Randomness and computable analysis

Results and open questions

André Nies

The University of Auckland

CCR 2011, Jan 31-Feb 4, Cape Town

Main thesis

Randomness

is equivalent to

Differentiability

Main thesis, in more detail

A real $z \in [0, 1]$ satisfies an algorithmic randomness notion (such as Martin-Löf random, computably random)

$$\Longleftrightarrow$$

each effective function in an appropriate class of functions is differentiable at z.

Computable functions on the unit interval

Definition

Let $f \colon [0, 1] \to \mathbb{R}$. We say that f is computable if

(a) For each rational $q \in [0, 1]$, the real $f(q)$ is computable uniformly in q.

(b) f is effectively uniformly continuous:
there is a computable $h \colon \mathbb{N} \to \mathbb{N}$ such that for each n,

$$|x - y| < 2^{-h(n)} \text{ implies } |f(x) - f(y)| < 2^{-n}.$$

Proposition

If a nondecreasing function f satisfies (a) and is continuous, then it is already computable.

Example: computable randomness and differentiability

- Computable randomness is defined for infinite sequences Z of bits: no computable betting strategy succeeds on Z.
- Via the binary expansion, this notion also makes sense for reals.

Theorem (Brattka, Miller, N: to appear)

A real z is computably random

$$\iff$$

each computable monotone function $f\colon [0,1] \to \mathbb{R}$ is differentiable at z.

Computable randomness and differentiability: Lipschitz functions

Different classes of functions can describe the same randomness notion: instead of monotone, we can take Lipschitz functions.

Theorem (Freer, Kjos-Hanssen, N: to appear)

A real z is computably random

$$\Longleftrightarrow$$

each computable Lipschitz function $f\colon [0,1] \to \mathbb{R}$ is differentiable at z.

In this talk...

- We recall algorithmic randomness notions.
- We review classes of functions from classical real analysis, such as functions of bounded variation, and Lipschitz functions.
- We characterize the algorithmic randomness notions in terms of differentiability of effective functions in these classes.

Being almost everywhere well-behaved

- Classically, to say a property holds for a "random" real in $[0, 1]$ simply means that the property has Lebesgue measure 1.
- Several theorems in real analysis state that an appropriate function is well-behaved at a "random" real.

Theorem (Lebesgue, 1904)

Let $f : [0, 1] \to \mathbb{R}$ be non-decreasing. Then $f'(z)$ exists for a.e. z, that is, with uniform probability 1.

Algorithmic randomness notions

The idea in algorithmic randomness

z is random $\iff$ z avoids each algorithmic null set.

- One has to specify a kind of algorithmic null sets.
- To do so, one introduces a test notion. Failing the test means to be in the null set.
- For instance, a Martin-Löf test is a uniformly c.e. sequence of open sets $(\mathcal{G}_m)_{m\in\mathbb{N}}$ in the unit interval such that $\lambda\mathcal{G}_m \leq 2^{-m}$ for each m.
- The algorithmic null set it describes is $\bigcap_m \mathcal{G}_m$.

Understanding an algorithmic randomness notion via analysis

The characterizations via differentiability can be used to better understand the algorithmic randomness notion:

- Randomness notions of reals are preserved under maps such as $z \to \sqrt{z}$ (computable bijections with positive derivative).
- Computable randomness is base invariant.
- An analog of computable randomness can be defined in spaces other than the reals via differentiability of computable Lipschitz functions.

Understanding analysis via algorithmic randomness notions

The results also yield a better understanding of the classical theorems.

- The exception sets for differentiability of nondecreasing functions are simpler than the exception sets for bounded variation functions.
- We can calibrate, in the sense of reverse mathematics, the strength of theorems saying that a certain function is a.e. well behaved.
- The benchmark principles have the form "for each oracle X there is a set R that is random in X". An example of such a principle is WWKL_0, which is the existence principle for Martin-Löf random sets.

Tests versus functions

- We will convert tests to computable functions on the unit interval, and conversely.
- A real fails the test $\iff$ the function is non-differentiable at the real.
- A test concept for an algorithmic randomness notion

  corresponds to

  a natural class, taken from analysis, of effective functions.

