Effective Randomness and Continuous Measures

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

University of California, Berkeley

October 8, 2010

Mathematical Logic and Randomness

Question

What insight can Mathematical Logic provide into the mathematical understanding and application of randomness?

Caveat.

- Randomness is a primitive mathematical concept, like size, shape, number, or proof.
- We will not be able to capture it, but we will investigate its descriptive properties.
  - What does it mean to look random?
  - What limits are there to the applicability of a random source?

The Form of our Investigation

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.*

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, $[\sigma] = \{X : \sigma \subset X\}$ is the open ball determined by σ.
  - Similarly, for $M \subseteq 2^{<\omega}$, $[M] = \cup_{\sigma \in M}[\sigma]$.
- *Measure.* λ represents Lebesgue measure. $\lambda([\sigma]) = 1/2^{|\sigma|}$, 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.

Effective Randomness for Lebesgue Measure

Definition (Martin-Löf)

A sequence R is *effectively random or 1-random* iff it does not belong to any effectively-presented set of measure 0.

- Here, we are formalizing the intuition that the properties of randomness are those which hold almost everywhere.
- We are identifying property with definable set and a real's being random with its having all the properties of randomness.

Effective Randomness for Lebesgue Measure

More technically,

R is 1-random iff whenever $(M_n : n \in \mathbb{N})$ is a uniformly recursively enumerable sequence such that each $[M_n]$ has measure less than $1/2^n$, it is the case that $R \notin \bigcap_n [M_n]$.

So, a random R must avoid every effectively-presented, null, G_δ subset of 2^ω.

Example

- No eventually constant sequence is effectively random.
- The binary representation of π is not effectively random.

Similarly, R is $(n+1)$-random iff it does not belong to any $0^{(n)}$-presented G_δ set of measure 0.

Representations of Measures

Definition

A *representation* m of a probability measure μ on 2^ω provides rational approximations to each $\mu([\sigma])$ meeting any required accuracy.

Definition

$X \in 2^\omega$ is $(n+1)$-random relative to a representation m of μ if and only if it does not belong to any $m^{(n)}$-presented G_δ set of μ-measure 0.

We will drop the explicit reference to presentations and speak of randomness relative to μ.

The Precise Question

Question

For which sequences $X \in 2^\omega$ do there exist continuous probability measures μ such that X is n-random for μ?

We will show *for all but countably many*, but the proof takes some interesting turns.

Continuous Measures

degree theoretically characterizing relative randomness

It is useful to work with a sequence-based recursion-theoretic characterization of relative continuous randomness.

Definition

- For X, Y, and Z in 2^ω, we write $X \equiv_{T,Z} Y$ to indicate that there are Turing reductions (i.e. representations of continuous functions) Φ and Ψ which are recursive in Z such that $\Phi(X) = Y$ and $\Psi(Y) = X$.
- When Φ and Ψ have domain 2^ω, we write $X \equiv_{tt,Z} Y$.

Turing reductions correspond to continuous functions defined on subsets of 2^ω. Truth-table (tt) reductions correspond to continuous functions defined on all of 2^ω.

Continuous Measures

degree theoretically characterizing relative randomness

Proposition

For X and Z in 2^ω, the following conditions are equivalent.

- *There is a continuous measure μ which is recursive in Z such that X is n-random for μ and Z.*
- *There is a continuous dyadic measure μ which is recursive in Z such that X is n-random for μ and Z.*
- *There is an R such that R is n-random relative to Z and an order preserving homeomorphism $f : 2^\omega \to 2^\omega$ such that f is recursive in Z and $f(R) = X$.*
- *There is an R such that R is n-random relative to Z and $X \equiv_{tt,Z} R$.*

Constructing continuous measures

In order to conclude that X is n-random relative to some continuous measure, it is sufficient to find a Z relative to which X is computationally equivalent to some n-random sequence R.

Theorem (Martin, Borel Determinacy)

Suppose that $\mathcal{B}$ is a Borel subset of 2^ω and that for every A there is a Y such that $Y \geq_T A$ and $Y \in \mathcal{B}$. There is a $B \in 2^\omega$ such that for every $X \geq_T B$ there is a Y such that $Y \equiv_T X$ and $Y \in \mathcal{B}$.

Corollary

For any $n \in \mathbb{N}$, there is a B such that for all $X \geq_T B$, there is a continuous measure μ such that X is n-random relative to μ.

Constructing continuous measures

the first interesting turn

- In Martin's proof, the later $\mathcal{B}$ appears in the Borel hierarchy, the more iterates of the power set of $\mathbb{R}$ are used in producing the B such that $X's$ computing B have $\equiv_T$-equivalents in $\mathcal{B}$.
- Martin's proof implies that if G is a real parameter used to define a Borel game $\mathcal{B}$, then the B for that game belongs to the smallest countable model of a sufficiently large subset of ZFC, the axioms of set theory.

Constructing continuous measures

Fix n and let $L_{\lambda(n)}$ be the smallest countable model satisfying ZFC^-, set theory without the power set axiom, and the existence of n-iterates of the power set applied to $\mathbb{R}$.

