Effective Randomness and Continuous Measures

Theodore A. Slaman
(on joint work with Jan Reimann)

University of California, Berkeley

July 26, 2010

Motivation

Question

For which sequences $X \in 2^\omega$ do there exist (representations of) continuous probability measures μ such that X is effectively random for μ?

Example

Different measures give different notions of randomness. Flipping a biased coin does not produce a random sequence for the uniform probability distribution, but it does give a random sequence for an appropriately weighted distribution.

In the above, we consider the following inverse problem.

> *Given the sequence X, find a distribution μ for which it is typical.*

Outline

1. Overview of the effective theory of randomness (for Lebesgue measure)
   1.1 Aspects of randomness, their recursion theoretic expressions, implications and equivalences
   1.2 Recursion theoretic properties of random reals
   1.3 Indications of other lines of active research
2. Randomness relative to non-uniform measures
   2.1 The general, possibly atomic, case. Constructions of measures by compactness.
   2.2 The continuous case. Constructions of continuous measures by metamathematics and transfer of randomness
3. Failures of continuous randomness
   3.1 Connections with definability, jump hierarchies and master codes
   3.2 Speculations

Effective Randomness for Lebesgue measure

topology

- *Cantor space.* 2^ω, the set of infinite binary sequences.
- *Open sets.*
  - For σ in $2^{<\omega}$, a finite binary sequence, $U_\sigma = \{X : \sigma \subset X\}$ is the open ball determined by σ.
  - Similarly, for $M \subseteq 2^{<\omega}$, $U_M = \cup_{\sigma \in M} U_\sigma$.
- *Measure.* λ represents Lebesgue measure. $\lambda(U_\sigma) = 1/2^{|\sigma|}$, where $|\sigma|$ is the length of σ.

Effective Randomness for Lebesgue measure

recursion theoretic definitions

Definition

- A set A is *recursive* iff there is an algorithm to determine membership in A.
  - Write $X \geq_T Y$ when Y is recursive relative to X.
- A is *recursively enumerable* iff it has a definition of the form $(\exists k_1, \ldots, k_n) P(k_1, \ldots, k_n)$, where all the numbers mentioned in P are explicitly bounded.
- A is *arithmetically definable* iff there is a definition of A expressed solely in terms of addition, multiplication, and quantification ($\exists$, $\forall$) within the natural numbers.

Effective Randomness for Lebesgue measure

recursion theoretic facts

- There is a $\geq_T$-greatest recursively enumerable subset of $\mathbb{N}$ denoted by $0'$ (the Halting Problem, the Turing jump, the Existential Theory of $\mathbb{N}$). Similarly, for any X, X' is the $\geq_T$-greatest set which is recursively enumerable relative to X.
- The arithmetically definable sets are obtained by starting with the empty set, iterating relative existential definability (i.e. the map $X \mapsto X'$), and closing under relative computability.

Randomness: Measure

In the measure theoretic foundation of randomness, being true of a random sequence is understood as being true almost everywhere, that is except for a set of measure 0.

This translates into the effective setting as follows. A sequence is random if it does not belong to any effectively presented set of measure 0.

Randomness: Measure

Definition

1. A *Martin-Löf test* is a uniformly recursively enumerable sequence $(M_n : n \geq 1)$ of subsets of $2^{<\omega}$ such that for each n, $\lambda(U_{M_n}) \leq 1/2^n$.
2. For $R \in 2^\omega$, R is *Martin-Löf random* or 1-random iff for every Martin-Löf test $(M_n : n \geq 1)$, $R \notin \cap_{n \geq 1} U_{M_n}$.

Here we have made precise the statement, R does not belong to any effectively presented null set.

Observations

Proposition

There is a universal Martin-Löf test. Any sequence that passes this particular test passes all Martin-Löf tests.

Example

- No eventually constant sequence is 1-random. Similarly, the binary representation of π is not 1-random.
- There is a sequence R which is recursive in $0'$ and 1-random.
- (Good enough for Monte Carlo) No recursive betting strategy wins against a 1-random sequence.

