Differentiability of polynomial time computable functions

André Nies

March 7

STACS 2014

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

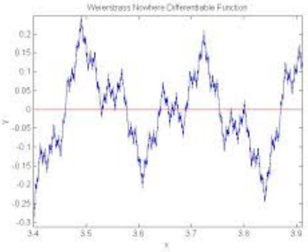
Lebesgue's measure

- In 1904 Lebesgue introduced his measure on the real line $\mathbb{R}$.
- It assigns a size to (all reasonable) subsets of $\mathbb{R}$.
- One can now say that a property holds for almost every real z: the set of exceptions has measure 0.

Differentiability

Differentiability of a function f at a real z means that the rate of change ("velocity") at z is defined:

$$f'(z) = \lim_{h \to 0} \frac{f(z+h) - f(h)}{h}.$$



Weierstrass proved in 1872 that some continuous function is nowhere differentiable.

In contrast:

Theorem (Lebesgue, 1904)

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

The plan

Theorem (Recall)

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

We study effective forms of Lebesgue's result.

- We assume that the non-decreasing function f will be computable in some sense.
- Then the exception set will consist of reals that fail an appropriate test for randomness. (Such exception sets have Lebesgue measure 0.)

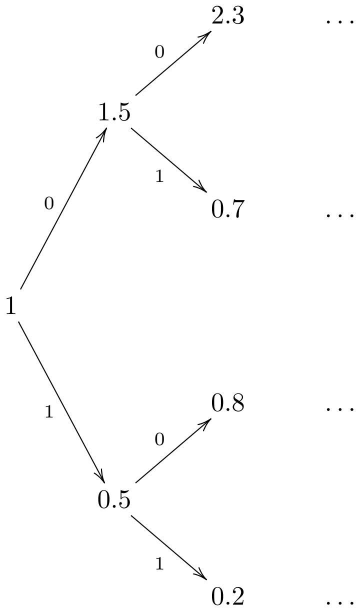
Computable randomness

Can one bet on bits of this sequence to make an unbounded profit?

10100111000101111010101000010101101111011000010111101010
10010101100011111010110001100111111101100000111001111000
00110011011110100011110100011100101011011001011100010110
01100110001111000010011001011101100100101000001110001111
11100100011000101111110100010111110011011100100110011010
00111111011010101101001101010110000011000001001101011100
01001001001011010001010000110100010100011100001100000100
11000111110111001000011001011010100111101111010101111111
00000001010011110010000000011011001010011010101101000010 . . .

A betting strategy M satisfies the "fairness condition" that the average of the values of the children is the value at the node.

We call a sequence of bits computably random if no computable betting strategy (martingale) has unbounded capital along the sequence.



Computable randomness and differentiability

Brattka, Miller and N (2011) proved an effective version of Lebesgue's theorem.

We say that function f is uniformly computable on the rationals if $f(q)$ is a computable real, uniformly in a rational $q \in [0,1]$.

Theorem (Brattka, Miller, Nies, 2011)

Let $z \in [0,1]$. Then
z (in binary) is computably random $\Longleftrightarrow$
$f'(z)$ exists, for each *non-decreasing* function f that is uniformly computable on the rationals.

Note that in this effective setting, we have the converse "$\Leftarrow$" as well. The theorem also works for the slightly stronger computability condition on f used in effective analysis.

First main theorem of the paper

For polynomial time computable non-decreasing functions, we obtain an analog of the Brattka, Miller, N 2011 result.

Theorem

$z \in [0, 1]$ is polynomial time random $\Longleftrightarrow$
$f'(z)$ exists, for each non-decreasing function f
that is polynomial time computable.

Second main theorem of the paper

Similar methods work for a class of non-decreasing functions larger than computable.

- A real z is called left-c.e. if the left cut $\{q \in \mathbb{Q}\colon\ q < z\}$ is computably enumerable.
- A non-decreasing function f is interval c.e. if $f(0) = 0$, and for any rational $q > p$, $f(q) - f(p)$ is a uniformly left-c.e. real.

Theorem

Every uniformly left-c.e. betting strategy converges along $z \in [0, 1]$
$\iff f'(z)$ exists for each interval-c.e. function f

The first condition is equivalent to:

z is Martin-Löf-random and every effectively closed set $\mathcal{C} \ni z$ has Lebesgue density 1 at z. (Miller et al., 2012).

Polynomial time computable functions

We represent a real z by an infinite string $b_0, b_1, \ldots$ over $\{-1, 0, 1\}$:

$$z = \sum_{k=0}^{\infty} b_k 2^{-k}.$$

The string $b_0, b_1, \ldots$ is called a special Cauchy name for z.

