A generalization of Levin/Schnorr's theorem

Keita Yokoyama

Japan Advanced Institute of Science and Technology

May 14, 2013, University of Tokyo

Outline

1. Introduction
   - Randomness
   - Complexity
   - Correspondence
2. Generalizations of randomness/complexity
   - Generalized randomness
   - Generalized complexity
3. A generalization of Levin/Schnorr's theorem
   - Generalized correspondence
   - Characterizing basic properties

Outline

1. Introduction
   - Randomness
   - Complexity
   - Correspondence
2. Generalizations of randomness/complexity
   - Generalized randomness
   - Generalized complexity
3. A generalization of Levin/Schnorr's theorem
   - Generalized correspondence
   - Characterizing basic properties

Maritin-Löf randomness

Measure theoretic approach for randomness:

- Let μ be a fair-coin measure on 2^ω.
- For given $A \subseteq 2^{<\omega}$, $[A] := \{X \in 2^\omega \mid \exists \sigma \in A\ \sigma \subseteq X\}$.
- A sequence $\{A_n \subseteq 2^{<\omega}\}_{n \in \omega}$ is (uniformly) c.e. if $\{(\sigma, n) \mid \sigma \in A_n\}$ is c.e.

Definition

A c.e. sequence $\{A_n\}_{n\in\omega}$ is said to be a Martin-Löf test (ML-test) if $\mu([A_n]) \leq 2^{-n}$.
A real X is said to be a Maritin-Löf random if $X \notin \bigcap_n [A_n]$ for any ML-test $\{A_n\}_{n\in\omega}$.

Partial randomness

We can generalize the previous notion of randomness: instead of using measure, we use "weight functions".

- Let $h : 2^{<\omega} \to \omega$ be a computable function.
- For $A \subseteq 2^{<\omega}$, define

$$\mathrm{dwt}_h(A) = \sum_{\sigma \in A} 2^{-h(\sigma)}.$$

- A set $P \subseteq 2^{<\omega}$ is said to be *prefix-free* if $\forall \sigma, \tau \in P(\sigma \subseteq \tau \Leftrightarrow \sigma = \tau)$.
- For $A \subseteq 2^{<\omega}$, define

$$\mathrm{pwt}_h(A) = \sup\{\mathrm{dwt}_h(P) \mid P \text{ is a prefix-free subset of } A\}.$$

Partial randomness

Definition

A c.e. sequence $\{A_n\}_{n\in\omega}$ is said to be an h-test if $\mathrm{dwt}_h(A_n) \leq 2^{-n}$.
A real X is said to be an h-random if $X \notin \bigcap_n [A_n]$ for any h-test $\{A_n\}_{n\in\omega}$.

Definition

A c.e. sequence $\{A_n\}_{n\in\omega}$ is said to be a strong-h-test if $\mathrm{pwt}_h(A_n) \leq 2^{-n}$.
A real X is said to be a strong-h-random if $X \notin \bigcap_n [A_n]$ for any strong-h-test $\{A_n\}_{n\in\omega}$.

Prefix-free complexity

- A Turing machine (partial computable function) $M :\subseteq 2^{<\omega} \to 2^{<\omega}$ is said to be *prefix-free* if $\mathrm{dom}(M)$ is prefix-free.
- A prefix-free Turing machine U is said to be *universal* if for any prefix-free Turing machine M, there exists $\tau \in 2^{<\omega}$ such that $M(\sigma) = U(\tau^\frown\sigma)$.
- There exists a universal prefix-free Turing machine.

Definition (prefix-free complexity)

The prefix-free complexity $\mathrm{KP} : 2^{<\omega} \to \omega$ is define as follows:

$$\mathrm{KP}(\sigma) := \min\{|\tau| \mid U(\tau) = \sigma\},$$

where U is a prefix-free universal Turing machine.
Note that this is well-defined up to constant.

Prefix-free complexity

Using a complexity function, we can say that a real X is complex/random if it is not compressible:

Definition

A real $X \in 2^\omega$ is said to be *weakly Chaitin random* or KP-*complex* if there exists $c \in \omega$ such that for any $n \in \omega$,

$$\mathrm{KP}(X \upharpoonright n) \geq n - c.$$

Similarly, if $h : 2^{<\omega} \to \omega$ be a computable function, then $X \in 2^\omega$ is said to be KP-*h*-*complex* if there exists $c \in \omega$ such that for any $n \in \omega$,

$$\mathrm{KP}(X \upharpoonright n) \geq h(X \upharpoonright n) - c.$$

Characterization by the Kraft inequality

KP can be characterized as a minimal (abstract) complexity which satisfies the following Kraft inequality.

