EXTRACTING INFORMATION IS HARD: A TURING DEGREE OF NON-INTEGRAL EFFECTIVE HAUSDORFF DIMENSION

JOSEPH S. MILLER

Abstract. We construct a Δ^0_2 infinite binary sequence with effective Hausdorff dimension $1/2$ that does not compute a sequence of higher dimension. Introduced by Lutz, effective Hausdorff dimension can be viewed as a measure of the information density of a sequence. In particular, the dimension of $A \in 2^\omega$ is the $\liminf$ of the ratio between the information content and length of initial segments of A. Thus the main result demonstrates that it is not always possible to extract information from a partially random source to produce a sequence that has higher information density.

1. Introduction

Question. *Given a sequence that is known to contain, on average, at least one bit of information for every two bits, can we produce a sequence with a higher information density?*

This is an informal statement of a question asked as early as 2000 by Sebastiaan Terwijn and soon after by Jan Reimann; it will be the main focus of this paper. We will eventually give a negative answer to their question. To state it rigorously, we need a way to measure the information density of an infinite binary sequence. It is important to understand that what we mean by *information* in this context is substantially different from the colloquial use the word. It might better be called unpredictability or *randomness*.

One measure of the information content of a finite binary string $\sigma \in 2^{<\omega}$ is its *prefix-free Kolmogorov complexity*[1] $K(\sigma)$. Therefore, a natural measure of the information density of an infinite sequence $A \in 2^\omega$ is its *effective (or constructive) dimension*

$$\dim(A) = \liminf_{n\to\infty} \frac{K(A \upharpoonright n)}{n}.$$

In other words, a sequence of effective dimension $1/2$ is guaranteed to have nearly $n/2$ bits of information in the first n bits, although it can have more for some n. This is not the original definition of effective dimension. That was given by Lutz [12], who effectivized a martingale characterization of Hausdorff dimension and defined $\dim(A)$ to be the effective Hausdorff dimension of $\{A\}$. Note that although

Date: October 20, 2010.

2010 *Mathematics Subject Classification.* Primary 03D32; Secondary 68Q30, 28A78.

The author was supported by the National Science Foundation under grants DMS-0945187 and DMS-0946325, the latter being part of a Focused Research Group in Algorithmic Randomness.

[1] The next section contains a brief review of algorithmic randomness, including prefix-free complexity and Martin-Löf randomness.

the classical Hausdorff dimension of a singleton set is zero, the effective Hausdorff dimension may not be. The equivalence of these two definitions, proved by Mayordomo [15] (but essentially implicit in Ryabko [21]), is evidence that effective dimension is a robust notion. Another indication is that the use of prefix-free complexity in the definition above is unnecessary; replacing it with plain Kolmogorov complexity or monotone complexity would not change the value of the limit inferior.

The question can now be asked more formally.

Question 1.1 (Reimann, Terwijn)**.** If $\dim(A) = 1/2$, does A compute a sequence with higher effective dimension?

It is not hard to show that the effective dimension of the Turing degree of A (the class of all sequences that both compute and are computable from A) is the supremum of the dimensions of all sequences computable from A. Thus a negative answer to Question 1.1 provides the example promised by the title.

Let us start by considering some simple examples. We can produce a random sequence by flipping a coin and assigning 1 and 0 to heads and tails, respectively. With probability 1, the resulting sequence has effective dimension 1 (and is Martin-Löf random). To produce a sequence with effective dimension 1/2, we could use a coin to determine the odd bits and make every even bit 0. Of course, such a sequence is just a dilution of a random sequence and clearly computes a random sequence. Another way to produce a semi-random sequence is to use a biased coin. Classical information theory allows us to calculate, based on the bias, what the effective dimension of the resulting sequence will (almost surely) be. The right choice of bias—in particular, if heads comes up about 89% of the time—will produce a sequence with effective dimension 1/2. As it turns out, using a simple technique described by von Neumann [26], randomness can also be extracted from these sequences. Consider pairs of coin flips; output a 1 if you see HT and a 0 if you see TH. Produce no output for pairs of the form HH or TT. The resulting sequence looks exactly as if it were produced by an unbiased coin.

The sequences in both examples have the property that the information they contain is spread out fairly regularly. To formalize this observation, define the *effective strong dimension* of $A \in 2^\omega$ to be $\operatorname{Dim}(A) = \limsup_{n\to\infty} K(A \upharpoonright n)/n$. Clearly $\operatorname{Dim}(A) \geq \dim(A)$. Athreya, Hitchcock, Lutz and Mayordomo [1] proved that effective strong dimension is the effective analogue of packing dimension, another classical fractal dimension, in the same way that effective dimension is the analogue of Hausdorff dimension. If $A \in 2^\omega$ is a sequence of effective dimension 1/2 obtained either through dilution or from a biased coin, as described above, then $\operatorname{Dim}(A)$ is also 1/2. Bienvenu, Doty and Stephan [2] showed that this is enough to guarantee that A computes sequences of higher effective dimension. Specifically, they proved that if $\varepsilon > 0$ and $\operatorname{Dim}(A) > 0$, then A computes a set B such that $\dim(B) \geq \dim(A)/\operatorname{Dim}(A) - \varepsilon$. So if $\dim(A) = \operatorname{Dim}(A) = 1/2$, then A computes sequences with effective dimension arbitrarily close to 1. (Note that it is open whether such an A must always compute a sequence with effective dimension 1, but it follows from Greenberg and Miller [8] that A need not compute a Martin-Löf random sequence.) The result of Bienvenu et al. demonstrates that any sequence refuting Question 1.1 must be irregular, having periods of nearly random behavior unpredictably followed by periods of relative order.

We mention two other positive results on the problem of extracting information from infinite sequences. Fortnow et al. [7] proved that if $\operatorname{Dim}(A) > 0$, then A

computes sequences with effective strong dimension arbitrarily close to 1 (see also Bienvenu et al. [2]). Secondly, Zimand [27] showed that if $A, B \in 2^\omega$ are sufficiently independent and both have positive effective dimension, then together they compute (in fact, truth-table compute, uniformly in a lower bound on the dimensions) a sequence with effective dimension 1. Of course, the independence assumption plays a significant role. Both papers use ideas from the study of randomness extractors, a subject that is discussed in more detail below.

