ALGORITHMIC ASPECTS OF LIPSCHITZ FUNCTIONS

CAMERON FREER, BJØRN KJOS-HANSSEN, ANDRÉ NIES AND FRANK STEPHAN

ABSTRACT. We characterize the variation functions of computable Lipschitz functions. We show that a real z is computably random if and only if every computable Lipschitz function is differentiable at z. Beyond these principal results, we show that a real z is Schnorr random if and only if every Lipschitz function with L_1-computable derivative is differentiable at z.

1. INTRODUCTION

Lipschitz functions are of fundamental importance in analysis. They appear naturally in various contexts, such as the solvability of differential equations. For a set $A \subseteq \mathbb{R}^n$, recall that a function $f\colon A \to \mathbb{R}^m$ is *Lipschitz* if there is a constant c, called a Lipschitz bound, such that for all x and y we have $\|f(x) - f(y)\| \leq c\,\|x - y\|$ (say, $\|\cdot\|$ denotes the Euclidean norm). There are many theorems stating that Lipschitz functions are in one sense or another well-behaved. For instance, the McShane–Whitney extension theorem says that a Lipschitz function $f\colon A \to \mathbb{R}^m$ can be extended to a Lipschitz function, with the same least Lipschitz bound, that is defined on all of $\mathbb{R}^n$. Rademacher's theorem states that f is differentiable at almost every point in A. In dimensions $n = m = 1$ this is immediate from the well-known theorem of Lebesgue that every real function of bounded variation is differentiable almost everywhere. In higher dimensions one uses arguments particular to Lipschitz functions. See [8] and the references given there for more background on Lipschitz functions.

Computable analysis seeks algorithmic analogues of theorems from analysis when effectiveness conditions are imposed on the functions. Several important theorems from analysis state almost everywhere well-behavior of functions in certain classes. In recent years, such theorems have been studied intensely from the point of view of algorithmic randomness [15, 2, 17, 20]; this provides a way of understanding the complexity of exception null sets, and to characterize algorithmic randomness notions via computable analysis. Much earlier, the constructivist Demuth already observed this connection in papers such as [5]. Our purpose is to carry out some of this program in the setting of Lipschitz analysis.

We briefly discuss some basic concepts in computable analysis. 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 $(q_n)_{n\in\mathbb{N}}$ 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.

In Subsection 2.1 we will in detail discuss computability of functions defined on the unit interval. For now, it suffices to know that a Lipschitz function f is computable if and only if $f(q)$ is a computable real uniformly in a rational $q \in [0, 1]$. This is not the original definition of computability for functions defined on $[0, 1]$; see the discussion after Definition 2.1. The same condition defines computability of a continuous monotonic function.

A real x is called *left-r.e.* (short for left-recursively enumerable) if the set of rationals less than x is recursively enumerable. Equivalently, there is an increasing computable sequence of rationals $(q_n)_{n\in\mathbb{N}}$ such that $x = \sup_n q_n$.

Key words and phrases. Lipschitz functions, Computability.

In the following subsections we will give an overview of our main results. Possible extensions and open questions will be discussed in the concluding section.

1.1. **The variation of a computable Lipschitz function.** Let $g\colon [0,1] \to \mathbb{R}$. For $0 \leq x < y \leq 1$ recall the *variation* of g in $[x,y]$:

$$V(g,[x,y]) = \sup\left\{\sum_{i=1}^{n-1} \left|g(t_{i+1}) - g(t_i)\right| : x \leq t_1 \leq t_2 \leq \ldots \leq t_n \leq y\right\}.$$

We have $V(g,[x,y]) + V(g,[y,z]) = V(g,[x,z])$ for $x < y < z$ (see [3, Prop. 5.2.2]). Note that if g is (uniformly) continuous, then we may restrict the sequences $t_1 \leq t_2 \leq \ldots \leq t_n$ above to a dense subset of $[0,1]$, such as the dyadic rationals. We write V_g for the function $x \mapsto V(g,[0,x])$. Each Lipschitz function is of bounded variation. In fact, it is easy to see that g is Lipschitz iff V_g is, and they have the same least Lipschitz constant.

We will provide a characterization of the class of variation functions V_g for computable Lipschitz functions g. If v is any non-decreasing function with $v(0) = 0$ then $v = V_v$, so classically, the functions V_g for Lipschitz functions g are simply the nondecreasing Lipschitz functions starting at the origin. In an effective setting, this simple correlation breaks down, because the variation function of a computable Lipschitz function is not necessarily computable. In fact, even the total variation $V_g(1)$ of a computable Lipschitz functions g defined on $[0,1]$ need not be computable as a real. Note that $V_g(1)$ is always left-r.e. Conversely, we will show in Fact 3.1 that every left-r.e. real in $[0,1]$ is of the form $V_g(1)$ for some computable function g with Lipschitz constant 1.

If g is a computable Lipschitz function and $f = V_g$, then f is non-decreasing Lipschitz, we have $f(0) = 0$, and $f(y) - f(x)$ is left-r.e. uniformly in rationals $x < y$. We call nondecreasing functions f satisfying the last two conditions *interval-r.e.* Our first main result, Theorem 3.4, shows that this weak effectiveness condition on f is sufficient: *every Lipschitz interval-r.e. function f is of the form V_g for some computable Lipschitz function g.*

Our proof relies on the following notion. A *signed martingale* is a function $2^{<\omega} \to \mathbb{R}$ such that the fairness condition $M(\sigma 0) + M(\sigma 1) = 2M(\sigma)$ holds for each string σ. We proceed via the fact, of interest in itself, that every left-r.e. positive martingale with a non-atomic associated measure on Cantor space (see Subsection 2.3) is the variation martingale of a signed computable martingale. The definition of the variation martingale corresponds to the variation measure $|\mu|$ of a signed measure μ. Recall that $|\mu|(E)$ is the supremum over all $\sum_i |\mu(E_i)|$ where $(E_i)_{i\in\mathbb{N}}$ ranges over partitions of E into measurable sets. See, for instance, [19, Section 6.1].

After seeing our Theorem 3.4, Jason Rute has provided an extension of our construction to all continuous interval-r.e. functions f, by showing that $f = V_g$ for some computable g. We include this as a theorem joint with Rute at the end of Section 3.

One can also ask whether a similar result holds in the context of effective measure theory developed by Gács, Hoyrup, Rojas and others (see [9]). For instance, is every lower semicomputable measure on $[0,1]^n$ without point masses the variation, in the sense of [19, Section 6.1], of a computable signed measure? Rute has pointed out that our Theorem 3.4 implies an affirmative answer in the case $n = 1$, and that the hypothesis to have no point masses is necessary.

1.2. **Lipschitz functions and computable randomness.** The following is due to Brattka, Miller, and Nies [2, Thm. 4.1]:

Theorem 1.1. *Let $z \in [0,1]$. Then z is computably random $\Leftrightarrow$*

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

Our second main result, Theorem 4.2, provides an analogous fact for computable Lipschitz functions.

1.3. **Lebesgue points and Schnorr randomness.** Let $L_1([0,1]^n)$ denote the set of integrable functions $g\colon [0,1]^n \to \mathbb{R}$. Recall that a vector $z \in [0,1]^n$ is called a *Lebesgue point* of such a function g if

$$\lim_{z\in Q \ \wedge \ \lambda Q \to 0} (\lambda Q)^{-1} \int_Q |g - g(z)| = 0,$$

where Q ranges over n-cubes. We say that z is a *weak Lebesgue point* of g if the limit

$$\lim_{z\in Q \ \wedge \ \lambda Q \to 0} (\lambda Q)^{-1} \int_Q g$$

exists. The Lebesgue differentiation theorem states the following.

Theorem 1.2. *Let $g \in L_1([0,1]^n)$. Then almost every point in $[0,1]^n$ is a Lebesgue point of g.*

For a proof see for instance Rudin [19, Thm. 7.7]. One can replace the cubes in the definition of Lebesgue points by other geometric objects, such as balls centered at z. Rudin [19, Thm. 7.10] has given a general definition of a sequence of Borel sets $(E_k)_{k\in\mathbb{N}}$ "shrinking nicely" to z that makes the theorem hold; this encompasses both cubes and balls.

We will formulate the results related to Schnorr randomness (see Subsection 5.1 for a definition) first in terms of weak Lebesgue points. In dimension 1 they will later on be translated to results on differentiability of Lipschitz functions that are effective in a strong sense.

