Definability and Randomness

Jan Reimann

January 27, 2010

Question

Given an infinite binary sequence, does there exist a (continuous) probability measure for which this sequence is random?

Algorithmic Randomness

Algorithmic randomness investigates individual random objects.

Objects are usually infinite binary sequences (reals).

- Randomness: Obey statistical laws.

  Example: Law of large numbers

  In general: Measure 1 properties.

- Algorithmic: Only effective laws.

  There are only countably many.

  Hence their intersection describes an almost sure event.

Randomness

Cantor space

- $2^{\mathbb{N}}$ with standard product topology.
- Clopen basis: cylinder sets

$$[\sigma] := \{X \in 2^{\mathbb{N}} : \sigma \subset X\}.$$

  where σ is a finite binary string.
- Given a set of strings W, we write $[W]$ for the open set induced by W, i.e. $[W] = \bigcup_{\sigma \in W} [\sigma]$.

Measures on $2^{\mathbb{N}}$

- Determined by values on cylinders.
- $\mu[\sigma] = \mu[\sigma^\frown 0] + \mu[\sigma^\frown 1]$.
- Example: Lebesgue measure $\lambda[\sigma] = 2^{-|\sigma|}$.

Recursion Theory Basics

We identify binary sequences with subsets of $\mathbb{N}$.

- A set $X \subseteq \mathbb{N}$ is recursive (computable) iff there is an algorithm to determine membership in A.
- Write $Y \leqslant_T X$ when Y is recursive relative to X, i.e. if we can effectively decide membership in Y given X as an oracle.
- X is recursively enumerable (r.e.) iff it has a definition of the form $\exists y P(x, y)$, where P is a recursive predicate of natural numbers.

  Example: Diophantine sets $\{a \in \mathbb{N} \colon \exists \vec{x}\, p(a, x) = 0\}$,
  $p(a, \vec{x})$ a polynomial with integer coefficients.
  (In fact, every r.e. set can be represented this way (MDPR).)

- X is arithmetically definable iff there is a definition of X expressed solely in terms of addition, multiplication, and quantification ($\exists$, $\forall$) within the natural numbers.

Recursion Theory Basics

- There is a $\leqslant_T$-greatest r.e. subset of $\mathbb{N}$ denoted by $0'$ (the Halting Problem, the Turing jump).

  Similarly, for any X, X' is the $\leqslant_T$-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.

Martin-Löf Randomness

Every nullset is subset of a G_δ nullset.

A test for randomness is an effectively presented G_δ nullset.

Definition

- A Martin-Löf test is a recursively enumerable set $W \subseteq \mathbb{N} \times 2^{<\mathbb{N}}$ such that
$$\sum_{\sigma \in W_n} 2^{-|\sigma|} \leqslant 2^{-n},$$
where $W_n = \{\sigma : (n, \sigma) \in W\}$
- A sequence $X = X_0 X_1 X_2 \ldots$ is Martin-Löf random if $X \notin \bigcap_n [W_n]$ for every Martin-Löf test W.

Martin-Löf Randomness

We can make tests more powerful by giving them access to an oracle Z.

Martin-Löf Z-test: W recursively enumerable relative to Z.

n-randomness: random relative to $0^{(n-1)}$.

Hence Martin-Löf random is the same as 1-random.

Summary

The set of n-random sequences

- has λ-measure 1
  (there are only countably many r.e. sets in a given oracle, hence at most countably many tests)
- is decreasing in n
  (more computational power for tests, more non-randomness detected)

Martin-Löf Randomness

Examples

- A recursive sequence is not Martin-Löf random.

  For example, π is not random. (It fails the test of "being π").
- Likewise, anything recursive in $0^{(n-1)}$ is not n-random.
- However, there is a recursively approximated ($\leqslant_T 0'$), but not recursive, sequence X such that X is Martin-Löf random.
- All commonly used statistical laws are effective in Martin-Löf's sense, so a Martin-Löf random sequence satisfies the law of large numbers, etc.

Definability and randomness

Understand the relation between two properties of sequences:

information theoretic	computability theoretic
randomness properties	degrees of unsolvability

Kolmogorov Complexity

Let M be a Turing-machine. Define

$$C_M(\sigma) = \text{min}\{|p| : p \in 2^{<\mathbb{N}}, M(p) = \sigma\},$$

i.e. $C_M(\sigma)$ is the length of the shortest program (for M) that outputs σ.

