Differentiability of polynomial time computable functions

André Nies

Department of Computer Science, University of Auckland, Auckland, New Zealand
andre@cs.auckland.ac.nz

Abstract

We show that a real z is polynomial time random if and only if each nondecreasing polynomial time computable function is differentiable at z. This establishes an analog in feasible analysis of a recent result of Brattka, Miller and Nies, who characterized computable randomness in terms of differentiability of nondecreasing computable functions.

Further, we show that a Martin-Löf random real z is a density-one point if and only if each interval-c.e. function is differentiable at z. (To say z is a density-one point means that every effectively closed class containing z has density one at z. The interval-c.e. functions are, essentially, the variation functions of computable functions.)

The proofs are related: they both make use of the analytical concept of porosity in novel ways, and both use a basic geometric fact on shifting dyadic intervals by 1/3.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Polynomial time randomness, feasible analysis, differentiability, porosity

Digital Object Identifier 10.4230/LIPIcs.STACS.2014.602

1 Main results

Recent research in algorithmic randomness has focussed on its interactions with computable analysis. Theorems from analysis stating the well-behaviour of a function almost everywhere (in the sense of measure) form a rich source of such interactions: effective versions of such theorems usually correspond to algorithmic randomness notions that have been studied in other contexts. For instance, Brattka, Miller and Nies showed the following effective version of a classical theorem due to Lebesgue.

▶ **Theorem 1** ([5], Thm. 4.1)**.** *Let $z \in [0,1]$. Then z is computably random $\Leftrightarrow$ $f'(z)$ exists for each nondecreasing computable function $f\colon [0,1] \to \mathbb{R}$.*

Here, a real z is computably random if no computable betting strategy can make unbounded profit when betting on the bits of a binary expansion of z; a nondecreasing function f is computable if and only if f is continuous and $f(q)$ is a computable real uniformly in a rational q. A result of Demuth [8] set in constructive language can be interpreted as the first theorem of this kind: Martin-Löf randomness of a real z corresponds to the differentiability at z of all computable functions of bounded variation. Other results along these lines are in [16, 17, 12].

An algorithm is called feasible if it can be carried out with bounded resources, which often means a running time that is polynomial in the size of the input. In feasible randomness/ feasible analysis, the underlying algorithmic concepts are re-interpreted in terms of feasible algorithms. For instance, a real $z \in [0,1]$ is called polynomial time random if no polynomial time betting strategy can make unbounded profit on the initial segments of its binary

© André Nies;
licensed under Creative Commons License CC-BY
31st Symposium on Theoretical Aspects of Computer Science (STACS'14).
Editors: Ernst W. Mayr and Natacha Portier; pp. 602–613
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

expansion. Despite its naturalness and potential applications, this concept is still poorly understood. First studied by Wang [18], its base-invariance was only recently shown [11]. Base-invariance means that to show the real z is non-random, we can equivalently bet on the symbols in a base-b expansion of z, for any $b > 2$. (The proof used lower derivatives, a concept from analysis.)

Our first main result, Theorem 4 below, is the full analog of Theorem 1 in the polynomial time setting. We use a particular case of the base invariance proved in [11], namely that polynomial time randomness is invariant under adding or subtracting 1/3.

Our second main result, Theorem 7 below, also starts from Theorem 1, but now relaxes the effectiveness hypothesis on the nondecreasing functions f considered. Instead of being computable, we only require that f is interval-c.e., which means that $f(0) = 0$ and the ternary relation "$q < f(y) - f(x)$", for $q, x, y \in \mathbb{Q} \cap [0, 1]$ and $x < y$, is computably enumerable. We show that the corresponding randomness notion obtained through Lebesgue's theorem is also one that had been previously studied: Martin-Löf randomness together with being a density-one point. Another classical result, the Lebesgue density theorem [13] asserts that for almost every point z in a measurable class $\mathcal{C} \subseteq [0, 1]$, the class is "thick" around z in that the relative measure of $\mathcal{C}$ converges to 1 as one "zooms in" on z. $\mathcal{C}$ is called effectively closed if its complement is an effective union of open intervals with rational endpoints. We say that a real z is a density-one point if the assertion of this theorem holds for every effectively closed class $\mathcal{C}$. In Theorem 4 we show that *a ML-random real z is a density-one point* $\Leftrightarrow$ *$f'(z)$ exists for each interval-c.e. function $f\colon [0, 1] \to \mathbb{R}$*. In fact we formulate Theorem 7 via a randomness condition that is known to be equivalent to being a Martin-Löf random density-one point (Andrews et al.; see [10]): every left-c.e. betting strategy (technically: a martingale as defined below) converges along the binary expansion of z.

The implication "$\Leftarrow$" is not hard to see: if a ML-random real z is not a density-one point as shown by an effectively closed class $\mathcal{P} \subseteq [0, 1]$, then the interval-c.e. function $f(x) = \lambda([0, x] - \mathcal{P})$ is not differentiable at z (where λ denotes Lebesgue measure). Below, we give an alternative argument using the martingale formulation.

Despite being at very different levels of effectiveness, our two main results can be proved by similar methods. They can be broadly described as "geometric", in the sense that measure is not needed, because it suffices to talk about interaction of classes with intervals. One main concept used is the following: a class $\mathcal{C}$ of reals is porous at a real z if $\mathcal{C}$ has 'holes' of fixed positive proportion in arbitrarily small intervals containing z (see Subsection 2.1). Both results rest on the fact that ill-behaviour of a function f at z (such as non-differentiability in a particular way) means that a class related to f is porous at z. This implies that z is not random in the appropriate sense. For instance, in the feasible case, porosity can be used directly to construct a polynomial time betting strategy that succeeds on z.

The other 'geometric' ingredient was observed for instance by Morayne and Solecki [14]: the endpoints of a basic dyadic interval of length 2^{-n}, and the shift by 1/3 of another basic dyadic interval of the same length, have to be apart by at least $2^{-n}/3$ (Subsection 3.2).

I thank Santiago Figueira and Alexander Galicki for helpful comments. I thanks Santiago and his parents for providing their apartment in Miramar, Argentina where most of this research was carried out.

