Algorithmic randomness theory and its applications

Liang Yu
Mathematical Department
Nanjing University

March 24, 2021
What is randomness?
History

What is randomness?

1. Incompressible;
What is randomness?

1. Incompressible;
2. No distinguish property;
What is randomness?

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

We always identify a reals as its binary expansion.
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 $C_M(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$. 
Fix a Turing machine $M$, for each finite string $\sigma \in 2^{<\omega}$, define $C_M(\sigma) = \min\{|\tau| : M(\tau) = \sigma\}$.

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.
Basic facts

1. $C(\sigma) \leq |\sigma| + c$ and so $C(n) \leq \log n + c$ for some constant $c$;
Basic facts

1. \( C(\sigma) \leq |\sigma| + c \) and so \( C(n) \leq \log n + c \) for some constant \( c \);
2. There is some \( \sigma \) (or number \( n \)) so that \( C(\sigma) \geq |\sigma| \) (or \( C(n) \geq \log n \)).
Basic facts

1. $C(\sigma) \leq |\sigma| + c$ and so $C(n) \leq \log n + c$ for some constant $c$;
2. There is some $\sigma$ (or number $n$) so that $C(\sigma) \geq |\sigma|$ (or $C(n) \geq \log n$).
3. $C((\sigma, \tau)) \leq C(\sigma) + C(\tau) + C(|\sigma|) + c$. 
Martin-Löf test

Definition (Martin-Löf)

(i) Given a real $x$, a $\Sigma^0_1$ 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 $\Sigma^0_1$ 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.
Theory aspect

Betting strategy

Definition

1. A martingale is a function \( f: 2^{<\omega} \rightarrow \mathbb{R} \) such that for all \( \sigma \in 2^{<\omega} \),
\[
f(\sigma) = \frac{f(\sigma^0) + f(\sigma^1)}{2}.
\]

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 Martin-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 Martin-Löf test;
4. No effective strategy can win on $x$. 

Theorem (Schnorr) (1) does not exist and the others are equivalent.
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 Martin-Löf test;
4. No effective strategy can win on $x$.

Theorem (Schnorr)

(1) does not exist and the others are equivalent.
The Kolmogorov complexity of random reals

**Theorem (Miller and Y)**

\[ x \text{ is 1-random iff } \sum_n 2^n - K(x|n) < \infty. \]
The Kolmogorov complexity of random reals

Theorem (Miller and Y)

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

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

Yu (Math Dept of Nanjing University)
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.
Theory aspect

*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 $x \leq_{LR} y$ for $x$, $y$ random. This gives an explicit description for comparing randomness with power.
Definition

1. \( x \leq_K y \) if \( \forall n(K(x \uparrow n) \leq K(y \uparrow n)) \);
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)

\[ x \leq_K y \text{ implies } x \leq_{vL} y. \]

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.

\[ L_0 = \emptyset, \]

\[ L_{\alpha+1} \text{ is the closure of recursive operators over } L_{\alpha}, \]

\[ L_\alpha = \bigcup_{\beta < \alpha} L_\beta, \text{ when } \alpha \text{ is limit}. \]

\[ L = \bigcup_{\alpha} L_\alpha \]
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 $\omega_1^{CK}$. 

The real world for recursion theorists

Not every ordinal exists.

Only computable ordinals exist.
The lease upper bound of computable ordinal is $\omega_1^{CK}$.

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

For logicians, a computation is a $\Sigma_1$-procedure. So a computation in $L_{\omega_1^{CK}}$ is a searching procedure over the elements of $L_{\omega_1^{CK}}$. 
Computation in $L_{\omega_1^{CK}}$

For logicians, a computation is a $\Sigma_1$-procedure. So a computation in $L_{\omega_1^{CK}}$ is a searching procedure over the elements of $L_{\omega_1^{CK}}$.

The time in $L_{\omega_1^{CK}}$ is longer than the space. This results in that some techniques in computable world do not work in $L_{\omega_1^{CK}}$. 
\( \Pi^1_1 \)-randomness

**Definition**

A real \( x \) is \( \Pi^1_1 \)-random if it does not belong to any \( \Pi^1_1 \)-null set.

