“Almost everywhere” theorems and algorithmic randomness

André Nies

U of Auckland

CCA 2012, Cambridge

“Almost everywhere” theorems (1)

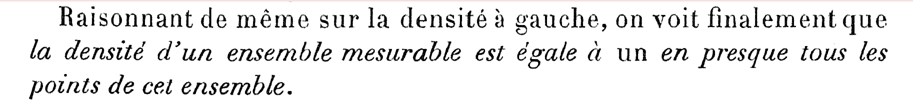
Several important theorems in analysis assert a property for almost every real z. We give two examples due to Lebesgue.

Theorem (Lebesgue’s Theorem, 1904/1910)

Let $f : [0,1] \to \mathbb{R}$ *be non-decreasing.*
Then the derivative $f'(z)$ *exists for almost every real* z.

“Almost everywhere” theorems (2)

From HENRI LEBESGUE, Sur l’ intégration des fonctions discontinues, Annales scientifiques de l’ É.N.S. 3e série, tome 27 (1910), p. 361-450; p. 407.



Raisonnant de même sur la densité à gauche, on voit finalement que *la densité d’un ensemble mesurable est égale à* un *en presque tous les points de cet ensemble.*

Translation:

Theorem (Lebesgue Density Theorem, 1910)

Let $E \subseteq [0,1]$ *be measurable. For almost every* $z \in [0,1]$*:*

if $z \in E$*, then* E *has density* 1 *at* z*.*

Effective versions of almost everywhere theorems

Now consider the case where the given objects are effective in some sense.

- How strong an algorithmic randomness notion for a real z is needed to make the theorem hold at z?
- Will the theorem in fact characterize the randomness notion?

- I will give an overview of results linking algorithmic randomness to differentiability.
- I will discuss exciting recent developments: the density of effectively closed sets at random members, and applications of this to the study of K-triviality.

1. A brief introduction to algorithmic randomness

Idea in algorithmic randomness

- One defines a notion of algorithmic null set.
- A real z is random in a particular sense if it avoids all null sets of this kind.
- There are only countably many null sets of this kind. So almost every z is random in that sense.

Randomness notions relevant to us:

Martin-Löf random $\Rightarrow$ computably random $\Rightarrow$ Schnorr random.

These implications are proper.

Computable randomness

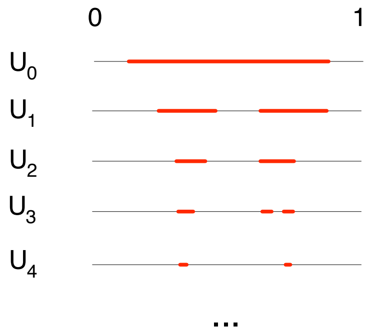
Computable betting strategies (martingales) are computable functions M from binary strings to the non-negative reals.

- 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. (These Z form an algorithmic null set.) We call a set Z computably random if no computable betting strategy wins on Z.

Martin-Löf's 1966 randomness notion

Infinite sequences Z of bits can be "identified" with reals numbers in $[0,1]$ via the binary expansion.

- A Martin-Löf test is an effective descending sequence $(U_m)_{m\in\mathbb{N}}$ of open sets in $[0,1]$ such that the measure of U_m is at most 2^{-m}.
- Intuitively, U_m is an attempt to approximate a real Z with accuracy 2^{-m}.
- Z passes the test if Z is not in all U_m.
- Z is ML-random if it passes all ML-tests.



Randomness via effective Vitali covers

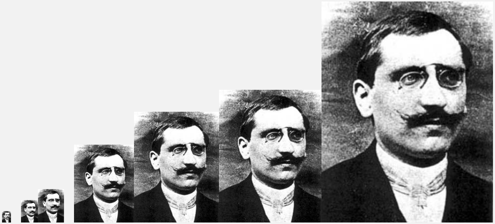
Let $(G_k)_{k\in\mathbb{N}}$ be a computable sequence of rational open intervals with $|G_k| \to 0$.
The set of points Vitali covered by $(G_k)_{k\in\mathbb{N}}$ is

$$\mathcal{V}(G_k)_{k\in\mathbb{N}} = \{z \colon\ z \text{ is in infinitely many } G_k\text{'s}\}.$$

Martin-Löf and Schnorr randomness also can be defined via effective Vitali covers.