Theorem 1.3 (Pathak, Rojas, and Simpson [17] and Rute [20])**.** *Let $z \in [0,1]^n$. Then z is Schnorr random $\Leftrightarrow$ z is a weak Lebesgue point of every L_1-computable function.*

In Theorem 5.1 we give a proof of the implication "$\Leftarrow$" in Theorem 1.3, which we obtained independently from [17][1]. We show that *if z is not Schnorr random, then there is a bounded L_1-computable function $g\colon [0,1]^n \to \mathbb{R}$ such that z is not a weak Lebesgue point of g.* We note that the function obtained in [17] is also bounded. In comparison, the proof of Theorem 5.1 shows that our function does not have z as a weak Lebesgue point because of a technical property (1), which was not achieved in [17].

As a corollary, we characterise Schnorr randomness in terms of differentiability of Lipschitz functions that are computable in the variation norm.

We note that in dimension 1, the implication "$\Leftarrow$" in Theorem 1.3 can also be derived from the proof of Brattka, Miller, and Nies [2, Theorem 6.7]. In their implication (iii)$\to$(i), given a real z that fails a Martin-Löf test $(G_m)_{m\in\mathbb{N}}$, they build a computable function f of bounded variation that is not differentiable at z. (This result was already announced by Demuth [5], albeit in constructive language.) It suffices to observe that, if the given test $(G_m)_{m\in\mathbb{N}}$ is a Schnorr test, then the function g with $\int_0^x g = f(x)$ constructed in [2, Claim 6.6] is L_1-computable.

[1]This and most other results of this paper were presented by Cameron Freer as a contributed talk on March 24, 2011 at the 2011 North American Annual Meeting of the ASL (held in Berkeley, CA, from March 24 to March 27, almost a year before [17] was available). The abstract, entitled "Effective Aspects of Lipschitz Functions", was published in the June 2012 Bull. Symb. Logic.

1.4. **Lipschitz functions and Schnorr randomness.** Since the function $g\colon [0,1] \to \mathbb{R}$ obtained in Theorem 5.1 is bounded, the function f given by $f(x) = \int_0^x g$ is Lipschitz, and $f'(x) = g(x)$ for almost every x. Thus, if z is not Schnorr random, we can build a computable Lipschitz function f with f' L_p–computable for each computable real $p \geq 1$ that is not differentiable at z.

To formulate an appropriate effectiveness condition for f itself rather than f', recall that any Lipschitz function is absolutely continuous. For any absolutely continuous function f, we have $V(f, [0, x]) = \int_0^x |f'|$. Then f' is L_1-computable iff f is computable in the variation norm, defined by $\|f\|_V = |f(0)| + V(f, [0, 1])$ This means that there is an effective sequence of rational polynomials $(q_n)_{n\in\mathbb{N}}$ such that $\|f - q_n\|_V \leq 2^{-n}$. The latter condition is stronger than the mere computability of f. At the end of Subsection 2.5 we will give somewhat more technical detail. Also see [4, p. 376] for detail on the variation norm.

Let us compare our results on computable randomness and on the weaker notion of Schnorr randomness. Note that in each case we pass from a randomness test failed by a real z to a computable Lipschitz function not differentiable at z. If the real z is not computably random, as shown by a computable martingale M that succeeds on z, we obtain a computable Lipschitz function f that is not differentiable at z. If z is not even Schnorr random, as shown by a Schnorr test, we obtain a computable Lipschitz function f such that f' is L_p-computable for each p; in particular, f is computable in the variation norm.

2. Preliminaries

We collect some background and definitions for later use.

2.1. **Computability of functions on the unit interval.** We paraphrase Definition A in Pour-El and Richards [16, p. 26].

Definition 2.1. *A function $f\colon [0,1] \to \mathbb{R}$ is called* computable *if*

(a) *$f(q)$ is a computable real uniformly in a rational $q \in [0,1]$, 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.*

The definition can be extended almost verbatim to functions $f\colon [0,1]^n \to \mathbb{R}$; in (a) we take n-tuples of rationals. Also, it suffices to consider dyadic rationals in (a).

Every Lipschitz function f is effectively uniformly continuous. Thus (a) is sufficient for the computability of f. If $n = 1$ and f is a continuous monotonic function, then (a) is also sufficient by [2, Prop. 2.2].

2.2. **Differentiability.** We use notation from [2]. For a function $f\colon [0,1] \to \mathbb{R}$, the *slope* at a pair x, y of distinct reals is

$$S_f(x,y) = \frac{f(y) - f(x)}{y - x}.$$

Note that both $x < y$ and $y < x$ are allowed here. Recall that the upper and lower derivatives at z are defined by

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

2.3. Martingales and measures.

Definition 2.2. A *martingale* is a function $2^{<\omega} \to \mathbb{R}_0^+$ such that the fairness condition $M(\sigma 0) + M(\sigma 1) = 2M(\sigma)$ holds for each string σ. We say that M *succeeds* on a sequence of bits Z if $M(Z\upharpoonright_n)$ is unbounded, where $Z\upharpoonright_n$ as usual denotes the length n prefix of Z. 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.

Each martingale M determines a measure on the algebra of clopen sets by assigning $[\sigma]$ the value $M(\sigma)2^{-|\sigma|}$. Via Carathéodory's extension theorem this can be extended to the Borel sets in Cantor space. Measures on Cantor space correspond to measures on $[0,1]$ as long as there are no atoms on dyadic rationals. The measure on $[0,1]$ corresponding to M is denoted by μ_M. Thus, μ_M is determined by the condition

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

Given a 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 non-decreasing and left-continuous. Hence it is determined by its values on the rationals.

Lemma 2.3. *Let $f = \mathsf{cdf}(B)$ for a martingale B. Suppose that $0 \le c < d$ are constants such that $B(\sigma) \in [c,d]$ for each string σ. Then for each pair of reals x, y such that $0 \le x < y \le 1$ we have*

$$c(y-x) \le f(y) - f(x) \le d(y-x).$$

In particular, f is Lipschitz with constant d.

Proof. To verify the second inequality, for an arbitrary n, let $(i,j) \in \mathbb{N}\times\mathbb{N}$ be given by

$$(i,j) = (\lfloor x \cdot 2^n \rfloor, \lceil y \cdot 2^n \rceil).$$

Thus

$$\begin{aligned} i \cdot 2^{-n} &\le x < (i+1)2^{-n} \quad \text{and} \\ (j-1)\cdot 2^{-n} &< y \le j \cdot 2^{-n} \end{aligned}$$

Then

$$\begin{aligned} f(y) - f(x) &= \mu_M[x,y) \\ &\le \sum_{r=i}^{j-1} \mu_M[r2^{-n}, (r+1)2^{-n}) \\ &\le d((j-1)-i)2^{-n} = d((j-1)2^{-n} - (i+1)2^{-n} + 2^{-n}) \\ &< d(y - x + 2^{-n}). \end{aligned}$$

The first inequality is proved in a similar way. □

2.4. Dyadic cubes.

Let $\mathcal{Q}$ be the subset of $[0,1]^n$ consisting of the vectors with a dyadic rational component. By a *dyadic cube* we mean a closed subset C of $[0,1]^n$ which for some k is a product of n intervals of the form $[i2^{-k}, (i+1)2^{-k}]$.

Note that the binary expansion of reals yields a measure preserving map from $[0,1]^n \setminus \mathcal{Q}$ to $(2^\omega)^n$ with the product measure. A dyadic cube with edges of length 2^{-k} corresponds to a clopen subset of the form $[\sigma_1] \times \ldots \times [\sigma_n]$ in $(2^\omega)^n$, where each σ_i has length k.

We say that $G \subseteq [0,1]^n$ is Σ^0_1 if G is an effective union of open cubes with rational coordinates. By transfering a well known basic fact in Cantor space, this shows that from each Σ^0_1 set $V \subseteq [0,1]^n$ we can effectively determine a sequence $(C_i)_{i\in\mathbb{N}}$ of dyadic cubes that are disjoint outside $\mathcal{Q}$, so that $V \setminus \mathcal{Q}$ equals their union outside $\mathcal{Q}$. We let $V_t = \bigcup_{i\le t} C_i$ and say that C_i is enumerated into V at stage t.