The following has been formulated in equivalent forms by Ker-i-Ko (1989), Weihrauch (2000), Braverman (2008), and others.

Definition

A function $g\colon [0,1] \to \mathbb{R}$ is polynomial time computable if there is a polynomial time TM turning every special Cauchy name for $x \in [0,1]$ into a special Cauchy name for $g(x)$.

This means that the first n symbols of $g(x)$ can be computed in time $\mathrm{poly}(n)$, thereby using polynomially many symbols of the oracle tape holding x.

Examples of polynomial time computable functions

- Functions such as $e^x, \sin x$ are polynomial time computable.

  To see this one uses rapidly converging approximation sequences, such as $e^x = \sum_n x^n/n!$. As Braverman points out, e^x is computable in time $O(n^3)$. Namely, from $O(n^3)$ symbols of x we can in time $O(n^3)$ compute an approximation of e^x with error $\leq 2^{-n}$.

- Breutzman, Juedes and Lutz (2001) give an example of a polynomial time computable function that is nowhere differentiable.

Polynomial time randomness

A betting strategy $M: 2^{<\omega} \to \mathbb{R}$ is called polynomial time computable if from string σ and $i \in \mathbb{N}$ we can in time polynomial in $|\sigma| + i$ compute the i-th component of a special Cauchy name for $M(\sigma)$.

Definition

We say Z is polynomial time random if no polynomial time betting strategy succeeds on Z.

This was studied in Yongge Wang's 1992 thesis, and more recently in Figueira, N 2013. There we showed that the notion is base invariant, and thus is about reals rather than bit sequences.

Theorem

The following are equivalent.

(I) $z \in [0, 1]$ is polynomial time random

(II) $f'(z)$ exists, for each non-decreasing function f that is polynomial time computable.

Proof of the easy direction (II) $\to$ (I)

Theorem

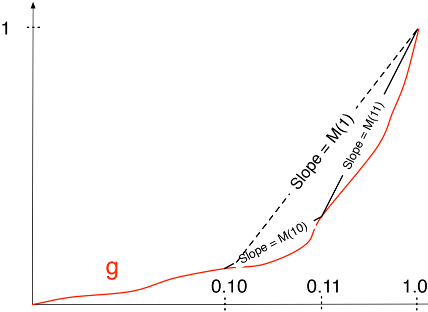
The following are equivalent.

(I) $z \in [0,1]$ is polynomial time random

(II) $f'(z)$ exists, for each non-decreasing function f that is polynomial time computable.

Let $S_g(\sigma)$ denote the slope of a non-decreasing function g at the dyadic interval given by string σ. This is a betting strategy.

Essentially each betting strategy M is of the form S_g. If M is polynomial time then so is g. Since $g'(z)$ exists, M is bounded along z.



Slopes and their limits

For a function $f\colon \mathbb{R} \to \mathbb{R}$, for a pair a, b of distinct reals let

$$S_f(a,b) = \frac{f(a) - f(b)}{a - b}.$$

The lower and upper (pseudo-)derivatives are

$$\underset{\sim}{D} f(x) = \liminf_{h \to 0^+} \{S_f(a,b) \mid a \le x \le b \wedge 0 < b - a \le h\},$$
$$\widetilde{D} f(x) = \limsup_{h \to 0^+} \{S_f(a,b) \mid a \le x \le b \wedge 0 < b - a \le h\}.$$

where a, b range over rationals in $[0,1]$.
The subscript 2 indicate restriction to basic dyadic intervals $[\sigma]$ containing z:

$$\widetilde{D}_2 f(x) = \limsup_{|\sigma| \to \infty} \{S_f(\sigma) \mid x \in [\sigma]\}.$$

Recall: if f is non-decreasing then $M(\sigma) = S_f(\sigma)$ is a betting strategy. We have basic connections:

- M succeeds on $z \Leftrightarrow \widetilde{D}_2 f(z) = \infty$.
- M converges on $z \Leftrightarrow \underset{\sim}{D}_2 f(z) = \widetilde{D}_2 f(z) < \infty$

Proof of the hard direction (I) → (II)

Theorem (Recall)

The following are equivalent.

(I) $z \in [0,1]$ is polynomial time random

(II) $f'(z)$ exists, for each non-decreasing function f that is polynomial time computable.

Main problem in proving the hard direction: to get from slope oscillation at arbitrary intervals around z to success of a betting strategy at dyadic intervals corresponding to prefixes of z's binary expansion.