Proposition (the Kraft ienequality)

$$\sum_{\sigma \in 2^{<\omega}} 2^{-\mathrm{KP}(\sigma)} < 1.$$

- A function $K : 2^{<\omega} \to \omega \cup \{\infty\}$ is said to be an abstract complexity if K is right c.e., or equivalently, there exists a c.e. set $A \subseteq 2^{<\omega} \times \omega$ such that $K(\sigma) = \min\{n \mid (\sigma, n) \in A\}$.

Characterization by the Kraft inequality

Theorem (the Kraft/Chaitin theorem)

For any abstract complexity K such that

$$\sum_{\sigma \in 2^{<\omega}} 2^{-K(\sigma)} < 1,$$

there exists $c \in \omega$ such that for any $\sigma \in 2^{<\omega}$,

$$K(\sigma) \geq \mathrm{KP}(\sigma) - c.$$

This theorem means that KP is minimal up to constant in all abstract complexities which satisfy the Kraft inequality.

In fact, several complexity functions can be defined in this way.

Several other complexities

Definition (Uspensky/Shen)

- The a priori complexity KA is defined as a minimal complexity which satisfies the following:
  for any prefix-free $P \subseteq 2^{<\omega}$, $\sum_{\sigma \in P} 2^{-K(\sigma)} < 1$.
- The simple complexity KS is defined as a minimal complexity which satisfies the following:
  $\{\sigma \in 2^{<\omega} \mid K(\sigma) < n\}^{\#} < 2^n$.
- The decision complexity KD is defined as a minimal complexity which satisfies the following:
  for any prefix-free $P \subseteq 2^{<\omega}$, $\{\sigma \in P \mid K(\sigma) < n\}^{\#} < 2^n$.

We can also define KA-h-complex, KS-h-complex and KD-h-complex similarly to KP-h-complex.

Levin/Schnorr's theorem

The previous two definitions of randomness have a nice correspondence.

Theorem (Levin/Schnorr's theorem)

A real $X \in 2^\omega$ is ML-random if and only if it is KP-complex.

More generally, the following holds.

Theorem (Tadaki/Calude/Staiger/Terwijn)

Let $h : 2^{<\omega} \to \omega$ be a computable function.

- *A real $X \in 2^\omega$ is h-random if and only if it is KP-h-complex.*
- *A real $X \in 2^\omega$ is strongly-h-random if and only if it is KA-h-complex.*

Levin/Schnorr's theorem

For KS and KD, we need new weight functions.
Let $h : 2^{<\omega} \to \omega$ be a computable function.

- For $A \subseteq 2^{<\omega}$, define
$$\mathrm{dct}_h(A) = \sup_{n\in\omega}\{\sigma \in A \mid h(\sigma) < n\}^{\#}/2^n.$$
- For $A \subseteq 2^{<\omega}$, define
$$\mathrm{pct}_h(A) = \sup\{\mathrm{dct}_h(P) \mid P \text{ is a prefix-free subset of } A\}.$$

We can define dct_h-randomness or pct_h-randomness similar to h-randomness or strong-h-randomness.

Levin/Schnorr's theorem

Then, we have the following.

Theorem (Some more variations)

Let $h : 2^{<\omega} \to \omega$ be a computable function.

- *A real $X \in 2^\omega$ is h-random if and only if it is KP-h-complex.*
- *A real $X \in 2^\omega$ is strongly-h-random if and only if it is KA-h-complex.*
- *A real $X \in 2^\omega$ is dct_h-random if and only if it is KS-h-complex.*
- *A real $X \in 2^\omega$ is pct_h-random if and only if it is KD-h-complex.*

We have seen that there are several versions of randomness/complexity defined by a "measure-like" function/complexity function.

Questions.

- Is there a generalization of all of these randomness or complexity notions?
- Can we generalize the correspondence of randomness and complexity?

Outline

Weight function

We first generalize a notion of randomness defined by a wight function.

Definition

A *weight function* is a computable function $m : [2^{<\omega}]^{<\omega} \to [0, \infty)$ which satisfies the following:

1. $m(\emptyset) = 0$,
2. if $F_1 \subseteq F_2$, then $m(F_1) \leq m(F_2)$,
3. $m(F_1 \cup F_2) \leq m(F_1) + m(F_2)$.

For arbitrary $A \subseteq 2^{<\omega}$, we expand $m : [2^{<\omega}]^{\leq\omega} \to [0, \infty)$ as follows:

$$m(A) = \sup\{m(F) \mid F \subseteq_{\text{fin}} A\}.$$

Note that $m(A) = \inf\{\sum_{i\in\omega} m(F_i) \mid \bigcup_{i\in\omega} F_i \supseteq A\}$ if m is bounded.