1.1 Polynomial time randomness and differentiability

A Cauchy name is a sequence $(p_i)_{i\in\mathbb{N}}$ of rationals such that $|p_i - p_k| \leq 2^{-i}$ for each $k > i$. It is used to represent the real $\lim_i p_i$. For feasible analysis, one uses a compact set of Cauchy names. A *special* Cauchy name is given by an infinite sequence $b_0, b_1, \ldots$ from $\{-1, 0, 1\}^\omega$.

We let $p_i = \sum_{k=0}^{i} b_k 2^{-k}$. We call the b_k the *symbols* of the special Cauchy name. If we want to ensure that the represented real is in $[0,1]$, we ask that the sequence is 0^∞, or starts with $0^k 1 \ldots$ for some $k \in \mathbb{N}$, or starts with $10^k(-1)\ldots$, or is 10^∞. Since we have a 3-element input alphabet, a Turing machine (which has to rely on a fixed alphabet of symbols) can process the initial segments of such a sequence.

A martingale is a function $M\colon 2^{<\omega} \to \mathbb{R}_0^+$ such that $2M(\sigma) = M(\sigma 0) + M(\sigma 1)$ for each string σ. For a bit sequence $Z \in \{0,1\}^\omega$ we let $Z\restriction_n$ denote the initial segment of length n. We say that M *succeeds* on Z if $\limsup_n M(Z\restriction_n) = \infty$.

▶ **Definition 2.** A martingale M is called *polynomial time computable* if from a string σ and $i \in \mathbb{N}$ we can in time polynomial in $|\sigma| + i$ compute the first i symbols of a special Cauchy name for $M(\sigma)$.

We say that a bit sequence Z is *polynomial time random* if no polynomial time martingale succeeds on Z. Polynomial time randomness was first studied by Wang [18]. For a recent publication on it that also provides background see [11].

▶ **Definition 3** (see e.g. [19])**.** A function $g\colon [0,1] \to \mathbb{R}$ is called *polynomial time computable* if there is a polynomial time Turing machine turning every special Cauchy name for $x \in [0,1]$ into a special Cauchy name for $g(x)$.

In more detail, the first n symbols of $g(x)$ can be computed in time polynomial in n, thereby using polynomially many symbols of the oracle tape holding a special Cauchy name for x. Commonly occurring functions such as $e^x, \sin x$ are polynomial time computable, essentially because analysis gives us rapidly converging approximation sequences, such as $e^x = \sum_n x^n/n!$. We can extend the definition in an obvious way to functions $g\colon [0,1]^n \to \mathbb{R}$. The use of special Cauchy names ensures that basic functions such as addition and multiplication are polynomial time computable. Our first main result is:

▶ **Theorem 4.** *Let $z \in [0,1]$. Then z is polynomial time random $\Leftrightarrow$ $f'(z)$ exists for each nondecreasing polynomial time computable function $f\colon [0,1] \to \mathbb{R}$.*

We note that the implication "$\Rightarrow$" was independently announced by Miyabe and Kawamura (2013), who directly adapted the proof of [5, Thm. 4.1] to the polynomial time setting.

1.2 Left-c.e. martingales and differentiability of interval c.e. functions

A real z is called *left-computably-enumerable* (left-c.e. for short) if the set $\{q \in \mathbb{Q} : q < z\}$ is computably enumerable. A martingale $M\colon 2^{<\omega} \to \mathbb{R}_0^+$ is called left-c.e. if $M(\sigma)$ is a left-c.e. real uniformly in σ.

Consider a real $z \in [0,1] - \mathbb{Q}$. If a martingale M converges to a finite value at the binary expansion of z, we write $M(z)$ for this value.

▶ **Definition 5.** We say that z is a *convergence point for left-c.e. martingales* if $M(z)$ exists for each left-c.e. martingale M.

Recall that for a function $f\colon [0,1] \to \mathbb{R}$, the variation function at $x \in [0,1]$ is the supremum of the sums $\sum_i |f(t_{i+1}) - f(t_i)|$ for finer and finer partitions $0 = t_1 < \ldots < t_n = x$ of $[0,x]$. In order to identify the variation functions of computable functions, Freer, Kjos-Hanssen, Nies and Stephan [12] studied a class of non-decreasing functions which they called *interval-c.e.*

▶ **Definition 6.** A non-decreasing function $f\colon [0,1] \to \mathbb{R}$ is *interval-c.e.* if $f(0) = 0$, and $f(y) - f(x)$ is a left-c.e. real, uniformly in rationals $x < y$.

Note that the variation function of each computable function of bounded variation is continuous and interval-c.e. Freer et al. [12], together with Rute, showed that conversely, every continuous interval-c.e. function is the variation function of a computable function. For continuous functions, in Def. 6 we can drop the condition that x, y are rationals and instead require the seemingly stronger condition that $f(y) - f(x)$ is a left-c.e. real relative to Cauchy names for $x < y$ [12]. Our second main result is:

▶ **Theorem 7.** *$z \in [0,1]$ is a convergence point for left-c.e. martingales $\Leftrightarrow$ $f'(z)$ exists for each interval-c.e. function $f\colon [0,1] \to \mathbb{R}$.*

2 Preliminaries

2.1 Porosity and density

The proofs of our two main results use the notion of *porosity* which originates in the work of Denjoy. See for instance [6, Ex. 7:9.12], or [4, 5.8.124] (but note the typo in the definition there).

▶ **Definition 8.** We say that a set $\mathcal{C} \subseteq \mathbb{R}$ is *porous at z* via the constant $\varepsilon > 0$ if there exist arbitrarily small $\beta > 0$ such that $(z - \beta, z + \beta)$ contains an open interval of length $\varepsilon\beta$ that is disjoint from $\mathcal{C}$. We say that $\mathcal{C}$ is *porous at z* if it is porous at z via some $\varepsilon > 0$.

