a}}, y) \to y \approx \mathsf{b}。$$

□

推论 9.1. 如果一个函数 f （的图像）作为关系是可表示的，则 f 作为函数也是可表示的（但表示它们的公式可能不相同）。

证明: 只需注意到如果 G_f 是函数 f 的图像，则函数 $\vec{a} \mapsto \mu b[G_f(\vec{a}, b)]$ 就是 f 自身。 □

所以对一个函数来说，就可表示性而言，作为关系和作为函数没有什么不同，不同的只是表达它们的公式而已。

引理 9.5 还告诉我们可表示的函数类对正则极小算子是封闭的。为了强调，我们把它列为定理：

定理 9.3. 假定函数 $g(x, y)$ 是可表示的并且 $\forall x \exists y\ g(x, y) = 0$。则函数 $f(x) =_{df} \mu y\ g(x, y) = 0$ 也是可表示的。

附带提以下，在哥德尔 1931 年的文章中，他只证明了原始递归函数都是可表示的，而没有考虑正则极小算子和所有的递归函数。我们可以进一步说，哥德尔的可表示的函数实际上是递归函数的一个等价刻画（见推论 9.2）。

9.1.4　仅用加法和乘法编码

我们已经证明了所有的初始函数都是可表示的，并且可表示函数的类对复合和正则的极小算子封闭。我们还剩下原始递归有待处理。

回忆一下我们通常（例如在集合论中）是怎样论证原始递归的合理性的。假设函数 $f(\vec{x}, y)$ 是通过 g 和 h 由原始递归得到的。我们可以直接写出 $f(\vec{x}, n) = m$ 的显式定义：“存在一个有穷序列（的编码） s，它的长度是 $n + 1$ 使得 $(s)_0 = g(\vec{x})$ 且对所有的 $i < n$，$(s)_{i+1} = h(\vec{x}, i, (s)_i)$ 和 $(s)_n = m$”。这里的编码和解码通常是利用指数函数 x^y 和素数分解来完成的。但是，指数函数 x^y 和 p_n 本身都是利用原始递归来定义的。论证它们的可表示性和论证原始递归的可表示性难度是一样的。要想打破这种“鸡生蛋，蛋生鸡”的怪圈，我们需要一个可表示的编码和解码函数。哥德尔利用了中国剩余定理，巧妙地解决了这个问题。

我们需要下面关于整数的引理：

引理 9.6 (欧几里得)**.** 假定 a, b 为互素的整数。则存在整数 u 和 v 使得 $ua + vb = 1$。

通常的证明是利用欧几里得的辗转相除法。我们后面会证明一个在 PA 中的版本。这里我们就不证了。

定理 9.4 (中国剩余定理)**.** 令 $d_0, \cdots, d_n$ 为两两互素的自然数、$a_0, \cdots, a_n$ 为满足 $a_i < d_i$ $(0 \leq i \leq n)$ 的自然数。则存在自然数 c 使得对所有的 $i \leq n$，a_i 是 $\frac{c}{d_i}$ 的余数。换句话说，c 是下列同余方程组的解：

$$\begin{aligned} x &\equiv_{d_0} a_0 \\ x &\equiv_{d_1} a_1 \\ &\vdots \\ x &\equiv_{d_n} a_n。 \end{aligned}$$

证明: 我们对 n 施行归纳。当 $n = 0$ 时是显然的。假定命题对 $n = k$ 成立。我们考察 $n = k + 1$ 的情形。根据归纳假定，存在自然数 b 使得 对所有 $i \leq k$ 都有 $b \equiv_{d_i} a_i$。令 d 为自然数 $d_0, \cdots, d_k$ 的最小公倍数。不难验证，d 和 d_{k+1} 是互素的。

我们先找到整数 r, s 使得 $b + rd = sd_{k+1} + a_{k+1}$：由于 d 和 d_{k+1} 互素，根据欧几里得引理，存在整数 u 和 v 使得 $ud + vd_{k+1} = 1$。将等式两边都乘上 $a_{k+1} - b$，再通过简单移项便可以知道，取 $r = (a_{k+1} - b)u$ 和 $s = (b - a_{k+1})v$ 即可。

令 $z = b + rd = sd_{k+1} + a_{k+1}$。一方面，对 $i \leq k$，我们有

$$z \equiv_{d_i} b + rd \equiv_{d_i} b \equiv_{d_i} \equiv_{d_i} a_i。$$

另一方面，$z \equiv_{d_{k+1}} sd_{k+1} + a_{k+1} \equiv_{d_{k+1}} a_{k+1}$。最后，由于同余方程组的解具有周期 D - $d_0, \cdots, d_{k+1}$ 的最小公倍数。存在足够大的自然数 m 使得 $c = z + mD$ 是非负整数。c 就是我们所要的。 □

要想使用中国剩余定理来将有穷序列 $(a_0, \cdots, a_n)$ 编码，我们需要足够大的两两互素的自然数 $d_0, \cdots, d_n$，下面的引理说明怎样找它们。

引理 9.7. 对任意的 $s \geq 0$，下列 $s + 1$ 个自然数

$$1 + 1 \cdot s!,\ \ 1 + 2 \cdot s!,\ \ \cdots,\ \ 1 + (s + 1) \cdot s!$$

是两两互素的。

证明: 假定某个素数 p 满足 $p|1 + (i + 1)s!$ 且 $p|1 + (j + 1)s!$。则 $p|(j - i)s!$。所以，或者 $p|(j - i)$ 或者 $p|s!$。无论哪种情形，都有 $p|s!$，进而 $p|1$，矛盾。 □

引理 9.8. 定义函数 $\alpha : \mathbb{N}^3 \to \mathbb{N}$ 为

$$\begin{aligned}\alpha(c,d,i) &= \frac{c}{1+(i+1)d} \text{ 中的余数} \\ &= \mu r\,[\exists q \le c(c = q(1+(i+1)d)+r)]。\end{aligned}$$

则 α 在 Q 中是可表示的。

证明: 因为它是从可表示的关系经有界量词和正则极小算子得到的。 □

我们在系统外面（即在 $\mathbb{N}$ 中）验证对所有的 $n, a_0, \cdots, a_n$，存在 c 和 d 使得对任意 $i \le n$ 都有 $\alpha(c,d,i) = a_i$；所以 $\alpha(c,d,i)$ 可以胜任可表示的编码函数。给定 $n, a_0, \ldots, a_n$，让 $s = \max\{n, a_0, \cdots, a_n\}$、$d = s!$、$d_i = 1 + (i+1)\cdot s!$、和 $c =$ 中国剩余定理中的那个数 c。显然我们有 $\alpha(c,d,i) = a_i$.

我们利用数对的编码函数来把 c 和 d 压缩成一个数。

引理 9.9. 令

$$\begin{aligned}J(a,b) &= \frac{1}{2}(a+b)(a+b+1)+a。\\ K(p) &= \mu a \le p\ \exists b \le p\ J(a,b) = p。\\ L(p) &= \mu b \le p\ \exists a \le p\ J(a,b) = p。\end{aligned}$$

则函数 J, K, L 在 Q 中都是可表示的。

引理 9.10. 定义**哥德尔的 β-函数** 为 $\beta(s,i) = \alpha(K(s), L(s), i)$。则 $\beta(s,i)$ 在 Q 中是可表示的。且对任何自然数 $n, a_0, \cdots, a_n$ 都存在自然数 s 使得对任意 $i \le n$ 都有 $\beta(s,i) = a_i$。

这两个引理的证明我们都留作练习。

定理 9.5. 可表示函数形成的类对原始递归封闭。

证明: 假设 f 的递归定义为：$f(\vec{m}, 0) = g(\vec{m})$ 和 $f(\vec{m}, n) = h(\vec{m}, n, f(\vec{m}, n))$，其中 g 和 h 都是可表示的。则关系

$$P(\vec{m}, n, s) := \beta(s,0) = g(\vec{m}) \wedge \forall i < n\,[\beta(s, i+1) = h(\vec{m}, n, \beta(s,i))]$$

也是可表示的，因为它是可表示关系和函数的复合。直观上看，$P(\vec{m}, n, s)$ 说的是“s 是 f 从 $i = 0$ 到 $i = n$ 的计算历史的编码”。令 $F(\vec{m}, n) = \mu s\ P(\vec{m}, n, s)$。因为 $\mathfrak{N} \models \forall \vec{m}, n \exists s\ P(\vec{m}, n, s)$，根据可表示函数对正则极小算子的封闭性，$F$ 是可表示的。所以，$f(\vec{m}, n) = \beta(F(\vec{m}, n), n)$ 也是可表示的。 □

9.1.5　可表示性定理

由于递归函数类是最小的包含初始函数并且对复合，原始递归和正规 μ- 算子封闭的函数类；综合前面的结果，我们立刻得到下列定理：

定理 9.6 (可表示性定理)**.** 所有的递归函数在 Q 中都是可表示的。因而，所有的递归关系在 Q 中也都是可表示的。

证明: 习题。 □

回忆一下，在给出可表示的关系的定义后，我们立刻知道：所有可表示关系都是递归关系。因此可表示关系就是递归关系。我们把它单列出来，以加深印象：

推论 9.2. 对任何的 k-元关系 $R \subseteq \mathbb{N}^k$ 和任何递归且相容 的扩张 $T \supseteq \mathsf{Q}$，下列命题等价：

(i) R 在 T 中可表示；

(ii) R 是一个递归关系。

对于关心定义复杂性的读者，借助递归论的知识，我们有进一步的推论：

推论 9.3. 对任何的 k-元关系 $R \subseteq \mathbb{N}^k$ 和任何递归且相容 的扩张 $T \supseteq \mathsf{Q}$，下列命题等价：

(i) R 在 T 中可表示；

(ii) R 在 T 中可被一个 Δ_1 的公式表示。

证明: 我们只证明“(i) $\Rightarrow$ (ii)”。如果 R 在 T 中是可表示的，则 R 是递归的。由于 R 和 R 的否定都是递归可枚举的，根据引理 **??**，R 在结构 $\mathfrak{N}$ 中可以被一个 Δ_1 的公式定义。再由 Q 的 Σ_1- 完全性，我们就得到 R 可以被一个 Δ_1 的公式所表示。 □

第 2 节　语法的算术化

回忆一下，我们选择算术语言 $\mathcal{L}_{ar}$ 的初衷是讨论自然数的算术性质。例如，闭语句 $\forall v\,(1 \not\approx 2 \cdot v + 21)$ 表达了关于自然数 1 和 21 的某些性质。表面上看，语言 $\mathcal{L}_{ar}$ 不适合讨论逻辑中的语法性质，例如，“量词符号 $\forall$ 不是一个变元符号”这一事实似乎不属于语言 $\mathcal{L}_{ar}$ 的讨论范围。

下面我们将论证：在语言 $\mathcal{L}_{ar}$ 中我们能够讨论逻辑中的语法，甚至在某种程度上我们还可以讨论语义。关键的想法是用编码。这一想法是哥德尔在不完全性定理证明中首先使用的，通常被称为*哥德尔 编码*。与前面简化版本的算术语言不同，一旦语言中同时包含

加法和乘法，我们可以把各种对象进行编码，然后通过讨论它们的码间接地讨论对象的性质。我们在递归论部分曾经体验过编码带来的好处，例如，我们把（图灵机或其它）程序用它的码 e 来代表。这样一来，关于程序的命题就转换成关于自然数 e 的命题。我们要做的是把逻辑语法中的对象，如“公式”、“证明”等等都用自然数来编码，从而在语言 $\mathcal{L}_{ar}$ 中研究它们的性质。这一过程就是所谓的**语法的算术化**。

显然，编码的方法不是唯一的，我们的兴趣也不在编码的细节上，除了一点：为了可表示性的需要，我们所感兴趣的对象（如公式，证明等等）在编码之后应该是自然数的递归子集。哥德尔编码在 1930 年代被视为非常神奇的技巧。但现在由于计算机的普及，把各种对象数字化已经是司空见惯了。直观上看，我们下面列出的清单中的所有对象（除了最后一项“可证性”）都是可以用计算机处理的，因而都是递归的。

9.2.1　哥德尔编码

我们首先给每一个逻辑符号指派一个自然数。

符号 ζ	$\forall$	0	S	$+$	$\cdot$	(	)	$\neg$	$\to$	$=$	v_0	v_1	$\dots$
哥德尔数 $\sharp\zeta$	1	3	5	7	9	11	13	15	17	19	21	23	$\dots$

接下来，我们指派给字符串 $\xi = \zeta_0 \dots \zeta_n$ 的哥德尔数为 $\langle \sharp\zeta_0, \cdots, \sharp\zeta_n \rangle = p_0^{\sharp\zeta_0+1} \dots p_n^{\sharp\zeta_n+1}$。

注：

- 下面我们给项编码时会把项当作有穷序列来处理，因此所有项（和公式）的编码都是偶数。所以用奇数来代表原始符号有一个小小的好处，我们可以区别作为符号的 0 还是作为项的 0；前者的编码是 3 而后者是 $2^{3+1} = 16$。
- 上述的编码方法也可以推广到更一般的语言，只要语言中的参数集 L 是可判定的即可。
- 我们这一节中的一切都是在标准自然数上完成的，与形式系统无关。因此使用指数函数等等均不会带来任何问题。

(1) $V = \{\sharp\alpha : \alpha$ 是一个变元 $\}$ 是原始递归的。

由于 $V = \{n \in \mathbb{N} : (\exists k < n) n = 2k + 21\}$，所以显然是原始递归的。

注意：我们实际上是在自然数中创造一个逻辑中变元符号的同构像。例如，21 就是 v_0 在这个同构下的像。为了强调逻辑中的对象与其在自然数中的像的联系，我们用加下划线的方法来增强暗示性，例如，V 中的元素就被称为一个“变元”。现在 $\forall v\ (1 \not\approx$

$2v+21$) 说的是“$\underline{\forall}$ 不是一个$\underline{\text{变元}}$”。这样，通过讨论自然数里的同构像，我们间接地可以在算术语言 $\mathcal{L}_{ar}$ 内讨论逻辑中的语法。

一般地，对于一个逻辑中的对象 O，我们用 $\underline{O}$ 表示 O 在自然数中的同构像，即 $\underline{O}=\{\sharp a : a\in O\}$。

当然，$\underline{v_0}$ 和 $\sharp v_0$ 都是 21。必要的时候，我们仍会使用符号 $\sharp$。我们用 $\flat\underline{a}$ 表示 $\sharp a$ 的逆运算，即，$\sharp\xi = x$ 当且仅当 $\flat x=\xi$。（对不属于编码值域的自然数 y，我们不关心 $\flat y$ 的值，可以定义它为任何事先给定的符号。）

(2) 集合 $\{t : t$ 是一个$\underline{\text{项}}\}$ 是原始递归的。

证明：仿照项的递归定义，$\underline{\text{项}}$ 具有如下的递归定义：t 是一个$\underline{\text{项}}$，如果

- $\exists s<t$ 使得 $t=\langle s\rangle$ 且 s 是一个$\underline{\text{变元}}$ 或者 $s=\underline{0}$；或者
- $\exists r,s<t$ 使得 $t=\langle r\rangle\hat{}s$ 且 $r=\underline{\mathsf{S}}$ 且 s 是一个$\underline{\text{项}}$；或者
- $\exists q,r,s<t$ 使得 $t=\langle q\rangle\hat{}r\hat{}s$ 且 $q=\underline{+}\vee q=\underline{\cdot}$ 且 r 和 s 都是$\underline{\text{项}}$。

所以结论成立。 □

注意，定义项的哥德尔数通常由两种办法。以 $t=\mathsf{SS0}$ 为例，一种是 $\sharp t=\langle\sharp\mathsf{S},\sharp\mathsf{S},\sharp\mathsf{0}\rangle$ 序列长度为 3；一种是 $\sharp t=\langle\sharp\mathsf{S},\langle\sharp\mathsf{S},\sharp\mathsf{0}\rangle\rangle$ 序列长度为 2。我们采用的是前者。

类似地，

(3) 集合 $\{a : a$ 是一个$\underline{\text{原子公式}}\}$ 是原始递归的。

(4) 集合 $\{a : a$ 是一个$\underline{\text{公式}}\}$ 是原始递归的。

(5) 存在一个原始递归函数 Sb 使得对任意项或公式 α，对任意变元 x 和任意项 t，我们有：

$$\mathrm{Sb}(\sharp\alpha,\sharp x,\sharp t)=\sharp\alpha_t^x。$$

证明：仿照替换的定义

$$\alpha_t^x=\begin{cases} t, & \text{如果 } \alpha \text{ 是变元 } x;\\ \mathsf{S}u_t^x, & \text{如果 } \alpha \text{ 是项 } \mathsf{S}u;\\ (u_1)_t^x\square(u_2)_t^x, & \text{如果 } \alpha \text{ 是 } u_1\square u_2 \text{ 其中 } \square \text{ 是 } + \text{ 或 } \cdot;\\ (u_1)_t^x\approx(u_2)_t^x, & \text{如果 } \alpha \text{ 是 } u_1\approx u_2;\\ (\neg\beta_t^x) & \text{如果 } \alpha=(\neg\beta);\\ (\beta_t^x\to\gamma_t^x) & \text{如果 } \alpha=(\beta\to\gamma);\\ \forall y\ \beta_t^x & \text{如果 } y\neq x \text{ 且 } \alpha \text{ 是 } \forall y\beta;\\ \alpha, & \text{其它情形。}\end{cases}$$

我们可以利用强递归来定义 $\mathrm{Sb}(a,b,c)$。具体步骤我们留作习题。 □

(6) 函数 $f(n) = \natural(\mathsf{S}^n\mathsf{0})$ 是原始递归的，因而，集合 $\{m : m$ 是一个数码$\}$ 是原始递归的。

证明：$f(0) = \langle\underline{0}\rangle$ 且 $f(n+1) = \langle\underline{\mathsf{S}}\rangle\hat{}f(n)$。 □

