Polynomial-Time Rademacher Theorem, Porosity and Randomness

Alex Galicki

The University of Auckland, Auckland, New Zealand
agal629@aucklanduni.ac.nz

Abstract

The main result of this paper is a polynomial time version of Rademacher's theorem. We show that if $z \in \mathbb{R}^n$ is p-random, then every polynomial time computable Lipschitz function $f : \mathbb{R}^n \to \mathbb{R}$ is differentiable at z. This is a generalization of the main result of [19].

To prove our main result, we introduce and study a new notion, p-porosity, and prove several results of independent interest. In particular, we characterize p-porosity in terms of polynomial time computable martingales and we show that p-randomness in $\mathbb{R}^n$ is invariant under polynomial time computable linear isometries.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases Rademacher, porosity, p-randomness, differentiability

Digital Object Identifier 10.4230/LIPIcs.ICALP.2017.30

1 Introduction

The topic of interactions between algorithmic randomness [11, 18] and computable analysis [17, 27] has been extensively studied in the recent years. The general idea is that classical theorems about properties holding almost everywhere in $\mathbb{R}^n$ have effective variants formulated in terms of algorithmic randomness. Differentiability of well-behaved functions is a sub-area that attracted particular interest of researchers (see [8, 13]). Most of results in this area are concerned with computable real functions of one variable. Less is known about functions of several variables (however, see [20, 15, 14]) and still less is known about differentiability and randomness in resource bounded settings [19].

The randomness notion this paper is concerned about is *p-randomness*, first studied by Wang [26]. It is usually defined in terms of polynomial time computable betting strategies.

In [19], Nies characterized p-randomness in terms of differentiability of polynomial time computable real-valued monotone functions of one variable. He showed that $z \in [0, 1]$ is p-random if and only if every polynomial time computable monotone function $f : [0, 1] \to \mathbb{R}$ is differentiable at z. Note that if $f : \mathbb{R} \to \mathbb{R}$ is a $K-$Lipschitz function, then $x \to f(x) + Kx$ is a monotone function. Hence the $\Rightarrow$ direction of this result also shows that polynomial time computable Lipschitz functions are differentiable at p-random reals.

The following classical result by Hans Rademacher [23] shows that Lipschitz real valued functions on $\mathbb{R}^n$ are almost everywhere differentiable.

▶ **Theorem 1** (Rademacher, 1919). *If $f : \mathbb{R}^n \to \mathbb{R}$ is Lipschitz, then it is differentiable at almost every $x \in \mathbb{R}^n$ (with respect to the Lebesgue measure).*

In this paper we prove the following polynomial time version of Rademacher's theorem:

▶ **Theorem 2** (Polynomial time Rademacher). *If $f : \mathbb{R}^n \to \mathbb{R}$ is Lipschitz and polynomial time computable, then it is differentiable at every p-random $x \in \mathbb{R}^n$.*

44th International Colloquium on Automata, Languages, and Programming (ICALP 2017).
Editors: Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl;
Article No. 30; pp. 30:1–30:13

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The notion of porosity, which originated in works of Denjoy, is crucial for this paper. Informally, x is a porosity point of $S \subseteq \mathbb{R}^n$ if it is possible to find relatively large balls disjoint from S (called *holes in* S) arbitrarily close to x. Most proofs of Rademacher's theorem, as well as our proof of the Theorem 1, have two distinct steps:

- The "one-dimensional" step, showing that directional derivatives (of a given Lipschitz function $f : \mathbb{R}^n \to \mathbb{R}$) exist almost everywhere. This part can be seen as concerned with differentiability of real functions of one variable.
- The step which shows that the set of points where the full derivative does not exist despite existence of some of the directional derivatives is negligible too.

Porosity can be observed and exploited in both steps. For real functions of one variable, porosity appears in sets where different types of derivatives disagree (see [9, 25] and [1]). In a polynomial time setting this phenomenon has been exploited by Nies in [19]. In the second step porosity appears in sets witnessing failures of linearity of directional derivatives (that is, when the directional derivative at a point as a function of direction is not a linear function). This particular phenomenon has been observed and studied for functions exhibiting Lipschitz-like regularity (for example, see [22] and [7]).

Since our main goal is to prove a polynomial-time version of Rademacher's theorem, we need a polynomial-time version of porosity. In the Section 3 we define a suitable notion, which we call *p-porosity*. It is worth mentioning that at least one effective version of porosity and its connections to algorithmic randomness has been studied before (see [6, 16]). We will briefly explain the difference between this notion of porosity and ours later in the paper.

The paper is structured as follows: in the Section 2 we review the relevant basic notions and define the notation used in the paper. In the Section 3 we define and study the notion of p-porosity. In the Section 4 we outline the proof of the Theorem 2.

2 Preliminaries and notation

In this paper we often have to go back and forth between the Cantor space and $\mathbb{R}^n$. Mostly, we use the standard notation (for notation related to the Cantor space and strings of finite length, please consult [18]). However, for the sake of readability and expressiveness, we will introduce some custom notation which is described below.

2.1 Dyadic cubes in $\mathbb{R}^n$, 1/3-shift trick

Let $\mathcal{D}^n$ denote the collection of half-open basic dyadic cubes in $\mathbb{R}^n$. That is

$$\mathcal{D}^n = \left\{2^{-k}([m_1, m_1+1) \times \cdots \times [m_n, m_n+1)) : \ k \in \mathbb{Z},\ m_1, \ldots, m_n \in \mathbb{Z}\right\}.$$

For $k \in \mathbb{Z}$, let $\mathcal{D}^n(k)$ denote the collection of basic dyadic cubes in $\mathbb{R}^n$ with its side length equal to 2^{-k}. If $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ is a linear isometry, let $\mathcal{D}_\Omega$ denote the set of images of elements of $\mathcal{D}^n$ under Ω. Analogously, let $\mathcal{D}_\Omega(k)$ be the collection of images of elements of $\mathcal{D}^n(k)$ under Ω. For $x \in \mathbb{R}^n$ and $i \in \mathbb{N}$, define $\mathcal{D}^n(x, i)$ (respectively, $\mathcal{D}_\Omega(x, i)$) to be the unique element of $\mathcal{D}^n(i)$ (respectively, $D_\Omega(i)$) containing x.