For the definitions below we follow [3]. Let λ denote Lebesgue measure. The *lower density* of a set $\mathcal{C} \subseteq \mathbb{R}$ at a point z is :

$$\varrho(\mathcal{C}|z) = \liminf_{z \in I \wedge |I| \to 0} \frac{\lambda(I \cap \mathcal{C})}{|I|},$$

where I ranges over intervals. The *lower dyadic density* $\varrho_2(\mathcal{C}|z)$ is the variant one obtains when one only considers basic dyadic intervals containing z. Clearly $\varrho_2(\mathcal{C}|z) \geq \varrho(\mathcal{C}|z)$. We say that z is a (full) *density-one point* if $\varrho(\mathcal{C}|z) = 1$ for every effectively closed class $\mathcal{C}$ containing z; z is a dyadic density-one point if $\varrho_2(\mathcal{C}|z) = 1$ for every effectively closed class $\mathcal{C}$ containing z.

▶ **Proposition 9** (Khan and Miller, see [10], Part 3)**.** *For a Martin-Löf random real z, being a dyadic density-one point implies being a full density-one point.*

The convergence points for left-c.e. martingales coincide with the Martin-Löf random density-one points. This was obtained by 2012 work of a group in Madison consisting of U. Andrews, M. Cai, D. Diamondstone, S. Lempp, and J. S. Miller. The implication "left-c.e. martingale convergence $\Rightarrow$ density one point" was already pointed out in [2]. The converse is harder to prove. See [10, Part 3] for a write-up due to Nies.

2.2 Slopes and martingales

First we need notation and a few definitions, mostly taken from [5] or [3]. For a function $f\colon [0,1] \to \mathbb{R}$, the *slope* at a pair a, b of distinct reals in its domain is

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

For a nontrivial interval A with endpoints a, b, we also write $S_f(A)$ instead of $S_f(a,b)$.

We let σ, τ range over (binary) strings. For such a string σ, by $[\sigma]$ we denote the closed basic dyadic interval $[0.\sigma, 0.\sigma + 2^{-|\sigma|}]$. The corresponding open basic dyadic interval is denoted (σ).

▶ **Fact 10.** *Let f be a non-decreasing polynomial time computable function. Then the function M_f given by $\sigma \to S_f([\sigma])$ is a martingale that is polynomial time computable.*

Proof. To compute the i-th symbol of a special Cauchy name for $M(\sigma)$, it suffices to compute the first $(|\sigma| + i + c)$ symbols of special Cauchy names for $f(0.\sigma)$ and $f(0.\sigma + 2^{-|\sigma|})$, where c is an appropriate constant. This can be done in time polynomial in $|\sigma| + i$. ◀

Derivatives. If z is in an open neighborhood of the domain of f, the *upper* and *lower derivatives* of f at z are

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

where as usual, h ranges over positive and negative values. The derivative $f'(z)$ exists if and only if these values are equal and finite.

We will also consider the upper and lower *pseudo*-derivatives defined by:

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

where a, b range over rationals in $[0, 1]$. We only use them because in our arguments it is often convenient to consider (rational) intervals containing x, rather than intervals with x as an endpoint.

▶ Remark. Brattka et al. [5, after Fact 2.4] verified that $\underline{D}f(z) \le \underset{\sim}{D}f(z) \le \widetilde{D}f(z) \le \overline{D}f(z)$ for any real $z \in [0, 1]$; furthermore, in [5, Fact 7.2] they showed that for continuous functions with domain $[0, 1]$, the lower and upper pseudo-derivatives of f coincide with the usual lower and upper derivatives.

These two pseudo-derivatives also coincide with the usual ones if f is nondecreasing. To show $\overline{D}f(z) \le \widetilde{D}f(z)$, fix an arbitrarily small $\epsilon > 0$. Given $h \neq 0$, choose rationals $a \le z$, $z + h \le b$ such that $(b - a) \le (1 + \epsilon)|h|$. Then $S_f(z, z + h) \le (1 + \epsilon)S_f(a, b)$. To show $\underset{\sim}{D}f(z) \le \underline{D}f(z)$, choose $[a, b]$ inside the interval given by $z, z + h$ with $|h| \le (1 + \epsilon)(b - a)$ and verify that $S_f(a, b) \le (1 + \epsilon)S_f(z, z + h)$.

We will use the subscript 2 to indicate that all the limit operations are restricted to the case of basic dyadic intervals containing z. Thus,

$$\widetilde{D}_2 f(x) = \limsup_{|A|\to 0} \{S_f(A) \mid x \in A \wedge A \text{ is basic dyadic interval}\},$$
$$\underset{\sim}{D}_2 f(x) = \liminf_{|A|\to 0} \{S_f(A) \mid x \in A \wedge A \text{ is basic dyadic interval}\}.$$

3 Lemmas on comparing derivatives, and on shifting intervals

3.1 A pair of analytical lemmas

The proofs of our main results combine effectiveness considerations with a pair of purely analytical lemmas. We show that discrepancy of dyadic and full upper/lower derivatives at z implies that some closed set is porous at z. The proof extends the idea in the proof of Proposition 9 due to Khan and Miller.

We denote by $\sigma \preceq \tau$ that σ is an initial segment of τ; $\sigma \prec \tau$ denotes that σ is a proper initial segment of τ; $\sigma \prec Z$ that σ is an initial segment of the infinite bit sequence Z.

▶ **Lemma 11.** *Suppose $f\colon [0,1] \to \mathbb{R}$ is a nondecreasing function. Suppose for a real $z \in [0,1]$, with binary representation $z = 0.Z$, there is rational p such that*

$$\widetilde{D}_2 f(z) < p < \widetilde{D} f(z).$$

Let $\sigma^* \prec Z$ be any string such that $\forall \sigma\, [\sigma^* \preceq \sigma \prec Z \Rightarrow S_f([\sigma]) \leq p]$. Then the closed set

$$\mathcal{C} = [\sigma^*] - \bigcup\{(\sigma) \mid S_f([\sigma]) > p\}, \tag{1}$$

which contains z, is porous at z.

Proof. Suppose $k \in \mathbb{N}$ is such that $p(1 + 2^{-k+1}) < \widetilde{D} f(z)$. We show that there exists arbitrarily large n such that some basic dyadic interval $[a, \tilde{a}]$ of length 2^{-n-k} is disjoint from $\mathcal{C}$, and contained in $[z - 2^{-n+2}, z + 2^{-n+2}]$. In particular, we can choose 2^{-k-2} as a porosity constant.

