

可计算性与可判定性

第五讲：哥德尔不完备性定理

喻良

南京大学现代数学研究所

December 25, 2013

语言编码

定义 $\sharp$ 为逻辑符号到自然数上的函数:

$$\sharp(\forall) = 1, \sharp(\exists) = 2, \sharp(\vee) = 3, \sharp(\neg) = 4,$$

$$\sharp(=) = 5, \sharp(() = 6, \sharp()) = 7。$$

$$\sharp(v_i) = 8i + 1, \sharp(c_i) = 8i + 2, \sharp(R_i) = 8i + 3, \sharp(f_i) = 8i + 4。$$

公式的编码

对于一串语言符号 $s_0, s_1, \dots, s_n$,

$$\sharp(s_0, s_1, \dots, s_n) = \langle s_0, s_1, \dots, s_n \rangle.$$

公式的编码

对于一串语言符号 $s_0, s_1, \dots, s_n$,

$$\sharp(s_0, s_1, \dots, s_n) = \langle s_0, s_1, \dots, s_n \rangle.$$

例如: $\sharp(\exists v_i(v_i = v_i)) = \langle 2, 8i + 1, 6, 8i + 1, 5, 8i + 1, 7 \rangle.$

编码的能行性

Theorem

在哥德尔编码下，变量集合，项集合，原子公式集合以及公式集合都是递归的。

证明是一连串公式的集合，因此证明也是递归的，从而关系“存在 φ 到 ψ 的证明”是递归可枚举的。

可表示性

从现在起，我们只讨论算术语言。

Definition

一个关系 $R(v_0, \dots, v_n)$ 是可表示的，如果存在一个公式 $\varphi(v_0, \dots, v_n)$ 使得对于所有的自然数 $k_0, \dots, k_n$,

$$R(k_0, \dots, k_n) \leftrightarrow \text{PA} \vdash \varphi(\overline{k_0}, \dots, \overline{k_n})$$

并且

$$\neg R(k_0, \dots, k_n) \leftrightarrow \text{PA} \vdash \neg \varphi(\overline{k_0}, \dots, \overline{k_n})$$

注意公式右端 $\overline{k_i}$ 是 $1 + 1 + \dots + 1$, k_i 个 1 连续相加的缩写。

可表示性定理

Definition

一个函数 f 是可表示的, 如果存在一个公式 $\varphi(v_0, \dots, v_n, v_{n+1})$ 使得对于所有的 $k_0, \dots, k_n$,

$$\text{PA} \vdash \forall v (\overline{\#(f(k_0, \dots, k_n))} = v \leftrightarrow \varphi(\overline{k_0}, \dots, \overline{k_n}, v))$$

Theorem

一个关系 R 是可表示的当且仅当 R 是递归的。而且每一个递归函数是可表示的。

Proof.

考虑原始递归 $h(0, x_2, \dots, x_n) = g(x_2, \dots, x_n)$ 并且 $h(y+1, x_2, \dots, x_n) = f(y, h(y, x_2, \dots, x_n), x_2, \dots, x_n)$. □

不动点定理

Theorem

给定一个公式 $\beta(v)$, 存在一个句子 ψ 使得 $PA \vdash \psi \leftrightarrow \beta(\overline{\#(\psi)})$.

Proof.

令 $f(n, m) = \#(\#^{-1}(n)(\bar{m}))$. 则 f 是递归的, 因此存在一个公式 θ 使得函数 f 被 θ 所表示。

对于任意一个公式 $\beta(v)$, 令 $q = \#(\forall v(\theta(u, u, v) \rightarrow \beta(v)))$,

令 ψ 为 $\forall v(\theta(\bar{q}, \bar{q}, v) \rightarrow \beta(v))$. 则 $f(q, q) = \#(\psi)$.

即 $PA \vdash \forall v(\theta(\bar{q}, \bar{q}, v) \rightarrow v = \#(\psi))$.

因此 $PA \vdash \beta(\#(\psi)) \rightarrow \forall v(\theta(\bar{q}, \bar{q}, v) \rightarrow \beta(v))$, 即 $PA \vdash \beta(\#(\psi)) \rightarrow \psi$.