By $B(x, r)$ we denote the open ball in $\mathbb{R}^n$ with radius r and centered at x. The following proposition is known as the "$1/3-$shift trick" in $\mathbb{R}^n$.

▶ **Proposition 3** (cf. Theorem 3.8 in [24]). *For any ball $B = B(x, r) \subset \mathbb{R}^n$, there exists $k \in \mathbb{Z}$, $Q \in \mathcal{D}^n(k)$ and $t \in \{0, 1/3, 2/3\}^n$ such that $B \subset (Q + t)$ and $6r < 2^{-k} \leq 12r$.*

2.2 Binary expansion of elements in $\mathbb{R}^n$

Each real number $r \in [0,1)$ can be written in the form $r = \sum_{i\geq 0} r_i 2^{-i-1}$ where $r_i \in \{0,1\}$. We say $r_0 r_1 ...$ is the binary expansion of r. The binary expansion of r is unique unless r is a dyadic rational.

Let $x \in \mathbb{R}^n$. For every $1 \leq i \leq n$, let X_i denote the binary expansion of x_i, the $i-$th component of x. Then $X \in 2^\omega$ is the binary expansion of x if for all $1 \leq i \leq n$ and all j, $X(nj+i-1) = X_i(j)$.

Fix a positive $m \in \mathbb{N}$. Let $A \in 2^\omega$. We denote by $0._m A$ an element of $\mathbb{R}^m$, whose binary expansion is A. We omit the m subscript, when it is clear from the context.

Let $\sigma \in 2^{<\omega}$ with $|\sigma| = nk + m$ for some natural numbers n, k, m with $n > 0$ and $m < n$. Define $\{\sigma\}_n$ by $\{\sigma\}_n = \sigma\restriction_{nk}$. By $[\sigma]_n$ we denote the basic (open) dyadic cube (in $\mathbb{R}^n$) corresponding to $\{\sigma\}_n$.

2.3 Polynomial time computability and p-randomness

Intuitively, a function $f : \mathbb{R}^n \to \mathbb{R}$ is computable in polynomial time if for any $s \in \mathbb{N}$ and $x \in \mathbb{R}^n$, we can compute, uniformly in s and x, an approximate value e to $f(x)$ within an error 2^{-s} in time $O(s^k)$ for some constant k. For the rigorous definition, please see the Section 2.5 in [17]. This approach is equivalent to the one used in [19].

A *martingale* is a function $M\colon 2^{<\omega} \to \mathbb{R}_0^+$ such that $2M(\sigma) = M(\sigma 0) + M(\sigma 1)$ for all $\sigma \in 2^{<\omega}$. This notion of martingales is meant to formalize the intuitive notion of a betting strategy:

- $M(\sigma)$ represents the capital available after betting on bits of σ, which is always positive,
- betting the amount $\alpha \leq M(\sigma)$ on the next bit being 0, will result in losing α in the case when the next bit is 1 ($M(\sigma 1) = M(\sigma) - \alpha$) and winning α otherwise ($M(\sigma 0) = M(\sigma) + \alpha$).

We say that M *succeeds* on Z if $\limsup_n M(Z\restriction_n) = \infty$. For more details, please see [18].

▶ **Definition 4.** A martingale M is called *polynomial time computable* if from a string σ and $i \in \mathbb{N}$ we can in time polynomial in $|\sigma| + i$ compute an approximate value $(M(\sigma))_i$ to $M(\sigma)$ with $|M(\sigma) - (M(\sigma))_i| \leq 2^{-i}$.

▶ **Definition 5.** We say that $Z \in 2^\omega$ is *p-random* if no polynomial time martingale succeeds on Z. An element of $\mathbb{R}^n$ is said to be p-random if its binary expansion is p-random.

p-randomness is a polynomial time variant of *computable randomness* (see [18]). Computable randomness is usually defined in terms of succeeding of computable martingales. However, it is known that in the context of computable randomness, succeeding can be replaced with *divergence*. That is, $Z \in 2^\omega$ is not computably random iff there exists a computable martingale M with $\liminf_i M(Z\restriction_i) < \limsup_i M(Z\restriction_i)$. An analogous result holds for p-randomness and a somewhat stronger proposition will be shown later in this paper.

2.4 Martingales-measures correspondence and derivatives

We denote the Lebesgue measure (both on $\mathbb{R}^n$ and on 2^ω) by λ. By $\mathcal{M}_\lambda$ we denote the class of measures μ on $\mathbb{R}^n$ for which $\mu(A) \leq k \cdot \lambda(A)$ holds for some k and all Borel A.

Most of martingales considered in this paper are bounded. We will use repeatedly the following correspondence between measures from $\mathcal{M}_\lambda$ and bounded martingales.

▶ **Definition 6.** Let M be a martingale bounded from above. For all $\sigma \in 2^{<\omega}$ define

$$\mu_0([\sigma]_n) = M(\{\sigma\}_n)\lambda([\sigma]_n).$$

This defines a pre-measure on $[0,1]^n$. We can extend μ_0 to a measure $\mu \in \mathcal{M}_\lambda$ on $\mathbb{R}^n$ supported on a subset of the unit cube. We say μ is *a corresponding (to M) measure.*

For the other direction, let $\mu \in \mathcal{M}_\lambda$. We define *the corresponding (to μ) martingale M* by setting

$$M(\sigma) = \frac{\mu([\sigma]_n)}{\lambda([\sigma]_n)}.$$

Clearly, M is a bounded martingale.

