# 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 $z$. Furthermore, a real $z$ is Schnorr random if and only if every Lipschitz function with $L_1$-computable derivative is differentiable at $z$. For the implications from left to right we rely on literature results. The converse implications are obtained by novel constructions of computable Lipschitz functions from randomness tests.

## 1. INTRODUCTION

Let $A \subseteq \mathbb{R}^n$. Recall that a function $f : A \to \mathbb{R}^m$ is *Lipschitz* if there is a constant $c$, called a Lipschitz bound, such that for all $x$ and $y$ we have $\|f(x) - f(y)\| \le c \|x - y\|$ (say, $\|\cdot\|$ denotes the Euclidean norm). Lipschitz functions are of fundamental importance in analysis. They appear naturally in various contexts, such as the solvability of differential equations.

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 $f : A \to \mathbb{R}^m$ 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 [Hei05] 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. In recent years, theorems stating well-behavior almost everywhere of functions in certain classes have been studied from the point of view of algorithmic randomness [BMN, PRS, Rut12]; this provides a way of understanding the complexity of exception null sets, and to characterize algorithmic randomness notions via computable analysis. Despite the importance of Lipschitz functions, their algorithmic aspects have not been studied much. 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 $|q_n - q_k| \le 2^{-n}$ 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.

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 $q \in [0,1]$ (even though this is not the original definition of computability for functions defined on $[0,1]$). 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 $x = \sup_n q_n$.

We proceed to 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 $[x,y]$:

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

We have $V(g,[x,y]) + V(g,[y,z]) = V(g,[x,z])$ for $x < y < z$ (see [Bog07, 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 $x \to V(g,[0,x])$. 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 $g$. Each non-decreasing function equals its own variation function, so classically, the functions $V_g$ for Lipschitz functions $g$ are simply the nondecreasing Lipschitz functions. 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. 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 nondecreasing 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 $\sigma$. We proceed via the fact, of interest by 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 $\mu$. 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, [Rud87, 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 Gacs, Hoyrup, Rojas and others (see [HR09]). For instance, is every lower semi-computable measure on $[0,1]^n$ without point masses the variation, in the sense of [Rud87, 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 [BMN, 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, is the analogous fact for computable Lipschitz functions $f$. The implication "$\Rightarrow$" is immediate by [BMN, Thm. 4.1] since $g(x) = f(x) + cx$ is nondecreasing and computable, where $c \in \mathbb{N}$ is a Lipschitz bound for $f$. For (the contraposition of) the implication "$\Leftarrow$", suppose $z$ is not computably random. This means that some computable martingale $M$ succeeds on $z$. We will build a computable Lipschitz function $f$ that is not differentiable at $z$.

We obtain $f$ as the distribution of the measure associated with a computable bounded martingale $B$ that oscillates between two extreme values when processing longer and longer initial segments of the binary expansion of $z$. We build $B$ from $M$. Note that for any string $\sigma$, the value $B(\sigma)$ is the slope of $f$ between the dyadic rationals $0.\sigma, 0.\sigma + 2^{-|\sigma|}$, so $f$ is not differentiable at $z$. The argument in the usual proof of the Doob martingale convergence theorem (see, e.g., [Dur96]) turns oscillation of a martingale into success of another martingale. In a sense, we reverse this argument, turning success into oscillation.

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

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

where $Q$ ranges over $n$-cubes. We say that $z$ is a *weak Lebesgue point* of $g$ if the limit 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 [Rud87, 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 [Rud87, 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 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.

In Subsection 2.5 we will define the $L_p$-computability of a function in $L_1([0,1]^n)$, where $p \geq 1$ is a computable real. For now we note that for $p \leq q$, every $L_q$-computable function is $L_p$-computable. Pathak, Rojas, and Simpson [PRS] and Rute [Rut12] have shown the following effective version of Lebesgue differentiation where the mere existence of the limit is concerned.

