Randomness, computability, effective descriptive set theory

André Nies
The University of Auckland

TAMC 07, Shanghai
May 2007

Sets

We study sets of natural numbers.

- A set $Z \subseteq \mathbb{N}$ can be identified with an infinite string over $\{0, 1\}$.
- If Z is co-infinite, it can also be identified with a real number in $[0, 1)_{\mathbb{R}}$.
- Example. We identify
  - The set $Z = \{2n : n \in \mathbb{N}\}$
  - the infinite string $10101010\ldots$
  - the real number $0.101010\ldots = 2/3$.

Two aspects of randomness

The intuitive concept of randomness for a set Z has two related aspects:

(a) Z satisfies no exceptional properties, and
(b) Z is hard to describe.

In an attempt to find formal counterparts for the intuitive concept of randomness, at first we will consider each aspect separately.

(A) Exceptional properties are null classes

- Think of the set Z as the overall outcome of an idealized physical process that proceeds in time, producing infinitely many bits. (For instance, the two-slit experiment in quantum physics.)
- The bits are independent, and zero and one have the same probability. The probability that a string $\sigma \in \{0, 1\}^*$ is an initial segment of Z is $2^{-|\sigma|}$.
- Given this view, exceptional properties are represented by null classes $\mathcal{C}$, namely $\lambda\mathcal{C} = 0$, where λ is the uniform outer measure on Cantor space $\{0, 1\}^{\mathbb{N}}$.

Examples

Some examples of exceptional properties of a set Y.

- Having every other bit zero:

$$\forall i \, Y(2i) = 0.$$

- Having at least twice as many zeros as ones in the limit:

$$\liminf |\{i < n : Y(i) = 0\}|/n \geq 2/3.$$

The corresponding classes are null, so they should not contain a random set.

Restricting null classes

- In order to obtain a sound formal definition of randomness, we have to restrict the classes that have to be avoided. Otherwise, no set Z would be random at all, because the singleton $\{Z\}$ itself is a null class.
- To do so, an effectivity or a definability requirement of some kind is imposed on the class. For instance, we could require that the null class is Π^0_2. This would include the classes given by the properties above; $\{Y : \forall i\, Y(2i) = 0\}$ is even Π^0_1.
- Here, a Π^0_2-class is a class of the form
$$\{X \in \{0,1\}^{\mathbb{N}} : \forall n \exists k\, S(n, X\restriction_k)\},$$
where S is a computable relation.

(B) Being hard to describe

A random object has no patterns, is disorganized. The intuition in that some degree of organization would make the object easier to describe.
For finite binary strings, the intuitive notion of randomness can be identified with being hard to describe.

- This is so because there are description systems (universal machines) that describe every possible string.
- Being hard to describe for strings can be formalized by incompressibility with respect to a universal machine, and incompressible strings have the properties one typically expects from a random string.

Close descriptions

For sets, the intuition still is:
being organized implies being easier to describe.
However, we cannot formalize being hard to describe in such a simple way as we did for strings, since each description system only yields countably many sets and misses out on all the rest.
To make more precise what is meant by being hard to describe, we need a type of close descriptions, which could for instance be the Π^0_1 null classes, or the Π^0_2 null classes. A set is hard to describe, in a particular sense (say Π^0_2 classes) if it does not admit a close description in that sense (for instance, it is not in any Π^0_2 null class).

Formal notions of randomness

We will now formalize the intuitive notion of randomness.

(A) if random means typical, we need a restricting condition on null classes.

(B) if random means being hard to describe, we need a formal notion of close description.

Tests

Both are given by specifying a test concept. This determines a formal randomness notion: Z is random, in that specific sense, if it passes all the tests of the given type.

Tests are themselves objects that can be described in a particular way; thus only countably many null classes are given by such tests.

