OSCILLATION IN THE INITIAL SEGMENT COMPLEXITY OF RANDOM REALS

JOSEPH S. MILLER AND LIANG YU

ABSTRACT. We study oscillation in the prefix-free complexity of initial segments of 1-random reals. For upward oscillations, we prove that $\sum_{n\in\omega} 2^{-g(n)}$ diverges iff $(\exists^\infty n)\ K(X\upharpoonright n) > n+g(n)$ for every 1-random $X \in 2^\omega$. For downward oscillations. we characterize the functions g such that $(\exists^\infty n)\ K(X\upharpoonright n) < n+g(n)$ for almost every $X \in 2^\omega$. The proof of this result uses an improvement of Chaitin's counting theorem—we give a tight upper bound on the number of strings $\sigma \in 2^n$ such that $K(\sigma) < n + K(n) - m$.

The work on upward oscillations has applications to the K-degrees. Write $X \leq_K Y$ to mean that $K(X\upharpoonright n) \leq K(Y\upharpoonright n) + O(1)$. The induced structure is called the K-degrees. We prove that there are comparable (Δ^0_2) 1-random K-degrees. We also prove that every lower cone and some upper cones in the 1-random K-degrees have size continuum.

Finally, we show that it is independent of ZFC, even assuming that the Continuum Hypothesis fails, whether all chains of 1-random K-degrees of size less than $2^{\aleph_0}$ have a lower bound in the 1-random K-degrees.

"Although this oscillatory behaviour is usually considered to be a nasty feature, we believe that it illustrates one of the great advantages of complexity: the possibility to study degrees of randomness."

Michiel van Lambalgen, Ph.D. Dissertation [25, p. 145].

1. Introduction

We study both the hight and depth of oscillations in the prefix-free complexity of initial segments of random reals. By definition, X is 1-random if and only if $K(X\upharpoonright n) \geq n - O(1)$.[1] On the other hand, $K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1)$ for any string $\sigma \in 2^{<\omega}$ [4]. Hence $K(X\upharpoonright n) \leq n + K(n) + O(1)$. How does $K(X\upharpoonright n)$ behave between these bounds? This is the subject of the present paper and, from a different perspective, of our companion paper [21]. Our results have many forerunners in the literature; we mention the most relevant ones below.

First note that there is a subtle difference in the nature of the upper and lower bounds on $K(X\upharpoonright n)$. The constant in the lower bound depends in an essential way on X, unlike the constant in the upper bound. More substantially, though neither

2000 *Mathematics Subject Classification.* 68Q30, 03D30, 03E35.

The first author was partially supported by the Marsden Fund of New Zealand and then by an NSF VIGRE postdoctoral fellowship at Indiana University. After that, he was partially supported by the National Science Foundation under grants DMS-0601021 and DMS-065267, the latter being part of a Focused Research Group in Algorithmic Randomness. The second author was supported by NSF of China No. 10701041 as well as Research Fund for Doctoral Program of Higher Education No. 0070284043.

[1] Here K denotes *prefix-free complexity.* See Section 2 for a brief review of effective randomness.

the lower nor the upper bound can be improved (if they are to hold for *all* 1-random X), they are not tight in quite the same sense. Solovay [24] showed that almost all reals infinitely often achieve the upper bound, i.e., $\liminf_{n\to\infty} n+K(n)-K(X\upharpoonright n)$ is finite for almost all $X\in 2^\omega$ (see [27]). This is *not* true of all 1-random reals, and in fact, it turns out to be a characterization of 2-randomness [20]. To see that the upper bound cannot be improved at all, note that a straightforward modification of Solovay's proof shows that if $S\subseteq\omega$ is infinite, then almost all reals infinitely often achieve the upper bound *on* S. On the other hand, Chaitin proved that *no* 1-random can infinitely often achieve the lower bound: if $X\in 2^\omega$ is 1-random, then $\liminf_{n\to\infty} K(X\upharpoonright n)-n=\infty$. This does not mean that the lower bound can be improved. In Corollary 3.2, we show that if $h\colon\omega\to\omega$ is unbounded, then there is a 1-random $X\in 2^\omega$ such that $(\exists^\infty n)\ K(X\upharpoonright n)<n+h(n)$.

If $X\in 2^\omega$ is 1-random, it cannot be the case that $K(X\upharpoonright n)$ stays close to either bound; instead it oscillates, sometimes being "close" to the upper bound and sometimes being "close" to the lower bound. This behavior was first explored by Solovay [24]. In Section 3 we examine upward oscillations, starting from a characterization of 1-randomness proved by the authors [21].

