

# Functions that preserve p-randomness\*

Stephen A. Fenner<sup>†</sup>  
Computer Science and Engineering Department  
University of South Carolina  
Columbia, SC 29208 USA  
fenner.sa@gmail.com

July 20, 2011

## Abstract

We show that polynomial-time randomness (p-randomness) is preserved under a variety of familiar operations, including addition and multiplication by a nonzero polynomial-time computable real number. These results follow from a general theorem: If  $I \subseteq \mathbb{R}$  is an open interval,  $f : I \rightarrow \mathbb{R}$  is a function, and  $r \in I$  is p-random, then  $f(r)$  is p-random provided

1.  $f$  is p-computable on the dyadic rational points in  $I$ , and
2.  $f$  varies sufficiently at  $r$ , i.e., there exists a real constant  $C > 0$  such that either

$$(\forall x \in I - \{r\}) \left[ \frac{f(x) - f(r)}{x - r} \geq C \right]$$

or

$$(\forall x \in I - \{r\}) \left[ \frac{f(x) - f(r)}{x - r} \leq -C \right].$$

Our theorem implies in particular that any analytic function about a p-computable point whose power series has uniformly p-computable coefficients preserves p-randomness in its open interval of absolute convergence. Such functions include all the familiar functions from first-year calculus.

**Keywords:** Randomness, p-randomness, complexity, polynomial time, measure, martingale, real analysis

**Subject Classification:** Computational complexity

## 1 Introduction

Informally, we might call an infinite binary sequence “random” if we see no predictable patterns in the sequence. Put another way, a sequence is random if it looks “typical,” that is, it enjoys no easily identifiable properties not shared by almost all other sequences. Here, the notion of “almost all”

---

\*An extended abstract of this paper appeared in FCT 2011 [5].

<sup>†</sup>Partially supported by NSF grants CCF-0515269 and CCF-0915948.

comes from Lebesgue measure on the unit interval  $[0, 1]$ . What we mean by “easily identifiable,” on the other hand, can vary greatly with the situation. In statistics, random sequences are useful to avoid bias in sampling or in simulating processes (e.g., queueing systems) that are too complex for us to determine exactly. In statistics, desirable properties for random sequences include instances of the law of large numbers: a fixed sequence of length  $n$  should occur in the sequence asymptotically a  $2^{-n}$  fraction of the time, for example. Other examples include the law of the iterated logarithm. In cryptography and network security, “easily identifiable” must be strengthened to “unpredictable by an adversary.” In computer science generally, random sequences should produce successful results most of the time when used in various randomized algorithms.

There is always a trade-off between the amount of randomness possessed by a sequence and the ease with which it can be produced. Random sequences that can be produced algorithmically (i.e., pseudorandom sequences) are of course desirable, provided they have enough randomness for the task at hand. The study of algorithmic randomness has a long and rich history (see, for example, [4, 3] for references to the literature). Complexity theoretic notions of randomness were first suggested by Schnorr, and resource-bounded measure and randomness were developed more fully by Lutz (see [8]). For a survey on the subject, see [1].

A natural trade-off in the context of polynomial-time computation is the notion of polynomial-time randomness, or p-randomness for short (see Definition 2.1, below), which is closely tied with the notion of p-measure introduced by Lutz [6, 7]. There are p-random sequences that can be computed in exponential time; in fact, almost all sequences in **EXP** (in a resource-bounded measure theoretic sense) are p-random. Yet p-random sequences are still strong enough for many common tasks, both statistical and computational. For example, p-random sequences satisfy the laws of large numbers and the iterated logarithm (see [13]), and they provide adequate sources for **BPP** computations and have many other desirable computational properties (see [8]).

The current work addresses some geometric aspects of p-random sequences. Recently, connections between the geometry of Euclidean space and effective and resource-bounded measure and dimension have been found [9, 10]. The question of how the complexity or measure theoretic properties of a real number are altered when it is transformed via a real-valued function goes back at least to Wall [12], who showed that adding or multiplying a nonzero rational number to a real number whose base- $k$  expansion is normal<sup>1</sup> yields another real with a normal base- $k$  expansion. Doty, Lutz, & Nandakumar recently extended Wall’s result, showing that the finite-state dimension of the base- $k$  expansion of a real number is preserved under addition or multiplication by a nonzero rational number [2]. At the other extreme of the complexity spectrum, it is not hard to show that algorithmic randomness (Martin-Löf randomness [11]) is preserved under addition or multiplication by a nonzero computable real, regardless of the base of the expansion.

In this paper we take a middle ground, considering how polynomial-time computable functions mapping reals to reals preserve p-randomness. We show (Theorem 4.1, below) that such a function  $f$  maps a p-random real  $r$  to a p-random real  $f(r)$  provided  $f$  satisfies a kind of anti-Lipschitz condition in some neighborhood of  $r$ :  $f(x)$  varies from  $f(r)$  at least linearly in  $x - r$ . (This result still holds even if  $f$  is not monotone in any neighborhood of  $r$ , or if  $f$  is only polynomial-time computable on dyadic rational inputs, or if  $f$  enjoys no particular continuity properties.)

Our result has a number of corollaries: p-randomness is preserved under addition and multiplication by nonzero p-computable reals (complementing the results in [12, 2] and the folklore

---

<sup>1</sup>An infinite sequence  $s$  over a  $k$ -letter alphabet  $\Sigma$  is *normal* iff for any finite string  $w \in \Sigma^*$ , there are  $nk^{-|w|}(1+o(1))$  occurrences of  $w$  as a substring among the first  $n$  letters of  $s$ , as  $n$  tends to infinity.

result about algorithmically random reals); it is also preserved by polynomial and rational functions (with p-computable coefficients) and all the familiar transcendental functions on the reals, e.g., exponential, logarithmic, and trigonometric functions.

The polynomial-time case presents some technical challenges not present with unbounded computational resources. Roughly speaking, given a polynomial-time approximable function  $f : \mathbb{R} \rightarrow \mathbb{R}$ , our goal is to define a betting strategy (i.e., a martingale; see Section 2) that bets on the next bit of the binary expansion of a real number  $r$ , given previous bits. The strategy is based on the behavior of an assumed strategy  $d$  that successfully bets on  $f(r)$ . If we had no resource bounds, then we could approximate  $f$  at various points as closely as needed to obtain a good sample of  $d$ 's behavior on  $f$  applied to those points, allowing us to mimic  $d$  and thus succeed on  $r$ . Since we are polynomial-time-bounded, however, we have no such luxury, and we have to settle for rougher approximations of  $f$ . For example,  $d$  could succeed on  $f(0.0111111111 \dots)$  (where there is a long string of 1's before the next 0 in the argument to  $f$ ) but lose everything on  $f(0.10000 \dots)$ , which is close by. If we only have a poor approximation to  $f$ , then we cannot distinguish the two cases above, and so  $d$  is no good at telling us how to bet on the first digit after the decimal point. Fortunately, we may assume that  $d$  is conservative—in the sense that it does not bet drastically—so that  $d$ 's assets are relatively insensitive to slight variations in the real numbers corresponding to the sequences it bets on.

Section 2 has basic definitions, including martingales and p-randomness. Section 3 describes the conditions on real-valued functions sufficient to preserve p-randomness. Our main results are in Section 4, where we prove that these conditions indeed suffice; Theorem 4.1 is the main result of that section. In Section 5, we show that these conditions hold for a variety of familiar functions. In Section 6, we give evidence that the strongly varying hypothesis in Theorem 4.1 is tight. We suggest further research in Section 7.

## 2 Notation and basic definitions

We let  $\mathbb{N} = \{0, 1, 2, \dots\}$ . We let  $\mathbb{Q}$  be the set of rational numbers. A *dyadic rational* is some  $q \in \mathbb{Q}$  expressible as  $\pm a/2^b$  for some  $a, b \in \mathbb{N}$ . We let  $\mathbb{Q}_2$  denote the set of dyadic rational numbers.

For real  $x > 0$ , we let  $\lg x$  denote  $\log_2 x$ .

In this paper, we only consider the binary expansions of real numbers. If need be, all our results can easily be modified to other bases.

Our basic notions and results about p-computability, martingales, and randomness in complexity theory are standard. See, for example, [7, 8, 1].

Let  $w \in \{0, 1\}^*$  and  $s \in \{0, 1\}^\infty$ . We let  $|w|$  denote the length of  $w$ , and for any  $0 \leq i < |w|$  we let  $w[i]$  be the  $(i + 1)$ st bit of  $w$ . Similarly, for any  $i \in \mathbb{N}$  we let  $s[i]$  denote the  $(i + 1)$ st bit of  $s$ . For any  $m, n \in \mathbb{N}$  with  $m \leq n$ , we let  $s[m \dots (n - 1)] = s[m]s[m + 1] \dots s[n - 1] \in \{0, 1\}^*$  denote the substring consisting of the  $(m + 1)$ st through the  $n$ th bit of  $s$ . We let  $\{0, 1\}^n$  denote the set of strings in  $\{0, 1\}^*$  of length  $n$ . If  $v \in \{0, 1\}^* \cup \{0, 1\}^\infty$ , we let  $w \sqsubseteq v$  mean that  $w$  is a prefix of  $v$ , and we let  $w \sqsubset v$  mean that  $w$  is a proper prefix of  $v$ . We denote the empty string by  $\lambda$ .