Via the usual isometry $(2^\omega)^n \cong 2^\omega$, we may define the binary expansion of a tuple $z = (z_0,\dots,z_{n-1}) \in [0,1]^n \setminus \mathcal{Q}$: this is the bit sequence Z given by $Z(ni+k) = Z_k(i)$, where $i,k\in\mathbb{N}$, $k<n$, and Z_k is the binary expansion of the real z_k.

2.5. **L_p-computability.** Recall that for $p\ge 1$, by $L_p([0,1]^n)$ one denotes the set of integrable functions $g\colon [0,1]^n \to \mathbb{R}$ such that $\|g\|_p = (\int |g|^p d\lambda)^{1/p} < \infty$. In the following let $p\ge 1$ be a computable real. Pour-El and Richards [16, p. 84] define g to be *L_p-computable* if from a rational $\epsilon>0$ one can determine a computable function h on $[0,1]^n$ such that $\|g-h\|_p<\epsilon$. Here the notion of computability for h is the usual one of Subsection 2.1; in particular, h is continuous. By [16, Cor. 1a on p. 86] the polynomials in n variables with rational coefficients are effectively dense with respect to $\|\cdot\|_\infty$, so we might as well assume that h is such a polynomial.

The following is well-known in principle.

Fact 2.4. *If $V \subseteq [0,1]^n$ is Σ^0_1 and λV is a computable real, then the characteristic function 1_V is L_p-computable, uniformly in a presentation of V and Cauchy names for λV and p.*

Proof. Given rational $\epsilon>0$, compute t such that $\lambda(V-V_t) < (\epsilon/2)^p$. Since V_t is effectively given as a finite union of dyadic cubes, we can determine a computable function h such that $\|1_{V_t} - h\|_p < \epsilon/2$. (For instance, let $h(x) = \max(0, 1 - Nd(x,V_t))$, where d denotes Euclidean distance, and $N\in\mathbb{N}$ is an appropriate large number computed from ϵ and p.) This implies $\|1_V - h\|_p < \epsilon$. □

For $1\le q\le p$, then $\|g\|_q \le \|g\|_p$, so every L_p-computable function is L_q-computable. The following fact and its proof suggested by a referee shows that for bounded functions, the converse holds. It is sufficient to consider $q=1$.

Fact 2.5 (due to the referee). *If g is L_1-computable and bounded, then g is L_p-computable for each computable real $p\ge 1$.*

Proof. Suppose $|g(x)|\le C$ for a constant $C\ge 1$. Uniformly in a positive rational $\epsilon\le 1$, we can determine a computable function h on $[0,1]^n$ such that $\|g-h\|_1 < (2C)^{1-p}\epsilon^p$. We can assume that $|h(x)|\le C$ for each x, and so $\alpha := |\frac{g(x)-h(x)}{2C}| \le 1$ for each x, and so $\alpha^p \le \alpha$. Then

$$\begin{aligned}(2C)^{-p}\|g-h\|_p^p &= \int \left|\frac{g-h}{2C}\right|^p d\lambda \le \int \left|\frac{g-h}{2C}\right| d\lambda \\ &= (2C)^{-1}\|g-h\|_1 < (2C)^{-p}\epsilon^{-p}\end{aligned}$$

Thus, $\|g-h\|_p < \epsilon$. □

2.6. **The p-variation norm.** The functions $f\colon [0,1]\to\mathbb{R}$ of bounded variation form a Banach space under the variation norm defined by

$$\|f\|_V = |f(0)| + V(f,[0,1]).$$

We have $\|f\|_V \ge \|f\|_\infty$ (the usual sup norm). Let $AC_0[0,1]$ be the vector space of absolutely continuous functions $f\colon[0,1]\to\mathbb{R}$ such that $f(0)=0$. Let $\mathcal{L}_1[0,1]$ denote the usual set of equivalence classes of functions in $L_1[0,1]$ modulo equality almost everywhere. The map $g \mapsto \lambda x.\int_0^x g$ is a computable Banach space isometry

$$(\mathcal{L}_1[0,1], \|\cdot\|_1) \to (AC_0[0,1], \|\cdot\|_V).$$

Its inverse is the derivative, which is a.e. defined for an absolutely continuous function. See, e.g., [4, p. 376] for more detail. Note that the inverse is automatically computable.

Let $p > 1$. For a function $g\colon [0,1] \to \mathbb{R}$, and $0 \le x < y \le 1$ the *p-variation* of g in $[x,y]$ is

$$V_p(g,[x,y]) = \sup\left\{\sum_{i=1}^{n-1} \frac{|g(t_{i+1}) - g(t_i)|^p}{|t_{i+1} - t_i|^{p-1}} : x \le t_1 < t_2 < \ldots < t_n \le y\right\}.$$

Let

$$\|f\|_{V_p} = |f(0)| + (V_p(f,[0,1]))^{1/p},$$

and let $A_p[0,1]$ denote the class of functions f defined on $[0,1]$ with $f(0) = 0$ and $\|f\|_{V_p} < \infty$. Riesz [18] showed that each function in $A_p[0,1]$ is absolutely continuous. In analogy to the isometry of Banach spaces above, he also showed that the map $g \to \lambda x.\int_0^x g$ yields an isometry

$$(\mathcal{L}_p[0,1], \|\cdot\|_p) \to (A_p[0,1], \|\cdot\|_{V_p}),$$

with inverse the derivative. Note that for computable p, this map is computable with respect to the relevant norms.

We remark that for computable $p \ge 1$, the space $(\mathcal{L}_p[0,1], \|\cdot\|_p)$ is also effectively isomorphic, in the sense of computable Banach spaces, to the Sobolev space $W^{1,p}(0,1)$. This uses the so-called ACL characterization of Sobolev spaces. See, e.g., [22, Thm. 2.1.4].

2.7. **Interval-r.e. functions.** We recall that a real $x \in [0,1]$ is *left-r.e.* if the set $\{q \in \mathbb{Q}\colon q < x\}$ is r.e. If this left cut equals W_e, we say that e is an *index* for x. (Such a real is also called "left-computable", and sometimes "lower semicomputable", in the literature.)

Definition 2.6. *A non-decreasing function f defined on* $[0,1]$ *is called* interval-r.e. *if $f(0) = 0$, and $f(y) - f(x)$ is left-r.e. uniformly in rationals $x < y$.*

Suppose in Definition 2.6 we drop the restriction on x, y being rational, and require the stronger condition that $f(y) - f(x)$ is left-r.e. relative to Cauchy names of reals $x < y$. The variation of a computable function, and the functions f_M defined below, satisfy this stronger condition. For continuous functions, the two conditions are equivalent. For suppose the weaker condition in Definition 2.6 holds. If $(p_n)_{n\in\mathbb{N}}$ and $(q_n)_{n\in\mathbb{N}}$ are Cauchy names for x and y respectively, then $x \le p_n + 2^{-n}$ and $q_n - 2^{-n} \le y$ for each n. Then by continuity $f(y) - f(x)$ is the sup of the values $f(q_n - 2^{-n}) - f(p_n + 2^{-n})$ where $p_n + 2^{-n} \le q_n - 2^{-n}$. This is left-r.e. in the Cauchy names by hypothesis.

See [11, Ch. 2] or [6] or [10] for background on prefix-free machines and prefix-free complexity K. For a set $B \subseteq 2^{<\omega}$ let $[B]^{\prec}$ denote the open set $\{X \in 2^\omega\colon \exists n\, X \restriction_n \in B\}$. Let S be a prefix-free machine. We identify a binary string γ with the dyadic rational $0.\gamma$. The following function is interval-r.e.:

$$f_S(x) = \lambda[\{\sigma\colon\, S(\sigma) < x\}]^{\prec}.$$

Thus, $f_S(x)$ is the probability that S prints a dyadic rational less than x. Note that f_S is left continuous ($f_S(x) = f_S(x^-)$ for each x) and hence, being increasing, lower semi-continuous. Furthermore, f_S is discontinuous at x (namely, $f_S(x) < f_S(x^+)$) precisely if $x < 1$ is a dyadic rational in the domain of S.

Let $\mathbb{U}$ be a universal prefix free machine, and consider the increasing interval-r.e. function $f_{\mathbb{U}}(x)$. Then $f_{\mathbb{U}}(1) = \Omega_{\mathbb{U}}$, and thus $f_{\mathbb{U}}$ is not computable on the rationals.

