

一阶逻辑 (I)

第 8 章 - 哥德尔第一不完备性定理 (简化版)

姚宁远

复旦大学哲学学院

December 20, 2021

目录

1 可表示性

2 鲁宾逊算术 Q

- 可表示性
- 函数的可表示性
- 仅用加法和乘法的编码
- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

算术模型

标准算术模型

结构 $\mathfrak{N} = (\mathbb{N}, 0, 1, \times, +)$, 语言是 $L = \{0, 1, \times, +\}$ 。称 $\text{Th}(\mathfrak{N})$ 算术理论。

- 我们已经研究过结构 $\mathfrak{N}_S, \mathfrak{N}_<, \mathfrak{N}_+$;
- 其一阶理论可以分别被 $T_S, T_<, T_+$ 公理化;
- 我们将证明 $\text{Th}(\mathfrak{N})$ 不能被公理化;
- 与之前的结构相比较, \mathfrak{N} 的表达能力的本质提升;
- \mathfrak{N} 可以表述有穷集合的理论。
- $\exists x_0 \dots \exists x_n \phi(\bar{x})$ 是一个合法的一阶表达式;
- 该公式的含义是: 存在一个长度为 $n+1$ 的序列使得 ϕ 成立
- 如何表述 “存在一个有穷序列 x , 使得 $\phi(x)$ 成立”?

目录

1 可表示性

2 鲁宾逊算术 Q

- 可表示性
- 函数的可表示性
- 仅用加法和乘法的编码
- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

鲁宾逊算术理论 Q

鲁宾逊算术理论 Q

- 1 (Q1) $Sx \neq 0$;
- 2 (Q2) $Sx = Sy \rightarrow x = y$;
- 3 (Q3) $x \neq 0 \rightarrow \exists y(x = sy)$;
- 4 (Q4) $x + 0 = x$;
- 5 (Q5) $x + Sy = S(x + y)$;
- 6 (Q6) $x \cdot 0 = 0$;
- 7 (Q7) $x \times Sy = x \times y + x$ 。

显然 $\mathfrak{N} \models Q$.

引理

- 1 $Q \not\models \forall x(Sx \neq x)$;
- 2 对每个标准自然数 $n \in \mathbb{N}$, $Q \vdash Sn \neq n$, 其中 n 代表 $S^n 0$ 。

证明

- 1 构造一个非标准的 $\mathfrak{M} = \mathbb{N} \cup \{\infty\}$;
- 2 对 $n \in \mathbb{N}$ 归纳证明。

注

- 1 标准自然数 n 对应闭项 $S^n 0$;
- 2 非标准数不是“自然的”。
- 3 断言“对每个标准自然数 $n \in \mathbb{N}$, $Q \vdash S^n \neq n$ ”不是一个证明，而是一族证明。
- 4 数学归纳法是元定理；

用 $x \leq y$ 表示 $\exists z(x + z = y)$ 。用 \vdash 表示 $Q \vdash$

引理

对所有的 $m, n \in \mathbb{N}$, 有

- 1 $\vdash \forall x(Sx + n = x + Sn)$;
- 2 $\vdash m + n = S^{m+n}0$ 并且 $\vdash m \cdot n = S^{m \cdot n}0$;
- 3 如果 $n \neq m$ 则 $\vdash n \neq m$;
- 4 如果 $n \neq m$ 则 $\vdash n \neq m$;
- 5 $\vdash \forall x(x \leq n \leftrightarrow x = 0 \vee \dots \vee x = n)$;
- 6 $\vdash \forall x(x \leq n \vee n \leq x)$ 。

注

设 $\mathfrak{M} \models Q$, \mathfrak{N} 是标准模型, 则

- 1 $n \mapsto n^{\mathfrak{M}}$ 是 \mathfrak{N} 到 \mathfrak{M} 的嵌入;
- 2 $\mathfrak{N} \subseteq \mathfrak{M}$;
- 3 如果 $b \in \mathfrak{N}$ 且 $a \leq^{\mathfrak{M}} b$, 则 $a \in \mathfrak{N}$;
- 4 \mathfrak{M} 是 \mathfrak{N} 的尾节扩张;

注

- 1 设 t 是一个含有 n 个变元的项;
- 2 则存在 $f \in \mathbb{N}[x_1, \dots, x_n]$ 使得 $Q \vdash t(x_1, \dots, x_n) = f(x_1, \dots, x_n)$;
- 3 如果 t 不含自由变元, 则称 t 是一个闭项;
- 4 如果 t 是一个闭项, 则存在 $n \in \mathbb{N}$ 使得 $Q \vdash t = n$;
- 5 对于闭项 t, s ,

$$Q \vdash t = s \iff \mathfrak{N} \models t = s \quad (\mathfrak{N} \models t = s)$$