Recall that a *martingale* is a function  $d : \{0, 1\}^* \rightarrow \mathbb{R}$  such that for every  $w \in \{0, 1\}^*$ ,

$$0 \leq d(w) = \frac{d(w0) + d(w1)}{2}.$$

We will also assume without loss of generality that  $d(\lambda) \leq 1$ . We say that  $d$  *succeeds* on a sequence  $s \in \{0, 1\}^\infty$  iff

$$\limsup_{n \rightarrow \infty} d(s[0 \dots (n-1)]) = \infty .$$

We say that  $d$  *strongly succeeds* on  $s$  iff

$$\liminf_{n \rightarrow \infty} d(s[0 \dots (n-1)]) = \infty .$$

A function  $d : \{0, 1\}^* \rightarrow \mathbb{R}$  is *p-computable* if there is a polynomial time computable function  $\hat{d} : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Q}$  such that

$$\left| d(w) - \hat{d}(w, 0^r) \right| \leq 2^{-r}$$

for every  $w \in \{0, 1\}^*$  and  $r \in \mathbb{N}$ . We say that  $\hat{d}$  is a *p-approximator* for  $d$ . A real number  $c$  is *p-computable* if the constant function  $\{0, 1\}^* \rightarrow \{c\}$  is p-computable, and we may suppress the first argument in a p-approximator for  $c$ .

**Definition 2.1.** A sequence  $s \in \{0, 1\}^\infty$  is *p-random* if no p-computable martingale succeeds on  $s$ .

**Definition 2.2.** We will say that a martingale  $d$  is *conservative* iff

1. for any  $w \in \{0, 1\}^*$  and  $b \in \{0, 1\}$ ,

$$\frac{d(w)}{2} \leq d(wb) \leq \frac{3d(w)}{2} ,$$

and

2. for any  $s \in \{0, 1\}^\infty$ , if  $d$  succeeds on  $s$ , then  $d$  strongly succeeds on  $s$ .

Note that if  $d$  is conservative, then  $d(w) \leq (3/2)^{|w|}$  for all  $w$ . It is well-known (and easy to show) that if there is a p-computable martingale that succeeds on  $s$ , then there is a conservative p-computable martingale that succeeds on  $s$ .

We identify a sequence  $s \in \{0, 1\}^\infty$  with a real number  $0.s \in [0, 1]$  via the usual binary expansion:  $0.s := \sum_{i=0}^{\infty} s[i]2^{-(i+1)}$ . This correspondence is one-to-one except on  $\mathbb{Q}_2$ , where it is two-to-one. For every  $x \in \{0, 1\}^*$ , we define  $0.x := 0.x000\dots$ , and we define the *dyadic interval*

$$\Gamma_x := [0.x, 0.x + 2^{-|x|}] = \{0.s : s \in \{0, 1\}^\infty \wedge x \sqsubset s\} .$$

For  $s \in \{0, 1\}^\infty$ , we define  $0.s$  to be p-random iff  $s$  is p-random. If  $x \in \mathbb{R}$ , then we define  $x$  to be p-computable (p-random) just as we do for  $x - \lfloor x \rfloor$ . It is well-known that no p-computable real number is p-random.

### 3 Functions of interest

We will restrict our attention to certain types of real-valued functions of a real variable. We are only interested in the behavior of these functions on p-random inputs. For simplicity, we will only consider functions with domain  $[0, 1]$ , but this is in no way an essential restriction. Our functions will possess a certain p-computability property and a certain strong variation property. Both these properties are *local* in the sense that we only care about them in the vicinity of a p-random number.

**Definition 3.1.** A function  $f : [0, 1] \rightarrow \mathbb{R}$  is *weakly p-computable* if there exists a polynomial-time computable function  $\hat{f} : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Q}$  such that for any  $w \in \{0, 1\}^*$  and  $r \in \mathbb{N}$ ,

$$\left| \hat{f}(w, 0^r) - f(0.w) \right| \leq 2^{-r} .$$

Note that a weakly p-computable function can behave arbitrarily on  $[0, 1] - \mathbb{Q}_2$ .

**Definition 3.2.** Let  $f : [0, 1] \rightarrow \mathbb{R}$  be a function and let  $\Gamma_y \subseteq [0, 1]$  be some dyadic interval with  $y \in \{0, 1\}^*$ . We say that  $f$  is *weakly p-computable on  $\Gamma_y$*  iff there exists a ptime computable function  $\hat{f} : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Q}$  such that for any  $w \in \{0, 1\}^*$  and  $r \in \mathbb{N}$ ,

$$\left| \hat{f}(w, 0^r) - f(0.(yw)) \right| \leq 2^{-r} .$$

If  $x \in [0, 1]$ , then we say that  $f$  is *weakly p-computable at  $x$*  iff  $f$  is weakly p-computable on some dyadic interval containing  $x$ .

We say that  $f$  is *locally weakly p-computable* if  $f$  is weakly p-computable at all p-random points in  $[0, 1]$ .

[Note that  $0.(yw) \in \mathbb{Q}_2$  is the dyadic rational number corresponding to the string  $yw$  (the concatenation of  $y$  and  $w$ ).]

In other words,  $f$  is weakly p-computable at  $x$  iff we can approximate  $f$  on the dyadic rationals in some dyadic interval containing  $x$  in polynomial time. Notice that we are *not* insisting that  $f$  have any continuity properties. This means in particular that  $\hat{f}$  may not uniquely determine  $f$  on  $\Gamma_x$ . Notice also that a function may be locally weakly p-computable but not “globally” p-computable, being patched together nonuniformly with various p-computable functions on different dyadic intervals.

We can extend Definition 3.2 to weak p-computability at an arbitrary point  $x \in \mathbb{R}$  in the natural way.

**Definition 3.3.** Let  $I \subseteq \mathbb{R}$  be an interval, let  $f : I \rightarrow \mathbb{R}$  be a function, and let  $x \in I$  be some point. We say that  $f$  *strongly varies at  $x$  on  $I$*  iff there is some real constant  $C > 0$  such that either

1. for all  $z \in I - \{x\}$ ,

$$\frac{f(z) - f(x)}{z - x} \geq C ,$$

or

2. for all  $z \in I$ ,

$$\frac{f(z) - f(x)}{z - x} \leq -C .$$

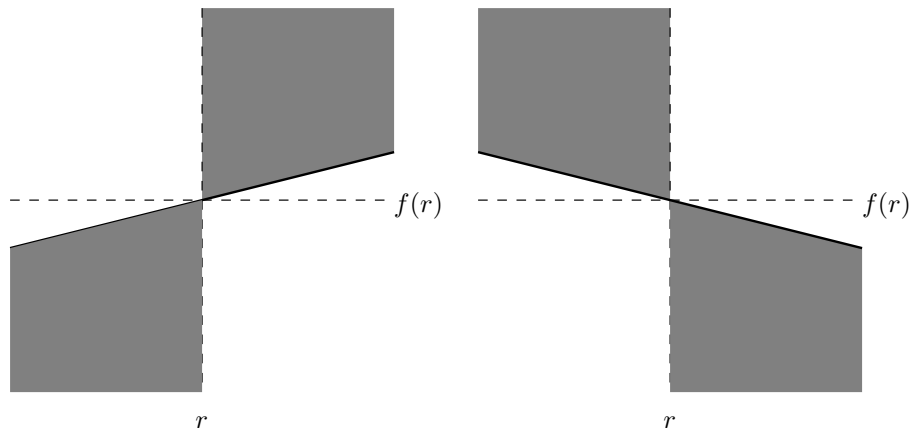


Figure 1: For  $f$  to strongly vary at  $r$ , its graph must confine itself to the shaded region on the left (if strongly increasing) or the right (if strongly decreasing) in some neighborhood of  $r$ . The thick line on the left has slope  $C$  (satisfying  $y - f(r) = C(x - r)$ ), and the line on the right has slope  $-C$  (satisfying  $y - f(r) = -C(x - r)$ ), for some constant  $C > 0$ . Both diagrams depict an arbitrarily small neighborhood of  $r$ .

In case (1) we say that  $f$  *strongly increases at  $x$  on  $I$* , and in case (2)  $f$  *strongly decreases at  $x$  on  $I$* .

We say that  $f$  *strongly varies at  $x$*  if  $f$  strongly varies at  $x$  on  $N$  for some open interval  $N$  containing  $x$ . We define  $f$  strongly increasing/decreasing at  $x$  analogously.

The notion of strong variation is illustrated in Figure 1.

**Example 3.4.** *If  $f$  is  $C^1$  in a neighborhood of  $x$  and  $f'(x) \neq 0$ , then  $f$  strongly varies at  $x$ .*

## 4 Main result

Here is our main technical theorem, from which the other results in the paper follow easily.

**Theorem 4.1.** *Let  $I \subseteq \mathbb{R}$  be some interval and  $f : I \rightarrow \mathbb{R}$  some function. Suppose  $r$  is a  $p$ -random point in the interior of  $I$ . If  $f$  is weakly  $p$ -computable at  $r$  and strongly varies at  $r$ , then  $f(r)$  is  $p$ -random.*

### 4.1 Establishing Theorem 4.1

We start this section with two easy observations which we give without proof.