Attempts to answer Question 1.1 in the negative have also led to interesting results. Kjos-Hanssen, Merkle and Stephan [9] call A *complex* if there is an unbounded, nondecreasing computable function f such that $(\forall n)\ K(A \upharpoonright n) \geq f(n)$. Although a complex sequence can have very low information density, we can effectively find initial segments with as much information as we want. Reimann and Slaman [19], and independently Kjos-Hanssen, et al. [9, Corollary 7], proved that complex sets need not compute Martin-Löf random sequences. Along similar lines, Downey and Greenberg [5] proved that there is an $A \in 2^\omega$ such that $\mathrm{Dim}(A) = 1$ and A has *minimal* (*Turing*) *degree*, meaning that any noncomputable set computed from A must compute A. This property implies that A does not compute a Martin-Löf random sequence. Greenberg and Miller [8] recently constructed a sequence with effective dimension 1 that does not compute a Martin-Löf random sequence. This gives a negative answer to a variant of Question 1.1 that appeared, for example, in the open questions paper of Nies and the author [16].

Another line of attack that yielded partial negative solutions was to place a limit on the type of algorithms used to extract information from A. The first such result was given by Reimann and Terwijn (see [19]) who constructed a Δ^0_2 sequence A with effective dimension $1/2$ such that if B is many-one reducible to A, then $\dim(B) \leq 1/2$. Nies and Reimann later generalized this to weak truth-table reducibility [18]. Many-one and weak truth-table reduction are strong forms of computation; without going into the definitions, the point is that each of these results showed that a certain restricted family of algorithms is not sufficient to distill randomness from a semi-random source.

The result of Nies and Reimann on weak truth-table reducibility was shown to have an interesting consequence by Bienvenu, Doty and Stephan [2]. They proved that there is no *single* algorithm such that, given any sequence A such that $\dim(A) \geq 1/2$, the algorithm always computes a sequence of effective dimension strictly greater than $1/2$.

No summary of the work on extracting information from infinite sequences would be complete without discussing the analogous problem for finite strings. One result of interest is that of Vereshchagin and Vyugin [25, Theorem 4] on the impossibility of condensing the information in a string with high Kolmogorov complexity. They construct a long string $x \in 2^{<\omega}$ with high Kolmogorov complexity such that any short string that is simple relative to x is unconditionally simple. Moving beyond algorithmic information theory, there is a large body of work on randomness extractors, much of which is surveyed by Shaltiel [23]. The usual assumption is that you are given a distribution on 2^n with a certain guaranteed *min-entropy*, which simply means that no element of 2^n is too likely. Intuitively, the min-entropy is a lower bound on the information content of any output generated by the distribution. The goal is to map 2^n to a smaller space, independently of the distribution, in such a way that the induced distribution is nearly uniform. In other words, composing the distribution with the map essentially produces a random source. Sántha and Vazirani [22] observed that this ideal goal cannot be met with a single source, but proved that extraction can be done with several independent sources. The fact that two independent sources were sufficient was proved soon after by Vazirani [24]. The analogy with infinite sequences is clear and, as we have pointed out, the study of randomness extractors has been applied to variants of Question 1.1 [7, 27].

Outline. In the next section we give a brief overview of the notation and concepts that will be used throughout the paper, focusing on notions from algorithmic randomness. Section 3 introduces *weight* and *optimal covers* and describes the forcing conditions that are used in Section 4 to give a negative answer to Question 1.1. The proof of our main result is an oracle construction, relative to the halting set $\emptyset'$, but it can be viewed as forcing construction where the conditions are Π^0_1 classes of a specific form. Several lemmas in Section 3 establish the basic properties of these classes, including the fact that they all have positive measure and their measures have effective Hausdorff dimension at most 1/2.

2. Preliminaries

The reader is presumed to have some knowledge of basic computability theory (recursion theory). In particular, the terms *computable*, *computably enumerable* (*c.e.*), *Turing reduction* ($\leq_T$), and *Turing functional* will be used without explanation. By Δ^0_2 we mean computable from $\emptyset'$, the halting problem. Elements of $2^{<\omega}$ will be referred to as (finite binary) *strings* and elements of 2^ω will be referred to as (infinite binary) *sequences*. If $\sigma \in 2^{<\omega}$, we let $[\sigma]^{<\omega} = \{\tau \in 2^{<\omega} \colon \sigma \preccurlyeq \tau\}$, in other words, the strings extending σ. Similarly, we let $[\sigma] = \{A \in 2^\omega \colon \sigma \prec A\}$. For $S \subseteq 2^{<\omega}$, we define $[S]^{<\omega} = \bigcup_{\sigma\in S}[\sigma]^{<\omega}$ and $[S] = \bigcup_{\sigma\in S}[\sigma]$. We treat 2^ω as Cantor space; the sets of the form $[\sigma]$ are a clopen basis for the topology and every open set is of the form $[S]$, for some $S \subseteq 2^{<\omega}$. If $S \subseteq 2^{<\omega}$ is a c.e. set, then $[S]$ is called a Σ^0_1 *class*. These are the effectively open subsets of Cantor space. The complement of a Σ^0_1 class is called a Π^0_1 *class*. Finally, we use μ to denote the Lebesgue measure on Cantor space determined by setting $\mu([\sigma]) = 2^{-|\sigma|}$, for each $\sigma \in 2^{<\omega}$.

Algorithmic randomness. An introduction to algorithmic randomness can be found in the upcoming monographs of Downey and Hirschfeldt [4] and Nies [17] or the excellent survey paper of Downey, Hirschfeldt, Nies and Terwijn [6]. Li and Vitányi [11] is another useful source, although it does not cover effective dimension.

One common approach to measuring the information content of binary strings is *prefix-free complexity*, as introduced by Levin [10] and Chaitin [3]. Call $S \subseteq 2^{<\omega}$ *prefix-free* if no element of S is a proper prefix of anther element. A *prefix-free machine* $M \colon 2^{<\omega} \to 2^{<\omega}$ is a partial computable function whose domain is prefix-free. We say that U is a *universal* prefix-free machine iff for any other prefix-free machine M, there is a $\tau \in 2^{<\omega}$ such that $(\forall\sigma)\ U(\tau\sigma) = M(\sigma)$. It is not difficult to prove that a universal machine U exists; fix such a machine. This U will automatically be *effectively universal* in the sense that if we know an index for a prefix-free machine M, then we can compute the τ by which U simulates M.

