Algorithmic randomness theory: its philosophical and mathematical aspects

Liang Yu

Mathematical Department
Nanjing University

September 27, 2019

History

What is randomness?

History

What is randomness?

1. Incompressible;

History

What is randomness?

1. Incompressible;
2. No distinguish property;

History

What is randomness?

1. Incompressible;
2. No distinguish property;
3. Unpredictable.

Notations

We always identify a reals as its binary expansion.

Classical Randomness

People interested in classical randomness live in a computable world.
To them, randomness means random relative to the computable world.

Kolmogorov complexity

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

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

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 $K_M(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$.

If U is a universal Turing machines, both C_U and K_U have the minimality property.

Martin-Löf test

Definition (Martin-Löf)

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

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

(iii) Given a real x, a real y is said to be 1-x-random if it passes all $\Sigma^0_1(x)$ Martin-Löf tests.

Martin-Löf test

Definition (Martin-Löf)

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

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

(iii) Given a real x, a real y is said to be 1-x-random if it passes all $\Sigma^0_1(x)$ Martin-Löf tests.

There exists a universal c.e. Martin-Löf test.

Betting strategy

Definition

1. A martingale is a function $f : 2^{<\omega} \mapsto \mathbb{R}$ 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 $\limsup_n f(y \upharpoonright n) = \infty$.

What is randomness?

A real x is random if

1. $\forall n C(x \upharpoonright n) \geq n$;

What is randomness?

A real x is random if

1. $\forall n C(x \upharpoonright n) \geq n$;
2. $\forall n K(x \upharpoonright n) \geq n$;

What is randomness?

A real x is random if

1. $\forall n C(x \upharpoonright n) \geq n$;
2. $\forall n K(x \upharpoonright n) \geq n$;
3. x doesn't belong to any effective Matin-Löf test;

What is randomness?

A real x is random if

1. $\forall n C(x \upharpoonright n) \geq n$;
2. $\forall n K(x \upharpoonright n) \geq n$;
3. x doesn't belong to any effective Matin-Löf test;
4. No effective strategy can win on x.

What is randomness?

A real x is random if

1. $\forall n C(x \upharpoonright n) \geq n$;
2. $\forall n K(x \upharpoonright n) \geq n$;
3. x doesn't belong to any effective Matin-Löf test;
4. No effective strategy can win on x.

Theorem (Schnorr)

(1) does not exist and the others are equivalent.

Chaitin's Ω

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

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

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.

The Kolmogorov complexity of random reals

Theorem (Miller and Y)

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

The Kolmogorov complexity of random reals

Theorem (Miller and Y)

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

So if x is random, then $K^x(n) \leq K(x \upharpoonright n) - n + c$ for some constant c.

Van Lambalgen's theorem

Theorem (Van Lambalgen)

(x, y) is random iff x is random and y is random relative to x.

Rich v.s. Power

How to compare randomness? Does higher complexity mean higher randomness?

Rich v.s. Power

How to compare randomness? Does higher complexity mean higher randomness?
Obviously a random real can compress itself.

Rich v.s. Power

How to compare randomness? Does higher complexity mean higher randomness?
Obviously a random real can compress itself.
But can it do more? Does richer mean more power?

Some evidence from computability theory

Theorem (de Leeuw, Moore, Shannon, Shapiro; Sacks)

If x is noncomputable, then $\mu(\{y : y \geq_T x\}) = 0$.

Some evidence from computability theory

Theorem (de Leeuw, Moore, Shannon, Shapiro; Sacks)

If x is noncomputable, then $\mu(\{y : y \geq_T x\}) = 0$.

Theorem (Stephan)

A random real x is PA-complete iff x can compute the halting problem.

Some evidence from computability theory

Theorem (de Leeuw, Moore, Shannon, Shapiro; Sacks)

If x is noncomputable, then $\mu(\{y : y \geq_T x\}) = 0$.

Theorem (Stephan)

A random real x is PA-complete iff x can compute the halting problem.

Theorem (Merkle and Y)

Let $E(n) = \int K^x(n)dx$, then $E(n) =^* K(n)$.

So a random real cannot be very powerful.

K-degrees, vL-degrees, LR-degrees and LK-degrees

Definition

1. $x \leq_K y$ if $\forall n(K(x \upharpoonright n) \leq K(y \upharpoonright n))$;
2. $x \leq_{vL} y$ if for all z, $x \oplus z$ is random implies $y \oplus z$ is random;
3. $x \leq_{LR} y$ if for all z, z is y-random implies z is x-random;
4. $x \leq_{LK} y$ if $\exists c \forall n(K^y(n) \leq K^x(n) + c)$.

K-degrees, vL-degrees, LR-degrees and LK-degrees

Definition

1. $x \leq_K y$ if $\forall n(K(x \upharpoonright n) \leq K(y \upharpoonright n))$;
2. $x \leq_{vL} y$ if for all z, $x \oplus z$ is random implies $y \oplus z$ is random;
3. $x \leq_{LR} y$ if for all z, z is y-random implies z is x-random;
4. $x \leq_{LK} y$ if $\exists c \forall n(K^y(n) \leq K^x(n) + c)$.

Note that $x \leq_{vL} y$ implies $x \geq_{LR} y$ for x, y random. This gives an explicit description for comparing randomness with power.

Relationships of the reductions

Theorem (Miller, Yu)

$x \leq_K y$ implies $x \leq_{vL} y$.

So more complicated means more random.

