第三讲：算法随机性导论

喻良

南京大学数学学院

July 23, 2025

Kraft-Chaitin Theorem (I)

A set $A \subseteq 2^{<\omega}$ is prefix-free if any two different strings in A are incompatible.

Lemma

If A is prefix-free, then $\sum_{\sigma \in A} 2^{-|\sigma|} \leq 1$.

Proof.

We may assume that A is finite. Then there is some n so that $A \subseteq 2^{\leq n}$. Let $B = \{\tau \in 2^n \mid \exists \sigma \in A(\sigma \preceq \tau)\}$. Then since A is prefix-free, we have

$$\sum_{\sigma \in A} 2^{-|\sigma|} \leq \sum_{\sigma \in B} 2^{-|\sigma|} \leq \sum_{\tau \in 2^n} 2^{-|\tau|} \leq 1.$$

□

Kraft-Chaitin Theorem (II)

Theorem

For any infinite r.e. set $A \subset \omega$, $\sum_{n \in A} 2^{-n} \leq 1$ if and only if there is a a recursive prefix-free sequence $\{\sigma_i\}_{i \in \omega}$ so that $A = \{|\sigma_i| \mid i \in \omega\}$.

Proof.

By the lemma, the direction from right to left is immediate.
For the direction from right to left. Assigning finite strings to A economically....

□

Kolmogorov complexity (I)

1. Fix a Turing machine M, for each finite string $\sigma \in 2^{<\omega}$, define $C_M(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$.

Kolmogorov complexity (I)

1. Fix a Turing machine M, for each finite string $\sigma \in 2^{<\omega}$, define $C_M(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$.
2. Fix a prefix free Turing machine M, for each finite string $\sigma \in 2^{<\omega}$, define $K_M(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$.

.

Kolmogorov complexity (II)

Theorem

- *There is a Turing machine U so that for any machine M, there is some c_M so that* $\forall n C_U(n) \leq C_M(n) + c_M$.
- *There is a prefix-free Turing machine U so that for any prefix-free machine M, there is some c_M so that* $\forall n K_U(n) \leq K_M(n) + c_M$.

Proof.

Both machines are built by a standard coding. □

Basic properties of Kolmogorov complexity (I)

Theorem

1. $\exists c \forall \sigma C(\sigma) \leq |\sigma| + c.$
2. $\exists c \forall \sigma K(\sigma) \leq |\sigma| + 2\log|\sigma| + c$
3. $\exists c \forall \sigma K(\sigma) \leq |\sigma| + K(|\sigma|) + c.$
4. $\exists c \forall \sigma \forall \tau K(\sigma^\frown \tau) \leq K(\sigma) + K(\tau) + c.$

Proof.

(1) is clear.
(2). Let $(|\sigma| + \log|\sigma|, \sigma) \in V$. Then $\sum_{m \in Dom(V)} 2^{-m} \leq \sum_{\sigma} 2^{-|\sigma| - \log|\sigma|} = \sum_n \sum_{|\sigma|=n} 2^{-n-2\log n} \leq \sum_n 2^{-2\log n} \leq \sum_n \frac{1}{n^2}$. By KC-theorem, V can be viewed as a prefix-machine. Then $K_V(\sigma) \leq |\sigma| + 2\log|\sigma| + d$ for a constant d. □

Basic properties of Kolmogorov complexity (II)

Proof.