▶ **Notation 7.** *Let μ be a measure on $\mathbb{R}^n$. Let $x \in \mathbb{R}^n$ and let $i \in \mathbb{N}$. Define*

$$\frac{\partial_2 \mu}{\partial_2 \lambda}(x,i) = \frac{\mu(\mathcal{D}^n(x,i))}{\lambda(\mathcal{D}^n(x,i))}$$

and

$$\frac{\partial_2 \mu}{\partial_2 \lambda}(x) = \lim_{i \to +\infty} \frac{\partial_2 \mu}{\partial_2 \lambda}(x,i).$$

If $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ is a linear isometry, we define

$$\frac{\partial_\Omega \mu}{\partial_\Omega \lambda}(x,i) = \frac{\mu(\mathcal{D}_\Omega(x,i))}{\lambda(\mathcal{D}_\Omega(x,i))}$$

and

$$\frac{\partial_\Omega \mu}{\partial_\Omega \lambda}(x) = \lim_{i \to +\infty} \frac{\partial_\Omega \mu}{\partial_\Omega \lambda}(x,i).$$

▶ **Notation 8.** *Let $n \geq 1$. By $e_1, \ldots, e_n$ we denote the unit vectors of the standard basis for $\mathbb{R}^n$.*

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a function and let $v, x \in \mathbb{R}^n$. By $D_1 f(x), \ldots, D_n f(x)$ we denote the partial derivatives of f. We denote the directional derivative (in the direction of v) of f at x by $D_v f(x)$.

3 p-porosity

Let (X,d) be a metric space. $x \in X$ is said to be a *porosity point* of $S \subseteq X$ if

$$\mathbf{por}(x,S) = \limsup_{r \to 0} \gamma(x,r,S)/r > 0,$$

where $\gamma(x,r,S)$ is defined for any $r > 0$ as

$$\sup\{r' > 0 : \quad \text{for some } z \in X,\ B(z,r') \subseteq B(x,r) \text{ and } B(z,r') \cap S = \emptyset\}.$$

A set S is said to be *porous* if all its points are porosity points of S. A set is said to be *$\sigma-$porous* if it is a countable union of porous sets.

The following definitions are meant to formalize an efficient version of the above notion of porosity.

▶ **Definition 9.** Let C be a subset of 2^ω and let $Z \in C$. Define

$$\mathbf{por}_2(Z, C) = \liminf_{i\to\infty}\{|\sigma| - i \ : \ \sigma \succ Z\restriction_i \wedge \ [\sigma] \cap C = \emptyset\}.$$

If $\mathbf{por}_2(Z, C) < \infty$, then we say that Z is a *dyadic porosity point of* C.

Since we are interested in polynomial time computable betting strategies, we need to restrict our attention to subsets of 2^ω for which finding holes can be done in polynomial time.

▶ **Definition 10.** Let $A \subseteq 2^\omega$ be a Σ^0_1 set. We say A is *polynomial time computable* if there is a function $p : 2^{<\omega} \to \{0, 1\}$ computable in polynomial time such that $p(\sigma) = 1 \iff [\sigma] \subset A$ for all σ. Let $B \subseteq 2^\omega$ be a Π^0_1 set. We say it is polynomial time computable in if its complement is polynomial time computable.

▶ **Definition 11.** Let $X \in 2^\omega$. We say X is a *polynomial time porosity point (p-porosity point)* if there exists a polynomial time computable Π^0_1 set $A \subseteq 2^\omega$ such that X is a dyadic porosity point of A. If $C \subseteq A$ and $X \in C$, we say X is a p-porosity point of C.

We say $X \in 2^\omega$ is a *p-nonporosity point* if it is not a p-porosity point.

To show that $Z \in 2^\omega$ is a p-porosity point, it is sufficient to describe a polynomial-time algorithm for locating holes in some $S \subset 2^\omega$ arbitrarily close to Z. That is, to exhibit a function $p : 2^{<\omega} \to \{0, 1\}$ computable in polynomial time, such that

1. $p(\sigma) = 1 \iff [\sigma] \cap S = \emptyset$ and
2. Z is a dyadic porosity point of the complement of $\bigcup_{p(\sigma)=1}[\sigma]$.

▶ Remark. While our definitions admit straightforward generalizations to $\mathbb{R}^n$, for the sake of simplicity, we have defined our notion of p-porosity in terms of the Cantor space.

▶ Remark. As was mentioned in the introduction, one other effective version of porosity has been studied in the context of algorithmic randomness [6, 16]. $X \in 2^\omega$ is said to be a *porosity point* if there exists a Π^0_1 set $S \subseteq 2^\omega$ such that X is a dyadic porosity point of S. The main difference between this notion and p-porosity is that the latter requires a polynomial time algorithm for finding holes, while holes in a Π^0_1 set in general can only be enumerated.

3.1 p-porosity and polynomial time computable martingales

Since out main result, Theorem 2, is concerned with p-randomness, and we plan to use the notion of p-porosity extensively in the proof of it, we need to characterize the notion of p-porosity in terms of success sets of polynomial time computable martingales. This subsection is devoted to this task.

▶ Remark. A closely related notion, *p-genericity*, has been studied extensively (see [3], [2]). $Z \in 2^\omega$ is said to be *p-generic* if it does not belong to the boundary of any polynomial time computable Σ^0_1 subset of 2^ω. Since every p-porosity point belongs to the boundary of some polynomial time computable Σ^0_1 set, p-genericy implies p-nonporosity. Moreover, it is known that p-randomness implies p-genericity (see [4]). Hence, p-randomness implies p-nonporosity.

▶ **Definition 12.** Let μ be a measure on $\mathbb{R}^n$ and let $\epsilon > 0$. We say $x \in \mathbb{R}^n$ is *an $\epsilon-$oscillation point of μ* if for infinitely many $i \in \mathbb{N}$,

$$\left|\frac{\partial_2\mu}{\partial_2\lambda}(x, i) - \frac{\partial_2\mu}{\partial_2\lambda}(x, i + 1)\right| \geq \epsilon.$$

We say $x \in \mathbb{R}^n$ is *an oscillation point of μ* if x is an $\epsilon-$oscillation point of μ for some $\epsilon > 0$.

Analogously, we say $X \in 2^\omega$ is *an $\epsilon-$oscillation point of a martingale M* if for infinitely many $i \in \mathbb{N}$,

$$|M(X\restriction_i) - M(X\restriction_{i+1})| \geq \epsilon.$$

Let M be a martingale and let $\epsilon > 0$. By $\mathbf{Osc}(M, \epsilon)$ we denote the set of $\epsilon-$oscillation points of M. Finally, we let

$$\mathbf{Osc}(M) = \bigcup_{\epsilon > 0} \mathbf{Osc}(M, \epsilon).$$

▶ **Definition 13.** For $A, B \subseteq \mathbb{R}^n$ we say A and B are *$\epsilon-$separated by μ* if

$$\left| \frac{\mu(A)}{\lambda(A)} - \frac{\mu(B)}{\lambda(B)} \right| \geq \epsilon.$$

The following proposition provides a characterization of p-randomness in terms of $\epsilon-$oscillation points of polynomial time computable martingales.