The Kolmogorov complexity of $\sigma \in 2^{<\omega}$ with respect to a (prefix-free) machine M is defined to be $K_M(\sigma) = \min\{|\tau| \colon M(\tau) = \sigma\}$, the length of the shortest M-program for σ. The *prefix-free complexity* of σ is $K(\sigma) = K_U(\sigma)$. The effective universality of U implies that, given any prefix-free machine M, we can find a

$d \in \omega$ such that $(\forall \sigma)\ K(\sigma) \le K_M(\sigma) + d$. Having a notion of complexity for finite strings, we can study infinite sequences by looking at the complexity of their initial segments. The most well-known property defined along these lines is *Martin-Löf randomness*. A sequence $A \in 2^\omega$ is Martin-Löf random (often called 1-*random*) if the initial segments of A are not compressible by more than some fixed constant. In other words, there is a $c \in \omega$ such that $(\forall n)\ K(A \restriction n) \ge n - c$. Note that this was not the definition given by Martin-Löf; it was proposed independently by Levin [10] and Chaitin [3] and proved by Schnorr to be equivalent to Martin-Löf's definition of randomness [14].

Another notion characterized in terms of initial segment complexity is effective dimension. A thorough survey of effective dimension is given by Lutz [13]. As stated in the introduction, the *effective (Hausdorff) dimension* of $A \in 2^\omega$ is $\dim(A) = \liminf_{n\to\infty} K(A \restriction n)/n$ and the *effective strong dimension* is $\mathrm{Dim}(A) = \limsup_{n\to\infty} K(A \restriction n)/n$. Note that $0 \le \dim(A) \le \mathrm{Dim}(A) \le 1$ and that these are the only restrictions on effective dimension [1]. Also note that if A is Martin-Löf random, then $\dim(A) = 1$. It is not hard to show that the converse fails. For $X \in [0, 1]$, we define $\dim(X)$ to be the effective dimension of the binary expansion of X. An alternate characterization can be given in terms of *Solovay* s*-tests*. Let T be a computably enumerable collection of rational subintervals of $[0, 1]$. Then T is a Solovay s-test if $\sum_{I\in T} |I|^s$ is finite. We say that X is covered by T if infinitely many $I \in T$ contain X. Reimann [19] showed that $\dim(X) = \inf\{s \ge 0 \colon X \text{ is covered by a Solovay } s\text{-test}\}$.

3. Weight, optimal covers, and the forcing conditions

Definition 3.1. Let $S \subseteq 2^{<\omega}$. Define the *direct weight* of S to be $\mathrm{DW}(S) = \sum_{\sigma\in S} 2^{-|\sigma|/2}$. The *weight* of S is

$$\mathrm{W}(S) = \inf \{\mathrm{DW}(V) \colon [S] \subseteq [V]\}.$$

Note that $W(S) \le 1$ because $[S] \subseteq [\{\lambda\}]$ and $\mathrm{DW}(\{\lambda\}) = 1$, where λ is the string of length zero. The weight of S is *essentially*[2] the minimum cost of compressing some initial segment of every sequence in $[S]$ by a factor of 2. Of course, there is no reason to think that this compression could be realized effectively. In other words, even if S is c.e., there may not be a prefix-free machine M compressing each sequence in $[S]$ by a factor of 2 and such that the measure of the domain of M is close to $W(S)$.

Assume that S is finite. Consider $V \subseteq 2^{<\omega}$ such that $[S] \subseteq [V]$. It is suboptimal for V to contain any string incomparable with every $\sigma \in S$ or to contain a proper extension of some $\sigma \in S$. In other words, it is always possible to find a $\widehat{V} \subseteq 2^{<\omega}$ such that $[S] \subseteq [\widehat{V}]$, $\mathrm{DW}(\widehat{V}) \le \mathrm{DW}(V)$, and $\tau \in \widehat{V}$ implies that $(\exists \sigma \in S)\ \tau \preccurlyeq \sigma$. Therefore, there are only finitely many V that need to be considered in the infimum. Hence the infimum is achieved, justifying the following definition when $S \subseteq 2^{<\omega}$ is finite.

Definition 3.2. The *optimal cover* of $S \subseteq 2^{<\omega}$ is a set $S^{oc} \subseteq 2^{<\omega}$ such that $[S] \subseteq [S^{oc}]$ and $\mathrm{DW}(S^{oc}) = \mathrm{W}(S)$. For the sake of uniqueness, we also require $[S^{oc}]$ to have the minimum measure among all possible contenders.

[2] The difference is that descriptions cannot have fractional length, so to compress a string of length 9 by a factor of 2 requires giving it a description of length at most 4. The cost of such a description is at least 2^{-4}, not $2^{-4.5}$.

Clearly, optimal covers are unique and prefix-free. The analysis above shows that when S is finite, we can compute both the optimal cover of S and $\mathrm{W}(S)$.

Examples. First let $S = \{00, 01\}$. Note that the direct weight of S is 1, but that this is not optimal. Instead, $S^{oc} = \{0\}$ and $\mathrm{W}(S) = \sqrt{2}$.

Now consider $S = \{00, 10\}$. It is not hard to see that $\mathrm{W}(S) = \mathrm{DW}(S) = 1$. Two different covers of S achieve this weight: $\{\lambda\}$ and S itself. Therefore, $S^{oc} = S$, since this is the choice that minimizes $\mu([S^{oc}])$.

We turn to the case when $S \subseteq 2^{<\omega}$ is infinite. Let $\{S_t\}_{t\in\omega}$ be an enumeration of S, i.e., an increasing sequence of finite sets such that $S = \bigcup_{t\in\omega} S_t$. Note that if $\sigma \in S_t^{oc}$, then the only way for σ to not be in S_{t+1}^{oc} is for some $\tau \prec \sigma$ to be in S_{t+1}^{oc}. This has some nice consequences. First, it implies a *nesting property*: $[S_t^{oc}] \subseteq [S_{t+1}^{oc}]$, for all t. Second, it proves that the S_t^{oc} have a pointwise limit V. It is not hard to see that $V = S^{oc}$, demonstrating that the definition above is valid for any $S \subseteq 2^{<\omega}$.