**Theorem 1.3.** *Let $z \in [0,1]^n$. Then $z$ is Schnorr random $\Leftrightarrow$ $z$ is a weak Lebesgue point of every $L_1$-computable function.*

As our third main result, in Theorem 5.1 we will provide a stronger form of the implication "$\Leftarrow$" which we proved independently from [PRS]:

> *if $z$ is not Schnorr random, then there is a bounded function $g : [0,1]^n \to \mathbb{R}$ that is $L_p$-computable for each computable real $p \geq 1$, so that $z$ is not a Lebesgue point of $g$.*

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 [BMN, 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 not differentiable at $z$. (This result was already announced by Demuth [Dem75], 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 [BMN, Claim 6.6] is $L_1$-computable.

1.4. **Lipschitz functions and Schnorr randomness.** Since the function $g : [0,1] \to \mathbb{R}$ obtained in Theorem 5.1 is bounded, the function $f$ given by $f(x) = \int_o^x g$ 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 willl give somewhat more technical detail. Also see [Car00, p. 376] for detail on the variation norm.

To 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

### 2.1. **Computability of functions on the unit interval.**

We paraphrase Definition A in Pour-El and Richards [PER89, 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 [BMN, Prop. 2.2].

### 2.2. **Differentiability.**

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

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

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 $\sigma$. We say that $M$ *succeeds* on a sequence of bits $Z$ if $M(Z\upharpoonright_n)$ 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 $\sigma$.

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 $\mu_M$. Thus, $\mu_M$ 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 $\sigma$. Then for each pair of reals $x, y$ such that $0 \le x < y \le 1$ we have*

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

*In particular, $f$ is Lipschitz with constant $c$.*

*Proof.* For the second inequality, given arbitrary $n$, let $i \in \mathbb{N}$ be greatest such that $i2^{-n} \le x$, and let $j \in \mathbb{N}$ be least such that $y \le j2^{-n}$. Then

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

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 $\sigma_i$ has length $k$.

We say that $G \subseteq [0,1]^n$ is $\Sigma^0_1$ 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 $\Sigma^0_1$ 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 $g : [0,1]^n \to \mathbb{R}$ 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 [PER89, 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 [PER89, 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 $\Sigma^0_1$ and $\lambda V$ is a computable real, then the characteristic function $1_V$ is $L_p$-computable, uniformly in a presentation of $V$ and Cauchy names for $\lambda V$ and $p$.*

*Proof.* Given rational $\epsilon > 0$, compute $t$ such that $\lambda(V - V_t) < \epsilon/2$. 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 $\epsilon$ and $p$.) This implies $\|1_V - h\|_p < \epsilon$. □

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 almost equality. The map $g \to \lambda x. \int_0^x g$ 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., [Car00, p. 376] for more detail. Note that the inverse is automatically computable.

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

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

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 [Rie10] 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., [Zie89, 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 2.5.** *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 2.5 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 2.5 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 [Nie09, Ch. 2] or [DH10] or [LV08] 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 $\gamma$ 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 lower semi-continuous (namely, $f_S(x) = f_S(x^-)$) for each $x$. 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 2.6.** *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 $K(z\upharpoonright_n) \le n - c$. 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 [BGK+12] 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 $\Omega$. Simply let the domain of $S$ generate the open set in Cantor space corresponding to $[0, \Omega)$ (i.e., $x < \Omega$ iff $\exists n\, S(x\upharpoonright_n)\downarrow$). Then $f_S$ increases to $\Omega$ in smaller and smaller steps, and it is constant equal to $\Omega$ thereafter. It is easy to check that $f'_S(\Omega)$ fails to exist. [BGK+12] 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, then the function $g$ is necessarily Lipschitz, 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 $\alpha$, $0 \le \alpha \le 1$, 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 $\pm 1$. 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 $\alpha_s$ of the form $i2^{-n}$ with $n < s$. Let

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

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 $\alpha$. (For intuition, note that as $\alpha_s$ approaches $\alpha$, the oscillations become flatter and flatter. To the right of $\alpha$, $g$ is constant.) □

For any $L_1$-computable function $h$, the function $x \mapsto \int_0^x h$ is computable, as shown in [BMN]. They also noticed that the converse fails by an argument involving algorithmic randomness. We provide a rather more concrete counterexample.