If $(\mathcal{A}_n)_{n\in\mathbb{N}}$ is a list of all null classes of that kind, then the class of random sets is $\{0,1\}^{\mathbb{N}} - \bigcup_n \mathcal{A}_n$ and has uniform measure 1. For strings, the analogue of this is: most strings of each length are incompressible.

Martin-Löf-tests

- A ML-test is a uniformly computably enumerable sequence $(G_m)_{m \in \mathbb{N}}$ of open sets such that $\forall m \in \mathbb{N}\ \lambda G_m \leq 2^{-m}$.
- Z is ML-random if Z passes each ML-test, in the sense that $Z \notin \bigcap_m G_m$.

Machines and K

A machine is a partial recursive function $M : \{0,1\}^* \mapsto \{0,1\}^*$.
M is prefix free if its domain is an antichain under inclusion of strings.
Let $(M_d)_{d \geq 0}$ be an effective listing of all prefix free machines.
The standard universal prefix free machine U is given by

$$U(0^d 1\sigma) = M_d(\sigma).$$

The prefix free version $K(y)$ of Kolmogorov complexity is the length of a shortest prefix free description of y:

$$K(y) = \min\{|\sigma| : U(\sigma) = y\}.$$

Facts and examples

Example of a ML-random set:

$$\Omega = \sum_{U(\sigma)\downarrow} 2^{-|\sigma|},$$

where U is the universal prefix free machine. (Recall we view reals in $[0, 1)$ as subsets of $\mathbb{N}$ via the binary representation.)

Theorem (Schnorr 1971)

Z is Martin-Löf random iff for some c, $\forall n\, K(Z\restriction_n) \geq n - c$.

Schnorr randomness

- A Schnorr test is a ML-test $(G_m)_{m\in\mathbb{N}}$ such that λG_m is computable, uniformly in m.
- Z is Schnorr random if Z passes each Schnorr test, in the sense that $Z \notin \bigcap_m G_m$.
- Each ML-random is Schnorr random, but not conversely. There even is a left-c.e. counter example.

Computable measure machines

A prefix free machine M is called computable measure machine if its halting probability $\Omega_M = \sum_{M(\sigma)\downarrow} 2^{-|\sigma|}$ is a computable real number.
Recall Z is Martin-Löf random iff for some c, $\forall n\, K(Z\upharpoonright_n) \geq n - c$. The following is an analog for Schnorr randomness. Since there is no universal computable measure machine, we have to quantify over all of them.

Theorem (Downey, Griffiths, 2005)

Z is Schnorr random iff for each computable measure machine, for some c, $\forall n\, K_M(Z\upharpoonright_n) \geq n - c$.

Low for K

Andrej A. Muchnik (1999) defined A to be low for K if

$$\forall y\ K(y) \leq K^A(y) + O(1).$$

He proved that there is a c.e. noncomputable A that is low for K.

Low for ML-random

Let MLRand denote the class of Martin-Löf-random sets.

- Because an oracle A increases the power of tests, $\mathrm{MLRand}^A \subseteq \mathrm{MLRand}$.
- A is low for ML-random if $\mathrm{MLRand}^A = \mathrm{MLRand}$ (Zambella, 1990).

By Schnorr's Theorem relativized,

- MLRand can be defined in terms of K, and
- MLRand^A in terms of K^A.

So low for K implies low for ML-random.

Low for K = Low for ML = base for ML

Theorem (Nies 2003)

A is low for ML-randomness $\Leftrightarrow$ A is low for K.

A is a base for ML-randomness if A can be computed from a set ML-random relative to A.
Each low for ML-random set is a base for ML-randomness, by the Kučera-Gacs Theorem.

Theorem (Hirschfeldt, Nies, Stephan, 2005)

If A is a base for ML-randomness, then A is low for K.

Low for computable measure machines

The following is a Schnorr analog of being low for K. However, the definition is more complicated because there is no universal computable measure machine.