By choice of k there is an interval $I \ni z$ of arbitrarily short positive length such that $p(1 + 2^{-k+1}) < S_f(I)$. Let n be such that $2^{-n+1} > |I| \geq 2^{-n}$. Let a_0 be greatest of the form $\ell 2^{-n-k}$, $\ell \in \mathbb{Z}$, such that $a_0 < \min I$. Let $a_v = a_0 + v2^{-n-k}$. Let r be least such that $a_r \geq \max I$. Since f is nondecreasing and $a_r - a_0 \leq |I| + 2^{-n-k+1} \leq (1 + 2^{-k+1})|I|$, we have

$$S_f(I) \leq S_f(a_0, a_r)(1 + 2^{-k+1}),$$

and therefore $S_f(a_0, a_r) > p$. Then, by the averaging property of slopes at consecutive intervals of equal length, there is a $u < r$ such that

$$S_f(a_u, a_{u+1}) > p.$$

Since $(a_u, a_{u+1}) = (\sigma)$ for some string σ, this gives the required 'hole' in $\mathcal{C}$ which is near $z \in I$ and large on the scale of I: in Definition 8 (porosity), let $\beta = 2^{-n+2}$ and note that we have $[a_u, a_{u+1}] \subseteq [z - 2^{-n+2}, z + 2^{-n+2}]$ because $z \in I$ and $|I| < 2^{-n+1}$. ◀

There is a dual lemma for lower derivatives. Note that it can *not* simply be obtained from the preceding lemma by taking $-f$, because the function in the dual lemma is still non*de*creasing. In fact, now the shortish dyadic intervals we choose in the proof are all *contained in* I. (So we can achieve a porosity constant of 2^{-k-1}.)

▶ **Lemma 12.** *Suppose $f\colon [0,1] \to \mathbb{R}$ is a nondecreasing function. Suppose for a real $z \in [0,1]$, with binary representation $z = 0.Z$, there a rational q such that*

$$\underline{D} f(z) < q < \underline{D}_2 f(z).$$

Let $\sigma^* \prec Z$ be any string such that $\forall \sigma\, [\sigma^* \preceq \sigma \prec Z \Rightarrow S_f([\sigma]) \geq q]$. Then the closed set

$$\mathcal{C} = [\sigma^*] - \bigcup\{(\sigma) \mid S_f([\sigma]) < q\},$$

which contains z, is porous at z.

Proof. The argument is similar to the preceding one. We will show that we can choose as a porosity constant 2^{-k-1} where $k \in \mathbb{N}$ is such that $\underline{D} f(z) < q(1 - 2^{-k+1})$. There is an interval $I \ni z$ of arbitrarily short positive length such that $S_f(I) < q(1 - 2^{-k+1})$. As before, let n be such that $2^{-n+1} > |I| \geq 2^{-n}$. Let a_0 be least of the form $\ell 2^{-n-k}$, $\ell \in \mathbb{Z}$, such that $a_0 \geq \min(I)$. Let $a_v = a_0 + v2^{-n-k}$. Let r be greatest such that $a_r \leq \max(I)$.

Since f is nondecreasing and $a_r - a_0 \geq |I| - 2^{-n-k+1} \geq (1 - 2^{-k+1})|I|$, we have

$S_f(I) \geq S_f(a_0, a_r)(1 - 2^{-k+1})$,

and therefore $S_f(a_0, a_r) < q$. Then there is $u < r$ such that

$$S_f(a_u, a_{u+1}) < q.$$

As before, this gives the required 'hole' in $\mathcal{C}$ near $z \in I$. ◀

3.2 Basic dyadic intervals shifted by $1/3$

We prove the hard directions "⇒" in our main results by contraposition. We need to transform a condition formulated in the setting of real analysis (that a function is not differentiable at a real z) into a condition in Cantor space (that a martingale succeeds on the binary expansion Z of the real). To do so, we use a basic 'geometric' fact for instance observed by Morayne and Solecki [14]. For $m \in \mathbb{N}$ let $\mathcal{D}_m$ be the collection of intervals of the form

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

where $k \in \mathbb{Z}$. Let $\widehat{\mathcal{D}}_m$ be the set of intervals $(1/3) + I$ where $I \in \mathcal{D}_m$.

▶ **Lemma 13.** *Let $m \geq 1$. If $I \in \mathcal{D}_m$ and $J \in \widehat{\mathcal{D}}_m$, then the distance between an endpoint of I and an endpoint of J is at least $1/(3 \cdot 2^m)$.*

To see this, assume that $|k2^{-m} - (p2^{-m} + 1/3)| < 1/(3 \cdot 2^m)$. This yields $|3k - 3p - 2^m|/(3 \cdot 2^m) < 1/(3 \cdot 2^m)$, and hence $3|2^m$, a contradiction.

In order to apply Lemma 13, we may need values of nondecreasing functions $f\colon [0,1] \to \mathbb{R}$ at endpoints of any such intervals, which may lie outside $[0,1]$. So we think of f as extended to $[-1,2]$ via $f(x) = f(0)$ for $-1 \leq x < 0$ and $f(y) = f(1)$ for $1 < y \leq 2$. The effectiveness properties we consider here, polynomial time computable or interval-c.e. (defined in Section 2), are preserved by this. For the interval-c.e. functions, this is clear because it suffices to determine values of the function at rationals. In the polynomial time case, to represent reals in $[-1,2]$ by special Cauchy names (see Subsection 1.1), we now also allow sequences in $\{-1,0,1\}^\omega$ starting with $0^k(-1)\ldots$ and $10^k1\ldots$. To compute a value of the extended function for such a sequence, we let the Turing machine internally replace an input of the form $0^k(-1)\ldots$ by 0^∞ (which yields as an overall output a Cauchy name for $f(0)$), and an input of the form $10^k1\ldots$ by 10^∞ (which yields $f(1)$).

4 Proof of Theorem 4

We prove Theorem 4: a real z is polynomial time random ⇔ $f'(z)$ exists for each nondecreasing polynomial time computable function $f\colon [0,1] \to \mathbb{R}$.