In the case that S is c.e., its optimal cover S^{oc} is clearly Δ^0_2. More importantly, the nesting property implies that $[S^{oc}]$ is a Σ^0_1 class. There will not generally be a c.e. set $V \subseteq 2^{<\omega}$ such that $[S^{oc}] = [V]$ and $DW(V) = W(S)$, or even such that the direct weight of V is finite. However, we can find such a V for which the direct weight of any prefix-free subset is bounded by $W(S)$.

Lemma 3.3. *For any c.e. set $S \subseteq 2^{<\omega}$, we can (effectively) find a c.e. $V \subseteq 2^{<\omega}$ such that $[V] = [S^{oc}]$ and if $P \subseteq V$ is prefix-free, then* $\mathrm{DW}(P) \le \mathrm{W}(S)$.

Proof. Let $\{S_t\}_{t\in\omega}$ be an enumeration of S. Define $V = \bigcup_{t\in\omega} S_t^{oc}$. Note that V is c.e. and $[V] = [S^{oc}]$. If there were an infinite prefix-free $P \subseteq V$ such that $\mathrm{DW}(P) > \mathrm{W}(S)$, then there would be a finite $P' \subset P$ with the same property. So assume that $P \subseteq V$ is finite and prefix-free. We will prove the following claim: if $\tau \in V$, then $\mathrm{DW}(P \cap [\tau]^{<\omega}) \le \mathrm{DW}(\{\tau\})$. This will be proved by induction on the distance k from τ to its longest extension in P (the claim is trivial if $P \cap [\tau]^{<\omega}$ is empty). The case $k = 0$ is immediate. Now take $\tau \in V \smallsetminus P$. There is a unique t such that $\tau \in S_{t+1}^{oc} \smallsetminus S_t^{oc}$; so $\mathrm{DW}(S_t^{oc} \cap [\tau]^{<\omega}) \le \mathrm{DW}(\{\tau\})$, or else we would have $\tau \in S_t^{oc}$. The nesting property implies that $[S_t^{oc}] \cap [\tau]$ covers $[P] \cap [\tau]$, since every element of $P \cap [\tau]^{<\omega}$ must have entered V by stage t. Hence, applying the inductive hypothesis to the elements of $S_t^{oc} \cap [\tau]^{<\omega}$, we have $\mathrm{DW}(P \cap [\tau]^{<\omega}) \le \mathrm{DW}(S_t^{oc} \cap [\tau]^{<\omega})$. This proves the claim. Of course, $[S^{oc}]$ covers $[P]$, so $\mathrm{DW}(P) \le \mathrm{DW}(S^{oc}) = \mathrm{W}(S)$. □

It is worth noting that the previous lemma can be used to give a direct proof that *strong s-randomness* implies *vehement s-randomness*, for $s \in [0, 1]$, which follows from results of Kjos-Hanssen and Reimann. (Although we have specialized to the case $s = 1/2$, the proof works generally.) Kjos-Hanssen showed that *s-capacitability* implies vehement s-randomness, which together with Reimann's result that strong s-randomness implies s-capacitability, proves that all three notions are the same. See [20] for the relevant definitions and proofs.

The forcing conditions. In the proof of Theorem 4.1 we will build a set A by approximations. As usual, the type of approximation—or in terminology borrowed from set theory, the type of *forcing condition*—determines the nature of the requirements that we can satisfy during the construction. Our conditions will be pairs $\langle \sigma, S\rangle$ such that $\sigma \in 2^{<\omega}$, $S \subseteq [\sigma]^{<\omega}$ is a c.e. set, and $\sigma \notin S^{oc}$. A condition describes a restriction on the sequence A that is being constructed. Specifically, the set of all sequences consistent with a condition $\langle\sigma, S\rangle$ is the Π^0_1 class $P_{\langle\sigma,S\rangle} = [\sigma] \smallsetminus [S^{oc}]$. Our definition of condition guarantees that $P_{\langle\sigma,S\rangle}$ is nonempty. We say that a condition $\langle\tau, T\rangle$ *extends* $\langle\sigma, S\rangle$ and write $\langle\tau, T\rangle \preccurlyeq \langle\sigma, S\rangle$ iff $P_{\langle\tau,T\rangle} \subseteq P_{\langle\sigma,S\rangle}$. This corresponds, of course, to further restricting the possibilities for A.

We prove several basic lemmas about our forcing conditions. The first shows that there is a forcing condition $\langle\lambda, S\rangle$ such that every element of $P_{\langle\lambda,S\rangle}$ has effective dimension at least 1/2. Recall that λ denotes the string of length zero.

Lemma 3.4. *Let $S = \{\sigma \in 2^{<\omega} \colon K(\sigma) \leq |\sigma|/2\}$. Then $\langle\lambda, S\rangle$ is a valid condition.*

Proof. All that needs to be shown is that $\lambda \notin S^{oc}$. But if this were the case, then $\mathrm{DW}(S) \geq \mathrm{W}(S) = 1$. On the other hand, $\mathrm{DW}(S) = \sum_{\sigma\in S} 2^{-|\sigma|/2} \leq \sum_{\sigma\in S} 2^{-K(\sigma)} < \sum_{\sigma\in 2^{<\omega}} 2^{-K(\sigma)} \leq 1$, where the strict inequality follows from the fact that $S \neq 2^{<\omega}$. □

The next two lemmas show that the Π^0_1 class corresponding to a condition has positive measure and that the effective Hausdorff dimension of its measure is at most 1/2.

