Randomness in Logic

Jan Reimann

Outline of the Course

Lecture 1: Martin-Löf tests and martingales.

Lecture 2: Kolmogorov complexity.

Lecture 3: The computational power of randomness.

Lecture 4: Randomness for non-uniform distributions.

Lecture 5: The Metamathematics of randomness.

Outline of Lectures 4 and 5

Randomness for Non-Uniform Distributions and Metamathematics

- Randomness for Arbitrary Probability Measures.
- Randomness and Computability.
- Continuous Probability Measures.
- Higher Randomness for Continuous Measures.
- Randomness and Iterates of the Power Set.

Measures on Cantor Space

Definition

A measure on $2^{\mathbb{N}}$ is a function $\mu : 2^{<\mathbb{N}} \to [0, \infty)$ such that for all $\sigma \in 2^{<\mathbb{N}}$

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

If $\mu(2^{\mathbb{N}}) = \mu(\epsilon) = 1$, μ is a probability measure.

The Caratheodory Extension Theorem ensures that μ has a unique extension to the family of all Borel sets.

In the following, all measures are assumed to be probability measures.

Borel Sets

The Borel sets are obtained from open sets by closing under complementation and countable unions.

- The Borel sets can be ordered according their topological complexity: open/closed sets, intersections of open sets/unions of closed sets, unions of intersections of ....
- This yields a hierarchy, the Borel hierarchy, similar to the arithmetical hierarchy for sets of natural numbers: $\exists/\forall$, $\exists\forall/\forall\exists$, $\exists\forall\exists/\forall\exists\forall$, ...

Borel Sets

The Borel sets are obtained from open sets by closing under complementation and countable unions.

- The Borel sets can be ordered according their topological complexity: open/closed sets, intersections of open sets/unions of closed sets, unions of intersections of ....
- This yields a hierarchy, the Borel hierarchy, similar to the arithmetical hierarchy for sets of natural numbers: $\exists/\forall$, $\exists\forall/\forall\exists$, $\exists\forall\exists/\forall\exists\forall$, ...

Representation of measures

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

- Therefore, represent it by an infinite binary sequence.
- A measure on $2^{\mathbb{N}}$ is completely determined by its values on the cylinder sets, so represent these values via approximation by rational intervals.

Definition

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

$$\langle \sigma, q_1, q_2 \rangle \in r_\mu \iff q_1 < \mu(\sigma) < q_2.$$

Definition

Let μ be a probability measure on $2^{\mathbb{N}}$.

- A μ-test relative to $Z \in 2^{\mathbb{N}}$ is a set $W \subseteq \mathbb{N} \times 2^{<\mathbb{N}}$ which is recursively enumerable in $Z \oplus r_\mu$ such that

  $$\sum_{\sigma \in W_n} \mu([\sigma]) \leq 2^{-n},$$

  where $W_n = \{\sigma : (n, \sigma) \in W\}$
- A sequence X passes a test W if $x \notin \bigcap_n [W_n]$.
- A sequence X is μ-random relative to Z if X passes all μ-tests relative to Z.

Relative Randomness for Probability Measures

As with Lebesgue measure, we can relativize μ-randomness.

- Given $Z \in 2^{\mathbb{N}}$, require for a μ-test relative to Z that W is enumerable in $r_\mu \oplus Z$.
- For μ-n-randomness relative to Z, require that W is enumerable in $(r_\mu \oplus Z)^{(n)}$.

Question: Does randomness for arbitrary measures differ fundamentally from randomness for λ?

Atomic Measures

Trivial Randomness

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

If we rule out trivial randomness, then being random means being non-computable.

Theorem [Reimann and Slaman]

For any sequence X, the following are equivalent.

- There exists a measure μ such that $\mu(\{X\}) = 0$ and X is μ-random.
- X is not computable.

Making Sequences Random

Features of the proof

- Conservation of randomness.
  If Y is random for Lebesgue measure λ, and $f : 2^{\mathbb{N}} \to 2^{\mathbb{N}}$ is computable, then $f(Y)$ is random for λ_f, the image measure.
- A cone of λ-random sequences.
  By the Kucera-Gacs Theorem, every real above $0'$ is Turing equivalent to a λ-random real.
- Relativization using the Posner-Robinson Theorem.
  If a real is not computable, then it is above the jump relative to some G.
- A compactness argument for measures.

