TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 368, Number 1, January 2016, Pages 581–605
http://dx.doi.org/10.1090/tran/6484
Article electronically published on May 27, 2015

RANDOMNESS AND DIFFERENTIABILITY

VASCO BRATTKA, JOSEPH S. MILLER, AND ANDRÉ NIES

Abstract. We characterize some major algorithmic randomness notions via differentiability of effective functions.
(1) As the main result we show that a real number $z \in [0,1]$ is computably random if and only if each nondecreasing computable function $[0,1] \to \mathbb{R}$ is differentiable at z.
(2) We prove that a real number $z \in [0,1]$ is weakly 2-random if and only if each almost everywhere differentiable computable function $[0,1] \to \mathbb{R}$ is differentiable at z.
(3) Recasting in classical language results dating from 1975 of the constructivist Demuth, we show that a real z is Martin-Löf random if and only if every computable function of bounded variation is differentiable at z, and similarly for absolutely continuous functions.

We also use our analytic methods to show that computable randomness of a real is base invariant and to derive other preservation results for randomness notions.

1. Introduction

The main thesis of this paper is that algorithmic randomness of a real is equivalent to differentiability of effective functions at the real. In more detail, for every major algorithmic randomness notion, one can provide a class of effective functions on the unit interval so that

$(*)$ a real $z \in [0,1]$ satisfies the randomness notion $\Leftrightarrow$ each function in the class is differentiable at z.

For instance, z is computably random $\Leftrightarrow$ each computable nondecreasing function is differentiable at z. Furthermore, z is Martin-Löf random $\Leftrightarrow$ each computable function of bounded variation is differentiable at z. The second result was proved by Demuth [4], who used constructive language; we will reprove it here in the usual language, using the first result relativized to an oracle set.

Classically, to say that a property holds for a "random" real $z \in [0,1]$ simply means that the reals failing the property form a null set. For instance, a well-known

Received by the editors November 21, 2012 and, in revised form, November 22, 2013.
2010 *Mathematics Subject Classification.* Primary 03D32, 03F60; Secondary 26A27, 26A48, 26A45.
Key words and phrases. Computable analysis, algorithmic randomness, differentiability, monotonic function, bounded variation.
The first author was supported by the National Research Foundation of South Africa.
The second author was supported by the National Science Foundation under grants DMS-0945187 and DMS-0946325, the latter being part of a Focused Research Group in Algorithmic Randomness.
The third author was partially supported by the Marsden Fund of New Zealand, grant no. 08-UOA-187.

theorem of Lebesgue [11] states that every nondecreasing function $f\colon [0,1] \to \mathbb{R}$ is differentiable at all reals z outside a null set (depending on f). That is, $f'(z)$ exists for a random real z in the sense specified above. Via Jordan's result that each function of bounded variation is the difference of two nondecreasing functions (see, for instance, [1, Cor. 5.2.3]), Lebesgue's theorem can be extended to functions of bounded variation. In most of the results of the type $(*)$ above, the implication " $\Rightarrow$ " can be seen as an effective form of Lebesgue's theorem.

For background on algorithmic randomness see [5, 12]. We work with the generally accepted notion of a computable function $[0,1] \to \mathbb{R}$ going back to work of Grzegorczyk and Lacombe from the 1950s. See Pour-El and Richards, [15, Def. A, p. 25].

We note that this paper has been shortened for space reasons. The unabridged version [2] is available at `http://arxiv.org/abs/1104.4465`. It contains some background on randomness and computable analysis, includes some proofs of basic facts omitted here, and also illustrates proofs given here. The arXiv version will be occasionally referred to in this paper.

1.1. **Results of type $(*)$: the implication "$\Rightarrow$".**

(a) We will show in Theorem 4.3 that

a real $z \in [0,1]$ is computably random $\Rightarrow$
each nondecreasing computable function is differentiable at z.

This is an effectivization of Lebesgue's theorem in terms of the concepts given above. Lebesgue's theorem is usually proved via Vitali coverings. This method is nonconstructive; a new approach is needed for the effective version. The proof is by contraposition. The main problem is to proceed from the nonexistence of $f'(z)$, which is based on the behaviour of slopes at arbitrarily small intervals I containing z, to the success of a betting strategy, which only has access to basic dyadic intervals (namely, intervals of the form $[i2^{-n}, (i+1)2^{-n})$ for $n \in \mathbb{N}, i < 2^n$). The solution is to bet with basic dyadic intervals that are scaled by a rational factor $p > 0$, and then shifted by a rational additive constant q. We show that the scaling and shifting parameters taken from a finite set are sufficient to approximate I from the outside and also from the inside by such intervals.

(b) The corresponding result of Demuth [4] involving Martin-Löf randomness and computable functions of bounded variation will be re-obtained as a corollary, using an effective form of Jordan's theorem. We note that Demuth's proof is somewhat obscure, which is partly due to the fact that it uses constructive language and notation. The attribution to Demuth relies on an interpretation, rather than a straightforward reading, of [4]. For background on Demuth's work see the survey [10]. Demuth's original proof is sketched in Thm. 7 of the upcoming extended survey [9].

(c) For weak 2-randomness, we take the largest class of computable functions that makes sense in this setting: the almost everywhere differentiable computable functions. The implication $\Rightarrow$ is obtained by observing that the points of nondifferentiablity for any computable function is a Σ^0_3 set (i.e., an effective $G_{\delta\sigma}$ set). If the function is a.e. differentiable, this set is null, and hence cannot contain a weakly 2-random real.

1.2. **Results of type $(*)$: the implication "$\Leftarrow$".** This is typically proved by contraposition. Given a test in the sense of the algorithmic randomness notion,

one builds a computable function f on the unit interval such that, for each real z failing the test, $f'(z)$ fails to exist. We will provide direct, uniform constructions of this kind for weak 2-randomness (c), and then for Martin-Löf randomness (b). The computable functions we build are sums of "sawtooth functions". For computable randomness (a), the simulation is less direct, though still uniform. The implication "$\Leftarrow$" is also rooted in results from classical analysis. For instance, Zahorski [19] proved that each null G_δ subset of $\mathbb{R}$ is the nondifferentiability set of a monotonic Lipschitz function. For a recent proof, see Fowler and Preiss [7].

1.3. **Classes of effective functions, and randomness notions.** The results of type $(*)$ mean that all the major algorithmic randomness notions for a real can now be matched with at least one class of effective functions on the unit interval in such a way that randomness of a real is equivalent to differentiability at the real. The analytical properties of functions we use are the well-known ones from classical real analysis.

The matching is onto, but not 1-1: in a sense, randomness notions are coarser than classes of effective functions. Computable randomness is characterized not only by differentiability of nondecreasing computable functions, but also of computable Lipschitz functions [8]. Furthermore, as an effectiveness condition on functions, one can choose anything between computability [15, Def. A, p. 25], and the weaker condition that $f(q)$ is a computable real (see Subsection 2.1), uniformly in a rational $q \in [0,1]$. Several notions lying in between have received attention. One of them is Markov computability, which is discussed in [2, Section 7]. Note that for nondecreasing continuous functions, the effectivity notions coincide by Proposition 2.2.

To characterize Schnorr randomness in terms of differentiability, we need a stronger notion of effectivity for functions. Call a function f *variation computable* if it is a computable point in the Banach space $AC_0[0,1]$ of absolutely continuous functions vanishing at 0, where the norm of a function is its variation on $[0,1]$. The computable structure (in the sense of [15, Ch. 2]) is given, for instance, by the polynomials with rational coefficients. Thus, $f \in AC_0[0,1]$ is variation computable iff for each n, one can determine a polynomial P_n with rational coefficients, vanishing at 0, such that the variation of $f - P_n$ is at most 2^{-n}. By the effective version of a classical theorem from analysis (see, for instance, [3, Ch. 20]), $AC_0[0,1]$ is effectively isometric with the space $(\mathcal{L}_1[0,1], ||.||_1)$, where the computable structure is also determined by the polynomials with rational coefficients. The isometry is given by differentiation, and its inverse by the indefinite integral.

Recent results of J. Rute [17], and, independently, Pathak, Rojas and Simpson [14], can be restated as follows: z is Schnorr random $\Leftrightarrow$ each absolutely continuous function that is computable in the variation norm is differentiable at z. Freer, Kjos-Hanssen, and Nies [8] showed the analogous result for Lipschitz functions.

The matching between algorithmic randomness notions and classes of effective functions is summarized in Figure 1.

1.4. **Structure of the paper.** Section 2 provides background from computable analysis. Section 3 introduces computable randomness and shows its base invariance. The central Section 4 characterizes computable randomness in terms of differentiability of computable functions. The short Section 5 discusses some consequences of this result. Section 6 characterizes weak 2-randomness and ML-randomness in terms of differentiability of computable functions.

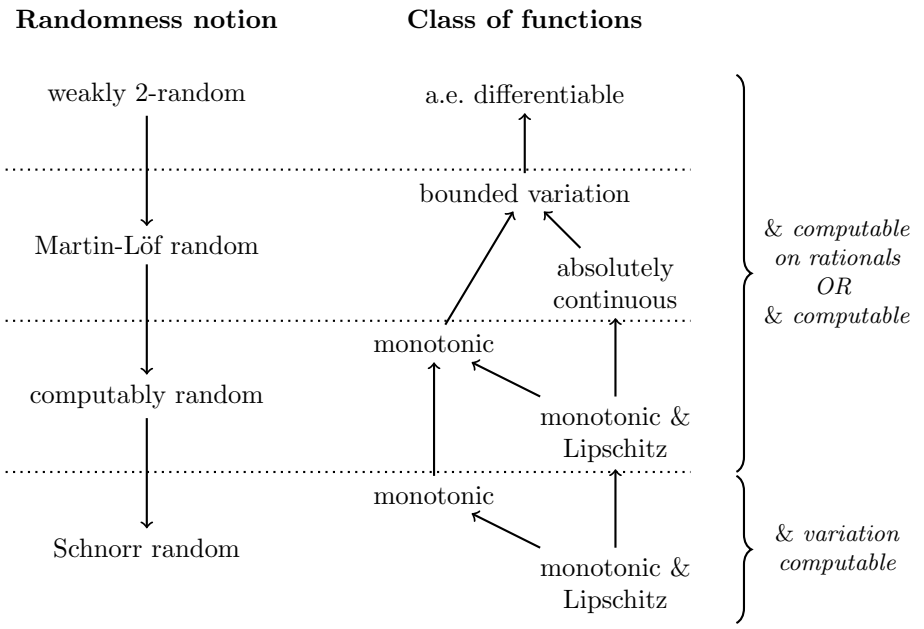

FIGURE 1. Randomness notions matched with classes of effective functions defined on $[0,1]$ so that $(*)$ holds

2. Preliminaries on computable analysis

2.1. **Computable functions defined on the unit interval.** A sequence $(q_n)_{n\in\mathbb{N}}$ of rationals is called a *Cauchy name* if $|q_n - q_k| \leq 2^{-n}$ for each $k \geq n$. If $\lim_n q_n = x$ we say that $(q_k)_{k\in\mathbb{N}}$ is a *Cauchy name* for x. Thus, q_n approximates x up to an error $|x - q_n|$ of at most 2^{-n}. A real x is called *computable* if it has a computable Cauchy name. A sequence $(x_n)_{n\in\mathbb{N}}$ of reals is *computable* if x_n is computable uniformly in n. That is, there is a computable double sequence $(q_{n,k})_{n,k\in\mathbb{N}}$ of rationals such that each x_n is a computable real as witnessed by its Cauchy name $(q_{n,k})_{k\in\mathbb{N}}$.