**Observation 4.2.** *Let  $n$  be any integer, and let  $a \in \mathbb{Q}_2$ . A number  $r \in \mathbb{R}$  is  $p$ -random if and only if  $2^n r$  is  $p$ -random, if and only if  $r + a$  is  $p$ -random, if and only if  $-r$  is  $p$ -random.*

**Observation 4.3.** Let  $I \subseteq \mathbb{R}$  be an interval, let  $f : I \rightarrow \mathbb{R}$  be a function, let  $n$  be any integer, and let  $a \in \mathbb{Q}_2$ . Define

$$\begin{aligned} g(x) &= 2^n f(x) , \\ h(x) &= f(x) + a , \\ j(x) &= f(2^n x) , \\ k(x) &= f(x + a) . \end{aligned}$$

Then  $f$  strongly varies at some  $x \in I$  on  $I$  (respectively, is  $p$ -computable at  $x$ ) if and only if all of  $(-f), g, h$  strongly vary (respectively, are  $p$ -computable) at  $x$  on  $I$ , if and only if  $j$  strongly varies (respectively, is  $p$ -computable) at  $2^{-n}x$  on  $2^{-n}I$ , if and only if  $k$  strongly varies (respectively, is  $p$ -computable) at  $x - a$  on  $I - a$ . The sense of variation (strongly increasing or strongly decreasing) of  $f$  is the same as that of  $g, h, j, k$  and opposite that of  $(-f)$ .

Theorem 4.1 is a corollary of the next lemma, which gives the theorem its essential technical content. We prove this lemma later in this section. For convenience, we will assume that our function  $f$  is monotone ascending. We will show later that this is not an essential restriction.

**Lemma 4.4.** Let  $f : [0, 1] \rightarrow \mathbb{R}$  be weakly  $p$ -computable and monotone ascending on  $[0, 1]$ . Suppose that  $x_0 \in [0, 1]$  and that  $f$  strongly increases at  $x_0$  on  $[0, 1]$ . Then if  $f(x_0)$  is not  $p$ -random, then  $x_0$  is not  $p$ -random.

To prove Lemma 4.4, we need to construct a martingale  $d_f$  that succeeds on  $x_0$ , given one that succeeds on  $f(x_0)$ . If martingale  $d$  succeeds on  $f(x_0)$ , then we can define  $d_f(w)$  (for a given string  $w$ ) to sample the values of  $d$  on points in  $f(\Gamma_w)$ . We do this by sandwiching  $d_f(w)$  between a lower bound  $d^-(w; n)$  and an upper bound  $d^+(w; n)$ . We get  $d^+(w; n)$  by overestimating  $d$ 's total contribution in an interval around  $f(0.w)$  (Equation (1), below), and we get  $d^-(w; n)$  by underestimating it (Equation (2)). These estimates become more refined as  $n$  increases, and, provided  $d$  is conservative, they reach a common limit as  $n$  goes to infinity, yielding a well-defined martingale  $d_f$ .

**Definition 4.5.** Let  $f : [0, 1] \rightarrow [0, 1]$  be monotone ascending on  $[0, 1]$  and let  $d$  be a martingale. For every  $x \in \{0, 1\}^*$ , let  $\Delta_x$  denote the interval  $f(\Gamma_x) = [f(0.x), f(0.x + 2^{-|x|})]$ , and for every  $n \in \mathbb{N}$ , define

$$d^+(x; n) = 2^{|x|-n} \sum_{y \in \{0, 1\}^n : \Gamma_y \cap \Delta_x \neq \emptyset} d(y) , \quad (1)$$

and define

$$d^-(x; n) := 2^{|x|-n} \sum_{y \in \{0, 1\}^n : \Gamma_y \subseteq \Delta_x} d(y) . \quad (2)$$

The only differences between the sums in Equations (1) and (2) are at most two terms  $d(y)$  where  $\Gamma_y$  straddles the boundary of  $\Delta_x$ . The assumption that  $d$  is conservative is needed to ensure that these terms are not too large, and thus that  $d^+(x; n)$  and  $d^-(x; n)$  are close to each other. The following lemma is routine and easy to check.

**Lemma 4.6.** *Let  $f$  and  $d$  be as in Definition 4.5. For any  $x \in \{0, 1\}^*$ , if  $\Gamma_y$  is any dyadic interval contained in  $\Delta_x$  (that is,  $\Gamma_y \subseteq \Delta_x$ ), then letting  $n = |y|$ ,*

$$\begin{aligned} 2^{|x|-n}d(y) &\leq d^-(x; n) \leq d^-(x; n+1) \leq d^-(x; n+2) \leq \\ &\dots \leq d^+(x; 2) \leq d^+(x; 1) \leq d^+(x; 0). \end{aligned}$$

*Proof.* The first inequality holds because  $\Gamma_y \subseteq \Delta_x$ , and hence  $2^{|x|-n}d(y)$  is one of the terms in the sum defining  $d^-(x; n)$ . To see the other inequalities on the top line, notice that each term  $2^{|x|-(n+i)}d(y')$  in the expression for  $d^-(x; n+i)$  (for some  $i \in \mathbb{N}$ ) is equal to the sum  $2^{|x|-(n+i+1)}d(y'0) + 2^{|x|-(n+i+1)}d(y'1)$  of two terms occurring in  $d^-(x; n+i+1)$ .

Clearly, all terms in  $d^-(x; n+i)$  are included in  $d^+(x; n+i)$ , and so every quantity on the top line is less than or equal to the corresponding quantity on the bottom line.

Finally, the inequalities on the bottom line all hold because splitting each term  $2^{|x|-i}d(y')$  in the expression for  $d^+(x; i)$  into the equivalent sum

$$2^{|x|-(i+1)}d(y'0) + 2^{|x|-(i+1)}d(y'1)$$

accounts for all the terms in  $d^+(x; i+1)$  (and possibly more). □

**Definition 4.7.** Let  $f$  and  $d$  be as in Definition 4.5. We define the *upper  $f$ -shift* of  $d$  to be the function defined for all  $x \in \{0, 1\}^*$  as

$$d^+(x) := \lim_{n \rightarrow \infty} d^+(x; n).$$

Similarly, we define the *lower  $f$ -shift* of  $d$  to be

$$d^-(x) := \lim_{n \rightarrow \infty} d^-(x; n).$$

Since for any fixed  $x \in \{0, 1\}^*$ ,  $d^+(x; n)$  and  $d^-(x; n)$  are both monotone functions of  $n$  (decreasing and increasing, respectively) by Lemma 4.6, the limits in the definition above clearly exist, and

$$d^-(x; n) \leq d^-(x) \leq d^+(x) \leq d^+(x; n)$$

for all  $n$ .

For some martingales, the upper and lower  $f$ -shifts may differ, but they coincide for conservative martingales.

**Lemma 4.8.** *Fix  $f$  and  $d$  as in Definition 4.5. Suppose further that  $d$  is conservative. For any  $x \in \{0, 1\}^*$  and  $n \in \mathbb{N}$ ,*

$$d^+(x; n) - d^-(x; n) \leq 2^{|x|+1} \left( \frac{3}{4} \right)^n. \quad (3)$$

*Proof.* Here we only use Property (1) of being conservative. All the terms in the two sums on the left-hand side of the inequality (3) cancel except for at most two dyadic intervals—one containing the left endpoint of  $\Delta_x$  and the other containing the right endpoint. These two intervals correspond to two strings  $y$  and  $z$  respectively, both of length  $n$ . Thus we get

$$\begin{aligned} d^+(x; n) - d^-(x; n) &\leq 2^{|x|-n}(d(y) + d(z)) \leq 2^{|x|-n} \left[ \left( \frac{3}{2} \right)^n + \left( \frac{3}{2} \right)^n \right] \\ &= 2^{|x|+1} \left( \frac{3}{4} \right)^n. \end{aligned}$$

□



**Corollary 4.9.** *Let  $f$  and  $d$  be as in Definition 4.5. If  $d$  is conservative, then  $d^+(x) = d^-(x)$  for all  $x \in \{0, 1\}^*$ .*

*Proof.* Immediate from Lemma 4.8. □

**Definition 4.10.** If  $f$  and  $d$  are as in Definition 4.5 and  $d$  is conservative, then we let  $d_f(x)$  denote the common value  $d^+(x) = d^-(x)$ , and we call  $d_f$  the  $f$ -pullback of  $d$ .

On input string  $x$ ,  $d_f(x)$  merely samples  $d$  over the the interval  $\Delta_x = f(\Gamma_x)$ .

**Lemma 4.11.** *If  $f$  and  $d$  are as in Definition 4.5 and  $d$  is conservative, then its  $f$ -pullback  $d_f$  is a martingale.*

*Proof.* To see that  $d_f$  is a martingale, first we notice that

$$d_f(\lambda) \leq d^+(\lambda; 0) = d(\lambda) \leq 1 .$$

Next, by examining terms in the sums and using Lemma 4.6, we notice that for any  $x \in \{0, 1\}^*$  and  $n \in \mathbb{N}$ ,

$$d^-(x0; n) + d^-(x1; n) \leq 2d^-(x; n) \leq 2d^+(x; n) \leq d^+(x0; n) + d^+(x1; n) .$$

Taking the limit of all sides as  $n \rightarrow \infty$ , we get

$$d^-(x0) + d^-(x1) \leq 2d^-(x) \leq 2d^+(x) \leq d^+(x0) + d^+(x1) .$$

All these quantities are equal, since the two extremes are equal. Thus

$$d_f(x) = \frac{d_f(x0) + d_f(x1)}{2} .$$

□

The next lemma is key. Here is where we make essential use of the strongly increasing property of  $f$ . (The hypothesis here is slightly weaker, though).

