Computable Randomness for Computable Probability Spaces

Jason Rute

Department of Mathematical Science
Carnegie Mellon University

Asian Logic Conference
December 2011

Outline

Schnorr's Legacy

Schnorr gave us computable randomness.

Can it be extended to computable probability spaces?

Schnorr gave us Schnorr's Critique.

Has it already been answered in the negative?

Two Goals

Goal 1

Give (a number of) definitions of computable randomness for arbitrary computable probability spaces.

Goal 2

Describe a new type of randomness in between Martin-Löf randomness and Kolmogorov-Loveland randomness (possibly equal to either/both).

Computable Randomness on 2^ω

Definition

A computable martingale is a computable function $M : 2^{<\omega} \to \mathbb{R}^+$ such that for all $\sigma \in 2^{<\omega}$,

$$\frac{1}{2} \cdot M(\sigma 0) + \frac{1}{2} \cdot M(\sigma 1) = M(\sigma).$$

Given $X \in 2^\omega$, M succeeds on $X \Leftrightarrow \limsup_n M(X \upharpoonright n) = \infty$.

$X \in 2^\omega$ is computably random if there is not any computable martingale M which succeeds on X.

Measures on 2^ω.

Definitions

A computable measure on 2^ω can be represented by a computable function $\mu : 2^{<\omega} \to \mathbb{R}^+$ such that

$$\mu(\sigma 0) + \mu(\sigma 1) = \mu(\sigma).$$

By the Carathéodory extension theorem this can be uniquely extended to a measure on 2^ω.

A probability measure is a measure with $\mu(\text{empty string}) = 1$.
The fair-coin measure is defined by $\mu(\sigma) = 2^{-|\sigma|}$.

We write $\mu(\sigma)$ instead of $\mu([\sigma])$.

Measures and martingales are closely related.

How do we define computable randomness on other probability spaces?

Easy Cases:

- $[0,1]$ with Lebesgue measure.
  Use the binary representation of the reals.
- $(2^\omega, \mu)$ where μ is computable probability space.
  Use martingales $M : 2^{<\omega} \to \mathbb{R}^+$ which satisfy

$$M(\sigma 0) \cdot \mu(\sigma 0) + M(\sigma 1) \cdot \mu(\sigma 1) = M(\sigma) \cdot \mu(\sigma).$$

(Convention: If $\mu(\sigma) = 0$, then $M(\sigma)$ is not defined.)

Harder Cases:

- $[0,1]^n$ with the Lebesgue measure.
- Arbitrary computable probability spaces.

We do not want an ad-hoc definition, but a robust one.

Test Definition on 2^ω

Computable randomness can be defined using "tests".

Definition (Merkle, Mihailović, and Slaman)

Let (U_n) be a computable sequence of Σ^0_1 (effectively open) sets.

- (U_n) is an ML test if for all n,

$$\mu(U_n) \leq 2^{-n}.$$

- (U_n) is a bounded ML test if there is a computable measure ν on 2^ω such that for all n and all $\sigma \in 2^{<\omega}$,

$$\mu(U_n \cap [\sigma]) \leq 2^{-n} \cdot \nu(\sigma).$$

(There is a similar definition by Downey, Griffiths, and LaForte.)

Theorem

$X \in 2^\omega$ is CR $\Leftrightarrow X \notin \bigcap_n U_n$ for any bounded ML test (U_n).

Outline

Computable Metric Spaces

A Crash course!

Definition

A triple (X, d, S) is a computable metric space if

- X is a complete metric space with metric $d : X \times X \to \mathbb{R}^+$,
- $S = \{a_i\}_{i \in \mathbb{N}} \subseteq X$ is a countable dense set (the simple points),
- $d(a_i, a_j)$ is computable from i, j.

From this, we can define computable points, Σ^0_1 sets, Π^0_1 sets, etc.

Examples.

- $(\mathbb{R}^n, |x - y|,$ rational vectors$)$
- $(C[0,1], \|f - g\|_\infty,$ rational piecewise-affine functions$)$

Computable Probability Spaces

A Crash course!

Definition

A pair $(\mathscr{X}, \mu)$ is a computable (Borel) probability space if

- $\mathscr{X} = (X, d, S)$ is a computable metric space,
- μ is a Borel probability measure on X, and
- $\mu(U)$ of a Σ^0_1 set U is lower semi-computable from U.

Hence, Π^0_1 sets are upper semi-computable:

$$\mu(K) = 1 - \mu(X \setminus K)$$

A.e. Decidable Sets

Definition (Hoyrup, Rojas)

A pair A, B is μ-a.e. decidable if

- A and B are Σ^0_1 (can decide if a point is in A or in B)
- $A \cap B = \varnothing$ (points cannot be in both sets)
- $\mu(A \cup B) = 1$ (almost every point is in A or B)

We abuse notation and say $C \subseteq X$ is μ-a.e. decidable if $A \subseteq C \subseteq X \setminus B$ for a μ-a.e. decidable pair A, B.