Kolmogorov's invariance theorem: There exists a machine U such that C_U is optimal (up to an additive constant), i.e. for all other machines M,

$$C_U(\sigma) \leqslant C_M(\sigma) + O(1)$$

Fix such a U and set $C(\sigma) = C_U(\sigma)$, the plain Kolmogorov complexity of σ.

A prefix-free Turing machine is a machine with prefix-free domain. The prefix-free version of C (use universal prefix free TM) is denoted by K.

Randomness and Incompressibility

Schnorr's Theorem
A sequence X is Martin-Löf random iff there exists a constant c such that

$$(\forall n)\ K(X\restriction_n) \geqslant n - c,$$

Proof: Short descriptions $\leftrightarrow$ open cover

Generalized Martin-Löf Tests

Other measures

To extend the notion of randomness to other distributions, we give the tests access to the measure we want to test for.

- A representation $\mathfrak{m}$ of a probability measure μ on $2^{\mathbb{N}}$ provides rational approximations to each $\mu[\sigma]$ meeting any required accuracy.
- A μ-test is a set W that is recursively enumerable relative to $\mathfrak{m}$ such that
$$\sum_{\sigma \in W_n} \mu[\sigma] \leqslant 2^{-n},$$
- Accordingly, X is μ-random if for any μ-test W, $X \notin \bigcap_n [W_n]$.

Similarly, we can define μ-n-randomness, by giving tests access to $\mathfrak{m}^{(n-1)}$, the n-th jump relative to $\mathfrak{m}$.

The Precise Question

Given a sequence $X \in 2^{\mathbb{N}}$ *and* $n \geqslant 1$,
does there exist a probability measure μ *on* $2^{\mathbb{N}}$
such that X *is* μ-n-*random?*

Randomness and Computability

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 [R. 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 recursive.

Non-trivial Randomness

Features of the proof

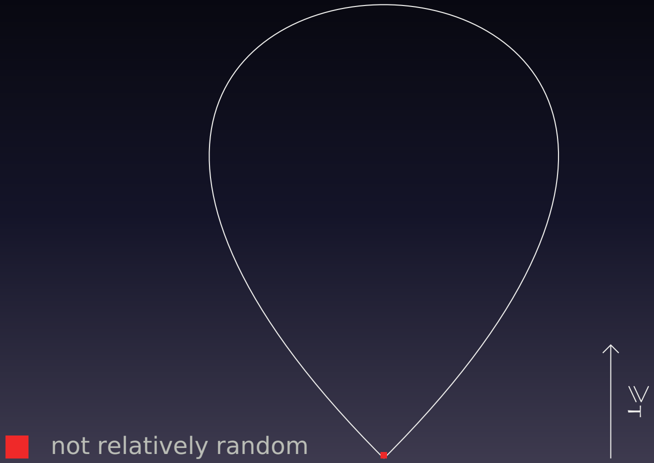
- Conservation of randomness.
  If Y is random for Lebesgue measure λ, and $f : 2^{\mathbb{N}} \to 2^{\mathbb{N}}$ is computable, then $f(Y)$ is random for λ_f, the image measure.

- A cone of λ-random reals.
  By the Kucera-Gacs Theorem, every sequence $\geqslant_T 0'$ is Turing equivalent to a λ-random real.

- Relativization using the Posner-Robinson Theorem.
  If X is not recursive, then $X \oplus G \geqslant_T G'$. ($X$ looks like a jump relative to G)

- A compactness argument for measures.

$2^{\mathbb{N}}$ ordered by $\geqslant_T$



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?.

Randomness for Continuous Measures

A thorough analysis of the previous theorem yields a criterion for continuous n-randomness via conservation of randomness:

Turing-equivalent (relative to some parameter) to an $(n+1)$-random sequence.

Can we obtain a cone of continuously random sequences?