**Lemma 4.12.** *Let  $f$  and  $d$  be as in Definition 4.5 with  $d$  being conservative. Suppose that there exist  $r, s \in \{0, 1\}^\infty$  and a real  $C > 0$  such that*

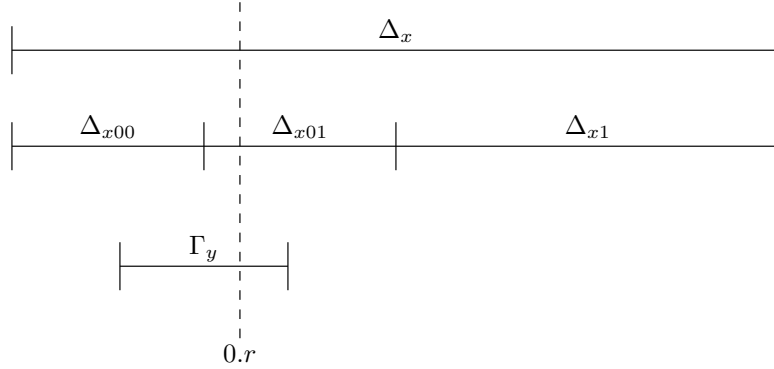
$$\frac{f(x) - 0.r}{x - 0.s} \geq C \tag{4}$$

*for all  $x \in [0, 1] - \{0.s\}$ . If  $d$  succeeds on  $r$  and  $0.s \notin \mathbb{Q}_2$ , then  $d_f$  succeeds on  $s$ .*

*Proof.* Note that Equation (4) implies  $f(x) < 0.r$  if  $x < 0.s$  and  $f(x) > 0.r$  if  $x > 0.s$ .

Set  $\ell := \max(0, \lceil \lg(1/C) \rceil)$ . We then have  $C \geq 2^{-\ell}$ .

Since  $0.s \notin \mathbb{Q}_2$ ,  $s$  has infinitely many 0's and infinitely many 1's. This implies that  $s$  has infinitely many occurrences of "01" as a substring, that is, there are infinitely many  $n \in \mathbb{N}$  such that  $s[n]s[n+1] = 01$ . Fix any real  $M > 0$ . Since  $d$  succeeds on  $r$  and is conservative,  $d$  strongly succeeds on  $r$ , and so there is some  $n_0 \in \mathbb{N}$  such that  $d(r[0 \dots (n-1)]) \geq M$  for all  $n \geq n_0$ . Fix some  $n \geq n_0$  such that  $s[n]s[n+1] = 01$ . Let  $x = s[0 \dots (n-1)]$ . We have  $|x| = n$  and  $x01 \sqsubset s$ . Let  $y = r[0 \dots (n+\ell+1)]$  be the first  $n+\ell+2$  bits of  $r$ , noting that  $d(y) \geq M$ . Here is the situation at  $0.r$ :



We have  $0.r \in \Gamma_y$ . Also, since  $0.s \in \Gamma_{x01} - \mathbb{Q}_2$ , we have  $0.x01 < 0.s < 0.x01 + 2^{-|x01|}$ , which implies  $f(0.x01) \leq 0.r \leq f(0.x01 + 2^{-|x01|})$ , as noted above. It follows immediately that  $0.r \in \Delta_{x01}$ .

**Claim 4.13.**  $\Gamma_y \subseteq \Delta_x$ .

*Proof of Claim 4.13.* By Equation (4) we have

$$0.r - f(0.x) \geq C(0.s - 0.x) \geq C(0.x01 - 0.x) = C2^{-(n+2)} \geq 2^{-(n+\ell+2)} .$$

Since  $0.r \in \Gamma_y$ , we have

$$0.r - 0.y \leq 2^{-|y|} = 2^{-(n+\ell+2)} .$$

Combining these two inequalities gives  $0.r - 0.y \leq 0.r - f(0.x)$ , or equivalently,  $f(0.x) \leq 0.y$ . Similarly, we have

$$\begin{aligned} f(0.x + 2^{-n}) - 0.r &\geq C((0.x + 2^{-n}) - 0.s) \geq C(0.x11 - 0.x1) \\ &= C2^{-(n+2)} \geq 2^{-(n+\ell+2)} = 2^{-|y|} \geq 0.y + 2^{-|y|} - 0.r , \end{aligned}$$

whence  $0.y + 2^{-|y|} \leq f(0.x + 2^{-n})$ . Thus

$$\Gamma_y = [0.y, 0.y + 2^{-|y|}] \subseteq [f(0.x), f(0.x + 2^{-n})] = \Delta_x$$

as claimed. This concludes the proof of Claim 4.13.  $\square$

Continuing with the proof of Lemma 4.12, we use Lemma 4.6 again, noting that  $|y| = |x| + \ell + 2$ , to get

$$2^{-(\ell+2)} d(y) = 2^{|x| - (|x| + \ell + 2)} d(y) \leq d^-(x; |x| + \ell + 2) \leq d_f(x) .$$

Since  $d(y) \geq M$ , we then get

$$d_f(x) \geq 2^{-(\ell+2)} M .$$

Since  $M$  is arbitrary,  $x \sqsubseteq s$ , and  $\ell$  is a constant independent of  $x$ , this means that  $d_f$  succeeds on  $s$ .  $\square$

Finally, we need a lemma regarding  $p$ -computability. The challenge in the proof is in finding an easy (i.e., polynomial-time) way to approximate the  $d^-(x; n)$  and  $d^+(x; n)$ .

**Lemma 4.14.** *Let  $d$  be a conservative martingale, let  $f : [0, 1] \rightarrow [0, 1]$  be monotone ascending on  $[0, 1]$ , and let  $d_f$  be the corresponding  $f$ -pullback of  $d$ . Also assume  $f(1) = 1$ . If  $d$  is  $p$ -computable and  $f$  is weakly  $p$ -computable on  $[0, 1]$ , then  $d_f$  is  $p$ -computable.*

*Proof.* The idea is that, given input  $x \in \{0, 1\}^*$  of length  $n$  and accuracy parameter  $r \in \mathbb{N}$ , we will approximate some number between  $d^-(x; m)$  and  $d^+(x; m)$  for some sufficiently large  $m$  (but still polynomial in  $n$  and  $r$ ). We have no hope of computing the sum of Equations (1) or (2) directly, as there are exponentially many terms. Fortunately, large blocks of the sum can be computed all at once by evaluating  $d$  on shorter inputs. The condition that  $f(1) = 1$  is only for technical convenience and is not necessary; it is only required that  $f(1)$  be p-computable.

Fix polynomial-time functions

$$\hat{d} : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Q} \quad \text{and} \quad \hat{f} : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Q}$$

such that for all  $w \in \{0, 1\}^*$  and  $r \in \mathbb{N}$ ,

$$\left| \hat{d}(w, 0^r) - d(w) \right| \leq 2^{-r} \quad \text{and} \quad \left| \hat{f}(w, 0^r) - f(0.w) \right| \leq 2^{-r} .$$

Fix an input  $x \in \{0, 1\}^*$  and let  $n = |x|$ .

Fix an  $r \in \mathbb{N}$ . We will choose  $m$  to be a sufficiently large integer (depending on  $n$  and  $r$ ) to be determined later. We prove the lemma by describing a procedure (running time polynomial in  $m$ ) to compute a number  $v \in \mathbb{Q}$  such that  $|d_f(x) - v| \leq 2^{-r}$ .

Here is the procedure:

1. Compute dyadic rationals  $0 \leq a \leq b \leq 1$ , both with denominator  $2^m$ , so that  $[a, b]$  approximates  $\Delta_x$  to within less than  $2^{-m}$  for each endpoint:

- (a) Compute  $c_0 = \hat{f}(x, 0^{m+2})$  and round  $c_0$  to the nearest  $a \in \mathbb{Q}_2$  with denominator  $2^m$  so that  $|c_0 - a| \leq 2^{-(m+1)}$ . Notice that

$$|f(0.x) - a| \leq |f(0.x) - c_0| + |c_0 - a| \leq 2^{-(m+2)} + 2^{-(m+1)} < 2^{-m} .$$

In other words,

$$a - 2^{-m} < f(0.x) < a + 2^{-m} .$$

(Note that  $f(0.x)$  is the left endpoint of  $\Delta_x$ .)

- (b) If  $x = 1^n$ , then let  $b := 1$ . Otherwise, let  $x'$  be the lexicographical successor of  $x$  in  $\{0, 1\}^n$ , and compute  $c_1 = \hat{f}(x', 0^{m+2})$ . Let  $b$  be the dyadic rational with denominator  $2^m$  closest to  $c_1$ . Similarly to  $a$ , we have

$$b - 2^{-m} < f(0.x') = f(0.x + 2^{-n}) < b + 2^{-m} .$$

(Note that  $f(0.x + 2^{-n})$  is the right endpoint of  $\Delta_x$ .)

- (c) Without loss of generality, we can assume that  $0 \leq a \leq b \leq 1$ : if necessary, reset  $a := \min(\max(a, 0), 1)$  and  $b := \min(\max(a, b), 1)$ . These adjustments don't affect the inequalities above.

2. Let  $S$  be the set of all  $\sqsubseteq$ -minimal strings  $w$  such that  $\Gamma_w \subseteq [a, b]$ .

3. Finally, compute

$$v := 2^n \sum_{w \in S} 2^{-|w|} \hat{d}(w, 0^m) .$$

Notice that no string in  $S$  is a proper prefix of any other string in  $S$ ; hence the sets  $\Gamma_w$  for  $w \in S$  are pairwise disjoint except for endpoints. Further, it is clear that  $\bigcup_{w \in S} \Gamma_w = [a, b]$  if  $a < b$  (otherwise,  $S = \emptyset$ ).