(7) 定义自然数上的二元关系“x 在 a 中自由出现”如下：x 是一个变元，a 是一个项或公式，且 $\natural x$ 在 $\natural a$ 中自由出现。（显然，当 $\natural a$ 为一个项时，自由出现和出现的意思是一样的。）则关系“x 在 a 中自由出现”是原始递归的。

证明：x 在 a 中自由出现 当且仅当 $\mathrm{Sb}(a, x, \langle\underline{0}\rangle) \neq a$。 □

(8) 集合 $\{a : a$ 是一个闭语句$\}$ 是原始递归的。

证明：a 是一个闭语句 当且仅当 a 一个公式 且对任何 $x < a$，如果 x 是一个变元 则 x 不在 a 中自由出现。 □

(9) 定义自然数上的三元关系“t 在 a 中可以替换 x”，如果 x 是一个变元，a 是一个公式，t 是一个项，且 $\natural t$ 在 $\natural a$ 中可以替换 $\natural x$。则关系“t 在 a 中可以替换 x”是原始递归的。

证明：首先请读者自己给出“a 是 $\neg b$”、“a 是 $b \to c$”和“a 是 $\forall y b$”的定义，并验证它们可以是原始递归的。

关系“t 在 a 中可以替换 x”可以递归地定义如下：

- 如果 a 是原子公式，则 t 在 a 中可以替换 x 永远成立；
- 如果 a 是 $\neg b$，则 t 在 a 中可以替换 x 当且仅当 t 在 b 中可以替换 x；
- 如果 a 是 $b \to c$，则 t 在 a 中可以替换 x 当且仅当 t 在 b 和 c 中都可以替换 x；
- 如果 a 是 $\forall y b$，则 t 在 a 中可以替换 x 当且仅当 y 不在 t 中自由出现 且 t 在 b 中可以替换 x。

□

(10) 关系“a 是 b 的一个全称概括”是原始递归的。

证明：细节留给读者。 □

(11) 集合 $\{a : a$ 是一个（一阶逻辑意义下的）形如 (A1)、(A2) 或 (A3) 的（命题逻辑）公理$\}$ 是原始递归的。

证明: 我们只验证 (A1) 的情形，即，$\alpha := \natural a$ 具有 $(\sigma \to (\tau \to \sigma))$ 的形式且 σ 和 τ 为素公式。

注意：一个公式 σ 是素公式当且仅当它的第一个符号不是左括号 (。所以，“s 是一个素公式” 是原始递归的。

因此，a 是形如 (A1) 的公理 当且仅当 $(\exists s, t < a)$，s 和 t 是素公式，且

$$a = \underline{(}\hat{}s\hat{}\underline{\to}\hat{}\underline{(}\hat{}t\hat{}\underline{\to}\hat{}s\hat{}\underline{)}\hat{}\underline{)}。$$

□

下面 5 条分别对应一阶逻辑的第 2 到第 6 组公理:

(12) 集合 $\{a : a$ 是形如 $\forall x\varphi \to \varphi_t^x$ 的公理，其中 t 在 φ 中可以替换 $x\}$ 是原始递归的。

证明: （梗概）根据 (9) 我们只需原始递归地判断 a 具有 $\forall x\varphi \to \varphi_t^x$ 的形式即可。而 a 具有正确的形式当且仅当 $(\exists x, p, t, b, c < a)$ [a 是 $b \to c$ 且 b 是 $\forall xp$ 且 $c = \mathrm{Sb}(p, x, t)$ 且 t 在 p 中可替换 x]；其中 $\mathrm{Sb}(p, x, t)$ 是第 (5) 条中定义的替换函数。 □

(13) 集合 $\{a : a$ 是 形如 $\forall x(\alpha \to \beta) \to \forall x\alpha \to \forall x\beta$ 的公理$\}$ 是原始递归的。

(14) 集合 $\{a : a$ 是形如 $\varphi \to \forall x\varphi$ 的公理，其中 x 不在 a 中自由出现$\}$ 是原始递归的。

(15) 集合 $\{a : a$ 是形如 $x \approx x$ 的公理$\}$ 是原始递归的。

(16) 集合 $\{a : a$ 是形如 $x \approx y \to \varphi \to \varphi'$ 的公理 其中 φ 是一个原子公式且 φ' 是将 φ 中的若干个 x 替换成 y 而得到的 $\}$ 是原始递归的。

证明: a 具有正确的形式当且仅当 $(\exists x, y, b, c, p, p' < a)$ [a 是 $b \to c$、b 是 $x \approx y$、c 是 $p \to p'$ 且 x 和 y 是 p 是一个原子公式、$\mathrm{lh}(p') = \mathrm{lh}(p)$、且 $\forall j < \mathrm{lh}(p)((p)_j = (p')_j \vee ((p)_j = x \wedge (p')_j = y))$]。 □

总结一下从 (10) 到 (16) 我们就有:

(17) 集合 $\{a : a$ 是一个逻辑公理$\}$ 是原始递归的。

证明: 因为逻辑公理 都是 (11)–(16) 中公式 的全称概括。 □

(18) 令 T 为一个被集合 $X \subseteq T$ 所公理化的理论。根据公理化的定义，X 必须是可判定的，即集合 X 是递归的。则谓词“b 是一个 T 上的一个证明序列”是递归的。

证明: “b 是一个 T 上的一个证明序列” 当且仅当 b 是一个有穷序列的哥德尔 数、$b \neq 1$ 并且 $\forall k < \mathrm{lh}(b)[(b)_k \in X$ 或 $(b)_k$ 是逻辑公理 或 $(\exists i, j < k)(b)_i = (b)_j \to (b)_k]$。 □

(19) 令 T 同前。定义谓词 $\mathrm{bew}_T(b,a)$ 为“b 是一个 T 上的一个证明序列 且 $b_{\mathrm{lh}(b)-1}=a$”。则 $\mathrm{bew}_T(b,a)$ 是递归的。(“Beweis”是“证明”的德语。)

(20) 令 T 同前。定义谓词 $\mathrm{bwb}_T(a)$ 为 $\exists b\,\mathrm{bew}_T(b,a)$。则 $\mathrm{bwb}_T(a)$ 是递归可枚举的。在一般情况下是不递归的。(“Beweisbar”是“可证”的德语。)

$\mathrm{bew}_T(b,a)$ 说的是“b 是一个 T 上对公式 a 的一个证明”，而 $\mathrm{bwb}_T(a)$ 说的是“公式 a 在 T 中是 可证的”。由于我们后面经常会用到它们，我们特别引入这两个新的记号。

第 3 节　不动点引理和递归定理

9.3.1　不动点引理

引理 9.11 (不动点引理)**.** 给定一个公式 $\beta(v_1)$ 其中只有变元 v_1 自由出现，我们可以能行的找到一个闭语句 σ 使得:

$$\mathsf{Q}\vdash \sigma\leftrightarrow\beta(\mathsf{S}^{\sharp\sigma}\mathsf{0})。$$

直观上看，σ 说的是“β 对我成立”。人们经常使用 $\ulcorner\sigma\urcorner$ 来表示 $\mathcal{L}_{ar}$ 中的项 $\mathsf{S}^{\sharp\sigma}\mathsf{0}$，即，$\sharp\sigma$ 的数码。从而不动点引理的结论可以表达得更有暗示性：$\mathsf{Q}\vdash\sigma\leftrightarrow\beta(\ulcorner\sigma\urcorner)$。

证明: 令 $\theta(v_1,v_2,v_3)$ 表示递归函数

$$\langle\sharp\alpha,n\rangle\mapsto\sharp\,\alpha(\mathsf{n})$$

的一个公式，其中 α 为一个仅含一个自由变元的公式。所以

$$\mathsf{Q}\vdash\forall v_3\,[\theta(\ulcorner\alpha\urcorner,\mathsf{n},v_3)\leftrightarrow v_3\approx\ulcorner\alpha(\mathsf{n})\urcorner] \tag{9.3}$$

[注意：这是我们使用可表示性以及句法算术化的地方。]

考察公式 $\tau(v_1)$:

$$\tau(v_1):=\forall v_3\,[\theta(v_1,v_1,v_3)\to\beta(v_3)]。$$

令 q 为公式 $\tau(v_1)$ 的哥德尔编码。再令闭语句 σ 为

$$\sigma:=\forall v_3(\theta(\mathsf{q},\mathsf{q},v_3)\to\beta(v_3))。 \tag{9.4}$$

注意 σ 是在公式 $\tau(v_1)$ 中将唯一的变元 v_1 用 $\tau(v_1)$ 自己的哥德尔编码 q 代入而得到的。

我们验证

$$\mathsf{Q}\vdash\sigma\leftrightarrow\beta(\ulcorner\sigma\urcorner)。 \tag{9.5}$$

根据 θ 的选择，如果我们在 (9.3) 式中将 α 和 n 分别用 τ 和 $q = \sharp\tau$ 代入，我们就得到

$$\mathsf{Q} \vdash \forall v_3[\theta(\mathsf{q}, \mathsf{q}, v_3) \leftrightarrow v_3 \approx \ulcorner\sigma\urcorner]。 \tag{9.6}$$

先看 (9.5) 式中从左向右 “$\Rightarrow$” 的方向：由 (9.4) 式，我们有 $\sigma \vdash \theta(\mathsf{q}, \mathsf{q}, \ulcorner\sigma\urcorner) \to \beta(\ulcorner\sigma\urcorner)$。根据 (9.6)，$\mathsf{Q} \vdash \theta(\mathsf{q}, \mathsf{q}, \ulcorner\sigma\urcorner)$。所以 $\mathsf{Q} \cup \{\sigma\} \vdash \beta(\ulcorner\sigma\urcorner)$。

再看 (9.5) 式中从右向左 “$\Leftarrow$” 的方向：根据 (9.6)，$\beta(\ulcorner\sigma\urcorner) \to [\forall v_3(\theta(\mathsf{q}, \mathsf{q}, v_3) \to \beta(v_3))]$，原因是只有唯一的那样的 v_3，也就是 $\ulcorner\sigma\urcorner$。而方括号中的公式恰恰是 σ，我们就得到了 (9.5) 式。 □

注意：尽管我们把不动点引理写得富有暗示性，但不动点 σ 本身可能 “什么都没说”，或者与 β 毫无关系。例如，令 $\beta(v_1)$ 为 $\exists x(v_1 \approx x + x)$ （即表达，v_1 是一个偶数），则由于我们的编码保证了任何闭语句的哥德尔数都是偶数，我们可以取不动点 σ 为 $\mathsf{0} \approx \mathsf{0}$ 或 $\mathsf{0} \not\approx \mathsf{S0}$ 等等，显然它与变元的奇偶性毫无关系。

这正是哥德尔伟大的地方。说谎者悖论 “这句话为假” 是真正的循环论证。我们无法直接定义 “这句话”。哥德尔巧妙地利用了哥德尔编码（即利用语法对象的同构像）打破了这种循环。不动点定理中只是断言存在某个闭语句 σ 和某个数码 n 可以使得 $\sigma \leftrightarrow \beta(\mathsf{n})$。这里面没有任何的循环。只不过碰巧，$\sigma$ 的同构像 $\ulcorner\sigma\urcorner$ 刚好也可以被选作 n。

9.3.2　克林尼递归定理

在递归论中，克林尼证明了著名的递归定理：

定理 9.7 (克林尼)**.** 令 $\varphi_0, \varphi_1, \cdots$ 为所有部分递归函数的能行枚举（见通用函数定理）。对任何的递归函数 $f(x)$ 都存在一个自然数 e，使得 $\varphi_{f(e)} = \varphi_e$。

递归定理也被称为不动点定理，它在递归论中有非常广泛的应用。它的证明并不长，但需要用到 s-m-n-定理，所以我们略去不讲。递归定理可以看作是哥德尔不动点引理在递归论中的版本，都与自指示有关。证明也很类似，短但充满神秘。在递归论中，为了帮助理解，人们给出了一些对递归定理证明的直观解释。大致上说是某种 “对角化策略的失败”。这里，我们借用递归论中的解释来看不动点引理的证明，这种解释对证明的理解和定理的应用都不重要，我们只希望能减少一点神秘感而已。

让我们能行地列出所有只含有自由变元 v_1 公式：$\varphi_0(v_1), \varphi_1(v_1), \cdots$。其次，对自然数 $0, 1, 2, \cdots$，我们用下表的第 i 行记录所有 Q 是否证明 $\varphi_i(\mathsf{0})$，证明 $\varphi_i(\mathsf{S0})$，证明 $\varphi_i(\mathsf{S^20}), \cdots\cdots$ 等等。我们用 $\surd$ 表示 Q 能证明，$\times$ 表示 Q 不能证明。例如，结果可能是：

	0	1	2	3	⋯	q	⋯
$\varphi_0(v_1)$	√	√	×	×	⋯	×	⋯
$\varphi_1(v_1)$	×	√	√	×	⋯	×	⋯
$\varphi_2(v_1)$	√	×	×	×	⋯	√	⋯
⋮			⋮		⋮		⋮
⋮			⋮		⋮		⋮
$\varphi_q(v_1)$	√	×	√	×	⋯	√	⋯
⋮			⋮		⋮		⋮

现考察 Q 是否能证“施 β 于对角线上的数码”，即 Q 是否能证 $\beta(\ulcorner\varphi_n(n)\urcorner)$。由于函数 $n \mapsto \sharp\varphi_n(n)$ 是递归的，$\beta(\ulcorner\varphi_{v_1}(v_1)\urcorner)$ 逻辑等价于某个公式只含有 v_1 为自由变元的公式，比如说 $\varphi_q(v_1)$。所以它也会出现在我们表中的第 q 行，即，对任意的 n，$\mathsf{Q} \vdash \beta(\ulcorner\varphi_n(n)\urcorner)$ 当且仅当 $\mathsf{Q} \vdash \varphi_q(\mathsf{n})$。

	0	1	2	3	⋯	q	⋯
$\varphi_0(v_1)$	$\beta(\sharp\,\varphi_0(0))$				⋯		⋯
$\varphi_1(v_1)$		$\beta(\sharp\,\varphi_1(1))$			⋯		⋯
$\varphi_2(v_1)$			$\beta(\sharp\,\varphi_2(2))$		⋯		⋯
⋮			⋮		⋮		⋮
⋮			⋮		⋮		⋮
$\varphi_q(v_1)$					⋯	$\beta(\sharp\,\varphi_q(q))$	⋯
⋮			⋮		⋮		⋮

特别地，在对角线的位置 q，我们有 $\mathsf{Q} \vdash \varphi_q(\mathsf{q}) \leftrightarrow \beta(\ulcorner\varphi_q(q)\urcorner)$。所以，令 σ 为 $\varphi_q(\mathsf{q})$，我们就有 $\mathsf{Q} \vdash \sigma \leftrightarrow \beta(\ulcorner\sigma\urcorner)$。

第 4 节　不可定义性，不完全性和不可判定性

9.4.1　塔尔斯基定理

定理 9.8 (塔尔斯基不可定义性定理)**.** 集合 $\sharp\,\mathrm{Th}\,(\mathfrak{N})$ 在结构 $\mathfrak{N}$ 中是不可定义的。

证明: 考察任何一个（潜在的 $\sharp\,\mathrm{Th}\,(\mathfrak{N})$ 的定义）公式 $\beta(v_1)$。对 $\neg\beta$ 使用不动点引理，我们就得到一个闭语句 σ 使得

$$\mathsf{Q} \vdash \sigma \leftrightarrow \neg\beta(\ulcorner\sigma\urcorner)。$$

于是

$$\mathfrak{N} \models \sigma \leftrightarrow \neg\beta(\ulcorner\sigma\urcorner)。$$

所以 $\mathfrak{N} \models \sigma$ 当且仅当 $\mathfrak{N} \not\models \beta(\ulcorner\sigma\urcorner)$。这就排除了 $\beta(v_1)$ 定义 $\sharp\,\mathrm{Th}\,(\mathfrak{N})$ 的可能性。 □

推论 9.4. Th $(\mathfrak{N})$ 是不是可判定的，即，$\sharp\,\mathrm{Th}\,(\mathfrak{N})$ 不是一个递归集。

9.4.2　ω-相容性与哥德尔第一不完全性定理

我们先给出一个与塔尔斯基定理较接近的不完全性定理的版本。回忆一下，我们说一个理论是可公理化的时候，隐含地要求其公理集是递归的。

定理 9.9 (哥德尔第一不完全性定理)**.** 如果理论 $T \subseteq \mathrm{Th}\,(\mathfrak{N})$ 是可公理化的，则 T 是不完全的。特别地，没有 Th $(\mathfrak{N})$ 的完全的公理化。

证明: 假定 $T \subseteq \mathrm{Th}\,(\mathfrak{N})$ 是完全的，则 $T = \mathrm{Th}\,(\mathfrak{N})$。由于任何可公理化的理论 T 都是递归可枚举的，Th $(\mathfrak{N})$ 就变得可定义了，事实上被一个 Σ_1-公式定义。这与塔尔斯基定理矛盾。 □

当然哥德尔定理还有其它版本，最终我们会证明罗瑟的改进版，不仅证明中不需要塔尔斯基的定理，就连叙述中也没有谈到标准自然数 $\mathfrak{N}$，是一个关于纯语法的命题。我们下面先讲哥德尔本人的版本，其中用到了 ω-相容性的概念。我们的动机一方面是了解历史，另一方面 ω-相容性本身对我们将来学习（如理解第二不完全性定理）也有帮助。

定义 9.3. 令 T 为语言 $\mathcal{L}_{ar}$ 上的一个理论。我们称 T 是ω- **不相容的**，如果存在一个公式 $\varphi(x)$ 使得 $T \vdash \exists x\varphi(x)$ 并且对所有 $n \in \mathbb{N}$，都有 $T \vdash \neg\varphi(\mathsf{n})$。我们称 T 是ω-**相容的**，如果 T 不是 ω-不相容的，也就是说，如果 $T \vdash \exists x\varphi(x)$ 则对某一个 $n \in \mathbb{N}$，我们有 $T \nvdash \neg\varphi(\mathsf{n})$。

我们看几个有关 ω-相容性的简单事实:

- 如果 T 是 ω-相容的，则 T 是相容 的。
- ω-相容性的概念涉及了标准自然数 $\mathbb{N}$ （或 ω），因此并不是一个“纯语法”的概念，这一点与相容性很不一样。
- 根据 ω-不相容性的定义，如果 T 是 ω- 不相容 的，则 $\mathfrak{N} \not\models T$。取逆否命题，我们得到：如果 $\mathfrak{N} \models T$ 则 T 是 ω-相容 的。因此我们通常讨论的理论，如 Q 或 PA，都是 ω-相容的。
- 考察一个包含常数 c 的语言，如 $\mathcal{L}_{ar} \cup \{c\}$，则理论 $\mathsf{PA} + \{c \neq \mathsf{n} : n \in \mathbb{N}\}$ 是相容但不是 ω-相容的。(这里记号 $T + T'$ 表示包含 T 和 T' 的最小的理论。)

- 后面我们要讲的哥德尔第二不完全性定理会告诉我们：（假定 PA 是相容的）在语言 $\mathcal{L}_{ar}$ 上，理论 $\mathsf{PA}+\neg\mathsf{con}(\mathsf{PA})$ 是相容但不是 ω-相容 的。

下面是哥德尔第一不完全性定理的最初版本。

定理 9.10. 令 $T \supseteq \mathsf{Q}$ 为一个可（递归）公理化的理论。如果 T 是 ω-相容的，则存在一个 Π_1-闭语句 σ 使得 $T \nvdash \sigma$ 并且 $T \nvdash \neg\sigma$。

证明: 令 $\mathsf{bew}(y,x)$ 为 T 中表示递归关系 bew_T 的公式，并且定义 $\mathsf{bwb}(x)$ 为 $\exists y\mathsf{bew}(y,x)$。再令 σ 为公式 $\neg\mathsf{bwb}(x)$ 的不动点。注意：根据推论 **??**，我们可以假定 $\mathsf{bew}(y,x)$ 是 Δ_1 的，因而 $\mathsf{bwb}(x)$ 是 Σ_1 的，再根据不动点引理的证明，可以假定 σ 是 Π_1 的。我们有：

$$T \vdash [\sigma \leftrightarrow \neg\mathsf{bwb}(\ulcorner\sigma\urcorner)]。 \quad (*)$$

如果 $T \vdash \sigma$，则根据前面练习，$T \vdash \mathsf{bwb}(\ulcorner\sigma\urcorner)$。再根据 **(*)**，$T \vdash \neg\mathsf{bwb}(\ulcorner\sigma\urcorner)$，这与 T 的相容性矛盾。所以，$T \nvdash \sigma$。

接下来，根据可表示性定义，我们有对任意的 $n \in \mathbb{N}$，$T \vdash \neg\mathsf{bew}(\mathsf{n},\ulcorner\sigma\urcorner)$。由 T 的 ω-相容 性，$T \nvdash \exists y\mathsf{bew}(y,\ulcorner\sigma\urcorner)$，即，$T \nvdash \mathsf{bwb}(\ulcorner\sigma\urcorner)$。再次利用 **(*)**，我们有 $T \nvdash \neg\sigma$。 □

9.4.3　罗瑟的改进

在 1936 发表的一篇文章中，罗瑟[4]证明了哥德尔定理最初版本中关于 T 的 ω- 相容性的假设可以减弱成“T 是相容的”。从而完全摆脱了对语义的依赖，第一不完全性定理成为一个关于纯语法的命题。

定理 9.11 (哥德尔-罗瑟)**.** 令 $T \supseteq \mathsf{Q}$ 为一个可（递归）公理化的理论。如果 T 是相容的，则存在一个 Π_1-闭语句 σ 使得 $T \nvdash \sigma$ 并且 $T \nvdash \neg\sigma$。

在叙述罗瑟的改进之前，让我们再看一下前面证明中用到 ω-相容性的地方，或许对理解罗瑟的技巧有所帮助。我们从 $T \vdash \neg\sigma$ 开始。假定 $T \vdash \neg\sigma$，则，一方面可表示性告诉我们 $T \vdash \exists y_1\mathsf{bew}(y_1,\ulcorner\neg\sigma\urcorner)$；而另一方面，根据 **(*)**，我们也有 $T \vdash \exists y_2\mathsf{bew}(y_2,\ulcorner\sigma\urcorner)$。假如 $\mathfrak{N}$ 是 T 的一个模型（这是一个比 ω-相容还要强的条件），我们立刻可以从标准的“y_1”和“y_2”中解码得到 $T \vdash \neg\sigma$ 和 $T \vdash \sigma$。尽管对一般的情形，如 T 是 ω-不相容的时候，我们无法这样做；但这多少提示我们考虑“y_1”和“y_2”的关系。

证明: 给定一个相容的理论 T，令 $\mathsf{prov}(x)$（其实为 $\mathsf{prov}_T(x)$，我们略去下标）为公式

$$\exists y[\mathsf{bew}(y,x) \wedge (\forall z < y)\neg\mathsf{bew}(z,\tilde{\neg}x)],$$

[4]罗瑟，J. Barkley Rosser，美国数学家，逻辑学家。

其中 $\tilde{\neg}$ 是原始递归函数 $\sharp\alpha \mapsto \sharp(\neg\alpha)$ 在 T 中的表示。具体地说，令 $\theta(x,y)$（作为函数）表示 $\sharp\alpha \mapsto \sharp(\neg\alpha)$，则 $\mathsf{bew}(z,\tilde{\neg}x)$ 就是 $\exists y(\mathsf{bew}(z,y)\wedge\theta(x,y))$。注意：当 x 为 $\ulcorner\alpha\urcorner$ 时，$\tilde{\neg}x$ 就是 $\ulcorner\neg\alpha\urcorner$。

断言 1. 如果 $T\vdash\alpha$ 则 $T\vdash\mathsf{prov}(\ulcorner\alpha\urcorner)$。

断言 1 的证明. 假定 $T\vdash\alpha$，则对某个 $n\in\mathbb{N}$，$T\vdash\mathsf{bew}(\mathsf{n},\ulcorner\alpha\urcorner)$。由 T 的相容性，$T\nvdash\neg\alpha$，所以对所有的 $k\in\mathbb{N}$，$T\vdash\neg\mathsf{bew}(\mathsf{k},\ulcorner\neg\alpha\urcorner)$。所以 $T\vdash(\forall z<\mathsf{n})\neg\mathsf{bew}(z,\ulcorner\neg\alpha\urcorner)$，因而断言 1 成立。(注意：断言 1 对 bew 也成立。)

断言 2. 如果 $T\vdash\neg\alpha$ 则 $T\vdash\neg\mathsf{prov}(\ulcorner\alpha\urcorner)$。

断言 2 的证明. 假定 $T\vdash\neg\alpha$，则对某个 $m\in\mathbb{N}$，$T\vdash\mathsf{bew}(\mathsf{m},\ulcorner\neg\alpha\urcorner)$。我们通过“比较 y 和 m 的大小”来证明

$$\forall y[\neg\mathsf{bew}(y,\ulcorner\alpha\urcorner)\vee(\exists z<y)\mathsf{bew}(z,\ulcorner\neg\alpha\urcorner)]。$$

注意：虽然在 Q 中我们无法证明 $\forall x\forall y(x<y\vee x\approx y\vee y<x)$，但对每一个 $m\in\mathbb{N}$，$\mathsf{Q}\vdash\forall y(\mathsf{m}<y\vee\mathsf{m}\approx y\vee y<\mathsf{m})$。因为 $T\nvdash\alpha$，所以 $T\vdash\forall y\leq\mathsf{m}\neg\mathsf{bew}(y,\ulcorner\alpha\urcorner)$。另一方面，$T\vdash y>\mathsf{m}\to(\exists z<y)\mathsf{bew}(z,\ulcorner\neg\alpha\urcorner)$（$z=\mathsf{m}$ 就是存在的证据)。这就验证了断言 2。(注意：对 bew，我们无法照搬证明。)

最后，令 σ 为 $\neg\mathsf{prov}(x)$ 的不动点，即，$T\vdash\sigma\leftrightarrow\neg\mathsf{prov}(\ulcorner\sigma\urcorner)$。通过与前面类似的分析，我们可以假定 σ 是 Π_1 的。我们验证 σ 是独立于 T 的：

如果 $T\vdash\sigma$，则根据断言 1，$T\vdash\mathsf{prov}(\ulcorner\sigma\urcorner)$，这与 T 的相容性矛盾。如果 $T\vdash\neg\sigma$，则根据断言 2，$T\vdash\neg\mathsf{prov}(\ulcorner\sigma\urcorner)$，这同样地与 T 的相容 性矛盾。　□

注意：断言 2 告诉我们 $T\vdash\neg\mathsf{prov}(\ulcorner\bot\urcorner)$，其中 $\bot$ 是 $0\neq0$（或其它恒假的公式)。

我们不能用 bwb_T 来取代 prov_T。我们将会把 $\neg\mathsf{bwb}_T(\ulcorner\bot\urcorner)$ 记为 con_T，它就是相容性的“形式化”。哥德尔的第二不完全性定理说的就是 $T\nvdash\mathsf{con}_T$。

所以，从“T 的”角度看，bwb 和 prov 是很不一样的，但它们的不同在标准自然数模型 $\mathfrak{N}$ 中体现不出来。再有，$T\vdash\neg\mathsf{prov}(\ulcorner\bot\urcorner)$ 说的是 $T\vdash\forall y[\neg\mathsf{bew}(y,\ulcorner\bot\urcorner)\vee(\exists z<y)\mathsf{bew}(z,\ulcorner\top\urcorner)]$，而 $T\vdash\neg\mathsf{bwb}(\ulcorner\bot\urcorner)$ 说的是 $T\vdash\forall y\neg\mathsf{bew}(y,\ulcorner\bot\urcorner)$。析取式的后项使前者比后者弱得多，这也说明了为什么我们不用 $\neg\mathsf{prov}(\ulcorner\bot\urcorner)$ 来形式化相容性。

9.4.4　强不可判定性

人们也许会问，把那些独立的语句添加到公理集中是否能消除不完全的现象呢？下面我们证明添加任何公理集，只要是递归的公理集，都无法消除不完全性。注意：要求公理集是递归的是起码的条件。事实上，我们有下列更强的结论。

定理 9.12 (Q 强不可判定性)**.** 任何一个理论 T 如果满足 $T\cup\mathsf{Q}$ 是相容 的，则 T 不是递归的。

注意我们的背景语言是算术语言 $\mathcal{L}_{ar}$，因此在逻辑公理中就包括含有加法和乘法的语句。所以像普莱斯伯格算术的可判定性与本定理并无矛盾。

证明: 令 $T' = T + \mathsf{Q}$。假如 T 是递归的，则 T' 也是：因为对任一句子 α，α 属于 T' 当且仅当 $(Q1 \wedge Q2 \wedge \cdots \wedge Q7) \to \alpha$ 属于 T。（这里我们看出 T 的有穷性给我们带来的方便。）根据可表示性定理，存在某个公式 $\beta(v)$ 在 Q 中表示递归集 T'。

对 $\neg\beta(v)$ 使用不动点引理，我们得到一个闭语句 σ 使得

$$\mathsf{Q} \vdash \sigma \leftrightarrow \neg\beta(\ulcorner\sigma\urcorner)。$$

直观上说，σ 说“我不属于 T'”。

假如 $\sigma \notin T'$，则根据可表示性，$\mathsf{Q} \vdash \neg\beta(\ulcorner\sigma\urcorner)$。因为 σ 是 $\neg\beta(v)$ 的不动点，$\mathsf{Q} \vdash \sigma$。所以 $\sigma \in T'$，因为任何理论对推导都是封闭的。这一矛盾表明 $\sigma \in T'$。但是，如果 $\sigma \in T'$，则也由可表示性，我们得到 $\mathsf{Q} \vdash \beta(\ulcorner\sigma\urcorner)$。同样，因为 σ 是不动点，$\mathsf{Q} \vdash \neg\sigma$。所以，$\neg\sigma \in T'$。这与 $T \cup \mathsf{Q}$ 的相容性矛盾。

所以，T 不是递归的。　□

推论 9.5 (丘奇)**.** 固定语言 $\mathcal{L}_{ar}$。一阶逻辑的普遍有效性是不可判定的；即，集合 $\{\ulcorner\sigma\urcorner : \vdash \sigma\}$ 不是一个递归集。

注意：该集合是递归可枚举的。

第 10 章　哥德尔第二不完全性定理

这一章的内容是证明哥德尔第二不完全性定理。它与哥德尔第一不完全性定理的证明有类似之处。据说冯诺依曼知道了哥德尔第一不完全性定理之后，立刻意识到同样的思路可以证明更强的第二不完全性定理，但哥德尔在 1931 的文章中已经叙述了这一点。但是我们会看到并不是所有人都是冯诺依曼。即便在第一不完全性定理的基础上，想证明哥德尔第二不完全性定理还是不容易的。当然有可能直接证明哥德尔第二不完全性定理，而把第一不完全性定理当作推论。我们分开证明的动机仍然是分散难点，并且必要的反复可以加深我们的理解。

哥德尔第二不完全性定理的一种通俗表达如下：如果一个足够强的可公理化的理论 T，例如 PA，是相容的，则它的相容性在 T 中不可证。这样的通俗表达足以用来解释为什么希尔伯特纲领不能按照原封不动的设想实现。

让我们看得稍微仔细一点。结论中的短语“它的相容性”是语言 $\mathcal{L}_{ar}$ 中的一个闭语句 con_T，我们马上会严格定义它。而另一方面，前提中的“相容”以及结论中的“可证”都是在“外面”看的，是在元数学中的；换句话说，前提中的“相容”说的是没有从 T 到矛盾式 $0 = 1$ 的“标准”证明。这样的通俗表达和说我们可以把 con_T 当作不完全性的例证差不了多少。

我们下面将要证明的哥德尔第二不完全性定理比上面的通俗表达要强得多。它断言上述表达的一个*形式化表述*可以*在 T 内*得到证明，即，

$$\vdash_T \mathsf{con}_T \to \neg \mathsf{bwb}_T(\mathsf{con}_T)。$$

注意这里前提里的“相容”以及结论中的“可证”都和通俗表达不同，它们已经被分别形式化到语言 $\mathcal{L}_{ar}$ 中，变成了 con_T 和 bwb_T；而且整个证明还要在 T 内完成：这里要求的是 $\vdash_T$，而在通俗表达中则没有任何限制。

对于初学者来说，最大的困难在于如何区分所谓“外面”和“里面”，即，区分哪些是元数学中的，哪些是“形式化在系统内”的。我们下面会针对这个困难多做些解释。粗略地说，一个断言在“外面”成立是指它在标准模型中成立，而在“里面”则要它在所有的 T 模型中都成立。

这方面的参考书有：G. Boolos 的《The Logic of Provability》前 3 章和 W. Rautenberg 的《A Concise Introduction to Mathematical Logic》。

第 1 节　可证性条件

我们首先引入三个**可证性条件**，它们是由希尔伯特和贝尔纳斯，之后还有勒布从哥德尔的证明中提炼出来的。然后证明 PA 满足这三个可证性条件。最后从可证性条件我们很容易推导出哥德尔第二不完全性定理。

固定一个数论语言上的理论 T，由于我们主要的兴趣是 PA，我们把 PA 视作 T 的典型例子（我们在多数时候甚至可以把 T 就看作是 PA，虽然 PA 的一个片断如 $\mathsf{PA}^- + I\Sigma_1$ 已经足以证明哥德尔第二不完全性定理），特别地，我们总是假定 T 是可以递归公理化的，并且总有 $\mathsf{Q} \subseteq T$。我们先引进一个新的符号 $\Box_{\mathsf{T}}\alpha$。

由于 T 是可以递归公理化的，前面讲过，自然数上的关系 $\mathsf{bew}_T(y,x)$ 是递归的，我们也有 $\mathcal{L}_{ar}$ 中的公式 $\mathsf{bew}_{\mathsf{T}}(y,x)$ 使得 $\mathsf{bew}_{\mathsf{T}}(y,x)$ Q 中表示 $\mathsf{bew}_T(y,x)$。令 $\mathsf{bwb}_{\mathsf{T}}(x)$ 为 $\exists y\mathsf{bew}_{\mathsf{T}}(y,x)$，我们把它简记为 $\Box_{\mathsf{T}}(x)$。对于任意的 $\mathcal{L}_{ar}$ 中的公式 α，我们用 $\Box_{\mathsf{T}}\alpha$ 来记 $\mathsf{bwb}_{\mathsf{T}}(\ulcorner\alpha\urcorner)$。注意，$\Box_{\mathsf{T}}(x)$ 是一个含有唯一自由变元 x 的公式，而 $\Box_{\mathsf{T}}\alpha$ 则总是一个闭语句，就连当 α 中有自由变元时也是这样。

对一个理论 T，T 的三个**可证性条件** 如下：令 σ 和 τ 为 $\mathcal{L}_{ar}$ 中的闭语句。

(D1) 如果 $\vdash_T \sigma$，则 $\vdash_T \Box_{\mathsf{T}}\sigma$。

(D2) $\vdash_T \Box_{\mathsf{T}}(\sigma \to \tau) \to \Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}\tau$。

(D3) $\vdash_T \Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}\Box_{\mathsf{T}}\sigma$。

引理 10.1. 假定 T 满足 (D1) 和 (D2)，则它也满足下面的 (D0)：

(D0) 如果 $\sigma \vdash_T \tau$ 则 $\Box_{\mathsf{T}}\sigma \vdash_T \Box_{\mathsf{T}}\tau$。

Proof. 假设 $\sigma \vdash_T \tau$。根据演绎定理，我们有 $\vdash_T \sigma \to \tau$。由 (D1)，$\vdash_T \Box_{\mathsf{T}}(\sigma \to \tau)$；再由 (D2)，$\vdash_T \Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}\tau$。所以结论成立。 □

推论 10.1. 如果 $\vdash_T \sigma \leftrightarrow \tau$ 则 $\vdash_T \Box_{\mathsf{T}}\sigma \leftrightarrow \Box_{\mathsf{T}}\tau$。