1 可表示性

2 鲁宾逊算术 Q

■ 可表示性

- 函数的可表示性
- 仅用加法和乘法的编码
- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

令 T 是包含 Q 的一个理论。

定义

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 (简称可表示的), 如果存在公式 $\rho(x)$, 称为 P 的一个表示公式, 使得

$$(n_1, \dots, n_k) \in P \Rightarrow T \vdash \rho(n_1, \dots, n_k); \text{ 且}$$

$$(n_1, \dots, n_k) \notin P \Rightarrow T \vdash \neg \rho(n_1, \dots, n_k)$$

注

与

$$(n_1, \dots, n_k) \in P \iff T \vdash \rho(n_1, \dots, n_k); \text{ 且}$$

不等价。

引理

如果 T 可公理化, 则 T 是递归可枚举的。

证明:

- 1** T 是可公理化的 \iff 存在可判定的 Σ 使得

$$T = \{\sigma \mid \Sigma \vdash \sigma\}$$

- 2** Σ 可判定: $\#\Sigma = \{\#\sigma \mid \sigma \in \Sigma\} \subseteq \mathbb{N}$ 是可判定 (递归) 集合;

- 3** Σ 的证明的集合 P_Σ 可判定 (递归)

- 公式序列 $(\#\sigma_1, \dots, \#\sigma_n) \mapsto p \in \mathbb{N}$;
- $p \in P_\Sigma \iff \forall i < \text{lh}(p)$
 - $p_i \in \Sigma \cup Ax$;
 - 或 $\exists j, k < \text{lh}(p)(\alpha_k := \alpha_j \rightarrow \alpha_i), \# \alpha_{ijk} = p_{ijk}$;
- P_Σ 是递归的。

4 $\sigma \in T \iff \exists p(p \in P_\Sigma \wedge \exists i < \text{lh}(p)(p_i = \# \sigma))$;

5 $T(\#T)$ 是递归可枚举的;

6 $\#T$ 递归函数的值域。

引理

- 1 自然数上的等同关系 $\{(n, n) \mid n \in \mathbb{N}\}$ 被公式 $x = y$ 所表示;
- 2 小于关系 \leq 被公式 $x \leq y$ 所表示;
- 3 如果 P 是可表示的, 则 P 是递归的;
- 4 可表示的关系在布尔运算下是封闭的;
- 5 如果 P 在 Q 中被 ρ 表示, 则 P 在 Q 的任何一致扩张中都被 ρ 表示;
- 6 P 在 $\text{Th}(\mathfrak{N})$ 中被 ρ 表示当且仅当 P 在结构 \mathfrak{N} 中被 ρ 定义。

证明

证明:

[3] 如果 P 是可表示的, 则 P 是递归的。

- 1** T 有一个枚举函数 (程序) f , 即 $\#T = f(\mathbb{N})$;
- 2** 设 $P(x_1, \dots, x_k)$ 被 ρ 表示;
- 3** 设 $n_1, \dots, n_k \in \mathbb{N}$;
- 4** 用 T 的枚举函数 (程序) 检测 $\rho(n_1, \dots, n_k)$ 与 $\neg\rho(n_1, \dots, n_k)$ 是否属于 T ;
- 5** 如果 $\rho(n_1, \dots, n_k) \in T$, 则 $(n_1, \dots, n_k) \in P$;
- 6** 如果 $\neg\rho(n_1, \dots, n_k) \in T$, 则 $(n_1, \dots, n_k) \notin P$ 。
- 7** 以上的“算法”可以有效判定关系 $P(n_1, \dots, n_k)$ 。

证明

【4】 可表示的关系在布尔运算下是封闭的。

1 设 $P, R \subseteq \mathbb{N}^k$ 分别被 ψ 和 ρ 表示；

2 $P \cup R$ 被 $\psi \vee \rho$ 表示, $\mathbb{N} \setminus P$ 被 $\neg\psi$ 表示。

证明

[5] 如果 P 在 Q 中被 ρ 表示, 则 P 在 Q 的任何一致扩张中都被 ρ 表示。

1 对任意的 $n_1, \dots, n_k \in \mathbb{N}^k$

$Q \vdash \rho(n_1, \dots, n_k)$ 和 $Q \vdash \neg \rho(n_1, \dots, n_k)$ 有且仅有一个成立

2 如果 $Q \subseteq T$, 则

$$T \vdash \rho(n_1, \dots, n_k) \iff P \vdash \rho(n_1, \dots, n_k)$$

$$T \vdash \neg \rho(n_1, \dots, n_k) \iff P \vdash \neg \rho(n_1, \dots, n_k).$$

证明

【6】 P 在 $\text{Th}(\mathfrak{N})$ 中被 ρ 表示当且仅当 P 在结构 \mathfrak{N} 中被 ρ 定义。

■ 这是因为 $\text{Th}(\mathfrak{N})$ 是完备的。

推论

P 在 Q 中可表示, 则 P 在 \mathfrak{N} 中可定义。(反之则不成立)