Lemma 3.5. *Let $\sigma \in 2^{<\omega}$ and $S \subseteq [\sigma]^{<\omega}$. If $[\sigma] \smallsetminus [S^{oc}]$ is nonempty, then it has positive measure.*

Proof. Let $n = |\sigma|$. The fact that $[S] \subseteq [\sigma]$ implies that $\mathrm{W}(S) \leq 2^{-n/2}$. Since $[\sigma] \smallsetminus [S^{oc}]$ is nonempty, we know that $\sigma \notin S^{oc}$. Hence $\tau \in S^{oc}$ implies that $|\tau| > n$. Using these observations,

$$\begin{aligned}\mu([S^{oc}]) = \sum_{\tau\in S^{oc}} 2^{-|\tau|} < \sum_{\tau\in S^{oc}} 2^{-|\tau|/2-n/2} &= 2^{-n/2} \sum_{\tau\in S^{oc}} 2^{-|\tau|/2} \\ &= 2^{-n/2}\,\mathrm{DW}(S^{oc}) = 2^{-n/2}\,\mathrm{W}(S) \leq 2^{-n}.\end{aligned}$$

Therefore, $\mu([\sigma] \smallsetminus [S^{oc}]) > 0$. □

Lemma 3.6. *Let $\langle\sigma, S\rangle$ be a condition. Then $\dim(\mu(P_{\langle\sigma,S\rangle})) \leq 1/2$.*

Proof. We prove that $\dim(\mu([S^{oc}])) \leq 1/2$, which is sufficient because $\mu(P_{\langle\sigma,S\rangle}) = 2^{-|\sigma|} - \mu([S^{oc}])$. We may assume, without loss of generality, that S^{oc} is infinite, since otherwise $\mu([S^{oc}])$ is rational. Let $w = \mathrm{W}(S)$. Let $V \subseteq 2^{<\omega}$ be the c.e. set guaranteed by Lemma 3.3; so $[V] = [S^{oc}]$ and $\mathrm{DW}(P) \leq w$ whenever $P \subseteq V$ is prefix-free. Note that V must be infinite. Let $\{V_t\}_{t\in\omega}$ be an effective enumeration of V such that $V_0 = \emptyset$.

Fix $s > 1/2$. We produce a Solovay s-test T covering $\mu([V])$. It consists of two parts. The first part, T_0, attempts to cover $\mu([V])$ whenever a string τ enters V; it succeeds as long as no string as short as τ enters V at a later stage *and* longer strings do not eventually contribute too much to $\mu([V])$. While the first assumption is met for the right choice of τ, the second assumption may not be met. The role of T_1, the second part of the Solovay test, is to keep trying to cover $\mu([V])$ when the second assumption fails.

- If $\tau \in V_{t+1} \smallsetminus V_t$, then put $\big[\mu([V_{t+1}]), \mu([V_{t+1}]) + 2^{-|\tau|}\big]$ into T_0.
- If $\mu([V_t \cap 2^{>n}]) \leq k2^{-n}$ and $\mu([V_{t+1} \cap 2^{>n}]) > k2^{-n}$ for some $n, k \in \omega$, then put $[\mu([V_{t+1}]), \mu([V_{t+1}]) + 2^{-n}]$ into T_1.

This ensures that $T = T_0 \cup T_1$ is a c.e. set of rational intervals. Note that T does not actually depend on s. Using the fact that $V \cap 2^n$ is prefix-free, we have

$$\sum_{I \in T_0} |I|^s = \sum_{\tau \in V} 2^{-s|\tau|} = \sum_{n \in \omega} 2^{-sn} |V \cap 2^n| = \sum_{n \in \omega} 2^{(1/2-s)n} 2^{-n/2} |V \cap 2^n|$$
$$= \sum_{n \in \omega} 2^{(1/2-s)n} \operatorname{DW}(V \cap 2^n) \leq \sum_{n \in \omega} 2^{(1/2-s)n} w = \frac{w}{1 - 2^{1/2-s}} < \infty.$$

Now fix $n \in \omega$ and let k be the number of intervals of length 2^{-n} added to T_1. By construction, $2^{-n}k < \mu([V \cap 2^{>n}])$. Let $P \subseteq V \cap 2^{>n}$ be a prefix-free set such that $[P] = [V \cap 2^{>n}]$. Then by the same argument as in the previous lemma, $\mu([P]) < 2^{-n/2} \operatorname{DW}(P)$. Putting it all together we have $2^{-n}k < 2^{-n/2} \operatorname{DW}(P) \leq 2^{-n/2} w$, so $k < 2^{n/2} w$. Thus

$$\sum_{I \in T_1} |I|^s < \sum_{n \in \omega} 2^{n/2} w (2^{-n})^s = \sum_{n \in \omega} 2^{(1/2-s)n} w < \infty.$$

This proves that T is a Solovay s-test.

Next we prove that T covers $\mu([V])$. Call $\tau \in V_{t+1} \setminus V_t$ *timely* if $V_{t+1} \cap 2^{\leq |\tau|} = V \cap 2^{\leq |\tau|}$, in other words, if only strings longer than τ enter V after τ. Because V is infinite, there are infinitely many timely $\tau \in V$; fix one. Let $t+1$ be the stage that τ enters V and let $n = |\tau|$. We claim that there is an interval of length 2^{-n} in T that contains $\mu([V])$. Note that if $u > t$, then $\mu([V]) - \mu([V_u]) \leq \mu([V \cap 2^{>n}]) - \mu([V_u \cap 2^{>n}])$. In response to τ entering V, we put the interval $[\mu([V_{t+1}]), \mu([V_{t+1}]) + 2^{-n}]$ into $T_0 \subseteq T$ at stage $t+1$. Let $I = [\mu([V_u]), \mu([V_u]) + 2^{-n}]$ be the last interval of length 2^{-n} added to T. If $\mu([V]) \notin I$, then $\mu([V]) > \mu([V_u]) + 2^{-n}$. Since $u > t$, we have $\mu([V \cap 2^{>n}]) > \mu([V_u \cap 2^{>n}]) + 2^{-n}$, so another interval of length 2^{-n} is added to $T_1 \subseteq T$ after stage u. This is a contradiction, so $\mu([V]) \in I$. We have proved that for any n that is the length of a timely element of V, there is an interval of length 2^{-n} in T that contains $\mu([V])$. Since there are infinitely many timely strings, $\mu([V])$ is covered by T.

Since T is a Solovay s-test for every $s > 1/2$, we have shown that $\dim(\mu([V])) \leq 1/2$. But $[V] = [S^{oc}]$, so this completes the proof. ☐

By applying the method of Theorem 4.1 to the identity functional, it can be proved that if $\langle \sigma, S \rangle$ extends the condition from Lemma 3.4, then $\dim\left(\mu\left(P_{\langle \sigma, S \rangle}\right)\right) \geq 1/2$. Hence, Lemma 3.6 is tight. We will not use this observation, so the details are omitted.