定义 $\mathsf{con}_{\mathsf{T}}$ 为闭语句 $\neg\Box_{\mathsf{T}}(\ulcorner 0 \neq 0\urcorner)$。推论 10.1 告诉我们定义中选择 $0 \neq 0$ 是非本质的，我们可以选取任何的自相矛盾的闭语句来代替它。注意：这并不意味着我们可以随便地定义 $\mathsf{con}_{\mathsf{T}}$，例如我们前面已经指出不能用罗瑟的 prov_T 来代替 $\mathsf{bwb}_{\mathsf{T}}$。

引理 10.2. 可证性条件 (D1) 对任何 Q 的扩张 T 都成立，即，如果 $\vdash_T \sigma$，则 $\vdash_T \Box_{\mathsf{T}}\sigma$。

证明：假定 $\vdash_T \sigma$。令 n 为 σ 的某个证明序列的编码。我们有 $\mathfrak{N} \models \mathsf{bew}_{\mathsf{T}}(\mathsf{n},\ulcorner\sigma\urcorner)$。由 Σ_1-完全性，我们有 $\vdash_{\mathsf{Q}} \mathsf{bew}_{\mathsf{T}}(\mathsf{n},\ulcorner\sigma\urcorner)$，所以 $\vdash_{\mathsf{Q}} \mathsf{bwb}_{\mathsf{T}}(\ulcorner\sigma\urcorner)$。所以，$\vdash_T \Box_{\mathsf{T}}\sigma$。 □

注意：可证性条件 (D1) 对理论 T 的要求不高，T 甚至可以弱到 Q。在本节的剩余部分，我们做一些零星的注释，以期加深我们对 (D1) 和一般的“形式化”概念的理解。

首先 (D1) 并不蕴涵 $\vdash_T \sigma \to \Box_{\mathsf{T}}\sigma$。事实上，后者不一定成立。例如，令 T 为 Q 并且 σ 为 $\forall x(\mathsf{S}x \not\approx x)$。则 $\nvdash_T \sigma \to \Box_{\mathsf{T}}\sigma$，原因是 $\mathfrak{N} \not\models \sigma \to \Box_{\mathsf{T}}\sigma$。

人们常常把 $\Box_{\mathsf{T}}\sigma$ 称为 $\vdash_T \sigma$ *在 T 中的形式化版本*。注意：$\Box_{\mathsf{T}}\sigma$ 本身只是一个语言 $\mathcal{L}_{ar}$ 上的闭语句，即一个字符串；而 $\vdash_T \sigma$ 则是“元数学”或系统“外面”的一个命题，说明 σ 是 T 的一个内定理。

那么 $\vdash_T \sigma$ 和 $\vdash_T \Box_T\sigma$ 到底有哪些区别和联系呢？(D1) 告诉我们前者蕴涵后者，即，如果 σ 是 T 的一个内定理，则 $\Box_{\mathsf{T}}\sigma$ 也是。反过来对不对呢？这需要更细微的考察。

如果 T 是 ω-相容的（例如，$T = \mathsf{Q}$ 或者 PA），则 (D1) 的逆命题也成立。证明我们留作练习。因此，要想把这两者区分开，即论证 (D1) 的逆命题不成立，我们必须利用 ω-不相容的理论。假定 PA 是相容 的，令 $T = \mathsf{PA} + \neg\mathsf{con}_{\mathsf{PA}}$。哥德尔的第二不完全性定理将会告诉我们 T 是相容的但不是 ω-相容的。因为 $\neg\mathsf{con}_{\mathsf{PA}} \in T$，我们有 $T \vdash \Box_{\mathsf{T}}(\ulcorner 0 \not\approx 0 \urcorner)$（这里我们跳过了一步，后面会详细讨论。）但是，$T$ 的相容性告诉我们 $T \nvdash 0 \not\approx 0$。

上面的例子说明，有些“系统内的”或者说“形式化后”的证明不能够移到“系统外面”来。那么系统内的证明到底是什么呢？让我们利用非标准模型来做一些（不太严格的）说明，这对我们理解下一节的内容也帮助。固定一个理论 T （不妨想象它就是 $\mathsf{PA} + \neg\mathsf{con}_{\mathsf{PA}}$，但这一点不重要)。假定 $\mathfrak{M}$ 是 T 的一个非标准模型。对于任何的“形式化后”的概念，$\mathfrak{M}$ 都会有它自己的版本。比如，标准自然数上“偶数”的概念，形式化在 $\mathcal{L}_{ar}$ 中，就是公式 $\exists y(x \approx y + y)$，因此，在 $\mathfrak{M}$ 中所有满足这一公式的元素*在 $\mathfrak{M}$ 中* 都被视为偶数，我们称它们为“$\mathfrak{M}$-偶数”。这些 $\mathfrak{M}$-偶数除了标准的偶数之外，还有非标准的偶数。类似地，$\mathfrak{M}$ 中也有 $\mathfrak{M}$-素数的概念。同样地，自然数上我们有“合式公式的哥德尔数”（简称“公式”）的概念，经形式化后，$\mathfrak{M}$ 中也就有 $\mathfrak{M}$-公式的概念。但这些 $\mathfrak{M}$-公式“从外面看”可能是无穷长的，但从 $\mathfrak{M}$ 内部看，它们的长度是某个（非标准）数，因此是 $\mathfrak{M}$-有穷长的。“公理”的概念也是。甚至 T 也被它自己的递归定义所形式化，$\mathfrak{M}$-中看到的 T 可能包括非标准的公式。“证明”这个概念也一样，外面的“n 是 m 的证明的哥德尔数”形式化为 Δ_1-公式 $\mathsf{bew}_{\mathsf{T}}(y, x)$，$\mathfrak{M}$-中的一个证明（的编码）$y$ 完全有可能是非标准的。因此我们自然不能把这样的 $\mathfrak{M}$-证明与标准的证明同等看待。

第 2 节　第二可证性条件 (D2) 的证明

与 (D1) 不同，(D2) 的证明需要比 Q 更强的理论。先简单分析一下：条件 (D2) 是“如果 $T \vdash \sigma \to \tau$ 并且 $T \vdash \sigma$，则 $T \vdash \tau$”的形式化。未形式化的断言是很容易证明的：假定 $\vec{u}$ 和 $\vec{v}$ 分别是 $\sigma \to \tau$ 和 σ 的证明序列，只需要把它们串在一起再缀上 $\langle\tau\rangle$，便得到了 τ 的一个证明序列 $\vec{u}^\frown\vec{v}^\frown\langle\tau\rangle$。

对 (D2) 的证明思路也是一样，假定 $\Box_{\mathsf{T}}(\sigma \to \tau)$ 且 $\Box_{\mathsf{T}}\sigma$。直观上说，对 $\sigma \to \tau$ 和 σ，我们分别有它们“形式化的证明序列”(的编码) u 和 v。通过“形式化的串接运算”我们得到 $u^\frown v^\frown\langle\ulcorner\tau\urcorner\rangle$，它就是 τ 的一个“形式化的证明序列”。或者，我们也可以向上节末尾那样用非标准模型来解释。令 $\mathfrak{M}$ 为 T 的任何一个模型 (可以是非标准的)。$\mathfrak{M}$ 内部就分别有对 $\sigma \to \tau$ 和 σ 的“$\mathfrak{M}$-证明” u 和 v；因此通过 “$\mathfrak{M}$-串接”运算，可以得到一个新的“$\mathfrak{M}$- 证明” $u^\frown v^\frown\langle\ulcorner\tau\urcorner\rangle$。

所以我们要做的就是把像串接这样的运算形式化在 PA 中 (即用一个 $\mathcal{L}_{ar}$ 中的公式定义它)，或者等价地说，把串接运算推广到每一个 PA 的非标准模型当中；并且还要证明在推广后仍然具有我们所需要的串接函数的性质，即，我们需要用 PA 去证明这些性质。

这样的工作多半都是直接的验证，不难但很繁。唯一需要特别注意的是“有穷序列”这一概念，它的形式化是需要一番努力的。因为有些 $\mathfrak{M}$-有穷的集合从外面看可能像是无穷的。具体的难点我们在形式化中国剩余定理时会仔细谈。

10.2.1　利用定义新的符号来扩张语言

在数论语言 $\mathcal{L}_{ar}$ 中的函数符号只有 S、$+$ 和 $\times$，语言 $\mathcal{L}_{ar}$ 中包含自由变元 x 的项只能是关于 x 的多项式。因此，PA 可以“直接”讨论的函数是很受局限的。然而，通过利用公式，PA 可以定义新的函数和关系，并引进相应的新的函数和谓词符号来扩充语言，从而使我们摆脱语言 $\mathcal{L}_{ar}$ 带来的局限。

在数学中，使用定义的符号是很常见的。例如，在集合论中，我们定义 $x \subseteq y$ 为 $\forall z(z \in x \to z \in y)$，并把 $\subseteq$ 当作我们语言的一部分来使用。从我们在本节开始的讨论中也可以看出，我们在形式化好了“有穷序列”的概念后，会把它当作我们语言中的一部分，用来进一步定义诸如证明序列等概念；尤其是我们会对包含这些新引入符号的公式做归纳。我们用本小节来论证这样做的合理性。

由于所有的结论都很自然，我们略去所有的证明。而且我们只讨论一个特殊的情形，即直接在 PA 中只添加一个新的函数 (或谓词) 符号。最一般的情形是：我们已经作了有穷多次的添加，得到语言 $\mathcal{L}'$ 和理论 $\mathsf{PA}(\mathcal{L}')$，我们在它们的基础上再添加有穷多个函数和谓词符号。

令 $\varphi(\vec{x}, y)$ 为一个语言 $\mathcal{L}_{ar}$ 上的公式且 $\mathsf{PA} \vdash \forall\vec{x}\exists!y\varphi(\vec{x}, y)$，即，

$$\mathsf{PA} \vdash \forall\vec{x}\exists y(\varphi(\vec{x}, y) \wedge \forall z(\varphi(\vec{x}, z) \to y \approx z))。$$

我们把语言 $\mathcal{L}_{ar}$ 扩张成 $\mathcal{L}' = \mathcal{L}_{ar} \cup \{f\}$ 其中 f 是一个新的函数符号，并添入新的公理：$\forall\vec{x}\varphi(\vec{x}, f(\vec{x}))$。直观上看，$f(\vec{x})$ 就是唯一满足 $\varphi(\vec{x}, y)$ 的那个 y。类似地，令 $\varphi(\vec{x})$ 为一个语言 $\mathcal{L}_{ar}$ 上的公式，我们也可以引入一个新的谓词符号 R 和新公理 $\forall\vec{x}(\varphi(\vec{x}) \leftrightarrow R(\vec{x}))$。由于对谓词的处理比对函数处理简单，我们下面只处理函数符号。对每一个 $\mathcal{L}'$ 上的公式 $\theta(\vec{v})$，在语言 $\mathcal{L}_{ar}$ 中都有一个自然的翻译 $\theta^*(\vec{v})$。例如，当 θ 为 $\psi(f(\vec{x}), z)$ 时，θ^* 就

是 $\exists y(\varphi(\vec{x},y)\wedge\psi(y,z))$，此外，由于 PA 证明 y 的唯一性，θ^* 也等价于 $\forall y(\varphi(\vec{x},y)\to\psi(y,z))$。翻译 $\theta\mapsto\theta^*$ 的严格定义可以通过对公式 θ 递归来完成（练习）。

引理 10.3. 给定 φ 如前。令 $\mathfrak{M}$ 为一个语言 $\mathcal{L}'$ 的结构使得 $\mathfrak{M}\models\forall\vec{x}\varphi(\vec{x},f(\vec{x}))$，且 $\mathfrak{M}$ 满足原本语言 $\mathcal{L}_{ar}$ 上的 PA。则对所有的 $\mathcal{L}'$ 上的公式 $\theta(\vec{v})$ 和所有 $\vec{a}\in|\mathfrak{M}|^k$，

$$\mathfrak{M}\models\theta[\vec{a}]\quad\text{当且仅当}\quad\mathfrak{M}\models\theta^*[\vec{a}]。$$

定理 10.1. 给定 $\mathcal{L}'$ 和 $\mathfrak{M}$ 如前。则对所有 $\mathcal{L}'$ 上的公式 θ，$\mathfrak{M}$ 都满足对 θ 的归纳公理 $I\theta$。

推论 10.2. 给定 $\mathcal{L}'$ 如前。对每一个 $\mathcal{L}'$ 上的公式 θ，我们都在 PA 中添入一条新的归纳公理 $I\theta$。令 $\mathsf{PA}(\mathcal{L}')$ 为如此扩充后的公理系统。则 $\mathsf{PA}(\mathcal{L}')$ 是 PA 的一个**保守扩张**，即，对每一个 $\mathcal{L}_{ar}$ 上的闭语句 σ，

$$\mathsf{PA}(\mathcal{L}')\vdash\sigma\quad\text{当且仅当}\quad\mathsf{PA}\vdash\sigma。$$

以上是利用定义引入新的符号的一般讨论。在哥德尔定理的证明中，我们更关心的是 Σ_1 水平以下的定义。特别地，我们把由 Σ_1 公式引入的函数和 Δ_1 公式引入的谓词称为可证递归的。

定义 10.1. 我们称一个函数 f 在 T 中是**可证递归的**，如果存在一个 Σ_1-公式 $\varphi(\vec{x},y)$ 使得

$$T\vdash\forall\vec{x}\forall y\,[\varphi(\vec{x},y)\leftrightarrow y=f(\vec{x})]。$$

我们称一个谓词（或关系）R 在 T 中是**可证递归的**，如果存在 Σ_1- 公式 $\varphi(\vec{x})$ 和 $\psi(\vec{x})$ 使得

$$T\vdash\forall\vec{x}\,[R(\vec{x})\leftrightarrow\varphi(\vec{x})\leftrightarrow\neg\psi(\vec{x})]。$$

换句话说，T 证明 R 是 Δ_1 的。

注意：这里的 f 是一个符号，或者是一个 Σ_1 公式，把它称为“函数”是不太严格的 (因为它没有确定的定义域)。我们可以把它理解成由同一个模式定义出来的一族函数，当落实到每个 PA 的模型 $\mathfrak{M}$ 中的时候，$f^{\mathfrak{M}}$ 都是 $\mathfrak{M}$ 上的“递归（全）函数”。也有教科书把它放在标准模型的语境下来描述。考虑标准模型 $\mathbb{N}$ 上的所有部分递归函数 $\varphi_e(\vec{x})$，它们都是 Σ_1 可定义的。其中 PA 可以证明是全函数的 $\varphi_e(\vec{x})$ 就是可证递归的。例如，所有原始递归函数都是可证递归的。所以，(标准模型上的) 可证递归函数类是递归（全）函数的一个子类。可以进一步证明它是一个真子类（见习题)，后面提到的古德斯坦定理会诱导出一个递归但不可证递归的自然例子。

在引入了新的符号之后，原本复杂的公式很可能表面看上去变得简单了。但对于可证递归函数和谓词，我们可以控制住它们的复杂性。

引理 10.4. 令 $\mathcal{L}'=\mathcal{L}_{ar}\cup\{f,R\}$ 其中 f 和 R 分别是可证递归的函数和谓词。令 $\mathsf{PA}(\mathcal{L}')$ 如前。则任何 $\mathsf{PA}(\mathcal{L}')$ 中的可证递归函数和谓词都是 PA 中可证递归的。

可证递归函数和关系还有一个好处是它们对所有的 PA 模型是“绝对的”，即，

引理 10.5. 令 f 为一个在 PA 中可证递归的函数。令 $\mathfrak{N}$ 和 $\mathfrak{M}$ 为 PA 的两个模型且 $\mathfrak{M}$ 是 $\mathfrak{N}$ 的尾节扩张。则对所有的 $\vec{a}, b \in \mathfrak{N}$，$f^{\mathfrak{N}}(\vec{a}) = b$ 当且仅当 $f^{\mathfrak{M}}(\vec{a}) = b$。类似的结果对可证递归关系也成立。

证明: （梗概）令 φ 为定义 f 的 Σ_1 公式。首先，用类似于 Q 的 Σ_1 完全性的证明，我们可以得到任何 Δ_0 公式对 $\mathfrak{N}$ 和 $\mathfrak{M}$ 是绝对的。

如果 $f^{\mathfrak{N}}(\vec{a}) = b$ 则 $\mathfrak{N} \models \varphi[\vec{a}, b]$。所以，$\mathfrak{M} \models \varphi[\vec{a}, b]$ （这是因为 φ 是 Σ_1 的，在 $\mathfrak{N}$ 中的 Σ_1 事实的证据自然也出现在 $\mathfrak{M}$）。

另一方面，如果 $f^{\mathfrak{N}}(\vec{a}) \neq b$ 则 存在 $b' \in \mathfrak{N}$ 满足 $b' \neq b$ 且 $\mathfrak{N} \models \varphi[\vec{a}, b']$。根据上面的论证，$\mathfrak{M} \models \varphi[\vec{a}, b']$。所以 $f^{\mathfrak{M}}(\vec{a}) \neq b$。 □

10.2.2　PA 的基本推论

我们下面将在 PA 中推导出若干命题，尤其是要叙述和证明中国剩余定理，和将有穷序列的概念形式化。在这一节中，符号 $\vdash$ 代表 PA $\vdash$，“可证递归”代表“在 PA 中可证递归”。

我们不打算从最基本的事实验证起，因为过多的枝叶会遮住我们要讲的主干。因此我们假定已经验证了下面的事实:

- PA 可以证明所有通常用的关于加法和乘法，以及线序 $\leq$ 的定律和性质。
- PA 可以证明强归纳原理和最小数原理。(练习)

引理 10.6. 下列关系和函数是可证递归的:

(a) 整除关系 $d|x$，(其定义为 $\exists q \leq x\ (q \cdot d \approx x)$);

(b) 余数函数 $\mathsf{rem}(x, d) = r$，（其定义为 $[r < d \wedge \exists q(x \approx q \cdot d + r)] \vee (d \approx 0 \wedge r \approx 0)$);