Q 的 Σ_1 -完备性

- 1 称一个 L_{ar} 公式是 Δ_0 的, 如果它只包含有界量词。;
- 2 如果一个公式 ϕ (在 Q 下) 等价于 $\exists x_1 \dots \exists x_n \theta$, 其中 θ 是 Δ_0 的, 则称 ϕ 是 Σ_1 公式;
- 3 如果一个公式 ϕ 等价于 $\forall x_1 \dots \forall x_n \theta$, 其中 θ 是 Δ_0 的, 则 ϕ 是 Π_1 公式;
- 4 如果一个公式既等价于 Σ_1 公式, 又等价于 Π_1 公式。则它是 Δ_1 公式;

定理 (Σ_1 -完备性)

对任何一个 Σ_1 -闭语句 τ , 我们有

$$\mathfrak{N} \models \tau \iff Q \vdash \tau$$

证明 I

■: \Leftarrow : 对任意的 τ 都成立;

■: \Rightarrow :

■: 断言: 对任何 Δ_0 -闭语句 σ , 对任何的 $\mathfrak{M} \models Q$, 有

$$\mathfrak{M} \models \sigma \iff \mathfrak{N} \models \sigma$$

(Δ_0 -完备性)

1 对 σ 归纳证明 ($\mathfrak{N} \subseteq \mathfrak{M}$);

2 σ 不含量词时, $\sigma = \psi(n)$:

$$\mathfrak{N} \models \psi(n) \iff \mathfrak{M} \models \psi(n^{\mathfrak{M}}) \iff \mathfrak{M} \models \psi(n).$$

3 \vee 与 \neg 显然保持归纳假设;

4 设 σ 为 $(\forall x \leq t)\psi$ 且 ψ 是一个 Δ_0 公式, t 是一个闭项

证明 II

- 5 注意: 存在 $n \in \mathbb{N}$ 使得 $Q \vdash t = n$;
- 6 如果 $\mathfrak{M} \models (\forall x \leq t)\psi(x, t)$, 则 $\mathfrak{M} \models (\forall x \leq n)\psi(x, n)$;
- 7 $Q \vdash x \leq n \leftrightarrow \bigvee_{k \leq n} (x = k)$;
- 8 $\mathfrak{M} \models (\forall x \leq t)\psi(x, t) \iff \mathfrak{M} \models \bigwedge_{k \leq n} \psi(k, n)$;
- 9 由归纳假设: $\mathfrak{M} \models \psi(k, n) \iff \mathfrak{N} \models \psi(k, n)$;
- 10 $\mathfrak{N} \models \bigwedge_{k \leq n} \psi(k, n) \iff \mathfrak{N} \models (\forall x \leq t)\psi(x, t)$

现在设 σ 形如 $\exists x \psi(x)$, $x = x_1, \dots, x_n$, ψ 是 Δ_0 公式。

- 1 设 $\mathfrak{N} \models \sigma$;
- 2 则存在 $m \in \mathbb{N}^n$ 使得 $\mathfrak{N} \models \psi(m)$;
- 3 $Q \vdash \psi(m) \Rightarrow Q \vdash \exists x \psi(x)$.

引理

如果关系 $P \subseteq \mathbb{N}^{k+1}$ 被公式 $\rho(x, y)$ 所表示, 则关系

$$(\exists c < b)P(a, c) \text{ 和 } (\forall c < b)P(a, c)$$

分别被

$$(\exists z < b)\rho(x, z) \text{ 和 } (\forall z < b)\rho(x, z)$$

所表示。

证明: $Q \vdash x \leq n \leftrightarrow \bigvee_{k \leq n} (x = k)$ 。

1 可表示性

2 鲁宾逊算术 Q

- 可表示性

- 函数的可表示性

- 仅用加法和乘法的编码

- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

函数的可表示性

定义

称一个函数 $f: \mathbb{N}^k \rightarrow \mathbb{N}$ 为在 T 中可表示的, 如果存在一个 L_{ra} 中的公式 $\phi(x_1, \dots, x_k, y)$, 使得对所有的 $(n_1, \dots, n_k) \in \mathbb{N}^k$, 有

$$T \vdash \forall y \left(\phi(n_1, \dots, n_k, y) \leftrightarrow y = f(n_1, \dots, n_k) \right)$$

此时称 ϕ 作为一个函数表示 f 。

注

- 以上定义中的 f 是任意函数，不必可定义；
- 可以推出 f 在 \mathfrak{N} 中是可定义的；
- 公式 $\phi(x, y)$ 使得

$$\mathfrak{N} \models \phi(m, n) \Leftrightarrow n = f(m),$$

$$\mathfrak{N} \models \neg\phi(m, n) \Leftrightarrow n \neq f(m) \quad (\forall m, n \in \mathbb{N})$$

- 在 T 中可表示意味着：存在一个公式 $\psi(x, y)$ 表示函数 f 的图像，且对任意的 $a \in \mathbb{N}^k$ ，有

$$T \vdash \exists! y \psi(a, y) \quad (\text{注意: } \mathfrak{N} \models \forall x \exists! y \psi(x, y) \text{ 总是成立})$$