Definition

A is low for computable measure machines if for each computable measure machines M^A relative to A, there is a computable measure machines N such that

$$\forall x\, K_N(x) \leq K_{M^A}(x) + O(1).$$

Low for Schnorr

Let SR denote the class of Schnorr-random sets. A is low for Schnorr-randomness if $\mathrm{SR}^A = \mathrm{SR}$.
Terwijn and Zambella 2000 proved indirectly that there are $2^{\aleph_0}$ many; see below.

Theorem (Downey, Greenberg, Mikhailovich, Nies 2005)

A is low for ML-randomness $\Leftrightarrow$ A is low for computable measure machines.

Schnorr randomness can be characterized in terms of computable measure machines, relative to each oracle, so the direction $\Leftarrow$ is clear.

Bases for Schnorr-randomness

A is a base for Schnorr-randomness if A can be computed from a set Schnorr-random relative to A.

Clearly each low for Schnorr random set is a base for Schnorr randomness.

But there are more bases for Schnorr randomness.

For instance, each Δ^0_2 set that fails to be diagonally noncomputable is a base for Schnorr randomness (even for computable randomness, a notion in between ML and Schnorr), by Hirschfeldt, Nies, Stephan, 2005.

On the other hand, a noncomputable set that is low for Schnorr randomness is not Δ^0_2, as we will see shortly.

Computably traceable

Recall A is of hyper-immune free degree if each $f \leq_T A$ is computably bounded.

- Being computably traceable strengthens the property that A is of hyper-immune free degree:
- for each $f \leq_T A$: for all x, $f(x)$ is in a small effectively given set $D_{g(x)}$. Here $D_n \subseteq \mathbb{N}$ is the n-th finite set.
- Here, g is a computable function depending on f, but $|D_{g(x)}| \leq h(x)$ for a fixed computable bound h.
- it turns out that the choice of the bound h is irrelevant, as long as h is nondecreasing and unbounded.

Existence of computably traceable sets

Theorem (Terwijn and Zambella 2000)

There are $2^{\aleph_0}$ many computably traceable sets.

To prove this, essentially one uses Sacks forcing with computable perfect trees.
Each generic set for this forcing notion is computably traceable.

Computably traceable= Low for Schnorr tests

A is low for Schnorr tests if for each Schnorr test $(G_m^A)_{m\in\mathbb{N}}$ relative to A, there is a Schnorr test $(S_n)_{n\in\mathbb{N}}$ such that $\bigcap_m G_m \subseteq \bigcap_n S_n$.

This implies being low for Schnorr.

Theorem (Terwijn and Zambella 2000)

A is low for Schnorr tests $\Leftrightarrow$ A is computably traceable.

In particular, $2^{\aleph_0}$ many sets are low for Schnorr randomness.

Computably traceable= Low(SR)

The result was improved later, eliminating the mention of tests.

Theorem (Kjos-Hanssen, Nies, Stephan 2005)

A is low for Schnorr-randomness $\Leftrightarrow$ A is computably traceable.

To show A is low for ML-randomness $\Leftrightarrow$ A is low for computable measure machines, Downey e.a. 2005 made use of the Terwijn/Zambella result. Given that, it was sufficient to prove:

Lemma

A is computably traceable $\Rightarrow$ A is low for computable measure machines.

Strongly jump traceable sets

Given the characterization of low for Schnorr randomness via computable traceability, one might hope such a thing can also be done for lowness for ML-randomness.

Let W_e be the e-th c.e. set. Let $J^A(e)$ be the value of the A-jump at e, namely, $J^A(e) = \Phi_e(e)$.

A c.e. trace with bound h is a sequence $(W_{g(n)})_{n \in \mathbb{N}}$, where g is a computable function and $|W_{g(x)}| \leq h(x)$ for each x.

Figueira, N, Stephan (2004) called A strongly jump traceable if for each order function h, there is a c.e. trace $(W_{g(n)})_{n \in \mathbb{N}}$ with bound h such that $J^A(e) \in W_{g(e)}$ whenever it is defined.