Proposition 2.7. *Let $z \in [0,1]$. If $\overline{D} f_{\mathbb{U}}(z) < \infty$ then z is Martin-Löf random.*

Proof. Suppose that z is not ML-random. Given $c \in \mathbb{N}$ pick n such that $K(z\restriction_n) \le n - c$. Let $h = -2^{-n}$. We have

$$2^{-n+c} \le \lambda[\{\sigma\colon\ \mathbb{U}(\sigma) \in [z+h, z)\}]^{\prec} = f_{\mathbb{U}}(z) - f_{\mathbb{U}}(z+h).$$

Therefore $2^c \le (f_{\mathbb{U}}(z+h) - f_{\mathbb{U}}(z))/h$. □

In [1] it is shown that, conversely, if z is Martin-Löf random then each interval-r.e. function has finite upper derivative. In contrast, there is a function of the form f_S for a prefix-free machine S that is not differentiable at Chaitin's Ω. Simply let the domain of S generate the open set in Cantor space corresponding to $[0, \Omega)$ (i.e., $x < \Omega$ iff $\exists n\, S(x\restriction_n)\downarrow$). Then f_S increases to Ω in smaller and smaller steps, and it is constant equal to Ω thereafter. It is easy to check that $f'_S(\Omega)$ fails to exist. [1] also show that a randomness property of a real z slightly stronger than Martin-Löf's ensures that each interval-r.e. function is differentiable at z. We will discuss this in the concluding section of the paper.

3. Characterizing the variation of computable (Lipschitz) functions

Let $g\colon [0,1] \to \mathbb{R}$ be a computable function. Since $V(g,[x,y]) + V(g,[y,z]) = V(g,[x,z])$ for $x < y < z$, we see that the function $f(x) = V(g,[0,x])$ is interval-r.e. and continuous. Note that if f is Lipschitz with constant c, then the function g is necessarily Lipschitz with constant at most c, because for $x < y$ we have

$$|g(y) - g(x)| \le V(g,[x,y]) = V(g,[0,y]) - V(g,[0,x]).$$

As our main result in this section, we will prove the converse for Lipschitz functions: every interval-r.e., non-decreasing Lipschitz function f is of the form $V(g,[0,x])$ for some computable Lipschitz function g. We begin with the simpler result that the total variation can be any given left-r.e. real.

Fact 3.1. *For each left-r.e. real α, $0 \le \alpha \le 1$, there is a computable function g which is Lipschitz with constant 1 such that $V(g,[0,1]) = \alpha$.*

Proof. For each interval of dyadic rationals $[p,q]$, where $p = i2^{-n}$, $q = j2^{-n}$, $0 \le i \le j < 2^n$, and each $k > n$, let $W(p,q;k)$ be the function that zigzags

$$(q-p)2^k = (j-i)2^{k-n}$$

times within $[p,q]$, with slope ± 1. Then the total variation of $W(p,q;k)$ is $q-p$.

Now let $\alpha = \lim_s \alpha_s$ where $(\alpha_s)_{s\in\mathbb{N}}$ is an increasing effective sequence of dyadic rationals α_s of the form $i2^{-n}$ with $n < s$. Let

$$g = \textstyle\sum_s W(\alpha_s, \alpha_{s+1}; s+1).$$

It is easy to check that g is a computable function that is Lipschitz with constant 1. Furthermore, since variation is additive over partitions into disjoint intervals, g has variation α. (For intuition, note that as α_s approaches α, the oscillations become flatter and flatter. To the right of α, g is constant.) □

It is well known that for any L_1-computable function h, the function $x \mapsto \int_0^x h$ is computable. Using the foregoing fact we provide an example showing that the converse fails.

Corollary 3.2. *Some nondecreasing computable Lipschitz function u is not of the form $x \mapsto \int_0^x v$ for any L_1-computable function v.*

Proof. Let α be a left-r.e. noncomputable real, and let g be as in Fact 3.1. Let $u(x) = x - g(x)$. Then u is nondecreasing and Lipschitz with constant 2. Assume for a contradiction that u is of the form $\int_0^x v$ for an L_1-computable function v.

We have $g(x) = \int_0^x h$, where $h = 1 - v$. Then $V(g, [0, x]) = \int_0^x |h|$ by a classic result of analysis (see [3, Prop. 5.3.7]). Furthermore, $|h|$ is L_1-computable. Thus, $V(g, [0, 1])$ is a computable real, a contradiction. □

The proof of our main result in this section makes use of signed martingales, namely, functions $L\colon 2^{<\omega} \to \mathbb{R}$ satisfying the martingale equality $2L(\sigma) = L(\sigma 0) + L(\sigma 1)$ for each string σ. Given a signed martingale L, let

$$V_L(\sigma) = \sup_k 2^{-k} \sum_{|\eta|=k} |L(\sigma\eta)|.$$

It is easy to build a computable L such that $V_L(\emptyset) = \infty$. If $V_L(\sigma) < \infty$ for each σ, we say that V_L is the *variation martingale* of L. Note that the expression on the right is nondecreasing in k. Thus, if L is computable then the variation martingale V_L is a left-r.e. (non-negative) martingale.

We say that a martingale $M\colon 2^{<\omega} \to \mathbb{R}_0^+$ is *non-atomic* if the corresponding measure μ on Cantor space is non-atomic (see the discussion after Definition 2.2). This means that for each $X \in 2^\omega$ we have $M(X \restriction_n) = o(2^n)$. By compactness of Cantor space, the function $X \mapsto \mu[0, X]$ is uniformly continuous. So, in fact we have the apparently stronger condition that $M(\sigma) = o(2^{|\sigma|})$ for each string σ.

Lemma 3.3. *Let $M\colon 2^{<\omega} \to \mathbb{R}_0^+$ be a left-r.e. non-atomic martingale. Then there is a computable signed rational-valued martingale L such that $M = V_L$. Furthermore, $|L(\sigma)| \leq M(\sigma)$ for each σ.*

Proof. Since M is left-r.e., we may assume that $M(\sigma) = \sup_s M_s(\sigma)$ where each M_s is a recursive martingale uniformly in s, sending strings to rational numbers, and $M_s(\sigma) \leq M_t(\sigma)$ whenever $s \leq t$. For natural numbers $a < b$ and a string σ of length a, define the approximation of V_L on level b by

$$V_{L,b}(\sigma) = 2^{-(b-a)} \sum_{|\eta|=b-a} |L(\sigma\eta)|.$$

Now one defines the new martingale L inductively with $L(\varnothing) = 0$ where $\varnothing$ is the empty string. At stage s, the idea is to define L for strings of lengths

$$\ell_s + 1, \ell_s + 2, \dots, \ell_{s+1}$$

where ℓ_{s+1} will be chosen so that for all $\sigma \in \{0,1\}^{\ell_s}$, the difference between $M_s(\sigma)$ and $V_{L,\ell_{s+1}}(\sigma)$ is less than 2^{-s}.

One defines inductively for all strings of length $\ell_s, \ell_s + 1, \dots$ the value of $L(\sigma 0)$ and $L(\sigma 1)$, using that $|L(\sigma)| \leq M_s(\sigma)$ and imposing the same on $L(\sigma 0)$ and $L(\sigma 1)$. Choose $a \in \{0, 1\}$

such that $M_s(\sigma a) \le M_s(\sigma(1-a))$ and define L on $\sigma 0$ and $\sigma 1$ as follows:

$$L(\sigma a) = \begin{cases} M_s(\sigma a) & \text{if } L(\sigma) \ge 0; \\ -M_s(\sigma a) & \text{if } L(\sigma) < 0; \end{cases}$$

$$L(\sigma(1-a)) = \begin{cases} M_s(\sigma a) + 2 \cdot (L(\sigma) - M_s(\sigma a)) & \text{if } L(\sigma) \ge 0; \\ -M_s(\sigma a) + 2 \cdot (L(\sigma) + M_s(\sigma a)) & \text{if } L(\sigma) < 0. \end{cases}$$

Note that L satisfies the martingale equality. If $L(\sigma) \ge 0$ then

$$L(\sigma(1-a)) \le M_s(\sigma a) + 2 \cdot (M_s(\sigma) - M_s(\sigma a)) = M_s(\sigma(1-a))$$

and

$$L(\sigma(1-a)) \ge -M_s(\sigma a) \ge -M_s(\sigma(1-a)).$$

Hence $|L(\sigma a)| = M_s(\sigma a) \le M(\sigma a)$ and $|L(\sigma(1-a))| \le M_s(\sigma(1-a)) \le M(\sigma(1-a))$ in this case. If $L(\sigma) < 0$ then

$$L(\sigma(1-a)) \ge -M_s(\sigma a) + 2(-M_s(\sigma) + M_s(\sigma a)) = -M_s(\sigma(1-a))$$

and

$$L(\sigma(1-a)) \le M_s(\sigma a) \le M_s(\sigma(1-a)).$$

Again this implies $|L(\sigma a)| = M_s(\sigma a) \le M(\sigma a)$ and $|L(\sigma(1-a))| \le M_s(\sigma(1-a)) \le M(\sigma(1-a))$.