注

表示函数图像的公式不能表示函数：

- 设 f 是一个函数；
- 令 $G_f = \{(x, y) \mid y = f(x)\}$ ；
- 设公式 $\phi(x, y)$ 表示 G_f ；
- 对任意的 $a \in \mathbb{N}^k, b \in \mathbb{N}$, 有

$$f(a) = b \Rightarrow T \vdash \phi(a, b), \quad f(a) \neq b \Rightarrow T \vdash \neg \phi(a, b)$$

- 设 $\mathfrak{M} \models T$, 对于非标准的 $y \in M$

$$\mathfrak{M} \models y \neq f(a) \rightarrow \neg \phi(a, y)$$

不一定成立。

例

- 函数 $Z(x) = 0$;
- 公式 $\phi(x, y) : y + y = y$ 表示 G_Z ;
- Q 不能证明 $y + y = y \rightarrow y = 0$

■: 如果 $\phi(x, y)$ 表示一个函数 f , 则 $\phi(x, y)$ 表示 f 的函数图像;
■: 反之则不成立。

引理

令 t 为语言 L_{ar} 中的项, 则 t 诱导出来的函数是可表示的。

证明

$$\mathfrak{N} \models t(n_1, \dots, n_k) = m \iff T \models t(n_1, \dots, n_k) = m$$

$$T \models \forall x \exists! y (t(x) = y).$$

定理

可表示函数类关于复合封闭。

证明 I

■ 设 $f(x) = g(h_1(x), \dots, h_k(x))$

1 $h_i(x)$ 被 $\theta_i(x, y_i)$ 表示;

2 $g(y_1, \dots, y_k)$ 被 $\psi(y_1, \dots, y_k, z)$ 表示;

■ 断言: f 被

$$\varphi(x, z) := \forall y_1, \dots, y_k \left(\bigwedge_i \theta_i(x, y_i) \rightarrow \psi(y_1, \dots, y_k, z) \right)$$

表示, 即需要证明: $\forall n \in \mathbb{N}, T \vdash \forall z \left(\varphi(n, z) \leftrightarrow z = f(n) \right)$

■ \Rightarrow

证明 II

显然 $T \vdash \bigwedge_i \theta_1(n, y_i) \leftrightarrow \bigwedge_i y_i = h_i(n)$;

$$\left(\bigwedge_i \theta_1(n, y_i) \rightarrow \psi(y_1, \dots, y_k, z) \right) \leftrightarrow \left(\bigwedge_i y_i = h_i(n) \rightarrow \psi(y_1, \dots, y_k, z) \right)$$

$$T \cup \left\{ \bigwedge_i y_i = h_i(n) \rightarrow \psi(y_1, \dots, y_n, z) \right\} \vdash \psi(h_1(n), \dots, h_k(n), z)$$

$$T \cup \left\{ \bigwedge_i y_i = h_i(n) \rightarrow \psi(y_1, \dots, y_n, z) \right\} \vdash z = g(h_1(n), \dots, h_k(n))$$

故

$$T \cup \left\{ \bigwedge_i \theta_i(n, y_i) \rightarrow \psi(y_1, \dots, y_n, z) \right\} \vdash z = f(n)$$

证明 III

故

$$T \vdash \forall z \left(\forall y_1, \dots, y_n \left(\bigwedge_i \theta_i(n, y_i) \rightarrow \psi(y_1, \dots, y_k, z) \right) \rightarrow z = f(n) \right)$$

$$\text{即 } T \vdash \forall z \left(\varphi(n, z) \rightarrow z = f(n) \right)$$

■ \Leftarrow

$$T \cup \{z = g(h_1(n), \dots, h_k(n)), \bigwedge_i \theta_i(n, y_i)\} \vdash \psi(h_1(n), \dots, h_k(n), z)$$

$$T \cup \{z = g(h_1(n), \dots, h_k(n)), \bigwedge_i \theta_i(n, y_i)\} \vdash \bigwedge_i y_i = h_i(n)$$

证明 IV

$$T \cup \{z = f(n), \bigwedge_i \theta_i(n, y_i)\} \vdash \psi(y_1, \dots, y_k, z)$$

$$T \cup \{z = f(n)\} \vdash \bigwedge_i \theta_i(n, y_i) \rightarrow \psi(y_1, \dots, y_k, z)$$

引理

可表示函数类关于极小算子封闭:

- 1 设 $P \subseteq \mathbb{N}^{k+1}$ 被 $\alpha(x, y)$ 表示;
- 2 令 $\phi(x, y)$ 为 $\alpha(x, y) \wedge (\forall z < y) \neg \alpha(x, z)$;
- 3 则 $f : a \mapsto \mu b [P(a, b)]$ 被 $\phi(x, y)$ 表示:

证明:

首先证明: $\vdash \forall(y = f(a) \rightarrow \phi(a, y))$:

- 1 $y = f(a) \implies P(a, f(a))$ 且对每个 $c < f(a)$ 有 $\neg P(a, c)$;
- 2 故 $\vdash \alpha(a, f(a))$ 且;
- 3 $\vdash \bigwedge_{0 \leq i < f(a)} \neg \alpha(a, i)$;
- 4 $\vdash \bigwedge_{0 \leq i < f(a)} \neg \alpha(a, i) \longrightarrow (\forall z < f(a)) \neg \alpha(a, i)$.
- 5 故 $\vdash \forall(y = f(a) \rightarrow \phi(a, y))$.