We claim that  $S$ , and hence  $v$ , can be computed in time polynomial in  $m$ . This follows from three facts:

1.  $a$  and  $b$  can be computed in time polynomial in  $m$ .
2. Every string in  $S$  has length at most  $m$ .
3. There are at most two strings in  $S$  of any given length.

Fact 1 is clear from the procedure description. For Fact 2, notice that, since  $a$  and  $b$  have denominator  $2^m$ , if  $w$  is any string such that  $\Gamma_w \subseteq [a, b]$  and  $|w| > m$ , then removing the last bit of  $w$  yields a proper prefix  $w' \sqsubset w$  such that  $\Gamma_{w'} \subseteq [a, b]$  as well, and so  $w$  is not  $\sqsubseteq$ -minimal, and thus  $w \notin S$ .

Similarly for Fact 3, if  $w_1, w_2, w_3 \in S$  are any three distinct strings given in lexicographical order, and  $|w_1| = |w_3|$ , then  $|w_2| < |w_1|$ . To see this, suppose  $|w_2| \geq |w_1|$ . Let  $w'$  be the result of removing the last bit of  $w_2$ . Then  $\Gamma_{w'}$  includes  $\Gamma_{w_2}$  and another dyadic interval of length  $2^{-|w_2|}$  immediately to the left or right of  $\Gamma_{w_2}$ . In either case, the left end point of  $\Gamma_{w'}$  is not to the left of that of  $\Gamma_{w_1}$ , and the right endpoint of  $\Gamma_{w'}$  is not to the right of that of  $\Gamma_{w_3}$ . So  $\Gamma_{w'} \subseteq [a, b]$ , which means that  $w_2$  is not  $\sqsubseteq$ -minimal, and thus  $w_2 \notin S$ .

Thus  $S$  has at most  $2m + 1$  strings, each of length at most  $m$ , and so the following greedy algorithm for computing  $S$  runs in time polynomial in  $m$ :

```

 $S \leftarrow \emptyset$ 
 $z \leftarrow a$ 
WHILE  $z < b$  DO
  Let  $w \in \{0, 1\}^*$  be shortest such that  $z = 0.w$  and  $z + 2^{-|w|} \leq b$ 
   $S \leftarrow S \cup \{w\}$ 
   $z \leftarrow z + 2^{-|w|}$ 
END-WHILE
return  $S$ 

```

It remains to show that  $v$  is sufficiently close to  $d_f(x)$ .

First, note that, due to the closeness of our approximations to the endpoints of  $\Delta_x$ ,

$$d^-(x; m) \leq 2^{n-m} \sum_{y \in \{0,1\}^m : \Gamma_y \subseteq [a,b]} d(y) \leq d^+(x; m). \quad (5)$$

(The sum in the middle includes all the terms of the sum on the left, and the sum on the right includes all the terms of the sum in the middle.)

Since  $[a, b] = \bigcup_{w \in S} \Gamma_w$ , and the intervals  $\Gamma_w$  intersect only at endpoints, we can rewrite the sum in the middle of (5) as

$$2^{n-m} \sum_{w \in S} \left( \sum_{y \in \{0,1\}^m : w \sqsubseteq y} d(y) \right) = 2^{n-m} \sum_{w \in S} 2^{m-|w|} d(w) = 2^n \sum_{w \in S} 2^{-|w|} d(w),$$

the equalities owing to the fact that  $d$  is a martingale. So Equation (5) becomes

$$d^-(x; m) \leq 2^n \sum_{w \in S} 2^{-|w|} d(w) \leq d^+(x; m) . \quad (6)$$

Now we use the fact that  $|\hat{d}(w, 0^m) - d(w)| \leq 2^{-m}$  for all  $w \in S$ . From (6) we get

$$\begin{aligned} d^-(x; m) - 2^{n-m} \sum_{w \in S} 2^{-|w|} &\leq 2^n \sum_{w \in S} 2^{-|w|} [d(w) - 2^{-m}] \\ &\leq 2^n \sum_{w \in S} 2^{-|w|} \hat{d}(w, 0^m) \\ &= v \leq 2^n \sum_{w \in S} 2^{-|w|} [d(w) + 2^{-m}] \\ &\leq d^+(x; m) + 2^{n-m} \sum_{w \in S} 2^{-|w|} . \end{aligned}$$

We have  $\sum_{w \in S} 2^{-|w|} = b - a \leq 1$ , so the above inequality implies

$$d^-(x; m) - 2^{n-m} \leq v \leq d^+(x; m) + 2^{n-m} .$$

Since  $d^-(x; m) \leq d_f(x) \leq d^+(x; m)$  (as follows from Lemma 4.6), it is clear then that

$$\begin{aligned} |d_f(x) - v| &\leq d^+(x; m) - d^-(x; m) + 2^{n-m} \\ &\leq 2^{n-m} + 2^{n+1} \left(\frac{3}{4}\right)^m \\ &= 2^{n-m} + 2^{n-2m+1} 3^m \end{aligned}$$

by Lemma 4.8. To bound  $|d_f(x) - v|$  above by  $2^{-r}$ , it suffices that  $2^{n-m} \leq 2^{-(r+1)}$  and that  $2^{n-2m+1} 3^m \leq 2^{-(r+1)}$ . That is,

$$m \geq n + r + 1 \quad \text{and} \quad m \geq \frac{n + r + 2}{2 - \log_2 3} .$$

So it suffices to set  $m := 4(n + r + 2)$ . This makes the computation time for  $v$  polynomial in  $n$  and  $r$ , because  $m$  is polynomial in  $n$  and  $r$ .  $\square$

*Proof of Lemma 4.4.* Let  $f$  and  $x_0$  be as in Lemma 4.4. If  $x_0 \in \mathbb{Q}_2$ , then it is clearly not p-random, and we are done. Otherwise, let  $\ell = \lfloor f(0) \rfloor$ , let  $h = \lceil f(1) \rceil$ , and let  $m \geq 0$  be the least natural number such that  $2^m \geq h - \ell$ . For all  $x \in [0, 1)$ , define

$$g(x) := 2^{-m}(f(x) - \ell) ,$$

and define  $g(1) := 1$ . Then  $g : [0, 1] \rightarrow [0, 1]$  is monotone ascending, weakly p-computable on  $[0, 1]$ , and strongly increasing at  $x_0$  on  $[0, 1]$  by Observation 4.3. Further, since  $f(x_0)$  is not p-random, it follows from Observation 4.2 that  $g(x_0) = 2^{-m}(f(x_0) - \ell)$  is not p-random, either. Thus there is a conservative, p-computable martingale  $d$  that succeeds on  $g(x_0)$ . By Lemmata 4.12 and 4.14 (letting  $0.s$  be  $x_0$ ), the  $g$ -pullback  $d_g$  of  $d$  succeeds on  $x_0$  and is p-computable. Thus  $x_0$  is not p-random.  $\square$

To prove Theorem 4.1, we first show that the monotonicity assumption in Lemma 4.4 is dispensable. We do this by tweaking a nonmonotone function into a monotone one with the same desirable properties.

**Lemma 4.15.** *Let  $f : [0, 1] \rightarrow \mathbb{R}$  be weakly  $p$ -computable on  $[0, 1]$ . Suppose that there exists  $x_0 \in [0, 1]$  such that  $f$  strongly increases at  $x_0$  on  $[0, 1]$ . Then there exists a monotone ascending function  $g : [0, 1] \rightarrow \mathbb{R}$  that is weakly  $p$ -computable on  $[0, 1]$ , strongly increases at  $x_0$  on  $[0, 1]$ , and satisfies  $g(x_0) = f(x_0)$ .*

*Proof of Lemma 4.15.* We first define  $g$  on  $\mathbb{Q}_2 \cap [0, 1]$  to be monotone. Extending  $g$  to domain  $[0, 1]$  will then be trivial.

The idea is that we give priority to dyadic rationals with smaller denominators, and for any point  $x \in \mathbb{Q}_2$ , we let  $g(x) := f(x)$  unless this violates monotonicity with a neighboring point of higher priority (i.e., lower denominator). If so, we adjust  $g(x)$  just enough to avoid the violation.

Here we give a recursive definition of  $g$  restricted to  $\mathbb{Q}_2 \cap [0, 1]$  based on  $f$ . For any  $q \in \mathbb{Q}_2 \cap (0, 1)$ , let  $y_q \in \{0, 1\}^*$  be the unique string such that  $q = 0.y_q1$ . We define  $e_q := |y_q| + 1$  and call this the *exponent* of  $q$ . By convention, the exponents  $e_0$  of 0 and  $e_1$  of 1 are both 0. Define

$$q^- := 0.y_q,$$

and define

$$q^+ := \begin{cases} 1 & \text{if } y_q \in \{1\}^*, \\ 0.z1 & \text{if } (\exists z \in \{0, 1\}^*)(\exists w \in \{1\}^*)[y_q = z0w]. \end{cases}$$

(Note that  $z$  and  $w$  are unique if they exist.) The points  $q^-$  and  $q^+$  are the dyadic rationals closest to  $q$  (on the left and right side, respectively) whose exponents are less than that of  $q$ .

Now we define  $g(0) := f(0)$ ,  $g(1) := f(1)$ , and for each  $q \in \mathbb{Q}_2 \cap (0, 1)$ ,

$$g(q) := \max(g(q^-), \min(g(q^+), f(q))). \quad (7)$$

The recursion is well-founded because  $q^-$  and  $q^+$  have smaller exponents than  $q$ .