(3). Let U be a universal prefix-free machine. Let $(|\sigma| + |\tau|, \sigma) \in V$ if $U(\tau) = |\sigma|$. Then

$$\sum_{m \in Dom(V)} 2^{-m} \leq \sum_{\sigma} 2^{-|\sigma|} \Big(\sum_{U(\tau)=|\sigma|} 2^{-|\tau|} \Big) = \sum_{n} 2^{-n} \Big(\sum_{|\sigma|=n} \sum_{U(\tau)=n} 2^{-|\tau|} \Big)$$

$$\leq \sum_{n} 2^{-n} 2^{n} \sum_{U(\tau)=n} 2^{-|\tau|} \leq 1.$$

(4) Let $(\nu_0^\frown \nu_1, \sigma^\frown \tau) \in M$ if (ν_0, σ) and $(\nu_1, \tau) \in U$. M is prefix-free since $\sum_{\nu_0 \in Dom(U)} \sum_{\nu_1 \in Dom(U)} 2^{-|\nu_0|-|\nu_1|} \leq \sum_{\nu_0 \in Dom(U)} 2^{-|\nu_0|} \leq 1$. □

Counting theorem for C

Theorem

1. $\exists c \forall n \forall d (|\{\sigma \mid C(\sigma) < n - d\}| \leq 2^{n-d} - 1)$.
2. $\exists c \forall n \forall d |\{\sigma \mid |\sigma| = n \wedge C(\sigma) \leq C(n) + d\}| \leq d^2 \cdot 2^{c+d}$.

Proof.

(1) is clear.
(2). Suppose not. For any c and m, by (1), there are at most $\frac{2^{m+d+1}}{d^2 \cdot 2^{c+d}} = 2^{m-2\log d - c+1}$ many $n's$ so that $|\{\sigma \mid |\sigma| = n \wedge C(\sigma) \leq C(n) + d\}| > d^2 \cdot 2^{c+d}$ with $C(n) = m$. We use recursion theorem to define a machine M so that $e_M < c$ and $M(0^{|d|}1\rho) = n$ where $|\rho| \leq m - c - 2\log d$. □

Coding lemma

Theorem

If M is a prefix-free machine, then $\exists c \forall n 2^{-K(n)+c} \geq \sum_{M(\sigma)=n} 2^{-|\sigma|}$.

Proof.

Put $(l, n) \in V$ if $l = \left\lceil -\log \sum_{M(\sigma)=n} 2^{-|\sigma|} \right\rceil + 1$. By KC-theorem, there is some constant c so that $\forall n K(n) \leq c + K_V(n)$.

□

Counting theorem for K

Theorem

$\exists c \forall n \forall d |\{\sigma \mid |\sigma| = n \wedge K(\sigma) \leq n + K(n) - d\}| \leq 2^{n-d+c}$.

Proof.

Let U be a universal prefix-free machine. Then by the coding lemma, there is some c so that for every n, $2^{-K(n)+c} \geq \sum_{|\sigma|=n \wedge K_U(\sigma) \leq n+K_U(n)-d} 2^{-n-K(n)+d} \geq |\{\sigma \mid |\sigma| = n \wedge K(\sigma) \leq n + K(n) - d\}| \cdot 2^{-n-K(n)+d}$. □

Martin-Löf test

Definition (Martin-Löf)

(i) A Σ^0_1 Martin-Löf test is a computable collection $\{V_n : n \in \mathbb{N}\}$ of c.e. sets such that $\mu(V_n) \leq 2^{-n}$.

(ii) A real y is said to pass the Σ^0_1 Martin-Löf test if $y \notin \bigcap_{n\in\omega} V_n$.

(iii) A real y is said to be Martin-Löf-random if it passes all Σ^0_1 Martin-Löf tests.

Universal Martin-Löf test

Theorem

There is a Martin-Löf test covering all the Martin-Löf tests.

Proof.

For any e, let $\sigma \in U_e$ if there is some $i > e$ so that there is some stage s for which $M_i(\sigma)$ converges at stage s and $\sum_{\{\tau \mid M(\tau)\downarrow \text{at stage s}\}} 2^{-|\tau|} \leq 2^{-i}$.
Then $\{U_e\}_{e\in\omega}$ is as required. □

Corollary

There is a nonempty Π^0_1 set which only contains Martin-Löf random reals.