Ample Excess Lemma. *$X\in 2^\omega$ is 1-random iff $\sum_{n\in\omega} 2^{n-K(X\upharpoonright n)}<\infty$.*

Note that this strengthens Chaitin's result: if $X\in 2^\omega$ is 1-random, then not only does $K(X\upharpoonright n)-n$ tend to infinity, but it does so fast enough to make the series converge. An immediate consequence is that if $\sum_{n\in\omega} 2^{-g(n)}$ diverges, then $(\exists^\infty n)\ K(X\upharpoonright n)>n+g(n)$ for every 1-random $X\in 2^\omega$. This generalizes a result of Solovay, who assumed additionally that g was computable. Furthermore, this result is *tight*. We prove that if $\sum_{n\in\omega} 2^{-g(n)}<\infty$, then there is a 1-random $X\in 2^\omega$ such that $K(X\upharpoonright n)\le n+g(n)$ for almost all $n\in\omega$. So the ample excess lemma gives the strongest possible lower bound on the growth of $K(X\upharpoonright n)-n$.

We turn to the investigation of downward oscillations in Section 5. Li and Vitányi proved that if $f\colon\omega\to\omega$ is computable and $\sum_{n\in\omega} 2^{-f(n)}$ diverges, then $(\exists^\infty n)\ K(X\upharpoonright n)<n+K(n)-f(n)$ for all $X\in 2^\omega$ (this is sketched in [17, Exercise 3.6.3(a)] and proved below as Theorem 5.3). We cannot drop the computability assumption on f; in Corollary 5.5 we show that there is an f such that $\sum_{n\in\omega} 2^{-f(n)}=\infty$ but $(\forall^\infty n)\ K(X\upharpoonright n)\ge n+K(n)-f(n)$ for *almost every* $X\in 2^\omega$. In Theorem 5.1, we show that the right series to consider is actually $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)}$. If this series converges, then $(\forall^\infty n)\ K(X\upharpoonright n)\ge n+K(n)-f(n)$ for almost every X; if it diverges, then $(\exists^\infty n)\ K(X\upharpoonright n)<n+K(n)-f(n)$ for almost every X. The proof of these results uses an improvement of Chaitin's counting theorem. His upper bound on the number of strings $\sigma\in 2^n$ such that $K(\sigma)<n+K(n)-m$ turns out not to be tight. We give an optimal bound in Section 4.

Corollary 5.6 restates Theorem 5.1 to give the precise condition on a function g needed to guarantee that $(\exists^\infty n)\ K(X\upharpoonright n)<n+g(n)$ for almost every $X\in 2^\omega$. Note that our results on downward oscillations are not stated, and do not hold, for all 1-random X. A result that does was given by Solovay [24]: if h and g are computable functions such that $\sum_{n\in\omega} 2^{-g(n)}$ diverges and h is unbounded and monotone, then for every 1-random $X\in 2^\omega$ we have $(\exists^\infty n)\ [K(X\upharpoonright n)\le n+h(n)$ and $K(n)>g(n)]$. It should be clear that we cannot drop the computability assumption on h.

Our review of results on oscillation in initial segment complexity would be badly incomplete if we did not mention the work of Martin-Löf [19]. Although he studied the *plain* (as opposed to prefix-free) Kolmogorov complexity of initial segments of

X, the results are similar. Martin-Löf proved that if f is a computable function such that $\sum_{n\in\omega} 2^{-f(n)} = \infty$, then $(\exists^\infty n)\ C(X\restriction n) < n - f(n)$ for all $X \in 2^\omega$. The analogous result for prefix-free complexity is Theorem 5.3 (which Li and Vitányi actually derive from Martin-Löf's result, modulo a constant term [17]). Martin-Löf also showed that if f is any function such that $\sum_{n\in\omega} 2^{-f(n)} < \infty$, then $(\forall^\infty n)\ C(X\restriction n\,|\,n) \geq n - f(n)$ for almost every $X \in 2^\omega$. This is comparable to part (i) of Theorem 5.1, and in fact, both results are proved using the first Borel–Cantelli lemma.

Comparing $K(X\restriction n)$K(X—n) to $n+\varepsilon K(n)$n+epsilon K(n). Let $X \in 2^\omega$ be 1-random. When trying to understand how $K(X\restriction n)$ oscillates between $n - O(1)$ and $n + K(n) + O(1)$, it is natural (if naïve) to ask how $K(X\restriction n)$ compares to $n + \varepsilon K(n)$, for $\varepsilon \in (0,1)$. We will see that $K(X\restriction n)$ neither dominates $n+\varepsilon K(n)$, nor is dominated by it. In a weak sense, this says that $K(X\restriction n)$ uses up all the space between its bounds.

In the following proof, we use that $K(n) \leq \delta \log n + O(1)$ for any $\delta > 1$, and equivalently, that $\varepsilon K(n) \leq \log n + O(1)$ for any $\varepsilon < 1$.