Definition 2.1 ([15], p. 26)**.** One says that $f\colon [0,1] \to \mathbb{R}$ is *computable* if

(a) for each computable sequence of reals $(x_k)_{k\in\mathbb{N}}$, the sequence $f(x_k)$ is computable, and
(b) f is *effectively uniformly continuous*: there is a computable $h\colon \mathbb{N} \to \mathbb{N}$ such that $|x - y| < 2^{-h(n)}$ implies $|f(x) - f(y)| < 2^{-n}$ for each n.

If f is effectively uniformly continuous, we can replace (a) by the following apparently weaker condition:

(a′) for *some* computable sequence of reals $(v_i)_{i\in\mathbb{N}}$ that is dense in $[0,1]$ the sequence $f(v_i)_{i\in\mathbb{N}}$ is computable.

Typically, the sequence $(v_i)_{i\in\mathbb{N}}$ in (a′) is an effective listing of the rationals in $[0,1]$ without repetition.

An *index* for a computable function on the unit interval f is a pair consisting of a computable index for the double sequence $(q_{n,k})_{n,k\in\mathbb{N}}$ of rationals determining the values of f at the rationals, together with a computable index for h.

We will frequently work with nondecreasing functions. Mere continuity and (a′) are sufficient for such a function to be computable. This easy fact will be very useful later on. For a proof see [2, Prop. 2.2].

Proposition 2.2. *Let g be a nondecreasing function. Suppose there is a computable dense sequence $(v_i)_{i\in\mathbb{N}}$ of reals in $[0,1]$ such that the sequence of reals $g(v_i)_{i\in\mathbb{N}}$ is computable. Suppose that g is also continuous. Then g is computable.*

2.2. **Arithmetical complexity of sets of reals.** By an *open interval* in $[0,1]$ we mean an interval of the form (a,b), $[0,b)$, $(a,1]$ or $[0,1]$, where $0\le a\le b\le 1$. A Σ^0_1 *set* in $[0,1]$ is a set of the form $\bigcup_k A_k$ where $(A_k)_{k\in\mathbb{N}}$ is a computable sequence of open intervals with dyadic rational endpoints. A Π^0_2 *set* has the form $\bigcap_m \mathcal{G}$ where the $\mathcal{G}_m$ are Σ^0_1 sets uniformly in m.

The following well-known fact will be needed later.

Lemma 2.3. *Let $f\colon [0,1]\to\mathbb{R}$ be computable. Then the sets $\{x\colon f(x)<p\}$ and $\{x\colon f(x)>p\}$ are Σ^0_1 sets, uniformly in a rational p.*

Actually there is uniformity at a higher level: effectively in an index for f, one can obtain an index for the function mapping p to an index for the Σ^0_1 set $\{x\colon f(x)<p\}$.

2.3. **Some notation and facts on differentiability.** Unless otherwise mentioned, functions will have a domain contained in the unit interval.

For a function f, the *slope* at a pair a,b of distinct reals in its domain is

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

Clearly, $S_f(a,b)=S_f(b,a)$. If A is a nontrivial interval with endpoints a,b, we also write $S_f(A)$ for $S_f(a,b)$.

Recall that if z is in the domain of f and the domain is dense around z, then

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

Note that we allow the values $\pm\infty$. By the definition, a function f is differentiable at z if $\underline{D}f(z)=\overline{D}f(z)$ and this value is finite.

For $a<x<b$ we have

$$S_f(a,b)=\frac{x-a}{b-a}S_f(a,x)+\frac{b-x}{b-a}S_f(x,b). \tag{1}$$

This implies the following:

Fact 2.4. Let $a<x<b$. Then

$$\min\{S_f(a,x),S_f(x,b)\}\le S_f(a,b)\le\max\{S_f(a,x),S_f(x,b)\}.$$

Consider a set $V \subseteq \mathbb{R}$ that is dense in $[0,1]$. If V is contained in the domain of a function f, we let

$$\begin{aligned} D^V f(x) &= \lim_{h\to 0+} \sup\{S_f(a,b)\colon \\ &\qquad a,b \in V \cap [0,1] \ \&\ a \le x \le b \ \&\ 0 < b-a \le h\}, \\ D_V f(x) &= \lim_{h\to 0+} \inf\{S_f(a,b)\colon \\ &\qquad a,b \in V \cap [0,1] \ \&\ a \le x \le b \ \&\ 0 < b-a \le h\}. \end{aligned}$$

If $f(z)$ is defined, then Fact 2.4 implies that

$$\underline{D} f(z) \le D_V f(z) \le D^V f(z) \le \overline{D} f(z). \tag{2}$$

The *middle third* of an interval $(a, a+d)$, where $0 < d$, is the closed interval $[a + d/3, a + d \cdot 2/3]$. The following lemma will be used in the proof of the main Theorem 4.3. It implies that if a function f is not differentiable at z, then this fact is witnessed on intervals that contain z in their middle third.

Lemma 2.5. *Suppose that $f\colon [0,1] \to \mathbb{R}$ is continuous at z. For any $h > 0$ let*

$$\mathcal{I}_h = \{(a,b)\colon 0 < b-a < h \ \&\ z \text{ is in the middle third of } (a,b)\}.$$

Suppose that

$$v := \lim_{h\to 0} \sup\{S_f(a,b)\colon (a,b) \in \mathcal{I}_h\} = \lim_{h\to 0} \inf\{S_f(a,b)\colon (a,b) \in \mathcal{I}_h\}.$$

Then $f'(z) = v$.

Proof. The continuity of f at z implies that $f'(z)$ equals the limit of $S_f(a,b)$ over all open intervals (a,b) that contain z, as $b - a \to 0$. Take h and $t < s$ such that $t < S_f(a,b) < s$ for all $(a,b) \in \mathcal{I}_h$. Consider an interval (c,d) containing z such that $d - c < h/3$. We will prove that

$$5t - 4s < S_f(c,d) < 5s - 4t.$$

Note that we can take t and s to approach v as $h \to 0$, in which case both $5t - 4s$ and $5s - 4t$ also approach v. This implies that $f'(z) = v$.

Assume, without loss of generality, that z is closer to c than to d. The idea is to define a sequence of intervals (a_n, b_n), (a_{n+1}, b_n) in $\mathcal{I}_h$ of increasing length. We start with $a_0 = c$ and $b_0 = a_0 + 3(z - c)$. The real z is the least in the middle third of (a_n, b_n), and the greatest in the middle third of (a_{n+1}, b_n). The intervals "see-saw" around z until we reach N such that $b_N < d \le b_{N+1}$. We first overestimate $f(d) - f(c)$ by $f(d) - f(a_{N+1})$, then subtract an over-correction $f(b_N) - f(a_{N+1})$, then add a second correction $f(b_N) - f(a_N)$, and so on, until we add $f(b_0) - f(a_0)$ and get the right value. The terms we add are bounded from above by the length of the corresponding interval times s. The terms we subtract are bounded from below by the length of the interval times t. This will show that $S_f(c,d) < 5s - 4t$.

For the details, let $\delta = z - c$. We let $a_n = z - 2^{2n}\delta$ and $b_n = z + 2^{2n+1}\delta$ for all $n \in \omega$. We may assume that $b_0 < d$, because otherwise z would be in the middle third of (c,d). Note that z is in the middle third of (a_{N+1}, d) because $b_{N+1} \ge d$. This interval is the longest we will consider. Note that

$$d - a_{N+1} = (d - z) + (z - a_{N+1}) < (d - c) + 2^{2N+2}\delta < 3(d - c) \le h,$$

because $2^{2N+1}\delta = b_N - z < d - c$. Therefore, all of the intervals that occur in the first four lines of the following estimates are in $\mathfrak{I}_h$. We have

$$\begin{aligned} f(d)-f(c) &= (f(d)-f(a_{N+1}))-(f(b_N)-f(a_{N+1}))+(f(b_N)-f(a_N)) \\ &\quad -\cdots+\cdots-(f(b_0)-f(a_1))+(f(b_0)-f(a_0)) \\ &\le s(d-a_{N+1})-t(b_N-a_{N+1})+s(b_N-a_N) \\ &\quad -\cdots+\cdots-t(b_0-a_1)+s(b_0-a_0) \qquad (3) \\ &= s(d-c)+s(a_0-a_{N+1})-t(2^{2N+3}-2)\delta+s(2^{2N+2}-1)\delta \\ &= s(d-c)+(s-t)(2^{2N+3}-2)\delta \\ &< s(d-c)+4(s-t)2^{2N+1}\delta \\ &< s(d-c)+4(s-t)(d-c). \end{aligned}$$

This proves that $S_f(c,d) < 5s-4t$. The lower bound $5t-4s < S_f(c,d)$ is obtained in an analogous way. □

2.4. **Binary expansions.** By a *binary expansion* of a real $x \in [0,1)$ we will always mean the one with infinitely many 0s. Co-infinite sets of natural numbers are often identified with reals in $[0,1)$ via the binary expansion. In this way, the product measure on Cantor space 2^ω is turned into the *uniform* (Lebesgue) measure on $[0,1]$.

3. Computable randomness

For background on computable randomness see [12, Ch. 7] or [5]. We provide the necessary definitions for later reference.

Definition 3.1. A *martingale* is a function $2^{<\omega} \to \mathbb{R}_0^+$ such that

$$M(\sigma 0) + M(\sigma 1) = 2M(\sigma) \qquad (4)$$

for each string σ. M *succeeds* on a sequence of bits Z if $M(Z\restriction_n)$ is unbounded. A martingale $M\colon 2^{<\omega} \to \mathbb{R}_0^+$ is called *computable* if $M(\sigma)$ is a computable real uniformly in a string σ.

Definition 3.2. An infinite sequence of bits Z is called *computably random* if no computable martingale succeeds on Z. A real $z \in [0,1)$ is called *computably random* if its binary expansion is computably random.

In fact, it suffices to require that no rational-valued martingale succeeds on the binary expansion of z ([18], also see [12, 7.3.8]).

3.1. **The savings property.**

Definition 3.3. We say that a martingale M has the *savings property* if $M(\rho) \ge M(\sigma) - 2$ for any strings σ, ρ such that $\rho \succeq \sigma$.