Furthermore, note that whenever $L(\sigma) = M_s(\sigma)$ then $L(\sigma 0) = M_s(\sigma 0)$ and $L(\sigma 1) = M_s(\sigma 1)$; whenever $L(\sigma) = -M_s(\sigma)$ then $L(\sigma 0) = -M_s(\sigma 0)$ and $L(\sigma 1) = -M_s(\sigma 1)$.

So one can show by induction that there are on each of the levels $\ell_s + 1, \ell_s + 2, \ldots$ at most 2^{ℓ_s} strings σ with $|L(\sigma)| \ne M_s(\sigma)$. As $M(\sigma) = o(2^{|\sigma|})$, there is some level ℓ_{s+1} such that for all $\sigma \in \{0,1\}^{\ell_s}$ the difference between $V_{L,\ell_{s+1}}(\sigma)$ and $M_s(\sigma)$ is at most 2^{-s}. From this fact, one can conclude that for each string σ, the difference between $M(\sigma)$ and $V_{L,\ell_t}(\sigma)$ is for $\ell_t \ge |\sigma|$ bounded by $M(\sigma) - M_t(\sigma) + 2^{-t}$. So $V_L(\sigma) = M(\sigma)$ for all strings σ.

The condition $|L(\sigma)| \le M(\sigma)$ can be verified by an easy induction using that $M_s(\sigma) \le M_{s+1}(\sigma) \le M(\sigma)$ for all s. □

Theorem 3.4. *Let f be a non-decreasing interval-r.e. function with Lipschitz constant c. Then there is a computable function g with the same Lipschitz constant c such that $f(x) = V(g, [0, x])$ for each $x \in [0, 1]$.*

Proof. We define a left-r.e. martingale M by $M(\sigma) = S_f(0.\sigma, 0.\sigma + 2^{-|\sigma|})$. Note that M is bounded by the Lipschitz constant c for f. Let L be the signed computable rational-valued martingale with $V_L = M$ obtained through Lemma 3.3. Then $|L|$ is bounded by c as well.

For a dyadic rational $0.\sigma$, σ a binary string, we let

$$g(0.\sigma) = 2^{-|\sigma|} \sum \{L(\tau) : \ 0.\tau < 0.\sigma \ \wedge \ |\tau| = |\sigma|\}.$$

Note that by the martingale equality, g is well defined on the dyadic rationals in $[0, 1)$. Clearly, for strings σ, ρ of the same length n, we have

$$|g(0.\sigma) - g(0.\rho)| \le 2^{-n} \sum \{|L(\tau)| : \ 0.\rho \le 0.\tau < 0.\sigma \ \wedge \ |\tau| = n\} \le c|0.\sigma - 0.\rho|.$$

Thus g is Lipschitz on the dyadic rationals. Therefore by the remark after Definition 2.1, g can be extended to a computable function on $[0, 1]$ with Lipschitz constant c, also denoted g.

We claim that $f(x) = V(g,[0,x])$ for each $x \in [0,1]$. By continuity of f and g, we may assume that $x = 0.\sigma$ for string σ of length n, and that in the definition of $V(g,[0,x])$ we only consider partitions consisting of all the dyadic rationals $0.\rho < 0.\sigma$, where all ρ have the same length $k \geq |\sigma|$. Then

$$V(g,[0,x]) = 2^{-n}\sum\{V_L(\tau)\colon\ 0.\tau < 0.\sigma\ \wedge\ |\tau| = n.\}$$

Since $f(0) = 0$ we have

$$f(x) = 2^{-n}\sum\{S_f(0.\tau, 0.\tau + 2^{-n})\colon\ 0.\tau < 0.\sigma\ \wedge\ |\tau| = n\}.$$

Since $M(\tau) = S_f(0.\tau, 0.\tau + 2^{-n})$ and $M = V_L$, this establishes the claim. □

Extension to all continuous interval-r.e. functions. After seeing our result, Jason Rute has extended the technique of Theorem 3.4, discarding the hypothesis that the given function be Lipschitz:

Theorem 3.5 (with Rute). *Let f be a continuous non-decreasing interval-r.e. function. Then there is a computable function g such that $f(x) = V(g,[0,x])$ for each $x \in [0,1]$.*

Proof. Suppose that M is the left-r.e. martingale associated with f. It is not enough to just do what we did before. The problem is that given a signed martingale L, the function g is not necessarily computable. (Here, although L can be negative, it is correct to write $g = \mathsf{cdf}(L)$.) This can be fixed by being a bit more careful about which L we construct in Lemma 3.3.

To construct L from M, we follow the proof of Lemma 3.3, with one adjustment. Note that for each M_s in the proof of Lemma 3.3, there is some stage k_s in which $2^{-|\sigma|} \cdot M_s(\sigma) \leq 2^{-s}$ for all $|\sigma| \geq k_s$.

Indeed, M_s has no atoms, hence for each x, $2^{-k} \cdot M_s(x \upharpoonright_k) \searrow 0$ as $k \to \infty$. In particular, for each x there is a k such that $2^{-k} \cdot M_s(x \upharpoonright_k) \leq 2^{-s}$. By compactness, there is in fact a single k such that for all x, $2^{-k} \cdot M_s(x \upharpoonright_k) \leq 2^{-s}$.

Do not switch from M_{s-1} to M_s in the construction until after stage k_{s+1} (we can assume $M_0 = M_1 = 0$).

Let j_s be the stage at which we switch to M_s. Clearly, $j_s \geq k_{s+1}$. So for any σ such that $j_{s+1} > |\sigma| \geq j_s$ we have $|L(\sigma)| \leq M_s(\sigma)$ by construction. Therefore,

$$2^{-|\sigma|} \cdot |L(\sigma)| \leq 2^{-|\sigma|} \cdot M_s(\sigma) \leq 2^{-|\sigma|} \cdot M_{s+1}(\sigma) \leq 2^{-(s+1)}.$$

Let $g = \mathsf{cdf}(L)$. By the same proof as in Theorem 3.4, $f(x) = V(g,[0,x])$.

It remains to show that g is computable. Clearly, $g(0.\sigma)$ is uniformly computable for all σ. Let ν be the signed measure associated with L, so that

$$\nu([0.\sigma, 0.\sigma + 2^{-|\sigma|})) = 2^{-|\sigma|}L(\sigma) \quad \text{and} \quad \mathsf{cdf}(\nu) = \mathsf{cdf}(L).$$

Also, for each s, let μ_s be the measure associated with M_s. The above formula then becomes (writing $\nu(\sigma)$ for $\nu([0.\sigma + 2^{-|\sigma|}))$

$$|\nu(\sigma)| \leq \mu_s(\sigma) \leq \mu_{s+1}(\sigma) \leq 2^{-(s+1)}$$

for $j_{s+1} > |\sigma| \geq j_s$. Pick $a \in [0,1]$. To compute $g(a)$ within $2^{-(s-1)}$ uniformly from a, let $\sigma = a \upharpoonright j_s$ (i.e., $a \in [\sigma]$ and $|\sigma| = j_s$). From the Cauchy name for a, one can determine one of the values $\{g(0.\sigma), g(0.\sigma + 2^{-j_s})\}$. Notice that

$$|g(0.\sigma + 2^{-j_s}) - g(0.\sigma)| = |\nu(\sigma)| \leq 2^{-(s+1)}.$$

We claim that $|g(a) - g(0.\sigma)| \leq 2^{-s}$.