The final lemma gives a simple hypothesis on a collection of conditions that guarantees that they have a common extension.

Lemma 3.7. *Assume that $\langle \sigma_0, S_0 \rangle, \ldots, \langle \sigma_n, S_n \rangle$ is a sequence of conditions such that $P_{\langle \sigma_0, S_0 \rangle} \cap \cdots \cap P_{\langle \sigma_n, S_n \rangle}$ has positive measure. Then there is a condition $\langle \tau, T \rangle$ such that $\langle \tau, T \rangle \preccurlyeq \langle \sigma_i, S_i \rangle$, for each $0 \leq i \leq n$.*

Proof. The σ_i are comparable by hypothesis, so let $\sigma = \sigma_0 \cup \cdots \cup \sigma_n$. Let $P = P_{\langle \sigma_0, S_0 \rangle} \cap \cdots \cap P_{\langle \sigma_n, S_n \rangle} = [\sigma] \setminus [S_0^{oc} \cup \cdots \cup S_n^{oc}]$. In particular, $P \subseteq [\sigma]$. It is not necessarily the case that P corresponds to a condition. Instead, it is quite possible that $(S_0^{oc} \cup \cdots \cup S_n^{oc})^{oc}$ contains σ. However, we will show that there is a condition $\langle \tau, T_\tau \rangle$ such that $P_{\langle \tau, T_\tau \rangle} \subseteq P$.

Choose $b \in \omega$ such that $\mu(P) \geq 2^{-b}$. Take $m \geq b$ and define

$$D_m = \{\tau \succcurlyeq \sigma \colon |\tau| = m \text{ and no prefix of } \tau \text{ is in } S_i^{oc} \text{ for any } 0 \leq i \leq n\}.$$

Now $\mu(P) \leq |D_m| 2^{-m}$, because if $\tau \in 2^m$ is not in D_m, then $[\tau]$ is disjoint from $[P]$. Hence $|D_m| \geq 2^{m-b}$.

Take $\tau \in D_m$ and let $T_\tau = [\tau]^{<\omega} \cap (S_0^{oc} \cup \cdots \cup S_n^{oc})$. If $\tau \notin T_\tau^{oc}$, then $\langle \tau, T_\tau \rangle$ is the condition required by the lemma. On the other hand, $\tau \in T_\tau^{oc}$ implies that $\mathrm{DW}(T_\tau) \geq \mathrm{W}(T_\tau) = 2^{-m/2}$. So assuming that $\tau \in T_\tau^{oc}$ for each $\tau \in D_m$:

$$n+1 \geq \sum_{0 \leq i \leq n} \mathrm{W}(S_i) = \sum_{0 \leq i \leq n} \mathrm{DW}(S_i^{oc}) \geq \mathrm{DW}(S_0^{oc} \cup \cdots \cup S_n^{oc})$$
$$\geq \sum_{\tau \in D_m} \mathrm{DW}(T_\tau) \geq \sum_{\tau \in D_m} 2^{-m/2} \geq 2^{m-b} 2^{-m/2} = 2^{m/2-b}.$$

But $m \geq b$ was arbitrary, so we have a contradiction. □

Note that $\emptyset'$ can find the common extension guaranteed by the lemma.

4. The counterexample

We prove the main result.

Theorem 4.1. *There is an* $A \leq_T \emptyset'$ *such that* $\dim(A) = 1/2$ *and if* $B \leq_T A$*, then* $\dim(B) \leq 1/2$*.*

Proof. We build a sequence of conditions $\langle \sigma_0, S_0 \rangle \succcurlyeq \langle \sigma_1, S_1 \rangle \succcurlyeq \langle \sigma_2, S_2 \rangle \succcurlyeq \cdots$ and take $A = \bigcup_t \sigma_t$, which will be total. Equivalently, A will be the unique element of $\bigcap_t P_{\langle \sigma_t, S_t \rangle}$. The construction will be carried out with a $\emptyset'$ oracle, so $A \leq_T \emptyset'$. We take $\langle \sigma_0, S_0 \rangle$ to be the condition from Lemma 3.4. This guarantees that $\dim(A) \geq 1/2$, because this is true of every element of $P_{\langle \sigma_0, S_0 \rangle}$.

Let $\{\Psi_e\}_{e \in \omega}$ be an effective enumeration of the partial computable functionals. For all $e, n \in \omega$, we must meet the requirement

$$R_{e,n}\colon \text{ if } \Psi_e^A \text{ is total, then } (\exists k > n)\; K(\Psi_e^A \upharpoonright k) \leq (1/2 + 2^{-n})k.$$

These requirements guarantee that if $B \leq_T A$, then $\dim(B) \leq 1/2$. In particular, $\dim(A) = 1/2$.

Stage $t = 0$. Take $\langle \sigma_0, S_0 \rangle$ to be the condition from Lemma 3.4.

Stage $t + 1 = \langle e, n \rangle$ *(we satisfy* $R_{e,n}$*).* Choose $b \in \omega$ such that $2^{-b} < \mu(P_{\langle \sigma_t, S_t \rangle})$. Note that b exists by Lemma 3.5 and can be found using $\emptyset'$ because the set $\{r \in \mathbb{Q} \colon \mu(P) < r\}$ is Σ_1^0 uniformly in an index for a Π_1^0 class P. We define a prefix-free machine M. The idea will be that M waits for a large set of oracles that appear to be in $P_{\langle \sigma_t, S_t \rangle}$ to compute the same sufficiently long initial segment via Ψ_e and then compresses that initial segment.

We define $M(\rho)$ for $\rho \in 2^{<\omega}$ as follows. First, wait until $U(\rho)\downarrow$. If this never happens, then $M(\rho)\uparrow$. So the domain of M is a subset of the domain of U, hence prefix-free. Let $\sigma = U(\rho)$ and $m = |\sigma|$. The only case that will be of interest will be when σ is an initial segment of the binary expansion of $\mu(P_{\langle \sigma_t, S_t \rangle})$.[3] We write $.\sigma$ for the dyadic rational whose binary expansion, after the radix point, is $\sigma 0^\omega$. To each $\tau \in 2^{<\omega}$ we associate a c.e. set $T_\tau = \{\nu \succcurlyeq \sigma_t \colon \tau \preccurlyeq \Psi_e^\nu\}$. Now search for a $\tau \in 2^{m-b}$ such that $\mu(P_{\langle \sigma_t, S_t \cup T_\tau \rangle}) < .\sigma$; this is a Σ_1^0 condition, so if it is true, we will eventually find out. For the first such τ found, let $M(\rho) = \tau$. This completes the definition of M.