- Consider the polynomial time computable betting strategy
$$M(\sigma) = S_f(\sigma) .$$
- $\lim_n M(Z \restriction_n)$ exists and is finite for each polynomially random Z. This is an effective version of Doob's martingale convergence theorem.
- Returning to the language of slopes, the convergence of M on Z means that $\underset{\sim}{D}_2 f(z) = \widetilde{D}_2 f(z) < \infty$.

(I) → (II): High dyadic slopes lemma

We say that a set $\mathcal{C} \subseteq \mathbb{R}$ is porous at z via the porosity factor $\varepsilon > 0$ if there exists arbitrarily small $\beta > 0$ such that $(z - \beta, z + \beta)$ contains an open interval of length $\varepsilon\beta$ that is disjoint from $\mathcal{C}$.

- Assume for a contradiction that $f'(z)$ fails to exist. First suppose that
$$\widetilde{D}_2 f(z) < p < \widetilde{D} f(z).$$
- Since $\widetilde{D}_2 f(z) < p$ there is a string $\sigma^* \prec Z$ such that $\forall \sigma\, [Z \succ \sigma \succeq \sigma^* \Rightarrow S_f(\sigma) \leq p]$.
- Choose k with $p(1 + 2^{-k+1}) < \widetilde{D} f(z)$.

Lemma (High dyadic slopes)

The closed set

$$\mathcal{C} = [\sigma^*] - \bigcup\{(\sigma)\colon\ \sigma \succeq \sigma^* \wedge S_f(\sigma) > p\}$$

contains z, but is porous at z via the factor $\varepsilon = 2^{-k-2}$.

(I) → (II): lucky and unlucky cases

Recall we are assuming that for a rational p

$$\widetilde{D}_2 f(z) < p \text{ and } p(1+2^{-k+1}) < \widetilde{D} f(z).$$

We may suppose $S_f(\sigma) < p$ for all dyadic intervals $[\sigma]$ containing z.

By the "high dyadic slopes" lemma, there exists arbitrarily large n such that some basic dyadic interval $[\tau_n]$ of length 2^{-n-k} has slope $> p$ and is contained in $[z - 2^{-n+2}, z + 2^{-n+2}]$.
Let $0.Z = z$ where Z is a sequence of bits.
$\prec$ denotes the prefix relation of strings.

Lucky case: there are infinitely many n with $\eta = Z\restriction_{n-4} \prec \tau_n$. Then the strategy that from such η on bets everything on the strings of length $n+k$ other than τ_n gains a fixed factor $2^{k+4}/(2^{k+4}-1)$ each time.

Unlucky case: for almost all n we have $Z\restriction_{n-4} \not\prec \tau_n$.
This means $0.\tau_n$ is on the left side of z, so the strategy can't use it as it splits off from Z before η is read.

(I) $\to$ (II): 1/3- shifting trick

Fix $m \in \mathbb{N}$. Consider an interval

$$I = [k2^{-m}, (k+1)2^{-m}]$$

where $k \in \mathbb{Z}$. Consider an interval

$$J = 1/3 + [r2^{-m}, (r+1)2^{-m}]$$

where $r \in \mathbb{Z}$.

The distance between an endpoint of I and an endpoint of J is at least $1/(3 \cdot 2^m)$.

(I) $\to$ (II): Using this trick to finish the proof

We may assume that $z > 1/2$. In the "unlucky" case that $Z \upharpoonright_{n-4} \not\prec \tau_n$ for almost all τ_n, we instead bet on the dyadic expansion Y of $z - 1/3$.

- Given $\eta' = Y \upharpoonright_{n-4}$, where n is as above, look for an extension $\tau' \succ \eta'$ of length $n + k + 1$, such that $1/3 + [\tau'] \subseteq [\tau]$ for a string $[\tau]$ with $S_f(\tau) > p$.
- If it is found, bet everything on the other extensions of η' of that length.

This strategy gains a fixed factor $2^{k+5}/(2^{k+5} - 1)$ each time.

So we get a polytime martingale that wins on $z - 1/3$. By Figueira and N (2013), polytime randomness is base invariant, so $z - 1/3$ is polynomially random. So this gives a contradiction.

The case $\underset{\sim}{D} f(z) < \underset{\sim}{D}_2 f(z)$ is analogous, using a "low dyadic slopes" lemma instead.

Further directions

Rademacher's theorem states that a Lipschitz function f on $\mathbb{R}^n$ is differentiable at almost every vector.

Question

Let the Lipschitz function f be polytime computable and z be a polynomial time random vector. Does $f'(z)$ exist?

Also, study Lebesgue density in feasible analysis.