A proper subclass of the low for ML-random sets

Theorem (Figueira, N, Stephan 2004)

There is a c.e. noncomputable strongly jump traceable set.

They also prove that A is strongly jump traceable $\Leftrightarrow$ A is "lowly" for the plain Kolmogorov complexity C, namely, for every order function h and almost every x, $C(x) \leq C^A(x) + h(C^A(x))$.

SJT doesn't characterize low for K, but it is closely related.

Theorem (Cholak, Downey, Greenberg 2006)

The c.e. strongly jump traceable sets form a proper subideal of the low for K sets.

It is open whether this also holds within the Δ^0_2 sets.

K-trivial and facile sets

A set A is K-trivial if $\forall n\, K(A\restriction_n) \leq^+ K(n) + b$
(here $\leq^+$ means $\leq$ up to an additive constant).

Theorem

A is low for K $\Leftrightarrow$ A is K-trivial.

(This was obtained joint with Hirschfeldt, via a modification of Nies' result that K-trivial sets are closed downward under $\leq_T$.)
$h : \mathbb{N} \to \mathbb{N}$ is an order function if h is computable, nondecreasing and unbounded.
Z is facile if $\forall n\, K(Z\restriction_n \mid n) \leq^+ h(n)$, for any order function h.

Theorem (Kjos-Hanssen & Nies)

Let A be of hyper-immune free degree. Then
A is computably traceable $\Leftrightarrow$ A is facile.

Effective descriptive set theory

Π^1_1 sets of numbers are a high-level analog of c.e. sets, where the steps of an effective enumeration are recursive ordinals.

Hjorth and Nies (Proc. LMS, ta) have studied the analogs of K and of ML-randomness based on Π^1_1-sets.

The analog of Schnorr's Theorem holds (the proof takes considerable extra effort because of limit stages).

There is a Π^1_1 set of numbers which is K-trivial (in this new sense) and not hyperarithmetic. In contrast:

Theorem (Hjorth and Nies)

If A is low for Π^1_1-ML-random, then A is hyperarithmetic.

Π^1_1-classes and Δ^1_1-classes

Definition

A class $\mathcal{C} \subseteq 2^{\mathbb{N}}$ is Π^1_1 iff there is a functional Ψ such that

- for each Z, Ψ^Z is a (code for a) linear order with domain $\mathbb{N}$, and
- $Z \in \mathcal{C} \Leftrightarrow \Psi^Z$ wellordered.

We think of the length of Ψ^Z as the stage when Z enters $\mathcal{C}$.

Definition

A class $\mathcal{C} \subseteq 2^{\mathbb{N}}$ is Δ^1_1 if $\mathcal{C}$ and $2^{\mathbb{N}} - \mathcal{C}$ are Π^1_1.

Δ^1_1-randomness

Martin-Löf (1970) suggested to use the Δ^1_1 null classes as tests:

Definition

Z is Δ^1_1-random if Z is in no null Δ^1_1-class.

Δ^1_1-random is the effective descriptive set theory analog of both computably random and Schnorr random.

Π^1_1-ML-random implies Δ^1_1-random but not conversely.

Lowness for Δ^1_1-randomness

Theorem (Chong, N and Yu)

low for Δ^1_1 random $\Leftrightarrow$ Δ^1_1 traceable $\Leftrightarrow$ Π^1_1 traceable.

This helps to prove existence outside the hyperarithmetic sets.

Theorem (Chong, N and Yu)

There is a perfect class of sets that are low for Δ^1_1-randomness.

It suffices to prove that any Sacks generic (for forcing with hyperarithmetical perfect trees) is Δ^1_1 traceable.

References other than the original papers

- September 2006 Bull Symb. Logic
- My survey “Eliminating concepts”
- My book Computability and Randomness, OUP; available at

  http://www.cs.auckland.ac.nz/nies/Niesbook.pdf.