The following is well known (see [5] or [12, 7.1.14]).

Proposition 3.4. *For each computable martingale L there is a computable martingale M with the savings property that succeeds on the same sequences as L.*

In general, if M is a martingale, then $M(\sigma) \leq 2^{|\sigma|}M(\emptyset)$ for each string σ. If M has the savings property, then in fact

$$M(\sigma) \leq 2|\sigma| + M(\emptyset). \tag{5}$$

For otherwise, there is $\tau\widehat{\ }i \preceq \sigma$ for some $i \in \{0,1\}$ such that $M(\tau\widehat{\ }i) > M(\tau) + 2$, whence $M(\tau\widehat{\ }(1-i)) < M(\tau) - 2$.

3.2. **A correspondence between martingales and nondecreasing functions.** For a string $\sigma \in 2^{<\omega}$ we will write

$$[\sigma) = [0.\sigma, 0.\sigma + 2^{-|\sigma|});$$

we use the notation $[\sigma]$ either to denote the cone $\{X\colon X \succ \sigma\}$ in Cantor space, or the corresponding closed subinterval of $[0,1]$.

Each martingale M determines a measure on the algebra of clopen sets by assigning $[\sigma]$ the value $2^{-|\sigma|}M(\sigma)$. Via Carathéodory's extension theorem this measure can be extended to a Borel measure on Cantor space. We say that M is *atomless* if this measure is atomless, i.e., has no point masses. Note that, by (5) every martingale with the savings property is atomless. If the measure is atomless, via the binary expansion of reals (see Subsection 2.4) we can also view it as a Borel measure μ_M on $[0,1]$. Thus, μ_M is determined by the condition

$$\mu_M[\sigma) = 2^{-|\sigma|}M(\sigma). \tag{6}$$

We use the equality (6) above to establish a relationship between atomless martingales and nondecreasing continuous functions.

Atomless martingales to nondecreasing continuous functions on $[0,1]$. Given an atomless martingale M, let $\mathsf{cdf}(M)$ be the cumulative distribution function of the associated measure. That is,

$$\mathsf{cdf}(M)(x) = \mu_M[0,x).$$

Then $\mathsf{cdf}(M)$ is nondecreasing and continuous since the measure is atomless. Hence it is determined by its values on the rationals.

We let $I_{\mathbb{Q}} = [0,1] \cap \mathbb{Q}$.

Nondecreasing functions with domain containing $I_{\mathbb{Q}}$ *to martingales.* Suppose f is a nondecreasing function with a domain containing $I_{\mathbb{Q}}$. We will write

$$\mathsf{mart}(f)(\sigma) = S_f(\sigma) = (f(0.\sigma + 2^{-|\sigma|}) - f(0.\sigma))/2^{-|\sigma|}. \tag{7}$$

Let $M = \mathsf{mart}(f)$. We have, for instance, $M(10) = S_f(\frac{1}{2}, \frac{3}{4})$, and $M(11) = S_f(\frac{3}{4}, 1)$. That M is a martingale follows from the averaging condition on slopes in (1).

Fact 3.5. The transformations defined above induce a correspondence between atomless martingales and nondecreasing continuous functions on $[0,1]$ that vanish at 0. In particular:

(i) Let M be an atomless martingale. Then $\mathsf{mart}(\mathsf{cdf}(M)) = M$.
(ii) Let f be a nondecreasing continuous function on $[0,1]$ such that $f(0) = 0$. Then $\mathsf{cdf}(\mathsf{mart}(f)) = f$.

Proof. (i) is clear. For (ii), let $M = \mathsf{mart}(f)$. Let μ be the measure on $[0,1]$ such that $\mu[0,x) = f(x)$ for each x. Then $M(\sigma) = 2^{|\sigma|}\mu[\sigma)$ for each σ. Hence $\mu_M = \mu$ and $\mathsf{cdf}(M)(x) = \mu_M[0,x) = f(x)$ for each x. □

Recall the definition of $D_V(z)$ from Subsection 2.3.

Theorem 3.6. *Suppose M is a martingale with the savings property (see Section 3). Let $g = \mathsf{cdf}(M)$. Suppose $z \in [0,1]$ is not a dyadic rational. Then the following are equivalent:*

(i) *M succeeds on the binary expansion of z.*
(ii) *$\underline{D}g(z) = \infty$.*
(iii) *$D_{\mathbb{Q}}g(z) = \infty$.*

The proof will show that the implications (ii)→(iii)→(i) do not rely on the hypothesis that M has the savings property. However, we always need the weaker property that M is atomless to ensure that $\mathsf{cdf}(M)$ is defined.

Proof. Note that, since $z \in [0,1)$ is not a dyadic rational, its binary expansion Z is unique.

(ii) → (iii). This is immediate because, by (2) in Subsection 2.3, we have $\underline{D}g(z) \leq D_{\mathbb{Q}}g(z)$.

(iii)→(i). Given $c > 0$, choose n such that $S_g(p,q) \geq c$ whenever p, q are rationals, $p \leq z \leq q$, and $q - p \leq 2^{-n}$. Let $\sigma = Z\restriction_n$. Then we have $z \in [\sigma]$, and the length of this interval is 2^{-n}. Hence $M(\sigma) \geq c$.

(i) → (ii). We show that for each $r \in \mathbb{N}$ there is $\epsilon > 0$ such that $0 < |h| < \epsilon$ implies $(g(z+h) - g(z))/h \geq r$. This implies that $\underline{D}g(z) = \infty$.

Note that the binary expansion Z of z has infinitely many 0s and infinitely many 1s. Since M has the savings property, there is $i \in \mathbb{N}$ such that $Z(i) = 0$, $Z(i+1) = 1$, and for $\rho = Z\restriction_i$, we have $\forall \tau\, M(\rho\tau) \geq r$. Let $j > i$ be least such that $Z(j) = 0$. Let $\epsilon = 2^{-j-1}$. If $0 < |h| < \epsilon$, then the binary expansion of $z + h$ extends ρ. If $h > 0$, this is because $z + 2^{-j-1} < 0.\rho 1$. If $h < 0$, then adding h to z can at worst change the bit $Z(i+1)$ from 1 to 0.

For $V \subseteq 2^{<\omega}$ let $[V]^{\prec}$ denote the set of infinite sequences of bits extending a string in V. Let $W \subseteq 2^{<\omega}$ be a prefix free set of strings such that $[W]^{\prec}$ is identified with the open interval $(z, z+h)$ in case $h > 0$, and $[W]^{\prec}$ is identified with $(z+h, z)$ in case $h < 0$. All the strings in W extend ρ. So we have in case $h > 0$,

$$g(z+h) - g(z) = \mu_M(z, z+h) = \sum_{\sigma \in W} M(\sigma) 2^{-|\sigma|} \geq r \sum_{\sigma \in W} 2^{-|\sigma|} = rh,$$

and in case $h < 0$

$$g(z) - g(z+h) = \mu_M(z+h, z) = \sum_{\sigma \in W} M(\sigma) 2^{-|\sigma|} \geq r \sum_{\sigma \in W} 2^{-|\sigma|} = -rh.$$

In either case we have $(g(z+h) - g(z))/h \geq r$. □

3.3. **Computable randomness is base-invariant.** We give a first application of the analytical view of algorithmic randomness.

If the definition of a randomness notion for Cantor space is based on measure, it can be transferred right away to the reals in $[0,1]$ by the correspondence in Subsection 2.4.

Among the notions in the hierarchy mentioned in the introduction, computable randomness is the only one not directly defined in terms of measure. We argue that computable randomness of a real is independent of the choice of base for expansion. We will use that the condition (iii) in Theorem 3.6 is base-independent. First, we give the relevant definitions.

Let $k \geq 2$. A *martingale for base k* is a function

$$M\colon \{0,\dots,k-1\}^{<\omega} \to \mathbb{R}_0^+$$

with the fairness condition $\sum_{i=0}^{k-1}(M(\sigma i) - M(\sigma)) = 0$, or equivalently,

$$\sum_{i=0}^{k-1} M(\sigma i) = kM(\sigma).$$

The topics in Subsections 3.1 and 3.2 can be developed more generally for martingales M in base k. Such a martingale induces a measure μ_M on k^ω via $\mu_M([\sigma]) = M(\sigma)k^{-|\sigma|}$. As before, we call M atomless if μ_M is atomless as a measure. The remarks on the savings property after Definition 3.3 remain true; the condition (5) turns into $M(\sigma) \leq 2(k-1)|\sigma| + M(\emptyset)$. We have a transformation cdf turning an atomless martingale in base k into a nondecreasing continuous function on $[0,1]$ vanishing at 0, namely, the distribution function of μ_M. There is an inverse transformation mart^k turning such a function f into a martingale in base k via

$$\mathsf{mart}^k(f)(\sigma) = S_f(0.\sigma, 0.\sigma + k^{-|\sigma|}).$$

We call a sequence Z of numbers in $\{0,\dots,k-1\}$ *computably random in base k* if no computable martingale in base k succeeds on Z. Let us temporarily say that a real $z \in [0,1)$ is *computably random in base k* if its base k expansion (with infinitely many entries different from $k-1$) is computably random in base k.

Theorem 3.7. *Let $z \in [0,1)$. Let $k, r \geq 2$ be natural numbers. Then*

$$z \text{ is computably random in base } k \Rightarrow z \text{ is computably random in base } r.$$

Proof. We may assume z is irrational. Let Z be the base k expansion, and let Y be the base r expansion of z. Suppose Y is not computably random in base r. Then some computable martingale M in base r with the savings property succeeds on Y. By (5) for base r we have $M(\sigma) \leq 2(r-1)|\sigma| + O(1)$, whence M is atomless. Hence μ_M is defined and the associated distribution function $f = \mathsf{cdf}(M)$ is continuous. Clearly, $f(q)$ is uniformly computable for any rational $q \in [0,1]$ of the form ir^{-n}, $i \in \mathbb{N}$. Hence, by Proposition 2.2, f is computable. Therefore the martingale in base k corresponding to f, namely $N = \mathsf{mart}^k(f)$, is atomless and computable.

The proof of (i)→(ii) in Theorem 3.6 works for base r: replace 2 by r, and replace the digits 0,1 by digits $b < c < r$ that both occur infinitely often in the r-ary expansion of z (they exist because z is irrational). So, since M has the savings property, we have $\underline{D}f(z) = \infty$. Note that $f = \mathsf{cdf}(N)$ by Fact 3.5 in base k. Hence by (ii)→(i) of the same Theorem 3.6, but for base k, the computable martingale N succeeds on Z. □

4. Computable randomness and differentiability

In this section we characterize computable randomness in terms of differentiability. In the introduction, Subsection 1.1, we explained the need for working with scaled and shifted basic dyadic intervals. To elaborate on this, our main technical concept is the following. For $p, q \in \mathbb{Q}$, $p > 0$, we say that an interval is a (p,q)–*interval* if it is the image of a basic dyadic interval under the affine transformation $y \mapsto py + q$. Thus, a (p,q)–interval has the form

$$[pi2^{-n} + q, p(i+1)2^{-n} + q]$$

for some $i \in \mathbb{Z}, n \in \mathbb{N}$.

