可计算性理论

杨睿之

复旦大学哲学学院

2021 年春季

前情回顾

- 柯尔莫哥洛夫复杂度 $C(\tau) = C_U(\tau)$
- $C(\tau)$ 可以被“自上而下”可计算地逼近
- 对部分可计算函数 h，$C(h(\tau)) \leq C(\tau) + c$

前情回顾

- 对任意合理的 c.e. 请求集 W，都有程序满足之
- 对任意 n 总有长度为 n 的 τ 有 $C(\tau) \geq n$
- 对任意 $n \geq d$，至少存在 $2^n - 2^{n-s} + 1$ 个长度为 n 的 d-C-随机 01 串
- $C(\sigma\tau) \leq C(\sigma) + C(\tau) + c$ 未必成立

相对柯尔莫哥洛夫复杂度

定理

对任意 $d \in \mathbb{N}$，存在足够长的字符串 μ，使得 $C(\mu) \geq |\mu|$，并且对所有这样的 μ，存在 $\sigma \prec \mu$，使得 $\mu = \sigma\tau$，且

$$C(\mu) > C(\sigma) + C(\tau) + d$$

故 $C(\sigma\tau) \leq C(\sigma) + C(\tau) + c$ 未必成立

相对柯尔莫哥洛夫复杂度

事实

存在常量 c 使得，对所有 $\sigma, \tau \in 2^{<\omega}$ 有

$$C(\sigma\tau) \leq C(\sigma, \tau) + c$$

因而，不存在 c 使得 $C(\sigma, \tau) \leq C(\sigma) + C(\tau) + c$ 总成立。

相对柯尔莫哥洛夫复杂度

事实

存在常量 c，使得对所有 $\sigma, \tau \in 2^{<\omega}$ 有

$$C(\sigma, \tau) \leq C(\sigma) + C(\tau) + 2\log C(\sigma) + c$$

因而，也有 c 使得

$$C(\sigma\tau) \leq C(\sigma) + C(\tau) + 2\log C(\sigma) + c$$

总成立

相对柯尔莫哥洛夫复杂度

定义

对字符串 σ，τ，定义 σ 相对于 τ 的柯尔莫哥洛夫复杂度

$$C(\sigma|\tau) = \min\{|\mu| : U^{\bar{\tau}}(\mu) = \sigma\}$$

其中 $U^{\bar{\tau}}$ 表示把有穷字符串 $\bar{\tau}$ 作为信息源的通用程序。

相对柯尔莫哥洛夫复杂度

之所以用 $\bar{\tau}$ 而不是直接用 τ 作为信息源，是因为 $\bar{\tau}$ 可以告诉我们在一条无穷长的纸带上有效的信息源在哪里结束。

例

我们希望 $C(\sigma|\sigma)$ 是一个常量，但

$$\min\{|\mu| : U^{\sigma}(\mu) = \sigma\}$$

会随着 σ 的增长而增长

C 的递归论性质

事实

- 对任意解压缩程序 M，$C_M \leq_{wtt} 0'$
- $B = \{\sigma \in 2^{<\omega} \mid C(\sigma) < |\sigma|\}$ 是单集并且是 wtt-完全的 $(0' \leq_{wtt} B)$
- C 不是可计算的

无前束柯尔莫哥洛夫复杂度

定义

我们称集合 $A \subset 2^{<\omega}$ 是 无前束的 ，当且仅当 A 中的任何字符串都不是 A 中其他字符串的前段，即：对任意 σ，$\tau \in A$，若 $\sigma \neq \tau$，则 $\sigma|\tau$。

无前束柯尔莫哥洛夫复杂度

例

- $2^n = \{\sigma \in 2^{<\omega} \mid |\sigma| = n\}$
- $\{0, 10, 110, 1110, \dots\}$
- $\{\bar{\tau} \mid \tau \in 2^{<\omega}\}$

无前束柯尔莫哥洛夫复杂度

定义

我们称一个程序 / 图灵机 / 部分函数 M 是 无前束的，当且仅当它的定义域 $\{\sigma \mid M(\sigma)\downarrow\}$ 是无前束的字符串集合。

例

- 不存在无前束程序 M，使得对每个 $\tau \in 2^{<\omega}$ 有 $M(\tau) = |\tau|$
- 存在无前束程序 M，使得对任意字符串 τ 都有 $M(\bar{\tau}) = |\tau|$。