Betting strategy

Definition

1. A martingale is a function $f\colon 2^{<\omega} \mapsto \mathbb{R}^+$ such that for all $\sigma \in 2^{<\omega}$, $f(\sigma) = \frac{f(\sigma^\frown 0)+f(\sigma^\frown 1)}{2}$.
2. A martingale f is said to succeed on a real y if $\limsup_n f(y \upharpoonright n) = \infty$.

f is super-martingale if $f(\sigma) \geq \frac{f(\sigma^\frown 0)+f(\sigma^\frown 1)}{2}$.

Counting theorem for supermartingales

Note that if f is a supermartingale, then $\lambda(\sigma) = 2^{-|\sigma|} f(\sigma)$ defines a semi-measure over 2^ω.

Theorem

If f is a supermartingale with $f(\emptyset) < a$, then $\mu(\{x \mid \exists n f(x \upharpoonright n) > a\}) \leq \frac{f(\emptyset)}{a}$.

Proof.

It is sufficient to prove that for any finite prefix-free set A with $\forall \sigma \in A f(\sigma) > a$, $\sum_{\sigma \in A} 2^{-|\sigma|} \leq \frac{f(\emptyset)}{a}$.
Note that $\sum_{\sigma \in A} 2^{-|\sigma|} \leq \sum_{\sigma \in A} 2^{-|\sigma|} \frac{f(\sigma)}{a} \leq \frac{f(\emptyset)}{a}$. □

Left-r.e. supermartingales

Definition

A supermartingale f is left-r.e. if the set $\{(\sigma, q) \mid q \in \mathbb{Q} \wedge q < f(\sigma)\}$ is r.e.

Schnorr's theorem (I)

Theorem (Schnorr)

For any real x,

1. *x doesn't belong to any effective Matin-Löf test;*
2. $\exists c \forall n K(x \upharpoonright n) \geq n - c$;
3. *No left-r.e. supermartingale can win on x.*

Proof.

(1) implies (2): By the counting theorem for the Kolmogorov complexity, the sequence $V_d = \{x \mid \exists n K(x \upharpoonright n) < n - d\}$ is a Martin-Löf test with $\mu(V_d) < \sum_n 2^{-K(n)-d+c} < 2^{-d+c}$.
(2) implies (1): Suppose that x is covered by a Martin-Löf test $\{V_n\}_{n\in\omega}$. So $\sum_n \sum_{\sigma \in V_{2n}} 2^{-|\sigma|+n} \leq \sum_n 2^{-n} \leq 1$. We may assume that V_n is a prefix-free set for every n. Then by KC-theorem. □

Schnorr's theorem (II)

Proof.

(1) implies (3): By the counting theorem for supermartingales.
(3) implies (2): Note that $f(\sigma) = 2^{|\sigma|} \sum_{\tau \succeq \sigma} 2^{-K(\tau)}$ is a left-r.e. supermartingale.

□

Why not C?

Theorem

For any real x, $\overline{\lim}_n n - C(x \upharpoonright n) = +\infty$.

Proof.

Given any m, let $n = m + x \upharpoonright m$. Then
$C(x \upharpoonright n) \leq C(x \upharpoonright [m, n]) \leq n - m + c$ for some constant c.
So $n - C(x \upharpoonright n) \geq m - c$. □

Left-r.e. reals

Definition

A real x is left-r.e. if there is a recursive non-decreasing sequence of rationals $\{q_s\}_{s\in\omega}$ so that $\lim_s q_s = x$.

Since there is a non-empty Π^0_1-set only containing Martin-Löf random reals, there is a left-r.e. random real.

Chaitin's Ω

Let U be a universal prefix-free Turing machine, define

$$\Omega_U = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|}.$$

Theorem (Chaitin)

Ω_U is a random real.

Proof.