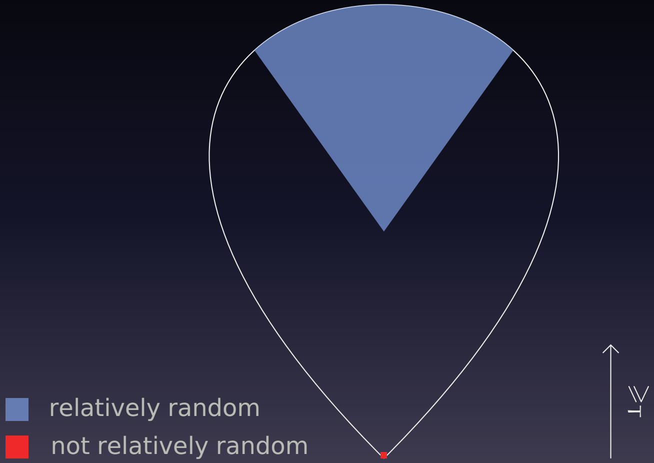
(*Looking for an analogue of Kucera-Gacs for continuous randomness.*)

Use Borel Turing Determinacy:
If E is a Borel subset of $2^{\mathbb{N}}$ that is closed under $\equiv_T$, then either E or $2^{\mathbb{N}} \setminus E$ contains a $\geqslant_T$-cone.

This is a consequence of Borel Determinacy (Martin):
Two-player game with a Borel winning sets are determined.

To obtain a cone, consider 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.

$2^{\mathbb{N}}$ ordered by $\geqslant_T$



Locating the Base of the Cone

The base of the randomness cone is given by the Turing degree of a winning strategy in a game given by Martin's Theorem.

Martin's proof of Borel Determinacy is constructive.

Gödel's hierarchy of constructible sets L:

- $\mathrm{L}_0 = \emptyset$
- $\mathrm{L}_{\alpha+1} = \mathrm{Def}(\mathrm{L}_\alpha)$, the set of subsets of L_α which are first order definable in parameters over L_α.
- $\mathrm{L}_\lambda = \cup_{\alpha<\lambda} \mathrm{L}_\alpha$, λ limit ordinal.
- $\mathrm{L} = \bigcup_\alpha \mathrm{L}_\alpha$.

Locating the Base of the Cone

The winning strategy of a Borel game can be located in L.

- 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.
- The winning strategy (for Borel complexity n) is contained in $L_{\beta(n)}$, where β_n is the least ordinal such that

  $$L_{\beta(n)} \models \text{ZFC}_n^-,$$

  where ZFC_n^- is Zermelo-Fraenkel set theory without the Power Set Axiom + "exist n many iterates of the power set of $\mathbb{R}$".
- Note that $L_{\beta(n)}$ is countable.

Relativization via Forcing

Now get from a cone of sequences to co-countably many sequences.

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

$$Y \in L_{\beta(n)}[G] \cap 2^{\mathbb{N}} \quad \text{implies} \quad Y \leqslant_T X \oplus G$$

- If X is not in $L_{\beta(n)}$, it will belong to every cone with base in the accordant $L_{\beta(n)}[G]$, in particular, it will belong to the cone in which every sequence is continuously random.
  (Use absoluteness)

Corollary (Co-Countability Theorem, R. and Slaman)

For any n, all but countably many sequences are n-random with respect to a continuous measure.

$2^{\mathbb{N}}$ ordered by $\geqslant_T$

Metamathematics necessary?

Question

Do we really need the existence of iterates of the power set of the reals to prove the Co-Countability Theorem, a statement about sequences?

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

- H. Friedman showed that infinitely many iterates of the power set of $\mathbb{R}$ are necessary to prove Borel Determinacy.
- We can prove a similar fact concerning the Co-Countability Theorem.

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 n-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.

Iterates of the Power Set

A cofinal sequence of non-randoms

- Show that there is an n such that the set of non-n-randoms is cofinal in the Turing degrees of $L_{\beta(0)}$. (The approach does not change essentially for higher k.)
- The non-random witnesses will be codes of the full inductive constructions of the initial segments of $L_{\beta(0)}$.

The following is a key lemma.

Higher randomness has little computational power

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

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

Relative to μ, X and instances of the jump form a minimal pair.

