10. The incompressibility approach to randomness

2016年11月3日 14:11

Recall: $K(\sigma) = K_U(\sigma)$ is the length of shortest U-description of σ, where U is an universal prefix-free machine

we have shown: $\forall \sigma$, $K(\sigma) \le |\sigma| + K(|\sigma|) + O(1)$

or $K(\sigma) \le |\sigma| + 2\log|\sigma| + O(1)$ $(\ast)$

or even $K(\sigma) \le |\sigma| + \log|\sigma| + \log\log|\sigma| + \cdots + 2\log|\overbrace{\log\cdots\log}^{n}|\sigma|| + O(1)$ for any $n \ge 1$

We can use prefix-free machine existence theorem to show $(\ast)$:

Consider the computable sequence: $\{(d_\tau, \tau) \mid \tau \in 2^{<\omega}\}$

where $d_\varnothing = 1$, and $d_\tau = |\tau| + 2\log|\tau| + 2$ for $|\tau| > 0$

Then $\sum_{\tau \in 2^{<\omega}} 2^{-d_\tau} = \frac{1}{2} + \sum_{n \ge 1} 2^n \cdot \frac{1}{2^{(n + 2\log n + 2)}} = \frac{1}{2} + \sum_{n \ge 1} \frac{1}{n^2} \cdot \frac{1}{4}$

$= \frac{1}{2} + \frac{\pi^2}{6} \cdot \frac{1}{4} \le 1$

$\left[\sum_{n \ge 1} \frac{1}{n^2} = \frac{\pi^2}{6} \right]$

So there is a prefix-free machine M satisfies the request,

i.e. For each τ, $K(\tau) \le K_M(\tau) + C_M = d_\tau + C_M = |\tau| + 2\log|\tau| + 2 + C_M$

On the other hand

Proposition For any d, there are σ with $K(\sigma) > |\sigma| + \log|\sigma| + d$

Proof Assume to contradiction that there is d s.t. for each σ,

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

Then $\sum_{\sigma \in 2^{<\omega}} 2^{-K(\sigma)} \ge \sum_{\sigma} 2^{-(|\sigma| + \log|\sigma| + d)} = \sum_{n \ge 1} 2^n \cdot 2^{-n} \cdot 2^{-\log n} \cdot 2^{-d}$

$= \sum_{n \ge 1} 2^{-\log n - d}$

$= 2^{-d} \cdot \sum_{n \ge 1} \frac{1}{n} = \infty$

But we know $\sum_{\sigma} 2^{-K(\sigma)} \le 1$ 矛盾 $\square$

Def $\sigma \in 2^{<\omega}$ is (weakly) K-random for $d \in \mathbb{N}$ if $K(\sigma) \ge |\sigma| - d$

Note if σ is C-random for d $(C(\sigma) \ge |\sigma| - d)$, then σ is K-random for d

the inverse does not hold!

Def (1-randomness)

A sequence $A \in 2^\omega$ is 1-random if there is $d \in \mathbb{N}$ s.t.

$K(A \upharpoonright n) \ge n - d$ for all $n \in \mathbb{N}$

i.e. every finite initial segment of A is K-random for d

Note By the theorem we prove last time, if we define randomness as

$C(A \upharpoonright n) \ge n - d$ for all n,

Then no sequence is random. Since for each sequence $A \in 2^\omega$, we can always find $\sigma \prec A$ s.t. $C(\sigma) < |\sigma| - d$.

Recall $\Omega = \mu(\llbracket \operatorname{dom} U \rrbracket) = \sum_{\sigma \in \operatorname{dom} U} 2^{-|\sigma|}$ (most of the properties we concern are independent from the choice of universal machine)

Note Ω in binary representation looks like $0.1001101001\cdots$

Let $\Omega_s = \mu\llbracket\{\sigma \mid U_s(\sigma)\downarrow\}\rrbracket$, then $\langle \Omega_s : s \in \mathbb{N} \rangle$ is an approximation to Ω from left

Def For $\sigma \in 2^{<\omega}$, Let $\tilde{\sigma} = \sigma^\frown 000\cdots$

For $\sigma \in 2^{<\omega}, \tau \in 2^{\le\omega}$, we say $\sigma <_L \tau$ if there is $n \in \mathbb{N}$ s.t.

$\tilde{\sigma} \upharpoonright n = \tilde{\tau} \upharpoonright n$ and $\tilde{\sigma}(n) = 0$, $\tilde{\tau}(n) = 1$

/ or equivalent: $\sigma <_L \tau$ iff there is $n \in \mathbb{N}$ s.t.

$\sigma \upharpoonright n = \tau \upharpoonright n$ and (1) $\sigma(n) = 0$, $\tau(n) = 1$

or (2) $|\sigma| = n$, $\tau(m) = 1$ for some $m \ge n$

Exe $<_L$ is transitive

For $A \in 2^\omega$, define $L(A) = \{\sigma \in 2^{<\omega} \mid \sigma <_L A\}$

Proposition $L(\Omega)$ is c.e.