▶ **Proposition 14.** *Let $Z \in 2^\omega$. The following are equivalent:*
1. *Z is p-random and*
2. *$Z \notin \boldsymbol{Osc}(M)$ for every bounded from above polynomial time computable martingale M.*

Proof Sketch. The (1) $\Rightarrow$ (2) direction is a polynomial time version of the Doob martingale convergence theorem. A straightforward adaptation of the proof of Theorem 7.1.3 from [10] suffices.

For the (2) $\Rightarrow$ (1) direction, suppose M is a polynomial time computable martingale succeeding on $Z \in 2^\omega$. We may assume M has the *saving property*, that is $M(\sigma\nu) \geq M(\sigma) - 1$ and $M(\sigma) > 1$ for all $\sigma, \nu \in 2^{<\omega}$. (See the proof of the Proposition 5.3.8 in [10])

Our proof is a suitable modification of the construction found in the proof of Theorem 4.2 from [13]. There, given a computable martingale M with the saving property, succeeding on Z, authors construct a computable martingale B that diverges on Z and for all $\sigma \in 2^{<\omega}$, $1 \leq B(\sigma) \leq 4$. It is easy to verify, that when M is polynomial time computable, B is polynomial time computable too. The construction turns the success of M into oscillations of B. It does so by having B alternating between two "phases": in the *up phase* B adds the capital that M risks, until $B(\sigma)$ reaches 3, while in the *down phase*, B subtracts the capital that M risks, until $B(\sigma)$ reaches 2. The required modification is following: the last bet of every up phase is a $1/4-$bet. It can be verified that for all $\sigma \in 2^{<\omega}$, $1 - 1/4 \leq B(\sigma) \leq 4 + 1/4$ and $Z \in \mathbf{Osc}(B, 1/4)$. ◀

▶ **Definition 15.** Let M be a martingale. We define $\mathcal{E}_{\geq}(M)$ to be the set of those X such that M does not make any losses while betting on X. More formally,

$$\mathcal{E}_{\geq}(M) = \{Z \ : \ \forall_i \ M(Z\restriction_{i+1}) \geq M(Z\restriction_i)\}.$$

The following proposition provides a characterization of p-porosity points in terms of martingales: p-porosity points are precisely those X for which there exists a martingale computable in polynomial time that succeeds on X without making any losses and places infinitely many ϵ-bets in the process.

▶ **Proposition 16.** *Let $Z \in 2^\omega$. The following two are equivalent:*
1. *Z is a p-porosity point, and*
2. *$Z \in \boldsymbol{Osc}(M) \cap \mathcal{E}_{\geq}(M)$ for some computable in polynomial time martingale M.*

Proof 1 ⇒ 2. Let A be a polynomial time computable Σ^0_1 set and let $p : 2^{<\omega} \to \{0,1\}$ be as in the Definition 10. Suppose Z is a dyadic porosity point of $2^\omega \setminus A$. Let $s = \mathbf{por}_2(Z, 2^\omega \setminus A)$. We define a martingale M in the following way. Let $M(\emptyset) = 1$ (by $\emptyset$ we denote the empty string). For all strings $\sigma \in 2^{<\omega}$ with $l = |\sigma| = k(s+1)$ for some $k > 1$, we let $M(\sigma) = M(\sigma\restriction_{l-1})$. Suppose $M(\sigma)$ has been defined, where $l = |\sigma| = k(s+1)$. If there is a string $\tau \succ \sigma$ of length $l+s$ such that $p(\tau) = 1$, then let $M(\tau) = 0$ and let $M(\sigma_1) = M(\sigma)\frac{2^s}{2^s-1}$ for all $\sigma_1 \succ \sigma$ with $\sigma_1 \neq \tau$ and $|\sigma_1| = s + l$. Otherwise, if such string τ does not exist, let $M(\sigma_1) = M(\sigma)$ for all $\sigma_1 \succ \sigma$ with $|\sigma_1| < (k+1)(s+1)$. M is clearly computable in polynomial time. Since Z is a dyadic porosity point of $2^\omega \setminus A$, for infinitely many i, we have

$$M(Z\restriction_{i+s}) - M(Z\restriction_i) \geq \frac{1}{2^s - 1}.$$

It follows that $Z \in \mathbf{Osc}\left(M, \frac{1}{s(2^s-1)}\right) \cap \mathcal{E}_{\geq}(M)$. ◀

Proof 2 ⇒ 1. Suppose $Z \in \mathbf{Osc}(M, \epsilon) \cap \mathcal{E}_{\geq}(M)$, where M is a computable in polynomial time martingale and $\epsilon > 0$. Let $s \in \mathbb{N}$ be such that $\epsilon > 2^{-s}$. For every $\sigma \in 2^{<\omega}$ with $\sigma \neq \emptyset$, let $\overline{\sigma}$ denote the string obtained from σ by flipping the last bit.

Define $p : 2^{<\omega} \to \{0,1\}$ by letting

- $p(\emptyset) = 0$ and
- for all $\sigma \neq \emptyset$, if $\left(M(\sigma) - M(\sigma\restriction_{|\sigma|-1})\right)_s > 0$, then $p(\overline{\sigma}) = 1$. Otherwise, let $p(\overline{\sigma}) = 0$.

Since $\left(M(\sigma) - M(\sigma\restriction_{|\sigma|-1})\right)_s > 0$ is decidable in polynomial time, p is computable in polynomial time too. Hence the set $A = 2^\omega \setminus \bigcup_{p(\sigma)=1}[\sigma]$ is polynomial time computable. For infinitely many i, we have $M(Z\restriction_{i+1}) - M(Z\restriction_i) > 2^{-s}$ and hence $p\left(\overline{Z\restriction_{i+1}}\right) = 1$. It follows that Z is a dyadic porosity point of A. ◀

4 Polynomial-time Rademacher's theorem

4.1 Overview of the proof

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a Lipschitz function. Let us denote by $N(f)$ the set of points where f is not differentiable. Classical Rademacher's theorem asserts that it is a Lebesgue nullset. This can be proven in two steps.