**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 $\alpha$ 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 [Bog07, 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 $\sigma$. 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 $\sigma$, 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 $\mu$ on Cantor space is non-atomic (see the discussion after Definition 2.2). This means that for each $X \in 2^\omega$ we have $M(X(0) \dots X(n-1)) = o(2^n)$. By compactness of Cantor space, the function $X \to \mu[0, X]$ is uniformly continuous. So, in fact we have the apparently stronger condition that $M(\sigma) = o(2^{|\sigma|})$ for each string $\sigma$.

**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, $|L(\sigma)| \le M(\sigma)$ for each $\sigma$.*

*Proof.* 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. Furthermore, $M_s(\sigma) \leq M_t(\sigma)$ whenever $s \leq t$.

Now one defines the new martingale $L$ inductively with $L(\lambda) = 0$. In stage $s$, the idea is to define $L$ on length $\ell_s + 1, \ell_s + 2, \ldots, \ell_{s+1}$ where $\ell_{s+1}$ will be chosen adequately such that for all $\sigma \in \{0,1\}^{\ell_s}$ the difference between $M_s(\sigma)$ and $V_L(\sigma)$ approximated on level $\ell_{s+1}$ is less than $2^{-s}$.

One defines inductively for all strings of length $\ell_s, \ell_s + 1, \ldots$ 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 $a$ such that $M_s(\sigma a) \leq M_s(\sigma(1-a))$ and define $L$ on $\sigma 0$ and $\sigma 1$ as follows:

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

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

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

and

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

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

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

and

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

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

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 $\ell_s+1, \ell_s+2, \ldots, \ell_{s+1}$ at most $2^{\ell_s}$ strings $\sigma$ with $|L(\sigma)| \neq M_s(\sigma)$. As $M(\sigma) = o(2^{|\sigma|})$, there is some level $\ell_{s+1}$ 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 $\sigma$, the difference between $M(\sigma)$ and $V_{L,\sigma_s}(\sigma)$ is for $s \geq \ell_{|\sigma|}$ bounded by $M(\sigma) - M_s(\sigma) + 2^{-s}$. So $V_L(\sigma) = M(\sigma)$ for all strings $\sigma$.

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

**Theorem 3.4.** *Let $f$ be a non-decreasing interval-r.e. Lipschitz function. Then there is a computable Lipschitz function $g$ 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 any 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 $0.\sigma$, $\sigma$ a binary string, we let

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

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

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

Thus $g$ is Lipschitz on the dyadic rationals. Therefore by the remark after Definition 2.1, $g$ can be extended to a computable Lipschitz function on $[0, 1]$, 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 $\sigma$ 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 $\rho$ have the same length $k \ge |\sigma|$. 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 $\mathsf{cdf}(L)$ is not necessarily computable. 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 $2^{-|\sigma|} \cdot M_s(\sigma) \le 2^{-s}$ for all $|\sigma| \ge k_s$. This is true because $M_s$ has no atoms—hence $2^{-k} \cdot M_s(x \upharpoonright k) \searrow 0$ as $k \to \infty$—and because the space is compact—hence there is such a $k_s$ for all $x$. 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 $\sigma$ such that $j_{s+1} > |\sigma| \geq j_s$ we have $|L(\sigma)| \leq M_s(\sigma)$ by construction. Therefore,

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

Now, it remains to show that $f := \mathsf{cdf}(L)$ is computable. Clearly, $f(0.\sigma)$ is uniformly computable for all $\sigma$. Let $\nu$ be the signed measure associated with $L$, so that $\mathsf{cdf}(\nu) = \mathsf{cdf}(L)$. Also, for each $s$, let $\mu_s$ be the measure associated with $M_s$. The above formula then becomes

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

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

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

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

The claim is equivalent to saying that $|\nu[0.\sigma, a)| \leq 2^{-s}$. 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 $1 \leq i \leq n$, and $\tau_0 = a \restriction j_{s+1}$. Since $|\sigma| = j_s$ and $|\tau_i| = j_{s+1}$, we have

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

Continuing by recursion, we have for each $m$ that

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

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

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

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

## 4. Computable randomness and Lipschitz functions

4.1. **Characterizing computable randomness.** Schnorr [Sch71] 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 its binary expansion is computably random.