Upper and lower derivatives

Let $f\colon [0,1] \to \mathbb{R}$. We define

$$\begin{aligned} \overline{D}f(z) &= \limsup_{h\to 0} \frac{f(z+h)-f(z)}{h} \\ \underline{D}f(z) &= \liminf_{h\to 0} \frac{f(z+h)-f(z)}{h} \end{aligned}$$

Then

$$f'(z) \text{ exists} \iff \overline{D}f(z) \text{ equals } \underline{D}f(z) \text{ and is finite.}$$

Randomness via betting strategies

Computable betting strategies are certain computable functions M from binary strings to the non-negative reals.

- Let Z be a sequence of bits. When the player has seen the string σ of the first n bits of Z, she can make a bet q, where $0 \leq q \leq M(\sigma)$, on what the next bit $Z(n)$ is.
- If she is right, she gets q. Otherwise she loses q. Thus, we have
$$M(\sigma 0) + M(\sigma 1) = 2M(\sigma)$$
for each string σ.
- She wins on Z if M is unbounded along Z. We call a set Z computably random if no computable betting strategy wins on Z.

Martin-Löf random $\Rightarrow$ computably random, but not conversely.

Some facts on computable randomness

- Computable randomness lies strictly in between Martin-Löf and Schnorr randomness. Such sets can have very slowly growing initial segment complexity, e.g. $K(Z\upharpoonright_n) \leq 2\log n$.
- Left-c.e. computably random sets can be Turing incomplete. In fact they exist in each high c.e. degree (N, Stephan, Terwijn 2005).
- Low for computably random $\Rightarrow$ computable (N 2005).
- There is a characterization by Downey and Griffiths (2004) in terms of special ML-tests called “computably graded tests”.
- There is a characterization by Day (2009) via the initial segment complexity given by “quick process machines”.

Characterizing computable randomness via analysis

Theorem (Brattka, Miller, N: 2010)

A real z is computably random

$$\Longleftrightarrow$$

each computable non-decreasing function $f\colon [0,1] \to \mathbb{R}$ is differentiable at z.

- To prove the implication $\Longleftarrow$ (tests-to-functions), for each computable betting strategy, we define a non-decreasing computable function f.
- If the strategy succeeds on z, then $f'(z)$ does not exist.

Tests-to-functions for computable randomness

- Let M be a computable betting strategy (also called a computable martingale).
- Let μ be the measure induced by M. It is determined by its values on the basic clopen sets: $\mu([\sigma]) = M(\sigma)2^{-|\sigma|}$.
- Let
$$g_M(x) = \mu[0, x].$$
 Then g_M is nonincreasing, and $g_M(q)$ is computable for each dyadic rational q.
- Since $M(\sigma) = (g_M(0.\sigma 1) - g_M(0.\sigma))/2^{-|\sigma|}$ and M succeeds on z, we have $\overline{D}g_M(z) = \infty$.

Now suppose z is not computably random.
Then some computable martingale M with the savings property succeeds on z.
In this case g_M is continuous, and hence computable.

Functions-to-tests for computable randomness

We now discuss the implication $\Longrightarrow$ of

Theorem (Brattka, Miller, N: 2010)

A real z is computably random $\Longleftrightarrow$ each computable non-decreasing function $f\colon [0,1] \to \mathbb{R}$ is differentiable at z.

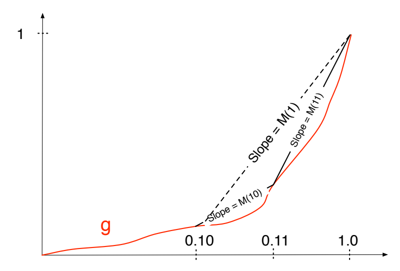
- For each non-decreasing computable function f, we build a computable betting strategy.
- If $f'(z)$ does not exist, then the strategy succeeds on z.