Proof claim $\Omega_s <_L \Omega$

Note: $\Omega_0 \le_L \Omega_1 \le_L \cdots \le_L \Omega_s \le_L \cdots$ has no $<_L$ maximum element

To enumerate $L(\Omega)$. For $s \in \mathbb{N}$, Let

$L_s(\Omega) = \{\delta \mid \delta <_L \Omega_s, |\delta| \le s\}$, then $\{L_s(\Omega) \mid s \in \mathbb{N}\}$ is computable $\Box$

Def We say A is left.c.e (i.e. $0.A$ is a left c.e. real) iff $L(A)$ is c.e.

Proposition TFAE.

(1) A is left c.e.

(2) there is a computable sequence $\delta_0 <_L \delta_1 <_L \cdots$ s.t.

$\lim_n \delta_n = A$

(i.e. for each m, there is δ_n s.t. $\delta_n \upharpoonright m = A \upharpoonright m$)

Proof (2) $\Rightarrow$ (1) obvious

(1) $\Rightarrow$ (2) Fix $\delta_0 \in L(A)$. Given δ_n, we enumerate $L(A)$ until some $\delta \in (L(A))_s$

s. $\delta_n <_L \delta$. such δ always exists. since $L(A)$ has no $<_L$ greatest element

[Assume $\delta \in L(A)$ is greatest, Let n be s.t. $\delta \upharpoonright n = A \upharpoonright n$ and $\delta(n) = 0$, $A(n) = 1$

take $\delta' = \delta \upharpoonright n ^\frown 01$] $\Box$

Fure If A is c.e. then A is left c.e.

But There is a left c.e. set, which is not c.e.

Let $A_0 = 010101 \cdots$

~~If~~ Assume A_s is defined. Assume $\Phi_{e,s}(2e+1)\downarrow$ for the first time

Then A_s: —— $\underset{2e\ 2e+1}{01}$ ——

Let A_{s+1}: —— 10 ——

Let A be the limit

Exe A is left c.e. A is not c.e.

Proposition If A is left c.e. then $A \le_T \emptyset'$

Proof To determined whether $n \in A$ we ask $\emptyset'$ whether $\delta \in L(A)$

for all $|\delta| = n+2$, there must be $\delta_1 = \tau^\frown 0 \in L(A)$

$\delta_2 = \tau^\frown 1 \notin L(A)$ for some τ s.t. $|\tau| = n+1$

Then $A(n) = \tau(n)$ $\Box$

Proposition $\Omega \equiv_T \emptyset'$

Proof $\Omega \le_T \emptyset'$, since Ω is left-c.e.

To show $\emptyset' \le_T \Omega$ $\overbrace{0\cdots0}^{e}1$

Let M be the machine: $M(0^e1)\downarrow = \langle\rangle$ once $\Phi_e(e)\downarrow$

so $\mathrm{dom}\, M = \{0^e1 \mid e \in \emptyset'\}$

Let ρ be the coding string of M, so $U(\rho 0^e 1) \simeq M(0^e 1)$

To decide whether $e \in \emptyset'$, we only need to know whether $U(\rho 0^e 1)\downarrow$

To decide whether $U(\rho 0^e 1)\downarrow$, wait until the step s. s.t. $\Omega - \Omega_s < 2^{-(|\rho|+e+1)}$

If $U_s(\rho 0^e 1)\downarrow$, then $e \in \emptyset'$; o.w. $U(\rho 0^e 1)$ will never converge, and so $e \notin \emptyset'$ $\square$

We show Ω is 1-random

Theorem Ω is 1-random

Proof We want to find a constant c and show that $K(\Omega \upharpoonright n) \geq n - c$ for all n.

that is for every τ s.t. $|\tau| < n-c$, $U(\tau) \neq \Omega \upharpoonright n$

To do so, every time $U_s(\tau)\downarrow = \Omega_s \upharpoonright n$, for some short τ, we ensure that $\Omega_s \upharpoonright n \neq \Omega \upharpoonright n$

Consider the prefix-free machine $M(\tau, d)$: input τ, d, it wait until some stage s s.t.

$U_s(\tau) = \Omega_s \upharpoonright n$ for some n s.t. $|\tau| < n - d$, then it choose a least $\mu \notin \operatorname{ran} U_s$

output μ

By parameter lemma, we have $M_{f(d)}(\tau)$ to do this. let c be a fix point of f

Then $M_c(\tau) \simeq M_{f(c)}(\tau) \simeq M(\tau, c)$ (the index of $M_c = c_{M_c} = c$)

Then $M_c(\tau) = \mu$, means $U_s(\tau) = \Omega_s \upharpoonright n$ for some n and $|\tau| < n-c$

(so $K(\Omega_s \upharpoonright n) < n - c$)

Also there is $\nu = \rho\tau$ s.t. $U(\nu) = \mu$, Note $|\nu| \leq |\tau| + c < n$

since $\mu \notin \operatorname{ran} U_s$, $\nu \notin \operatorname{dom} U_s$ so $\Omega - \Omega_s \geq 2^{-|\nu|} > 2^{-n}$

so $\Omega \upharpoonright n \neq \Omega_s \upharpoonright n = U_s(\tau)$ for any τ s.t. $|\tau| < n-c$

[Since if $U(\tau) = \Omega \upharpoonright n$ for some n s.t. $|\tau| < n-c$, then there is $s \in \mathbb{N}$, $U_s(\tau) = \Omega_s \upharpoonright n$

and so $M_c(\tau) = \mu$, and so $\Omega_s \upharpoonright n \neq \Omega \upharpoonright n$ 矛盾] $\square$