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

Define the image measure μ_f by setting

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

Conservation of randomness

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

Non-trivial Randomness

Cones and relativization

Kucera's coding argument:

- Every degree above $\emptyset'$ contains a λ-random.

Relativization:

- Posner-Robinson Theorem: For every non-computable sequence X there exists a G such that $X \oplus G \geq_T G'$, i.e. relative to G, X is above the jump.

Conclude that every non-computable sequence X is Turing equivalent to some λ-G-random sequence R for some real G.

Non-Trivial Randomness

Making reals random

The Turing equivalence to a λ-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 $B \subseteq 2^{\mathbb{N}}$ is nonempty and Π^0_1, then, for every R which is λ-random there is $Z \in B$ such that R is λ-Z-random.

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

Randomness for Continuous Measures

In the proof we have little control over the measure that makes x random.

- In particular, atoms cannot be avoided (due to the use of Turing reducibilities).

Question

What if one admits only continuous (i.e. non-atomic) probability measures?.

The Class NCR

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

Question

What is the structure/size of NCR_n*?*

- *Is there a level of logical complexity that guarantees continuous randomness?*
- *Can we reproduce the proof that a non-computable real is random at a higher level?*

The Class NCR

Upper bound

NCR_n is a Π^1_1 set, i.e. its complement is the image of an effectively closed set under an effectively continuous transformation.

- NCR_n does not have a perfect subset.
- Solovay, Mansfield: Every Π^1_1 set of reals without a perfect subset must be contained in L.

The Constructible Universe

Definition

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

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

Randomness for Continuous Measures

One can analyze the proof of the previous theorem to obtain a more recursion theoretic characterization of continuous randomness.

Theorem

Let X be a sequence. For any $Z \in 2^{\mathbb{N}}$, the following are equivalent.

- Z is random for a continuous measure computable in Z.
- There exists a functional Φ computable in Z which is an order-preserving homeomorphism of $2^{\mathbb{N}}$ such that $\Phi(X)$ is λ-Z-random.
- X is truth-table equivalent (relative to Z) to a λ-Z-random real.

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

The Structure of NCR_1

A sequence X is hyperarithmetic if it is recursive in some $\emptyset^{(\alpha)}$, where α is a recursive ordinal.

- Woodin: outside the hyperarithmetic sequences, the Posner-Robinson theorem holds for a truth-table reduction.
- Conclude that all elements of NCR_1 are hyperarithmetic. In other words, if X is not hyperarithmetic, it is random for some continuous measure.

The Structure of NCR_n

For larger n, we can still show:

Theorem [Reimann and Slaman]

For all n, NCR_n is countable.

Examples of higher order

Theorem

Kleene's $\mathcal{O}$ is an element of NCR_3.

Based on this, one can use the theory of jump operators (Jockusch and Shore) to obtain a whole class of examples.

Proof:

- Tree representation $\mathcal{O} = \{e :$ the eth computable tree $T_e \subseteq \omega^{<\omega}$ is well-founded$\}$.
- Suppose $\mathcal{O}$ is 3-random for some μ.
- We want to use domination properties of random reals.

The Class NCR

Examples of higher order

- Well-known (Kurtz and others): If X is n-random for μ, $n > 1$, then every function $f \leq_T X$ is dominated by a function computable in μ'.
- Therefore, μ' computes a uniform family $\{g_e\}$ of functions dominating the leftmost infinite path of T_e.
- Infer: For every e, the following are equivalent.

  (i) T_e is well-founded.

  (ii) The subtree of T_e to the left of g_e is finite.

- The latter condition is $\Pi^0_1(\mu')$, hence $\mathcal{O}$ is $\Pi^0_2(\mu)$.
- But this is impossible if $\mathcal{O}$ is 3-random for μ.

NCR_n is Countable

Main Features of the Proof

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

Borel Determinacy

Consider the following game: Let $\mathcal{A} \subseteq 2^{\mathbb{N}}$.

- Player I plays $X(0)$.
- Player II plays $X(1)$.
- I plays $X(2)$.
- II plays $X(3)$.

$$\vdots$$

The outcome of the play a sequence $X \in 2^{\mathbb{N}}$.

- Player I wins if $X \in \mathcal{A}$.
- Player II wins if $X \notin \mathcal{A}$.

Borel Determinacy

Theorem (Martin)

If $\mathcal{A}$ is Borel, then one of the players has a winning strategy.