Proof. ⇐: Suppose z is not polynomial time random. Then some polynomial time martingale succeeds on the binary expansion Z of z. A martingale M has the savings property if $M(\tau) \geq M(\sigma) - 2$ for each strings $\sigma \prec \tau$. By [11, Lemma 6], there is a polynomial time martingale M with the savings property that succeeds on Z.

Let μ_M be the corresponding measure given by $\mu_M([\sigma]) = 2^{-|\sigma|}M(\sigma)$. Let $f = \mathsf{cdf}_M$ be the cumulative distribution function of μ_M given by $\mathsf{cdf}_M(x) = \mu_M[0,x)$. Then $\underline{D}_2 f(z) = \infty$, so $f'(z)$ does not exist.

To show f is polynomial time computable, observe that by [11, Lemma 13], for each dyadic rational p, $f(p)$ is a dyadic rational that can be computed from p in polynomial time. Since M has the savings property, by [11, Prop. 12], f satisfies an 'almost-Lipschitz condition': there is $\epsilon > 0$ such that for every $x, y \in [0,1]$, if $x \leq y \leq x+\epsilon$, then $f(y) - f(x) = O((y-x)\cdot \log(1/y-x)$. This implies that f is polynomial time computable: Suppose we are given a special Cauchy name $(p_i)_{i\in\mathbb{N}}$ for a real z. We know that $|z - p_{n+\log n}| = O(2^{-n-logn})$. So by the almost-Lipschitz condition, we have $|f(z) - f(p_{n+\log n})| = O(2^{-n})$. Thus, a Turing machine can determine in polynomial time from the first $n + \log n$ symbols of the special Cauchy name for z the first n symbols of a special Cauchy name for $f(z)$.

$\Rightarrow$: We may assume $z > 1/2$. By the hypothesis on f and Fact 10, the martingale $M(\sigma) = S_f([\sigma])$ is polynomial time computable. Recall that a Cauchy name is a sequence $(p_i)_{i\in\mathbb{N}}$, $p_i \in \mathbb{Q}$, such that $\forall k > i\, |p_i - p_k| \leq 2^{-i}$. We denote by $M(\sigma)_u$ the u-th term of this Cauchy name, so that $|M(\sigma) - M(\sigma)_u| \leq 2^{-u}$.

Let Z be the bit sequence such that $z = 0.Z$. Since z is polynomial time random, $\lim_n M(Z\upharpoonright_n)$ exists. This is a polynomial time version of the Doob martingale convergence theorem; see, for instance [9, Thm. 7.1.3]. Returning to the language of slopes, the convergence of M on Z means that $\underset{\sim}{D}_2 f(z) = \widetilde{D}_2 f(z) < \infty$. Suppose now that $f'(z)$ fails to exist. Then by the remark near the end of Subsection 2.2, we have $\underset{\sim}{D} f(z) < \underset{\sim}{D}_2 f(z)$ or $\widetilde{D}_2 f(z) < \widetilde{D} f(z)$ since f is nondecreasing. We will show that Z is not polynomial time random for a contradiction.

First suppose that $\widetilde{D}_2 f(z) < \widetilde{D} f(z)$. Choose rationals r, p such that $\widetilde{D}_2 f(z) < r < p < \widetilde{D} f(z)$. Choose $u \in \mathbb{N}$ so large that $\widetilde{D}_2 f(z) < r - 2^{-u}$ and $r + 2^{-u} < p$. As usual let $Z \in \{0,1\}^\omega$ be such that $z = 0.Z$. Let n^* be sufficiently large so that $S_f(A) \leq r - 2^{-u}$ for each basic dyadic interval A containing z and of length $\leq 2^{-n^*}$. Choose k with $p(1 + 2^{-k+1}) < \widetilde{D} f(z)$. Then Lemma 11 applies via the string $\sigma^* = Z\upharpoonright_{n^*}$ (and the same value of k as in its proof).

We define polynomial time rational-valued martingales L, L' such that L succeeds on Z, or L' succeeds on Y, where $0.Y$ is the binary expansion of $z - 1/3$. By the base invariance of polynomial time randomness [11, Thm. 14], if the second case applies, the expansion of z in base 3 is not polynomial time random, and hence neither is Z, its expansion in base 2. Thus, in either case, Z is not polynomial time random.

Defining L. It suffices to consider strings $\sigma \succeq \sigma^*$. Let $L(\sigma^*) = 1$. Suppose $\eta \succeq \sigma^*$ and $L(\eta)$ has been defined. Check whether there is a string α of length $k+4$ such that $M(\eta\alpha)_u > r$.

If so, decrease the capital to 0 on $\eta\alpha$ (we know that $\eta\alpha \not\prec Z$, so this won't make us lose along Z). In return, increase the capital by a factor of $2^{k+4}/(2^{k+4}-1)$ along all strings $\eta\widehat{\alpha}$ such that $|\widehat{\alpha}| = k+4$ and $\widehat{\alpha} \neq \alpha$. Continue the strategy with all strings $\eta\widehat{\alpha}$.

If no such α exists, don't bet, that is, let $L(\eta 0) = L(\eta 1) = L(\eta)$. Continue with the strings $\eta 0$ and $\eta 1$.

Defining L'. Let $\rho^* = Y\upharpoonright_{n^*+1}$. It suffices to consider strings $\rho \succeq \rho^*$.

Let $L'(\rho^*) = 1$. Suppose $\rho \succeq \rho^*$ and $L'(\rho)$ has been defined. Check if there is a string β of length $k+5$ such that $[\rho\beta] + 1/3 \subseteq [\tau]$ for a string τ of length $|\rho\beta| - 1$, and $M(\tau)_u > r$.

If so, decrease the capital to 0 on $\rho\beta$ (we know that $\rho\beta \not\prec Y$). Increase the capital by a factor of $2^{k+5}/(2^{k+5}-1)$ along all strings $\rho\widehat{\beta}$ such that $|\widehat{\beta}| = k+5$ and $\widehat{\beta} \neq \beta$. Continue the strategy with all strings $\rho\widehat{\beta}$.

