The Metamathematics of Randomness

Jan Reimann
(joint work with Theodore Slaman)

June 30, 2007

Question

Which reals are random with respect to
a (continuous) probability measure?

The answer to this question takes an unexpected turn.

- Cantor space 2^ω, elements are reals.
- Finite initial segments $2^{<\omega}$, strings.
- The (partial) prefix order on $2^{<\omega} \cup 2^\omega$ is denoted by $\subseteq$.
- The basic clopen cylinder induced by a string σ is

$$N_\sigma := \{x \in 2^\omega : \sigma \subset x\}.$$

If $C \subseteq 2^{<\omega}$, we write N_C to denote the open set

$$N_C = \bigcup_{\sigma \in C} N_\sigma.$$

- Borel probability measure on 2^ω: countably additive, monotone function $\mu : \mathcal{B} \to [0,1]$, $\mathcal{B}$ the Borel sets, and $\mu(2^\omega) = 1$.
- Basic result of measure theory: measure is uniquely determined by the values on algebra $\mathcal{A} \subseteq \mathcal{B}$ that generates $\mathcal{B}$.
- Borel sets of 2^ω are generated by the algebra of clopen sets, i.e. finite unions of cylinders.
- Normalized, monotone, countably additive set functions on the algebra of clopen sets are induced by any function $\rho : 2^{<\omega} \to [0,1]$ satisfying $\rho(\emptyset) = 1$ and

$$\forall \sigma \, [\rho(\sigma) = \rho(\sigma^\frown 0) + \rho(\sigma^\frown 1)]$$

- Lebesgue measure $\mathcal{L}$: distribute a unit mass uniformly along the paths of 2^ω, i.e. set $\mathcal{L}(N_\sigma) = 2^{-|\sigma|}$.
- Dirac measure δ_x: put a unit mass on a single real, i.e. for $x \in 2^\omega$, let
$$\delta_x(\sigma) = \begin{cases} 1 & \text{if } \sigma \subset x, \\ 0 & \text{otherwise.} \end{cases}$$
- If, for a measure μ and $x \in 2^\omega$, $\mu(\{x\}) > 0$, then x is called an atom of μ.
- A measure that does not have any atoms is called continuous.

An immeadiate consequence of G_δ-regularity:

- $\mu(A) = 0$ iff there exists a sequence $(W_n)_{n \in \omega}$, $W_n \subseteq 2^{<\omega}$, such that for all n,

$$A \subseteq \bigcup_{\sigma \in W_n} N_\sigma \quad \text{and} \quad \sum_{\sigma \in W_n} \rho(\sigma) \leqslant 2^{-n}.$$

Thus,

every nullset is contained in a G_δ nullset.

By requiring that the covering nullset is effectively G_δ, we obtain a notion of effective nullsets.

Definition

- A test relative to $z \in 2^\omega$ is a set $W \subseteq \mathbb{N} \times 2^{<\omega}$ which is r.e. (Σ^0_1) in z.
- A real x passes a test W if $x \notin \bigcap_n N(W_n)$, where $W_n = \{\sigma : (n, \sigma) \in W\}$.

Hence a real passes a test W if it is not in the G_δ-set represented by W.

To test for randomness with respect to a measure μ, we want to ensure that W actually describes a nullset for μ.

Definition

Suppose μ is a measure on 2^ω. A test W is correct for μ if for all n,

$$\sum_{\sigma \in W_n} \mu(N_\sigma) \leqslant 2^{-n}.$$

Any test which is correct for μ will be called a test for μ.

An effective test for randomness should have access to the measure it is testing for.

- Therefore, represent it by an infinite binary sequence.
- It suffices to represent the values on cylinders.

Definition

Given a measure μ, define its rational representation r_μ by letting, for all $\sigma \in 2^{<\omega}$, $q_1, q_2 \in \mathbb{Q}$,

$$\langle \sigma, q_1, q_2 \rangle \in r_\rho \;\Leftrightarrow\; q_1 < \mu(\sigma) < q_2.$$

We will need to make use of the topological properties of the space of probability measures.

- If a space X is Polish, so is the space $\mathcal{P}(X)$ of all probability measures on X (under the weak topology). Also, if X is compact metrizable, so is $\mathcal{P}(X)$.
- This yields various ways to represent a measure: Cauchy sequences, list of basic open balls it is contained in, etc.
- We can obtain a nice effective representation (e.g. by following the framework in Moschovakis' book).

Theorem

There is a recursive surjection $\pi : 2^\omega \to \mathcal{P}(2^\omega)$ and a Π^0_1 subset P of 2^ω such that $\pi\restriction_P$ is one-to-one and $\pi(P) = \mathcal{P}(2^\omega)$.