1. Firstly, fix a countable set of unit vectors $V \subset \mathbb{R}^n$. Let $N(V, f) \subset \mathbb{R}^n$ denote the set where $D_v f(x)$ does not exist for at least one $v \in V$. A.e. differentiability of real-valued Lipschitz functions of one variable in conjunction with Fubini's theorem implies that this set is a Lebesgue nullset.
2. Secondly, consider the set $N(f) \setminus N(V, f)$. It can be proven that this set is $\sigma-$porous provided V is not empty (for example, see Theorem 3.1 in [5] and Theorem 2 in [21]). This concludes the proof, since $\sigma-$porous sets are Lebesgue nullsets.

Our proof of Theorem 2 follows a similar path. Firstly, let V_p be the set of polynomial time computable unit vectors in $\mathbb{R}^n$. Suppose $f : \mathbb{R}^n \to \mathbb{R}$ is a polynomial time computable Lipschitz function. We need to show that $N(f)$ contains no p-random elements. Just like in the classical case outlined above, we show this by splitting $N(f)$ in two parts - $N(f) \setminus N(V_p, f)$ and $N(V_p, f)$ - and then showing that neither of them contains a p-random element.

The proof has three nontrivial and relatively self-contained parts:

- Firstly, we show a result of independent interest. In the subsection 4.2 we prove that p-randomness in $\mathbb{R}^n$ is invariant under linear isometries computable in polynomial time.

It is worth mentioning that the one-dimensional version of this result follows from results in [12]. Higher dimensional result in this paper, requires, however, quite a different approach.

- Then, we show that p-randomness of z is sufficient for existence of partial derivatives of f at z. This is an adaptation of the one-dimensional proof from [19]. Existence of directional derivatives $D_v f(z)$ where $v \in V_p$ follows the preservation property mentioned in the previous point. This concludes the proof that $N(V_p, f)$ contains no p-random elements.
- Finally, we demonstrate that $N(f) \setminus N(V_p, f)$ contain no p-random points. This is accomplished by a careful analysis of structural properties of $N(f) \setminus N(V_p, f)$ and showing that binary expansions of elements of this set are p-porosity points.

Due to size limitations, this paper contains the full proof of the first part only (bar the proof of the technical lemma from the Section 4.2.2).

4.2 Invariance of p-randomness under linear isometries computable in polynomial time

In this subsection we will use the following notational convention.

▶ **Notation 17.** *Let μ be a measure on $\mathbb{R}^n$, and let $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ be a linear isometry. By μ_Ω we denote the measure defined by $\mu_\Omega(A) = \mu(\Omega(A))$ for all Borel A.*

If M is a martingale corresponding to μ, by M_Ω we denote the martingale corresponding to μ_Ω.

The main result of this subsection is that p-randomness is invariant under polynomial time computable linear isometries. Let us examine how an analogous result can be shown for computable randomness. Suppose $z \in \mathbb{R}^n$ be not computably random and let $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ be a computable linear isometry. We want to show that $\Omega^{-1}(z)$ is not computably random. Let M be a bounded computable martingale diverging on Z (where $z = 0.Z$) and let μ be a corresponding measure on $\mathbb{R}^n$. Define $y = \Omega^{-1}(z)$ and let Y be the binary expansion of y. Observe that M_Ω is also a bounded computable martingale. There are two possibilities:
(A) Either M_Ω diverges on Y, in which case Y is not computably random, or
(B) M_Ω converges on Y and then y belongs to the set

$$A = \left\{ x : \ \frac{\partial_2 \mu_\Omega}{\partial_2 \lambda}(x) \text{ exists and } \frac{\partial_\Omega \mu_\Omega}{\partial_\Omega \lambda}(x) \text{ does not exist} \right\}.$$

In this case it is possible to show that y is a porosity point of some subset of A and use this information to conclude that y is not computably random.

A similar argument can be made about p-randomness. However, there are two additional obstacles. Firstly, it is not clear what (additional) conditions on M and Ω ensure that M_Ω is polynomial time computable. Secondly, the porosity mentioned in (B) would have to be replaced with p-porosity. A significant portion of this section is dedicated to address those two problems. The plan is following:

- In the Subsection 4.2.1 we show that $\epsilon-$oscillation points of M_Ω are not p-random, even if it is not known whether M_Ω is computable in polynomial time;
- In the Subsection 4.2.2 we prove a technical lemma related to linear transformations and $\epsilon-$oscillation;
- Finally, in the Subsection 4.2.3 we combine those ideas to prove our main invariance theorem.

4.2.1 Betting on ϵ-oscillation points of M_Ω

▶ **Lemma 18.** *Let $A, B \subseteq \mathbb{R}^n$ be Borel with $A \subseteq B$ and $\lambda(B) > 0$. Let μ be a measure on $\mathbb{R}^n$ such that for some $k \in \mathbb{N}$, $\mu(C) \leq k\lambda(C)$ for all C. Suppose $\frac{\lambda(B\setminus A)}{\lambda(A)} \leq \epsilon$ for some $\epsilon \in \mathbb{R}$. Then*

$$\left|\frac{\mu(B)}{\lambda(B)} - \frac{\mu(A)}{\lambda(A)}\right| \leq 2k \cdot \epsilon.$$

Proof.

$$\begin{aligned}\left|\frac{\mu(B)}{\lambda(B)} - \frac{\mu(A)}{\lambda(A)}\right| &= \left|\frac{\mu(B)\lambda(A) - \mu(B)\lambda(B) + \mu(B\setminus A)\lambda(B)}{\lambda(B)\,\lambda(A)}\right| \\ &= \left|\frac{\mu(B)}{\lambda(B)}\frac{\lambda(B)-\lambda(A)}{\lambda(A)} + \frac{\mu(B\setminus A)}{\lambda(A)}\right| \\ &\leq 2k \cdot \epsilon.\end{aligned}$$