再证明: $\vdash \forall(\phi(a, y) \rightarrow y = f(a))$:

- 1 只需证明: $(f(a) < y \vee y < f(a)) \wedge \phi(a, y)$ 不一致;
- 2 $f(a) < y \vdash \exists z < y (\alpha(a, z))$;
- 3 $y < f(a) \vdash y = 0 \vee \dots \vee y = f(a) - 1$;
- 4 故 $(f(a) < y \vee y < f(a)) \wedge \phi(a, y)$ 不一致;
- 5 $\phi(a, y) \vdash y = f(a)$.

推论

函数 f 可表示当且仅当 G_f 可表示。

证明

$a \mapsto \mu b[G_f(a, b)]$ 是可表示函数，它是 f 自身。

推论

假定函数 $g(x, y)$ 可表示, 则函数

$$f(x) := \mu y (g(x, y) = 0)$$

也可表示

目标

可表示函数类关于原始递归封闭

- : 初始函数 Y
- : 复合 Y
- : 正则极小化 Y
- : 原始递归 ? (编码)
- : $f(x, n) = m \Leftrightarrow$

$$\exists s \left(\text{lh}(s) = n + 1, s_0 = g(x), \forall i < n (s_{i+1} = h(x, i, s_i)), s_n = m \right)$$

- : 哥德尔数编码函数和解码函数涉及指数映射 x^y , 不满足要求。

1 可表示性

2 鲁宾逊算术 Q

- 可表示性
- 函数的可表示性
- 仅用加法和乘法的编码
- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

哥德尔的 β 函数 I

定义

哥德尔函数 $\beta : \mathbb{N}^3 \rightarrow \mathbb{N}^{<\omega}$ 定义为: 对任意的 u, v, w , $\beta(u, v, w)$ 是一个长度为 w 的序列 a_0, \dots, a_{w-1} , 其中 a_i 满足:

$$u = d((i+1)v + 1) + a_i$$

注

- 定义 $\alpha(u, v, i)$ 为 $\frac{u}{v(i+1)+1}$ 的余数, 即 β 函数的坐标分量函数, 则 $\alpha(u, v, i)$ 是可表示的 (稍后证明)。
- β 将有穷序列 $\alpha(u, v, 0), \dots, \alpha(u, v, w)$ 编码为一个三元组

哥德尔的 β 函数 II

定理

哥德尔函数 $\beta : \mathbb{N}^3 \rightarrow \mathbb{N}^{<\omega}$ 是满射。

注

- 每个有穷序列被哥德尔函数编码为一个三元组；
- “存在一个有穷序列”可表述为 “ $(\exists u, v, w) \dots$ ”

接下来我们来证明该定理。

欧几里得引理 (PA 可证)

设 $a, b \in \mathbb{N}$ 是互素的, 则存在 $x, y \in \mathbb{Z}$ 使得 $ax + by = 1$ 。

证明:

- 令 $X = \{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}$;
- 则 X 有最小元 x_0 ;
- 如果 x_0 不能整除 a , 则 $a = cx_0 + r$;
- 从而 $0 < r < x_0$, 且 $r = a - cx_0 \in X$, 与 x_0 是最小元矛盾。
- x_0 是 a, b 的公约数, 即 $x_0 = 1$ 。

中国剩余定理 (PA 可证)

令 d_0, \dots, d_n 是两两互素的自然数, a_0, \dots, a_n 为满足 $a_i < d_i$ 的自然数, 则存在自然数 c , 使得 a_i 是 c 除 d_i 的余数。即 c 是以下同余方程组的解。

$$x \equiv_{d_0} a_0$$

$$x \equiv_{d_1} a_1$$

...

$$x \equiv_{d_n} a_n$$

证明

对 n 归纳证明:

- 1 $n = 0$ (一个方程) 时显然
- 2 设 $n = k$ 时成立, 下面证明 $n = k + 1$ 的情形;
- 3 令 b 为方程组 $\{x \equiv_{d_i} a_i \mid i \leq k\}$ 的解;
- 4 令 d 为 d_0, \dots, d_k 的最小公倍数, 则 $(d, d_{k+1}) = 1$;
- 5 显然, 对任意的 m , 以及 d_i , $b + md \equiv_{d_i} b$;
- 6 故 $b + md$ 也是方程组 $\{x \equiv_{d_i} a_i \mid i \leq k\}$ 的解;
- 7 **断言**: 存在 r, s 使得 $b + rd = sd_{k+1} + a_{k+1}$;
- 8 取 $u, v \in \mathbb{Z}$ 使得 $ud + vd_{k+1} = 1$;
- 9 $b = b(ud + vd_{k+1})$. $a_{k+1} = a_{k+1}(ud + vd_{k+1})$;
- 10 $b - a_{k+1} = b(ud + vd_{k+1}) - a_{k+1}(ud + vd_{k+1}) = -rd - sd_{k+1}$;
- 11 显然 $b + rd$ 是方程组 $\{x \equiv_{d_i} a_i \mid i \leq k + 1\}$ 的解.