In fact, it suffices to require that no rational-valued computable martingale succeeds on the binary expansion of $z$ by a result of [Sch71] (for a recent reference see [Nie09, 7.3.8]). Here computability of the martingale can even be taken in the strong sense that we can compute the rational from the string as a single output. For more background on computable randomness see [Nie09, Ch. 7] or [DH10].

We characterize computable randomness by differentiability of computable Lipschitz functions. This is analogous to Theorem 1.1 due to [BMN], as we discussed 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.* $\Rightarrow$: 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 non-decreasing. Since $g$ is computable, by [BMN, Thm. 4.1], $g'(z)$, and hence $f'(z)$, exists.

$\Leftarrow$: We may assume that $z$ is not a dyadic rational. Suppose a computable martingale $M$ succeeds on the unique binary expansion $Z$ of $z$. 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 will build a computable martingale $B$ with values in $[1,2] \cap \mathbb{Q}$ such that

$$\liminf_i B(Z\restriction_i) = 1 \quad \text{and} \quad \limsup_i B(Z\restriction_i) = 2. \tag{1}$$

For any function $f$, and for $p \le z \le q$, we have

$$\min\{S_f(p,z), S_f(z,q)\} \le S_f(p,q) \le \max\{S_f(p,z), S_f(z,q)\}.$$

For $f = \mathsf{cdf}(B)$ we obtain $\underline{D}f(z) \le 1$ and $\overline{D}f(z) \ge 2$, so $f$ is non-differentiable at $z$. (Note that by Fact 2.3 we also have the converse inequalities $\underline{D}f(z) \ge 1$ and $\overline{D}f(z) \le 2$.)

The *betting factors* of $M$ at a string $\sigma$ are the rationals defined by

$$\gamma_{\sigma k} = M(\sigma k)/M(\sigma) \qquad (k = 0, 1).$$

Note that $0 < \gamma_{\sigma 0}, \gamma_{\sigma 1}$ and $\gamma_{\sigma 0} + \gamma_{\sigma 1} = 2$. We build auxiliary computable martingales $M_0, M_1$ with values in $\mathbb{Q}^+$, and let

$$B(\sigma) = M_0(\sigma) - M_1(\sigma).$$

At each $\sigma$, the martingale $B$ is in one of two possible phases. In the *up phase*, it keeps $M_1$ constant and lets $M_0$ bet with the same betting factors as $M$, until its value $B(\sigma)$ reaches 2 (if this value would exceed 2, it lets $M_0$ bet less in order to ensure the value equals 2). In the *down phase*, $B$ keeps $M_0$ constant and lets $M_1$ bet with the same betting factors as $M$, until the value $B(\sigma)$ reaches 1.

In more detail, the construction of $B$ is as follows. Inductively we show that if $B$ is in the up phase at $\sigma$, then $B(\sigma) < 2$, and if $B$ is in the down phase at $\sigma$ then $B(\sigma) > 1$. At the empty string $\emptyset$, the martingale $B$ is in the up phase. We let $M_0(\emptyset) = 2$ and $M_1(\emptyset) = 1$ so that $B(\emptyset) = 1$. Thus the inductive condition holds at the empty string.

Suppose now that $M_i(\sigma)$ has been defined for $i = 0, 1$.