◀

▶ **Lemma 19** (Approximation lemma)**.** *Let M be a computable in polynomial time martingale bounded above by some $k \in \mathbb{N}$. Let μ be a corresponding measure on $\mathbb{R}^n$. Let $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ be a computable in polynomial time linear isometry. Fix $s \in \mathbb{N}$. There exists function $M_{\Omega,s} : 2^{<\omega} \to \mathbb{R}$ computable in polynomial time such that for all σ*

$$|M_{\Omega,s}(\sigma) - M_\Omega(\sigma)| \leq 2^{-s}.$$

Proof. This is a consequence of Lemma 18. For a given σ, we can find in polynomial time a finite collection of dyadic basic cubes $(D(\sigma)_i)_{i\in\mathbb{N}}$ such that

$$\frac{\lambda(\Omega([\sigma]_n) \setminus \bigcup_i D(\sigma)_i)}{\lambda(\bigcup_i D(\sigma)_i)} \leq \frac{2^{-s-1}}{k},$$

so that

$$\left|\frac{\mu(\Omega([\sigma]_n))}{\lambda(\Omega([\sigma]_n))} - \frac{\mu(\bigcup_i D(\sigma)_i)}{\lambda(\bigcup_i D(\sigma)_i)}\right| \leq 2^{-s}.$$

Define $M_{\Omega,s}(\sigma) = \frac{\mu(\bigcup_i D(\sigma)_i)}{\lambda(\bigcup_i D(\sigma)_i)}$. This function is computable in polynomial time and the following holds for every σ:

$$|M_\Omega(\sigma) - M_{\Omega,s}(\sigma)| = \left|\frac{\mu(\Omega([\sigma]_n))}{\lambda(\Omega([\sigma]_n))} - \frac{\mu(\bigcup_i D(\sigma)_i)}{\lambda(\bigcup_i D(\sigma)_i)}\right| \leq 2^{-s}.$$

◀

▶ **Lemma 20.** *Let M be a polynomial time computable martingale bounded above by some $k \in \mathbb{N}$ and let $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ be a polynomial time computable linear isometry. For every $\epsilon > 0$, there exists a polynomial time computable martingale H_ϵ such that every $\epsilon-$oscillation point of M_Ω is an $\epsilon/2-$oscillation point of H_ϵ.*

Proof. Let s be such that $2^{-s+1} < \epsilon$. By Lemma 19, there exists a polynomial time computable function $M_{\Omega,s}$ such that for all σ

$$|M_{\Omega,s}(\sigma) - M_\Omega(\sigma)| \leq 2^{-s}.$$

We define H_ϵ as following. We let $H_\epsilon(\emptyset) = M_{\Omega,s}(\emptyset)$. For any σ, suppose $H_\epsilon(\sigma)$ has been defined. We define $\alpha(\sigma) = H_\epsilon(\sigma) - \frac{1}{2}(M_{\Omega,s}(\sigma 0) + M_{\Omega,s}(\sigma 1))$ and we let

$$H_\epsilon(\sigma 0) = M_{\Omega,s}(\sigma 0) + \alpha(\sigma), \text{ and } H_\epsilon(\sigma 1) = M_{\Omega,s}(\sigma 1) + \alpha(\sigma).$$

It is easy to verify that H_ϵ is a polynomial time computable martingale. Now suppose $|M_\Omega(\sigma) - M_\Omega(\sigma 1)| \geq \epsilon$. We have

$$|H_\epsilon(\sigma) - H_\epsilon(\sigma 1)| = \frac{1}{2}\,|M_{\Omega,s}(\sigma 1) - M_{\Omega,s}(\sigma 0)| \geq \frac{1}{2}(2\epsilon - 2^{-s+1}) > \epsilon/2.$$

The case when $|M_\Omega(\sigma) - M_\Omega(\sigma 0)| \geq \epsilon$ is handled analogously. ◀

4.2.2 A technical lemma

Let M be a martingale computable in polynomial time, bounded from above, and let μ be a corresponding measure on $\mathbb{R}^n$. Suppose $y \in \mathbb{R}^n$ is an $\epsilon-$oscillation point of μ. It can be easily shown that for any $k > 0$ and for infinitely many i, $\mathcal{D}^n(y, i)$ contains two dyadic cubes from $\mathcal{D}^n(i + k)$, that are $\epsilon-$ separated by μ.

Now consider a linear isometry $\Omega : \mathbb{R}^n \to \mathbb{R}^n$. Suppose that for some $k > 0$, $\epsilon > 0$ and for infinitely many i, $D = \mathcal{D}^n(y, i)$ contains two cubes $D_1, D_2 \in \mathcal{D}_\Omega(i + k)$, that are $\epsilon-$separated by μ. In general, this does not imply that y is an oscillation point of μ. However, the following technical lemma shows that if y is not an oscillation point of μ, then it is a p-porosity point.

▶ **Lemma 21.** *Let M be a martingale computable in polynomial time, bounded from above. Let μ be a corresponding measure on $\mathbb{R}^n$. Let $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ be a linear isometry. Let $y \in \mathbb{R}^n$ with $Y \in 2^\omega$ being its binary expansion. Suppose that for some $k > 0$, $\epsilon > 0$ and for infinitely many i, $D = \mathcal{D}^n(y, i)$ contains two cubes $D_1, D_2 \in \mathcal{D}_\Omega(i + k)$, that are $\epsilon-$separated by μ. If y is not an oscillation point of μ, then Y is a p-porosity point.*

4.2.3 Invariance theorems

▶ **Theorem 22.** *Let $z \in [0, 1]^n$ and let $r \in \mathbb{R}$ be a polynomial time computable real. Suppose z is not p-random. Then $z + re_i$ is not p-random for any $1 \leq i \leq n$.*

Proof. Since we are only interested in the question whether $z + re_i$ is p-random or not, we may assume that z and r are such that $z + re_i \in [0, 1]^n$.