(c) “p 是一个素数” $\mathsf{prime}(p)$，（其定义为 $p \not\approx 1 \wedge \forall d(d|p \to (d \approx 1 \vee d \approx p))$);

(d) 互素关系 $\mathsf{coprime}(a, b)$ （其定义为 $\forall d(d|a \wedge d|b \to d \approx 1)$)。

证明: 同前面递归论中的讨论相似，只需注意所有的量词都可以被替换成某个有界量词。 □

因此，我们就把上面这些我们熟悉的关系和函数“形式化”在 PA 当中了。或者用模型论的语言，对每一个 PA 的模型 $\mathfrak{M}$，$\mathfrak{M}$ 都有类似的关系和函数。例如，在 $\mathfrak{M}$ 中就有 $\mathfrak{M}$- 素数。自然地，我们很容易验证，这些形式化了的关系和函数仍具有我们熟悉的性质。举例如下，为了增加可读性，我们用非形式化的语言叙述，不过把它们放到引号中间。

引理 10.7.　*(a)* $\vdash$ “2 是最小的素数”。

(b) $\vdash$ “如果 $x > 1$，则存在某个素数整除 x”。

引理 10.8. $\vdash \mathsf{coprime}(a, b) \leftrightarrow$ “不存在既整除 a 又整除 b 的素数”。

证明: 利用 $\vdash d|x \to x|y \to d|y$。细节留作练习。 □

引理 10.9 (欧几里得)**.** $\vdash a, b > 0 \wedge \mathsf{coprime}(a, b) \to \exists x \exists y(xa + 1 \approx yb)$。

证明: 我们对 $s = a + b$ 施行强归纳。初始情形 $s = 2$ 我们省略。

假定命题对所有 $< s$ 的数成立。考察满足 $a + b = s > 2$ 的 a, b。由于 $a \neq b$，我们可以不失一般性地假定 $a > b$。不难验证 $\vdash \mathsf{coprime}(a, b) \to \mathsf{coprime}(a - b, b)$（这里 $a - b$ 表示“截断减法”，在 PA 中不难证明它是可证递归的，且满足通常减法的性质)。根据强归纳假定，$\vdash \exists u \exists v[u(a - b) + 1 \approx vb]$。所以，$\vdash \exists u \exists v[ua + 1 = (u + v)b]$，所以，$\vdash \exists x \exists y[xa + 1 \approx yb]$。 □

引理 10.10. $\vdash (\mathsf{prime}(p) \wedge p|ab) \to (p|a \vee p|b)$。

证明: 习题。 □

10.2.3　中国剩余定理的 PA 版本

我们（短期的）的目标是形式化“有穷序列”这一概念。为此我们要在 PA 中证明中国剩余定理，即“对所有的 n，对所有的 d_i 和 a_i，如果……”且慢! 这里的 d_i 和 a_i 指的是什么？难道不正是有穷序列吗？如果没有有穷序列的概念，我们应该怎样叙述中国剩余定理呢？为了解决这个问题，我们只处理由某个可证递归函数 $m(x)$ 所给出的 d_i。(在这里可证递归可以被其它可定义函数 $m'(x)$ 取代，但我们会看到，任何由 $m'(x)$ 给出的 d_i 在编码之后，都可以被某个可证递归函数 $m(x)$ 给出。)

我们首先形式化最小公倍数的概念。读者最好把下文提到的数（如 i, k, l 等等）都想象成非标准的。作为范例，我们对最小公倍数处理得稍微仔细一点。之后的其它概念我们会较快地带过。

引理 10.11. 对任何一个可证递归的函数 $m(i)$，$\mathsf{PA} \vdash \forall k$ “如果对所有的 $i \leq k$ 都有 $m(i) > 0$，则存在（唯一的）最小正整数 l 使得对所有 $i < k$，$m(i)|l$”。

证明: 存在性可以通过对 k 归纳得到。利用最小数原理可以拿到最小的 l，它显然是唯一的。 □

假定 $m(x)$ 是 PA 中的可证递归函数。根据引理 10.11，公式 $\varphi(k,l)$

$$\begin{aligned}&[(\forall i<k\, m(i)>0)\wedge k>0\wedge(\forall i<k\, m(i)|l)\wedge\forall l'<l\neg(l'>0\wedge\forall i<k\, m(i)|l')]\\ \vee\ &(\exists i<k\, m(i)=0\wedge l=0)\end{aligned}$$

定义了一个**最小公倍数函数** $\mathrm{lcm}\{m(i):i<k\}$。[1] 不难看出 $\mathrm{lcm}\{m(i):i<k\}$ 是 PA 中可证递归的。

注意，$\varphi(k,l)$ 间接地依赖于 $m(i)$。引理 10.11 实际上是由无穷多条陈述构成的一个模式。对每一个可证递归函数 $m(x)$ 都有一条相应的陈述。

在最小公倍数函数的定义中，我们仅用到了有界量词而没有用到原始递归。大家可以与有界积函数 $\prod_{i<k} m(i)$ 做比较，有界积函数既不容易在 $\mathcal{L}_{ar}$ 定义也不容易在 PA 中证明它存在。

lcm 函数具有我们所熟悉的最小公倍数的一切性质：

引理 10.12. *(a)* $\mathsf{PA}\vdash j<k\to m(j)|\,\mathrm{lcm}\{m(i):i<k\}$。

(b) $\mathsf{PA}\vdash$ “$\mathrm{lcm}\{m(i):i<k\}$ 整除任何 $m(i)$ $(i<k)$ 的公倍数”。

(c) $\mathsf{PA}\vdash$ “如果 p 是素数且 $p|\,\mathrm{lcm}\{m(i):i<k\}$，则存在某个 $i<k$，$p|m(i)$”。

证明：练习。 □

定理 10.2 (形式化的中国剩余定理)**.** 令 $h(x)$ 和 $m(x)$ 为可证递归函数。则

$$\begin{aligned}\mathsf{PA}\vdash\ &[\forall i<k(m(i)>1\wedge m(i)>h(i))\wedge\forall i,j(i<j<k\to\mathsf{coprime}(m(i),m(j)))]\\ &\to(\exists a<\mathrm{lcm}\{m(i):i<k\})(\forall i<k)[\mathrm{rem}(a,m(i))=h(i)]。\end{aligned}$$

证明：假定方括号中的前提，我们对 $n\le k$ 施行归纳。对初始情形 $n=0$ 时，取 $a=0$ 即可。

考察归纳情形 $n<k$。假定 $a<\mathrm{lcm}\{m(i):i<n\}$ 满足对所有的 $i<n$，$\mathrm{rem}(a,m(i))=h(i)$。令 $l=\mathrm{lcm}\{m(i):i<n\}$ 和 $m=m(n)$。则 l 与 m 互素（练习）。根据欧几里得引理，存在 x 和 y 使得 $lx+1=my$。用 $a+(l-1)h(n)$ 同时乘两边，我们有：存在 u 和 v 使得

$$lu+a+(l-1)h(n)=mv。$$

令 $a^*=l(u+h(n))+a$。则 $a^*=mv+h(n)$。如果 $i<n$，则由于 $m(i)|l$，我们有 $\mathrm{rem}(a^*,m(i))=\mathrm{rem}(a,m(i))=h(i)$。如果 $i=n$，则有 $\mathrm{rem}(a^*,m(n))=\mathrm{rem}(h(n),m(n))=h(n)$。

令 $l'=\mathrm{lcm}\{m(i):i<n+1\}$。如果 $a^*<l'$ 则已经做完了。如果 $a^*>l'$，则令 b 为 $\le a^*$ 的最大的 l' 的倍数，和令 $A=a^*-b$。于是 $A<l'$ 且对所有 $i<n+1$，都有 $\mathrm{rem}(A,m(i))=h(i)$ （练习）。 □

[1] lcm 是英文“最小公倍数”（least common multiple）的简写。

同非形式化的中国剩余定理（定理 9.4）相比，首先我们在叙述中避免了有穷序列 d_i 和 a_i。在证明中我们一直没有离开自然数，即，避免用到任何整数 $\mathbb{Z}$ 的性质，而且是在 PA 中进行的。最后，我们还得到了一个明确的同余方程的解 a 的一个上界 $\text{lcm}\{m(i) : i < k\}$。这对后面的讨论有帮助。

同最小公倍数类似，我们有可证递归的一般极大值函数 $\max\{m(i) : i < k\}$，和二元的极大值函数 $\max(x, y)$。细节我们留给读者。

定义 10.2. 定义 $\alpha(a, b, i)$ 为公式 $\text{rem}(a, 1 + (i + 1)b) \approx r$ 所定义的函数。

引理 10.13. *(a)* 函数 $\alpha(a, b, i)$ 是可证递归的。

(b) 引理 9.9 中定义的二元编码函数 $J(a, b)$ 和解码函数 $K(p), L(p)$ 都是可证递归的。

(c) 哥德尔的 β-函数 $\beta(s, i) = \alpha(K(s), L(s), i)$ 是可证递归的。。

证明: 练习。 □

注意，与 lcm 不同，α 和 β-函数的定义中没有谈论其它的可证递归函数 $m(i)$。

定理 10.3 (哥德尔的 β-函数引理)**.** 令 $h(x)$ 为一个可证递归函数。PA $\vdash$ “对每一个 k，存在 c 使得对所有 $i < k$，$\beta(c, i) = h(i)$；而且，c 有一个可证递归的上界。

证明: 我们只需证明下列关于 $\alpha(a, b, i)$ 的命题：

PA $\vdash$ “对每一个 k，存在 a, b 使得对所有 $i < k$，$\alpha(a, b, i) = h(i)$；而且，令 s 为 $\max(k, \max\{h(i) : i < k\})+1$，则 a, b 可以进一步满足 $b < \text{lcm}\{i+1 : i < s\}+1$ 和 $a < \text{lcm}\{1+(i+1)b : i < k\}$”。

首先注意 $s > k$ 且对每一个 $i < k$，$s > h(i)$。令 $b = \text{lcm}\{i + 1 : i < s\}$。

断言. 如果 $i < j < k$，则 $1 + (i + 1)b$ 和 $1 + (j + 1)b$ 互素。

断言的证明. 假定某个素数 p 满足 $p|1 + (i + 1)b$ 和 $p|1 + (j + 1)b$。则 $p|(j - i)b$。所以 $p|(j - i)$ 或者 $p|b$。由于 $1 \leq j - i < k < s$，我们有 $(j - i)|b$。因此无论如何我们都有 $p|b$。于是 $p|(i + 1)b$，进而有 $p|1$，矛盾。这就证明了断言。

现在，对所有的 $i < k$，$h(i) < s \leq b < 1 + (i + 1)b$。根据形式化的中国剩余定理，并取 $m(i) = 1 + (i + 1)b$，我们就得到 $a < \text{lcm}\{1 + (i + 1)b : i < k\}$ 满足对所有 $i < k$，$\alpha(a, b, i) = h(i)$。

当 $h(x)$ 是可证递归时，证明中得到的 a 和 b 的上界显然都是可证递归的。 □

与前面第 9 章相比，我们在证明中避免了阶乘函数 $s!$（因为它的定义需要原始递归），并且我们还得到一个关于编码 c 的可证递归的上界。

10.2.4　形式化的有穷序列

我们现在可以定义形式化的有穷序列了，即，我们引进一个可证递归的一元谓词符号 $\mathsf{FinSeq}(s)$，表示 s 是一个“有穷序列”。

定义 10.3. 令 $\mathsf{FinSeq}(s)$ 为公式

$$\exists c, k < s[s = J(c,k) \wedge \forall c' < s(c' < c \to (\exists i < k)\ \beta(c',i) \neq \beta(c,i))]。$$

定义 $\mathsf{lh}(s) = L(s)$ 和 $\mathsf{val}(s,i) = \beta(K(s),i)$。

注：

- 我们以标准模型为例，解释一下定义中的末句。对一个固定的 k- 元组 $(n_1, \cdots, n_k)$，会有很多不同的自然数 c 使得对所有的 $i \leq k$，$\beta(c,i) = n_i$，我们只挑其中最小的 c。
- 从定义立刻可以看出，$\mathsf{FinSeq}(s)$ 是一个可证递归关系，且 $\mathsf{lh}(s)$ 和 $\mathsf{val}(s,i)$ 都是可证递归函数。
- 我们继续沿用 $\langle n_1, \cdots, n_k\rangle$ 来表示 $(n_1, \cdots, n_k)$ 的编码，也用 s_i（或 $(s)_i$）来表示 $\mathsf{val}(s,i)$。

PA 保证了 $\mathsf{FinSeq}(s)$ 具有我们所熟悉的有穷序列应有的性质。我们下面以串接函数为例说明这一点。

考察如下定义的公式 $\varphi(s,s',t)$：

$$\begin{aligned} & \mathsf{FinSeq}(t) \wedge (\mathsf{lh}(t) = \mathsf{lh}(s) + \mathsf{lh}(s')) \\ \wedge\ & [(\forall i < \mathsf{lh}(s))\ t_i = s_i] \wedge [(\forall i < \mathsf{lh}(s'))t_{\mathsf{lh}(s)+i} = s'_i]。 \end{aligned}$$

引理 10.14.

$$\vdash \forall s \forall s' \exists! t \varphi(s,s',t)。$$

因此，$\varphi(s,s',t)$ 定义了一个可证递归函数 $s^\frown s'$，称为 s 和 ‘s' 的串接。

令 $\langle\,\rangle$ 表示空序列，即，$\langle\,\rangle = J(0,0)$。

引理 10.15. *(1)* $\mathsf{PA} \vdash \mathsf{FinSeq}(s) \to \langle\,\rangle^\frown s = s = s^\frown\langle\,\rangle$。

(2) $\mathsf{PA} \vdash$ “如果 s, s' 和 s'' 都是有穷序列，则 $s^\frown(s'^\frown s'') = (s^\frown s')^\frown s''$”。

形式化了有穷序列的概念之后，我们可以用前面一样的方法来论证递归定义的合理性。例如，我们有：指数函数在 PA 中是可证递归的。事实上，如果函数 g 和 h 都是可证递归的，则从 g 和 h 上利用原始递归得到的函数 f 也是可证递归的。特别地，所有原始递归函数都是可证递归的。更进一步地，阿克曼函数也是可证递归的。

10.2.5　形式化版本的句法形式化

有了这些准备工作之后，我们就可以仿照标准模型上的句法算术化，把逻辑中的概念在 PA 中形式化。整个过程非常象从递归函数到可证递归函数的过程。我们因此略去所有的证明。

首先我们把 $\mathcal{L}_{ar}$ 中的符号，形式化为数码（比过去编码成标准自然数再进一步）。例如，符号 $\forall$ 和 $+$ 现在就分别形式化为 1 和 7，即，$\mathsf{S0}$ 和 $\mathsf{SSSSSSS0}$，而不再是自然数 1 和 7。我们循环利用 $\ulcorner\urcorner$ 的记号，把对象 O 所对应的数码记成 $\ulcorner O\urcorner$；例如，$\ulcorner\forall\urcorner = \mathsf{S0}$。

同前一章一样，我们最终会得到一个表示“可证性”的 $\mathcal{L}_{ar}$ 公式 $\mathsf{bwb}(x)$。它是我们原来的 $\mathsf{bwb}(x)$ 的形式化。从模型的角度来看，在每一个 PA 的模型 $\mathfrak{M}$ 中，$\mathfrak{M} \models \mathsf{bwb}[a]$ 表示 $\mathfrak{M}$-公式 a 在 $\mathfrak{M}$ 中是可证的；这里元素 a 可以是非标准的，它在 $\mathfrak{M}$ 的证明自然也可能是非标准的。

我们下面选择性地给出几个在 PA 中形式化的例子。

我们可以用 Δ_1-公式 $(\exists i < v)(v = 2 \cdot i + 21)$ 定义一个新的一元谓词 $\mathsf{variable}(v)$，它就是“变元”概念的形式化。“$\forall$ 不是一个变元”这个事实“形式化”后仍旧成立，因为 $\mathsf{PA} \vdash \neg\mathsf{variable}(\ulcorner\forall\urcorner)$。所以，在任何 PA 的模型中，“$\forall$ 不是一个变元”都（在这个意义下）成立。根据定义，$\mathsf{variable}(v)$ 是可证递归的。

类似地，我们也有一个可证递归的一元谓词 $\mathsf{term}(t)$ 来形式化“项”这个概念。它是可证递归的，因为它是利用可证递归的函数经强递归定义的，而不难验证，可证递归对强递归也是封闭的。一般的逻辑教科书上通常会避开递归论的讨论，而给出一个更直接 (但更繁琐) 的论证。我们大概叙述一下通常的论证，这也是出于对历史的兴趣，因为哥德尔文章中用的就类似的方法。

定义 10.4. $\mathsf{term}(t)$ 是由下列公式定义的：

$$\begin{aligned} & \exists s[\mathsf{FinSeq}(s) \wedge \mathsf{lh}(s) > 0 \wedge s_{\mathsf{lh}(s)-1} = t \\ \wedge\ & \forall i < \mathsf{lh}(s)(s_i = \langle\ulcorner\mathsf{0}\urcorner\rangle \vee \exists v < s_i[\mathsf{variable}(v) \wedge s_i = \langle v\rangle] \\ \vee\ & \exists j, k < i(s_i = \langle\ulcorner\mathsf{S}\urcorner\rangle\hat{}s_j \vee s_i = \langle\ulcorner+\urcorner\rangle\hat{}s_j\hat{}s_k \vee s_i = \langle\ulcorner\times\urcorner\rangle\hat{}s_j\hat{}s_k))]。\end{aligned}$$

方括号中的公式是 Δ_1 的，因此 $\mathsf{term}(t)$ 显然是 Σ_1 的。另一方面，每一个项 t 都有一个长度不超过 $t+1$ 的生成序列，我们还可以进一步假定这个生成序列的每一项都是 t 的子项，因此，定义中的 s 不会大于编码 $\langle t, t, \cdots, t\rangle$（长度为 $t+1$）。根据 β-函数引理，s 有一个可证递归的上界。所以，$\mathsf{term}(t)$ 是 Δ_1 的，即可证递归的。