Randomness defined by a weight function

All of the following are weight functions:

$$\mathrm{dwt}_h(F) := \sum_{\sigma \in F} 2^{-h(\sigma)},$$

$$\mathrm{pwt}_h(F) := \sup\{\mathrm{dwt}_h(P) \mid P \subseteq F \text{ is prefix free}\},$$

$$\mathrm{dct}_h(F) := \sup_{n \in \omega} \frac{\{\sigma \in F \mid h(\sigma) < n\}^{\#}}{2^n},$$

$$\mathrm{pct}_h(F) := \sup\{\mathrm{dct}_h(P) \mid P \subseteq F \text{ is prefix free}\}.$$

Definition

An *m-test* is a c.e. sequence $\{A_i\}_{i \in \omega}$ such that $m(A_i) \leq 2^{-i}$.
A real $X \in \omega$ is said to be *m-random* if $X \notin \bigcap_i [A_i]$ for any m-test $\{A_i\}_{i \in \omega}$.

Universal test

Proposition

For any weight function m, a universal m-test exists, i.e., there exists an m-test $\{A_i\}_{i\in\omega}$ such that $X \in 2^\omega$ is m-random if and only if $X \notin \bigcap_i [A_i]$.

Corollary

The class of all m-random reals is Σ^0_2.

In fact, any Σ^0_2-subclass of Cantor space can be considered as a set of m-random reals as follows:

Let $P \subseteq 2^\omega$ be a Σ^0_2-class. Take a computable sequence of trees $\{T_i \mid i \in \omega\}$ such that $X \in P$ if and only if X is a path of T_i for some $i \in \omega$. Define weight functions m_i and m as follows:

$$m_i(F) = \begin{cases} 1 & \text{if } F \cap T_i \neq \emptyset, \\ 0 & \text{otherwise,} \end{cases}$$

$$m(F) = \sum_{i \in \omega} 2^{-i} m_i(F).$$

Then, we can easily check that X is m-random if and only if $X \in P$.

Rule for a complexity

Next, we generalize complexity functions.
For this, we consider a generalization of the Kraft/Chaitin theorem.

- A finite complexity function is a finite set $r \subseteq 2^{<\omega} \times \mathbb{Z}$, we identify r as a function $K^r(\sigma) = \min\{d \mid (\sigma, d) \in r\} \cup \{\infty\}$.
- Given a finite complexity $r \subseteq 2^{<\omega} \times \mathbb{Z}$,
  - $\mathring{r} := \{\sigma \in 2^{<\omega} \mid \exists d \in \omega\ (\sigma, d) \in r\}$,
  - $r^{+i} := \{(\sigma, d + i) \mid (\sigma, d) \in r\}$,
  - given a computable function $h : 2^{<\omega} \to \omega$, $r^{+h} := \{(\sigma, d + h(\sigma)) \mid (\sigma, d) \in r\}$.
- Let $r, s \subseteq 2^{<\omega} \times \omega$ be finite complexity functions. We say that r is stronger than s ($s \prec r$) if $K^s(\sigma) \leq K^r(\sigma)$ for any $\sigma \in 2^{<\omega}$.

Rule for a complexity

Now, we construct a complexity function from finite complexity functions.

Definition

A *rule* (for a complexity function) is a computable set $R \subset [2^{<\omega} \times \mathbb{Z}]^{<\omega}$ which satisfies the following:

1. $\emptyset \in R$.
2. If $r \in R$ and $s < r$, then $s \in R$.
3. If $r, s \in R$, then $(r \cup s)^{+1} \in R$.

Condition 3 means that any two finite complexity functions can be combined into one function with an additional step.

Optimal complexity function

Definition (Complexity as a minimal function)

A *complexity function* is a right c.e. function $K : 2^{<\omega} \to \mathbb{Z}$.

Given a rule R, a complexity function $K = K_R$ is said to be *R-optimal* if

1. R-function: for any finite $F \subseteq 2^{<\omega}$, $\{(\sigma, K(\sigma)) \mid \sigma \in F\} \in R$.
2. R-minimal: if K' is also an R-function, then there exists $c \in \omega$ such that for any $\sigma \in 2^{<\omega}$,

$$K'(\sigma) \geq K(\sigma) - c.$$

Note that K_R is defined uniquely up to constant.

Proposition

For any rule R, R-optimal complexity function K_R exists.

Complex defined by a complexity function

Definition

$X \in 2^\omega$ is said to be R-complex if there exists $c \in \omega$ such that $K_R(X \restriction n) \geq n - c$ for any $n \in \omega$.

Examples.

- Let $R_{\mathrm{KP}} := \{r \in [2^{<\omega} \times \mathbb{Z}]^{<\omega} \mid \sum_{\sigma \in 2^{<\omega}} 2^{-K_r(\sigma)} < 1\}$, then, KP is an R_{KP}-optimal complexity.
- Let $R_{\mathrm{KP}h} := R_{\mathrm{KP}}^{+|\cdot|-h} = \{r^{+|\cdot|-h} \mid r \in R_{\mathrm{KP}}\}$, then, $K_{R_{\mathrm{KP}h}}(\sigma) = \mathrm{KP}(\sigma) + |\sigma| - h(\sigma)$, *i.e.*, X is $R_{\mathrm{KP}h}$-complex iff it is KP-h-complex.
- We can define $R_{\mathrm{KA}h}$, $R_{\mathrm{KS}h}$, and $R_{\mathrm{KD}h}$ similarly.