[3]If $\mu(P_{\langle \sigma_t, S_t \rangle})$ is a dyadic rational—which it is not—either expansion will do.

We can effectively find a $c \in \omega$ such that $(\forall \tau)\ K(\tau) \leq K_M(\tau) + c$. Now $\emptyset'$ can search for a $\sigma \in 2^{<\omega}$ such that σ is an initial segment of the binary expansion of $\mu(P_{\langle \sigma_t, S_t \rangle})$ of length $m > n + b$, and $K(\sigma) + c \leq (1/2 + 2^{-n})(m - b)$. Such a σ must exist by Lemma 3.6. Let ρ be a minimal U-program for σ. The construction breaks into two cases, depending on whether $M(\rho)$ converges (which $\emptyset'$ can determine, of course).

Case 1: $M(\rho) \downarrow = \tau$. In this case, we know that $\mu(P_{\langle \sigma_t, S_t \cup T_\tau \rangle}) < .\sigma$ and $\mu(P_{\langle \sigma_t, S_t \rangle}) \geq .\sigma$. Thus $P_{\langle \sigma_t, S_t \rangle} \smallsetminus P_{\langle \sigma_t, S_t \cup T_\tau \rangle} = [(S_t \cup T_\tau)^{oc}] \smallsetminus [S_t^{oc}]$ is nonempty. So there is a $\sigma_{t+1} \in T_\tau$ such that $[\sigma_{t+1}] \nsubseteq [S_t^{oc}]$; otherwise S_t^{oc} would be the optimal cover of $(S_t \cup T_\tau)^{oc}$. Note that $\emptyset'$ can find such a σ_{t+1}. By definition, $\sigma_{t+1} \not\succcurlyeq \sigma_t$; since T_τ is closed upwards, we may additionally require that σ_{t+1} properly extends σ_t. Let $S_{t+1} = [\sigma_{t+1}]^{<\omega} \cap S_t$. Since no prefix of σ_{t+1} is in S_t^{oc}, we have $S_{t+1}^{oc} = [\sigma_{t+1}]^{<\omega} \cap S_t^{oc}$. This implies that $P_{\langle \sigma_{t+1}, S_{t+1} \rangle} = [\sigma_{t+1}] \cap P_{\langle \sigma_t, S_t \rangle} \neq \emptyset$. Thus $\langle \sigma_{t+1}, S_{t+1} \rangle$ is a valid condition and $P_{\langle \sigma_{t+1}, S_{t+1} \rangle} \subseteq P_{\langle \sigma_t, S_t \rangle}$, so $\langle \sigma_{t+1}, S_{t+1} \rangle \preccurlyeq \langle \sigma_t, S_t \rangle$.

To verify that $R_{\langle e,n \rangle}$ has been satisfied, take $A \in P_{\langle \sigma_{t+1}, S_{t+1} \rangle}$. Since $\sigma_{t+1} \preccurlyeq A$ and $\sigma_{t+1} \in T_\tau$, we see that $\tau \preccurlyeq \Psi_e^A$. Let $k = |\tau| = m - b$, which is larger than n by our choice of σ. Then

$$\begin{aligned} K(\Psi_e^A \upharpoonright k) = K(\tau) \leq K_M(\tau) + c \leq |\rho| + c = K(\sigma) + c \\ \leq (1/2 + 2^{-n})(m - b) = (1/2 + 2^{-n})k. \end{aligned}$$

Case 2: $M(\rho) \uparrow$. In this case, $\mu(P_{\langle \sigma_t, S_t \cup T_\tau \rangle}) \geq .\sigma$ for each $\tau \in 2^{m-b}$. Thus $\langle \sigma_t, S_t \cup T_\tau \rangle$ is a valid condition extending $\langle \sigma_t, S_t \rangle$. Furthermore, since $P_{\langle \sigma_t, S_t \cup T_\tau \rangle} \subseteq P_{\langle \sigma_t, S_t \rangle}$ and $\mu(P_{\langle \sigma_t, S_t \rangle}) \leq .\sigma + 2^{-m}$, we have $\mu(P_{\langle \sigma_t, S_t \rangle} \smallsetminus P_{\langle \sigma_t, S_t \cup T_\tau \rangle}) \leq 2^{-m}$. So

$$\begin{aligned} \mu\left(\bigcap_{\tau \in 2^{m-b}} P_{\langle \sigma_t, S_t \cup T_\tau \rangle}\right) &= \mu\left(P_{\langle \sigma_t, S_t \rangle} \smallsetminus \bigcup_{\tau \in 2^{m-b}} (P_{\langle \sigma_t, S_t \rangle} \smallsetminus P_{\langle \sigma_t, S_t \cup T_\tau \rangle})\right) \\ &\geq \mu(P_{\langle \sigma_t, S_t \rangle}) - \sum_{\tau \in 2^{m-b}} \mu(P_{\langle \sigma_t, S_t \rangle} \smallsetminus P_{\langle \sigma_t, S_t \cup T_\tau \rangle}) > 2^{-b} - 2^{m-b} 2^{-m} = 0. \end{aligned}$$

Thus by Lemma 3.7, there is a condition $\langle \sigma_{t+1}, S_{t+1} \rangle$ that extends $\langle \sigma_t, S_t \cup T_\tau \rangle$ for every $\tau \in 2^{m-b}$. A fortiori, $\langle \sigma_{t+1}, S_{t+1} \rangle \preccurlyeq \langle \sigma_t, S_t \rangle$. Furthermore, $\emptyset'$ can find $\langle \sigma_{t+1}, S_{t+1} \rangle$ and we may assume, without loss of generality, that σ_{t+1} properly extends σ_t.

To verify that $R_{\langle e,n \rangle}$ is satisfied in this case as well, assume that Ψ_e^A is total and let $\tau = \Psi_e^A \upharpoonright (m-b)$. Since $\sigma_t \preccurlyeq A$, some $\rho \preccurlyeq A$ is in T_τ. Therefore, $A \in [(S_t \cup T_\tau)^{oc}]$ and hence $A \notin P_{\langle \sigma_t, S_t \cup T_\tau \rangle} \supseteq P_{\langle \sigma_{t+1}, S_{t+1} \rangle}$.