Examples.

- Half open intervals in $[0, 1]$.
- Closed balls (if boundary is null)
- Reals with binary representation starting with $0.01101\ldots$
- Sequences of 2^ω which have 1111 before 0000.

A.e. Decidable Sets

Definition

A pair A, B is μ-a.e. decidable if

- A and B are Σ^0_1 (can decide if a point is in A or in B)
- $A \cap B = \varnothing$ (points cannot be in both sets)
- $\mu(A \cup B) = 1$ (almost every point is in A or B)

We abuse notation and say $C \subseteq X$ is μ-a.e. decidable if $A \subseteq C \subseteq X \smallsetminus B$ for a μ-a.e. decidable pair A, B.

Properties.

- Boolean combinations of a.e. decidable sets are a.e. decidable.
- If A is μ-a.e. decidable, then $\mu(A)$ is computable from A.
- The boundaries of a.e. decidable sets are Π^0_1 null sets.
- The boundary points are not even Kurtz random!

A.e Decidable Representations

Theorem (reproved many times: Bosserhoff; Hoyrup and Rojas; possibly Levin; relates to Bishop's work)

If $(\mathscr{X}, \mu)$ is a computable probability space, then there is a computable sequence (A_i) of μ-a.e. decidable sets (even balls) such that (A_i) is constructively equivalent to the topology of (X, d, S). In particular, for each Σ^0_1 set U, there is a sequence of almost decidable sets (A_{i_k}) computable from U such that $U = \bigcup_k A_{i_k}$ a.e., and vice versa.

Whereas the measures of open balls are lower semi-computable, the measures of a.e. decidable sets are computable!

We will call this an μ-a.e decidable representation of (the topology) of (X, d, S).

Computable Randomness - Main Idea

1. Replace $2^{<\omega}$ with a suitable collection of a.e. decidable sets $\{A_i\}$.
2. Replace each σ with a Boolean combination of a.e. decidable sets.
3. Ignore the boundaries of these a.e. decidable sets. (Recall that these boundary points are not even Kurtz random!)

Computable Randomness on $(\mathscr{X}, \mu)$

Let (A_i) be a μ-a.e. decidable representation of (X, d, S).

If $\sigma \in 2^{<\omega}$ and $|\sigma| = k$, define $[\sigma]$ to be $A_0^{\sigma(0)} \cap \cdots \cap A_{k-1}^{\sigma(k-1)}$, where $A^0 = A$ and $A^1 = X \smallsetminus A$.

Write $\mu(\sigma)$ instead of $\mu([\sigma])$.

Computable Randomness on $(\mathscr{X}, \mu)$

Recall $[\sigma]$ is now a Boolean combination of a.e. decidable sets.

Definition

Let (U_n) be a computable sequence of Σ^0_1 sets.

- (U_n) is a bounded ML test (w.r.t. (A_i)) if there is a computable measure ν on 2^ω such that for all n and all $\sigma \in 2^{<\omega}$,
$$\mu(U_n \cap [\sigma]) \leq 2^{-n} \cdot \nu(\sigma).$$
- $x \in X$ is computably random (w.r.t. (A_i)) $\Leftrightarrow x \notin \bigcap_n U_n$ for any bounded ML test (U_n) and x is not in the boundary of A_i for any i.

Theorem (R.)

The above definition is invariant under the choice of the μ-a.e. decidable representation (A_i).

Applications

On 2^ω with fair-coin measure. The a.e. decidable sets are $A_i = \{X \mid X(i) = 1\}$. Then $[\sigma]$ has the same meaning. (So the definitions are the same.)

On $[0,1]$ with Lebesgue measure. The a.e. decidable sets can be picked so that each $[\sigma]$ is a dyadic interval. Then dyadic rationals are the boundary points. Can use bases other than binary, showing that computable randomness is base invariant (a "folklore" later proved by Bratkka-Miller-Nies).

On $[0,1]^n$ with the Lebesgue measure. $x \in [0,1]^n$ is computably random iff $x = (0.X_1, \ldots, 0.X_n)$ and $X_1 \oplus \cdots \oplus X_n$ is computably random in 2^ω.

Martingale Definition

Fix $(\mathscr{X}, \mu)$ and a μ-a.e. decidable representation (A_i).
Recall $[\sigma]$ is now a Boolean combination of a.e. decidable sets.

If x is not a boundary point, let $x \upharpoonright n$ be the unique σ such that $x \in [\sigma]$ and $|\sigma| = n$.