接下来，我们有：

- 可证递归的谓词 $\mathsf{formula}(x)$ 来形式化“公式”的概念。
- 可证递归的函数 $\tilde{\neg}(x)$ 和 $\tilde{\to}(x, y)$ 来形式化“否定”和“蕴涵”；它们的定义分别是 $\tilde{\neg}(x) := \langle\ulcorner(\urcorner\hat{}\langle\ulcorner\neg\urcorner\rangle\hat{}x\hat{}\langle\ulcorner)\urcorner\rangle$ 和 $\tilde{\to}(x, y) := \langle\ulcorner(\urcorner\hat{}x\hat{}\langle\ulcorner\to\urcorner\rangle\hat{}y\hat{}\langle\ulcorner)\urcorner\rangle$。

- 可证递归的谓词 $\mathsf{Axiom}_{\mathsf{T}}$ 来形式化“一阶逻辑的公理”，或者更广泛地，形式化任何一个可证递归的公理集 T。

- 可证递归的谓词

$$\mathsf{ModusPonens}(x,y,z) := \mathsf{formula}(x) \wedge \mathsf{formula}(z) \wedge y = \dot{\rightarrow}(x,z)$$

  来形式化分离规则。

最后，我们有可证递归的关系 $\mathsf{bew}_T(y,x)$ 来形式化“y 是 T 中对 x 的一个证明序列”，它是由下列 Δ_1-公式定义的：

$\mathsf{FinSeq}(y) \wedge s_{\mathsf{lh}(y)-1} = x \wedge (\forall i < \mathsf{lh}(y)-1)[\mathsf{Axiom}_{\mathsf{T}}(y_i) \vee (\exists j,k<i)\mathsf{ModusPonens}(y_k,y_j,y_i)]$。

我们还有公式 $\mathsf{bwb}_T(x)$ 来形式化“可证性”，它的定义是 $\exists y\, \mathsf{bew}_T(y,x)$。它显然是 Σ_1 的。我们将会看到它一般上不是 Δ_1 的，例如，$\mathsf{bwb}_{\mathsf{PA}}(x)$ 就不是 Δ_1 的，除非 PA 是不相容的。

10.2.6　(D2) 的证明

回忆一下 (D2) 说的是对所有的 $\mathcal{L}_{ar}$ 中的闭语句 σ 和 τ，都有

$$\vdash_T \Box_{\mathsf{T}}(\sigma \to \tau) \to \Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}\tau。$$

证明: 我们只需证明

$$\mathsf{PA} \vdash \mathsf{bew}_T(u, \ulcorner \sigma \to \tau \urcorner) \to \mathsf{bew}_T(v, \ulcorner \sigma \urcorner) \to \mathsf{bew}_T(u \hat{}\, v \hat{}\, \langle \ulcorner \tau \urcorner \rangle, \ulcorner \tau \urcorner)。$$

假定 u 和 v 分别满足 $\mathsf{bew}_T(u, \ulcorner \sigma \to \tau \urcorner)$ 和 $\mathsf{bew}_T(v, \ulcorner \sigma \urcorner)$。令 $y = u \hat{}\, v \hat{}\, \langle \ulcorner \tau \urcorner \rangle$。我们验证（具体过程省略了）：

- $\mathsf{FinSeq}(y)$;

- $s_{\mathsf{lh}(y)-1} = \ulcorner \tau \urcorner$;

- $\forall i < \mathsf{lh}(y)[\mathsf{Axiom}(y_i) \vee (\exists j,k<i)\mathsf{ModusPonens}(y_k,y_j,y_i)]$。

根据定义，我们有 $\mathsf{bew}_T(y, \ulcorner \tau \urcorner)$。　□

第 3 节　第三可证性条件 (D3) 的证明

我们还剩下最后一个可证性条件 (D3) 有待证明，即我们要证：$\vdash_T \Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}\Box_{\mathsf{T}}\sigma$。我们可以称之为“如果 $T \vdash \sigma$ 则 $T \vdash \mathsf{bwb}_T(\ulcorner\sigma\urcorner)$”的形式化版本，但这样做对我们没有什么帮助。我们要换一个思路。

注意到 $\Box_{\mathsf{T}}\sigma$ 是一个 Σ_1 的闭语句。因此我们只需证明对所有的 Σ_1 闭语句 τ 我们有 $\vdash_T \tau \to \Box_{\mathsf{T}}\tau$，它是某种形式化的 Σ_1-完全性。我们希望对 Σ_1 语句 τ 的句法结构施行归纳，这就需要处理带自由变元的公式 $\varphi(\vec{x})$。可是，$\Box_{\mathsf{T}}\varphi(\vec{x})$ 总是一个闭语句，象 $\vdash_T \varphi(\vec{x}) \to \Box_{\mathsf{T}}\varphi(\vec{x})$ 这样的硬套归纳模式是不行的，事实上，它不是普遍成立的 (即，有反例)。所以，我们需要引入一个新的符号 $\Box_{\mathsf{T}}[\varphi]$，它的作用是把锁在 $\ulcorner\varphi(\vec{x})\urcorner$ 中的自由变元解放出来。我们证明所谓的“可证 Σ_1-完全性引理”：对所有的 Σ_1 公式 φ，$\vdash \varphi \to \Box_{\mathsf{T}}[\varphi]$；进而导出 (D3)。

10.3.1　一个新符号 $\Box_{\mathsf{T}}[\varphi]$

我们首先把数码这个概念形式化。在标准模型 $\mathfrak{N}$ 上我们有递归函数 $n \mapsto \sharp\mathsf{S}^n0$ (见第 9 章第 2 节，第 (6) 款)，它把 n 映到数码 n 的哥德尔数。把它用 $\mathcal{L}_{ar}$ 中的公式写出来，我们有

$$\varphi(x,y) := \exists s[\mathsf{lh}(s) \approx x+1 \wedge s_0 \approx \ulcorner 0\urcorner \wedge (\forall i < x)s_{i+1} \approx \langle\ulcorner \mathsf{S}\urcorner\rangle^\frown s_i \wedge s_x \approx y]。$$

引理 10.16.

$$\mathsf{PA} \vdash \forall x\exists! y\varphi(y),$$

所以由公式 $\varphi(x,y)$ 定义的函数 $\mathsf{num}(x)$ 是可证递归的。

用通常的递归方程来写，它就是 $\mathsf{num}(0) = \ulcorner 0\urcorner$ 和 $\mathsf{num}(\mathsf{S}x) = \langle\ulcorner \mathsf{S}\urcorner\rangle^\frown\mathsf{num}(x)$。

我们还需要把函数 $n \mapsto \ulcorner v_n\urcorner$ (即第 n 个变元的哥德尔数) 形式化。只需选公式 $y \approx 2\cdot x + 21$ 就可以了。

引理 10.17. 由公式 $y \approx 2\cdot x + 21$ 定义的函数 $\mathsf{var}(x)$ 是可证递归的。

我们还需要把函数 $(n, v, \sharp\alpha) \mapsto \sharp\,\alpha^v_n$ 形式化 (细节省略)；我们用 $\mathsf{sub}(n,v,z)$ 来表示形式化后的函数，它是可证递归的。

这些都是为了引入下面这个函数：

引理 10.18. 函数 $\mathsf{su}(x,y,z) := \mathsf{sub}(\mathsf{num}(x), \mathsf{var}(y), z)$ 是可证递归的。

函数 $\mathsf{su}(x,y,z)$ 的计算方法是：首先将 z 解码成一个公式 (比如是 α)，再在 α 中找到标号为 y 的变元 (例如，当 $y = 4$ 时，我们要找的就是 v_4)，然后把这个变元替换成

标号为 x 的数码（比如，当 $x = 3$ 时，就是 SSS0），最后再计算所得到的公式对应的数码。例如，$\vdash \mathsf{su}(3, 4, \ulcorner v_4 \approx v_1 \urcorner) \approx \ulcorner 3 \approx v_1 \urcorner$。注意 $\mathsf{su}(3, 4, \ulcorner v_4 \approx v_1 \urcorner)$ 是一个闭项，即它没有自由变元。尽管 v_4 和 v_1 看上去像是自由变元，但它们经过 $\ulcorner\urcorner$ 之后，都分别变成了固定的数码 29 和 23。而 $\ulcorner v_4 \approx v_1 \urcorner$ 就是项 $\langle \ulcorner \approx \urcorner, \ulcorner v_4 \urcorner, \ulcorner v_1 \urcorner \rangle = \langle 19, 29, 23 \rangle$，它是某个自然数 $n_0 \in \mathbb{N}$ 的数码 n_0。

我们再比较一下 $\mathsf{su}(v_4, 4, \ulcorner v_4 \approx v_1 \urcorner)$ 并注意其中两个 v_4 的不同。不难看出，

$$\vdash \mathsf{su}(v_4, 4, \ulcorner v_4 \approx v_1 \urcorner) \approx \langle 19, \mathsf{num}(v_4), 23 \rangle。$$

第一个 v_4 仍然是自由的，它起的作用可以说是把第二个 v_4 激活。（当然直接用 v_4，而不用 $\mathsf{num}(v_4)$ 也能有激活的作用，但我们后面证明中需要用到 $\mathsf{num}(v_4)$。）在 $\mathsf{su}(v_4, 4, \ulcorner v_4 \approx v_1 \urcorner)$ 中，当 v_4 赋值成某个（可以是非标准的）a 时，则 $\mathsf{su}(v_4, 4, \ulcorner v_4 \approx v_1 \urcorner)$ 就是 $\ulcorner \mathsf{num}(a) \approx v_1 \urcorner$；如果赋值成 b，$\mathsf{su}(v_4, 4, \ulcorner v_4 \approx v_1 \urcorner)$ 就是 $\ulcorner \mathsf{num}(b) \approx v_1 \urcorner$ 等等。

现在我们可以引入 $\Box_{\mathsf{T}}[\varphi]$ 了：

定义 10.5. 令 φ 为 $\mathcal{L}_{ar}$ 上的一个公式，且 φ 中的自由变元恰好是 $v_{k_1}, \cdots, v_{k_m}$ 其中 $k_1 < \cdots < k_m$。定义 $\Box_{\mathsf{T}}[\varphi]$ 为

$$\Box_{\mathsf{T}}(\mathsf{su}(v_{k_m}, \mathsf{k}_m, \cdots, \mathsf{su}(v_{k_2}, \mathsf{k}_2, \mathsf{su}(v_{k_1}, \mathsf{k}_1, \ulcorner \varphi \urcorner)) \dots))。$$

让我们对 $\Box_{\mathsf{T}}[\varphi]$ 做一些解释并与 $\Box_{\mathsf{T}}\varphi$ 做一些比较。

- 首先注意 $\Box_{\mathsf{T}}[\varphi]$ 和 φ 具有相同的自由变元，即，$v_{k_1}, \cdots, v_{k_m}$；而 $\Box_{\mathsf{T}}\varphi$ 则永远是一个闭语句。例如，$\Box_{\mathsf{T}}[v_4 \approx v_1]$ 就是

  $$\Box_{\mathsf{T}}(\mathsf{su}(v_4, 4, \mathsf{su}(v_1, 1, \ulcorner v_4 \approx v_1 \urcorner))),$$

  它是 $\Box_{\mathsf{T}}(w)$ 和 $\mathsf{su}(v_4 \dots)$ 的复合，即，

  $$\exists w[w \approx \mathsf{su}(v_4, 4, \mathsf{su}(v_1, 1, \ulcorner v_4 \approx v_1 \urcorner)) \wedge \Box_{\mathsf{T}}(w)]。$$

  显然，变元 v_4 和 v_1 仍旧是自由的。而 $\Box_{\mathsf{T}}\, v_4 \approx v_1$ 则不同，它是 $\Box_{\mathsf{T}}(\ulcorner v_4 \approx v_1 \urcorner)$，不含任何自由变元。

- $\vdash_T \Box_{\mathsf{T}}[\varphi]$ 的直观解释如下：根据概括定理，它等价于 $\vdash_T \forall \vec{x} \Box_{\mathsf{T}}[\varphi]$。注意，量词 $\forall \vec{x}$ 出现在 $\Box_{\mathsf{T}}[\varphi]$ 之前，所以它说明我们有一族逐点的 φ 证明。用模型论的观点来看，给定任意一个 T 的（非标准）模型 $\mathfrak{M}$，$\mathfrak{M} \models \forall \vec{x} \Box_{\mathsf{T}}[\varphi]$ 说的是：“对所有 $\mathfrak{M}$ 中的数组 $\vec{a}$，都有一个 $\varphi(\vec{\mathsf{a}})$ 的 $\mathfrak{M}$-证明”（这个证明可以依赖于 $\vec{a}$，这一点同引理 9.1 (b) 很像）。所以，$\mathcal{L}_{ar}$ 的单一的公式 $\Box_{\mathsf{T}}[\varphi]$ 形式化了整个模式“对所有的 $\vec{n} \in \mathbb{N}^m$，$\vdash_T \varphi(\vec{\mathsf{n}})$”。

  与之相比，$\vdash_T \Box_{\mathsf{T}}\varphi$ 则更强。$\vdash_T \Box_{\mathsf{T}}\varphi$ 说的是“存在一个 $\varphi(\vec{x})$ 的相容证明”。因此，对不同的 $\vec{a}$，$\varphi(\vec{a})$ 的证明都是一个套路的，只不过是把 $\varphi(\vec{x})$ 的相容证明中的参数选为 $\vec{a}$ 即可。

- 当 φ 是一个闭语句时，$\Box_{\mathsf{T}}\varphi$ 就是 $\Box_{\mathsf{T}}[\varphi]$。
- 为了增强可读性，我们经常会将 v_{k_j} 换成更常见的字母，如 x 或 y 之类的。我们还会省掉 k_j，因为通常情况下我们会知道我们要“激活”哪一个变元。我们还假定函数 su 的自变量个数是有“弹性”的。例如，如果 φ 是一个只含有自由变元 v_4 和 v_1 的公式，我们会用 $\mathsf{su}(y, x, \ulcorner\varphi\urcorner)$ 而不用 $\mathsf{su}(v_4, 4, \mathsf{su}(v_1, 1, \ulcorner\varphi\urcorner))$。

10.3.2　形式化的可证性条件 (D1) 和 (D2)

从此直到本节末尾，$\vdash$ 表示 $\vdash_T$。

引理 10.19. 对任何 $\mathcal{L}_{ar}$ 上的公式 φ 和 ψ，我们有：

$$\vdash \Box_{\mathsf{T}}[\varphi \to \psi] \to \Box_{\mathsf{T}}[\varphi] \to \Box_{\mathsf{T}}[\psi]。$$

从模型的直观上看是非常自然的：如果我们有一族 $(\varphi \to \psi)(\vec{\mathsf{a}})$ 的逐点的 $\mathfrak{M}$-证明和一族 $\varphi(\vec{\mathsf{a}})$ 的逐点的 $\mathfrak{M}$-证明，则有一族 $\psi(\vec{\mathsf{a}})$ 的逐点的 $\mathfrak{M}$-证明。

证明：为了避免符号带来的不必要的干扰，我们证明一个特例。这个特例足以说明一般情形的证明思路。假定在 $\varphi(y, z)$ 中只有自由变元 y 和 z；在 $\psi(x, z)$ 中只有 x 和 z。

于是 $\Box_{\mathsf{T}}[\varphi]$ 就是 $\exists t\, \mathsf{bew}_T(t, \mathsf{su}(z, y, \ulcorner\varphi\urcorner))$、$\Box_{\mathsf{T}}[\psi]$ 就是 $\exists r\, \mathsf{bew}_T(r, \mathsf{su}(z, x, \ulcorner\psi\urcorner))$、而 $\Box_{\mathsf{T}}[\varphi \to \psi]$ 就是 $\exists s\, \mathsf{bew}_T(s, \mathsf{su}(z, y, x, \ulcorner\varphi \to \psi\urcorner))$。

注意

$$\vdash \mathsf{su}(z, y, x, \ulcorner\varphi \to \psi\urcorner) \approx \langle \ulcorner\to\urcorner, \mathsf{su}(z, y, \ulcorner\varphi\urcorner), \mathsf{su}(z, x, \ulcorner\psi\urcorner)\rangle,$$

直观上看就是数码的替换可以落实到子公式上。同 (D2) 的证明类似，我们有

$$\begin{aligned} \vdash \quad & \mathsf{bew}_T(s, \mathsf{su}(z, y, x, \ulcorner\varphi \to \psi\urcorner)) \to \mathsf{bew}_T(t, \mathsf{su}(z, y, \ulcorner\varphi\urcorner)) \\ \to \quad & \mathsf{bew}_T(s\hat{}t\hat{}\langle \mathsf{su}(z, x, \ulcorner\psi\urcorner)\rangle, \mathsf{su}(z, x, \ulcorner\psi\urcorner))。 \end{aligned}$$

取 r 为 $s\hat{}t\hat{}\langle \mathsf{su}(z, x, \ulcorner\psi\urcorner)\rangle$，$r$ 就是 $\Box_{\mathsf{T}}[\psi]$ 的证据。 □

引理 10.20. 对任何 $\mathcal{L}_{ar}$ 上的公式 φ，如果 $\vdash \varphi$ 则 $\vdash \Box_{\mathsf{T}}[\varphi]$。

从模型的直观上看这也非常自然：如果我们有一个相容的 $\varphi(\vec{x})$ 的证明，则有一族 $\varphi(\vec{\mathsf{a}})$ 的逐点的 $\mathfrak{M}$-证明。

证明：我们仍然用一个特例来解释证明的想法。假定在 $\varphi(x, y)$ 中只有自由变元 x 和 y。于是 $\Box_{\mathsf{T}}[\varphi]$ 就是 $\Box_{\mathsf{T}}(\mathsf{su}(y, x, \ulcorner\varphi\urcorner))$。

令 σ 为闭语句 $\forall x \forall y \varphi$。根据概括规则和 $\vdash \varphi$，我们有 $\vdash \sigma$。