The claim is equivalent to saying that $|\nu[0.\sigma, a)| \le 2^{-s}$. We know that $[0.\sigma, a) \subseteq [\sigma]$. Now, break up $[0.\sigma, a)$ into $[\tau_n] \cup \cdots \cup [\tau_1] \cup [0.\tau_0, a)$, where $\tau_n, \ldots, \tau_1, \tau_0$ are adjacent, $|\tau_i| = j_{s+1}$ for $1 \le i \le n$, and $\tau_0 = a \upharpoonright j_{s+1}$. Since $|\sigma| = j_s$ and $|\tau_i| = j_{s+1}$, we have

$$\begin{aligned}|\nu[0.\sigma, a)| &\le |\nu(\tau_n)| + \cdots + |\nu(\tau_1)| + |\nu[0.\tau_0, a)| \\ &\le \mu_{s+1}(\tau_n) + \cdots + \mu_{s+1}(\tau_1) + |\nu[0.\tau_0, a)| \\ &\le \mu_{s+1}(\sigma) + |\nu[0.\tau_0, a)| \\ &\le 2^{-(s+1)} + |\nu[0.\tau_0, a)|.\end{aligned}$$

Continuing by recursion, we have for each m that

$$|\nu[0.\sigma, a)| \le |\nu[0.\tau_0^m, a)| + \sum_{i=1}^{m} 2^{-(s+i)}$$

where $\tau_0^m = a \upharpoonright j_{s+m}$. Let μ be the measure associated with M. Then

$$|\nu[0.\tau_0^m, a)| \le \mu[0.\tau_0^m, a) \to 0 \quad \text{as} \quad m \to \infty,$$

and hence $|\nu[0.\sigma, a)| \le \sum_{i=1}^{\infty} 2^{-(s+i)} = 2^{-s}$. □

4. Computable randomness and Lipschitz functions

4.1. **Characterizing computable randomness.** Schnorr [21] introduced the following notion.

Definition 4.1. A 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 a binary expansion of z is computably random.

Note that we can ignore the case that there are two binary expansions of z, because in that case z is a dyadic rational and hence computable. Also, it suffices to require that no rational-valued computable martingale succeeds on a binary expansion of z by a result of [21] (for a recent reference see [11, 7.3.8]). Here computability of the martingale can even be taken in the strong sense that we can uniformly compute a canonical index for the rational value (rather than give a sequence of approximations that happen to converge to a rational value). For more background on computable randomness see [11, Ch. 7] or [6].

We now characterize computable randomness by differentiability of computable Lipschitz functions, analogously to Theorem 1.1 due to [2] mentioned in the introduction.

Theorem 4.2. *Let $z \in [0, 1]$. Then z is computably random $\Leftrightarrow$ each computable Lipschitz function $f\colon [0, 1] \to \mathbb{R}$ is differentiable at z.*

Proof of Theorem 4.2. $\Rightarrow$: Suppose f is a computable Lipschitz function with a Lipschitz bound $c \in \mathbb{N}$. As observed above, the function $g(x) = f(x) + cx$ is nondecreasing. Since g is computable, by [2, Thm. 4.1], $g'(z)$, and hence $f'(z)$, exists.

$\Leftarrow$: We may assume that z is not a dyadic rational. Suppose z is not computably random, so some computable martingale M succeeds on the binary expansion Z of z. We will build a computable Lipschitz function f that is not differentiable at z.

We let $f = \mathsf{cdf}(B)$ as defined in Subsection 2.3, for a computable bounded martingale B that oscillates between values ≥ 3 and values ≤ 2 when processing longer and longer initial segments of the binary expansion of z. We build B from M. Note that for any string σ, the value $B(\sigma)$ is the slope of f between the dyadic rationals $0.\sigma$ and $0.\sigma + 2^{-|\sigma|}$, so f is not differentiable at z. The argument in the usual proof of the Doob martingale convergence theorem (see, e.g., [7]) turns oscillation of a martingale into success of another martingale. In a sense, we reverse this argument, turning the success of M into oscillation of B.

As mentioned above, we may assume that M only takes positive rational values which can be computed in a single output from the input string. We may also assume that M has the savings property

$$M(\sigma\eta) \geq M(\sigma) - 1 \text{ for each strings } \sigma, \eta;$$

see e.g. Exercise [11, 7.1.14] and its solution, or [6]. At each σ, the martingale B is in one of two possible phases. In the *up phase*, it adds the capital that M risks, until its value $B(\sigma)$ reaches 3 (if this value would exceed 3, B adds less in order to ensure the value equals 3). In the *down phase*, B subtracts the capital that M risks, until the value $B(\sigma)$ reaches 2.

In more detail, the construction of B is as follows. Inductively we show that if B is in the up phase at σ, then $B(\sigma) < 3$, and if B is in the down phase at σ then $B(\sigma) > 2$. At the empty string $\emptyset$, the martingale B is in the up phase and $B(\emptyset) = 2$. Thus the inductive condition holds at the empty string. Suppose now that $B(\sigma)$ has been defined.

Case 1: B is in the up phase at σ. Let

$$r_k = B(\sigma) + M(\sigma k) - M(\sigma).$$

If $r_0, r_1 < 3$ then let $B(\sigma k) = r_k$; stay in the up phase at both $\sigma 0$ and $\sigma 1$. Otherwise, since M is a martingale and $B(\sigma) < 3$, there is a unique k such that $r_k \geq 3$. Let $B(\sigma k) = 3$ and $B(\sigma(1-k)) = 2B(\sigma) - 3$. Go into the down phase at σk, but stay in the up phase at $\sigma(1-k)$. Note that the inductive condition is maintained at both $\sigma 0$ and $\sigma 1$.

Case 2: $B(\sigma)$ is in the down phase. Let

$$r_k = B(\sigma) - (M(\sigma k) - M(\sigma)).$$

If $r_0, r_1 > 2$ then let $B(\sigma k) = r_k$; stay in the up phase at both $\sigma 0$ and $\sigma 1$. Otherwise, since M is a martingale and $B(\sigma) > 2$, there is a unique k such that $r_k \leq 2$. Let $B(\sigma k) = 2$ and $B(\sigma(1-k)) = 2B(\sigma) - 2$. Go into the up phase at σk, but stay in the down phase at $\sigma(1-k)$. The inductive condition is maintained at both $\sigma 0$ and $\sigma 1$.

Claim 4.3. *For each string τ we have $1 \leq B(\tau) \leq 4$.*

To see this, suppose first that B is in the up phase at τ. Then $B(\tau) \leq 3$. For the lower bound on $B(\tau)$, suppose that B entered the up phase at the string $\sigma \preceq \tau$ with $|\sigma|$ maximal. Then $B(\sigma) = 2$. By the savings property we have $M(\tau) - M(\sigma) \geq -1$. Therefore $B(\tau) = B(\sigma) + M(\tau) - M(\sigma) \geq 1$.

Next suppose that B is in the down phase at τ. Then $B(\tau) \geq 2$. For the upper bound on $B(\tau)$, suppose that B entered the down phase at the string $\sigma \preceq \tau$ with $|\sigma|$ maximal. Then $B(\sigma) = 3$. By the savings property we have $B(\tau) = B(\sigma) - (M(\tau) - M(\sigma)) \leq 4$. This shows the claim.

Since M succeeds on the binary expansion Z of z, it is clear that B oscillates along Z as described above. ☐

5. Schnorr randomness in $[0,1]^n$ and Lipschitz functions

5.1. **Schnorr randomness.** We let λ denote Lebesgue measure on $[0,1]^n$. For an introduction to algorithmic randomness in spaces other than Cantor space and $[0,1]$, see [9]. We say that $G \subseteq [0,1]^n$ is Σ^0_1 if $G = [0,1]^n \cap H$ where $H \subseteq \mathbb{R}^n$ is an effective union of open cubes with rational coordinates. A uniformly Σ^0_1 sequence $(G_m)_{m\in\mathbb{N}}$ is called *Schnorr test* if $\lambda G_m \leq 2^{-m}$

and λG_m is a computable real uniformly in m. A point $z \in [0,1]^n$ is called *Schnorr random* if $z \notin \bigcap_m G_m$ for each Schnorr test $(G_m)_{m\in\mathbb{N}}$.

5.2. **Characterizing Schnorr randomness.** We characterize Schnorr randomness of a real by being a weak Lebesgue point of each bounded L_1-computable function. As a corollary, we obtain a characterization in terms of differentiability at the real of all Lipschitz functions that are computable in the p-variation norm for a fixed computable real $p \geq 1$. (See the introduction for more background and the relationship of this result to [17].)

Theorem 5.1. *Let $z \in [0,1]^n$. Then z is Schnorr random $\Leftrightarrow$*
z is a weak Lebesgue point of each L_1-computable bounded function $g\colon [0,1]^n \to \mathbb{R}$.