Turning nondecreasing functions into martingales

For the simplest case suppose that $\overline{D}g(z) = \infty$ for g computable nondecreasing. Then martingale M succeeds on z, where for a string σ, we let

$$M(\sigma) = \frac{g(0.\sigma + 2^{-|\sigma|}) - g(0.\sigma)}{2^{-|\sigma|}}.$$

Thus $M(\sigma)$ is the slope of g between the points $0.\sigma$ and $0.\sigma + 2^{-|\sigma|}$. It is clear that this is a martingale. For instance, the following shows $2M(1) = M(10) + M(11)$.



Functions-to-tests for computable randomness

- For the general case, suppose $f'(z)$ fails to exist for nondecreasing computable f.
- We build a nondecreasing computable g such that $\overline{D}g(z) = \infty$ using a method related to the Doob martingale convergence theorem.
- The function g can be converted into a computable martingale M that succeeds on z. (We can't just take the slope of g at dyadic rationals, because $\overline{D}g(z) = \infty$ may not be "visible" there.)
- For detail see the paper, or my 2010 talk at CCR Notre Dame.

As a corollary, we obtain that computable randomness for reals is base invariant. For instance, we could equivalently define it via computable strategies betting on the ternary expansion of a real.

Computable randomness and Lipschitz functions

Recall that f is Lipschitz if $|f(x) - f(y| \leq C(|x - y|)$ for some $C \in \mathbb{N}$.

Theorem (Freer, Kjos-Hanssen, N: to appear)

A real z is computably random

$$\iff$$

each computable Lipschitz function $f\colon [0,1] \to \mathbb{R}$ is differentiable at z.

$\Longrightarrow$ (functions-to-tests):

- write
  $$f(x) = (f(x) + Cx) - Cx.$$
  Then $(f(x) + Cx)$ is computable and non-decreasing.
- From the monotone case, we obtain a test (martingale) for this function. If $f'(z)$ does not exists, then z fails this test.

Tests-to-functions (implication $\Longleftarrow$) for Lipschitz

- Suppose a computable martingale B succeeds on z. We use this to build a computable martingale M with range contained in $[1, 2]$, such that
$$\limsup_n M(z\upharpoonright_n) = 2 \text{ and } \liminf_n M(z\upharpoonright_n) = 1.$$
- Then the associated computable function g_M is Lipschitz, and has
$$\overline{D}g(z) = 2 \text{ and } \underline{D}g(z) = 1.$$
- We build M by a "reverse Doob strategy": we let
$$M = N_0 - N_1.$$
    - In "up phases" of M, the strategy N_0 bets with the same factors as the given strategy B and N_1 doesn't bet, until M's capital reaches 2;
    - in "down phases" of M, the strategy N_1 bets like B and N_0 doesn't bet, until M's capital is down to 1.

Variation of a function

The variation of a function $f\colon [0,1] \to \mathbb{R}$ is

$$V(f) = \sup \sum_{i=1}^{n-1} |f(t_{i+1}) - f(t_i)| < \infty,$$

where the sup is taken over all collections $t_1 \leq t_2 \leq \ldots \leq t_n$ in $[0,1]$.

f is of bounded variation if $V(f) < \infty$.

It is a classical result of Jordan that such an f is of the form $h_0 - h_1$ for some nondecreasing functions h_0, h_1. Therefore:

Theorem

Let $f\colon [0,1] \to \mathbb{R}$ be of bounded variation. Then

$f'(r)$ exists for each r outside a null set (depending on f).

Tests-to-functions for Martin-Löf randomness

Theorem (Demuth 1975/Brattka, Miller, Nies, to appear)

Let $z \in [0,1]$. Then

z is Martin-Löf random $\Longleftrightarrow$

each computable function of bounded variation is differentiable at z.