For a set L of rationals, an interval is called an *L–interval* if it is a (p,q)–interval for some $p,q \in L$. We begin with an algebraic lemma. Informally, given a "precision factor" of $\alpha > 1$, there is a finite set L such that we can approximate within precision α a given interval from the outside and from the inside by L–intervals.

Lemma 4.1. *For each rational $\alpha > 1$, we can effectively determine a finite set L of rationals in $[-1,1]$ such that for each interval $[x,y]$, $0 < x < y < 1$, there are L–intervals A, B as follows:*

$$\begin{aligned} [x,y] \subset A \quad \& \quad \frac{|A|}{y-x} < \alpha, \\ B \subset [x,y] \quad \& \quad \frac{y-x}{|B|} < \alpha. \end{aligned}$$

Proof. We may assume that $0 < x < y < 1/2$. Let k be an odd prime number such that $1 + 8/k < \alpha$. Let

$$\begin{aligned} P &= \{l/k\colon\ l \in \mathbb{N} \ \&\ k/2 < l \le k\}, \\ Q &= \{v/k\colon\ v \in \mathbb{Z} \ \&\ |v| \le k\}. \end{aligned}$$

We claim that $L = P \cup PQ$ is a finite set of rationals as required. Informally speaking, P is a set of scaling factors for intervals, and PQ is a set of possible shifts for intervals.

Finding A. To obtain $A \supset [x,y]$, let $n \in \mathbb{N}$ be largest such that $y - x < (1-1/k)2^{-n}$, and let $\eta = 1/(2^n k)$. Informally η is the "resolution" for a discrete version of the picture that will suffice to find A and B. By the definitions we have

$$y - x + \eta < 2^{-n}. \tag{8}$$

Pick the least scaling factor $p \in P$ such that

$$y - x + \eta < p2^{-n}. \tag{9}$$

Note that $p > \min P$: if $p! = \frac{k+1}{2k}$, then $y - x + \eta < p2^{-n}$ implies $y - x < (1-1/k)2^{-n-1}$ contrary to the maximality of n. Therefore we have

$$p2^{-n} \le y - x + 2\eta. \tag{10}$$

Let $M \in \mathbb{N}$ be greatest such that $M\eta < x/p$. Now comes the key step: since k and 2^n are coprime, in the abelian group $\mathbb{Q}/\mathbb{Z}$, the elements $1/k$ and $1/2^n$ together generate the same cyclic group as η. Working still in $\mathbb{Q}/\mathbb{Z}$, there are $i, v_0 \in \mathbb{N}$, $0 \le i < 2^n$, $v_0 \le k$ such that $[i/2^n] + [v_0/k] = [M\eta]$. Then, since $M\eta \le 1$, there is an integer v, $|v| \le k$, such that

$$i/2^n + v/k = M\eta. \tag{11}$$

To define the L–interval A, let $q = v/k \in Q$. Let

$$A = p[i2^{-n}, (i+1)2^{-n}] + pq.$$

Write $A = [a,b]$. We verify that A is as required.

First, $a = pi2^{-n} + pq = pM\eta < x$, and $x - a \le p\eta \le \eta$ because of the maximality of M and because $p \le 1$.

Second, $|A| = p2^{-n}$, so we have by (9) and (10) that $y < b < y + 2\eta$. Then

$$|A| \le y - x + 2\eta = y - x + 2/(2^n k) \le y - x + 8(y-x)/k,$$

where the last inequality holds because $2^{-n} \leq 4(y-x)$ by the maximality of n. Thus $|A|/(y-x) \leq 1 + 8/k < \alpha$, as required.

Finding B. Let $\alpha = 1 + 2\epsilon$. The second statement of the lemma can be derived from the first statement for the precision factor $1+\epsilon$. Let L be the finite set of rationals obtained in the first statement for $1+\epsilon$ in place of α. Given an interval $[x, y]$, let $[u, v] \subseteq [x, y]$ be the sub-interval such that

$$u - x = y - v = \epsilon(v - u).$$

By the first statement of the lemma there is an L–interval $B = [a, b] \supseteq [u, v]$ such that $|B|/(v-u) < 1 + \epsilon$. Then

$$\begin{aligned} u - a &< \epsilon(v-u) = u - x, \\ b - v &< \epsilon(v-u) = y - v, \end{aligned}$$

whence $B \subset [x, y]$. Clearly, $(y-x)/|B| < (y-x)/(v-u) = \alpha$. □

Remark 4.2. To illustrate the lemma and its proof, suppose $\alpha = 4$. We can choose k to be the prime 3. This yields a set L of at most 16 rationals. We have $P = \{\frac{2}{3}, 1\}$, but the proof shows that in order to find A we never choose $p = \min P$. Thus $p = 1$. The shift parameter q is of the form $v/3$, where v is an integer and $|v| \leq 3$. Thus, every interval $[x, y]$ is contained in a basic dyadic interval shifted by some q, and of length less than $4(y-x)$. For this special case, a similar fact can be shown with the usual "1/3-trick": the endpoints of a basic dyadic interval of length 2^{-m}, and another basic dyadic interval shifted by $1/3$ and of the same length, are at least $2^{-m}/3$ apart.

We are now ready for the main result.

Theorem 4.3. *Let $z \in [0, 1)$. Then the following are equivalent:*

(i) *z is computably random.*
(ii) *Each computable nondecreasing function $f\colon [0,1] \to \mathbb{R}$ is differentiable at z.*
(iii) *Each computable nondecreasing function $g\colon [0,1] \to \mathbb{R}$ satisfies $\overline{D}g(z) < \infty$.*
(iv) *Each computable nondecreasing function $g\colon [0,1] \to \mathbb{R}$ satisfies $\underline{D}g(z) < \infty$.*

Proof. The implications (ii)→(iii)→(iv) are trivial. For the implication (iv)→(i), suppose that z is not computably random.

If z is rational, we can let $g(x) = 1 - \sqrt{z - x}$ for $x \leq z$ and $g(x) = 1$ for $x > z$. Clearly, g is nondecreasing and $\underline{D}g(z) = \infty$. Since z is rational, g is uniformly computable on the rationals in $[0, 1]$. Hence g is computable by Proposition 2.2.

Now suppose that z is irrational. Let the bit sequence Z correspond to the binary expansion of z. By Proposition 3.4, there is a computable martingale M with the savings property such that $\lim_n M(Z\upharpoonright_n) = \infty$. Let $g = \mathsf{cdf}(M)$. Then $\underline{D}g(z) = \infty$ by Theorem 3.6. By the savings property of M, the associated distribution function $g = \mathsf{cdf}(M)$ is continuous. Clearly, $g(q)$ is uniformly computable on the dyadic rationals in $[0, 1]$. Then, once again by Proposition 2.2, we may conclude that g is computable.

It remains to prove the implication (i)→(ii). It turns out easier to actually prove (i)→(iii)→(ii).

For the rest of this proof, intervals will be closed with distinct rational endpoints unless otherwise mentioned. If $A = [a, b]$ we write $|A|$ for the length $b - a$. To say that intervals are *disjoint* means they are disjoint on $\mathbb{R} \setminus \mathbb{Q}$. Recall that a *basic dyadic interval* has the form $[i2^{-n}, (i+1)2^{-n}]$ for some $i \in \mathbb{Z}, n \in \mathbb{N}$.

4.1. **Proof of (i)→(iii).** Suppose $\overline{D}g(z) = \infty$ where $g\colon [0,1] \to \mathbb{R}$ is a computable nondecreasing function. We want to show that z is not computably random. We may assume that z is irrational. Applying Lemma 4.1 for some fixed $\alpha > 1$, we obtain a finite set $L \subseteq [-1,1]$ of rationals. There are p, q in L with $p > 0$ such that

$$\infty = \sup\{S_g(A)\colon A \text{ is a } (p,q)\text{–interval } \&\ z \in A\}. \tag{12}$$

For a binary string σ, recall that $[\sigma]$ is the closed basic dyadic interval determined by σ. Let

$$A_\sigma = p[\sigma] + q.$$

We may assume that the given computable nondecreasing function g is actually defined on $[-1,2]$, so that $S_g(A_\sigma)$ is defined for each σ. To do so we let $g(x) = g(0)$ for $x \in [-1,0]$ and $g(x) = g(1)$ for $x \in [1,2]$ and note that this extended function is computable by Proposition 2.2. We define a computable martingale N by

$$N(\sigma) = S_g(A_\sigma).$$

Now let w be the irrational number $(z-q)/p$. Then N succeeds on the binary expansion of the fractional part $w - \lfloor w \rfloor$. For, given $c > 0$, by (12) let σ be a string such that $z \in A_\sigma$ and $S_g(A_\sigma) \geq c$. Then σ is an initial segment of the binary expansion of $w - \lfloor w \rfloor$ and $N(\sigma) \geq c$.

It follows from the base invariance of computable randomness proved in Theorem 3.7 that $z = wp + q$ is also not computably random.

4.2. **Proof of (iii)→(ii).** Suppose a computable nondecreasing function f is not differentiable at z. We will eventually define a computable nondecreasing function g such that $\overline{D}g(z) = \infty$. We may assume f is increasing after replacing f by the function $x \mapsto f(x) + x$. If $\underline{D}f(z) = \infty$ we are done by letting $g = f$. Otherwise, we have

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

The nondecreasing computable function g is defined in conjunction with a betting strategy Γ. Instead of betting on strings, the strategy bets on nodes in a tree of rational intervals A. The root is $[0,1]$, and the tree is ordered by reverse inclusion. This strategy Γ proceeds from an interval A to subintervals A_k which are its successors on the tree. It maps these intervals to nonnegative reals representing the capital at that interval. If the tree consists of the basic dyadic subintervals of $[0,1]$, we have essentially the same type of betting strategy as before. However, it will be necessary to consider a more complicated tree where nodes have infinitely many successors.

We define the nondecreasing function g in such a way that the current capital at a node $A = [a,b]$ is the slope:

$$\Gamma(A) = S_g(a,b) = \frac{g(b) - g(a)}{b - a}. \tag{13}$$

Thus, initially we define g only on the endpoints of intervals in the tree, which will form a dense sequence of rationals in $[0,1]$ with an effective listing. Thereafter we will use Proposition 2.2 to extend g to all reals in the unit interval.

