Randomness and differentiability

André Nies

The University of Auckland

With V. Brattka and J. S. Miller

A two-way interaction

Randomness

interacts with

Computability

We can replace computability by other fields

Randomness

interacts with

Effective descriptive set theory

Work by Martin-Löf, 1970, Hjorth, Nies (2008); Chong, N, Yu (2009); Kjos, Nies, Stephan and Yu (2009); Philipp Schlicht (recent)

We can replace computability by further fields

Randomness

interacts with

Efficient computability

Work by Yongge Wang (1998), Lutz, Mayordomo, and others; Nies (2003), etc.

The interaction studied in this talk:

Randomness

interacts with

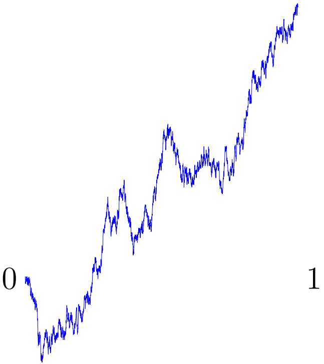
Computable analysis

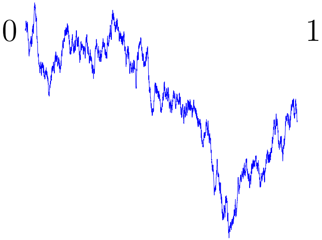
Main objects of study: computability theory versus analysis

- Computability: the focus is on sets of natural numbers. They can be identified with reals in $[0, 1)$.
- Computable analysis: the focus is on functions from reals to reals.

Random continuous functions

We can study randomness of continuous functions on the unit interval. Here are two examples (graphics due to M. Hoyrup):





This leads to Brownian motion and its effective aspects (Asarin, Fouché, P. and P. Potgieter, Kjos-Hanssen and Nerode, ...)

Functions as tests

A different approach is to

- retain the focus on the randomness of a real z, and
- use

  whether functions with particular properties
  are well-behaved at that real
  as a test for its randomness.

Main Thesis (details to follow)

Randomness of z is equivalent to differentiability at z.

Randomness

For many people, the primary intuition is of randomness for sequences of bits:

- 00100100 00111111 01101010 10001000 1000 ...
- 10010100 00010001 11110100 00101101 1111 ...
- 11101101 01111010 10101111 11001110 1110 ...

There is an (almost-) hierarchy of formal notions, corresponding to our intuition in varying degrees of accuracy:

$$\text{2-random} \Rightarrow \text{weakly 2-random} \Rightarrow \text{ML-random} \Rightarrow \text{Schnorr random.}$$

Randomness for reals

- Co-infinite sets of natural numbers can be identified with reals in $[0,1)$ via the binary representation. For instance,
  $0101010101\ldots$ becomes $1/3$;
  $00100100001111110110101010001000\ldots$ becomes $\pi - 3$
  (so that example from a previous slide wasn't really random).
- The product measure on Cantor space $2^{\mathbb{N}}$ is turned into the **uniform** (Lebesgue) measure on $[0,1]$, denoted λ.
- If a randomness notions is based on measure, it can be transferred right away to the reals in $[0,1]$ (in fact, to any computable probability space).

Computable randomness

- Schnorr (1975): ML-tests are already too powerful to be considered algorithmic.
- As a more restricted notion of a test, he proposed **computable betting strategies**, certain computable functions M from $\{0,1\}^*$ to the non-negative reals.
- Let $Z \subseteq \mathbb{N}$. When the player has seen $\sigma = Z\upharpoonright_n$, she can make a bet q, where $0 \le q \le M(\sigma)$, on what 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 $M(Z\upharpoonright_n)$ is unbounded.
- We call a set Z **computably random** if no computable betting strategy wins on Z.

Base invariance

- Computable randomness seems to be tied to sequences of bits, and hence to the binary representation of reals. Is it really?
- We can ask the same question about stronger variants of computable randomness: are they base dependent?
- Some notions between ML-randomness and computable randomness:

  Martin-Löf random $\Rightarrow$ KL-random $\Rightarrow$ permutation random
  $\Rightarrow$ partial comp'bly random $\Rightarrow$ comp'bly random.
- We know that computable randomness is base invariant.

A principle from classical analysis

- Let $\mathcal{P}$ be a "niceness" property of functions, taken from classical analysis.

- Several theorems from analysis say:

  "if you are nice, you behave well almost everywhere".

- More formally, we have:

"Nice $\Rightarrow$ well-behaved almost everywhere" principle

Every function $f\colon [0,1] \to \mathbb{R}$ satisfying niceness property $\mathcal{P}$ is well–behaved at almost every $x \in [0,1]$.

- We will give two instances of this principle.

Functions of bounded variation are differentiable a.e.

A function $f\colon [0,1] \to \mathbb{R}$ is of **bounded variation** if

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

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

Theorem (Classical Analysis)

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

λ-almost surely, $f'(x)$ exists.