- Demuth stated the existence of such a function without a proof.
- For the implication $\Longleftarrow$ (tests-to-functions), given a ML-test $(\mathcal{G}_m)_{m \in \mathbb{N}}$, we build a computable function f of bounded variation such that $f'(z)$ fails to exist for each $z \in \bigcap \mathcal{G}_m$.
- f is the sum of a uniform sequence of “sawteeth” functions f_m, where f_m has a sawtooth of slope 4^m on each interval entering $\mathcal{G}_m$.
- We actually need to modify $(\mathcal{G}_m)_{m \in \mathbb{N}}$ to make this work: we ensure $\lambda \mathcal{G}_m \le 8^{-m}$, and that each interval B enumerated in $\mathcal{G}_m$ is a subinterval of an interval A in $\mathcal{G}_{m-1}$ that is at least 8^m times longer.

Functions-to-tests for ML-randomness

Let f be a computable of bounded variation.

- We know $f = h_0 - h_1$ for some nondecreasing functions h_0, h_1.
- The pairs of (names for such) functions can be seen as a Π^0_1 class.
- Then, by the "low for z basis theorem", z is ML-random (hence computably random) relative to such a pair h_0, h_1.
- By the result for computable randomness relativized to z, the h_i are both differentiable at z. Thus $f'(z)$ exists.
- We have implicitly obtained a ML-test, but it depends on z!
  But then, the universal ML-test covers the sets of non-differentiability for all computable functions of bounded variation.

What did Demuth do? No idea.

Instead of a break...

Some results from the Logic Blog 2010

Theorem (Yu and Peng)

Z is Schnorr random relative to $\mathcal{H} \Leftrightarrow Z$ is random in each low set.

Theorem (Freer, Kjos, Nies)

If A is traceable with uniformly Δ^0_1 traces then A is already computably traceable.

Further contributions by Stephan, Kallimullin, Ng, ... Question section at the end:

Imagine we infinitely often toss a coin with probability δ for heads. Let r be the real whose binary expansion is obtained in this way. Describe the distribution $f_\delta(x) = P[r \leq x]$.

How to get ino Logicsharing

0. Install dropbox.com
1. Email andrenies@gmail.com to request access
2. Receive invitation to join
3. Move the folder (initially called ”np”) to somewhere convenient on your machine.

The dropbox folder contains useful things- have a look!

Web site is planned.

Schnorr randomness

- A Schnorr test is a ML-test $(\mathcal{G}_m)_{m\in\mathbb{N}}$ such that $\lambda\mathcal{G}_m$ is a computable real uniformly in m.
- A real z is Schnorr random if $z \notin \bigcap_m \mathcal{G}_m$ for each Schnorr test $(\mathcal{G}_m)_{m\in\mathbb{N}}$.
- Equivalently, for the binary expansion Z of z, there is no computable betting strategy M with an order function h such that $M(Z\restriction_n) \geq h(n)$ for infinitely many n.
- A Schnorr random set Z satisfies
  - all statistical criteria for randomness, such as the law of large numbers;
  - not all computability-theoretic criteria: for instance, even for a computably random set Z, one can have $Z_0 \equiv_T Z_1$, where Z_0 is the even bits and Z_1 is the odd bits of Z.

Variation norm

Recall that $V(f) = \sup \sum_{i=1}^{n-1} |f(t_{i+1}) - f(t_i)| < \infty$, where the sup is taken over all collections $t_1 \leq t_2 \leq \ldots \leq t_n$ in $[0, 1]$. Let

$$\|f\|_{BV} = V(f) + |f(0)|.$$

The functions $f \colon [0, 1] \to \mathbb{R}$ of bounded variation form a Banach space under this norm. We have $\|f\|_{BV} \geq \|f\|_\infty$ (the usual sup norm).

Let $AC_0[0, 1]$ be the absolutely continuous functions $f \colon [0, 1] \to \mathbb{R}$ such that $f(0) = 0$.

Fundamental theorem

The map $g \to \int_0^x g$ is a computable Banach space isometry

$$(L_1[0, 1], \|.\|_1) \to (AC_0[0, 1], \|.\|_{BV}).$$

The inverse is differentiation.

Computability in the variation norm

Definition

We say that a function $f\colon [0,1] \to \mathbb{R}$ of bounded variation is computable in the variation norm if there is an effective sequence $(q_n)_{n\in\mathbb{N}}$ of polygonal functions with rational slopes and corners such that $\|f - q_n\|_{BV} \le 2^{-n}$ for each n.