Theorem

Suppose that $X \notin L_{\lambda(n)}$. Then there is a G such that

- *$L_{\lambda(n)}[G]$ is a model of ZFC^- and the existence of n-iterates of the power set applied to $\mathbb{R}$.*
- *Every element of $2^\omega \bigcap L_{\lambda(n)}[G]$ is recursive in $X + G$.*

Consequently, if $X \notin L_{\lambda(n)}$, then relative to G, X is in the set of relatively random reals.

Constructing continuous measures

Theorem

For any X which is not in $L_{\lambda(n)}$, there is a continuous measure μ such that X is n-random relative to μ.

Theorem (Co-countability)

For all n, for all but countably many $X \in 2^\omega$ there is a continuous measure μ such that X is n-random relative to μ.

Necessity of power sets

the second interesting turn

The proof invoked infinitely many iterates of the power set in the form of Borel Determinacy. By work of H. Friedman, these are necessary in the proof of Borel Determinacy.

We will show that the infinitely many iterates of the power set cannot be removed from the analysis of relative randomness.

Necessity of power sets

How do you prove such a thing?

- To show that the axioms of group theory do not prove that the group operation commutes, exhibit a nonabelian group.
- To show that the axioms of set theory with k-many iterates of the power set of $\mathbb{R}$ do not prove the Co-countability Theorem, exhibit a structure satisfying these axioms in which the Co-countability Theorem fails.

We need a few more facts about random sequences and a few more about set theory.

Necessity of power sets

A little more about random sequences

Suppose that $n \geq 2$, $Y \in 2^\omega$, and X is n-random relative to μ.

If i is less than n, Y is recursive in $(X \oplus \mu)$ and recursive in $\mu^{(i)}$, then Y is recursive in μ.

In general, using arithmetic definitions with fewer than n quantifiers, n-random reals do not accelerate arithmetic definability.

Necessity of power sets

A connection between failure of randomness and definability

If X is μ-random then $\mu + X$ cannot simplify the descriptions of μ-definable sets.

Example

For all k, $0^{(k)}$ is not 2-random relative to any μ.

Proof.

- Say $0^{(k)}$ is 2-random relative to μ.
- $0'$ is recursively enumerable in μ and recursive in the supposedly 2-random $0^{(k)}$. Thus, $0'$ is recursive in μ and, thereby, $0^{(2)}$ is recursively enumerable in μ.
- Use induction to conclude $0^{(k)}$ is recursive in μ, a contradiction.

□

Necessity of power sets

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.

Necessity of power sets

Definition

Gödel's hierarchy of constructible sets L is defined by the following recursion.

- $L_0 = \emptyset$
- $L_{\alpha+1} = Def(L_\alpha)$, the set of subsets of L_α which are first order definable in parameters over L_α.
- $L_\lambda = \cup_{\alpha<\lambda} L_\alpha$.

Necessity of power sets

a little more about set theory

We focus on the least ordinal λ such that L_λ satisfies ZFC^-.

- For $\beta < \lambda$, L_β is a countable structure obtained by iterating first order definability over smaller L_α's and taking direct limits.
- There is a sequence $M_\beta \in 2^\omega \bigcap L_\lambda$, for $\beta < \lambda$, of representations these countable structures.
    - M_β is obtained from smaller M_α's by iterating the Turing jump and taking arithmetically definable direct limits.
    - Every $X \in 2^\omega \bigcap L_\lambda$ is recursive in some M_β.

Master Codes and Effective Randomness

failures of continuous randomness

Theorem

There is an n such that for all $\beta \in LOR$, if $\beta < \lambda$ then there is no continuous measure μ such that M_β is n-random relative to μ.

Corollary

ZFC^- does not prove the Co-countability Theorem.

Master Codes and Effective Randomness

failures of continuous randomness—outline of proof

Suppose that M_β were n-random relative to μ.

- Let $\mathcal{M}$ be the sequence of possible Master Codes which are recursive in μ.
  - The well-founded part of $\mathcal{M}$ is of the form $\mathcal{M}_{<\gamma} = (M_\alpha : \alpha < \gamma)$ for some $\gamma \leq \beta$.
  - $\mathcal{M}_{<\gamma}$ is uniformly arithmetically definable from M_β and hence from μ.
- M_γ is obtained by iterating uniformly arithmetically definable operations on $\mathcal{M}_{<\gamma}$.
- The results at each step and M_γ itself are recursive in M_β.
- The results at each step and M_γ itself are recursive in μ.
- M_γ is in the well-founded part of $\mathcal{M}$. Contradiction.

Master Codes and Effective Randomness

failures of continuous randomness

The higher iterates of the power set make it more complicated to define $\mathcal{M}$ and to define the process to go from $\mathcal{M}_{<\gamma}$ to M_γ.

Consequently, the failure of randomness for the M_β's for these models is more complicated to describe.

Even so, for each n, the first initial segment of L satisfying ZFC^- and there are k iterates of the power set of $\mathbb{R}$ does not satisfy the Co-countablity Theorem.

Finis

There is a deep and poorly-understood connection between the iterative hierarchy of definability, meta-mathematics, and randomness.