Lebesgue differentiation theorem

Theorem (Classical Analysis)

Let g be integrable (i.e., $g \in \mathcal{L}^1([0,1],\lambda)$. Then λ-almost surely,

$$g(x) = lim_{r,s \to +0} \frac{1}{r+s} \int_{x-r}^{x+s} g(t) d\lambda(t).$$

Computable functions on the unit interval

Recall that we want to study randomness using tools from computable analysis. First we define computability of functions.

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.

Demuth's principle

Let $\mathcal{P}$ be a niceness property of functions from classical analysis.
Let $\mathcal{E}$ be an effectiveness condition on functions (such as being computable).

Demuth's principle (effective version of previous principle)

At each random real, every $\mathcal{E}$ function satisfying $\mathcal{P}$ is well-behaved.

Thus, the exception set for a nice and effective function is an effective null set, in a sense depending on $\mathcal{P}$ and $\mathcal{E}$.

Instances:

- At each computably random real, every computable function that is non-decreasing is differentiable. (Our first result).
- At each ML-random real, every computable function of bounded variation is differentiable. (Demuth 1975/ our second result).
- At each ML-random real, every $\mathcal{L}^1$-computable function satisfies the statement of the Lebesgue differentiation theorem (Noopur Pathak).

Converse of Demuth's principle

We show the converse for two instances of Demuth's principle.
Recall $\mathcal{P}$ is a property of functions from classical analysis;
$\mathcal{E}$ is an effectiveness condition on functions.

Converse of Demuth's principle

At each non-random real, some $\mathcal{E}$ function satisfying $\mathcal{P}$ is mis-behaved.

(This has no classical version because there, one only talks about null sets, not effective null sets.)

Instances of the converse:

- For each real z that is not computably random, there is a computable non-decreasing function f such that $\overline{D}f(z) = \infty$.
- There is, in fact, a single computable function of bounded variation that fails to be differentiable at all non-ML-random reals.

Computable randomness and differentiability

Let

$$\overline{D}g(z) = \limsup_{h \to 0, h \neq 0} \frac{g(z+h) - g(z)}{h}$$

Theorem

Let $z \in [0,1]$. Then the following are equivalent.

(i) *z is computably random.*

(ii) *$f'(z)$ exists for each computable nondecreasing function f.*

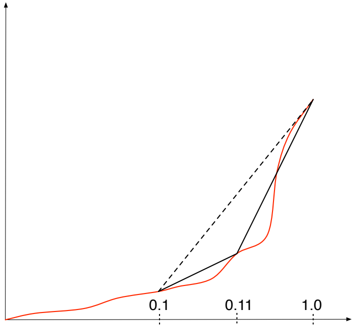
(iii) *$\overline{D}g(z) < \infty$ for each computable nondecreasing function g.*

Turning nondecreasing functions into martingales

(i)⇒(iii): If $\overline{D}g(z) = \infty$, then martingale M_g succeeds on z, where for a string σ, we let

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

Thus $M_g(\sigma)$ 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 $2M(1) = M(10) + M(11)$.



Turning martingales into nondecreasing functions

Proof of (iii)⇒(i):

Suppose z is not computably random. We want to show that $\overline{D}g(z) = \infty$ for some nondecreasing computable function g.

- Let M be a martingale with the savings property that succeeds on z.
- Let μ be the measure induced by M. It is determined by its values on the basic clopen sets: $\mu([\sigma]) = M(\sigma)2^{-|\sigma|}$. Then μ is non-atomic.
- Let

  $$g(x) = \mu[0, x].$$

  Then g is continuous nonincreasing, and $g(q)$ is computable for each dyadic rational q. So g is computable by a proposition we discussed earlier on.
- Since $M(\sigma) = (g(0.\sigma 1) - g(0.\sigma))/2^{-|\sigma|}$ and M succeeds on z, we have $\overline{D}g(z) = \infty$.

The implication (iii)⇒(ii)

(ii)⇒(iii) is trivial, so we are done if we can show (iii)⇒(ii).

- Recall the upper and lower derivatives:

$$\overline{D}f(z) = \limsup_{h\to 0} \frac{f(z+h)-f(z)}{h} \text{ and } \underline{D}f(z) = \liminf_{h\to 0} \frac{f(z+h)-f(z)}{h}$$

- Suppose that $f'(z)$ does not exist. We want to define a computable nondecreasing function g such that $\overline{D}g(z) = \infty$.
- If $\overline{D}f(z) = \infty$ we are done. Otherwise, since $f'(z)$ does not exist,

$$0 \leq \underline{D}f(z) < \overline{D}f(z).$$

Dyadic case

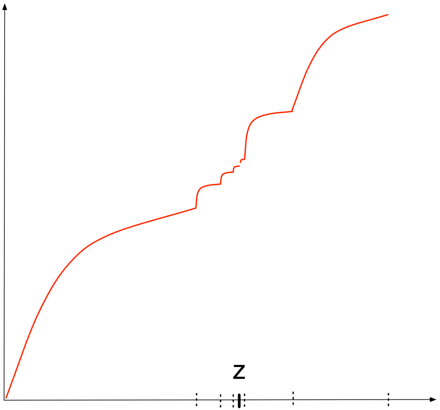
For a nonempty interval $A = [a, b]$ we let $S_f(A)$ be the **slope** $(f(b) - f(a))/(b - a)$.