Without loss of generality we may assume that every component of z is p-random and $n > 1$ (otherwise, the required result follows from preservation properties proven in [12]). Fix $i \in \mathbb{N}$ with $1 \leq i \leq n$ and define $\Phi, \Omega : \mathbb{R}^n \to \mathbb{R}^n$ by $\Omega(x) = x - re_i$ and $\Phi = \Omega^{-1}$. Let $y = \Phi(z)$. Let Z be the binary expansion of z and let Y be the binary expansion of y. Let M be the polynomial time computable martingale M from the (sketch of the)proof of the Proposition 14 such that Z is an $\epsilon-$oscillation point of M for some $\epsilon > 0$. M makes an infinite number of ϵ bets along Z. However, we need a modified version of M (which we also call M). First, let us introduce some notation. Let μ denote the measure corresponding to M. For every $\sigma \in 2^{<\omega}$ with $[\sigma]_n \in \mathcal{D}(j)$, let $D^1(\sigma), D^2(\sigma) \in \mathcal{D}_\Omega(j)$ be such that $[\sigma]_n \subseteq D^1(\sigma) \cup D^2(\sigma)$. $D^1(\sigma)$ and $D^2(\sigma)$ are not necessarily unique, but that does not matter. Our martingale M, instead of making an ϵ bet, waits until its input σ is such that $\frac{\lambda([\sigma]_n \cap D^1(\sigma))}{\lambda([\sigma]_n)} \geq 1/3$ and $\frac{\lambda([\sigma]_n \cap D^2(\sigma))}{\lambda([\sigma]_n)} \geq 1/3$ (this will occur sooner or later since all components of z are p-random). Once such input σ is found (with $[\sigma]_n \in \mathcal{D}(j)$ for some j), M places two $\epsilon/2$ bets on $\tau_1, \tau_2 \succ \sigma$ such that $[\tau_1]_n, [\tau_2]_n \in \mathcal{D}(j + 2)$, $[\tau_1]_n \subseteq [\sigma]_n \cap D^1(\sigma)$ and $[\tau_2]_n \subseteq [\sigma]_n \cap D^2(\sigma)$.

What is important in this construction is that for infinitely many i, both $D^1(Z{\restriction_i})$ and $D^2(Z{\restriction_i})$ contain two elements of $\mathcal{D}(i + 2)$ that are $\epsilon/2-$separated by μ and either $y \in \Phi(D^1(Z{\restriction_i}))$ or $y \in \Phi(D^2(Z{\restriction_i}))$.

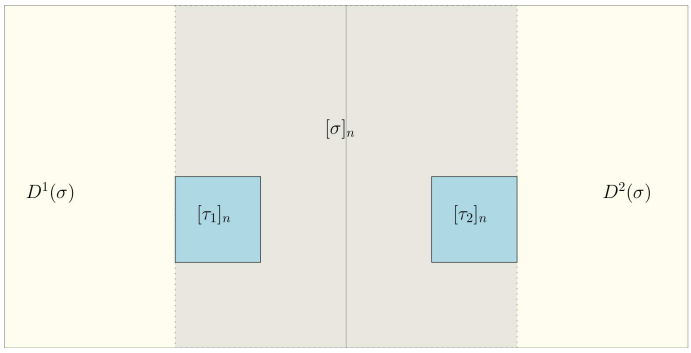

Figure 1 A particular betting pattern employed in the proof of the Theorem 22.

Clearly M is computable in polynomial time and Z is an $\epsilon/2-$oscillation point of M.

Consider the martingale M_Ω. By the Lemma 21, either $Y \in \mathbf{Osc}(M_\Omega)$ or Y is a p-porosity point. In both cases Y is not p-random. ◀

▶ Remark. There is an important implication of the above theorem. In those cases where we are only concerned whether some $x \in \mathbb{R}^n$ is p-random or not, we can always use the 1/3-shift trick freely. That is, since for every i, $x + 1/3e_i$ is p-random iff x is p-random, instead of x we can always consider a suitable shift of x. This will be used below, in the proof of our main result of this subsection.

▶ **Theorem 23.** *Let $\Omega : \mathbb{R}^n \to \mathbb{R}^n$ be a polynomial time computable linear isometry. Let $z \in [0,1]^n$. z is p-random iff $\Omega(z)$ is p-random.*

Proof. Since Ω^{-1} is polynomial time computable linear isometry as well, it is only required to show that if z is not p-random, then $\Omega^{-1}(z)$ is not p-random either. Again, we may assume $\Omega^{-1}(z) \in [0,1]^n$.

Let Z be the binary expansion of z. Let M be a bounded polynomial time computable martingale such that Z is an $\epsilon-$oscillation point of M for some $\epsilon > 0$. Define $\Phi = \Omega^{-1}$, let $y = \Phi(z)$ and let Y be the binary expansion of y.

Consider the martingale M_Ω and its corresponding measure μ_Ω. If y is an oscillation point of μ_Ω, Y is not p-random. Suppose y is not an oscillation point of μ_Ω.

There are infinitely many j, such that $\mathcal{D}_\Phi(j, y)$ and $\mathcal{D}_\Phi(j+1, y)$ are $\epsilon-$separated by μ_Ω. By the 1/3-shift trick and by Theorem 22, we may assume that for infinitely many such j's, $\mathcal{D}_\Phi(j, y)$ is contained in $\mathcal{D}^n(y, j - \hat{p})$ for some fixed $\hat{p}$. In that case, by the Lemma 21, Y is a p-porosity point and hence not p-random. ◀

4.3 Existence of directional derivatives

To prove our main result about directional derivatives, we need the following proposition:

▶ **Proposition 24.** *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a polynomial time computable Lipschitz function. If $z \in \mathbb{R}^n$ is p-random, then $D_n f(z)$ exists.*

▶ Remark. The proof of the above proposition is a generalization of the proof of the $\Rightarrow$ direction of the Theorem 4 in [19]. The most technically challenging part required by the proof is the $\Leftarrow$ part of van Lambalgen's theorem for p-randomness. That is, we had to show that if there is an oracle martingale computable in polynomial time diverging on A while having an oracle access to B, then there is a martingale computable in polynomial time succeeding on $A \oplus_n B$.

▶ **Theorem 25.** *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a Lipschitz function computable in polynomial time. Let $u \in V_p$ and let $x \in \mathbb{R}^n$ be p-random.*

The directional derivative $D_u f(x)$ exists.

Proof. Let $\Theta : \mathbb{R}^n \to \mathbb{R}^n$ be a change of basis map, such that $\Theta(e_1) = u$. We may assume it is computable in polynomial time. Define $z = \Theta^{-1}(x)$. By the Theorem 23, z is p-random too.