- Martin-Löf random: not in any set $\mathcal{V}(G_k)_{k\in\mathbb{N}}$ where $\sum_k |G_k| < \infty$
- Schnorr random: not in any set $\mathcal{V}(G_k)_{k\in\mathbb{N}}$ where $\sum_k |G_k|$ is a computable real.

2. Effective versions of Lebesgue's first theorem



Theorem (Brattka, Miller, N; submitted)

Let $f : [0,1] \to \mathbb{R}$ *be non-decreasing and computable. Then*

$$z \textit{ is computably random} \Rightarrow f'(z) \textit{ exists.}$$

If f has bounded variation, then $f'(z)$ exists for each Martin-Löf random real z (Demuth, 1975).

Proving this: Functions-to-tests

- If f is computable nondecreasing, we (uniformly in f) build a computable martingale M such that

$$f'(z) \text{ fails to exist} \Rightarrow M \text{ succeeds on } z.$$

- If f is computable of bounded variation, we build a Martin-Löf test such that

$$f'(z) \text{ fails to exist} \Rightarrow \text{the test succeeds on } z.$$

Corollary

Each computable nondecreasing function f is differentiable at a (uniformly obtained) computable real.

PROOF: Each computable martingale fails on some computable real, which can be obtained uniformly.

This argument doesn't work for functions of bounded variation in general.

Converses (tests-to-functions)

- Both the nondecreasing and the bounded variation cases also have converses: if z is not random in the appropriate sense, then some computable function of the respective type fails to be differentiable at z (BMN, submitted).
- So computable analysts could take these properties as definitions!

z is computably random $\iff$
each computable nondecreasing function is differentiable at z

z is Martin-Löf random $\iff$
each computable function of bounded variation differentiable at z.

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, N, Stephan: submitted]

A real z is computably random

$$\Longleftrightarrow$$

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

$\Longrightarrow$: Write $f(x) = (f(x) + Cx) - Cx$. Then $f(x) + Cx$ is computable and non-decreasing.

From the monotone case (BMN), we obtain a test (martingale) for this function. If $f'(z)$ does not exists, then z fails this test.

$\Longleftarrow$: Turn success of a martingale on a real into oscillation of the slopes, around the real, of a Lipschitz function.

Rademacher's theorem

Theorem (Rademacher, 1920)

Let $f : [0,1]^n \to \mathbb{R}$ be Lipschitz.
Then the derivative $Df(z)$ (an element of $\mathbb{R}^n$) exists for almost every vector $z \in [0,1]^n$.

To define computable randomness of a vector $z \in [0,1]^n$:

- Take the binary expansion of the n components of z.
- We can bet on the corresponding sequence of blocks of n bits.

Conjecture

$z \in [0,1]^n$ is computably random $\Longleftrightarrow$ every computable Lipschitz function $f : [0,1]^n \to \mathbb{R}$ is differentiable at z.

Schnorr randomness and L_1-computability

Pathak, Rojas, and Simpson (2012) and Rute (2012) proved:

$z \in [0,1]^d$ is Schnorr random $\Longleftrightarrow$

for every L_1-computable function $g\colon [0,1]^d \to \mathbb{R}$, the usual limit exists:

$$\lim_{r\to 0} \frac{1}{\lambda(B_r(z))} \int_{B_r(z)} g.$$

This is an effective version of the Lebesgue differentiation theorem (but takes into account only the existence of limits).

3. Polytime randomness and analysis

Polynomial time randomness

Definition

- A martingale $M \colon 2^{<\omega} \to \mathbb{Q}$ is called polynomial time if from string σ can compute the rational $M(\sigma)$ in poly. time.
- A real z is polynomial time random if no polynomial time martingale succeeds on its binary expansion.

What's known on poly time randomness?

- Exists in all time classes properly containing P, such as $\mathrm{DTIME}(n^{\log n})$.
- Incomparable with Schnorr randomness!
- Implies nice statistical properties, such as absolutely normal.

Polynomial time functions $g\colon [0,1] \to \mathbb{R}$

- Recall a sequence of rationals $(p_i)_{i\in\mathbb{N}}$ is a Cauchy name if $\forall k > i \, |p_i - p_k| \leq 2^{-i}$
- Use a compact set of Cauchy names to represent reals (signed digit representation does it).
- g is polytime computable if there is a polytime oracle TM turning every Cauchy name for x into a Cauchy name for $g(x)$.