- A **basic dyadic interval** has the form $[i2^{-n}, (i+1)2^{-n}]$ for some $i \in \mathbb{Z}, n \in \mathbb{N}$.
- Given $z \in [0, 1] - \mathbb{Q}$ let A_n be the dyadic interval of length 2^{-n} containing z.
- If we are lucky, then $\liminf_n S_f(A_n) < \beta < \gamma < \limsup_n S_f(A_n)$ for rationals $\beta < \gamma$.
- In this case we construct a computable M that succeeds on z essentially by the technique of the first Doob martingale convergence theorem.

(1) When $S_f(A) < \beta$, start betting like S_f on basic dyadic subintervals $B \subseteq A$. If $S_f(B) > \gamma$ switch to the non-betting state within B.
(2) On basic dyadic subintervals $C \subseteq B$, don't bet till $S_f(C) < \beta$. Now switch back to the betting state within C.

The dyadic case is not enough

It can happen that the hypothesis $\underline{D}f(z) < \overline{D}f(z)$ does not become apparent on the basic dyadic intervals. The following function f has $\underline{D}f(z) < \overline{D}f(z) = \infty$, but $S_f(A_n) = 1$ for each n.



The general case

- We define the desired nondecreasing computable function g such that $\overline{D}g(z) = \infty$ via a betting strategy Γ, with domain a tree rational intervals B, and range the non-negative reals. Then we determine g by $S_g(B) = \Gamma(B)$.
- For rationals q and $p > 0$, a (p, q)-interval is the image of a basic dyadic interval under the affine map $x \to px + q$.
- We show that there are rationals p, q and r, s such that

$$\liminf_{z \in A,\, A \text{ is } (p,q)-\text{interval}} S_f(A) < \limsup_{z \in B,\, B \text{ is } (r,s)-\text{interval}} .S_f(B)$$

- Strategy Γ is in the betting state on (p, q) intervals, and in the non-betting state on (r, s)-intervals.
- When Γ switches state, the current interval is split into intervals of the other type (usually, infinitely many). □

Martin-Löf randomness and differentiability

Recall that a function $f\colon [0,1] \to \mathbb{R}$ is of bounded variation if

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

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

Theorem

Let $z \in [0,1]$. Then
z is Martin-Löf random $\iff$
every computable function f of bounded variation
is differentiable at z.

For "$\Leftarrow$" we build a single computable function f of bounded variation that is only differentiable at ML-random reals.

Demuth's original result

A constructivist version of the implication "$\Rightarrow$" was already obtained by Demuth (1975).

Theorem (Demuth, 1975)

Every constructive function which cannot fail to be a function of weakly bounded variation is finitely pseudo-differentiable on each Π_2 number.

- A constructive function is a computable function well-defined on all indices for computable reals.
- Some constructive function does not extend to a computable function.

The implication "$\Rightarrow$" follows from the corresponding implication of the result for computable randomness

Suppose f is computable of bounded variation.
Let z is Martin-Löf random. We want to show $f'(z)$ exists.

- It is a classical result that $f = h_0 - h_1$ for some nondecreasing functions h_0, h_1.
- Even if f is computable, the functions h_0, h_1 cannot always be chosen computable. However, the pairs of names for such functions h_0, h_1 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 previous theorem relativized to z, the h_i are both differentiable at z. Thus $f'(z)$ exists.

Denjoy alternative

Theorem

Let f be an arbitrary function $[0,1] \to \mathbb{R}$. Then λ-almost surely, the **Denjoy alternative** *holds at x:*

$$f'(x) \text{ exists, or}$$

$$\overline{D}f(x) = \infty \text{ and } \underline{D}f(x) = -\infty.$$

Denjoy randomness

Definition (Kučera)

A real z is **Denjoy random** if for each computable f, the Denjoy alternative holds at z.

Corollary

Denjoy random implies computably random.

- Suppose z is Denjoy random.
- Let f be a nondecreasing computable function.
- Then $\underline{D}f(z) \geq 0$.
- Thus the Denjoy alternative at z implies that $f'(z)$ exists.
- Hence z is computably random.

Question

Does the converse implication hold?

Further questions

- Base invariance for partial computable and permutation randomness.
- Characterize further randomness notions by differentiability: Schnorr rd, Demuth rd, weakly 2-rd...
- Study left-c.e. nondecreasing functions g. For instance, is each continuous such g a variation, i.e., of the form $x \to V(f \upharpoonright [0, x])$ for some computable f?
- Connections to lowness properties.

References

- *Randomness and differentiability*, with Vasco Brattka and Joseph S. Miller.
  http://dl.dropbox.com/u/370127/papers/RandomnessAnalysis.pdf
- These slides, on Nies' web page at
  http://dl.dropbox.com/u/370127/talks/NiesRandomnessDifferentiability.pdf.
- Demuth's 1975 paper,
  http://dl.dropbox.com/u/370127/various/Demuth75.pdf