**Claim 4.16.** *The function  $g$  is monotone ascending on  $\mathbb{Q}_2 \cap [0, 1]$ .*

*Proof of Claim 4.16.* Let  $p$  and  $q$  be dyadic rationals with  $0 \leq p < q \leq 1$ . We proceed by induction on  $e := \max(e_p, e_q)$  to show that  $g(p) \leq g(q)$ . If  $e = 0$ , then we have  $p = 0$  and  $q = 1$ , and clearly,  $g(0) = f(0) < f(1) = g(1)$  by the constraints on  $f$ . If  $e > 0$ , we have three cases:

1. If  $e_p < e_q$ , then we have  $p \leq q^-$  by the maximality of  $q^-$ , and so by the inductive hypothesis,  $g(p) \leq g(q^-)$ . Then by the recursive definition of  $g(q)$ , we have  $g(q^-) \leq g(q)$ , hence  $g(p) \leq g(q)$ .
2. If  $e_p > e_q$ , then  $p^+ \leq q$ , and so by the inductive hypothesis,  $g(p^-) \leq g(p^+) \leq g(q)$ . By the recursive definition of  $g(p)$  (and the fact that  $g(p^-) \leq g(p^+)$ ), we have  $g(p) \leq g(p^+)$ , whence  $g(p) \leq g(q)$ .
3. If  $e_p = e_q > 0$ , then  $|y_p| = |y_q|$ . Let  $y$  be the longest common prefix of  $y_p$  and  $y_q$ . Then clearly,  $y0 \sqsubseteq y_p$  and  $y1 \sqsubseteq y_q$ . Let  $r = 0.y1$ . Since  $y$  is shorter than  $y_p$  and  $y_q$ , we have  $e_r < e_p$  and  $e_r < e_q$ , and in addition,  $p < r < q$ . Thus  $p^+ \leq r \leq q^-$ , and so by the inductive hypothesis,  $g(p^+) \leq g(r) \leq g(q^-)$ . By an argument similar to the other two cases, we have  $g(p) \leq g(p^+)$  and  $g(q^-) \leq g(q)$ . Thus  $g(p) \leq g(q)$ .

This ends the proof of Claim 4.16. □

**Claim 4.17.** *The function  $g$  is  $p$ -computable on  $\mathbb{Q}_2 \cap [0, 1]$ .*

*Proof of Claim 4.17.* First  $g(0) = f(0)$  and  $g(1) = f(1)$ , so  $g$  is  $p$ -computable at 0 and at 1. For any  $q \in \mathbb{Q}_2 \cap (0, 1)$ , we have

$$g(q) = \max(g(q^-), \min(g(q^+), f(q))) .$$

First notice that for any  $r \in \mathbb{N}$ , if  $a$ ,  $b$ , and  $c$  are such that  $|a - g(q^-)| \leq 2^{-r}$ ,  $|b - g(q^+)| \leq 2^{-r}$ , and  $|c - f(q)| \leq 2^{-r}$  then it is not hard to see that

$$|\max(a, \min(b, c)) - g(q)| \leq 2^{-r} .$$

Thus to approximate  $g(q)$  to within  $2^{-r}$ , it suffices to approximate  $g(q^-)$ ,  $g(q^+)$ , and  $f(q)$  each to within  $2^{-r}$ .

Let  $q = 0.y_q1$  where  $y_q$  is as above. Unwinding the recursion of Equation 7, it becomes apparent that  $g(q)$  only depends on  $f$  at 1 and at points of the form  $0.y$  and  $0.y1$  for  $y \sqsubseteq y_q$ . So to approximate  $g(q)$  we only need to approximate  $f$  on these points. Here is a nonrecursive polynomial-time algorithm, equivalent to Equation 7, to approximate  $g$  on  $\mathbb{Q}_2 \cap [0, 1)$ . It assumes a  $p$ -approximator  $\hat{f}$  for  $f$  on  $[0, 1)$  and a  $p$ -approximator  $\hat{f}_1$  for  $f(1)$ .

```

Algorithm for  $\hat{g}(x, 0^r)$ 
//  $x \in \{0, 1\}^*$  and  $r \in \mathbb{N}$ 
// Outputs a  $y \in \mathbb{Q}$  such that  $|y - g(0.x)| \leq 2^{-r}$ 
  Remove any trailing zeros from  $x$ 
   $\ell \leftarrow \hat{f}(\lambda, 0^r)$ 
   $h \leftarrow \hat{f}_1(0^r)$ 
   $s \leftarrow \lambda$ 
  FOR  $i \leftarrow 0$  TO  $|x| - 1$  DO
     $b \leftarrow x[i]$ 
    IF  $b = 0$  THEN
       $h \leftarrow \max(\ell, \min(h, \hat{f}(s1, 0^r)))$ 
    ELSE // IF  $b = 1$  THEN
       $\ell \leftarrow \max(\ell, \min(h, \hat{f}(s1, 0^r)))$ 
     $s \leftarrow sb$ 
  END-FOR
  OUTPUT  $\ell$  and STOP

```

The algorithm above clearly runs in polynomial time. The proof that it correctly approximates  $g(0.x)$  uses the following key loop invariant: At the start of each iteration of the FOR-loop,  $s \sqsubseteq x$ , and in addition,

$$|\ell - g((0.s1)^-)| \leq 2^{-r} \quad \text{and} \quad |h - g((0.s1)^+)| \leq 2^{-r} .$$

We omit the details. This ends the proof of Claim 4.17. □

**Claim 4.18.** *There exists a  $C > 0$  such that for all  $x \in [0, 1] \cap \mathbb{Q}_2 - \{x_0\}$ ,*

$$\frac{g(x) - f(x_0)}{x - x_0} \geq C . \tag{8}$$

*Proof of Claim 4.18.* We can let  $C$  be any constant witnessing the strong increase of  $f$  at  $x_0$  on  $[0, 1]$ . We proceed by induction on the exponent  $e_x$  of  $x$ . This is clear when  $e_x = 0$ . If  $e_x > 0$ , then

$$g(x) = \max(g(x^-), \min(g(x^+), f(x)))$$

by Equation 7. If  $g(x) = f(x)$ , then we are clearly done. Suppose  $g(x) < f(x)$ . Then Equation 8 is still satisfied if  $x < x_0$ , so suppose that  $x > x_0$ . We have  $g(x) = g(x^+)$ , and so, using the inductive hypothesis,

$$\frac{g(x) - f(x_0)}{x - x_0} = \frac{g(x^+) - f(x_0)}{x - x_0} \geq \frac{g(x^+) - f(x_0)}{x^+ - x_0} \geq C.$$

A similar argument using  $g(x^-)$  works if  $g(x) > f(x)$ . This ends the proof of Claim 4.18.  $\square$

We now extend the definition of  $g$  to all of  $[0, 1]$  by

$$g(x) := \sup\{g(y) \mid y \in \mathbb{Q}_2 \cap [0, x]\},$$

except that we define  $g(x_0) := f(x_0)$ . (If  $x_0 \in \mathbb{Q}_2$ , then we already have  $g(x_0) = f(x_0)$ , because  $g(x_0^-) < f(x_0) < g(x_0^+)$  by Equation 8.) The claims imply that  $g$  has all the requisite properties.  $\square$

*Proof of Theorem 4.1.* Let  $I$ ,  $f$ , and  $r$  be as in the statement of the theorem. We can assume that  $f$  strongly increases at  $x$ , for otherwise we apply the foregoing argument to  $-f$ , using Observations 4.2 and 4.3 to get that  $f(r)$  is p-random. We can choose some dyadic interval  $\Gamma_w = [0.w, 0.w + 2^{-|w|}] \subseteq I$  containing  $r$  on which  $f$  is weakly p-computable and strongly increases at  $x$ . For all  $x \in [0, 1]$ , define

$$g(x) := f(0.w + 2^{-|w|x}).$$

By Observation 4.3,  $g$  is weakly p-computable on  $[0, 1]$  and strongly increases at the point  $s := 2^{|w|}(r - 0.w)$  on  $[0, 1]$ . By Lemma 4.15, there is a monotone ascending function  $h$  that is weakly p-computable on  $[0, 1]$ , is strongly increasing at  $s$  on  $[0, 1]$ , and satisfies  $h(s) = g(s)$ . By Observation 4.2,  $s$  is p-random. By Lemma 4.4,  $h(s)$  is p-random, and clearly,  $h(s) = g(s) = f(r)$ , which proves the theorem.  $\square$

## 5 Some p-randomness-preserving functions

Here is the class of functions we will consider:

**Definition 5.1.** Let  $I \subseteq \mathbb{R}$  be an open interval. A function  $f : I \rightarrow \mathbb{R}$  is *well-behaved on  $I$*  if  $f$  is locally weakly p-computable and strongly varying at each of the p-random points in  $I$ .

Theorem 4.1 gives us the following corollary:

**Corollary 5.2.** *If a function  $f$  is well-behaved on an interval  $I$ , then  $f$  preserves p-randomness, i.e.,  $f$  maps p-random points in  $I$  to p-random points.*

A wide variety of functions are well-behaved and hence preserve p-randomness, including addition and multiplication by nonzero p-computable numbers, nonconstant polynomial and rational functions with p-computable coefficients, and all the familiar transcendental functions—exponential, logarithmic, trigonometric, etc. (Define a function to be 0 where it would otherwise be undefined.) Although these functions may not be strongly varying at all points, they are strongly varying at all p-random points.