Proof. $\Rightarrow$: This is immediate by [17, Thm. 1.6]. They show that in fact, z is a weak Lebesgue point of each L_1-computable function, bounded or not.
$\Leftarrow$: This implication is proved by contraposition Suppose $z \in [0,1]^n$ is not Schnorr random. We build a bounded L_1-computable function $g\colon [0,1]^n \to \mathbb{R}$, and a sequence of dyadic cubes $C_m \downarrow z$, such that

$$\limsup_m \frac{\int_{C_m} g}{\lambda C_m} = 1 \quad \text{and} \quad \liminf_m \frac{\int_{C_m} g}{\lambda C_m} = -1. \tag{1}$$

Then z is not a weak Lebesgue point of g.

Recall that $\mathcal{Q}$ denotes the subset of $[0,1]^n$ consisting of the vectors with a dyadic rational component. Clearly g exists for $z \in \mathcal{Q}$, so we may assume that $z \notin \mathcal{Q}$. In the following all assertions of inclusion relations and disjointness for subsets of $[0,1]^n$ are meant to hold only on $[0,1]^n \setminus \mathcal{Q}$.

Let $(V_m)_{m\in\mathbb{N}}$ be a Schnorr test in $[0,1]^n$ such that $z \in \bigcap_m V_m$. We will modify $(V_m)_{m\in\mathbb{N}}$ to obtain a new Schnorr test $(G_m)_{m\in\mathbb{N}}$ with $\bigcap_m V_m \subseteq \bigcap_m G_m$, and in particular $z \in \bigcap_m G_m$ (using that $z \notin \mathcal{Q}$). Thereafter we will show that the bounded function g defined by $g(x) = 0$ for $x \in \bigcap_m G_m$ and

$$g(x) = \sum_{m=0}^{\infty} (-1)^m 1_{G_m}(x) \tag{2}$$

for $x \notin \bigcap_m G_m$ is as required.

Recall from Subsection 2.4 that at each stage t we have a set $V_{m,t}$ which is a finite union of dyadic cubes that are disjoint (outside $\mathcal{Q}$).

Construction of the Schnorr test $(G_m)_{m\in\mathbb{N}}$. Set $G_{0,s} = [0,1]^n$ for each s. Suppose inductively we have defined a computable enumeration $(G_{m,s})_{s\in\mathbb{N}}$ of G_m. Suppose that a dyadic cube C is enumerated into $G_{m,s}$. Let $r \geq s$ be least such that

$$2^{-r} \leq 2^{-m-1}\lambda C. \tag{3}$$

(this will be used to show that z is not a weak Lebesgue point of g). Enumerate the set $V_r \cap C$ into G_{m+1}. In more detail, for all $t \geq s$ enumerate the set $V_{r,t} \cap C$ into $G_{m+1,t}$. This ends the construction.

Note that because C is disjoint from $G_{m,s-1}$, the set $V_r \cap C$ is also disjoint from $G_{m+1,s-1}$; this will be needed when we verify that the reals λG_m are uniformly computable.

Claim 5.2. *We have $\bigcap_{r\in\mathbb{N}} V_r \subseteq G_m$ for each m.*

We verify the claim by induction on m. Clearly $\bigcap_{r\in\mathbb{N}} V_r \subseteq G_0 = [0,1]^n$. Inductively suppose that $\bigcap_{r\in\mathbb{N}} V_r \subseteq G_m$. Thus every point in the set $\bigcap_{r\in\mathbb{N}} V_r \setminus \mathcal{Q}$ is in some cube C enumerated into G_m. Then by construction we have $\bigcap_{r\in\mathbb{N}} V_r \cap C \subseteq G_{m+1}$. This shows the claim.

We now verify that $(G_m)_{m\in\mathbb{N}}$ is a Schnorr test. Clearly (3) implies that $\lambda G_m \leq 2^{-m}$ for each m.

Claim 5.3. *$\lambda(G_m)$ is a computable real uniformly in m.*

Note that $\lambda(G_0) = 1$. Inductively suppose we have a procedure to compute the real λG_m. Given a rational $\epsilon > 0$, we will (uniformly in m) compute a t such that $\lambda(G_{m+1} \setminus G_{m+1,t}) < 2\epsilon$. By the inductive hypothesis we can compute s such that $\lambda(G_m \setminus G_{m,s}) < \epsilon$. Let N be the number of cubes in $G_{m,s}$. Denote these cubes $C_0, \ldots, C_{N-1}$.

Since the quantities $\lambda(V_m)$ are computable uniformly in $m \in \mathbb{N}$, we may compute $t \geq s$ such that for all $i < N$, we have

$$\lambda(V_{r_i} \setminus V_{r_i,t}) < \frac{\epsilon}{2N},$$

where V_{r_i} is the set selected on behalf of the cube C_i in the construction of G_{m+1}. By construction, for each $t \geq s$ we have

$$G_{m+1,t} \cap G_{m,s} = \bigcup_{i=0}^{N-1}(V_{r_i,t} \cap C_i).$$

Then, since $G_{m,s} = \bigcup_{i=0}^{N-1} C_i$,

$$\lambda\big((G_{m+1} \setminus G_{m+1,t}) \cap G_{m,s}\big) < \epsilon/2,$$

because every cube enumerated into G_m after stage s is disjoint from $G_{m,s}$ by construction. Recall that by choice of s we have $\lambda(G_m - G_{m,s}) < \epsilon$. Therefore

$$\lambda(G_{m+1} \setminus G_{m+1,t}) \leq \epsilon + \lambda\big((G_{m+1} \setminus G_{m+1,t}) \cap G_{m,s}\big) \leq 2\epsilon,$$

as desired.

Claim 5.4. *The function g defined in (2) is L_1-computable.*

By Claim 5.3 and Fact 2.4, the function 1_{G_i} is L_1-computable uniformly in i. Thus, the function $h_k = \sum_{i=0}^{m}(-1)^i 1_{G_i}$ is also L_1-computable uniformly in m. It now suffices to show that given a rational $\epsilon > 0$, we can compute k such that the 1-norm of the rest of the sum is less than ϵ.

For each $r \in \mathbb{N}$ we have

$$\|\textstyle\sum_{m=r}^{\infty}(-1)^m 1_{G_m}\|_1 \leq \sum_{m=r}^{\infty} \|1_{G_m}\|_1 \leq \sum_{m=r}^{\infty}(\lambda G_m) \leq 2^{-r+1}.$$

This shows the claim.

Claim 5.5. *Let C_m be the dyadic cube enumerated into G_m such that $z \in C_m$. Then the sequence $(C_m)_{m\in\mathbb{N}}$ is as required in the lemma.*

First we show that

$$\lim_{m\,\text{even}, m\to\infty} \frac{\int_{C_m} g}{\lambda C_m} = 1. \tag{4}$$

For $i \leq m$ we have $C_m \subseteq G_i$. Hence

$$\frac{\int_{C_m} \sum_{i=0}^{m}(-1)^i 1_{G_i}(x)}{\lambda C_m} = 1.$$

Now consider $i > m$. Note that by the choice of r in (3) we have $\lambda(G_i \cap C_m) \leq 2^{-(i-m)m}\lambda C_m$. Therefore

$$|\textstyle\int_{C_m} \sum_{i=m+1}^{\infty}(-1)^i 1_{G_i}(x)| \leq \lambda C_m \sum_{i=m+1}^{\infty} 2^{-(i-m)m} \leq 2^{-m+1}\lambda C_m.$$

This yields (4). In a similar way one shows that $\lim_{m \text{ odd}, m\to\infty} \frac{\int_{C_m} g}{\lambda C_m} = -1$. This establishes the claim, and the theorem. □

By Fact 2.5, the function g constructed above is actually L_p-computable for each computable real $p \geq 1$. For $p > 1$, recall the p-variation norm and the Riesz classes $A_p[0,1]$ from Subsection 2.6. Let $A_1[0,1] = AC_0[0,1]$ be the space of absolutely continuous functions.

