可计算性理论

杨睿之

复旦大学哲学学院

2024 年春季

前情回顾

- s-m-n 定理和递归定理
- 带信息源的图灵机、图灵归约、图灵跃迁
- 递归可枚举集、多一归约

定理: A 是 c.e. 的，当且仅当 $A \leq_m 0'$

定理: $X \leq_T Y$，当且仅当 $X' \leq_m Y'$

前情回顾

- s-m-n 定理和递归定理
- 带信息源的图灵机、图灵归约、图灵跃迁
- 递归可枚举集、多一归约

定理: A 是 B 中 c.e. 的，当且仅当 $A \leq_m B'$

定理: $X \leq_T Y$，当且仅当 $X' \leq_m Y'$

使用函数

回忆: $\Phi_e^Y(x) = y \leftrightarrow \exists s\ \Phi_{e,s}^Y(x) = y$

使用原则（use principal）

在计算的有穷步内，$\Phi_{e,s}^Y(x)$ 的计算过程只会问信息源 Y 有穷多个问题

使用函数

定义 (使用函数)

- 假设 $\Phi_e^Y(x)\downarrow$。定义 $\Phi_e^Y(x)$ 的使用，记作 $\mathrm{use}\,\Phi_e^Y(x)$，为最小的 n 使得计算过程中询问信息源 Y 的问题都 $< n$
- 定义 $\mathrm{use}\,\Phi_{e,s}^Y(x)$ 为最小的 n 使得计算到 s 步时询问过信息源 Y 的问题都 $< n$。注意: 这里不要求 $\Phi_{e,s}^Y(x)\downarrow$

约定

如果 $\Phi_{e,s}^Y(x)\downarrow= y$，那么 $e, x, y, \mathrm{use}\,\Phi_e^Y(x) < s$

使用函数

定义 (使用函数)

对有穷 01 串 σ,

- 我们用 $\Phi_e^\sigma(x) = y$ 表示存在集合 Z 有 $Z \geq \sigma$,
  $\Phi_e^Z(x) \downarrow = y$ 且 use $\Phi_e^Z(x) \leq |\sigma|$
- 我们用 $\Phi_e^\sigma(x) \uparrow$ 表示不存在 y 使 $\Phi_e^\sigma(x) = y$
- $\Phi_{e,s}^\sigma(x) = y$ 、 $\Phi_{e,s}^\sigma(x) \uparrow$

真值表归约

定义 (真值表归约)

称全函数 $f:\mathbb{N}\to\mathbb{N}$ 真值表归可归约到 Y (truth-table reducible)，记作 $f\leq_{tt} Y$ ，当且仅当存在图灵函项 Φ_e 使得，$f=\Phi_e^Y$ 并且对任意集合 Z，Φ_e^Z 都是全函数。集合 $X\leq_{tt} Y$ ，当且仅当 X 的特征函数真值表归可归约到 Y

真值表归约

假设 D 是由有穷 01 串组成的有穷集合。令

$m(D) = \max\{|\sigma| \mid \sigma \in D\}$，考虑布尔函数 $B_D : 2^{m(D)} \to 2$:

$$B_D(\tau) = \begin{cases} 1, & \text{若 } \exists \sigma \in D\ \sigma \preceq \tau \\ 0, & \text{否则} \end{cases}$$

显然，布尔函数 B_D（从而集合 D）唯一地对应一个真值表

真值表归约

引理

集合 $X \leq_{tt} Y$，当且仅当存在可计算函数 g 使得，对任意 n，

$$n \in X \ \leftrightarrow\ \exists\sigma \in D_{g(n)}\ \sigma \prec Y$$

证明.

($\Leftarrow$) 考虑程序：输入 n，生成 $B_{D_{g(n)}}$ 对应的真值表，比对信息源的前段与真值表。符合则输出 1，否则输出 0

真值表归约

引理

集合 $X \leq_{tt} Y$，当且仅当存在可计算函数 g 使得，对任意 n，

$$n \in X \ \leftrightarrow\ \exists \sigma \in D_{g(n)}\ \sigma \prec Y$$

证明.

$(\Rightarrow)$ 令 Φ_e 见证 $X \leq_{tt} Y$。对每个 n，树 $T_n = \{\tau \mid \Phi_e^{\tau}(n)\uparrow\}$ 有穷。令 $g(n) = \ulcorner\{\sigma \mid \Phi_e^{\sigma}(n) = 1 \wedge \forall \tau \precneqq \sigma\ \tau \in T_n\}\urcorner$

真值表归约

定理

函数 $f \leq_{tt} A$，当且仅当存在图灵函项 Φ_e 以及可计算函数 t 使得，对任意 n，$\Phi^A_{e,t(n)}(n) \downarrow = f(n)$。

证明.