*Case 1: $B(\sigma)$ is in the up phase.* For $k = 0, 1$, let $M_1(\sigma k) = M_1(\sigma)$. Let

$$r_k = \gamma_{\sigma k} M_0(\sigma) - M_1(\sigma).$$

If $r_0, r_1 < 2$ then let $M_0(\sigma k) = \gamma_{\sigma k} M_0(\sigma)$; 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 $r_k \geq 2$. So we can compute the positive rational $\gamma' \leq \gamma_{\sigma k}$ such that $\gamma' M_0(\sigma) - M_1(\sigma) = 2$. Define $M_0(\sigma k) = \gamma' M_0(\sigma)$ and $M_0(\sigma(1-k)) = (2 - \gamma')M_0(\sigma)$, so that $B(\sigma(1-k)) < 2$. Go into the down phase at $\sigma k$, 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.* This is symmetric with $M_0, M_1$ interchanged. For $k = 0, 1$, let $M_0(\sigma k) = M_0(\sigma)$ and

$$r_k = M_0(\sigma) - \gamma_{\sigma k} M_1(\sigma).$$

If $r_0, r_1 > 1$ then let $M_1(\sigma k) = \gamma_{\sigma k} M_1(\sigma)$; stay in the down phase at both $\sigma 0, \sigma 1$.

Otherwise, there is a unique $k$ such that $r_k \leq 1$. We can compute the positive rational $\gamma' \leq \gamma_{\sigma k}$ such that $M_0(\sigma) - \gamma' M_1(\sigma) = 1$. Define $M_1(\sigma k) = \gamma' M_1(\sigma)$ and $M_1(\sigma(1-k)) = (2 - \gamma')M_1(\sigma)$, so that $B(\sigma(1-k)) > 1$ . Go into up phase at $\sigma k$, but stay in the down phase at $\sigma(1-k)$. Again, the inductive condition is maintained.

By construction, if $M$ succeeds on the binary expansion $Z$ of $z$, then $B$ changes phase infinitely often on strings of the form $Z \upharpoonright_i$. This implies (1) and completes the proof. □

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

5.1. **Schnorr randomness.** We let $\lambda$ denote Lebesgue measure on $[0,1]^n$. Recall that we say $G \subseteq [0,1]^n$ is $\Sigma^0_1$ if $G$ is an effective union of open cubes with rational coordinates. A uniformly $\Sigma^0_1$ sequence $(G_m)_{m \in \mathbb{N}}$ is called *Schnorr test* if $\lambda G_m \leq 2^{-m}$ and $\lambda G_m$ 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 Lebesgue point of each bounded $L_p$ 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.

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

*Proof.* $\Rightarrow$: This is immediate by [PRS, Thm. 1.6]. They show that in fact, $z$ is a Lebesgue point of each $L_1$-computable function, bounded or not.
$\Leftarrow$: This implication is proved by contraposition, and will be immediate from the following lemma. In fact the same function $g$ works for each $p$.

**Lemma 5.2.** *Suppose $z \in [0,1]^n$ is not Schnorr random. Then there is a bounded function $g\colon [0,1]^n \to \mathbb{R}$ that is $L_p$-computable for each computable real $p \geq 1$, and a sequence of dyadic cubes $C_m \downarrow z$ such that*

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

*Proof of Lemma.* Recall that $\mathcal{Q}$ denotes the subset of $[0,1]^n$ consisting of the vectors with a dyadic rational component. Clearly the lemma holds for $z \in \mathcal{Q}$, so we may assume that $z \notin \mathcal{Q}$. In the following all assertions of inclusions 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 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 $\lambda G_m$ are uniformly computable.

**Claim 5.3.** *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 5.4.** *$\lambda(G_m)$ is a computable real uniformly in $m$.*

Note that $\lambda(G_0) = 1$. Inductively suppose we have a procedure to compute the real $\lambda G_m$. 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 $\lambda(G_m - G_{m,s}) < \epsilon$. 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 5.5.** *The function $g$ defined in (2) is $L_p$-computable.*

By Claim 5.4 and Fact 2.4, the function $1_{G_i}$ is $L_p$-computable uniformly in $i$. Thus, the function $h_k = \sum_{i=0}^{m} (-1)^i 1_{G_i}$ is also $L_p$-computable uniformly in $m$. It now suffices to show that given a rational $\epsilon > 0$, we can compute $k$ such that the $p$-norm of the rest sum is less than $\epsilon$.