**Definition 5.3.** A sequence  $c_0, c_1, c_2, \dots \in \mathbb{R}$  is *uniformly p-computable* if there exists a polynomial-time function  $\hat{c} : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Q}$  such that for all  $n, r \in \mathbb{N}$ ,

$$|\hat{c}(0^n, 0^r) - c_n| \leq 2^{-r} .$$

**Definition 5.4.** Let  $I \subseteq \mathbb{R}$  be an open interval. We say that a function  $f : I \rightarrow \mathbb{R}$  is *p-analytic on I* if there exists a p-computable point  $x_0 \in I$  and a uniformly p-computable sequence  $c_0, c_1, c_2, \dots$  such that for all  $x \in I$ ,

$$f(x) = \sum_{n=0}^{\infty} c_n (x - x_0)^n ,$$

and the power series on the right converges absolutely for all  $x \in I$ .

Note that if  $f$  is p-analytic on  $I$ , then  $f$  is  $C^1$  on  $I$ . In this section we prove the following theorem:

**Theorem 5.5.** *Let  $I \subseteq \mathbb{R}$  be an open interval. If  $f : I \rightarrow \mathbb{R}$  is nonconstant and p-analytic on  $I$ , then  $f$  is well-behaved on  $I$ .*

Theorem 5.5 follows from the two lemmas below:

**Lemma 5.6.** *Let  $J \subseteq \mathbb{R}$  be an open interval and let  $I$  be a dyadic interval such that  $I \subseteq J$ . If  $f$  is p-analytic on  $J$ , then  $f$  is weakly p-computable on  $I$ .*

*Proof of Lemma 5.6.* Our proof mirrors standard results from calculus. Let  $c_0, c_1, c_2, \dots$  be a uniformly p-computable sequence witnessed by  $\hat{c}$ , and let  $x_0 \in J$  be such that  $f(x) = \sum_{n=0}^{\infty} c_n (x - x_0)^n$ , with the right-hand side converging absolutely, for all  $x \in J$ . Let  $r = \sup\{|x - x_0| : x \in I\}$ , and let  $x \in I$  with  $|x - x_0| = r$ . Since  $x \in J$  and  $J$  is open, there must be an  $\varepsilon > 0$  such that  $\sum_{n=0}^{\infty} |c_n| (r + \varepsilon)^n < \infty$ . Hence all the terms  $|c_n| (r + \varepsilon)^n$  are upper bounded by some constant  $C \geq 1$  independent of  $n$ . This implies in turn that for all  $-r \leq z \leq r$  and  $m \geq 0$ , we can bound the tail of the series:

$$\left| \sum_{n=m}^{\infty} c_n z^n \right| \leq \sum_{n=m}^{\infty} |c_n| r^n \leq \sum_{n=m}^{\infty} C \left( \frac{r}{r + \varepsilon} \right)^n = C \left( \frac{r}{r + \varepsilon} \right)^m \frac{r + \varepsilon}{\varepsilon} \leq 2^{k-m/\ell} , \quad (9)$$

where  $k = \lceil \lg(C(r + \varepsilon)/\varepsilon) \rceil$  and  $\ell := \lceil 1/\lg((r + \varepsilon)/r) \rceil$ .

Let  $\hat{x}$  be a p-approximator for  $x_0$ . Fix  $w \in \{0, 1\}^*$  such that  $I = \Gamma_w$ . For  $a \in \{0, 1\}^*$  and  $s \in \mathbb{N}$ , define

$$\begin{aligned} m_s &:= \ell(s + k + 1) , \\ b_s &:= \left\lceil \lg \left( 2 + \max_{n < m_s} \{ |\hat{c}(0^n, \lambda)|, |0.wa - \hat{x}(\lambda)| \} \right) \right\rceil , \\ \hat{f}(a, 0^s) &:= \sum_{n=0}^{m_s-1} \hat{c}(0^n, 0^{s+b_s n+2m_s+1}) \left[ 0.wa - \hat{x}(0^{s+b_s n+2m_s+1}) \right]^n . \end{aligned}$$

Clearly,  $\hat{f}$  is polynomial-time computable. We then have, for all  $a \in \{0, 1\}^*$  and  $s \in \mathbb{N}$ , letting  $e(n, s)$  denote  $s + b_s n + 2m_s + 1$ ,

$$\begin{aligned}
& \left| \hat{f}(a, 0^s) - f(0.wa) \right| \\
&= \left| \sum_{n=0}^{m_s-1} \hat{c}(0^n, 0^{e(n,s)}) \left[ 0.wa - \hat{x}(0^{e(n,s)}) \right]^n - \sum_{n=0}^{\infty} c_n (0.wa - x_0)^n \right| \\
&\leq \left| \sum_{n=0}^{m_s-1} \left[ \hat{c}(0^n, 0^{e(n,s)}) \left[ 0.wa - \hat{x}(0^{e(n,s)}) \right]^n - c_n (0.wa - x_0)^n \right] \right| \\
&\quad + \left| \sum_{n=m_s}^{\infty} c_n (0.wa - x_0)^n \right| \\
&\leq \sum_{n=0}^{m_s-1} \left| \hat{c}(0^n, 0^{e(n,s)}) \left[ 0.wa - \hat{x}(0^{e(n,s)}) \right]^n - c_n (0.wa - x_0)^n \right| \\
&\quad + 2^{k-m_s/\ell},
\end{aligned}$$

by Equation (9) because  $|0.wa - x_0| \leq r$ . By our choice of  $m_s$ , we have  $2^{k-m_s/\ell} = 2^{-s-1}$ , which bounds the tail term. For the term being summed, we use the formula for the difference of two products as a telescoping sum:

$$\alpha_1 \cdots \alpha_n - \beta_1 \cdots \beta_n = \sum_{i=1}^n \alpha_1 \cdots \alpha_{i-1} (\alpha_i - \beta_i) \beta_{i+1} \cdots \beta_n.$$

Our choice of  $b_s$  ensures that

$$2^{b_s} \geq \max_{n < m_s} \left\{ |\hat{c}(0^n, 0^{e(n,s)})|, |c_n|, |0.wa - \hat{x}(0^{e(n,s)})|, |0.wa - x_0| \right\}.$$

Combining these gives

$$\begin{aligned}
& \left| \hat{c}(0^n, 0^{e(n,s)}) \left[ 0.wa - \hat{x}(0^{e(n,s)}) \right]^n - c_n (0.wa - x_0)^n \right| \\
&\leq 2^{b_s n} \left( \left| \hat{c}(0^n, 0^{e(n,s)}) - c_n \right| + n \left| x_0 - \hat{x}(0^{e(n,s)}) \right| \right) \\
&\leq 2^{b_s n} (n+1) 2^{-e(n,s)} = (n+1) 2^{-s-2m_s-1}
\end{aligned}$$

for all  $n < m_s$ . Thus

$$\left| \hat{f}(a, 0^s) - f(0.wa) \right| \leq (m_s)^2 2^{-2m_s} 2^{-s-1} + 2^{-s-1} \leq 2^{-s},$$

and so  $\hat{f}(a, 0^s)$  approximates  $f(0.wa)$  closely enough.  $\square$

**Lemma 5.7.** *Suppose  $f$  is  $p$ -analytic and nonconstant in some open interval  $I$ . If  $r \in I$  satisfies  $f(r) = 0$ , then  $r$  is  $p$ -computable.*

*Proof sketch of Lemma 5.7.* Let  $f(x) = \sum_{n=0}^{\infty} c_n(x - x_0)^n$ , where  $x_0$  is p-computable, the  $c_n$  are uniformly p-computable, and the sum converges absolutely on  $I$ . Let  $r$  be such that  $f(r) = 0$ . Expressing  $f(x)$  as a power series about  $r$  gives  $f(x) = \sum_{n=1}^{\infty} c'_n(x - r)^n$  for some constants  $c'_n$ . Since  $f$  is nonconstant, there is a least  $m > 0$  such that  $c'_m \neq 0$ . Then  $f(r) = f'(r) = f''(r) = \dots = f^{(m-1)}(r) = 0$ , but  $f^{(m)}(r) \neq 0$ .

It is easy to observe that if a function  $g$  is p-analytic on  $I$ , then so is its derivative  $g'$ . Letting  $g := f^{(m-1)}$ , we see that: (i)  $g$  is p-analytic and thus weakly p-computable; (ii)  $g(r) = 0$ ; and (iii)  $g'(r) \neq 0$ . Hence there is a neighborhood  $N$  of  $r$  such that  $g(x)$  changes sign at  $x = r$  and nowhere else. This allows us to find  $r$  quickly using binary search, testing the sign of  $g(x)$  for various  $x \in N$ .  $\square$

*Proof of Theorem 5.5.* We know already that, since  $f$  has a continuous derivative, it strongly varies at any point  $r$  such that  $f'(r) \neq 0$  (hence if  $r$  is p-random then so is  $f(r)$ ). If  $f'(r) = 0$ , then  $r$  is p-computable by Lemma 5.7, and thus not p-random.  $\square$

**Corollary 5.8.** *Let  $r$  be p-random. Then so are  $e^r$ ,  $\sin r$ ,  $\cos r$ , and  $\tan r$ . If  $r > 0$ , then  $\ln r$  is p-random. If  $f$  is any fixed rational function whose numerator and denominator have p-computable coefficients, and  $f$  is defined at  $r$ , then  $f(r)$  is p-random. If  $c \neq 0$  is p-computable, then  $cr$  and  $c + r$  are p-random.*

*Proof.* All these functions are p-analytic in some neighborhood of any point in their domains.  $\square$

## 6 The tightness of Theorem 4.1

In this section, we give evidence that the strongly varying property of  $f$  in Theorem 4.1 is essentially tight. To this end, we concoct monotone functions that deviate only slightly from strongly varying, but none of whose outputs are p-random. For example, one could have  $f(0.\sigma) = 0.\tau$ , where the sequence  $\tau$  results from the sequence  $\sigma$  by inserting zeros into  $\sigma$  very sparsely but infinitely often, in places that are easy for a martingale to find and bet on.