根据一阶逻辑的替换公理，我们有 $\vdash \sigma \to \varphi(x,y)^{x,y}_{\mathsf{num}(x),\mathsf{num}(y)}$。让我们用 φ^* 来简记 $\varphi(x,y)^{x,y}_{\mathsf{num}(x),\mathsf{num}(y)}$。根据 (D1)，我们有

$$\vdash \exists p\, \mathsf{bew}_T(p, \langle \ulcorner \to \urcorner, \ulcorner \sigma \urcorner, \mathsf{su}(y, x, \ulcorner \varphi^* \urcorner)\rangle)。$$

因为 $\vdash \sigma$，仍根据 (D1)，我们有 $\vdash \Box_{\mathsf{T}}\sigma$，于是

$$\vdash \exists q\, \mathsf{bew}_T(q, \ulcorner \sigma \urcorner)。$$

接下来，仍与 (D2) 的证明类似，我们有

$$\begin{aligned} \vdash \quad & \mathsf{bew}_T(p, \langle \ulcorner \to \urcorner, \ulcorner \sigma \urcorner, \mathsf{su}(y, x, \ulcorner \varphi^* \urcorner)\rangle) \to \mathsf{bew}_T(q, \ulcorner \sigma \urcorner) \\ \to \quad & \mathsf{bew}_T(p \hat{}\, q \hat{}\, \langle \mathsf{su}(y, x, \ulcorner \varphi^* \urcorner)\rangle, \mathsf{su}(y, x, \ulcorner \varphi^* \urcorner))。 \end{aligned}$$

所以 $\vdash \Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}[\varphi]$。于是引理得证。　□

10.3.3　关键引理

要证明 (D3)，最后一个障碍是下面的引理：

引理 10.21 (可证 Σ_1 完全性)**.** 对任何 Σ_1 公式 φ，$\vdash \varphi \to \Box_{\mathsf{T}}[\varphi]$。

从可证 Σ_1 完全性引理我们可以立刻得到 (D3)：由于 $\Box_{\mathsf{T}}\sigma$ 是 Σ_1 的，我们有 $\vdash \Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}[\Box_{\mathsf{T}}\sigma]$。而由于 $\Box_{\mathsf{T}}\sigma$ 是一个闭语句，$\Box_{\mathsf{T}}[\Box_{\mathsf{T}}\sigma] = \Box_{\mathsf{T}}\Box_{\mathsf{T}}\sigma$。于是便得到 (D3)。

由于我们经常要处理替换的情形，我们先证明一个引理作为工具。

引理 10.22. 令 $\varphi(v_1)$ 为一个含有自由变元 v_1 的公式（φ 中可以有其它的自由变元，但为简单起见，我们不将它们都写出来），且 v_k 为某个可以在 φ 中替换 v_1 的变元，则

(1) $\vdash \Box_{\mathsf{T}}[\varphi^{v_1}_0] \leftrightarrow (\Box_{\mathsf{T}}[\varphi])^{v_1}_0$。

(2) $\vdash \Box_{\mathsf{T}}[\varphi^{v_1}_{v_k}] \leftrightarrow (\Box_{\mathsf{T}}[\varphi])^{v_1}_{v_k}$。

(3) $\vdash \Box_{\mathsf{T}}[\varphi^{v_1}_{\mathsf{S}v_k}] \leftrightarrow (\Box_{\mathsf{T}}[\varphi])^{v_1}_{\mathsf{S}v_k}$。

证明*:* 在 (1) 中，左边是 $\Box_{\mathsf{T}}(\ulcorner \varphi(0) \urcorner)$；右边是 $\Box_{\mathsf{T}}(\mathsf{su}(0, 1, \ulcorner \varphi \urcorner))$，这里让我们用回标准的 su 的写法。由于

$$\mathsf{su}(0, 1, \ulcorner \varphi \urcorner) = \mathsf{sub}(\mathsf{num}(0), \mathsf{var}(1), \ulcorner \varphi \urcorner) = \ulcorner \varphi(0) \urcorner,$$

所以 (1) 成立。

由于 (2) 和 (3) 类似，且 (2) 比 (3) 更简单，让我们只证明 (3)。在 (3) 中，左边是 $\Box_{\mathsf{T}}(\mathsf{su}(v_k, \mathsf{k}, \ulcorner \varphi^{v_1}_{\mathsf{S}v_k} \urcorner))$；右边是 $\Box_{\mathsf{T}}(\mathsf{su}(\mathsf{S}v_k, 1, \ulcorner \varphi \urcorner))$。由于

$$\begin{aligned}
& \mathsf{su}(v_k, \mathsf{k}, \ulcorner \varphi^{v_1}_{\mathsf{S}v_k} \urcorner) \\
= \ & \mathsf{sub}(\mathsf{num}(v_k), \mathsf{var}(\mathsf{k}), \ulcorner \varphi^{v_1}_{\mathsf{S}v_k} \urcorner) \\
= \ & \ulcorner \varphi^{v_1}_{\mathsf{S}\mathsf{num}(v_k)} \urcorner \\
= \ & \ulcorner \varphi^{v_1}_{\mathsf{num}(\mathsf{S}v_k)} \urcorner \\
= \ & \mathsf{sub}(\mathsf{num}(\mathsf{S}v_k), \mathsf{var}(1), \ulcorner \varphi \urcorner) \\
= \ & \mathsf{su}(\mathsf{S}v_k, 1, \ulcorner \varphi \urcorner),
\end{aligned}$$

所以 (3) 成立。 □

本节剩余的部分全部用来证明引理 10.21。我们对 Σ_1-公式施行归纳，并把整个证明分解成若干个小的断言。

令严格的 Σ_1-公式类 为包含所有原子公式，且对 $\wedge$、$\vee$、存在量词 $\exists$、和有界的全称量词 $(\forall x < y)$-封闭的最小公式类。

断言 0. 我们只需证明引理对严格的 Σ_1- 公式类成立即可。

断言 0 的证明. 首先注意 PA 可以证明 $<$ 是一个线序。所以我们可以忽略到原子公式的否定式，例如，我们可以把 $x \not\approx y$ 用 $x < y \vee y < x$ 来取代，然后把 $x < y$ 用 $\exists z(x + \mathsf{S}z \approx y)$ 取代等等。所以，任何一个 Σ_1-公式 φ 都与某个严格的 Σ_1- 公式 ψ 可证等价，即，$\vdash_T \varphi \leftrightarrow \psi$。根据假设，我们已经有了 $\vdash_T \psi \to \Box_{\mathsf{T}}[\psi]$。

因为 $\vdash_T \psi \to \varphi$，根据形式化的 (D1) 我们有 $\vdash_T \Box_{\mathsf{T}}[\psi \to \varphi]$；所以，根据形式化的 (D2) 我们有 $\vdash_T \Box_{\mathsf{T}}[\psi] \to \Box_{\mathsf{T}}[\varphi]$。于是“$\varphi \vdash_T \psi \vdash_T \Box_{\mathsf{T}}[\psi] \vdash_T \Box_{\mathsf{T}}[\varphi]$”，这就证明了断言 0。[这一小段实际上是在证明形式化的 (D0)。]

我们验证初始情形，即原子公式的情形。我们可以进一步假定原子公式的形式为 $u \approx 0$、$u \approx v$、$\mathsf{S}u \approx v$、$u + v \approx w$ 和 $u \times v \approx w$，其中 u, v 和 w 都是变元。这是因为复合式，如 $t_1 + t_2 \approx t_3$ 可以被写成 $\exists u, v, w\,(t_1 \approx u \wedge t_2 \approx v \wedge t_3 \approx w \wedge u + v \approx w)$，这样逐层分解下去，我们只需处理变元的情形。

断言 1. $\vdash u \approx 0 \to \Box_{\mathsf{T}}[u \approx 0]$。

断言 1 的证明. 我们对 u 施行归纳。

当 u 是 0 的时候，我们需要证明

$$\vdash 0 \approx 0 \to \Box_{\mathsf{T}}[\mathsf{su}(0, \ulcorner u \approx 0 \urcorner)]。$$

我们只需证明 $\vdash \Box_{\mathsf{T}}[\mathsf{su}(0, \ulcorner u \approx 0 \urcorner)]$，也就是 $\vdash \Box_{\mathsf{T}}(\ulcorner 0 \approx 0 \urcorner)$。显然 $\vdash 0 \approx 0$。根据 (D1)，我们就有 $\vdash \Box_{\mathsf{T}}(\ulcorner 0 \approx 0 \urcorner)$。

对 u 的归纳情形自然成立，因为 $\vdash \mathsf{S}y \not\approx 0$；我们甚至不需要归纳假设。断言 1 证毕。

断言 2. $\vdash u \approx v \to \Box_{\mathsf{T}}[u \approx v]$。

断言 2 的证明. 我们对 v 施行归纳。

当 v 是 0 的时候，我们需要证明

$$\vdash u \approx 0 \to \Box_{\mathsf{T}}(\mathsf{su}(u, 0, \ulcorner u \approx v \urcorner))。$$

由于 $\mathsf{su}(u, 0, \ulcorner u \approx v \urcorner)$ 就是 $\mathsf{su}(u, \ulcorner u \approx 0 \urcorner)$，这可以从断言 1 得出。

假设命题对 $v = y$ 成立，即，

$$\vdash \forall u(u \approx y \to \Box_{\mathsf{T}}(\mathsf{su}(u, y, \ulcorner u \approx v \urcorner)))。$$

我们需要验证

$$\vdash \forall u(u \approx \mathsf{S}y \to \Box_{\mathsf{T}}(\mathsf{su}(u, \mathsf{S}y, \ulcorner u \approx v \urcorner)))。$$

我们再对 u 施行归纳。对 $u = 0$ 命题成立，因为前件为假。考察 $u = \mathsf{S}z$ 的归纳情形，我们证明

$$\vdash \mathsf{S}z \approx \mathsf{S}y \to \Box_{\mathsf{T}}(\mathsf{su}(\mathsf{S}z, \mathsf{S}y, \ulcorner u \approx v \urcorner))。$$

从 $\mathsf{S}z \approx \mathsf{S}y$ 我们得到 $z \approx y$。根据归纳假定，我们有 $\Box_{\mathsf{T}}(\mathsf{su}(z, y, \ulcorner u \approx v \urcorner))$，也就是 $(\Box_{\mathsf{T}}[u \approx v])^{u,v}_{z,y}$。根据引理 10.22，它与 $\Box_{\mathsf{T}}[z \approx y]$ 等价。

现在 $\vdash z \approx y \to \mathsf{S}z \approx \mathsf{S}y$。根据形式化的 (D1) 和 (D2)，$\vdash \Box_{\mathsf{T}}[z \approx y] \to \Box_{\mathsf{T}}[\mathsf{S}z \approx \mathsf{S}y]$。而 $\Box_{\mathsf{T}}[\mathsf{S}z \approx \mathsf{S}y]$ 就是 $\Box_{\mathsf{T}}[(u \approx v)^{u,v}_{\mathsf{S}z,\mathsf{S}y}]$。根据引理 10.22，它等价于 $(\Box_{\mathsf{T}}[u \approx v])^{u,v}_{\mathsf{S}z,\mathsf{S}y}$。所以我们得到 $\Box_{\mathsf{T}}(\mathsf{su}(\mathsf{S}z, \mathsf{S}y, \ulcorner u \approx v \urcorner))$，也就证明了断言 2。

我们把 $\mathsf{S}u \approx v$ 的情形留作习题。

断言 3. $\vdash u + v \approx w \to \Box_{\mathsf{T}}[u + v \approx w]$。

断言 3 的证明. 我们对 v 施行归纳。

当 v 是 0 的时候，我们需要证明

$$\vdash u + 0 \approx w \to \Box_{\mathsf{T}}(\mathsf{su}(u, 0, w, \ulcorner u + v \approx w \urcorner))。$$

假定 $u + 0 \approx w$。我们就有 $u \approx w$。根据断言 2，

$$\vdash u \approx w \to \Box_{\mathsf{T}}(\mathsf{su}(u, w, \ulcorner u \approx w \urcorner))。$$

在 PA 中我们有 $\vdash u \approx w \to u + 0 \approx w$。根据形式化的 (D1) 和 (D2)，$\vdash \Box_{\mathsf{T}}[u \approx w] \to \Box_{\mathsf{T}}[u + 0 \approx w]$，也就是

$$\vdash \Box_{\mathsf{T}}(\mathsf{su}(u, w, \ulcorner u \approx w \urcorner)) \to \Box_{\mathsf{T}}(\mathsf{su}(u, w, \ulcorner u + 0 \approx w \urcorner))。$$

利用 $\mathsf{su}(u,0,w,\ulcorner u+v\approx w\urcorner)\approx\mathsf{su}(u,w,\ulcorner u+0\approx w\urcorner)$ 这一事实，我们就证明了 v 是 0 的情形。

假定命题对 $v=y$ 成立。我们需要验证

$$\vdash u+\mathsf{S}y\approx w\to\Box_{\mathsf{T}}(\mathsf{su}(u,\mathsf{S}y,w,\ulcorner u+v\approx w\urcorner))。$$

假定 $u+\mathsf{S}y\approx w$。则 $\mathsf{S}(u+y)\approx w$。显然 $w\not\approx 0$，所以存在某个 z 使得 $w\approx\mathsf{S}z$。所以 $u+y\approx z$。根据归纳假定，我们有

$$\vdash\Box_{\mathsf{T}}(\mathsf{su}(u,y,z,\ulcorner u+v\approx w\urcorner)),$$

也就是 $(\Box_{\mathsf{T}}[u+v\approx w])^{u,v,w}_{u,y,z}$。根据引理 10.22，它与 $\Box_{\mathsf{T}}[u+y\approx z]$ 等价。

在 PA 中，我们有 $\vdash u+y\approx z\to u+\mathsf{S}y\approx\mathsf{S}z$。根据形式化的 (D1) 和 (D2)，我们有

$$\vdash\Box_{\mathsf{T}}[u+y\approx z]\to\Box_{\mathsf{T}}[u+\mathsf{S}y\approx\mathsf{S}z]。$$

于是我们得到 $\Box_{\mathsf{T}}[(u+v\approx w)^{u,v,w}_{u,\mathsf{S}y,\mathsf{S}z}]$。再次应用引理 10.22，它等价于 $(\Box_{\mathsf{T}}[u+v\approx w])^{u,v,w}_{u,\mathsf{S}y,\mathsf{S}z}$，也就是 $\Box_{\mathsf{T}}(\mathsf{su}(u,\mathsf{S}y,\mathsf{S}z,\ulcorner u+v\approx w\urcorner))$。断言 3 证毕。

我们把乘法 $u\times v\approx w$ 的情形留作习题。这就结束了对原子公式的讨论。

我们接下来讨论严格的 Σ_1-公式定义中出现的联词和量词。

断言 4. 如果 $\varphi=\psi\wedge\theta$，且引理对 ψ 和 θ 成立，则引理也对 φ 成立。

断言 4 的证明 根据假设，我们有

$$\vdash\psi\to\Box_{\mathsf{T}}[\psi]\quad\text{和}\quad\vdash\theta\to\Box_{\mathsf{T}}[\theta]。$$

所以 $\vdash\varphi\to(\Box_{\mathsf{T}}[\psi]\wedge\Box_{\mathsf{T}}[\theta])$。另一方面，我们有 $\psi\to\theta\to\varphi$。根据形式化的 (D1) 和 (D2)，我们有 $\vdash\Box_{\mathsf{T}}[\psi]\to\Box_{\mathsf{T}}[\theta]\to\Box_{\mathsf{T}}[\varphi]$。所以，$\vdash\varphi\to\Box_{\mathsf{T}}[\varphi]$。断言 4 证毕。

我们把 $\psi\vee\theta$ 的情形留作习题。

断言 5. 如果 $\varphi=\exists x\psi$ 且 $\vdash\psi\to\Box_{\mathsf{T}}[\psi]$，则 $\vdash\varphi\to\Box_{\mathsf{T}}[\varphi]$。

断言 5 的证明. 因为 $\vdash\psi\to\varphi$，所以 $\vdash\Box_{\mathsf{T}}[\psi]\to\Box_{\mathsf{T}}[\varphi]$。于是 $\vdash\psi\to\Box_{\mathsf{T}}[\varphi]$。由于 x 不在 φ 中自由出现，它也不在 $\Box_{\mathsf{T}}[\varphi]$ 中自由出现。应用概括规则，并将全称量词 $\forall$“推到”前件 ψ 上，全称于是变成存在，我们得到 $\vdash\exists x\psi\to\Box_{\mathsf{T}}[\varphi]$，也就是 $\vdash\varphi\to\Box_{\mathsf{T}}[\varphi]$。

断言 6. 如果 φ 是 $\forall u<v\,\psi(u)$ 且 $\vdash\psi\to\Box_{\mathsf{T}}[\psi]$，则

$$\vdash\varphi\to\Box_{\mathsf{T}}[\varphi]。$$

断言 6 的证明. 我们对 v 施行归纳。

当 v 是 0 的时候，我们需要证明

$$\vdash \forall u < 0\ \psi(u) \to \Box_{\mathsf{T}}(\mathsf{su}(0, \ulcorner \forall u < v\ \psi(u) \urcorner))。$$

我们只需要证明 $\vdash \Box_{\mathsf{T}}(\ulcorner \forall u < 0\ \psi(u) \urcorner)$，它可以由 $\vdash \forall u < 0\ \psi(u)$ 和 (D1) 得到。

假设命题对 $v = y$ 成立，我们验证

$$\vdash \forall u < \mathsf{S}y\ \psi(u) \to \Box_{\mathsf{T}}(\mathsf{su}(\mathsf{S}y, \ulcorner \forall u < v\ \psi(u) \urcorner))。$$