Definition

Suppose μ is a measure with a representation ρ_μ and $z \in 2^\omega$. A real is μ-random relative to z and ρ_μ if it passes all $\rho_\mu \oplus z$-tests which are correct for μ.

Hence, a real x is random with respect to an arbitrary measure μ if and only if it passes all tests which are enumerable in the representation ρ_μ of μ.

- n-randomness: tests r.e. in $\rho_\mu^{(n-1)}$.
- Accordingly, define arithmetical randomness.

Obviously, every real x is trivially random with respect to μ if $\mu(\{x\}) > 0$, i.e. if x is an atom of μ.

Question

Which reals are non-trivially random with respect to some measure?

It turns out: precisely the non-recursive reals.

Theorem

For any real x, the following are equivalent.

(i) *There exists (a representation of) a measure μ such that $\mu(\{x\}) = 0$ and x is 1-random for μ.*

(ii) *x is not computable.*

Features of the proof:

- Conservation of randomness.
- A cone of random reals.
- Relativization using the Posner-Robinson Theorem.
- A basis theorem for relative randomness for Π^0_1 sets of reals.

Let μ be a probability measure and $f : 2^\omega \to 2^\omega$ be a continuous (Borel) function.

Define the image measure μ_f by setting

$$\mu_f(\sigma) = \mu(f^{-1}N_\sigma)$$

Conservation of randomness

If the transformation f is recursive in z, then it preserves randomness, i.e. it maps a μ-z-random real to a μ_f-z-random one.

Kucera's coding argument:

- Every degree above $\emptyset'$ contains a $\mathcal{L}$-random.

Relativization:

- Posner-Robinson Theorem: For every non-recursive real x there exists a G such that $x \oplus G \geqslant_T G'$, i.e. relative to G, x is above the jump.

Conclude that every non-recursive real x is Turing equivalent to some $\mathcal{L}$-G-random real R for some real G.

The Turing equivalence to a $\mathcal{L}$-random real translates into an effectively closed set of probability measures.

- The following basis theorem (indep. by Downey, Hirschfeldt, Miller, and Nies) ensures that one of the measures will not affect the randomness of R.

Theorem

If $B \subseteq 2^\omega$ is nonempty and Π^0_1, then, for every R which is $\mathcal{L}$-random there is $z \in B$ such that R is $\mathcal{L}$-z-random.

- This argument seems to be applicable in more generality, proving existence of measures.

Randomness for Continuous Measures

In the proof there is no control over the measure that makes x random.

- Atoms cannot be avoided (due to the use of Turing reducibilities).

Question

What if one admits only continuous probability measures?.

One can analyze the proof of the previous theorem to obtain the following characterization of continuous randomness.

Theorem

Let x be a real. For any $z \in 2^\omega$, the following are equivalent.

(i) x *is random for a continuous (dyadic) measure recursive in* z.

(ii) *There exists a functional* Φ *recursive in* z *which is an order-preserving homeomorphism of* 2^ω *such that* $\Phi(x)$ *is* λ-z-*random.*

(iii) x *is truth-table equivalent (relative to* z*) to a* $\mathcal{L}$-z-*random real.*

This is an effective version of the classical isomorphism theorem for continuous probability measures.

The Class NCR

Question

Which level of logical complexity guarantees continuous randomness?

Let NCR_n be the set of all reals which are not n-random with respect to any continuous measure.

- Kjos-Hanssen and Montalban: Every member of a countable Π^0_1 class is contained in NCR_1. (It follows that elements of NCR_1 is cofinal in the hyperarithmetical Turing degrees.)
- Woodin: outside Δ^1_1 the Posner-Robinson theorem holds with tt-equivalence.
- Conclude that $\mathrm{NCR}_1 \subseteq \Delta^1_1$. (This can also be obtained by analyzing the complexity of winning strategies of Borel games, as we will see later.)

Upper Bounds for Continuous Randomness

What is the nature of NCR_n for arbitrary n?

Theorem

For all n, NCR_n is countable.

- Produce an upper cone in the Turing degrees of reals that are random for a continuous measure.
- Generalize the Posner-Robinson-Theorem to cases of higher complexity.

Show that the complement of NCR_n contains an upper Turing cone.

- Show that the complement of NCR_n contains a Turing invariant and cofinal (in the Turing degrees) Borel set.
- We can use the set of all x that are Turing equivalent to some $z \oplus R$, where R is $(n+1)$-random relative to a given z.
- These x will be n-random relative to some continuous measure and are T-above z.
- Use Martin's result on Borel Turing determinacy to infer that the complement of NCR_n contains a cone.
- The cone is given by the Turing degree of a winning strategy in the corresponding game.

Martin's proof of Borel determinacy starts with a description of a Borel game and constructs a winning strategy for one of the players.