Theorem

Assume $x \in X$ is not a boundary point. Then $x \in X$ is computably random $\Leftrightarrow \limsup_n M(x \upharpoonright n) < \infty$ for all computable martingales $M : 2^{<\omega} \to \mathbb{R}^+$ such that

$$M(\sigma 0) \cdot \mu(\sigma 0) + M(\sigma 1) \cdot \mu(\sigma 1) = M(\sigma) \cdot \mu(\sigma)$$

(where $M(\sigma)$ is undefined if $\mu(\sigma) = 0$).

Many More Definitions

Computable randomness can also be defined using

- Integral tests
- Vitali covers (Solovay tests)
- Martingale convergence (many versions)
- Convergence of computable functions
- Differentiability
- Lebesgue differentiation theorem (for $[0,1]^n$)

Main ideas in all these definitions:

- Use objects which the generate the topology of the metric.
- These objects are “bounded locally” (compared with ML randomness where the objects are “bounded globally”).

Outline

Morphisms and Isomorphisms

Definition (Hoyrup and Rojas?)

Let $(\mathscr{X}, \mu)$ and $(\mathscr{Y}, \nu)$ be computable probability spaces.
A morphism $T : (\mathscr{X}, \mu) \to (\mathscr{Y}, \nu)$ is a map $T : X \to Y$ such that

- T is μ-a.e. computable (so T converges on Kurtz randoms),
- T is measure preserving, i.e. for all Borel $A \subseteq Y$

$$\mu(T^{-1}(A)) = \nu(A).$$

An isomorphism is a pair of morphisms $T : (\mathscr{X}, \mu) \to (\mathscr{Y}, \nu)$ and $S : (\mathscr{Y}, \nu) \to (\mathscr{X}, \mu)$ such that $S \circ T = id_X$ μ-a.e. and $T \circ S = id_Y$ ν-a.e. (so $S(T(x)) = x$ on all Kurtz randoms $x \in X$).

Theorem

All atomless computable probability spaces are isomorphic to 2^ω with the fair-coin measure.

Randomness and Morphisms

Theorem

Morphisms preserve weak-2 randomness, ML randomness, Schnorr randomness, and Kurtz randomness. Hence if $T : (\mathscr{X}, \mu) \to (\mathscr{Y}, \nu)$ is an isomorphism, then $x \in X$ is (W2/ML/Sch/Ktz) random if and only if $T(x)$ is.

Computable randomness is not preserved by morphisms...
...but it is still preserved by isomorphisms.

Theorem (R.)

Isomorphisms preserve computable randomness. Hence if $T : (\mathscr{X}, \mu) \to (\mathscr{Y}, \nu)$ is an isomorphism, then $x \in X$ is computably random if and only if $T(x)$ is.

Kolmogrov-Loveland Randomness

KL randomness is similar to computable randomness except one is allowed to choose which bit to bet on.

Open Question

Does ML randomness = KL randomness?

Schnorr's Critique (Paraphrased)

ML randomness is not computable/finitary enough.

Some see a positive answer to the open question as a negative answer to Schnorr's critique?

"Finitary" Betting Strategy for ML Rand.

Assume you are allowed to bet on any a.e. decidable property A of the string. You are paid according to the odds of this event occurring given what you already know about the string.

In other words, assume you know $x \in B$ and you bet that $x \in A$.

- If $x \in A$, you win $\mu((X \smallsetminus A) \cap B)/\mu(A \cap B)$ times your bet.
- If $x \notin A$, you lose all your bet.

Since A, B are both a.e. decidable, this is a "finitary" scenario.

Theorem (basically Merkle, Milhailović, Slaman)

The randomness notion characterized by this betting strategy is ML randomness. (Uses "martingale processes".)

Does this answer Schnorr's critique of ML randomness?

Endomorphism Random

Instead, assume you are only allowed to bet on probability $\frac{1}{2}$ events conditioned on what you already know. (Hence we are assuming that $(\mathscr{X},\mu)$ has no atoms.)

Call this randomness notion endomorphism random.

Theorem (R.)

Assume $(\mathscr{X},\mu)$ has no atoms. The following are equivalent.

- *$x \in X$ is endomorphism random*
- *for all endomorphisms $T : (\mathscr{X},\mu) \to (\mathscr{X},\mu)$, $T(x)$ is computably random.*
- *for all morphisms $T : (\mathscr{X},\mu) \to (2^\omega,$ fair coin measure$)$, $T(x)$ is computably random.*

Endomorphism Random

Instead, assume you are only allowed to bet on probability $\frac{1}{2}$ events conditioned on what you already know. (Hence we are assuming that $(\mathscr{X}, \mu)$ has no atoms.)

Call this randomness notion endomorphism random.

Observations.

- Endomorphism randomness is trivially base-invariant on $[0, 1]$.
- ML random $\Rightarrow$ endomorphism random $\Rightarrow$ KL random

Question.
Does endomorphism random equal ML random or KL random?

Thank You!

These slides are available on my webpage:

`math.cmu.edu/~jrute`

Or just Google me, “Jason Rute”.