An application is Borel Turing Determinacy:

> If $\mathcal{A}$ is Borel and invariant under Turing equivalence, then either $\mathcal{A}$ or its complement contains an upper cone in the Turing degrees.

An Upper Cone of Random Sequences

An upper cone of continuously random sequences

- 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 Borel Turing determinacy to infer that the complement of NCR_n contains a cone.
- The base of the cone is given by the Turing degree of a winning strategy in the corresponding game.

Location inside the Constructible Hierarchy

- The direct nature of Martin's proof implies that the winning strategy for that game belongs to the smallest L_β such that L_β is a model of ZFC.
- 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 – trees, trees of trees, etc.
- More precisely, the winning strategy (for Borel complexity n) is contained in

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

where ZFC_n^- is Zermelo-Fraenkel set theory without the Power Set Axiom + "there exist n many iterates of the power set of $2^{\mathbb{N}}$".

Relativization via Forcing

Posner-Robinson-style relativization

- Given $X \notin L_{\beta_n}$, using forcing we construct a set G such that $L_{\beta_n}[G] \models \mathsf{ZFC}_n^-$ and

$$Y \in L_{\beta_n}[G] \cap 2^{\mathbb{N}} \quad \text{implies} \quad Y \leq_T X \oplus G$$

  (independently by Woodin).
- 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 avoiding NCR_n.

Metamathematics Necessary?

Question

Do we really need the existence of iterates of the power set of the reals to prove the countability of NCR_n*, a set of reals?*

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

Borel Determinacy and Iterates of the Power Set

Necessity of power sets – Friedman's result

- Friedman showed

  $$\mathsf{ZFC}^- \nvdash \boldsymbol{\Sigma}^0_5\text{-determinacy.}$$

  (Martin improved this to $\boldsymbol{\Sigma}^0_4$.)
- The proof works by showing that there is a model of ZFC^- for which $\boldsymbol{\Sigma}^0_4$-determinacy does not hold. This model is L_{β_0}.

Based on this, Friedman showed that in order to prove Borel determinacy, one has to assume the existence of infinitely many iterates of the power set.

NCR and Iterates of the Power Set

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

Theorem

For every k,

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

NCR and Iterates of the Power Set

NCR_n is not countable in L_{β_0}

- Show that there is an n such that NCR_n is cofinal in the Turing degrees of L_{β_0}. (The approach does not change essentially for higher k.)
- The non-random witnesses will be the reals which code the full inductive constructions of the initial segments of L_{β_0}.

Randomness does not accelerate defining reals

Suppose that $n \geq 2$, $Y \in 2^{\mathbb{N}}$, and X is n-random for μ. Then, for $i < n$,

$$Y \leq_T X \oplus \mu \text{ and } Y \leq_T \mu^{(i)} \quad \text{implies} \quad Y \leq_T \mu.$$

NCR and Iterates of the Power Set

Example

For all k, $0^{(k)}$ is not 3-random for any μ.

Proof.

- Suppose $0^{(k)}$ is 3-random relative to μ.
- $0'$ is computably enumerable relative to μ and computable in the supposedly 3-random $0^{(k)}$. Hence, $0'$ is computable in μ and so $0''$ is computablely enumerable relative to μ.
- Use induction to conclude $0^{(k)}$ is computable in μ, a contradiction.

$\square$

NCR and Iterates of the Power Set

As with arithmetic definability, for $n \geq 5$, 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 computable in μ, and I is the largest initial segment of $\prec$ which is well-founded. If I is computable in $X \oplus \mu$, then I is computable in μ.

L_α's and their master codes

Master codes

- L_α, $\alpha < \beta_0$, is a countable structure obtained by iterating first order definability over smaller L_γ's and taking unions.
- Jensen's master codes are sequences $M_\alpha \in 2^{\mathbb{N}} \cap L_{\beta_0}$, for $\alpha < \beta_0$, that represent these countable structures.
- M_α is obtained from smaller M_γ's by iterating the Turing jump and taking arithmetically definable limits.
- Every $X \in 2^{\mathbb{N}} \cap L_{\beta_0}$ is computable in some M_α.

Master codes are not random

An inductive argument similar to the example $0^{(k)} \in \mathrm{NCR}_3$, using the non-helpfulness lemmas, can be applied transfinitely to these master-codes.

Theorem

There is an n such that for all limit α, if $\alpha < \beta_0$, then there is no continuous measure μ such that M_α is n-random relative to μ.