- If f is absolutely continuous, then this is equivalent to saying that the almost everywhere defined function f' is L_1-computable.
- Since $\|f\|_{BV} \ge \|f\|_\infty$, computability in the variation norm implies usual computability of f.
- The implication is strict: for each left-c.e. real α, Freer, Kjos, N [2010] build a computable Lipschitz function f such that $V(f) = \alpha$. If α is non-computable, then f is not computable in the variation norm.

  (In fact, they characterize the variation functions of computable [Lipschitz] functions as the continuous “interval-c.e. functions” that vanish at 0.)

Characterizing Schnorr randomness via analysis

- J. Rute, and indendently Pathak and Simpson, have announced that a real z is Schnorr random iff z is a Lebesgue point of each L_1-computable function. The implication $\Rightarrow$ improved a result of Pathak, who needed the stronger hypothesis that z is ML-random.
- In our language, this result amounts to saying that each absolutely continuous function (= function of the form $\int_0^x g$) that is computable in the variation norm is differentiable at z.
- Subsequently, Freer, Kjos and N proved the analogous result for Lipschitz functions:

Characterizing Schnorr randomness via analysis

Theorem (Freer, Kjos-Hanssen, N: 2010)

A real z is Schnorr random

$$\Longleftrightarrow$$

each Lipschitz function $f\colon [0,1] \to \mathbb{R}$ *that is computable in the variation norm is differentiable at* z.

The implication $\Rightarrow$ (functions-to-tests) follows from the Rute / Pathak-Simpson result because each Lipschitz function is absolutely continuous.

Tests-to-functions for Schnorr randomness

To prove the implication $\Leftarrow$ (tests-to-functions),

- one approach would be to build a saw teeth function as in the case of ML-randomness, but now for a given Schnorr test. However, this merely yields an absolutely continuous function, not a Lipschitz function.
- Instead, we took some inspiration from Zahorsky's 1946 result that each $G_{\delta\sigma}$ set in $[0,1]$ is the set of non-differentiability points of a Lipschitz function.
- (A recent 2007 paper by Fowler and Preiss does a simpler version of this proof. The 2010 ICM paper by Alberti, Csörnyei and Preiss looks at Lipschitz functions in higher dimensions.)

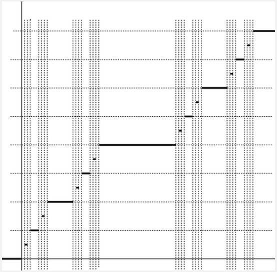
Tests-to-functions for Schnorr randomness

- Let $\mathcal{G} \subseteq [0,1]$ be c.e. open. Then $1_{\mathcal{G}}$ is L_1-computable $\Leftrightarrow \lambda\mathcal{G}$ is computable. This holds uniformly.
- Using this we can convert an (appropriately modified) Schnorr test $(\mathcal{G}_m)_{m\in\mathbb{N}}$ into a variation computable Lipschitz function f such that
$$\overline{D}f(z) = 1 \text{ and } \underline{D}f(z) = -1$$
for each z failing the test. The function has the form
$$f = \int_0^x \sum (-1)^m 1_{\mathcal{G}_m}.$$

Randomness notions that haven't yet been characterized by analysis

We say that z is weakly random (or Kurtz random) if z is in no null Π^0_1 class. A function h is called singular if $h'(x) = 0$ for a.e. x.

I think that weak randomness can be characterized via differentiability of computable singular functions; maybe they also need to be monotonic. An example is Cantor's function.



The graph of the Cantor function on the unit inverval

Randomness notions that haven't yet been characterized by analysis

Notions stronger than Martin-Löf's:

- Weak 2-randomness: open.
- Demuth randomness: Demuth showed that at a Demuth random z, each constructive f satisfies the Denjoy alternative. Martin-Löf randomness of z is not sufficient. The converse of Demuth's result is unknown.

Question: why do well-known notions in analysis correspond to algorithmic randomness notions? Could some analytic notion of functions yield a completely new randomness notion?