引理

对任意的 n , 存在 $n + 1$ 个数两两互素:

$$1 + n!, 1 + 2 \cdot n!, \dots, 1 + (n + 1) \cdot n!$$

证明

设 $p | 1 + (i + 1) \cdot s!$. $p | 1 + (j + 1) \cdot s!$, 则 $p | (j - i) \cdot s! \Rightarrow p | s!$. 矛盾。

哥德尔定理

定理

哥德尔函数 $\beta : \mathbb{N}^3 \rightarrow \mathbb{N}^{<\omega}$ 是满射。

证明：

- 设 a_0, \dots, a_{w-1} 是一个自然数的序列；
- 令 $n = \max\{a_0, \dots, a_{w-1}, w\}$
- 令 $v = n!$
- 则 $\{v(i+1) + 1 \mid i = 0, \dots, w-1\}$ 两两互素且 $a_i < v(i+1) + 1$;
- 根据中国剩余定理，存在 $u \in \mathbb{N}$ 使得 $u \equiv_{v(i+1)+1} a_i$;
- 故 β 是满射。

注

对 $i < w$ ，令 $\beta(u, v, w, i) = a_i$ ，则 $\beta(u, v, w, i)$ 是一个可定义函数，也是递归函数。

$\alpha(u, v, i)$ 的可表示性 I

引理

$$\alpha(u, v, i) = \frac{u}{v(i+1) + 1} \text{ 的余数}$$

是可表示的

- 1 关系 $P(c, d, i, r, q) =_{\text{def}} (c = q(1 + (i+1)d) + r)$ 可表示;
- 2 关系 $R(c, d, i, r) =_{\text{def}} \exists q \leq c P(c, d, i, r, q)$ 可表示:

$\alpha(u, v, i)$ 的可表示性 II

3

$$R(c, d, i, r) \Rightarrow \mathfrak{N} \models \exists q \leq c (P(c, d, i, r, q))$$

$$\Rightarrow Q \vdash \exists q \leq c (P(c, d, i, r, q));$$

$$\neg R(c, d, i, r) \Rightarrow \mathfrak{N} \models \forall q \leq c \neg (P(c, d, i, r, q))$$

$$\iff \mathfrak{N} \models \bigwedge_{k \leq c} \neg P(k, d, i, r, q) \iff Q \vdash \bigwedge_{k \leq c} \neg P(k, d, i, r, q);$$

$$\Rightarrow Q \vdash \forall q \leq c \neg (P(c, d, i, r, q));$$

4 $\mu r(R(c, d, i, r))$ 是可表示函数。

递归函数的可表示性 I

定义 $\alpha(u, v, i)$ 为 $\frac{u}{v(i+1)+1}$ 的余数。

定理

递归函数都是可表示的。

证明：

- 只需证明 \mathfrak{N} 中的可表示函数类包含初始函数，且对复合，极小化，以及原始递归封闭。
- 显然初始函数都是可表示的；
- 可表示函数显然对复合封闭；
- 可表示函数显然对极小化封闭；
- 可表示函数对原始递归封闭：

1 设 $f(x, 0) = g(x)$, $f(x, n+1) = h(x, n, f(x, n))$;

递归函数的可表示性 II

- 2 其中 g, h 均是可定义函数;
- 3 令 $\psi(u, v, x) := \alpha(u, v, 0) = g(x)$
- 4 令 $\phi(u, v, x) := \forall i < y (\alpha(u, v, i+1) = h(x, i, \alpha(u, v, i+1)))$
- 5 则定义 $f(x, y) = z$ 的公式为:

$$\exists u, v \left(\psi(u, v, x) \wedge \phi(u, v, x) \wedge z = \alpha(u, v, y) \right)$$

- 6 由 Q 的 Σ_1 -完备性, f 可表示。

推论

由以上证明可知: 原始递归函数都是 Σ_1 -可表示的, 从而也是 Π_1 -可表示的。

同理, 递归可枚举集合都是 Σ_1 -可表示的, 从而递归关系都是 Δ_1 -可表示的。

注

- 1 (在 PA 下) 根据中国剩余定理:
- 2 对任意的 n , 以及 a_0, \dots, a_n ;
- 3 存在 c, d 使得 $\alpha(c, d, i) = a_i$;
- 4 即 (c, d) 是 a_0, \dots, a_n 的编码, α 是一个解码函数。

引理 (\mathbb{N}^2 编码为 \mathbb{N})

令

$$J(a, b) = \frac{1}{2}(a + b)(a + b + 1) + a;$$

$$K(p) = \mu a \leq p \exists b \leq p (J(a, b) = p);$$

$$L(p) = \mu b \leq p \exists a \leq p (J(a, b) = p);$$

则函数 J, K, L 都在 Q 中可表示。

引理 (PA)

$J(a, b)$ 是双射函数。因此对任意的 $(a, b) \in \mathbb{N}^2$, 存在 $p \in \mathbb{N}$ ($p = J(a, b)$) 使得 $K(p) = a$, $L(p) = b$.