无前束柯尔莫哥洛夫复杂度

定理

存在对所有无前束程序的能行枚举 $\{\Psi_e\}_{e\in\mathbb{N}}$，因而存在通用无前束程序 U^{pf}，使得

$$U^{\mathrm{pf}}(\underbrace{1\cdots1}_{e\text{个}}0\sigma)=\Psi_e(\sigma)$$

无前束柯尔莫哥洛夫复杂度

定义

对任意字符串 σ，定义 σ 的 无前束柯尔莫哥洛夫复杂度 为

$$K(\sigma) = K_{U^{\mathsf{pf}}}(\sigma) = C_{U^{\mathsf{pf}}}(\sigma)$$

类似地，我们也可以定义 τ 相对于 σ 的无前束柯尔莫哥洛夫复杂度 为

$$K(\tau|\sigma) = \min\{|\mu| \,\big|\, (U^{\mathsf{pf}})^{\bar{\sigma}}(\mu) = \tau\}$$

无前束柯尔莫哥洛夫复杂度

记法

- 当 M 是无前束程序时，我们往往使用 $K_M(\sigma)$ 代替 $C_M(\sigma)$，以强调该解压缩程序是无前束的。
- 对每个字符串 σ，我们定义 σ^* 为它最小的无前束描述。即：最左边的 τ 满足

$$U^{\mathrm{pf}}(\tau) = \sigma \text{ 且 } |\tau| = K(\sigma)$$

无前束柯尔莫哥洛夫复杂度

无前束柯尔莫哥洛夫复杂度 K 修复了 C 的问题

事实

存在常量 c，对任意 $\tau_1, \tau_2 \in 2^{<\omega}$

$$K(\tau_1, \tau_2) \leq K(\tau_1) + K(\tau_2) + c$$

无前束柯尔莫哥洛夫复杂度

显然，对任何字符串 σ，$C(\sigma) \leq K(\sigma)$。虽然 K 函数对 01 串复杂度的估值比 C 函数更大，但仍然符合直观

事实

如果 $h : 2^{<\omega} \to 2^{<\omega}$，那么，存在常量 c 对任意字符串 σ，有 $K(h(\sigma)) \leq K(\sigma) + c$。

无前束柯尔莫哥洛夫复杂度

K 函数的上界也并不很远

事实

存在常量 c，对任意字符串 σ，有

$$K(\sigma) \leq 2|\sigma| + c$$

无前束柯尔莫哥洛夫复杂度

类似柯尔莫哥洛夫复杂度，我们可以利用这个上界来定义对无前束柯尔莫哥洛夫复杂度“自上而下”的能行逼近。

$$K_s(\sigma) = \min\left(\{|\tau| \mid U_s^{\mathrm{pf}}(\tau) \downarrow = \sigma\} \cup \{2|\sigma| + c\}\right)$$

注意：$\langle s, \sigma\rangle \mapsto K_s(\sigma)$ 是可计算的，$K(\sigma) \leq K_{s+1}(\sigma) \leq K_s(\sigma)$，并且 $K(\sigma) = \lim_{s\to\infty} K_s(\sigma)$

无前束柯尔莫哥洛夫复杂度

我们尝试给出一个 K 函数更“紧”的上界

事实

存在常量 $c_1, c_2 \in \mathbb{N}$，对任意字符串 σ，都有

$$K(\sigma) \leq K(|\sigma|) + |\sigma| + c_1 \leq 2\log|\sigma| + |\sigma| + c_2。$$

无前束柯尔莫哥洛夫复杂度

下面的“数数”事实表明，上述上界已经足够“紧”了

事实

对任意自然数 d 存在字符串 σ，它的无前束柯尔莫哥洛夫复杂度

$$K(\sigma) > |\sigma| + \log|\sigma| + d$$

无前束柯尔莫哥洛夫复杂度

记法 (柴廷数（Chaitin's constant）)

$$\Omega = \lambda([\mathrm{dom}\, U^{\mathsf{pf}}]^{\prec})$$

习题

- 存在常量 c_1，c_2，使得对任意字符串 σ，有

  $C(\sigma_C^*|\sigma) \leq C(C(\sigma)|\sigma) + c_1$，而

  $C(C(\sigma)|\sigma) \leq C(\sigma_C^*|\sigma) + c_2$。

- 2.2.10

下期预告

- 无前束程序存在定理
- 1-随机