If no such β exists, don't bet, that is, let $L'(\rho 0) = L'(\rho 1) = L'(\rho)$. Continue with the strings $\rho 0$ and $\rho 1$.

We check that the martingale L can be computed in polynomial time. The rational $\gamma = (2^{k+4}-1)/2^{k+4}$ is dyadic of length $k+4$. First assume that σ is not intermediate between η and $\eta\alpha$ as above, that is, we don't have $\eta \prec \sigma$ and $|\sigma| < |\eta| + k + 4$. We can

efficiently decide whether $L(\sigma) = 0$. If $L(\sigma) \neq 0$, for an appropriate $\ell \leq |\sigma|/k$ that we can compute from σ, we have $L(\sigma) = \gamma^{-\ell}$. We can compute γ^r using a polynomial in $|\sigma|$ number of operations. Hence, since division is computable in polynomial time, we can compute in time polynomial in $|\sigma| + i$ the i-th component of a special Cauchy name for $\gamma^{-\ell}$.

If we do have $\eta \prec \sigma$ and $|\sigma| < |\eta| + k + 4$, we simply compute $L(\eta\gamma)$ for all γ of length $k + 4$ with $\sigma \prec \eta\gamma$, and output the average of these values.

By a similar argument, the martingale L' can be computed in polynomial time. We now show that L succeeds on Z, or L' succeeds on Y. Let $\mathcal{C}$ be the class from (1) in Lemma 11. Consider $n \geq n^* + 4$ and a 'hole' $[a, \tilde{a}] \cap \mathcal{C} = \emptyset$ where $[a, \tilde{a}]$ is a basic dyadic interval of length 2^{-n-k}, and $[a, \tilde{a}] \subseteq [z - 2^{-n+2}, z + 2^{-n+2}]$.

▶ **Claim 14.** *One of the following is true.*
(i) *$z, a, \tilde{a}$ are all contained in a single interval A taken from $\mathcal{D}_{n-4}$.*
(ii) *$z, a, \tilde{a}$ are all contained in a single interval A' taken from $\widehat{\mathcal{D}}_{n-4}$.*

To see this note that $\{a, \tilde{a}, z\}$ is contained in an interval of length 2^{-n+2}. Apply Lemma 13 and that $2^{-n+4}/3 > 2^{-n+2}$.

In case (i) let $A = [\eta]$, so that $\eta \prec Z$ (recall that $z \notin \mathbb{Q}$ so z is not an endpoint of A). Let $[a, \tilde{a}] = \eta\alpha$ where $|\alpha| = k + 4$. We have $z \notin [a, \tilde{a}]$, and L increases its capital by a factor of $2^{k+4}/(2^{k+4} - 1)$ along all strings $\eta\hat{\alpha}$ as above.

Now suppose case (ii) applies. Let ρ be the string such that $A' = [\rho] + 1/3$. There is an interval $[b, \tilde{b}]$ in $\widehat{\mathcal{D}}_{n+k+1}$ with $[b, \tilde{b}] \subseteq [a, \tilde{a}]$. Since (ii) holds we have $[b, \tilde{b}] = [\rho\beta]$ for some string β of length $k + 5$. We have $z \notin [b, \tilde{b}]$ and L' increases its capital by a factor of $2^{k+5}/(2^{k+5} - 1)$ along all strings $\rho\widehat{\beta}$ as above.

Note that the capital of L along Z, and of L' along Y, never decreases, because there is no basic dyadic interval $[\tau]$ containing z with $|\tau| \geq n^*$ and $S_f(\tau)_u \geq r$. Suppose that L fails on Z. Then for all sufficiently small holes $[a, \tilde{a}]$ case (ii) applies, so for sufficiently long $\gamma \prec Y$ we can find ρ with $\gamma \preceq \rho \prec Z$ such that L' increases its capital by a fixed factor > 1 on the next $k + 5$ bits of Y. So L' succeeds on Y.

The case $\underline{D}f(z) < \underline{D}_2 f(z)$ is analogous, using Lemma 12 instead of Lemma 11. ◀

A bit sequence is called computably stochastic if no computable selection rule can lead to an asymptotic imbalance of 0s and 1s; see e.g. [15, 7.6.2] or [9] for the formal definition. Ambos-Spies et al. [1] also studied the polynomial time version of this notion. They showed that $X \in \{0, 1\}^\omega$ is computably [polynomial time] stochastic iff no computable [polynomial time] martingale that uses only finitely many, positive rational betting factors can win on X. The martingales L, L' constructed above are of this kind after a slight modification in order to avoid betting capital 0.

▶ **Corollary 15.** *Suppose that a binary expansion of a real z is polynomial time stochastic. Then for each nondecreasing polynomial time computable function $f\colon [0, 1] \to \mathbb{R}$, we have $\widetilde{D}_2 f(z) = \widetilde{D} f(z)$ and $\underline{D}_2 f(z) = \underline{D} f(z)$.*

5 Proof of Theorem 7

Theorem 7 states that a real z is a convergence point for left-c.e. martingales $\Leftrightarrow$ $f'(z)$ exists for each interval-c.e. function $f\colon [0, 1] \to \mathbb{R}$.

The implication "$\Leftarrow$" is the easier one as already noted above. For a proof in the language of martingales, suppose a left-c.e. martingale M diverges along the binary expansion of z.

Let μ_M be the measure on $[0,1]$ corresponding to M, and let $\mathsf{cdf}_M(x) = \mu_M[0,x)$. Then cdf_M is interval-c.e. and $\mathsf{cdf}'_M(z)$ fails to exist.

5.1 Porosity and upper derivatives

Recall that in Definition 8 we introduced the notion that a class of reals is porous at a real.

▶ **Definition 16** ([3]). We call a real $z \in [0,1]$ a *porosity point* if some effectively closed class to which z belongs is porous at z. Otherwise, z is a *non-porosity point*.

For instance, every density-one point in the sense of Subsection 2.1 is a non-porosity point. The converse fails: every Turing incomplete Martin-Löf random real is a non-porosity point by [3], but not necessarily a density-one point [7].