Corollary 5.6. *Let $p \geq 1$ be a computable real. The following are equivalent for a real $z \in [0,1]$:*

(i) *z is Schnorr random.*
(ii) *Every function in $A_p[0,1]$ that is computable in the p-variation norm is differentiable at z.*
(iii) *Every Lipschitz function f that is computable in the p-variation norm is differentiable at z.*

Proof. (i)→(ii) follows by Theorem 5.1 and the computable isometry $\mathcal{L}_p[0,1] \to A_p[0,1]$ in Subsection 2.6. For (ii)→(iii) it suffices to note that every Lipschitz function is in $A_p[0,1]$. Finally, for (iii)→(i), suppose that z is not Schnorr random. Note that by Fact 2.5, the bounded function g built in the proof of Theorem 5.1 is L_p computable. The image of this function under the same isometry is Lipschitz and not differentiable at z. □

6. Discussion and open problems

We have seen that the study of effective Lipschitz functions f is intimately connected to the study of left-r.e. bounded martingales and computable (signed) martingales.

Nondifferentiability of f at a real z corresponds is the conceptual analogue of oscillation of the martingale $M(\sigma) = S_f(0.\sigma, 0.\sigma + 2^{-|\sigma|})$ on the binary expansion of z; that is, for some $\alpha < \beta$, we have infinitely many initial segments where the value is less than α, and infinitely many where the value is greater than β. We make some points regarding the connection between non-differentiability and oscillation.

1. It can happen that $f'(z)$ fails to exist even if $M(Z)$ does not oscillate, because the martingale only looks at the slope for basic dyadic intervals $[0.\sigma, 0.\sigma+2^{-|\sigma|}]$ containing z, while for differentiability we need to consider arbitrary small intervals containing z. For instance, following [2, Section 4], the nondecreasing Lipschitz function $f_0(x) = x\sin(2\pi \log_2 |x|) + 10x$ satisfies $f(x) = 10x$ for each x of the form $\pm 2^{-n}$, but $9 = \underline{D}f(0) < \overline{D}f(0) = 11$. Let f be the right-shift by $1/2$ of f_0. Then f is as required for $z = 1/2$.

2. It is easy to show that if a bit sequence Z is not Martin-Löf random, then some unbounded left-r.e. martingale M oscillates on Z: take a left-r.e. martingale L that succeeds on Z. Each time M has passed 2, it ensures the capital decreases to 1 upon the next bit 1. Since Z has infinitely many 1's, M will oscillate between 1 and values of at least 2.

3. At the end of Subsection 2.7 we gave an example of an interval-r.e. Lipschitz function f_S that is not differentiable at Ω. For another example, let $P \subseteq [0,1]$ be an effectively closed class such that $v = \min P$ is Martin-Löf random, and define an interval-r.e. function with Lipschitz constant 1 by $f(x) = \lambda([0,x] \setminus P)$; then it is easy to see that the corresponding left-r.e. martingale oscillates on the binary expansion of v, using that v is Borel normal.

4. The work [1] shows that a randomness notion of a real z slightly stronger than Martin-Löf's, called by the authors "Oberwolfach randomness", suffices to ensure that each interval-r.e. function (not necessarily Lipschitz) is differentiable at z.

5. A ML-random real z is called density random if each effectively closed class $\mathcal{P} \subseteq [0,1]$ with $z \in \mathcal{P}$ has Lebesgue density 1 at z. Andrews, Cai, Diamondstone, Lempp and Miller in unpublished work (2012) have shown that this randomness notion is equivalent to non-oscillation of left-r.e. martingales (see [13]). Nies [14] has shown that z is density random if and only if all interval-r.e. functions are differentiable at z.

Oberwolfach randomness implies density randomness as shown in [1]. It is unknown whether the converse holds. In our Theorem 3.4 we represented any non-decreasing interval-r.e. Lipschitz function f mapping 0 to 0 as the variation V_g of a computable Lipschitz function. Even though there is no direct connection between differentiability of g and of f at a real z, this result may be helpful in resolving the question.

An interesting question is whether an effective version of Rademacher's theorem holds: can we extend Theorem 4.2 to higher dimensions? This would mean that

> $z \in [0,1]^n$ is computably random $\Leftrightarrow$ each computable Lipschitz function $f\colon [0,1]^n \to \mathbb{R}$ is differentiable at z.

We conjecture that the answer is yes. By work of Galicki, Nies and Turetsky available at [12], weak 2-randomness of z ensures differentiability at z of each computable a.e. differentiable function.

Acknowledgments

This material is based upon work supported by the National Science Foundation of the USA under Grants No. 0652669 and 0901020, the Marsden fund of New Zealand under Grant No. 08-UOA-187, a grant from the John Templeton Foundation, and NUS Grant R252-000-420-112. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation. Part of this work was done while F. Stephan was invited to the University of Auckland in February 2012.

We would like to thank Jason Rute for very helpful comments and corrections, and for providing the argument leading to Theorem 3.5. We would also like to thank the anonymous referees for numerous useful suggestions, and for providing Fact 2.5 and its proof.

References

[1] Laurent Bienvenu, Noam Greenberg, Antonín Kučera, André Nies and Dan Turetsky, *K-triviality, Oberwolfach randomness, and differentiability*, Mathematisches Forschungsinstitut Oberwolfach, Preprint Series, 2012.

[2] Vasco Brattka, Joseph S. Miller and André Nies, *Randomness and differentiability*, `http://arxiv.org/abs/1104.4465`.

[3] Vladimir I. Bogachev, *Measure theory. Vol. I, II*, Springer-Verlag, Berlin, 2007.

[4] Neal L. Carothers, *Real analysis*, Cambridge University Press, 2000.

[5] Osvald Demuth, *The differentiability of constructive functions of weakly bounded variation on pseudo numbers*, Comment. Math. Univ. Carolin. **16** (1975), no. 3, 583–599, Russian.

[6] Rodney Downey and Denis Hirschfeldt, *Algorithmic randomness and complexity*, Springer-Verlag, Berlin, 2010, 855 pages.

[7] Rick Durrett, *Probability: theory and examples*, second ed., Duxbury Press, Belmont, CA, 1996.

[8] Juha Heinonen, *Lectures on Lipschitz analysis*, Rep. Univ. Jyväskylä Dept. Math. Stat. **100** (2005), 1–77, `http://www.math.jyu.fi/research/reports/rep100.pdf`.

[9] Mathieu Hoyrup and Cristóbal Rojas, *Computability of probability measures and Martin-Löf randomness over metric spaces*, Inform. and Comput. **207** (2009), no. 7, 830–847.

[10] Ming Li and Paul Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications.* Third Edition, Springer, 2008.

[11] André Nies, *Computability and randomness*, Oxford Logic Guides, vol. 51, Oxford University Press, Oxford, 2009.

[12] André Nies (editor), *Logic Blog 2011*, University of Auckland, `http://dx.doi.org/2292/19205`.

[13] André Nies (editor), *Logic Blog 2013*, University of Auckland, `http://dl.dropboxusercontent.com/u/370127/Blog/Blog2013.pdf`.

[14] André Nies, *Differentiability of polynomial time computable functions*, to appear in Proceedings of STACS 2014.

[15] N. Pathak. *A computational aspect of the Lebesgue differentiation theorem*, J. Log. Anal. **1** (2009), Paper 9, 15 pp.

[16] Marian B. Pour-El and J. Ian Richards, *Computability in analysis and physics*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1989.

[17] Noopur Pathak, Cristóbal Rojas and Stephen G. Simpson, *Schnorr randomness and the Lebesgue differentiation theorem*, Proc. Amer. Math. Soc. **142** (2014), 335–349.

[18] Frigyes Riesz, *Untersuchungen über Systeme integrierbarer Funktionen*, Mathematische Annalen **69** (1910), 449–407.

[19] Walter Rudin, *Real and complex analysis*, third ed., McGraw-Hill Book Co., New York, 1987.

[20] Jason Rute, *Algorithmic randomness, martingales, and differentiability*, submitted for publication, 2013.

[21] Claus-Peter Schnorr, *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*, Springer-Verlag, Berlin, 1971, Lecture Notes in Mathematics, Vol. 218.

[22] William P. Ziemer, *Weakly differentiable functions*, Springer-Verlag, New York, 1989.

C. Freer, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, 32 Vassar Street, Cambridge, MA 02139

E-mail address: `freer@math.mit.edu`

B. Kjos-Hanssen, Department of Mathematics, University of Hawai'i at Mānoa, 2565 McCarthy Mall, Honolulu, HI 96822

E-mail address: `bjoern@math.hawaii.edu`

A. Nies, Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand

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

F. Stephan, Department of Mathematics, National University of Singapore, Singapore 119076, Republic of Singapore

E-mail address: `fstephan@comp.nus.edu.sg`