The Doob strategy. One idea in our proof is taken from the proof of the fact that $\lim_n M(Z\upharpoonright_n)$ exists for each computably random sequence Z and each computable martingale M: otherwise, there are rationals β, γ such that

$$\liminf_n M(Z\upharpoonright_n) < \beta < \gamma < \limsup_n M(Z\upharpoonright_n).$$

In this case one defines a new computable betting strategy G on strings that succeeds on Z. On each string, G is either in the betting state, or in the nonbetting state. Initially it is in the betting state. In the betting state G bets with the same factors as M (i.e., $G(\sigma a)/G(\sigma) = M(\sigma a)/M(\sigma)$ for the current string σ and each $a \in \{0,1\}$), until M's capital exceeds γ. From then on, G does not bet until M's capital is below β. On the initial segments of Z, the strategy G goes through infinitely many state changes; each time it returns to the nonbetting state, it has multiplied its capital by γ/β. Note that this is an effective version of the technique used to prove the first Doob martingale convergence theorem.

Recall that if $A = [x, y]$, for the slope of f we use the shorthand $S_f(A) = S_f(x, y)$. Given $z \in [0, 1] - \mathbb{Q}$, let A_n be the basic dyadic interval of length 2^{-n} containing z. Naively, one could hope that our case assumption $\underline{D}f(z) < \overline{D}f(z)$ becomes apparent on these basic dyadic intervals:

$$\liminf_n S_f(A_n) < \beta < \gamma < \limsup_n S_f(A_n)$$

for some rationals $\beta < \gamma$. In this case, we may carry out the Doob strategy for the martingale M given by $M(\sigma) = S_f(\sigma)$ as defined in (7), and view it as a betting strategy on nodes in the tree of basic dyadic intervals.

Unfortunately, this scenario is too simple. If we allow $z = 0$, then this already becomes apparent via the computable increasing function $f(x) = x \sin(2\pi \log_2 x) + 10x$, because $f(x) = 10x$ for each x of the form 2^{-n}, but $9 = \underline{D}f(0) < \overline{D}f(0) = 11$.

We will show in Lemma 4.4 that there are rationals p, q and r, s such that

$$\liminf_{\substack{|A|\to 0 \\ A \text{ is an } (r,s)-\text{interval} \\ z\in A}} S_f(A) \;<\; \limsup_{\substack{|B|\to 0 \\ B \text{ is a } (p,q)-\text{interval} \\ z\in B}} S_f(B). \tag{14}$$

The strategy Γ is in the betting state on (p, q) intervals in the tree of intervals, and in the nonbetting state on (r, s)–intervals. For each state, it proceeds exactly like the Doob strategy in the corresponding state. In addition, when Γ switches state, the current interval is split into intervals of the other type (usually, into infinitely many intervals). Nonetheless, the other state takes effect immediately. So, in the betting state, we have to immediately bet on all the components of this (usually) infinite splitting.

By the hypothesis that $f'(z)$ does not exist and Lemma 2.5, we can choose rationals $\widetilde{\beta} < \widetilde{\gamma}$ such that

$$\widetilde{\gamma} \;<\; \lim_{h\to 0} \sup\{S_f(x, y) \colon 0 \le y - x \le h \;\&\; z \in (x, y)\},$$
$$\widetilde{\beta} \;>\; \lim_{h\to 0} \inf\{S_f(x, y) \colon 0 \le y - x \le h \;\&\; z \in \text{ middle third of } (x, y)\}.$$

Let α, β, γ be rationals such that $1 < \alpha < \frac{4}{3}$ and

$$\widetilde{\beta}\alpha < \beta < \gamma < \widetilde{\gamma}/\alpha.$$

Lemma 4.4. *There are rationals p, q, r, s, such that $p, r > 0$ and*

$$\begin{aligned} \gamma &< \limsup_{h\to 0}\{S_f(A)\colon A \text{ is a } (p,q)\text{–interval } \&\ |A| \le h \ \&\ z \in A\},\\ \beta &> \liminf_{h\to 0}\{S_f(B)\colon B \text{ is an } (r,s)\text{–interval } \&\ |B| \le h \ \&\ z \in B\}. \end{aligned}$$

Proof. Let L be as in Lemma 4.1. For the first inequality, we use the first line in Lemma 4.1.

Let $h > 0$ be given. Choose reals $x < y$, where $x \le z \le y$, such that $y - x < h/\alpha$ and $S_f(x, y) > \widetilde{\gamma}$. By Lemma 4.1 there is an L–interval $A = [u, v]$ such that $[x, y] \subseteq A$ and $|A|/(y-x) < \alpha$. Then, since f is nondecreasing and $v - u < \alpha(y-x)$, we have

$$S_f(A) = \frac{f(v) - f(u)}{v - u} \ge \frac{f(y) - f(x)}{v - u} > \frac{f(y) - f(x)}{(y - x)\alpha} > \widetilde{\gamma}/\alpha > \gamma.$$

Since L is finite, we can now pick a single pair of rationals $p, q \in L$ which works for arbitrary small $h > 0$, as required.

For the second inequality, the argument is similar, based on the second line in Lemma 4.1. However, we also need the condition on middle thirds in the definition of $\widetilde{\beta}$, because when we replace an interval $[x, y]$ by a subinterval B that is an (r, s)-interval, we want to ensure that $z \in B$.

Given $h > 0$, choose reals $x < y$, where $x \le z \le y$ and z is in the middle third of $[x, y]$, such that $y - x < h/\alpha$ and $S_f(x, y) < \widetilde{\beta}$. By Lemma 4.1 there is an L–interval $B = [u, v]$ such that $B \subseteq [x, y]$ and $(y - x)/|B| < \alpha$. Since $\alpha < 4/3$ and z is in the middle third of $[x, y]$, we have $z \in B$. Similar to the estimates above, we have

$$S_f(B) \le \frac{f(y) - f(x)}{v - u} \le \frac{f(y) - f(x)}{(y - x)/\alpha} = \alpha S_f(x, y) < \alpha\widetilde{\beta} < \beta. \qquad \square$$

Definition of g on a dense set, and the strategy Γ. In the following fix p, q, r, s as in Lemma 4.4. Recall that we plan to define an infinitely branching tree of intervals, and that, on each node A in this tree, the strategy is either

- in a *betting state*, betting on smaller and smaller (p, q)–subintervals of A, or
- in a *nonbetting state*, processing smaller and smaller (r, s)–subintervals of A, but without betting.

The root of the tree is $A = [0, 1]$. Initially let $g(0) = 0$ and $g(1) = 1$ (hence $\Gamma(A) = 1$), and put the strategy Γ into the betting state.

One technical problem is that we never know a computable real such as $S_f(A)$ in its entirety; we only have rational approximations. For a real x named by a Cauchy sequence as in Subsection 2.1, we let x_n denote the n-th term of that sequence. Thus $|x - x_n| \le 2^{-n}$. To make use of the inequalities in Lemma 4.4, we choose $K \in \mathbb{N}$ large enough that the inequalities still hold with $\gamma + 2^{-K}$ instead of γ, and with $\beta - 2^{-K}$ instead of β, respectively. We also require that $\beta + 2^{-K} < \gamma - 2^{-K}$.

Suppose $A = [a, b]$ is an interval such that $\Gamma(A)$ has already been defined. By hypothesis $S_f(A)$ is a computable real uniformly in A. Proceed according to the case that applies.

(I): Γ *is in the betting state on A.*
(I.a) $S_f(A)_K \le \gamma$. If Γ has just entered the betting state on A, let

$$A = \bigsqcup_k A_k$$

where the A_k form an effective sequence of (p,q)–intervals that are disjoint (on $[0,1] \setminus \mathbb{Q}$). Otherwise, split $A = A_0 \cup A_1$ into disjoint intervals of equal length.

The function g interpolates between a and b with a growth proportional to the growth of f: if $v \in (a,b)$ is an endpoint of a new interval, define

$$g(v) = g(a) + (g(b) - g(a))\frac{f(v) - f(a)}{f(b) - f(a)}.$$

Continue the strategy on each subinterval.

(I.b) $S_f(A)_K > \gamma$. Switch to the nonbetting state on A and go to (II).

(II) Γ *is in the nonbetting state on* A.

(II.a) $S_f(A)_K \geq \beta$. If Γ has just entered the nonbetting state on A, let

$$A = \bigsqcup_k A_k$$

where the A_k form an effective sequence of (r,s)–intervals that are disjoint on $[0,1] \setminus \mathbb{Q}$, and further, $2|A_k| \leq |A|$ for each k. Otherwise split $A = A_0 \cup A_1$ into disjoint intervals of equal length.

If $v \in (a,b)$ is an endpoint of a new interval, then g interpolates linearly: let

$$g(v) = g(a) + (g(b) - g(a))\frac{v - a}{b - a}.$$

Continue the strategy on each subinterval.

(II.b) $S_f(A)_K < \beta$. Switch to the betting state on A and go to (I).

The verification. If the strategy Γ, processing an interval $A = [a,b]$ in the betting state, chooses a subinterval $[c,d]$, then

$$g(d) - g(c) = (g(b) - g(a))\frac{f(d) - f(c)}{f(b) - f(a)}.$$

Dividing this equation by $d - c$ and recalling the definition of the Γ-values in (13), we obtain

$$\Gamma([c,d]) = \Gamma([a,b])\frac{S_f(c,d)}{S_f(a,b)}. \tag{15}$$

The purpose of the following two claims is to extend g to a computable function on $[0,1]$. For the rest of the proof, we will use the shorthand

$$g[A] = g(b) - g(a)$$

for an interval on the tree $A = [a,b]$. Recall that we write $S_g(A)$ for the slope $S_g(a,b)$. Thus $\Gamma(A) = S_g(A) = g[A]/|A|$.

Claim 4.5. Let $x \in [0,1]$. Let $B_0 \supset B_1 \supset \cdots$ be an infinite path on the tree of intervals. Then $\lim_m g[B_m] = 0$.

We consider the states of the betting strategy Γ as it processes the intervals $A = B_m$.

Case 1: Γ *changes its state only finitely often when processing the intervals* B_m. If Γ is eventually in a nonbetting state, then clearly $\lim_m g[B_m] = 0$. Suppose otherwise, that is, Γ is eventually in a betting state. Suppose further that Γ enters

the betting state for the last time when it defines the interval $A = B_{m^*}$. Then for all $m \geq m^*$, by (15) and since $S_f(B_m)_K \leq \gamma$, we have

$$\Gamma(B_m) = \Gamma(B_{m^*})\frac{S_f(B_m)}{S_f(B_{m^*})} \leq (\gamma + 2^{-K})\frac{\Gamma(B_{m^*})}{S_f(B_{m^*})} =: C.$$

Hence $g[B_m] = \Gamma(B_m) \cdot |B_m| \leq C|B_m|$.

Case 2: Γ *changes its state infinitely often when processing the intervals* B_m. Let B_{m_i} be the interval A processed when the strategy is for the i-th time in a betting state at (I.b). Note that $g[B_{m_i+1}] \leq g[B_{m_i}]/2$ because at (II.a) we chose all the splitting components A_k at most half as long as the given interval A. Of course, by monotonicity of g we have $g[B_{m+1}] \leq g[B_m]$ for each m. Thus, $g[B_m] \leq 2^{-i}$ for each $m > m_i$. This completes the proof of the claim.