Randomness: Complexity

In the information theoretic formulation of randomness, a sequence is random if it exhibits no recognizable patterns.

Kolmogorov (and others) translated this into the effective setting as follows. A sequence is random if for each n the shortest program to describe the first n-bits of the sequence is roughly of size n.

Randomness: Complexity

Definition

For f a partial function from $2^{<\omega}$ to $2^{<\omega}$, f is *prefix free* iff the domain of f is an antichain.

We obtain natural examples of prefix-free functions on $2^{<\omega}$ from recursive functions on 2^{ω} by considering the uses of their convergent computations. $f(a)\downarrow$ indicates that a is in the domain of f.

Randomness: Complexity

Definition

Suppose that f is a prefix-free recursive function.

1. If b is in the range of f then the *f-complexity of b* is the least $|a|$ where $f(a) = b$. Otherwise, the f-complexity of b is ∞. We write $H_f(b)$ for the f-complexity of b.
2. The *halting probability* of f is $\Sigma_{f(a)\downarrow} 1/2^{|a|}$. The halting probability of f is a real number in $[0, 1]$. Identify such reals as elements of 2^ω.

Randomness: Complexity

Definition

A recursive function u is *universal* iff the following conditions hold:

1. u is prefix-free
2. For any prefix-free recursive function f there is a constant C such that for all a, $H_u(a) \leq H_f(a) + C$.

Proposition

There is a universal function.

Randomness: Complexity

Definition

For $R \in 2^\omega$, R is *Kolmogorov-random* iff there is a universal function u and a constant C such that for all n, $H_u(R \upharpoonright n) > n - C$.

This definition is the technically precise version of the statement, It takes roughly n bits of data to describe $R \upharpoonright n$.

Randomness: Equivalence

It is straightforward to check that Martin-Löf-random reals are Kolmogorov-random. Schnorr proved the converse.

Theorem (Schnorr)

For every $R \in 2^\omega$, if R is Kolmogorov-random then R is Martin-Löf random.

Henceforth, we will simply say that R is 1-random.

Randomness: Equivalence

Miller and Yu have given an more penetrating calculation of the initial segment complexity for 1-random sequences.

Theorem (Miller and Yu)

If R is 1-random, then $\sum_{n\in\omega} 2^{n-H_u(R\restriction n)} < \infty$.

Randomness: Equivalence

Some aspects of randomness are simply expressed by means of string complexity.

Example

Suppose that the sequence A is the characteristic function of a recursively enumerable set W. Then, A is not 1-random.

Proof.

For any n, $A \upharpoonright n$ is recursively described by specifying n and the cardinality of $W \bigcap n$, hence has a description of length approximately $\log(n)$. $\square$

K-trivial sequences

an aside

There have been a remarkable sequence of developments due to Chaitin and Solovay, then more recently Nies, Hirschfeldt, Kučera, and others, centered on the following class of sequences.

Definition

$A \in 2^\omega$ is K-*trivial* iff there is a constant k such that for all n, $H(A \upharpoonright n) < H(0^n) + k$. That is, $A \upharpoonright n$ is no more complex than n.

Remarkably, there are countably many K-trivials, some not recursive and all Δ^0_2. It's an interesting story, and there is a lot to tell.

Chaitin's Ω-numbers

Chaitin provided a class of natural examples of 1-random reals.

Definition (Chaitin)

An Ω-*number* is the halting probability of a universal function.

Theorem (Chaitin)

Every Ω-number is 1-random.

Recursive Enumerability

The Ω-numbers have monotonically recursive approximation. Reals with this property are called left-recursively enumerable reals.

Definition

For $A \in 2^\omega$, A is *left-recursively enumerable* iff there is a lexicographically nondecreasing recursive sequence $(a_n : n \in \omega)$ such that $\lim_{n \to \infty} a_n = A$.

Recursive Enumerability

By the previous slide, there are left-recursively enumerable reals, the Ω-numbers, which are 1-random.

Intuitively, random reals should be very difficult to approximate. This is the case, as we will make precise in the next few slides.