At any stage s, if a new τ so that $U(\tau) = \Omega_s \upharpoonright n$ at stage s, we let $M(\tau)$ be any finite string not in range of U before the stage $s+1$. If Ω_U is not random, then there is some τ so that $|\tau| < n - e_M - 1$ and so $M(\tau)$ would output a finite string σ with $K_U(\sigma) \geq n$ but $K_M(\sigma) \leq n - e_M - 1$. □

The Turing degree of Ω.

Theorem

$\Omega \equiv_T \emptyset'$.

Proof.

First note that for any r.e. A, $K(A \upharpoonright n) \leq 4\log n + c$ for some constant c.
Then the module function of Ω must dominate the module function of $\emptyset'$. □

Ample excess lemma

Theorem (Miller, Yu)

x is 1-random iff $\sum_n 2^{n-K(x\upharpoonright n)} < \infty$.

Proof.

$\sum_{|\sigma|=m}\sum_{n\leq m} 2^{n-K(\sigma\upharpoonright n)} = \sum_{n\leq m} 2^{m-n}\sum_{|\tau|=n} 2^{n-K(\tau)} = \sum_{|\tau|\leq m} 2^{m-K(\tau)} < 2^m$. So for any c, $\mu(\{x \mid \sum_n 2^{n-K(x\upharpoonright n)} > c\}) < c^{-1}$. So $V_c = \{x \mid \sum_n 2^{n-K(x\upharpoonright n)} > c\}$ is a Martin-Löf test. □

Random reals in Π^0_1-set.

Theorem (Kucera)

Suppose P is a Π^0_1 set having positive measure, then for every random real r, there is some random real $x \equiv_T r$ with $x \in P$.

Proof.

Suppose that $\mu(P) > p$ for some rational $p \in (0, 1]$. Then $U_0 = 2^\omega \setminus P$ can be viewed as a prefix-free r.e. set. For any n, let $U_{n+1} = \{\sigma^\frown\tau \mid \sigma \in U_n \wedge \tau \in U_0\}$. Then $\mu(U_{n+1}) \leq \sum_{\sigma \in U_n} 2^{-|\sigma|}\mu(U_0) \leq (1-p)^{n+1}$. So $\{U_n\}_{n+1}$ is a Martin-Löf test. If r is random, then there is some n so that $r \notin U_n$. Then there must be some m so that $r \upharpoonright m \in U_{n-1}$ but $r \upharpoonright (m, \infty) \in P$. □

C-triviality

Theorem (Chaitin)

If $\exists c \forall n C(x \upharpoonright n) \leq C(n) + c$, *then* x *is recursive.*

Proof.

Since $\exists c_0 \forall n C(n) \leq \log n + c_0$ and for every k, there is some $n \in [2^k, 2^{k+1})$ so that $C(x \upharpoonright n) \geq k = \log n$, we have that $\{x \mid \forall n C(x \upharpoonright n) \leq C(n) + c\} \subseteq A = \{x \mid \forall k \forall s \exists n \in [2^k, 2^{k+1})(\log n \leq C(n)[s] \leq C(x \upharpoonright n)[s] \leq \log n + c + c_0)\}$. By the counting theorem for C, A has only finitely many infinite paths. Moreover, A has a recursive subtree T with same infinite paths. □

K-triviality

Definition

x is *K-trivial* if $\exists c \forall n K(x \upharpoonright n) \leq K(n) + c$.

Theorem (Chaitin)

If x is K-trivial, then $x \leq_T \emptyset'$.

Proof.

By the counting theorem for K. □

K-triviality

Definition

x is *K-trivial* if $\exists c \forall n K(x \upharpoonright n) \leq K(n) + c$.

Theorem (Chaitin)

If x is K-trivial, then $x \leq_T \emptyset'$.

Proof.

By the counting theorem for K. □

A non-recursive K-trivial r.e. real

Theorem (Downey, Hirschfeldt, Nies)

There is a non-recursive r.e. K-trivial real.

Proof.

We build a simple set x which is K-trivial by KC-theorem. We build a prefix-fix machine M.