**Theorem (Sacks)**

*If \( x \) is \( \Pi^1_1 \)-random, then \( \omega_1^x = \omega_1^{CK} \).*
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.
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

\[
C(n) \leq \sum_{i \leq m} 2 \log n_i \leq 2m \max \{ \log n_i \mid i \leq m \} \leq 2m \log \log n.
\]

But if \( m \) is random, then \( C(n) \geq \log n \), a contradiction.
\[ p_n \leq n(\log n)^2 \]

Theorem

\[ p_n \leq n(\log n)^2. \]

Proof.

Given any number \( m \), let \( p_n \) be the largest prime dividing \( m \). Then

\[ C(m) \leq C(n, \frac{m}{p_n}) \leq \log n + \log \frac{m}{p_n} + 2 \log \log n \]

If \( m \) is random, then \( \log m \leq C(m) \) and so

\[ \log m \leq \log n + \log m - \log p_n + 2 \log \log n. \]

So \( p_n \leq n(\log n)^2. \)
Banach’s theorem

Theorem (Banach)

If $f$ is a continuous function and has property (N), then it has property $T_2$. I.e. for almost every real $r$, $f^{-1}(r)$ is countable.
Banach’s theorem

Theorem (Banach)

If $f$ is a continuous function and has property (N), then it has property $T_2$. I.e. for almost every real $r$, $f^{-1}(r)$ is countable.

Theorem (Russian school; Louveau)

If $f$ is has property (N) and measurable, then it has property $T_2$. 
A recursion theoretical proof of Banach’s theorem

Let $f$ be a recursive function having property $N$. Let $r$ be a $\Delta^1_1(O)$-random real. Then $f^{-1}(r)$ only contains $\Delta^1_1(O)$-random. So $f(x) = r$ implies $\omega^x_1 = \omega^{CK}_1$. Note that $f^{-1}(r)$ is a $\Delta^1_1(r)$ set and only contains reals Turing computing $r$. By Martin’s theorem, $f^{-1}(r)$ is countable.
A recursion theoretical proof of Banach’s theorem

Let $f$ be a recursive function having property $N$. Let $r$ be a $\Delta^1_1(O)$-random real. Then $f^{-1}(r)$ only contains $\Delta^1_1(O)$-random. So $f(x) = r$ implies $\omega^x_1 = \omega^{{\text{CK}}}_1$. Note that $f^{-1}(r)$ is a $\Delta^1_1(r)$ set and only contains reals Turing computing $r$. By Martin’s theorem, $f^{-1}(r)$ is countable.

To prove the second theorem, note that a measurable function $f$ equals to a Borel function almost everywhere. Since $f$ has property-$(N)$, we may ignore the null part. Then apply the method above to the Borel function.
Some more results (1)

Definition
A function $f$ has *Luzin-(M)-Property* if it maps a null set to a countable set.

Theorem (Pauly, Westrick, Y)
- *If* $f$ *is a continuous function and has property* $(M)$, *then* $f$ *is a constant function.*
- *If* $f$ *is has property* $(M)$ *and measurable, then the range of* $f$ *is countable.*
Some more results (2)

Proof.

We only prove (1) for a recursive function $f$. For any $x$, let $g$ be $\Delta^1_1(O^x)$-generic. Then $x$ and $g$ form a minimal pair of $\Delta^1_1$-degrees. Moreover, $x$ belongs to a $\Delta^1_1(g)$-null set $A$. So $f(A)$ is a $\Sigma^1_1(g)$ and countable set. Thus $f(x) \leq_{\Delta^1_1} g$, $x$ and so must be $\Delta^1_1$. In other words, the range of $f$ is countable and so constant.

Peng and I also proved that the general conclusion is independent of ZFC.
Some questions

Question

(1) Is there a function having property-\( (N) \) but not having property \( T_2 \)?

(2) Is there an uncountable ideal \( I \) of Turing degrees so that for any real \( x \) and almost every real \( r \), \( r \) is random relative to the ideal generated by \( I \cup \{x\} \)?

Both questions have positive answers under certain set theory assumptions.
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!