End of Construction.

Let $A = \bigcup_t \sigma_t$. This is total because we ensured that σ_{t+1} properly extended σ_t, for every $t \in \omega$. The construction was done relative to $\emptyset'$, so A is Δ_2^0. The remainder of the verification was given above. □

Acknowledgments

The author has discussed the problem of building a sequence of positive effective dimension that does not compute a Martin-Löf random (or indeed, a sequence of higher dimension) with many people over the last few years. Particular thanks go to George Barmpalias, Noam Greenberg, Andy Lewis, and Antonio Montalbán, with whom the author first discussed his idea of forcing with Π_1^0 classes whose measures

have effective dimension 1/2. It is this idea that eventually led to the solution of Question 1.1.

References

[1] Krishna B. Athreya, John M. Hitchcock, Jack H. Lutz, and Elvira Mayordomo. Effective strong dimension in algorithmic information and computational complexity. In *STACS 2004*, volume 2996 of *Lecture Notes in Comput. Sci.*, pages 632–643. Springer, Berlin, 2004.

[2] Laurent Bienvenu, David Doty, and Frank Stephan. Constructive dimension and Turing degrees. *Theory Comput. Syst.*, 45(4):740–755, 2009.

[3] Gregory J. Chaitin. A theory of program size formally identical to information theory. *J. Assoc. Comput. Mach.*, 22:329–340, 1975.

[4] R. Downey and D. Hirschfeldt. *Algorithmic randomness and complexity.* Springer-Verlag, Berlin. To appear.

[5] Rod Downey and Noam Greenberg. Turing degrees of reals of positive effective packing dimension. *Inform. Process. Lett.*, 108(5):298–303, 2008.

[6] Rod Downey, Denis R. Hirschfeldt, André Nies, and Sebastiaan A. Terwijn. Calibrating randomness. *Bull. Symbolic Logic*, 12(3):411–491, 2006.

[7] Lance Fortnow, John M. Hitchcock, A. Pavan, N. V. Vinodchandran, and Fengming Wang. Extracting Kolmogorov complexity with applications to dimension zero-one laws. In *Automata, languages and programming. Part I*, volume 4051 of *Lecture Notes in Comput. Sci.*, pages 335–345. Springer, Berlin, 2006.

[8] Noam Greenberg and Joseph S. Miller. Diagonally non-recursive functions and effective Hausdorff dimension. To appear.

[9] Bjørn Kjos-Hanssen, Wolfgang Merkle, and Frank Stephan. Kolmogorov complexity and the recursion theorem. In *STACS 2006*, volume 3884 of *Lecture Notes in Comput. Sci.*, pages 149–161. Springer, Berlin, 2006.

[10] L. A. Levin. Laws of information conservation (non-growth) and aspects of the foundation of probability theory. *Problems Inform. Transmission*, 10(3):206–210, 1974.

[11] M. Li and P. Vitányi. *An introduction to Kolmogorov complexity and its applications.* Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993.

[12] Jack H. Lutz. Gales and the constructive dimension of individual sequences. In *Automata, languages and programming (Geneva, 2000)*, volume 1853 of *Lecture Notes in Comput. Sci.*, pages 902–913. Springer, Berlin, 2000.

[13] Jack H. Lutz. Effective fractal dimensions. *Math. Log. Q.*, 51(1):62–72, 2005.

[14] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

[15] Elvira Mayordomo. A Kolmogorov complexity characterization of constructive Hausdorff dimension. *Inform. Process. Lett.*, 84(1):1–3, 2002.

[16] Joseph S. Miller and André Nies. Randomness and computability: open questions. *Bull. Symbolic Logic*, 12(3):390–410, 2006.

[17] André Nies. *Computability and randomness*, volume 51 of *Oxford Logic Guides.* Oxford University Press, Oxford, 2009.

[18] André Nies and Jan Reimann. A lower cone in the wtt degrees of non-integral effective dimension. In *Computational prospects of infinity. Part II. Presented talks*, volume 15 of *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, pages 249–260. World Sci. Publ., Hackensack, NJ, 2008.

[19] J. Reimann. *Computability and fractal dimension.* Doctoral dissertation, Universität Heidelberg, 2004. Available at `http://math.uni-heidelberg.de/logic/reimann/publications/phdthesis.pdf`.

[20] Jan Reimann. Effectively closed sets of measures and randomness. *Ann. Pure Appl. Logic*, 156(1):170–182, 2008.

[21] B. Ya. Ryabko. Coding of combinatorial sources and Hausdorff dimension. *Dokl. Akad. Nauk SSSR*, 277(5):1066–1070, 1984.

[22] Miklós Sántha and Umesh V. Vazirani. Generating quasirandom sequences from semirandom sources. *J. Comput. System Sci.*, 33(1):75–87, 1986. Twenty-fifth annual symposium on foundations of computer science (Singer Island, Fla., 1984).

[23] Ronen Shaltiel. Recent developments in extractors. In G. Paun, G. Rozenberg, and A. Salomaa, editors, *Current trends in theoretical computer science. The Challenge of the New Century. Vol 1: Algorithms and Complexity*. World Scientific, 2004.

[24] Umesh V. Vazirani. Strong communication complexity or generating quasirandom sequences from two communicating semirandom sources. *Combinatorica*, 7(4):375–392, 1987.

[25] Nikolai K. Vereshchagin and Michael V. Vyugin. Independent minimum length programs to translate between given strings. *Theoret. Comput. Sci.*, 271(1-2):131–143, 2002. Kolmogorov complexity.

[26] John von Neumann. Various techniques for use in connection with random digits. In *Collected works. Vol. V: Design of computers, theory of automata and numerical analysis*, General editor: A. H. Taub. A Pergamon Press Book, pages 768—770. The Macmillan Co., New York, 1963.

[27] Marius Zimand. Two sources are better than one for increasing the Kolmogorov complexity of infinite sequences. *CoRR*, abs/0705.4658, 2007. Informal publication.

Joseph S. Miller, Department of Mathematics, University of Wisconsin, Madison, WI 53706-1388, USA

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