Functions like e^x, x^2, $\sin x$ are polynomial time.

Tests-to-functions

For a martingale M, the measure μ_M is given by

$$\mu_M([\sigma]) = 2^{|\sigma|} M(\sigma),$$

and distribution $g_M(x) = \mu_M[0, x)$.

- M has the savings property if $M(\sigma) \geq M(\tau) - 2$ whenever $\sigma \succeq \tau$.
- This implies $M(\sigma) = O(|\sigma|)$ so M grows slowly.
- In particular, μ_M has no atoms.

If M is poly time and has savings property, then g_M is poly time.

Characterization of polytime randomness via the lower derivative

Theorem [Nies, using BMN 2011]

A real z is NOT polytime random $\Longleftrightarrow$
some nondecreasing polytime function g satisfies $\underline{D}g(z) = +\infty$.

We can develop the theory of martingales with bases other than 2. We get the same connections with nondecreasing functions. Since the right side of the theorem is base invariant, we obtain

Corollary

Polytime randomness of a real is base invariant.

Figueira and his student Javier Silveira have a direct proof of this (2011, master thesis).

Questions on polytime randomness

Let z be a polynomial time random real.

- Does $f'(z)$ exist for each nondecreasing polytime computable f?
- Easier: does $f'(z)$ exist for each Lipschitz polytime computable f?

4. Further “almost everywhere” theorems and their effective content

Sard's theorem (suggested by Alex Galicki)

Theorem (Sard)

Let $S \subseteq \mathbb{R}^n$ *be open, and let* $f\colon S \to \mathbb{R}$ *be a* $\mathcal{C}^1$ *function. Then the set of values* $f(y)$ *where* $Df(y) = 0$ *has measure* 0.

Such a value $f(y)$ is called a critical value.

Galicki and N (2012): Suppose $f \in \mathcal{C}^1(0,1)$ is computable. If z is Martin-Löf-random, then z is not a critical value. (This also works in higher dimensions.)

- Idea: into the m-th component U_m of the Martin-Löf test, enumerate all intervals $K = (\min f(I), \max f(I))$, where I is an elementary dyadic interval such that $|K| < 2^{-m}|I|$.
- Converse (work in progress): if z is not Martin-Löf random, it is critical value of some computable $f \in \mathcal{C}^1(0,1)$.

Carleson-Hunt (suggested by Manfred Sauter)

Theorem (Carleson, 1966 for $p = 2$; improved by Hunt 1968)

Let $f \in \mathcal{L}^p[-\pi, \pi]$ be a periodic function. Then the Fourier series $c_N(z) = \sum_{|n| \leq N} \hat{f}(n) e^{inz}$ converges for almost every z.

We say z is weakly 2-random if z is in no null effective G_δ set. This properly implies Martin-Löf randomness.

Easy consequence of Carleson-Hunt theorem: if f is $\mathcal{L}^p$-computable, then weak 2-randomness of z suffices to make the sequence $c_N(z)$ converge. This is currently all we know.

Theorem (Weyl, 1916)

Let $(a_i)_{i\in\mathbb{N}}$ be a sequence of distinct integers. Then for almost every real z, the sequence $a_i z \mod 1$ is uniformly distributed in $[0,1]$.

Suppose now $(a_i)_{i\in\mathbb{N}}$ is computable. Avigad (2012) shows that

- Schnorr randomness of z suffices to make the conclusion of Weyl's theorem hold.
- There is a z satisfying the conclusion of the theorem which is in some null effectively closed set (hence not even "Kurtz random".)

What is the common motif behind all these effective a.e. theorems?

5. Density of effectively closed classes at random members

Lebesgue density

Let λ denote uniform (Lebesgue) measure.

Definition

Let $\mathcal{E}$ be a subset of $[0,1]$. The (lower) density of $\mathcal{E}$ at a real z is

$$\rho(z \mid \mathcal{E}) = \liminf_{|J| \to 0} \frac{\lambda(J \cap \mathcal{E})}{|J|},$$

where J ranges over intervals with rational endpoints containing z.