**Definition 6.1.** Fix  $Z \subseteq \mathbb{N}$ , and define its *census function*  $c(i) := |Z \cap \{0, \dots, i\}|$  for all  $i \in \mathbb{N}$ .

1. For every  $s \in \{0, 1\}^{\infty}$ , define  $s_Z \in \{0, 1\}^{\infty}$  such that, for all  $i \in \mathbb{N}$ ,

$$s_Z[i] = \begin{cases} s[i - c(i)] & \text{if } i \notin Z, \\ 0 & \text{if } i \in Z. \end{cases}$$

2. Let  $f_Z : [0, 1) \rightarrow \mathbb{R}$  be the function mapping  $0.s$  to  $0.(s_Z)$  for every  $s \in \{0, 1\}^{\infty}$  with infinitely many zeros.

Note that  $s_Z$  results from  $s$  by inserting zeros at the positions  $i \in Z$ , shifting bits of  $s$  to the right to make room.

**Observation 6.2.** *Let  $Z \subseteq \mathbb{N}$  be arbitrary, and let  $c$  be its census function.*

1. For any  $s \in \{0, 1\}^{\infty}$  with infinitely many zeros,

$$f_Z(0.s) = 0.(s_Z) = \sum_{i=0}^{\infty} s[i] 2^{-(i+c(i)+1)}. \quad (10)$$

2. The function  $f_Z$  is monotone ascending, and if  $\mathbb{N} - Z$  is infinite, then  $f_Z$  is one-to-one.
3. If the predicate, “ $n \in Z$ ” is computable in time polynomial in  $n$ , then  $f_Z$  is weakly  $p$ -computable.
4. If  $Z$  is infinite and the predicate, “ $n \in Z$ ” is computable in time polynomial in  $n$ , then  $f(x)$  is never  $p$ -random for any  $x \in [0, 1)$ .

*Proof sketch.* Equation (10) is a routine application of the definition of  $s_Z$ . Point (2.) is obvious. For Point (3.), note that the list  $\langle c(0), c(1), \dots, c(n) \rangle$  is computable in time polynomial in  $n$ , which makes the sum in Equation (10) easy to approximate to polynomially many terms. For Point (4.), consider a martingale that bets on a string  $w$  iff  $|w| \in Z$ , in which case it puts all its money on the next bit being 0. This martingale will succeed on any sequence of the form  $s_Z$ .  $\square$

**Theorem 6.3.** *Let  $Z \in \mathbb{N}$  be arbitrary, and let  $c$  be its census function. For any real  $x$  and  $y$  such that  $0 \leq x < y < 1$ ,*

$$\frac{f_Z(y) - f_Z(x)}{y - x} > 2^{-c(\lceil -\lg(y-x) \rceil) - 1} . \quad (11)$$

If  $Z$  is finite, then its census function  $c$  is bounded from above, whence Theorem 6.3 says that  $f_Z$  is strongly increasing everywhere. The strength of Theorem 6.3 comes when  $Z$  is infinite but extremely sparse, e.g.,  $Z$  is the range of the one-argument Ackermann function. Then the theorem implies that  $f_Z$  comes very close to being strongly increasing, because the function  $c$  grows very slowly. If, in addition,  $Z$  satisfies Observation 6.2(4.), then we get a weakly  $p$ -computable, monotone function  $f_Z$  that is extremely close to being strongly increasing everywhere, but none of whose outputs is  $p$ -random.

*Proof of Theorem 6.3.* We first consider the case where  $n$  is a positive integer and  $y = x + 2^{-n}$ . In this case, we prove that

$$f_Z(x + 2^{-n}) - f_Z(x) \geq 2^{-c(n) - n} . \quad (12)$$

Once Equation (12) is established, Equation (11) follows easily by the monotonicity of  $f_Z$ : setting  $n := \lceil -\lg(y - x) \rceil$  and noting that  $x + 2^{-n} \leq y < x + 2^{1-n}$ , we have

$$\frac{f_Z(y) - f_Z(x)}{y - x} > 2^{n-1} [f_Z(y) - f_Z(x)] \geq 2^{n-1} [f_Z(x + 2^{-n}) - f_Z(x)] \geq 2^{-c(n) - 1} .$$

To establish Equation (12), we let  $s \in \{0, 1\}^\infty$  be such that  $x = 0.s$  (and  $s$  has infinitely many zeros). Similarly, let  $x + 2^{-n} = 0.t$  for some  $t \in \{0, 1\}^\infty$  with infinitely many zeros. It is not too hard to see that  $t$  results from  $s$  by adding 1 to  $s$  in the  $(n - 1)$ th position, then carrying 1's to the left until a zero is reached: Let  $k \in \mathbb{N}$  be largest such that  $k < n$  and  $s[k] = 0$ . Such a  $k$  must exist because  $x + 2^{-n} < 1$  by assumption. Then  $s$  and  $t$  differ only in positions  $k$  through  $n - 1$ , where

$$\begin{aligned} s[k \dots (n - 1)] &= 011 \dots 1, \\ t[k \dots (n - 1)] &= 100 \dots 0. \end{aligned}$$

Using Equation (10)—and noting that  $c$  is monotone ascending—we then get

$$\begin{aligned}
f_Z(x + 2^{-n}) - f_Z(x) &= f_Z(0.t) - f_Z(0.s) = \sum_{i=1}^{\infty} t[i]2^{-(i+c(i)+1)} - \sum_{i=1}^{\infty} s[i]2^{-(i+c(i)+1)} \\
&= \sum_{i=k}^{n-1} (t[i] - s[i])2^{-(i+c(i)+1)} = 2^{-(k+c(k)+1)} - \sum_{i=k+1}^{n-1} 2^{-(i+c(i)+1)} \\
&\geq 2^{-(k+c(k)+1)} - \sum_{i=k+1}^{n-1} 2^{-(i+c(k)+1)} = 2^{-c(k)} \left( 2^{-k-1} - \sum_{i=k+1}^{n-1} 2^{-i-1} \right) \\
&= 2^{-c(k)-n} \geq 2^{-c(n)-n},
\end{aligned}$$

which establishes Equation (12). □

## 7 Further research

P-randomness-preserving functions are clearly closed under composition. Are well-behaved functions closed this way also?

Theorem 6.3 notwithstanding, we are at a loss to prove a converse to Theorem 4.1. Is there even a partial converse? For example, consider the following conjecture about monotone functions:

**Conjecture 7.1.** *If  $f$  is weakly  $p$ -computable and monotone in a neighborhood of  $r \in \mathbb{R}$  but is not strongly varying at  $r$ , then  $f(r)$  is not  $p$ -random.*

Theorem 6.3 falls short of proving this conjecture, because it assumes that the set  $Z$  is easy to compute. In general, however, if  $f$  is not strongly varying, then the violations to strong variation may come in places that are difficult to detect by a martingale.

### Acknowledgments

I would like to thank Jack Lutz for suggesting this problem and for many interesting and valuable discussions. The presentation was also helped significantly from an earlier draft by comments from anonymous referees. I would also like to thank Lance Fortnow for his guidance at a crucial point.

## References

- [1] K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics, pages 1–47. 1997.
- [2] D. Doty, J. H. Lutz, and S. Nandakumar. Finite-state dimension and real arithmetic. *Information and Computation*, 205:1640–1651, 2007.
- [3] R. Downey, D. R. Hirschfeldt, A. Nies, and S. A. Terwijn. Calibrating randomness. *Bulletin of Symbolic Logic*, 12(3):411–491, 2006.

- [4] R. G. Downey and D. Hirschfeldt. *Algorithmic Randomness and Complexity*. Springer-Verlag, 2010.
- [5] S. A. Fenner. Functions that preserve p-randomness. In *Proceedings of the 18th International Symposium on Fundamentals of Computation Theory*, volume 6914 of *Lecture Notes in Computer Science*, pages 336–347, 2011.
- [6] J. H. Lutz. Category and measure in complexity classes. *SIAM Journal on Computing*, 19(6):1100–1131, December 1990.
- [7] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44:220–258, 1992.
- [8] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Theory Retrospective II*, pages 225–260. Springer-Verlag, 1997.
- [9] J. H. Lutz and E. Mayordomo. Dimensions of points in self-similar fractals. *SIAM Journal on Computing*, 38:1080–1112, 2008.
- [10] J. H. Lutz and K. Weihrauch. Connectivity properties of dimension level sets. *Mathematical Logic Quarterly*, 54:483–491, 2008.
- [11] P. Martin-Löf. On the definition of infinite random sequences. *Information and Control*, 9:602–619, 1966.
- [12] D. D. Wall. *Normal Numbers*. PhD thesis, University of California, Berkeley, California, USA, 1949.
- [13] Y. Wang. Resource bounded randomness and computational complexity. *Theoretical Computer Science*, 237:33–55, 2000.