- One can show that the winning strategy (for Borel complexity n) is contained in L_{β_n}, where β_n is the least ordinal such that

$$L_{\beta_n} \models \mathrm{ZFC}_n^-$$

where ZFC_n^- is Zermelo-Fraenkel set theory without the Power Set Axiom $+$ "there exist n many iterates of the power set $\mathcal{P}(\omega)$".

L_{β_n} is countable.

- Hence, if we can find a Posner-Robinson-style relativization, we can show that
$$\mathrm{NCR}_n \subseteq L_{\beta_n}.$$

Given $x \notin L_{\beta_n}$, we construct a set G such that

(i) $L_{\beta_n}[G]$ is a model of ZFC_n^-.

(ii) For all $y \in L_{\beta_n}[G] \cap 2^\omega$, $y \leqslant_T x \oplus G$.

G is constructed by Kumabe-Slaman forcing.

The existence of G allows to conclude:

- If x is not in L_{β_n}, it will belong to every cone with base in the accordant $L_{\beta_n}[G]$.
- In particular, it will belong to the cone given by Martin's argument (relativized to G – use absoluteness), i.e. the cone avoiding NCR_n.
- Hence x is n-random relative to G for some continuous μ, hence in particular μ-n-random.

Question

Do we need to use metamathematical methods (L_{β_n}) to prove the countability of NCR_n?

We make fundamental use of Borel determinacy; this suggests to analyze the metamathematics in this context.

The necessity of iterates of the power set is known from a result by Friedman.

- The more complicated the game is in the Borel hierarchy, the more iterates of the power set of the continuum are used in producing the winning strategy – auxiliary games have as moves trees, trees of trees, etc.

Theorem (Friedman)

$\mathrm{ZFC}^- \nvdash$ *All $\mathbf{\Sigma}^0_5$-games on countable trees are determined.*

Martin improved this to $\mathbf{\Sigma}^0_4$.

Friedman goes on to show that in order to prove full Borel determinacy, a result about sets of reals, one needs the existence of infinitely many iterates of the power set of the continuum.

- The proof works by showing that there is a model of ZFC^- for which $\mathbf{\Sigma}^0_4$-determinacy does not hold.
- This model is L_{β_1}.

We can proof a similar result concerning the countability of NCR_n.

Theorem

For every k,

$$\mathsf{ZFC}^-_k \nvdash \text{"For every } n,\ \mathsf{NCR}_n \text{ is countable"}.$$

The proof for $k = 1$ shows that for some n, NCR_n is not countable in L_{β_1}.

- Show that there is an n such that NCR_n is cofinal in the Turing degrees of L_{β_1}.
- The witnesses for NCR_n are Jensen's master codes of models L_α for limit ordinals $\alpha < \beta_1$.

This approach does not change for higher k.

For $n \geqslant 2$, random reals do not have a lot of computational/descriptive power.

- Random reals are not helpful when adding them as oracles/parameters.

Lemma

Suppose that $n \geqslant 2$, $y \in 2^\omega$, and R is $\mathcal{L}$-n-random relative to μ. If $i < n$, y is recursive in $(R \oplus \mu)$ and recursive in $\mu^{(i)}$, then y is recursive in μ.

Corollary: For all k, $\emptyset^{(k)}$ is not n-random relative to any μ, $n \geqslant 2$.

- Suppose $\emptyset^{(k)}$ is n-random relative to μ.
- $\emptyset'$ is recursively enumerable relative to μ and recursive in the supposedly n-random $\emptyset^{(k)}$. Hence, $\emptyset'$ is recursive in μ and so $\emptyset''$ is recursively enumerable relative to μ.
- Use induction to conclude $\emptyset^{(k)}$ is recursive in μ, a contradiction.

As with arithmetic definability, for $n \geqslant 5$, n-random reals cannot accelerate the calculation of well-foundedness.

Lemma

Suppose that x is 5-random relative to μ, $\prec$ is a linear ordering 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.

Building L: In the following, assume α is a limit ordinal (closure properties)

- For $\alpha < \beta_1$, L_α is a countable structure obtained by iterating first order definability over smaller L_γ's and taking unions.

Jensen's Master Codes are a sequence $M_\alpha \in 2^\omega \cap L_{\beta_1}$, for $\alpha < \beta_1$, of representations of these countable structures.

- M_α is obtained from smaller M_γ's by iterating the Turing jump and taking arithmetically definable direct limits.
- Every $x \in 2^\omega \cap L_{\beta_1}$ is recursive in some M_α.

Use the non-helpfulness properties of random reals to show that a sequence of M_α's (which are "extremely helpful") cannot be continuously random.

Theorem

There is an n such that for all limit α, if $\alpha < \beta_1$, then there is no continuous measure μ such that M_α is n-random relative to μ.