▶ **Proposition 17.** *Let $f\colon [0,1] \to \mathbb{R}$ be interval-c.e. Then $\widetilde{D}_2 f(z) = \widetilde{D} f(z)$ for each non-porosity point z.*

Proof. Assume $\widetilde{D}_2 f(z) < \widetilde{D} f(z)$. Since f is interval-c.e., the function $\sigma \to S_f([\sigma])$ is a left-c.e. martingale. In particular, the class $\mathcal{C}$ defined in (1) in Lemma 11 is effectively closed. This class is porous at z for a contradiction. ◀

▶ Remark. If f is interval *right*-c.e. (in the obvious sense), we can apply the dual Lemma 12 to conclude that $\underset{\sim}{D} f(z) = \underset{\sim}{D}_2 f(z)$ for each non-porosity point z. For instance, let f be the Lipschitz function given by $f(x) = \lambda([0,x] \cap \mathcal{P})$ for an effectively closed class $\mathcal{P}$. Then we may conclude that the (lower) dyadic density of $\mathcal{P}$ at a non-porosity point x coincides with the (lower) full density, a variation on Proposition 9.

5.2 From dyadic to full derivative

We proceed to the proof of the implication "⇒". We may assume $z > 1/2$. The real z is a dyadic density-one point, hence a (full) density-one point by Prop. 9. Then $z - 1/3$ is also a ML-random density-one point. So, using the work of the Madison group discussed at the end of Subsection 2.1, the real $z - 1/3$ is also a c.e. martingale convergence point. In particular, both z and $z - 1/3$ are non-porosity points.

By the hypothesis on z and since S_f is a left-c.e. martingale, we have $\underset{\sim}{D}_2 f(z) = \widetilde{D}_2 f(z)$. By Proposition 17, we have $\widetilde{D}_2 f(z) = \widetilde{D} f(z)$. To complete the proof of "⇒" in Theorem 7, it remains to be shown that

$$\underset{\sim}{D} f(z) = \underset{\sim}{D}_2 f(z). \tag{2}$$

Then, since f is nondecreasing, by the remark near the end of Subsection 2.2 $f'(z)$ exists.

The plan is to show for a contradiction that if $\underset{\sim}{D} f(z) < \underset{\sim}{D}_2 f(z)$, then one of z, $z - 1/3$ is a porosity point. Note that in Cantor space we can apply notions of porosity via the usual transfer to $[0,1]$ given by the binary expansion; further, if a class $\mathcal{G} \subseteq \{0,1\}^\omega$ is porous at $Y \in \{0,1\}^\omega$, then its image in $[0,1]$ is porous at $0.Y$. We will actually show one of z, $z - 1/3$ is a porosity point in the sense of Cantor space, via Π^0_1 classes $\mathcal{E}$ and $\widehat{\mathcal{E}}$ defined below.

As in Fact 10, let $M = M_f$ be the martingale given by $\sigma \to S_f([\sigma])$. Note that M converges on z by hypothesis (recall that we write $M(z)$ for the limit). Thus $\underset{\sim}{D}_2 f(z) = \widetilde{D}_2 f(z) = M(z)$.

Let $\widehat{f}(x) = f(x + 1/3)$, and let $\hat{M} = M_{\widehat{f}}$. We now show that $\hat{M}$ converges on $z - 1/3$, and that the limits coincide.

▶ **Claim 18.** $M(z) = \hat{M}(z - 1/3)$.

As remarked above, $z - 1/3$ is also a convergence point for c.e. martingales. So $\hat{M}$ converges on $z - 1/3$. If $M(z) < \hat{M}(z - 1/3)$ then $\widetilde{D}_2 f(z) < \widetilde{D} f(z)$. However, z is a non-porosity point, so this contradicts Proposition 17. If $\hat{M}(z - 1/3) < M(z)$ we argue similarly using that $z - 1/3$ is a non-porosity point. This establishes the claim.

Assume for a contradiction that (2) fails. We extend the method in the proof of Lemma 12, taking into account both dyadic intervals, and dyadic intervals shifted by 1/3. For this recall the notation in Subsection 3.2. Also recall that $\underset{\sim}{D}_2 f(z) = M(z)$.

We can choose rationals p, q such that

$$\underset{\sim}{D} f(z) < p < q < M(z) = \hat{M}(z - 1/3).$$

Let $k \in \mathbb{N}$ be such that $p < q(1 - 2^{-k+1})$. Let u, v be rationals such that

$$q < u < M(z) < v \text{ and } v - u \leq 2^{-k-3}(u - q).$$

Let $n^* \in \mathbb{N}$ be such that for each $n \geq n^*$ and any interval $A \in \mathcal{D}_n \cup \widehat{\mathcal{D}}_n$ containing z, we have $S_f(A) \geq u$. Let

$$\begin{aligned} \mathcal{E} &= \{X \in \{0,1\}^\omega \colon \forall n \geq n^* M(X\restriction_n) \leq v\} \\ \widehat{\mathcal{E}} &= \{W \in \{0,1\}^\omega \colon \forall n \geq n^* \hat{M}(W\restriction_n) \leq v\} \end{aligned}$$

Since f is interval-c.e., M and $\hat{M}$ are left-c.e. martingales, so these classes are effectively closed. Let Z be the bit sequence such that $z = 0.Z$. By the choice of n^* we have $Z \in \mathcal{E}$. Let Y be the bit sequence such that $0.Y = z - 1/3$. We have $Y \in \widehat{\mathcal{E}}$.

Consider an interval $I \ni z$ of positive length $\leq 2^{-n^*-3}$ such that $S_f(I) \leq p$. Let n be such that $2^{-n+1} > |I| \geq 2^{-n}$. Let a_0 [resp., b_0] be least of the form $w2^{-n-k}$ [resp., $w2^{-n-k} + 1/3$], where $w \in \mathbb{Z}$, such that a_0 [resp., b_0] $\geq \min(I)$. Let $a_i = a_0 + i2^{-n-k}$ and $b_j = b_0 + j2^{-n-k}$. Let r, s be greatest such that $a_r \leq \max(I)$ and $b_s \leq \max(I)$.