Relationships of the reductions

Theorem (Miller, Yu)

$x \leq_K y$ implies $x \leq_{vL} y$.

So more complicated means more random.

Theorem (Kjos-Hanssen, Miller, Solomon)

$x \leq_{LR} y$ iff $x \leq_{LK} y$.

So compressing random exactly means compressing everything.

Relationships of the reductions

Theorem (Miller, Yu)

$x \leq_K y$ implies $x \leq_{vL} y$.

So more complicated means more random.

Theorem (Kjos-Hanssen, Miller, Solomon)

$x \leq_{LR} y$ iff $x \leq_{LK} y$.

So compressing random exactly means compressing everything. Put two results together, we can say that more random means less power.

Higher Randomness Theory

It is arguable that the real world is computable.

Higher Randomness Theory

It is arguable that the real world is computable.

At least mathematicians do not live in the computable world.

Higher Randomness Theory

It is arguable that the real world is computable.

At least mathematicians do not live in the computable world.

But, really...?

Constructibility

We may perform recursive operators over sets just like numbers.

Constructibility

We may perform recursive operators over sets just like numbers.

$$L_0 = \emptyset,$$

$L_{\alpha+1}$ is the closure of recursive operators over J_α,

$$L_\alpha = \bigcup_{\beta<\alpha} J_\beta, \text{when } \alpha \text{ is limit.}$$

$$L = \bigcup_{\alpha} L_\alpha$$

Gödel's Theorem

Theorem

L satisfies ZFC.

Gödel's Theorem

Theorem

L satisfies ZFC.

So it is safe to say that mathematicians live in a "computable world".

The real world for recursion theorists

Not every ordinal exists.

The real world for recursion theorists

Not every ordinal exists.

Only computable ordinals exist.
The lease upper bound of computable ordinal is ω_1^{CK}.

The real world for recursion theorists

Not every ordinal exists.

Only computable ordinals exist.
The lease upper bound of computable ordinal is ω_1^{CK}.

$L_{\omega_1^{\mathrm{CK}}}$ is the world for recursion theorists.

Computation in $J_{\omega_1^{\mathrm{CK}}}$

For logicians, a computation is a Σ_1-procedure. So a computation in $J_{\omega_1^{\mathrm{CK}}}$ is a searching procedure over the elements of $L_{\omega_1^{\mathrm{CK}}}$.

Computation in $J_{\omega_1^{\mathrm{CK}}}$

For logicians, a computation is a Σ_1-procedure. So a computation in $J_{\omega_1^{\mathrm{CK}}}$ is a searching procedure over the elements of $L_{\omega_1^{\mathrm{CK}}}$.

The time in $L_{\omega_1^{\mathrm{CK}}}$ is longer than the space. This results in that some techniques in computable world do not work in $L_{\omega_1^{\mathrm{CK}}}$.

Π^1_1-randomness

Definition

A real x is Π^1_1-random if it does not belong to any Π^1_1-null set.

Randomness respect to a measure

For different measure λ, we may introduce corresponded randomness notions respected to its representation.

We are only interested in atomless measure.

On $NCR_{\Pi^1_1}$

Theorem (Chong and Y)

x is never Π^1_1-random respect to any atomless measure iff $x \in L_{\omega_1^x}$.

On $NCR_{\Pi^1_1}$

Theorem (Chong and Y)

x is never Π^1_1-random respect to any atomless measure iff $x \in L_{\omega_1^x}$.

The reals having the property $x \in L_{\omega_1^x}$ are considered to be the set theoretical halting problems.

Beyond *ZFC*

But Gödel's L is not the right model to push randomness theory further.

We need a "right" way to generalize "computation".

This relates to some deep results in set theory.

Ω as a continuous funciton

Let $\hat{\Omega} : 2^\omega \to \mathbb{R}$ be $\hat{\Omega}(x) = \sum_n 2^{-K(x\upharpoonright n)}$.

Theorem (Hölz, Merkle, Miller, Stephan, Y)

$\hat{\Omega}$ is a continuous, almost everywhere differentiable with derivation 0 and nowhere monotonic.

Euclid's theorem

Theorem (Euclid)

There are infinitely many prime numbers.

Proof.

Suppose that there are only m-many prime numbers. So for any number n, $n = p_1^{n_1} \cdots p_m^{n_m}$. Thus

$$C(n) \leq \sum_{i \leq m} C(n_i) + c \leq m \max\{C(n_i) \mid i \leq m\} + c \leq m \log\log n + c,$$

a contradiction. □

Erdös similarity problem

A is similar to B if there are two reals $p \neq 0$ and q so that $A = \{px + q \mid x \in B\}$.

Question (Erdös)

If $A \subseteq (0,1)$, is there a set $E \subset (0,1)$ having positive measure in which there is no subset similar to A?

Theorem (Kolountzakis)

If E is full, then Erdös question has a negative answer.

Proof.

Randomness can be considered as an invariant to the similarity transformation. But since E is conull, it contains all such invariants. So just let p be a sufficiently random real and $q = 0$. □

Some other applications

Theorem (Forklore ?)

- *If f is a continuous function mapping all null sets to meager sets, then f is constant.*
- *If f is a measurable function and mapping all null sets to null sets, then for almost every real x, $f^{-1}(x)$ is at most countable.*

Further readings

An introduction to Kolmogorov complexity, Li and Vitany, 2008.

Computability and randomness, Nies, 2012.

Algorithmic randomness and complexity, Downey and Hirschfeldt, 2010.

Recursion theory, Chong and Yu, 2015.

Thanks!