$(\Rightarrow)$ 考虑程序 P_e：对任意 n，类似上一个定理 $(\Rightarrow)$ 证明中，P_e 先计算一个有穷的树及其末端点对应的值，计算所需步数是确定的且可计算的，对比信息源的步数也是可计算的

真值表归约

定理

函数 $f \le_{tt} A$，当且仅当存在图灵函项 Φ_e 以及可计算函数 t 使得，对任意 n，$\Phi^A_{e,t(n)}(n)\downarrow = f(n)$。

证明.

$(\Leftarrow)$ 令 P_e 是见证右侧成立的程序。考虑程序 $P_{e'}$：在任何信息源 Z 和输入 n 下尝试计算 $\Phi^Z_e(n)$ 至 $t(n)$ 步。若 $\Phi^Z_{e,t(n)}(n)\downarrow$，输出 $\Phi^Z_{e,t(n)}(n)$，否则输出 0

弱真值表归约

定义 (弱真值表归约)

- 称函数 $f:\mathbb{N}\to\mathbb{N}$ 弱真值表可归约到 Y （weak truth table reducible），记作 $f\le_{wtt} Y$，如果存在图灵函项 Φ_e 以及可计算函数 $r:\mathbb{N}\to\mathbb{N}$ 使得，$f=\Phi_e^Y$ 且 $\forall n\,\mathrm{use}\,\Phi_e^Y(n)\le r(n)$。集合 $X\le_{wtt} Y$ ，当且仅当 X 的特征函数弱真值表可归约到 Y
- 弱真值表归约又称作有界图灵归约（bounded Turing reducibility），有的书上记作 $X\le_{bT} Y$

弱真值表归约

事实

$$X \leq_m Y \Rightarrow X \leq_{tt} Y \Rightarrow X \leq_{wtt} Y \Rightarrow X \leq_T Y$$

但每个反方向都不成立

定义 (联)

定义集合 A 和 B 的 **联** $A \oplus B = \{2n \mid n \in A\} \cup \{2n+1 \mid n \in B\}$

事实 (习题)

- $A, B \leq_m A \oplus B$
- 无论 $r = m, tt, wtt, T$，对任意集合 A, B, X

$$A, B \leq_r X \leftrightarrow A \oplus B \leq_r X$$

集合的算术层谱

Logic is about definability

(Gerald E. Sacks, 2003)

集合的算术层谱

定义

我们考虑一阶算术语言 $\mathcal{L}_A$ 及其结构 $\mathfrak{N} = (\mathbb{N}, 0, 1, \leq, +, \cdot, E)$

- 集合/关系 A 是 Σ^0_n 的，当且仅当存在只含有界量词的 $\mathcal{L}_A$ 公式 $\varphi(\bar{x}, y_1, \ldots, y_n)$，使得
  $A = \{\bar{x} \in \mathbb{N} \mid \mathfrak{N} \vDash \exists y_1 \forall y_2 \ldots Q y_n \varphi(\bar{x}, y_1, \ldots, y_n)\}$
- 集合 A 是 Π^0_n 的，当且仅当 $\mathbb{N} \setminus A$ 是 Σ^0_n 的
- 集合 A 是 Δ^0_n 的，当且仅当它即是 Σ^0_n 的也是 Π^0_n 的
- 集合 A 是算术的（arithmetical），当且仅当存在 n，A 是 Σ^0_n 的

集合的算术层谱

注意：

- 重复出现的同种量词可以合并：

$$\exists x_1 \exists x_2 \varphi(x_1, x_2, y) \leftrightarrow \exists p \varphi((p)_1, (p)_2, y)$$

- 有界量词可以被“向后移”

$$\forall x < k \exists y \varphi(x, y, z) \leftrightarrow \exists \sigma \ (|\sigma| = k \wedge \forall x < k \ (\varphi(x, \sigma(x), z)))$$

集合的算术层谱

定义

上述定义可以被相对化。考虑带参数（一个新的一元谓词符号 C）的一阶算术语言 $\mathcal{L}_A(C)$ 及其结构 $(\mathbb{N}, 0, 1, \leq, +, \cdot, C)$