因为 $PA \vdash \theta(\bar{q}, \bar{q}, \#(\psi))$, 因此 $PA \vdash \psi \rightarrow \beta(\#(\psi))$.

即 $PA \vdash \psi \leftrightarrow \beta(\#(\psi))$.



证明

定义关系 $R(x, y)$ 当且仅当 $\sharp^{-1}(y)$ 是 $\sharp^{-1}(x)$ 的一个证明。
则 R 是递归的，因此存在一个公式 $\text{Prov}(u, v)$ 表示 R 。

ω -协调性

Definition

一个理论 T 称为 ω -协调的如果不存在公式 $\varphi(v)$ 使得 $T \vdash \exists v \varphi(v)$, 但是对所有的 n , $T \vdash \neg \varphi(\bar{n})$ 。

如果 $(\omega, +, \cdot, <, 0, 1) \models T$, 则 T 是 ω -协调的。

哥德尔第一不完备性

Theorem

如果PA是 ω -协调的, 则存在一个句子 φ 使得它和它的否定都不能被PA证明。

Proof.

令 φ 使得 $PA \vdash \varphi \leftrightarrow \neg \exists y \text{Prov}(\overline{\#(\varphi)}, y)$.

如果 $PA \vdash \varphi$, 则存在 φ 的一个证明, 因此 $PA \vdash \exists \text{Prov}(\overline{\#(\varphi)}, y)$.

如果 $PA \vdash \neg \varphi$, 则 $PA \vdash \exists y \text{Prov}(\overline{\#(\varphi)}, y)$ 。由表示性定理, 对于所有 n , $PA \vdash \neg \text{Prov}(\overline{\#(\varphi)}, \bar{n})$ 。则PA不是 ω -协调的。 □

有穷主义

严格的有穷主义证明:

- ① 有穷个符号列表;
- ② 一个有穷集的有穷符号串;
- ③ 有穷个算子;
- ④ 所有表达式都通过以上方式生成。

Rosser定理

Theorem

如果PA是协调的，则存在一个句子 φ 使得它和它的否定都不能被PA证明。

Proof.

令 φ 使

得 $PA \vdash \varphi \leftrightarrow \neg(\exists y(\text{Prov}(\overline{\#(\varphi)}), y) \wedge \forall z < y(\neg \text{Prov}(\overline{\#(\neg\varphi)}), z)))$ 。

如果 $PA \vdash \varphi$ ，则存在 φ 的一个证明，因此存在一个自然数 n 编码 φ 的证明。所

以 $PA \vdash \exists y(\text{Prov}(\overline{\#(\varphi)}), y) \wedge \forall z < y(\neg \text{Prov}(\overline{\#(\neg\varphi)}), z))$ 。

如果 $PA \vdash \neg\varphi$ ，则存在一个自然数 n 编码 $\neg\varphi$ 的证明。因为PA是协调的，所有 φ 的证明必定大于 n 。因

此 $PA \vdash \exists y \text{Prov}(\overline{\#(\varphi)}), y \rightarrow \exists z < y(\text{Prov}(\overline{\#(\neg\varphi)}), z))$ ，矛盾！



Tarski真值定理

Theorem

没有一个公式 $\varphi(v)$ 使得对所有自然数 n , $(\omega, +, \cdot, <, 0, 1) \models \varphi(n)$ 当且仅当 $(\omega, +, \cdot, <, 0, 1) \models \sharp^{-1}(n)$ 。

Proof.

如果存在这样一个公式。由不动点定理, 存在一个自然数 n 使得 $(\omega, +, \cdot, <, 0, 1) \models \neg\varphi(n)$ 当且仅当 $(\omega, +, \cdot, <, 0, 1) \models \sharp^{-1}(n)$ 。矛盾!

Corollary

- $\{\sharp(\varphi) \mid (\omega, +, \cdot, <, 0, 1) \models \varphi\}$ 不是递归的。
- 对于任何PA的协调扩张 T , $\{\sharp(\varphi) \mid T \vdash \varphi\}$ 不是递归的。

三个引理

我们用 $\text{Prb}(v)$ 表示 $\exists u \text{Prov}(v, u)$.