Proof.

对 a, b 归纳证明。



定理 (PA)

存在一个由加法, 乘法, 以及极小算子复合而成的函数 $\beta^* : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, 使得对任意的

$$n, a_0, \dots, a_n \in \mathbb{N}$$

都存在 $s \in \mathbb{N}$ 满足 $\beta^*(s, i) = a_i$ ($i \leq n$)

证明

令 $\beta^*(s, i) = \alpha(K(s), L(s), i)$.

1 可表示性

2 鲁宾逊算术 Q

- 可表示性
- 函数的可表示性
- 仅用加法和乘法的编码
- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

定理

所有的递归函数都是可表示的，故递归关系也都是可表示的。

回忆：可表示关系是被 " $T \vdash$ " 表示的，从而是递归的。

推论

若 $R \subseteq \mathbb{N}^k$, $Q \subseteq T$ 是递归且一致的。则以下命题等价

- 1 R 在 T 中可表示；
- 2 R 是递归关系；

推论

若 $R \subseteq \mathbb{N}^k$, $Q \subseteq T$ 是递归且一致的。则以下命题等价

- 1 R 在 T 中可表示;
- 2 R 是在 T 中被一个 Δ_1 公式表示;

断言

递归关系被结构 \mathfrak{N} 中的一个 Δ_1 公式定义;

证明

$1 \Rightarrow 2$: R 被一个 Σ_1 公式定义, $\neg R$ 也被 Σ_1 公式定义 (在 \mathfrak{N} 中)。由 Q 的 Σ_1 完备性可得。

目录

1 可表示性

2 鲁宾逊算术 Q

- 可表示性
- 函数的可表示性
- 仅用加法和乘法的编码
- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

哥德尔编码

本节的目标是利用编码在 \mathfrak{N} (或 Q) 中讨论语法和部分语义

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

1 符号串 $\xi = \xi_0 \dots \xi_n$ 的编码为哥德尔数

$$(\# \xi_0, \dots, \# \xi_n) = p_0^{\# \xi_0 + 1} \dots p_n^{\# \xi_n + 1}$$

2 项与公式作为符号串，编码是一个偶数；

3 作为符号的 0 编码为 3，作为项的 0 编码为 16；

4 上述编码方案可以推广到一般的语言 L 上，要求 L 的符号集合可判定；

5 本节的工作都是在标准模型 \mathfrak{N} 中完成的。

语法算术化 I

变元集

$V = \{\# \alpha \mid \alpha \text{ 是一个变元}\}$ 是原始递归的:

$$\text{Var} = \{n \in \mathbb{N} \mid \exists k < n (n = 2k + 1)\}$$

注

一般地, 对逻辑对象 O , 我们用 \underline{O} 表示的编码集 (其在 \mathfrak{N} 中的同构像), 即

$$\underline{O} = \{\# \alpha \mid \alpha \in O\}$$

语法算术化 II

项集

$$\text{Term} = \{\alpha \mid \alpha \text{ 是一个 } \underline{\text{项}}\}$$

是原始递归的.

证明:

项的定义是递归的。 t 是一个 项，如果

- 1 $\exists s < t (t = (s) \wedge (s \in \text{Var} \vee s = 0))$ ，或者
- 2 $\exists r, s < t (t = (r)^{\wedge} s \wedge r = \underline{S} \wedge s \in \text{Term})$
- 3 $\exists q, r, s < t (t = (q)^{\wedge} r^{\wedge} s \wedge (q = \underline{\pm} \vee q = \underline{\cdot}) \wedge r, s \in \text{Term})$

故 Term 是原始递归的

语法算术化 III

类似地：

公式集

$$\text{Form} = \{\alpha \mid \alpha \text{ 是一个 公式}\}$$

是原始递归的.

替换函数

语法算术化 IV

存在一个原始递归函数 Sb 使得对任意的项或者公式 α , 对任意的变元 x 和任意的项 t , 有

$$Sb(\# \alpha, \# x, \# t) = \# \alpha_t^x$$

是原始递归的.