At any stage s, find the least e so that some $n > 2e$ enters W_e but $W_e \cap x = \emptyset$ and $\sum_{m \geq n} 2^{-K_s(m)} < 2^{-e-4}$, enumerate n into x and $(K_s(m), x_{s+1} \upharpoonright m)$ for every $m \geq n$ into M. □

Geometric measure theory (1)

Given a non-empty $U \subseteq \mathbb{R}$, the *diameter* of U is

$$diam(U) = |U| = \sup\{|x - y| : x, y \in U\}.$$

Given any set $E \subseteq \mathbb{R}$ and $d \geq 0$, let

$$\mathcal{H}^d(E) = \lim_{\delta \to 0} \inf\{\sum_{i<\omega} |U_i|^d : \{U_i\} \text{ is an open cover of } E \wedge \forall i\, |U_i| < \delta\},$$

$\mathcal{P}_0^d(E) = \lim_{\delta\to 0} \sup\{\sum_{i<\omega} |B_i|^d :$
$\{B_i\}$ is a collection of disjoint balls of radii at most δ with centres in $E\}$
and

$$\mathcal{P}^d(E) = \inf\{\sum_{i<\omega} \mathcal{P}_0^d(E_i) \mid E \subseteq \bigcup_{i<\omega} E_i\}.$$

Geometric measure theory (2)

Definition

Given any set E,

- the *Hausdorff dimension* of E, or $\mathrm{Dim}_H(E)$, is
$$\inf\{d \mid \mathcal{H}^d(E) = 0\};$$
- the *Packing dimension* of E, or $\mathrm{Dim}_P(E)$, is
$$\inf\{d \mid \mathcal{P}^d(E) = 0\}.$$

On geometric measure theory

Theorem

$\mathcal{H}^d(A) = 0$ if and only if there is some real x and some constant c so that for any $z \in A$, there are infinitely many n's so that $K^x(z \upharpoonright n) \leq dn + c$.

Proof.

From right to left, by the counting theorem of Kolmogorov complexity. From left to right, for any i, let $\{\sigma_j^i\}_{j\in\omega}$ be a prefix-free cover of A so that

- $\forall j |\sigma_j^i| > 2^i$;
- $\sum_j 2^{-d|\sigma_j^i|} < 2^{-i}$.

Let x code all such sequences. Then for any σ_j^i, $K^x(\sigma_j^i) \leq d|\sigma_j^i| + c$ for a fixed constant. □

Lutz-Lutz theorem

Theorem (Lutz-Lutz)

1. $\mathtt{Dim}_H(A) \leq d$ *if and only if* $\forall d' > d \exists x \forall r \in A \underline{\lim} \frac{K^x(r \upharpoonright n)}{n} < d'$.
2. $\mathtt{Dim}_H(A) \geq d$ *if and only if* $\forall d' < d \forall x \exists r \in A \underline{\lim} \frac{K^x(r \upharpoonright n)}{n} \geq d'$.

Some open problems

Question

1. *For any real x, does there exist a random real r and a constant* $c \in \omega$ *so that* $\exists m \forall n \geq m K(r \upharpoonright m) \geq K(x \upharpoonright m) - c$*?*
2. *Is there a degree invariant Borel function f so that for any real x,* $f(x)$ *is random relative to x?*

Exercise

1. Prove that $\forall d \exists \sigma \exists \tau C(\sigma^\frown \tau) > C(\sigma) + C(\tau) - d$.
2. Prove that both C and K have Turing degree $\emptyset'$.
3. Every random real computes a DNR-function.
4. If $\exists c \forall n C^x(n) \geq C(n) - c$, then x is recursive.
5. There is a non-recursive r.e. real x so that $\exists c \forall n K^x(n) \geq K(n) - c$.

Further readings

An introduction to Kolmogorov complexity, Li and Vitany, 2018.

Computability and randomness, Nies, 2012.

Algorithmic randomness and complexity, Downey and Hirschfeldt, 2010.