Claim 4.6. The function g can be extended to a computable function on $[0,1]$.

Let V be the set of endpoints of intervals on the tree. Clearly V is dense in $[0,1]$. For $x \in [0,1]$ let

$$\begin{aligned} \underline{g}(x) &= \sup\{g(v)\colon\ v < x, v \in V\}, \\ \overline{g}(x) &= \inf\{g(w)\colon\ w > x, w \in V\}. \end{aligned}$$

We show that $\underline{g}(x) \geq \overline{g}(x)$. Since g is nondecreasing on V, this will imply that $\underline{g} = \overline{g}$ is a continuous extension of g.

There is an infinite path $B_0 \supset B_1 \supset \cdots$ on the tree of intervals such that $x \in \bigcap_m B_m$. By Claim 4.5, we have

$$\underline{g}(x) \geq \sup_m g(\min B_m) = \inf_m g(\max B_m) \geq \overline{g}(x).$$

Clearly there is a computable dense sequence of rationals $\{v_i\}_{i\in\mathbb{N}}$ that lists without repetition the set V of endpoints of intervals in the tree. By definition, $g(v_i)$ is a computable real uniformly in i. Since $\underline{g}$ is continuous nondecreasing, by Proposition 2.2 we may conclude that $\underline{g}$ is computable. This establishes the claim.

From now on we will use the letter g to denote the function extended to $[0,1]$.

Claim 4.7. We have $\overline{D}g(z) = \infty$.

Let $\mathcal{C}$ denote the tree of intervals built during the construction. Note that for each $\epsilon > 0$ there are only finitely many intervals in $\mathcal{C}$ of length greater than ϵ. To prove the claim, we show that the strategy Γ succeeds on z in the sense that

$$\sup_{z\in A\in\mathcal{C}} \Gamma(A) = \infty.$$

By the definition of the Γ-values in (13) this will imply $\overline{D}g(z) = \infty$: let $([a_n, b_n])_{n\in\mathbb{N}}$ be a sequence of intervals containing z such that $\Gamma([a_n, b_n]) = S_g(a_n, b_n)$ is unbounded and $\lim_n(b_n - a_n) = 0$. If $z \in V$, then necessarily $a_n = z$ or $b_n = z$ for almost all n. This clearly implies $\overline{D}g(z) = \infty$. If $z \notin V$, then $a_n, b_n \neq z$ for all n, and we have $S_g(a_n, b_n) \leq \max\{S_g(a_n, z), S_g(z, b_n)\}$ by Fact 2.4. This also implies that $\overline{D}g(z) = \infty$.

Now we come to the crucial argument why Γ succeeds; first we verify that Γ changes its state infinitely often on intervals B such that $z \in B$. Suppose Γ entered the betting state in (II.b) and hence jumps to (I.a). Following the notation in (I.a), let A_k be the (p,q)–interval containing z. By the first line in Lemma 4.4 and the definition of K in Remark 4.2, there is a (p,q)–interval $A \subseteq A_k$ containing z such

that $S_f(A) > \gamma + 2^{-K}$. Thus $S_f(A)_K > \gamma$ and Γ enters the nonbetting state when it processes this interval, if not before.

Similarly, once Γ enters the nonbetting state on an interval A_k containing z, by the second line of Lemma 4.4 it will revert to the betting state on some (r, s)–interval $B \subseteq A_k$ containing z.

Now suppose Γ enters the betting state on A, B is a largest subinterval of A such that Γ enters the nonbetting state on B, and then again, C is a largest subinterval of B such that Γ enters the betting state on C. Then $S_f(A)_K < \beta$ while $S_f(B)_K > \gamma$, so $\Gamma(B) = \Gamma(A)S_f(B)/S_f(A) \geq \Gamma(A)\delta$ with $\delta = \frac{\gamma - 2^{-K}}{\beta + 2^{-K}} > 1$. Also $\Gamma(B) = \Gamma(C)$. Thus, after the strategy has entered the betting state for $n + 1$ times on intervals containing z, we have $\Gamma(A) \geq \delta^n$. This implies that Γ succeeds on z. □

Remark 4.8. Suppose we are given a computable function f as in Theorem 4.3 by an index in the sense of Subsection 2.1. The method of the foregoing proof enables us to uniformly obtain an index for a computable nondecreasing function p such that $f'(z) \uparrow$ implies $\overline{D}p(z) = \infty$ for all $z \in [0, 1]$. We simply sum up all the possibilities for g. This list of possibilities is effectively given: we have f itself (for the case that already $\underline{D}f(z) = \infty$), and all the functions g obtained for any possible values of the rationals p, q, r, s and $0 \leq \beta < \gamma$ in the construction above.

5. Consequences of Theorem 4.3

In this section we provide some interesting consequences of Theorem 4.3 and its proof. We say that a real $z \in \mathbb{R}$ satisfies an algorithmic randomness notion if its fractional part $z - \lfloor z \rfloor$ satisfies it.

Corollary 5.1. *Each computable nondecreasing function f is differentiable at a computable real. Moreover, the real can be obtained uniformly from an index for f.*

Proof. By Remark 4.8 above, from an index for f we can compute an index for a nondecreasing function g such that $f'(z) \uparrow$ implies $\overline{D}g(z) = \infty$ for all $z \in [0, 1]$. Our first goal is to show that one can compute an index for a function h such that $\underline{D}h(z) = \infty$ in case $f'(z) \uparrow$, for each $z \in [1/3, 2/3)$. The idea is to turn appropriate martingales into martingales with the savings property, and then apply the implication (i)→(ii) of Theorem 3.6.

We use the simple case of Lemma 4.1 with the parameters as in Remark 4.2. Let q range over rationals of the form $v/3$, where v is an integer and $|v| \leq 3$.

Let N_q be the computable martingale N obtained in the proof of (i)→ (iii) of Theorem 4.3 above for $p = 1$. By Proposition 3.4 from an index for N_q we can compute a martingale M_q with the savings property that succeeds on the binary expansion of a real $u \in [0, 1]$ if N does.

Let x range over $[1/3, 2/3]$. For $x < 2/3$ let $v_q(x)$ be the fractional part of $x - q$; let $v_q(2/3) = \lim_{x<2/3, x\to 2/3} v_q(x)$. Let $h_q(x) = \mathsf{cdf}(M_q)(v_q(x))$, and let $h(x) = \sum_q h_q(x)$. Clearly h is computable from an index for f.

Now consider $z \in [1/3, 2/3)$ such that $f'(z) \uparrow$. Then $\overline{D}g(z) = \infty$, so for some q, N_q succeeds on the binary expansion of $v_q(z)$ as observed in the proof of (i)→(iii) of Theorem 4.3. Hence M_q succeeds on the binary expansion of $v_q(z)$, which by the implication (i)→(ii) of Theorem 3.6 implies that $\underline{D}h_q(z) = \infty$. Therefore $\underline{D}h(z) = \infty$.

Let $r(x) = h(x) - h(1/3)$, extend this to a computable nondecreasing function on $[0,1]$ by assigning the value 0 to $y < 1/3$, and the value $h(2/3)$ to $y > 2/3$, and let V be the computable martingale $\mathsf{mart}(r)$. We have $\mathsf{cdf}(V) = r$ by Fact 3.5. By the implication (ii)→(i) of Theorem 3.6 (which does not rely on the savings property), we may conclude that V succeeds on the binary expansion of z. Note that an index for V, viewed as a function from binary strings to Cauchy names for reals, is computable from an index for g, and hence from an index for f.

It remains to compute, from an index for V, the binary expansion Z of a real $z \in [1/3, 2/3)$ such that $V(Z\restriction_n)$ is bounded. Let the first 3 bits of Z be $1, 0, 0$. For $n \geq 3$, if $\sigma = Z\restriction_n$ has been determined, use V to determine a bit $Z(n) = b$ such that $V(\sigma^\frown b) \leq V(\sigma^\frown(1-b)) + 2^{-n}$. Clearly, $\sup_n V(Z\restriction_n) < \infty$. □

Note that in the argument above, different indices for f might result in different reals. Next we obtain a preservation result for computable randomness. For instance, computable randomness is preserved under the map $z \mapsto e^z$, and, for each computable real $\alpha \neq 0$, under the map $z \mapsto z^\alpha$.

Corollary 5.2. *Suppose $z \in \mathbb{R}$ is computably random. Let H be a computable function that is* 1-1 *in a neighborhood of z. If $H'(z) \neq 0$, then $H(z)$ is computably random.*

Proof. Note that $H'(z)$ exists by Theorem 4.3. First suppose H is increasing in a neighborhood of z. If a function f is computable and nondecreasing in a neighborhood of $H(z)$, then the composition $f \circ H$ is nondecreasing in a neighborhood of z. Thus, since z is computably random, $(f \circ H)'(z)$ exists. Since $H'(z) \neq 0$, this implies that $f'(H(z))$ exists. Hence $H(z)$ is computably random.

If H is decreasing, we apply the foregoing argument to $-H$ instead. □

Corollary 5.3. *If a real $z \in [0,1]$ is computably random, then each computable Lipschitz function h on the unit interval is differentiable at z.*

Proof. Suppose h is Lipschitz via a constant $C \in \mathbb{N}$. Then the function f given by $f(x) = Cx - h(x)$ is computable and nondecreasing. Thus, by (i)→(ii) of Theorem 4.3, f and hence h is differentiable at z. □

The converse of Corollary 5.3 has been shown in [8]. Thus, monotonicity can be replaced by being Lipschitz in Theorem 4.3. Note that the function f in the foregoing proof is Lipschitz. Thus, computable randomness is characterized by differentiability of computable functions that are monotonic, or Lipschitz, or both monotonic and Lipschitz. This accounts for some arrows in Figure 1 in the introduction.

6. Weak 2-randomness and Martin-Löf randomness

In this section, when discussing inclusion, disjointness, etc., for open sets in the unit interval, we will ignore the elements that are dyadic rationals. For instance, we view the interval $(1/4, 3/4)$ as the union of $(1/4, 1/2)$ and $(1/2, 3/4)$. With this convention, the clopen sets in Cantor space 2^ω correspond to the finite unions of open intervals with dyadic rational endpoints.

6.1. **Characterizing weak 2-randomness in terms of differentiability.** Recall that a real z is *weakly 2-random* if z is in no null Π^0_2 set.

Theorem 6.1. *Let $z \in [0,1]$. Then*
z is weakly 2-random $\Leftrightarrow$
each a.e. differentiable computable function is differentiable at z.