Outline

Generalized correspondence

Now, we construct a concrete correspondence of randomness and complexity.

- For $r \in [2^{<\omega} \times \mathbb{Z}]^{<\omega}$,
  $||r|| := \min\{|\sigma| - d \mid (\sigma, d) \in r\} \in \mathbb{Z} \cup \{\infty\}$ ($||\emptyset|| = \infty$).
- We can easily check that $s \prec r$ if $\mathring{s} \subseteq \mathring{r}$ and $||s|| \leq ||r||$.

Definition

Let m be a weight function, and let R be a rule. Then, we define $m^{\surd} \subseteq [2^{<\omega} \times \mathbb{Z}]^{<\omega}$ and $R^{\surd} : [2^{<\omega}]^{<\omega} \to [0, \infty)$ as follows:

$$m^{\surd} := \{r \in [2^{<\omega} \times \mathbb{Z}]^{<\omega} \mid \forall s \subseteq r \; m(\mathring{s}) \leq 2^{-||s||}\},$$

$$R^{\surd}(F) := \inf\{2^{-||r_1||} + \cdots + 2^{-||r_l||} \mid r_1, \ldots, r_l \in R, \; F \subseteq \mathring{r}_1 \cup \cdots \cup \mathring{r}_l\}.$$

We can check that $m^{\surd}$ is a rule and $R^{\surd}$ is a weight function.

Generalized correspondence

Proposition

Let m be a weight function, and let R be a rule. Then,

1. $m \leq m^{\surd\surd} \leq 2m$,
2. $R \subseteq R^{\surd\surd} \subseteq R^{-2} = \{s \mid \exists r \in R \ s < r^{-2}\}$, *thus,* $K_R - c \leq K_{R^{\surd\surd}} \leq K_R + c$ *for some* $c \in \omega$.

Definition

Let m be a weight function, and let R be a rule.
Then, R is said to be a *dual rule* of m, or m is said to be a *dual weight function* of R,
if there exists $c \in \omega$ such that $K_R - c \leq K_{m^\surd} \leq K_R + c$,
or equivalently, there exists $c > 0$ such that $1/c \cdot m \leq R^\surd \leq cm$.

Generalized correspondence

Now, we have the following.

Theorem (Generalized Levin/Schnorr's theorem)

Let m be a weight function, and let R be its dual rule. Then, $X \in 2^\omega$ is m-random if and only if it is R-complex.

We can easily check the following:

- $R_{\mathrm{KP}h}$ is a dual of dwt_h,
- $R_{\mathrm{KA}h}$ is a dual of pwt_h,
- $R_{\mathrm{KS}h}$ is a dual of dct_h,
- $R_{\mathrm{KD}h}$ is a dual of pct_h.

Characterizing basic properties

We can characterize some basic properties of randomness:

- Non-triviality:
  X is not m-random relative to X
  $\Leftrightarrow$
  $\lim_{n\to\infty} \sup\{m(\{\sigma\}) \mid n < |\sigma|\} = 0$.
- Tail invariance:
  X is m-random iff its tail is m-random
  $\Leftrightarrow$
  $\forall \tau \in 2^{<\omega}\ \exists c \in \omega\ r \in m^{\surd} \to \{(\tau^\frown\sigma, d + c) \mid (\sigma, d) \in r\} \in m^{\surd}$.

Next, we focus on the property of relativization to a complete Π^0_1-class.
This is related to behaviors of randomness in arithmetic.

Monotonicity and propagation to CPA

- For $A, B \subseteq 2^{<\omega}$, we write $A \prec B$ if for any $\sigma \in A$ there exists $\tau \in B$ such that $\tau \subseteq \sigma$.
- A weight function m is said to be *monotonic* if for any $A, B \subseteq 2^{<\omega}$, $m(A) \leq m(B)$ if $A \prec B$.
- For a given weight function m, define a monotonic closure m^* of m as

$$m^*(F) := \inf\{m(C) \mid C \subseteq 2^{<\omega},\ F \prec C\}.$$

Theorem

Let m be a weight function. Then, the following are equivalent.

1. *X is m^*-random.*
2. *X is m^*-random relative to CPA.*
3. *X is m-random relative to CPA.*

Questions

Can we characterize specific properties of randomness?

- What is needed for the van Lambalgen theorem?
- What is needed for the ample excess lemma?
- ...

Question

Which condition is needed to define "randomness"?