As before, since f is nondecreasing and $a_r - a_0 \geq |I| - 2^{-n-k+1} \geq (1 - 2^{-k+1})|I|$, we have $S_f(I) \geq S_f(a_0, a_r)(1 - 2^{-k+1})$, and therefore $S_f(a_0, a_r) < q$. Then there is an $i < r$ such that $S_f(a_i, a_{i+1}) < q$. Similarly, there is $j < s$ such that $S_f(b_j, b_{j+1}) < q$.

▶ **Claim 19.** *One of the following is true.*

(i) *z, a_i, a_{i+1} are all contained in a single interval taken from $\mathcal{D}_{n-3}$.*

(ii) *z, b_j, b_{j+1} are all contained in a single interval taken from $\widehat{\mathcal{D}}_{n-3}$.*

For suppose that (i) fails. Then there is an endpoint of an interval $A \in \mathcal{D}_{n-3}$ (that is, a number of the form $w2^{-n+3}$ with $w \in \mathbb{Z}$) between $\min(z, a_i)$ and $\max(z, a_{i+1})$. Note that $\min(z, a_i)$ and $\max(z, a_{i+1})$ are in I. By Fact 13 and since $|I| < 2^{-n+1}$, there can be no endpoint of an interval $\hat{A} \in \widehat{\mathcal{D}}_{n-3}$ in I. Then, since $b_j, b_{j+1} \in I$, (ii) holds. This establishes the claim.

Suppose I is an interval as above and $2^{-n+1} > |I| \geq 2^{-n}$, where $n \geq n^* + 3$. Let $\eta = Z\restriction_{n-3}$ and $\hat{\eta} = Y\restriction_{n-3}$.

If (i) holds for this I then there is a string α of length $k + 3$ (where $[\eta\alpha] = [a_i, a_{i+1}]$) such that $M(\eta\alpha) < q$. So by the choice of $q < u < v$ and since $M(\eta) \geq u$ there is β of length $k + 3$ such that $M(\eta\beta) > v$. (The decrease along $\eta\alpha$ of the martingale M must be balanced by an increase along some $\eta\beta$.) This yields a hole in $\mathcal{E}$, large and near Z on the scale of I, which is required for porosity of $\mathcal{E}$ at Z. Similarly, if (ii) holds for this I, then there is a string α of length $k + 3$ (where $[\hat{\eta}\alpha] = [b_j, b_{j+1}]$) such that $M(\hat{\eta}\alpha) < q$. So by the choice of

$q < u < v$ and since $\hat{M}(\hat{\eta}) \geq u$ there is a string β of length $k+3$ such that $\hat{M}(\hat{\eta}\beta) > v$. This yields a hole large and near Y on the scale of I required for porosity of $\widehat{\mathcal{E}}$ at Y.

Thus, if case (i) applies for arbitrarily short intervals I, then $\mathcal{E}$ is porous at Z, whence z is a porosity point. Otherwise (ii) applies for intervals below a certain length. Then $\widehat{\mathcal{E}}$ is porous at Y, whence $z - 1/3$ is a porosity point.

References

1 K. Ambos-Spies, E. Mayordomo, Y. Wang, and X. Zheng. Resource-bounded balanced genericity, stochasticity and weak randomness. In *STACS 96 (Grenoble, 1996)*, volume 1046 of *Lecture Notes in Comput. Sci.*, pages 63–74. Springer, Berlin, 1996.

2 L. Bienvenu, N. Greenberg, A. Kučera, A. Nies, and D. Turetsky. K-triviality, Oberwolfach randomness, and differentiability. Mathematisches Forschungsinstitut Oberwolfach, preprint, 40 pages, 2012.

3 L. Bienvenu, R. Hölzl, J. Miller, and A. Nies. Demuth, Denjoy, and Density. Submitted, available at `http://arxiv.org/abs/1308.6402`, 2013.

4 V. I. Bogachev. *Measure theory. Vol. I, II.* Springer-Verlag, Berlin, 2007.

5 V. Brattka, J. Miller, and A. Nies. Randomness and differentiability. Submitted, `http://arxiv.org/abs/1104.4465`.

6 A. Bruckner, J. Bruckner, and B. Thomson. *Real Analysis.* Prentice Hall (Pearson), 2007.

7 A. R. Day and J. S. Miller. Density, forcing and the covering problem. Submitted, `http://arxiv.org/abs/1304.2789`, 2013.

8 O. Demuth. The differentiability of constructive functions of weakly bounded variation on pseudo numbers. *Comment. Math. Univ. Carolin.*, 16(3):583–599, 1975. Russian.

9 R. Downey and D. Hirschfeldt. *Algorithmic randomness and complexity.* Springer-Verlag, Berlin, 2010. 855 pages.

10 A. Nies (editor). Logic Blog 2013. Available at `http://dl.dropbox.com/u/370127/Blog/Blog2013.pdf`, 2013.

11 S. Figueira and A. Nies. Feasible analysis, randomness, and base invariance. Theory of Computing Systems, published electronically Oct 2013, DOI 10.1007/s00224-013-9507-7.

12 C. Freer, B. Kjos-Hanssen, A. Nies, and F. Stephan. Effective aspects of Lipschitz functions. To appear in Computability.

13 H. Lebesgue. Sur les intégrales singulières. *Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys. (3)*, 1:25–117, 1909.

14 M. Morayne and S. Solecki. Martingale proof of the existence of Lebesgue points. *Real Anal. Exchange*, 15(1):401–406, 1989/90.

15 A. Nies. *Computability and randomness*, volume 51 of *Oxford Logic Guides.* Oxford University Press, Oxford, 2009.

16 N. Pathak. A computational aspect of the Lebesgue differentiation theorem. *J. Log. Anal.*, 1:Paper 9, 15, 2009.

17 N. Pathak, C. Rojas, and S. G. Simpson. Schnorr randomness and the Lebesgue differentiation theorem. *Proc. Amer. Math. Soc.*, 142(1):335–349, 2014.

18 Y. Wang. *Randomness and Complexity.* PhD dissertation, University of Heidelberg, 1996.

19 K. Weihrauch. *Computable Analysis.* Springer, Berlin, 2000.