Proof. "$\Rightarrow$": For rationals p, q let

$$\begin{aligned} \underline{C}(p) &= \{z\colon \forall t>0\, \exists h \left[0<|h|\le t \ \&\ S_f(z,z+h)<p\right]\}, \\ \overline{C}(q) &= \{z\colon \forall t>0\, \exists h \left[0<|h|\le t \ \&\ S_f(z,z+h)>q\right]\}, \end{aligned}$$

where t, h range over rationals. The function $z \mapsto S_f(z, z+h)$ is computable, and its index in the sense of Subsection 2.1 can be obtained uniformly in h. Hence the set

$$\{z\colon S_f(z,z+h)<p\}$$

is a Σ^0_1 set uniformly in p, h by Lemma 2.3 and its uniformity in the strong form remarked after its proof. Thus $\underline{C}(p)$ is a Π^0_2 set uniformly in p. Similarly, $\overline{C}(q)$ is a Π^0_2 set uniformly in q. Clearly,

$$\begin{aligned} \underline{D}f(z)<p &\ \Rightarrow\ z\in\underline{C}(p) \ \Rightarrow\ \underline{D}f(z)\le p, \\ \overline{D}f(z)>q &\ \Rightarrow\ z\in\overline{C}(q) \ \Rightarrow\ \overline{D}f(z)\ge q. \end{aligned}$$

Therefore $f'(z)$ fails to exist iff

$$\forall p\,[\,z\in\underline{C}(p)\,]\ \vee\ \forall q\,[\,z\in\overline{C}(q)\,]\ \vee\ \exists p\exists q[p<q\ \&\ z\in\underline{C}(p)\ \&\ z\in\overline{C}(q)],$$

where p, q range over rationals. This shows that $\{z\colon f'(z)$ fails to exist$\}$ is a Σ^0_3 set (i.e., an effective union of Π^0_2 sets). If f is a.e. differentiable, then this set is null and thus cannot contain a weakly 2-random.

"$\Leftarrow$": For an interval $A \subseteq [0,1]$ and $p \in \mathbb{N}$ let $\Lambda_{A,p}$ be the "sawtooth function" that is constant 0 outside A, reaches $p|A|/2$ at the middle point of A and is linearly interpolated elsewhere. Thus $\Lambda_{A,p}$ has slope $\pm p$ between pairs of points in the same half of A, and

$$\Lambda_{A,p}(x) \le p|A|/2, \tag{16}$$

for each x.

Let $(\mathcal{G}_m)_{m\in\mathbb{N}}$ be a sequence of uniformly Σ^0_1 sets in the sense of Subsection 2.2, where $\mathcal{G}_m \subseteq [0,1]$, such that $\mathcal{G}_m \supseteq \mathcal{G}_{m+1}$ for each m. We build a computable function f such that $f'(z)$ fails to exist for every $z \in \bigcap_m \mathcal{G}_m$. To establish the implication $\Leftarrow$, we also show in Claim 6.4 that the function f is a.e. differentiable in the case that $\bigcap_m \mathcal{G}_m$ is null.

Recall the convention that we ignore the dyadic rationals when discussing inclusion, union, disjointness, etc., for open sets in the unit interval. We have an effective enumeration $(D_{m,l})_{m,l\in\mathbb{N}}$ of open intervals with dyadic rational endpoints such that

$$\mathcal{G}_m = \bigsqcup_{l\in\mathbb{N}} D_{m,l},$$

for each m (the symbol $\bigsqcup$ indicates a disjoint union). We may assume, without loss of generality, that for each m, k, there is an l such that $D_{m+1,k} \subseteq D_{m,l}$.

We construct by recursion on m a computable double sequence $(C_{m,i})_{m,i\in\mathbb{N}}$ of open intervals with dyadic rational endpoints such that $\bigsqcup_i C_{m,i} = \mathcal{G}_m$,

$$C_{m,i} \cap C_{m,k} = \emptyset \quad \text{and} \quad |C_{m,i}| \geq |C_{m,k}| \quad \text{for} \quad i < k, \tag{17}$$

and, furthermore, if $B = C_{m,i}$ for $m > 0$, then there is an interval $A = C_{m-1,k}$ such that

$$B \subseteq A \ \& \ |B| \leq 8^{-m}|A|. \tag{18}$$

Each interval of the form $D_{m,k}$ will be a finite union of intervals of the form $C_{m,i}$.

Construction of the double sequence $(C_{m,i})_{m,i\in\mathbb{N}}$. Suppose $m = 0$, or $m > 0$ and we have already defined $(C_{m-1,j})_{j\in\mathbb{N}}$. Define $(C_{m,i})_{i\in\mathbb{N}}$ as follows.

Suppose $N \in \mathbb{N}$ is greatest such that we have already defined $C_{m,i}$ for $i < N$. When a new interval $D = D_{m,l}$ with dyadic rational endpoints is enumerated into $\mathcal{G}_m$, if $m > 0$ we wait until D is contained in a union of intervals $\bigcup_{r\in F} C_{m-1,r}$, where F is finite. This is possible because D is contained in a single interval in $\mathcal{G}_{m-1}$, and this single interval was handled in the previous stage of the recursion. If $m > 0$, let δ be the minimum of $|D|$ and the lengths of these finitely many intervals; if $m = 0$, let $\delta = |D|$. Let ϵ be the minimum of $|C_{m,N-1}|$ (if $N > 0$), and $8^{-m}2^{-l}\delta$. (We will need the factor 2^{-l} when we show in Claim 6.4 that f is a.e. differentiable.)

We partition D into disjoint subintervals $C_{m,i}$ with dyadic rational endpoints, $i = N, \ldots, N' - 1$, and of nonincreasing length at most ϵ, so that in case $m > 0$ each of the subintervals is contained in an interval A of the form $C_{m-1,r}$ for some $r \in F$. For $m \in \mathbb{N}$ let

$$f_m = \sum_{i=0}^{\infty} \Lambda_{C_{m,i},4^m},$$

and let $f = \sum_{m=0}^{\infty} f_m$. Since $|C_{m,i}| \leq 8^{-m}$ for each i, we have $f_m(x) \leq 8^{-m}4^m/2 \leq 2^{-m-1}$ for each x.

Claim 6.2. The function f is computable.

Since $f_m(x) \leq 2^{-m-1}$ for each m, $f(x)$ is defined for each $x \in [0, 1]$. We first show that $f(q)$ is computable uniformly in a rational q. Given $m > 0$, since $|C_{m,i}| \to_i 0$, we can find i^* such that

$$|C_{k,i^*}| \leq 8^{-m}/(m + 1) \text{ for each } k \leq m.$$

Then, since the length of the intervals $C_{k,i}$ is nonincreasing in i and by (16), we have $\Lambda_{C_{k,i},4^k}(q) \leq 2^{-m-1}/(m+1)$ for all $k \leq m$ and $i \geq i^*$. So by the disjointness in (17), $\sum_{k\leq m}\sum_{i\geq i^*} \Lambda_{C_{k,i},4^k}(q) \leq 2^{-m-1}$. We also have $\sum_{k>m} f_k(q) \leq \sum_{k>m} 2^{-k-1} = 2^{-m-1}$. Hence the approximation to $f(q)$ at stage i^* based only on the intervals of the form $C_{k,i}$ for $k \leq m$ and $i < i^*$ is within 2^{-m} of $f(q)$.

To show f is computable, by Subsection 2.1 it suffices now to verify that f is effectively uniformly continuous. Suppose $|x - y| \leq 8^{-m}$. For $k < m$, we have $|f_k(x) - f_k(y)| \leq 4^k|x - y|$. For $k \geq m$ we have $f_k(x), f_k(y) \leq 2^{-k-1}$. Thus

$$|f(x) - f(y)| \leq |x - y| \sum_{k<m} 4^k + \sum_{k\geq m} 2^{-k} < 2^{-m+2}.$$

Claim 6.3. Suppose $z \in \bigcap \mathcal{G}_m$. Then $\overline{D}f(z) = \infty$ or $\underline{D}f(z) = -\infty$.

For each m there is an interval A_m of the form $C_{m,i}$ such that $z \in A_m$. Suppose first that there are infinitely many m such that z is in the left half of A_m. We show $\overline{D}f(z) = \infty$. Let m be one such value. Choose

$$h = \pm|A_m|/4$$

so that $z + h$ is also in the left half of A_m. We show that the slope

$$S_{f_m}(z, z + h) = 4^m$$

does not cancel out with the slopes, possibly negative, that are due to other f_k. If $k < m$, then we have $|S_{f_k}(z, z + h)| \leq 4^k$. Suppose $k > m$. Then by (16) and (18) we have $f_k(x) \leq 4^k 8^{-k}|A_m|/2 = 2^{-k-1}|A_m|$ for $x \in \{z, z + h\}$ and hence

$$|S_{f_k}(z, z + h)| \leq \frac{2^{-k}|A_m|}{|h|} = 2^{-k+2}.$$

Therefore, for $m > 0$

$$S_f(z, z + h) \geq 4^m - \sum_{k<m} 4^k - \sum_{k>m} 2^{-k+2} \geq 4^{m-1} - 4.$$

Thus $\overline{D}f(z) = \infty$.

If there are infinitely many m such that z is in the right half of A_m, then $\underline{D}f(z) = -\infty$ by a similar argument.

Claim 6.4. If $\bigcap_m \mathcal{G}_m$ is null, then f is differentiable almost everywhere.

Let $\widehat{D}_{m,l}$ be the open interval in $\mathbb{R}$ with the same middle point as $D_{m,l}$ such that $|\widehat{D}_{m,l}| = 3|D_{m,l}|$. Let $\widehat{\mathcal{G}}_m = [0, 1] \cap \bigcup_l \widehat{D}_{m,l}$. Clearly $\lambda\widehat{\mathcal{G}}_m \leq 3\lambda\mathcal{G}_m$, so that $\bigcap_m \widehat{\mathcal{G}}_m$ is null.

We show that $f'(z)$ exists for each $z \notin \bigcap_m \widehat{\mathcal{G}}_m$ that is not a dyadic rational. In the following, let h, h_0, etc., range over rationals. Note that

$$S_f(z, z + h) = \textstyle\sum_{k=0}^{\infty} S_{f_k}(z, z + h).$$

Let m be the least number such that $z \notin \widehat{\mathcal{G}}_m$. Since z is not a dyadic rational, we may choose $h_0 > 0$ such that for each $k < m$, the function f_k is linear in the interval $[z - h_0, z + h_0]$. So for $|h| \leq h_0$ the contribution of these f_k to the slope $S_f(z, z + h)$ is constant. It now suffices to show that

$$\lim_{h\to 0} \textstyle\sum_{r=m}^{\infty} |S_{f_r}(z, z + h)| = 0.$$

Note that f_r is nonnegative and $f_r(z) = 0$ for $r \geq m$. Thus it suffices, given $\epsilon > 0$, to find a positive $h_1 \leq h_0$ such that

$$\sum_{r=m}^{\infty} f_r(z + h) \leq \epsilon|h| \tag{19}$$

whenever $|h| \leq h_1$.