Replacing $p$ by $\lceil p \rceil$ we may suppose that $p \in \mathbb{N}$. For each $r \in \mathbb{N}$ we have

$$\left\| \sum_{m=rp}^{\infty} (-1)^m 1_{G_m} \right\|_p \leq \sum_{m=rp}^{\infty} \|1_{G_m}\|_p \leq \sum_{m=rp}^{\infty} (\lambda G_m)^{1/p} \leq p 2^{-r+1}.$$

This shows the claim.

**Claim 5.6.** *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

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

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, the lemma, and the theorem. □

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 5.7.** *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) apply Lemma 5.2 and the same isometry, noting that the image of a bounded function is Lipschitz. □

## 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 analog 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 $\alpha$, and infinitely many where the value is greater than $\beta$. We make some points regarding the connection of 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 [BMN, Section 4], the nondecreasing Lipschitz function $f_0(x) = x \sin(2\pi \log_2 |x|) + 2x$ satisfies $f(x) = 2x$ for each $x$ of the form $\pm 2^{-n}$, but $1 = \underline{D}f(0) < \overline{D}f(0) = 3$. Let $f$ be 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 $\Omega$. 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 [BGK$^+$12] 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 $z$. The proof uses some of the combinatorics in [BMN, Lemma 4.2] to pass from arbitrary intervals around $z$ to affine transformations of basic dyadic intervals. It is unknown at present whether Oberwolfach randomness is the same as Martin-Löf randomness together with being Turing incomplete. It is also unknown which algorithmic randomness notion correspond to differentiability of interval-r.e. Lipschitz functions, and which notion, possibly weaker, corresponds to non-oscillation of left-r.e. martingales. 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 these questions.

A major remaining 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 Nies and Turetsky available at [Nie11], 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.

## References

[BGK+12] Laurent Bienvenu, Noam Greenberg, Antonín Kučera, André Nies and Dan Turetsky, *K-triviality, Oberwolfach randomness, and differentiability*, Mathematisches Forschungsinstitut Oberwolfach, Preprint Series, 2012.

[BMN] Vasco Brattka, Joseph S. Miller and André Nies, *Randomness and differentiability*, submitted 2011.

[Bog07] Vladimir I. Bogachev, *Measure theory. Vol. I, II*, Springer-Verlag, Berlin, 2007.

[Car00] Neal L. Carothers, *Real analysis*, Cambridge University Press, 2000.

[Dem75] 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.

[DH10] Rodney Downey and Denis Hirschfeldt, *Algorithmic randomness and complexity*, Springer-Verlag, Berlin, 2010, 855 pages.

[Dur96] Rick Durrett, *Probability: theory and examples*, second ed., Duxbury Press, Belmont, CA, 1996.

[Hei05] 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.

[HR09] 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.

[LV08] Ming Li and Paul Vitányi. *An Introduction to Kolmogorov Complexity and Its Applications.* Third Edition, Springer, 2008.

[Nie09] André Nies, *Computability and randomness*, Oxford Logic Guides, vol. 51, Oxford University Press, Oxford, 2009.

[Nie11] André Nies (editor), *Logic Blog 2011*, University of Auckland, http://dx.doi.org/2292/19205.

[PER89] Marian B. Pour-El and J. Ian Richards, *Computability in analysis and physics*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1989.

[PRS] Noopur Pathak, Cristóbal Rojas and Stephen G. Simpson, *Schnorr randomness and the Lebesgue Differentiation Theorem*, Proceedings of the American Mathematical Society, accepted 17 February 2012 for publication.

[Rie10] Frigyes Riesz, *Untersuchungen über Systeme integrierbarer Funktionen*, Mathematische Annalen **69** (1910), 449–407.

[Rud87] Walter Rudin, *Real and complex analysis*, third ed., McGraw-Hill Book Co., New York, 1987.

[Rut12] Jason Rute, *Algorithmic randomness, martingales, and differentiability I*, In preparation, 2012.

[Sch71] Claus-Peter Schnorr, *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*, Springer-Verlag, Berlin, 1971, Lecture Notes in Mathematics, Vol. 218.

[Zie89] 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