假定 $\forall u < \mathsf{S}y\ \psi(u)$。则 $\forall u < y\ \psi(u)$ 且 $\psi(y)$。根据归纳假定和对 ψ 的假设，我们有 $\Box_{\mathsf{T}}(\mathsf{su}(y, \ulcorner \forall u < v\ \psi(u) \urcorner))$ 且 $\Box_{\mathsf{T}}(\mathsf{su}(y, \ulcorner \psi(y) \urcorner))$，也就分别是 $(\Box_{\mathsf{T}}[\forall u < v\ \psi(u)])^v_y$ 和 $(\Box_{\mathsf{T}}[\psi(u)])^u_y$。根据引理 10.22，我们得到 $\Box_{\mathsf{T}}[\forall u < y\ \psi(u)]$ 和 $\Box_{\mathsf{T}}[\psi(y)]$。因为

$$\vdash \forall u < y\ \psi(u) \to \psi(y) \to \forall u < \mathsf{S}y\ \psi(u),$$

和形式化的 (D1) 和 (D2)，我们有 $\Box_{\mathsf{T}}[\forall u < \mathsf{S}y\ \psi(u)]$。仍根据引理 10.22，我们可以“提出”$\mathsf{S}y$ 得到 $\Box_{\mathsf{T}}(\mathsf{su}(\mathsf{S}y, \ulcorner \forall u < v\ \psi(u) \urcorner))$，这就证明了断言 6，也结束了引理 10.21 的证明。

第 4 节　哥德尔第二不完全性定理

固定一个在数论语言 $\mathcal{L}_{ar}$ 上满足可证性条件 (D1)、(D2) 和 (D3) 的理论 T。为了使用不动点引理，我们进一步假定 $T \supseteq \mathsf{Q}$。

定理 10.4 (哥德尔第二不完全性定理)**.**

(1) 如果 T 是相容的，则 $\nvdash_T \mathsf{con}_{\mathsf{T}}$。

(2) $\vdash_T \mathsf{con}_{\mathsf{T}} \to \neg\Box_{\mathsf{T}}\mathsf{con}_{\mathsf{T}}$。

证明: 我们先证明 (2)。令 σ 为公式 $\neg\Box_{\mathsf{T}}(x)$ 的一个不动点，即，

$$\vdash_T \sigma \leftrightarrow \neg\Box_{\mathsf{T}}\sigma。 \tag{10.1}$$

断言. $\vdash_T \sigma \leftrightarrow \mathsf{con}_{\mathsf{T}}$。换句话说，$T$ 证明所有 $\neg\Box_{\mathsf{T}}(x)$ 的不动点都等价于 $\mathsf{con}_{\mathsf{T}}$，或者说 $\mathsf{con}_{\mathsf{T}}$ 是 $\neg\Box_{\mathsf{T}}(x)$ 的唯一不动点（在 T 等价的意义下）。

断言的证明. 把 $\neg\Box_{\mathsf{T}}\sigma$ 转写成 $\Box_{\mathsf{T}}\sigma \to \bot$，其中 $\bot$ 为任何固定的矛盾式，如 $0 \not\approx 0$。一方面，由 (10.1) 我们有 $\sigma \vdash_T \Box_{\mathsf{T}}\sigma \to \bot$。利用 (D0) 和 (D2)，我们得到 $\Box_{\mathsf{T}}\sigma \vdash_T \Box_{\mathsf{T}}\Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}\bot$。而根据 (D3)，我们已经有 $\Box_{\mathsf{T}}\sigma \vdash_T \Box_{\mathsf{T}}\Box_{\mathsf{T}}\sigma$，所以，$\Box_{\mathsf{T}}\sigma \vdash_T \Box_{\mathsf{T}}\bot$。另一方面，我们显然有 $\bot \vdash \sigma$，仍利用 (D0)，$\Box_{\mathsf{T}}\bot \vdash_T \Box_{\mathsf{T}}\sigma$。因此，$\vdash_T \Box_{\mathsf{T}}\sigma \leftrightarrow \Box_{\mathsf{T}}\bot$。把这个等价式代回到 (10.1)，即得到 $\vdash_T \sigma \leftrightarrow \mathsf{con}_{\mathsf{T}}$。断言证毕。

利用断言和 (D0) 我们还有 $\vdash_T \Box_{\mathsf{T}}\sigma \leftrightarrow \Box_{\mathsf{T}}\mathsf{con}_{\mathsf{T}}$。在 (10.1) 式中，用 $\mathsf{con}_{\mathsf{T}}$ 替换 σ，用 $\Box_{\mathsf{T}}\mathsf{con}_{\mathsf{T}}$ 替换 $\Box_{\mathsf{T}}\sigma$，即得到

$$\vdash_T \mathsf{con}_{\mathsf{T}} \leftrightarrow \neg\Box_{\mathsf{T}}\mathsf{con}_{\mathsf{T}}。 \tag{10.2}$$

特别地，(2) 成立。

再看 (1)，如果 $\vdash_T \mathsf{con}_T$ 则根据 (D1)，$\vdash_T \Box_{\mathsf{T}}\mathsf{con}_{\mathsf{T}}$。利用 (10.2)，我们得到 $\vdash_T \neg\mathsf{con}_T$，这与 T 的相容性矛盾。 □

我们再次重复一下：哥德尔第二不完全性定理说明希尔伯特的纲领不可能照原样实现。

假定 PA 是相容的。令 PA^* 为 $\mathsf{PA} + \neg\mathsf{con}_{\mathsf{PA}}$。理论 PA^* 给我们提供了很多有意思的例子。特别地，它很好地说明了“形式系统内部”和“外部”的区别。所谓“不是庐山真面目，只缘身在此山中”。

引理 10.23. 理论 PA^* 是相容的，但 $\mathsf{PA}^* \vdash \neg\mathsf{con}_{\mathsf{PA}^*}$。

证明: 由哥德尔第二不完全性定理，理论 PA^* 是相容 的。

显然，$\mathsf{PA}^* \vdash \neg\mathsf{con}_{\mathsf{PA}}$，但我们还需要论证，“如果 PA 是不相容的，则 $\mathsf{PA}+\neg\mathsf{con}_{\mathsf{PA}}$ 也是不相容的”这一事实可以形式化在 PA 中。

这需要利用形式化的演绎定理：令 $T' = T + \alpha$。则

$$\vdash_T \Box_{\mathsf{T}'}\varphi \leftrightarrow \Box_{\mathsf{T}}(\alpha \to \varphi)。$$

（证明我们留作习题。）

根据形式化的演绎定理，我们有：

$$\mathsf{PA} \vdash \Box_{\mathsf{PA}+\alpha}\bot \leftrightarrow \Box_{\mathsf{PA}}(\alpha \to \bot),$$

即，

$$\mathsf{PA} \vdash \Box_{\mathsf{PA}+\alpha}\bot \leftrightarrow \Box_{\mathsf{PA}}(\neg\alpha)。$$

令 α 为 $\neg\mathsf{con}_{\mathsf{PA}}$，我们有

$$\mathsf{PA} \vdash \Box_{\mathsf{PA}^*}\bot \leftrightarrow \Box_{\mathsf{PA}}\mathsf{con}_{\mathsf{PA}}。$$

所以，

$$\mathsf{PA} \vdash \neg\mathsf{con}_{\mathsf{PA}^*} \leftrightarrow \Box_{\mathsf{PA}}\mathsf{con}_{\mathsf{PA}}。$$

即，

$$\mathsf{PA} \vdash \neg\mathsf{con}_{\mathsf{PA}^*} \leftrightarrow \neg\mathsf{con}_{\mathsf{PA}}。$$

现在，从 $\mathsf{PA}^* \vdash \neg\mathsf{con}_{\mathsf{PA}}$ 我们立刻得到 $\mathsf{PA}^* \vdash \neg\mathsf{con}_{\mathsf{PA}^*}$。 □

注：

- 一个理论 T 的相容性从里面看和从外面看可以是不一样的。PA^* 自己说自己是不相容的，但我们从外面看它却是相容的。另一方面，任何一个外面看不相容的理论都可证明自己的相容 性（当然也证明自己的不相容性）。一个很有趣的事实是：一个相容的理论可以断言自己的不相容性，却永不断言自己的相容性。
- PA^* 是 ω-不相容理论的典型例子，也说明存在这样的相容的理论 T 使得 $T + \mathsf{con}_{\mathsf{T}}$ 是不相容的。

10.4.1　勒布定理

勒布定理的最初动机是为了回答辛钦提出的一个问题。我们知道 $\neg\Box(x)$ 的不动点本质上就是 $\mathsf{con}_{\mathsf{T}}$。辛钦的问题是：那 $\Box(x)$ 的不动点又是什么呢？任何一个这样的不动点 σ 都断言自身的可证性，即 $T \vdash \sigma \leftrightarrow \Box_{\mathsf{T}}(\sigma)$。

定理 10.5 (勒布)**.**

(a) $\vdash_T \Box_{\mathsf{T}}(\Box_{\mathsf{T}}\alpha \to \alpha) \to \Box_{\mathsf{T}}\alpha$。（该条件也被称作 *(D4)*。）

(b) 如果 $\vdash_T \Box_{\mathsf{T}}\alpha \to \alpha$，则 $\vdash_T \alpha$。

证明: 令 σ 为 $\Box_{\mathsf{T}}(x) \to \alpha$ 的一个不动点，即

$$\vdash_T \sigma \leftrightarrow (\Box_{\mathsf{T}}\sigma \to \alpha)。 \tag{10.3}$$

与前面第二不完全性定理的证明类似，我们一方面从 $\sigma \vdash_T (\Box_{\mathsf{T}}\sigma \to \alpha)$ 中得到 $\Box_{\mathsf{T}}\sigma \vdash_T (\Box_{\mathsf{T}}\Box_{\mathsf{T}}\sigma \to \Box_{\mathsf{T}}\alpha)$；再用 (D3) 得到 $\Box_{\mathsf{T}}\sigma \vdash_T \Box_{\mathsf{T}}\alpha$。另一方面，我们有 $\vdash_T \alpha \to (\Box_{\mathsf{T}}\sigma \to \alpha)$（命题逻辑公理 (A3)），也就是 $\vdash_T \alpha \to \sigma$（根据 (10.3)）；所以 $\Box_{\mathsf{T}}\alpha \vdash_T \Box_{\mathsf{T}}\sigma$。所以，

$$\vdash_T \Box_{\mathsf{T}}\sigma \leftrightarrow \Box_{\mathsf{T}}\alpha。 \tag{10.4}$$

把这个等价式代回 (10.3)，我们有

$$\vdash_T \sigma \leftrightarrow (\Box_{\mathsf{T}}\alpha \to \alpha)。$$

利用 (D1) 和 (D2)，我们有

$$\vdash_T \Box_{\mathsf{T}}\sigma \leftrightarrow \Box_{\mathsf{T}}(\Box_{\mathsf{T}}\alpha \to \alpha)。$$

再次利用等价式 (10.4)，即得到

$$\vdash_T \Box_{\mathsf{T}}\alpha \leftrightarrow \Box_{\mathsf{T}}(\Box_{\mathsf{T}}\alpha \to \alpha)。$$

特别地，(a) 成立。

我们再来证明 (b)。假定 $\vdash_T \Box_{\mathsf{T}}\alpha \to \alpha$。则 $\vdash_T \Box_{\mathsf{T}}(\Box_{\mathsf{T}}\alpha \to \alpha)$（由 (D1)）。根据 (a)，$\vdash_T \Box_{\mathsf{T}}\alpha$。所以，$\vdash_T \alpha$。　□

推论 10.3. 令 $\top$ 表示任何一个普遍有效的闭语句，如 $0 \approx 0$。则 $\top$ 是 $\Box_{\mathsf{T}}(x)$ 的唯一不动点 (在 T 等价的意义下)。

证明: 显然，$\vdash \top$。根据 (D1)，$\vdash_T \Box_{\mathsf{T}}\top$。所以，$\top$ 是 $\Box_{\mathsf{T}}(x)$ 的一个不动点。假设 σ 是 $\Box(x)$ 的一个不动点，即 $\vdash_T \sigma \leftrightarrow \Box_{\mathsf{T}}\sigma$。则特别地，$\vdash_T \Box\sigma \to \sigma$。由勒布定理，$\vdash_T \sigma$。所以，$\vdash_T \sigma \leftrightarrow \top$。 □

最后，从勒布定理我们可以得到哥德尔第二不完全性定理 (a) 的一个简单证明：假设 PA 是相容的。如果 $\mathsf{PA} \vdash \mathsf{con}_{\mathsf{PA}}$，则 $\mathsf{PA} \vdash \Box\bot \to \bot$。由勒布定理，$\mathsf{PA} \vdash \bot$，与 PA 的相容性矛盾。

第 5 节　自然的不可判定语句

哥德尔的不完全性定理的证明告诉我们怎么找到那些满足特定条件的公理系统中无法判定的句子。但这些证明中作为例证的句子几乎都是诸如“我不可证”这样刻意构造的算术命题。人们似乎可以认为，所有独立的语句都是那样“非自然”的，源于对角线构造并涉及自指。若果真如此，那么哥德尔定理的哲学价值便显得成色不足了。至少人们可以期待，存在一些足够好的算术的公理系统，以至于所有“自然”的算术命题都可以在其中得到判定。因此，现在的问题是，是否存在经典数学所关心的自然的不可判定句子？

根岑的下述定理为寻找自然的不可判定语句打开了一扇门。

定理 10.6 (根岑)**.** 对任意小于 ε_0 的序数 α，PA 可以证明 $TI(\alpha)$，即到 α 的超穷递归；但 PA 不能证明 $IT(\varepsilon_0)$。

我们曾定义 $\varepsilon_0 = \lim_n \alpha_n$，其中 α_n 是通过递归定义的：$\alpha_0 = \omega$，而 $\alpha_{n+1} = \omega^{\alpha_n}$。类似哥德尔编码，我们可以在 PA 中为每个小于 ε_0 的序数编码，定义它们之间的序关系，并证明到它们的超穷递归。这样就有了定理的前半部分。

定理的后半部分常被解读为 PA 的一致性证明，只不过根岑在证明中额外假设了到 ε_0 的超穷归纳。因此，PA 无法证明 $IT(\varepsilon_0)$，否则它就可以证明自己的一致性。根岑证明中所使用的是等价于 PA 的自然推演系统，其中归纳原理以推理规则的形式引入。我们可以把这个自然推演系统中的每一个证明树对应到一个小于 ε_0 的序数 (的编码)。我们还可以定义对每个证明树的简化或归约，使得每一次简化所得到的推演对应的序数比原推演的要小，除非该证明树中不存在对归纳规则的使用，并且它们所得到的无量词的结论 (譬如 $0 = 1$) 是一样的。借助于 ε_0 上的超穷归纳，我们就可以把每个对 $0 = 1$ 的证明树简化为一个不使用归纳规则的对 $0 = 1$ 的证明树。而后者可以被证明是不存在的。这样，我们就得到了 PA 的一致性证明。限于篇幅，我们略去 ε_0 以下序数的编码、经典算术的自然推演系统、证明树到序数的对应、证明树的简化等技术细节，读者可以在典型的证明论教材 (如 [**?**]) 中找到更详尽的处理。

当然，人们仍然可以拒绝承认 $TI(\varepsilon_0)$ 是自然的数学语句。在 1977 年，帕里斯和哈灵顿证明了有穷拉姆齐定理的下述版本在 $\mathbb{N}$ 中成立却不是 PA 可证的。

定理 10.7. 对任意正整数 n, k, m，我们可以找到 N 使得：如果我们把集合 $S = \{1, 2, 3, \cdots, N$ 的每个恰好有 n 个元素的子集染成 k 种颜色中的一种，那么我们就可以找到 S 的一个至少含有 m 个元素的子集 Y，使得 Y 的每个含有恰好 n 个元素的子集都被染成同一种颜色，并且 Y 中元素的个数不小于 Y 中的最小元。

这被认为是第一个的在 $\mathbb{N}$ 中成立而不在 PA 可证的自然的数学语句。它是一个典型的有穷组合问题。还有一个更流行的例子，卡比和帕里斯证明了古德斯坦定理在 PA 中不可证。

对任意自然数 $m \geq 1$ 和 $n \geq 2$，我们可以定义 m 的 n 进制表达和纯 n 进制表达。我们举个例子来说明这两个概念：假定 $m = 13$ 而 $n = 2$，那么 $13 = 2^3 + 2^2 + 1$，后者就是 13 的 2 进制表达；进一步把指数也以 2 进制表示得到的 $2^{2+1} + 2 + 1$ 就是纯 2 进制表达。

我们定义一组自然数上的运算 G_n $(n \geq 2)$：为计算 $G_n(m)$，先把 m 写成纯 n 进制表达式，然后把表达式中所有的 n 换成 $n + 1$，最后减去 1。

定义 m 的从 n 开始的古德斯坦序列为：$m_0 = m$，$m_1 = G_n(m_0)$，$m_2 = G_{n+1}(m_1)$，$G_{n+2}(m_2)$ ……

例如，13 的从 2 开始的古德斯坦序列就是：

$$\begin{aligned}
m_0 &= 13, \\
m_1 &= 3^{3+1} + 3^3 = 108, \\
m_2 &= 4^{4+1} + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 = 1279, \\
m_3 &= 5^{5+1} + 3 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5 + 2 = 16092, \\
m_4 &= 6^{6+1} + 3 \cdot 6^3 + 3 \cdot 6^2 + 3 \cdot 6 + 1 = \ldots \\
\ldots &\quad \ldots
\end{aligned}$$

定理 10.8 (古德斯坦)**.** 对任意 m，$\lim_{n\to\infty} m_n = 0$.

证明: 把古德斯坦序列中所有的底都改成 ω 进制的。我们就得到一个严格递减的小于 ε_0 的序数序列。利用到 ε_0 的超穷归纳，就可以证明这个序列必定会在有穷步内归零。 □

上述两个自然的不可判定语句的例子都利用了到 ε_0 的超穷归纳，事实上他们的强度等价于到 ε_0 的归纳，因此不可能是 PA 的定理。这些不可判定性结果最终都归结为哥德尔不完全性定理，我们将之归结为由一致性强度的不同带来的不可判定性。对数理逻辑感兴趣的读者还会了解到其他证明不可判定性的方法，例如集合论中的内模型和力迫法。但这些方法注定不能给我们带来关于算术的不可判定语句。那么，是否存在不依赖一致性强度的证明方法证明算术语句不可判定性？这是个有趣且仍有待回答的问题。