Recursive Enumerability

Suppose that the lexicographically nondecreasing recursive sequence $(a_n : n \in \omega)$ satisfies $\lim_{n\to\infty} a_n = A$.

Then, $(a_n : n \in \omega)$ gives a stage-by-stage approximation to A. At stage n, the *error* in the approximation is $\epsilon(n) = |A - a_n|$.

Recursive Enumerability

Definition (Solovay)

Let $(a_n : n \geq 1)$ and $(b_n : n \geq 1)$ be recursive lexicographically nondecreasing sequences in $2^{<\omega}$ which converge to A and B, respectively.

1. $(a_n : n \geq 1)$ *dominates* $(b_n : n \geq 1)$ iff there is a positive constant C such that for all n, $C(A - a_n) > (B - b_n)$, viewed in $[0, 1]$.
2. $(a_n : n \geq 1)$ is *universal* if it dominates every such recursive sequence.

RE: Complexity

Definition

A is Ω-*like* iff it is the limit of a universal recursive sequence.

Theorem (Solovay)

If A is Ω-like then A is 1-random.

Theorem (Kučera and Slaman)

If A is left-recursively enumerable and 1-random then A is Ω-like.

Thus, we obtain another characterization of randomness. Among left-recursively enumerable reals, the random ones are those which are the most difficult to approximate.

Recursion Theoretic Aspects of Random Reals

Theorem (Sacks)

If $X \in 2^\omega$ and $\{Y : Y \geq_T X\}$ has positive measure, then X is recursive.

Recursion theoretically, one should expect that random reals have no arithmetic/logical information that falls within the scope of their degree of randomness.

Being 1-random is not enough.

Theorem (Kučera, Gács)

Every set X such that $X \geq_T 0'$ is Turing equivalent to a 1-random set.

Higher Order Randomness

We can make Martin-Löf tests more powerful by requiring that the test sequence U_n is recursively enumerable relative to an oracle A, in which case we say that R is 1-random relative to A.

Definition

R is *n-random* iff R is 1-random relative to $0^{(n)-1)}$.

Many of the measure-theoretic anomalies which can be exhibited by (merely) 1-random reals disappear when one considers 2-randoms. See results of Miller and Nies.

Properties of Random Reals

Suppose that $n \geq 2$, $Y \in 2^\omega$, and R is n-random.

Proposition

If i is less than n, Y is recursive in R and recursive in $0^{(i)}$, then Y is recursive.

Proof.

Suppose Y is not recursive. For each Turing functional Φ, by Sacks's Theorem, the set of X such that $\Phi(X) = Y$ has measure 0. Thus, for each n, there is an m_n such that the set of σ such that $\Phi(\sigma) \upharpoonright m_n = Y \upharpoonright m_n$ specifies an open set U_n of measure less than 2^n. This sequence of open sets is uniformly recursively enumerable relative to $0^{(i+1)}$. Thus, if $\Phi(R) = Y$, then R is not $(i+1)$-random. □

In general, a random real cannot accelerate arithmetic definability.

Properties of Random Reals

Definition

A linear order $\prec$ on ω is *well-founded* iff every non-empty subset of ω has a least element.

As with arithmetic definability, random reals cannot accelerate the calculation of well-foundedness.

Theorem

Suppose that X is 5-random relative to μ, $\prec$ is recursive in μ, and I is the largest initial segment of $\prec$ which is well-founded. If I is recursive in $X \oplus \mu$, then I is recursive in μ.

Properties of Random Reals

We have seen that random reals do not accelerate definitions of arithmetic sets and do not accelerate the calculation of well-foundedness.

However, they do have common structural information.

Theorem (Greenberg, Montalbán, and Slaman)

There is a first order structure M with the following properties.

- *M has no hyperarithmetic representation.*
- *Every non-hyperarithmetic real can compute a representation of M.*

Hence, M is recursively represented relative to every element of a measure one set, but not hyperarithmetically represented.

Next Time

Next time, we will analyze randomness relative to non-uniform distributions.

We will develop methods by which X's being recursively equivalent to a random real R can be used to transfer R's randomness relative to the uniform distribution to X's being random relative to a transformed distribution.