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

Master Codes

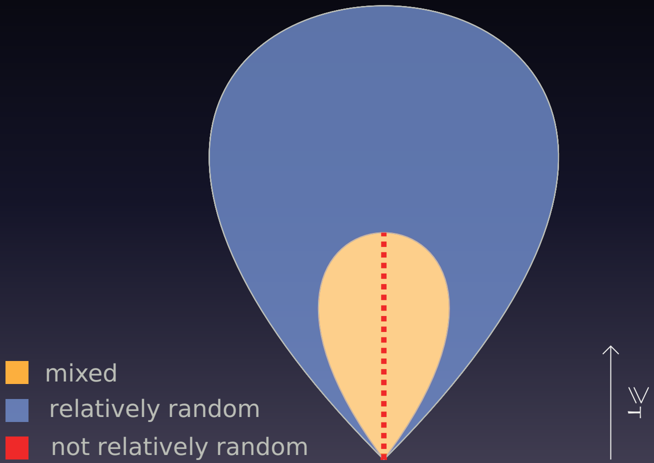
A set-theoretic analogue of the jump

- 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 a sequence $M_\alpha \in 2^{\mathbb{N}} \cap L_{\beta_0}$, for $\alpha < \beta_0$, of representations of these countable structures.

Master codes as witnesses for NCR

- An inductive argument similar to the non-randomness of $0^{(k)}$ can be applied transfinitely to these master-codes.
- There is an n such that for all limit λ, if $\lambda < \beta_0$ then M_β is not n-random for a continuous measure.

$2^{\mathbb{N}}$ ordered by $\geqslant_T$



A Different Application

Basic principle of the previous result

random sequences $+$ Turing reductions $=$ existence of measures

Application: Frostman's Lemma

Sets of positive Hausdorff dimension support a "nice" probability measure.

Hausdorff Dimension

Hausdorff measures and dimension

Given a real $s \geqslant 0$, let $\mathcal{H}^s$ denote the outer measure induced by the function

$$\mathcal{H}^s[\sigma] = 2^{-|\sigma|s}.$$

The Hausdorff dimension of a set $E \subseteq 2^{\mathbb{N}}$ is given by

$$\dim_H E = \inf\{s : E \text{ is } \mathcal{H}^s\text{-null}\}.$$

- Hausdorff dimension is invariant under bi-Lipschitz transformations.
- It captures the “right exponent” relation diameter to volume, possibly non-integer.
- Example: $\dim_H$ Middle-third Cantor Set $= \log 2/\log 3$.

Effective Dimension

Martin-Löf's approach to randomness works for outer measures, too.

Hence we can define the effective dimension $\dim^1_H$ of a sequence as

$$\dim^1_H X = \inf\{s \in \mathbb{Q}^+ : \text{ X is not } \mathcal{H}^s\text{-random}\}$$

Dimension and Kolmogorov complexity

$$\dim^1_H X = \liminf_n \frac{K(X\restriction_n)}{n}$$

(Ryabko, Mayordomo)

Example: If X is Martin-Löf random, then

$$\dim^1_H (X_0\, 0\, X_1\, 0\, X_2\, 0 \dots) = 1/2.$$

Pointwise Frostman Lemma

Theorem
If for $X \in 2^{\mathbb{N}}$ $\dim_H^1 X > s$, then X is random with respect to a probability measure μ such that

$$(\forall \sigma)\ \mu[\sigma] \leqslant c 2^{-|\sigma| s}. \qquad (*)$$

In particular, sequences of positive dimension are random with respect to a continuous measure.

This implies the classical Frostman Lemma:

If $\dim_H E > s$, $E \subseteq 2^{\mathbb{N}}$ Borel, then there exists a probability measure μ satisfying (*) such that

$$\mathrm{supp}(\mu) \subseteq E.$$

Pointwise Frostman Lemma

However, the proof is of an effective nature.

- By the Kucera-Gacs Theorem, there exists a λ-random real R such that $R \geqslant_{\text{wtt}} X$ via some reduction Φ.
- The effective process transforming R into X induces a "defective" probability measure on $2^{\mathbb{N}}$, a semimeasure.
- Using a recursion theoretic lowness argument,

  Every effectively closed set contains an element that has low computational power ("almost recursive").

  one can show that among the possible completions of this semimeasure into a probability measure, there must exist one that makes X random and satisfies (*).

Ende