语法算术化 V

数码集合

函数

$$f(n) = \#(S^n 0)$$

是原始递归的, 故数码集合

$$\text{Num} = \{m \mid m \text{ 是一个 数码}\} = \{m \mid \exists n < m (m = f(n))\}$$

是原始递归的。

语法算术化 VI

·
 设 x 是一个数, 则 $\ulcorner x \urcorner$ 表示 x 的解码后得到的“一阶语言”对应物。

自由出现

$\text{Free}(x, y)$ 表示: x 是 变元, y 是 项 或 公式, 且 $\ulcorner x \urcorner$ 在 $\ulcorner y \urcorner$ 中自由出现。则 $\text{Free}(x, y)$ 是原始递归的。

$$\text{Free}(x, a) \iff \text{Sb}(a, x, (0)) \neq a$$

语法算术化 VII

闭语句

$\text{Sen}(x)$ 表示: x 是 闭语句。则 $\text{Sen}(x)$ 是原始递归的。

$$\text{Sen}(x) \iff (x \text{ 是 } \underline{\text{公式}}) \wedge (\forall x < a \neg \text{Free}(x, a))$$

闭语句

$\text{Sub}(x, t, a)$ 表示: a 是 公式, t 是 项, x 是 变元, t 可在 a 中替换 x 。则 $\text{Sub}(x, t, a)$ 是原始递归的。

语法算术化 VIII

证明

- 1 a 是 $\neg b$, a 是 $b \rightarrow c$, 和 a 是 $\forall yb$ 均是原始递归的;
- 2 $\text{Sub}(x, t, a)$ 递归地定义为
 - 如果 a 是 原子公式, 则 $\text{Sub}(x, t, a)$ 总是成立;
 - 如果 a 是 $\neg b$, 则 $\text{Sub}(x, t, a) \iff \text{Sub}(x, t, b)$;
 - 如果 a 是 $b \rightarrow c$, 则
$$\text{Sub}(x, t, a) \iff \text{Sub}(x, t, b) \wedge \text{Sub}(x, t, c)$$
 - 如果 a 是 $\forall yb$, 则 $\text{Sub}(x, t, a) \iff \text{Sub}(x, t, b) \wedge y \notin t$;

⋮

语法算术化 IX

逻辑公理

集合

$$Ax = \{a \mid a \text{ 是一条 } \underline{\text{逻辑公理}}\}$$

是原始递归集。

证明序列

设 T 是可公理化的, 则 T 被可判定集合 X 公理化, 集 X 是递归集, 则谓词

$$b \text{ 是 } T \text{ 上的一个 } \underline{\text{证明序列}}$$

是递归的。

语法算术化 X

证明 + 结论

设 T 同上, 令 $\text{bew}_T(b, a)$ 表示

b 是 T 上的一个 证明序列 且 $b_{\text{lh}(b)-1} = a$

则 $\text{bew}_T(b, a)$ 是递归的

可证性

设 T 同上, 令 $\text{bwb}_T(a)$ 表示 $\exists b \text{ bew}_T(b, a)$ 。它是递归可枚举的。

目录

1 可表示性

2 鲁宾逊算术 Q

- 可表示性
- 函数的可表示性
- 仅用加法和乘法的编码
- 可表示定理

3 语法的算术化

4 不可定义性、不完全性、不可判定性

塔斯基定理 I

塔斯基定理

集合 $\# \text{Th}(\mathfrak{N})$ 在结构 \mathfrak{N} 中是不可定义的。

证明：

- 1 设一阶公式 $V(x)$ 定义了 $\# \text{Th}(\mathfrak{N})$;
- 2 即 $\mathfrak{N} \models V(n) \iff n \in \# \text{Th}(\mathfrak{N})$;
- 3 令 A 为含有一个变元 x 的公式的编码的集合;
- 4 则 A 可定义;
- 5 令 f 为部分函数: $A \times \mathbb{N} \rightarrow \mathbb{N}$,
- 6 $f : (a, m) \mapsto$ “ a 中变元 x 替换为 m 所得闭语句的编码”
- 7 显然, f 可定义;
- 8 令 $U(x, y)$ 为公式 $V(f(x, y)) \wedge A(x)$;

塔斯基定理 II

9 显然 $U(n, m)$ 成立当且仅当存在 $\phi(x)$ 使得

- $n = \# \phi(x)$;
- $\phi(m)$ 成立

10 令 n_0 为 $\psi(x) := \neg U(x, x)$ 的编码;

11 则 $U(n_0, n_0) \iff \psi(n_0) \iff \neg U(n_0, n_0)$;

12 矛盾

推论

集合 $\text{Th}(\mathfrak{N})$ 不是可判定的, 即 $\# \text{Th}(\mathfrak{N}) \subseteq \mathbb{N}$ 不是递归的。

证明:

递归集都是可定义的。

哥德尔第一不完全性定理

定理

如果 $T \subseteq \text{Th}(\mathfrak{N})$ 是可公理化的, 则 T 是不完全的。特别地, $\text{Th}(\mathfrak{N})$ 不能公理化。

证明

- 1 如果 $T \subseteq \text{Th}(\mathfrak{N})$ 是完全的, 则 $T = \text{Th}(\mathfrak{N})$;
- 2 如果 T 可得公理化, 则 $\text{Th}(\mathfrak{N})$ 可判定;

其他结论

定理

- $\#(\Sigma_n \cap \text{Th}(\mathcal{N}))$ 被一个 Σ_n 公式定义, 该公式不是 Π_n -公式
- $\#(\Pi_n \cap \text{Th}(\mathcal{N}))$ 被一个 Π_n 公式定义, 该公式不是 Σ_n -公式

Thanks!