Roughly, the idea is the following: take $r \geq m$. If $f_r(z + h) \neq 0$, then $z + h$ is in some $D_{m,l}$. Because $z \notin \widehat{D}_{m,l}$, $|h| \geq |D_{m,l}|$. We make sure that $f_r(z + h)$ is small compared to $|h|$ by using that the height of the relevant sawtooth depends on the length of its base interval $C_{r,v}$ containing $z + h$, and that this length is small compared to h.

We now provide the details on how to find h_1 as above. Choose $l^* \in \mathbb{N}$ such that $2^{-l^*} \leq \epsilon$. If $C_{m,i} \subseteq D_{m,l}$ and $l \geq l^*$, we have

$$|C_{m,i}| \leq 8^{-m}\epsilon|D_{m,l}|. \tag{20}$$

Let $h_1 = \min\{|D_{m,l}|\colon\ l < l^*\}$. Suppose $h > 0$ and $|h| \leq h_1$.

First we consider the contribution of f_m to (19). If $f_m(z+h) > 0$, then $z + h \in C_{m,i} \subseteq D_{m,l}$ for some (unique) l, i. Since $z \notin \widehat{D}_{m,l}$ and $|h| \leq h_1$, we have $|h| \geq |D_{m,l}|$ and $l \geq l^*$. By (16), (20) and the definition of f_m,

$$f_m(z+h) \leq 4^m|C_{m,i}|/2 \leq 2^{-m-1}|D_{m,l}|\epsilon.$$

Thus $f_m(z+h) \leq 2^{-m-1}\epsilon|h|$.

Next, we consider the contribution of f_r, $r > m$, to (19). If $f_r(z+h) > 0$, then $z + h \in C_{r,v} \subseteq C_{m,i}$ for some v. Thus, by construction,

$$f_r(z+h) \leq 4^r|C_{r,v}|/2 \leq 4^r 8^{-r}|C_{m,i}|/2 \leq 2^{-r-1}|D_{m,l}|\epsilon \leq 2^{-r-1}\epsilon|h|.$$

This establishes (19) and completes the proof. □

6.2. **Characterizing Martin-Löf randomness in terms of 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 $t_1 < t_2 < \ldots < t_n$ in $[0,1]$. A stronger condition on f is absolute continuity: for every $\epsilon > 0$, there is $\delta > 0$ such that

$$\epsilon > \sup \sum_{i=1}^{n} |f(b_i) - f(a_i)|,$$

for every collection $0 \leq a_1 < b_1 \leq a_2 < b_2 \leq \ldots \leq a_n < b_n \leq 1$ such that $\delta > \sum_{i=1}^{n} b_i - a_i$. The absolutely continuous functions are precisely the indefinite integrals of functions in $\mathcal{L}_1([0,1])$ (see [1, Thm. 5.3.6]). Note that it is easy to construct a computable differentiable function that is not of bounded variation.

We will characterize Martin-Löf randomness via differentiability of computable functions of bounded variation, following the scheme $(*)$ in the introduction. For the implication $\Leftarrow$, an appropriate single function suffices, because there is a universal Martin-Löf test.

Lemma 6.5 ([4], Example 2)**.** *There is a computable function f of bounded variation (in fact, absolutely continuous) such that $f'(z)$ exists only for Martin-Löf random reals z.*

Proof. Let $(\mathcal{G}_m)_{m\in\mathbb{N}}$ be a universal Martin-Löf test, where $\mathcal{G}_m \subseteq [0,1]$, such that $\mathcal{G}_m \supseteq \mathcal{G}_{m+1}$ for each m. We may assume that $\lambda\mathcal{G}_m \leq 8^{-m}$. Define a computable function f as in the proof of the implication $\Leftarrow$ of Theorem 6.1. By Claim 6.3, $f'(z)$ fails to exist for any $z \in \bigcap_m \mathcal{G}_m$, i.e., for any z that is not Martin-Löf random. It remains to show the following.

Claim 6.6. f is absolutely continuous, and hence of bounded variation.

For an open interval $A \subseteq [0,1]$, let $\Theta_{A,p}$ be the function that is undefined at the endpoints and the middle point of A, has value p on the left half, value $-p$ on the right half of A, and is 0 outside A. Then $\int_0^x \Theta_{A,p} = \Lambda_{A,p}(x)$.

Let $g_m = \sum_i \Theta_{C_{m,i},4^m}$. Note that $\lambda \mathcal{G}_m \leq 8^{-m}$ implies that g_m is integrable with $\int |g_m| \leq 2^{-m}$, and hence $\sum_m \int |g_m| \leq 2$. Then, by a well-known corollary to the Lebesgue dominated convergence theorem (see for instance [16, Thm. 1.38]), the function $g(y) = \sum_m g_m(y)$ is defined a.e., g is integrable, and $\int_0^x g = \sum_m \int_0^x g_m$. Since $f_m(x) = \int_0^x g_m$, this implies that $f(x) = \int_0^x g$. Thus, f is absolutely continuous. □

We now arrive at the analytic characterization of Martin-Löf randomness originally due to Demuth [4]. The implication (i)→(ii) below restates [4, Thm. 3] in classical language.

Theorem 6.7. *The following are equivalent for $z \in [0,1]$:*

(i) *z is Martin-Löf random.*
(ii) *Every computable function f of bounded variation is differentiable at z.*
(iii) *Every computable function f that is absolutely continuous is differentiable at z.*

Proof. The implication (iii)→(i) follows from Lemma 6.5. The implication (ii)→(iii) follows because each absolutely continuous function has bounded variation. For (i)→(ii), recall that a Jordan decomposition of f is a pair g_0, g_1 of nondecreasing functions such that $f = g_0 - g_1$. Every function of bounded variation admits a Jordan decomposition. However, this is noneffective: by the proof of [13, Prop. 7.1], there is a computable function f of bounded variation such that each continuous Jordan decomposition computes $\emptyset'$. We can lower the complexity of Jordan decomposition by considering g_0, g_1 as functions on the rationals (nondecreasing, but possibly discontinuous) and only requiring that $f = g_0 - g_1$ for rational arguments. This allows us to form a Π^0_1 class $\mathcal{P}$ of Jordan decompositions.

By the "low for z basis theorem" [6, Prop. 7.4], z is Martin-Löf random, and hence computably random, relative to some member (g_0, g_1) of $\mathcal{P}$. Theorem 4.3 can be extended to nondecreasing functions computable on the rationals, so g_0 and g_1 must both be (pseudo-)differentiable at z, hence $f = g_0 - g_1$ is differentiable at z. The details are given in [2, Section 7]. □

We obtain a preservation result for Martin-Löf randomness similar to Corollary 5.2. For a proof see [2].

Corollary 6.8. *Suppose $z \in \mathbb{R}$ is Martin-Löf random. Let H be a computable function that is Lipschitz and 1-1 in a neighborhood of z. If $H'(z) \neq 0$, then $H(z)$ is Martin-Löf random.*

Acknowledgments

We would like to thank Santiago Figueira, Jason Rute and Stijn Vermeeren for the careful reading of the paper, and Antonín Kučera for making Demuth's work accessible to us.

References

[1] V. I. Bogachev, *Measure theory. Vol. I, II*, Springer-Verlag, Berlin, 2007. MR2267655 (2008g:28002)

[2] V. Brattka, J. Miller, and A. Nies, *Randomness and differentiability* (long version on arxiv). `http://arxiv.org/abs/1104.4465`.

[3] N. L. Carothers, *Real analysis*, Cambridge University Press, Cambridge, 2000. MR1772332

[4] O. Demuth, *The differentiability of constructive functions of weakly bounded variation on pseudo numbers* (Russian), Comment. Math. Univ. Carolinae **16** (1975), no. 3, 583–599. MR0476442 (57 #16005)

[5] R. G. Downey and D. R. Hirschfeldt, *Algorithmic randomness and complexity*, Theory and Applications of Computability, Springer, New York, 2010. MR2732288 (2012g:03001)

[6] R. Downey, D. R. Hirschfeldt, J. S. Miller, and A. Nies, *Relativizing Chaitin's halting probability*, J. Math. Log. **5** (2005), no. 2, 167–192, DOI 10.1142/S0219061305000468. MR2188515 (2007e:68031)

[7] T. Fowler and D. Preiss, *A simple proof of Zahorski's description of non-differentiability sets of Lipschitz functions*, Real Anal. Exchange **34** (2009), no. 1, 127–138. MR2527127 (2010e:26003)

[8] C. Freer, B. Kjos-Hanssen, A. Nies, and F. Stephan, *Effective aspects of Lipschitz functions*, Computability **3** (2014), 45–61, DOI 10.3233/COM-14025.

[9] A. Kučera, A. Nies, and C. Porter, *Demuth's path to randomness*. To appear in Bull. Symb. Logic, 2014.

[10] A. Kučera and A. Nies, *Demuth's path to randomness*, Computation, physics and beyond, Lecture Notes in Comput. Sci., vol. 7160, Springer, Heidelberg, 2012, pp. 159–173, DOI 10.1007/978-3-642-27654-5_12. MR2965521

[11] H. Lebesgue, *Sur les intégrales singulières* (French), Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys. (3) **1** (1909), 25–117. MR1508308

[12] A. Nies, *Computability and randomness*, Oxford Logic Guides, vol. 51, Oxford University Press, Oxford, 2009. MR2548883 (2011i:03003)

[13] A. Nies (editor), Logic Blog 2013. Available at `http://arxiv.org/abs/1403.5719`, 2013.

[14] N. Pathak, C. Rojas, and S. G. Simpson, *Schnorr randomness and the Lebesgue differentiation theorem*, Proc. Amer. Math. Soc. **142** (2014), no. 1, 335–349. MR3119207

[15] M. B. Pour-El and J. I. Richards, *Computability in analysis and physics*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1989. MR1005942 (90k:03062)

[16] W. Rudin, *Real and complex analysis*, 3rd ed., McGraw-Hill Book Co., New York, 1987. MR924157 (88k:00002)

[17] J. Rute, *Algorithmic randomness, martingales, and differentiability I*. In preparation, 2012.

[18] C.-P. Schnorr, *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*, Lecture Notes in Mathematics, Vol. 218, Springer-Verlag, Berlin-New York, 1971. MR0414225 (54 #2328)

[19] Z. Zahorski, *Sur l'ensemble des points de non-dérivabilité d'une fonction continue* (French), Bull. Soc. Math. France **74** (1946), 147–178. MR0022592 (9,231a)

Faculty of Computer Science, Universität der Bundeswehr München, 85577 Neubiberg, Germany – and – Department of Mathematics and Applied Mathematics, University of Cape Town, Rondebosch 7701, South Africa

E-mail address: `Vasco.Brattka@cca-net.de`

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706-1388

E-mail address: `jmiller@math.wisc.edu`

Department of Computer Science, University of Auckland, Private bag 92019, Auckland, New Zealand

E-mail address: `andre@cs.auckland.ac.nz`