- 集合 A 是 $\Sigma_n^0(C)$ 的，当且仅当存在只含有界量词的 $\mathcal{L}_A(C)$ 公式 $\varphi^C(x, y_1, \ldots, y_n)$，使得
  $A = \{x \in \mathbb{N} \mid \exists y_1 \forall y_2 \ldots Q y_n \varphi^C(x, y_1, \ldots, y_n)\}$
- $\Pi_n^0(C)$、$\Delta_n^0(C)$ 定义类似

集合的算术层谱

事实

- $\Sigma^0_0 = \Pi^0_0 = \Delta^0_0$ 中的（也即只用有界量词定义的）集合都是可计算的
- 通用图灵机是 Σ^0_1 的，即 $\{(e,x,y) \mid \Xi(e,x) = \Phi_e(x) = y\}$

$$= \{(e,x,y) \mid \exists z\ (T(e,x,z) \wedge y = U(z))\}$$

其中 T 是 Kleene's T predicate

集合的算术层谱

事实

- 集合 A 是 Σ_1^0 的，当且仅当 A 是 c.e. 的
- 集合 A 是 Δ_1^0 的，当且仅当 A 是可计算的

定理

对 $n \geq 1$,

(1) A 是 Σ_n^0 的，当且仅当 A 是 $0^{(n-1)}$ 中 c.e. 的

(2) $0^{(n)}$ 是 Σ_n^0-完全的，即对任意 $A \in \Sigma_n^0$ 有 $A \leq_m 0^{(n)}$

证明.

对 $n \geq 1$ 归纳证明

Sheonfield 极限引理

引理 (Sheonfield 极限引理)

下列命题等价

(1) A 是 Δ^0_2 的

(2) $A \leq_T 0'$

(3) 存在可计算的强编码序列 $(A_s)_{s\in\mathbb{N}}$ 使得，每个 $A_s \subset s$，并且对每个 x，$\lim_s A_s(x) \downarrow= A(x)$

此时，我们称 $(A_s)_{s\in\mathbb{N}}$ 是 A 的一个可计算逼近

Sheonfield 极限引理

约定

$\langle Z_s\rangle_{s<\omega}$ 是一个可计算枚举 / 逼近（不妨设 $|Z_s\triangle Z_{s+1}|\leq 1$），我们写 $\Phi_{e,s}^{Z_s}(x)\downarrow$ 的时候，假设 use $\Phi_{e,s}^{Z_s}(x)\leq n_t+1$，其中 $t<s$ 是最大的使得 $Z_{t+1}\neq Z_t$，且 $Z_{t+1}\triangle Z_t=\{n_t\}$。

记法

如果 A 的特征函数是 $\Phi_e^{0'}$，我们称 e 是 A 的一个 Δ_2^0 编码

事实

$\{e \mid A$ 的特征函数是 $\Phi_e^{0'}\}$ 是不可计算的（习题）

n-c.e. 和 ω-c.e.

定义

- 我们称集合 A 是 ω-c.e. 的，当且仅当存在 A 的可计算的逼近 $(A_s)_{s\in\mathbb{N}}$ 以及可计算的函数 $b:\mathbb{N}\to\mathbb{N}$ 使得，对任意 x 有

$$b(x) \geq |\{s \mid A_s(x) \neq A_{s+1}\}|$$

- 不妨设对每个 x，$A_{x+1}(x) = 0$。如果可以找到常值函数 $b(x) = n$（$n \geq 1$）满足上述条件，则称 A 是 n-c.e. 的

n-c.e. 和 ω-c.e.

事实

- A 是 1-c.e. 的，当且仅当 A 是 c.e. 的
- A 是 2-c.e. 的，当且仅当存在 c.e. 集合 B 和 D 使得 $A = B \setminus D$。因此，2-c.e. 集合又被称作 d.c.e. 的 (difference of c.e. sets)
- 如果 A 是 ω-c.e. 的，那么 A 是 Δ^0_2 的。因此，我们有

$$\text{可计算} \subset \text{c.e.} \subset \text{d.c.e} \subset \text{3-c.e.} \subset \cdots \subset \omega\text{-c.e.} \subset \Delta^0_2$$

定理

下列命题等价

(1) A 是 ω-c.e. 的

(2) $A \leq_{wtt} 0'$

(3) $A \leq_{tt} 0'$

习题

- 1.2.23, 1.2.25
- 1.4.7 - 1.4.9
- 利用 1.2.25 证明：存在 $g:\mathbb{N}\to\mathbb{N}$，$g\leq_{wtt} 0'$，但 $g\not\leq_{tt} 0'$
- 1.4.19 - 1.4.22（其中 1.4.20 (iv)*），1.4.24, 1.4.25

下期预告

- 低效（low）与高效（high）
- Post 问题