This gauges how much of E is around z as we zoom in on z.
Note that $\rho(z \mid \mathcal{E}) = \underline{D}g(z)$ where $g(x) = \lambda([0,x) \cap \mathcal{E})$.

Theorem (Lebesgue Density Theorem, 1910)

Let $\mathcal{E} \subseteq [0,1]$ be measurable. For almost every $z \in [0,1]$:

if $z \in \mathcal{E}$, then $\mathcal{E}$ has lower density 1 at z .

Theorem (Recall)

Let $\mathcal{E} \subseteq [0,1]$ be measurable. Then for almost every $z \in [0,1]$: if $z \in \mathcal{E}$, then has density 1 in $\mathcal{E}$.

- If $\mathcal{E}$ is open this is trivial, and actually holds for all $z \in [0,1]$.
- $\mathcal{E}$ closed is the first case where there is something to prove.
- If $\mathcal{E}$ is closed then any 1-generic $z \in \mathcal{E}$ has density one.

Does the strongest notion we have considered, Martin-Löf randomness, ensure density one? Answer: NO!

A Martin-Löf random of density zero

Example

Let $\mathcal{P} \neq \emptyset$, $\mathcal{P} \subseteq [0,1]$ be an effectively closed set of Martin-Löf randoms. Let $z = \min \mathcal{P}$. Then $\rho(z \mid \mathcal{P}) = 0$

This uses that every Martin-Löf random is Borel normal. Given k, pick n such that from positions n to $n+k-1$ we have 1's in the binary expansion of z. Let J be the interval $[0.z_0 \ldots z_{n-1}, 0.z_0 \ldots z_{n-1} + 2^{-n}]$. Then

$$\frac{\lambda(J \cap \mathcal{P})}{|J|} \leq 2^{-k}.$$

Note that the real $z = \min \mathcal{P}$ above, is left-r.e.. This means it is Turing complete. Intuitively, Martin-Löf randomness isn't strong enough a notion to ensure Density, because it allows for Turing completeness.

Turing incompleteness and positive density

Definition

We say that a real z is a positive density point if $\rho(z \mid \mathcal{P}) > 0$ for every effectively closed $\mathcal{P} \ni z$.

The following result shows that for positive density, Turing incompleteness is all we need.

Theorem (Bienvenu, Hölzl, Miller, N, STACS 2012)

Let z be a Martin-Löf random real. Then
z is Turing above the halting problem $\Longleftrightarrow$
z is a positive density point.

Using this to solve a long-standing open question

Reals in $[0, 1]$ are identified with subsets of $\mathbb{N}$ via the binary expansion. K denotes prefix free string complexity. K-trivial sets are far from random in a specific sense: there is b such that

$$\forall n \, K(A\restriction_n) \leq K(0^n) + b.$$

Many results assert that K-trivials are also close to computable.

Theorem (Day and Miller, recent)

Let $A \subseteq \mathbb{N}$ be K-trivial. Suppose $Z \subseteq \mathbb{N}$ is a Martin-Löf random set such that $Z \oplus A \geq_T \emptyset'$. Then already $Z \geq_T \emptyset'$.

The idea is to translate Turing incompleteness into a downward closed property for Π^0_1 classes.

Recall BHMN '12: Let Z be a Martin-Löf random real. Then $z \geq_T \emptyset' \iff Z$ is a positive density point.

Theorem (Day and Miller, recent)

Let $A \subseteq \mathbb{N}$ be K-trivial. Suppose $Z \subseteq \mathbb{N}$ is a Martin-Löf random set such that $Z \oplus A \geq_T \emptyset'$. Then already $Z \geq_T \emptyset'$.

- A K-trivial implies $A' \equiv_T \emptyset'$
- By one direction of [BHMN '12], if $Z \oplus A \geq_T \emptyset'$ then $Z \in \mathcal{P}$ for some $\Pi^0_1(A)$ class $\mathcal{P} \ni Z$ with $\rho(Z \mid P) = 0$.
- Known fact: Since A is K-trivial and Z random, for each $\Pi^0_1(A)$ class $\mathcal{P} \ni Z$ has a Π^0_1 class $\mathcal{Q}$ with $\mathcal{P} \supseteq \mathcal{Q} \ni Z$.
- Then $\rho(Z \mid \mathcal{Q}) = 0$.
- Hence, by the converse direction of [BHMN '12], this means that $Z \geq_T \emptyset'$.