Lemma

- ① $\text{PA} \vdash \varphi \text{ 蕴含 } \text{PA} \vdash \text{Prb}(\overline{\# \varphi})$;
- ② $\text{PA} \vdash \overline{\text{Prb}(\#(\varphi))} \rightarrow \overline{\text{Prb}(\#(\text{Prb}(\#(\varphi))))}$;
- ③ $\text{PA} \vdash \overline{\text{Prb}(\#(\varphi \rightarrow \psi))} \rightarrow (\overline{\text{Prb}(\#(\varphi))} \rightarrow \overline{\text{Prb}(\#(\psi))})$.

协调性的不可证明性

我们用 Con 表示 $\neg \text{Prb}(\overline{\#(0 = 1)})$.

Theorem

如果PA是协调的, 那么 $\text{PA} \not\vdash \text{Con}$.

Proof.

由不动点定理, 存在 φ 使得 $\text{PA} \vdash \varphi \leftrightarrow \neg \text{Prb}(\overline{\#(\varphi)})$. 因此 $\text{PA} \vdash \varphi \rightarrow (\text{Prb}(\overline{\#(\varphi)}) \rightarrow 0 = 1)$. 由引理(1), $\text{PA} \vdash \text{Prb}(\overline{\#(\varphi \rightarrow (\text{Prb}(\overline{\#(\varphi)}) \rightarrow 0 = 1))})$. 由引理(2), (3), $\text{PA} \vdash \text{Prb}(\overline{\#(\varphi)}) \rightarrow \neg \text{Con}$. 从而 $\text{PA} \vdash \text{Con} \rightarrow \neg \text{Prb}(\overline{\#(\varphi)})$. 于是 $\text{PA} \vdash \text{Con} \rightarrow \varphi$.
如果 $\text{PA} \vdash \text{Con}$, 那么 $\text{PA} \vdash \varphi$, 从而 $\text{PA} \vdash \text{Prb}(\overline{\#(\varphi)})$ 并且 $\text{PA} \vdash \neg \text{Prb}(\overline{\#(\varphi)})$. 矛盾!



PA的非标准模型

Corollary

存在PA的可数模型 $\mathcal{M} \models \text{PA}$ 是不协调的.

不完备性的一些推广

PA可以替换成任何蕴含PA的递归的公理系统。
甚至可以推广到非算术语言中。只需要那些公理系统是递归的并且能“解释”PA. 例如ZF.

一些具体的不可证明性举例 (I)

令 $M \longrightarrow (k)_r^e$ 表示对于每一个函数 $f: [M]^e \rightarrow r$ 都存在一个集合 $H \subseteq M$ 使得

- $|H| = k$;
- $f'([H]^e)$ 是个常数;
- $|H| \geq \min(H)$.

Theorem (Harrington and Paris)

$\forall e \forall r \forall k \exists M (M \longrightarrow (k)_r^e)$ 是独立于 PA 的.

一些具体的不可证明性举例 (II)

Theorem (Godel, Cohen)

CH是独立于ZFC的。

阅读材料

- ① 《数理逻辑》，杨跃，郝兆宽
- ② 《A Mathematical Introduction to Logic》，Enderton

习题

- ① 给出一个协调但是非 ω -协调的理论。
- ② 证明如果PA不能否定歌德巴赫猜想，那么 $(\omega, +, \cdot, <, 0, 1)$ 必然满足歌德巴赫猜想。
- ③ 证明对于一个递归的协调理论 T ，如果 $\{\#(\varphi) \mid T \vdash \varphi\}$ 是递归的，那么存在一个递归的协调的完备理论 $T' \supseteq T$ 。
- ④ 证明存在PA的非标准可数模型 $\mathcal{N}$ 使得 $\mathcal{N}$ 中存在一个可定义的非标准自然数。
- ⑤ 证明存在PA的非标准模型 $\mathcal{N}$ 使得 $\mathcal{N}$ 中所有可定义的元素都是标准的。
- ⑥ 证明一阶逻辑是不完备的。