Define $g = f \circ \Theta$. g is a Lipschitz function computable in polynomial time. Then $D_u f(x) = D_1 g(z)$ and we know that $D_1 g(z)$ exists. ◀

4.4 Linearity of directional derivatives

Let $f : \mathbb{R}^n \to \mathbb{R}$ be a Lipschitz function computable in polynomial time. Recall that $N(f) \setminus N(V_p, f)$ is the set of points $x \in \mathbb{R}^n$ such that $D_v f(x)$ exists for all unit vectors v computable in polynomial time but f is not differentiable at x.

Let $u, v \in \mathbb{R}^n$. Define $D(f, u, v) \subseteq \mathbb{R}^n$ as the set of such x that $D_u f(x), D_v f(x)$ and $D_{u+v} f(x)$ exist, but

$$D_u f(x) + D_v f(x) \neq D_{u+v} f(x).$$

Since f is Lipschitz and V_p is dense in the set of unit vectors, it is known that

$$N(f) \setminus N(V_p, f) = \bigcup_{u,v \in V_p} D(f, u, v).$$

The following proposition is the last bit required to prove the Theorem 2:

▶ **Proposition 26.** *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a Lipschitz function computable in polynomial time. Let $x \in \mathbb{R}^n$ with $X \in 2^\omega$ being its binary expansion. If $x \in N(f) \setminus N(V_p, f)$, then X is a p-porosity point.*

References

1. G. Petruska A. M. Bruckner, M. Laczkovich and B. S. Thomson. Porosity and approximate derivatives. *Canadian Journal of Mathematics*, 38:1149–1180, 1986. doi:10.4153/CJM-1986-058-7.
2. K. Ambos-Spies, H. Fleischhack, and H. Huwig. *P-generic sets*, pages 58–68. Springer Berlin Heidelberg, 1984. doi:10.1007/3-540-13345-3_5.
3. K. Ambos-Spies, H. Fleischhack, and H. Huwig. Diagonalizations over polynomial time computable sets. *Theoretical Computer Science*, 51(1):177–204, 1987. doi:10.1016/0304-3975(87)90053-3.
4. K. Ambos-Spies, S. A. Terwijn, and Z. Xizhong. *Resource bounded randomness and weakly complete problems*, pages 369–377. Springer Berlin Heidelberg, 1994. doi:10.1007/3-540-58325-4_201.
5. D. N. Bessis and F. H. Clarke. Partial subdifferentials, derivatives and Rademacher's theorem. *Transactions of AMS*, 351(7):2899–2926, 1999.
6. Miller J. Bienvenu L., Hölzl R. and Nies A. Denjoy, Demuth and density. *Journal of Mathematical Logic*, 14(01):1450004, 2014. doi:10.1142/S0219061314500044.
7. J. M. Borwein and X. Wang. Cone-monotone functions: Differentiability and continuity. *Canadian Journal of Mathematics*, 57:961–982, 2005. doi:10.4153/CJM-2005-037-5.
8. V. Brattka, J. Miller, and A. Nies. Randomness and differentiability. *Transactions of the AMS*, 368:581–605, 2016. arXiv version at arxiv.org/abs/1104.4465.

9 A. M. Bruckner and B. S. Thomson. Porosity estimates for the Dini derivatives. *Real Anal. Exch.*, 9:508–538, 1984.

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

11 R. G. Downey and D. R. Hirschfeldt. *Algorithmic Randomness and Complexity*. Springer-Verlag, 2010.

12 Stephen A. Fenner. Functions that preserve p-randomness. *Inf. Comput.*, 231:125–142, October 2013. doi:10.1016/j.ic.2013.08.009.

13 C. Freer, B. Kjos-Hanssen, A. Nies, and F. Stephan. Algorithmic aspects of Lipschitz functions. *Computability*, 3(1):45–61, 2014. doi:10.3233/COM-14025.

14 A. Galicki. *Randomness and Differentiability of Convex Functions*, pages 196–205. Springer International Publishing, Cham, 2015. doi:10.1007/978-3-319-20028-6_20.

15 A. Galicki. Effective Brenier Theorem: Applications to Computable Analysis and Algorithmic Randomness. In *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS'16, pages 720–729, New York, NY, USA, 2016. ACM. doi:10.1145/2933575.2933596.

16 M. Khan. Lebesgue density and $\prod^0_1$ classes. *Journal of Symbolic Logic*, 81(1):80–95, 2016.

17 Ker-I Ko. *Complexity theory of real functions*. Birkhauser Boston Inc., 1991.

18 A. Nies. *Computability and randomness*, volume 51 of *Oxford Logic Guides*. Oxford University Press, Oxford, 2009. doi:10.1093/acprof:oso/9780199230761.001.0001.

19 André Nies. Differentiability of polynomial time computable functions. In Ernst W. Mayr and Natacha Portier, editors, *31st International Symposium on Theoretical Aspects of Computer Science (STACS 2014)*, volume 25 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 602–613, Dagstuhl, Germany, 2014. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.STACS.2014.602.

20 N. Pathak, C. Rojas, and S. G. Simpson. Schnorr randomness and the Lebesgue differentiation theorem. *Proc. Amer. Math. Soc.*, 142(1):335–349, 2014. doi:10.1090/S0002-9939-2013-11710-7.

21 D. Preiss and L. Zajíček. Directional derivatives of lipschitz functions. *Israel Journal of Mathematics*, 125(1):1–27, 2001. doi:10.1007/BF02773371.

22 J. Lindenstrauss, D. Preiss and J. Tišer. *Fréchet Differentiability of Lipschitz Functions and Porous Sets in Banach Spaces*. Annals of Mathematics Studies. Princeton University Press, 2012.

23 H. Rademacher. Über partielle und totale Differenzierbarkeit von Funktionen mehrerer Variabeln und über die Transformation der Doppelintegrale. *Math. Ann.*, 79(1):340–359, 1919.

24 O. Tapiola. Random and non-random dyadic systems in doubling metric spaces, 2012. MSc thesis. URL: http://hdl.handle.net/10138/37603.

25 Brian S. Thomson. Real functions. Lecture Notes in Mathematics. 1170. Berlin etc.: Springer-Verlag. VII, 229 p. DM 31.50 (1985)., 1985. doi:10.1007/BFb0074380.

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

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