A mystery notion: density-one points

Definition

We say that a real z is a density-one point if $\rho(z \mid \mathcal{P}) = 1$ for every effectively closed $\mathcal{P}$ containing z.

Question

Suppose z is Martin-Löf random. How much additional randomness is needed to ensure that z is a density-one point?

Interval-r.e. functions

Definition

A non-decreasing function f on $[0,1]$ with $f(0)=0$ is called interval-r.e. if $f(q)-f(p)$ is a left-r.e. real uniformly in rationals $p<q$.

If f is continuous, this implies lower semicomputable.

Recall that for $g\colon\ [0,1] \to \mathbb{R}$ we let

$$V(g,[0,x]) = \sup \textstyle\sum_{i=1}^{n-1} |g(t_{i+1}) - g(t_i)|,$$

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

Theorem (Freer, Kjos-Hanssen, N, Stephan, Rute 2012)

A continuous function f is interval-r.e. $\Longleftrightarrow$

there is a computable function g such that $f(x) = \mathrm{Var}(g,[0,x])$.

- If $\mathcal{U} \subseteq [0,1]$ is effectively open, then $g(x) = \lambda([0,x] \cap \mathcal{U})$ is interval-r.e.
- So, if $z \in \mathcal{P} = [0,1] \setminus \mathcal{U}$ and $g'(z)$ exists then $\rho(z \mid \mathcal{P}) = 1$.

For ML-random reals z, gauge deviation from T-complete:

$$\begin{tikzcd}
\text{z makes interval-r.e. functions differentiable} \arrow[r] & \text{z is a density one point} \arrow[r] & \text{z is a positive density point} \arrow[d, leftrightarrow] \\
& & z \not\geq_T \emptyset'
\end{tikzcd}$$

A new randomness notion

Definition

An interval test consists of a left-c.e. real α, and an effective monotone assignment of rational open intervals $I \subseteq [0,1]$ to Σ^0_1 classes $\mathcal{G}_I \subseteq [0,1]$, with $\lambda \mathcal{G}_I \leq \lambda I$; z fails the test if $z \in \bigcap_{\alpha \in I} \mathcal{G}_I$. z is Oberwolfach random if it passes each interval test.

- If α is computable, this yields the same as a ML-test. For various reasons OW-random is just slightly stronger than ML-random.
- For instance, recall that Y is LR-hard if every Y-random set is random relative to $\emptyset'$. Random Turing incomplete LR-hard sets exist, but are very close to Turing complete. We improved a result of BHMN 2012:

Theorem (Bienvenu et al. 2012)

If Y is ML-random but not OW-random, then Y is LR-hard.

Oberwolfach randomness and effective analysis

Theorem (Bienvenu, Greenberg, Kučera N, Turetsky 2012)

Let z be an Oberwolfach random real. Then

- every interval-r.e. nondecreasing function is differentiable at z.
- In particular, z is a density-one point.

No converses are known.

For ML-random reals z, gauge deviation from T-complete (2):

$$\begin{tikzcd}
\text{OW random} \arrow[r] & \text{z makes interval-r.e. functions differentiable} \arrow[r] & \text{z is a density one point} \arrow[r] & \text{z is a positive density point} \arrow[d, leftrightarrow] \\
z \not\geq_{LR} \emptyset' \arrow[u] & {} \arrow[r] & {} & z \not\geq_{T} \emptyset'
\end{tikzcd}$$

Summary

- Effective versions of “ almost everywhere” theorems frequently correspond to algorithmic randomness notions.
- Randomness to analysis: algorithmic randomness notions calibrate the strength of such theorems
- Analysis to randomness: the analytic theorems can be used to analyze the randomness notions. Analytic properties can gauge the deviation from Turing completeness of Martin-Löf randoms. This is in the focus of interest for the interaction of computability and randomness.

References

- "Randomness and Differentiability", with V. Brattka and J. Miller, submitted.
- "Algorithmic aspects of Lipschitz functions" with Freer and Kjos-Hanssen, submitted.
- "The Denjoy alternative for computable functions", with Bienvenu, Hoelzl, and Miller, STACS 2012.
- these and other slides, on my web page.
- The logic blog available on my web site