Theorem 1.1. *For any $\varepsilon \in (0,1)$ and $X \in 2^\omega$:*

(i) $(\exists^\infty n)\ K(X\restriction n) < n + \varepsilon K(n)$.

(ii) *If X is 1-random, then* $(\exists^\infty n)\ K(X\restriction n) > n + \varepsilon K(n)$.

Proof. (i) Let $f = \log n$. Pick $1 < \delta < 1/(1-\varepsilon)$. Then

$$(1-\varepsilon)K(n) \leq (1-\varepsilon)\delta \log n + O(1) \leq f(n),$$

for sufficiently large $n \in \omega$. For such n, we have $n + K(n) - f(n) \leq n + \varepsilon K(n)$. Since f is computable and $\sum_{n\in\omega} 2^{-f(n)}$ diverges, we can apply Theorem 5.3. Thus $(\exists^\infty n)\ K(X\restriction n) < n + K(n) - f(n) \leq n + \varepsilon K(n)$ for all $X \in 2^\omega$, completing the proof.

Alternate proof: A direct proof of (i) is not difficult. The result is immediate if X is not 1-random, so assume that it is. Fix an effective bijection between ω and 2^ω such that if σ is associated with n, then $|\sigma| = \log n + O(1)$ (see the next section). Consider $n \in \omega$ associated with $X\restriction m$. Then the initial bits of X code n (assuming that we know m), so

$$K(X\restriction n) \leq n + K(m) + O(1) \leq n + 2\log m + O(1) \leq n + 2\log\log n + O(1),$$

where the constant does not depend on n. On the other hand, the randomness of X ensures that $\varepsilon K(n) \geq \varepsilon K(X\restriction m) - O(1) \geq \varepsilon m - O(1) = \varepsilon \log n - O(1)$. Hence, for a sufficiently large $n \in \omega$ that is associated to $X\restriction m$ for some $m \in \omega$, we have $K(X\restriction n) < n + \varepsilon K(n)$.

(ii) We know that $\varepsilon K(n) \leq \log n + O(1)$, so $\sum_{n\in\omega} 2^{-\varepsilon K(n)} \geq 2^{-O(1)} \sum_{n\in\omega} 1/n$ diverges. Apply Theorem 3.4, of which we only need the direction that follows easily from the ample excess lemma. □

Applications to the KK-degrees. The Van Lambalgen quote at the beginning of this paper suggests that oscillation in the initial segment complexity of a real can be used to capture its *degree of randomness*. In Sections 6 and 7 we consider a specific realization of this idea. Downey, Hirschfeldt and LaForte [7, 8] defined $X \leq_K Y$ to mean that $K(X\restriction n) \leq K(Y\restriction n) + O(1)$. In other words, Y has higher initial segment prefix-free complexity than X, up to a constant. The induced partial order is called the *K-degrees.*

If higher complexity implies more randomness, then one can interpret $X \leq_K Y$ as saying that Y is more random than X. In [21], the authors back this intuition up by proving that if $Z \in 2^\omega$ is 1-random, $X \leq_K Y$, and X is Z-random, then Y is also Z-random. In other words, randomness relative to random reals is closed upward in the K-degrees. However, because there were no known examples of comparable 1-random K-degrees, it was not clear how much this result actually said. While it is easy to produce incomparable 1-random K-degrees (indeed, almost every pair of reals is K-incomparable [21]), the construction of comparable 1-random K-degrees is harder. The work of Section 3 allows us to produce many such degrees.

Using Theorems 3.1 and 3.3, we show that every countable collection of 1-random reals has a lower bound in the 1-random K-degrees and that every lower cone in the 1-random K-degrees has size continuum. In fact, we actually prove these results for a relation that appears stronger than $<_K$. For $X, Y \in 2^\omega$, we write $X \ll_K Y$ and say that X is *strongly K-below* Y if $\lim_{n\in\omega} K(Y \upharpoonright n) - K(X \upharpoonright n) = \infty$. Clearly $X \ll_K Y$ implies $X <_K Y$, but the strictness of this implication is open. It is also open if, given a 1-random $X \in 2^\omega$, there is always a $Y >_K X$. We show that it is possible for a 1-random K-degree to have continuum many reals strongly above it. On the other hand, the first author has proved that there are only countably many reals K-above any given 2-random [20].

In Section 7 we consider the following statement:

($\star$) *Every chain of 1-random K-degrees of size less than $2^{\aleph_0}$ has a lower bound in the 1-random K-degrees.*

We show that it follows from Martin's Axiom, so it is consistent with the negation of Continuum Hypothesis. On the other hand, the statement cannot be proved in ZFC. We use the countable support iterated Sacks forcing of length ω_2 to produce a model with a chain of size $\aleph_1 < 2^{\aleph_0}$ in the 1-random K-degrees that does not have a lower bound in the 1-random K-degrees. Therefore, ($\star$) is independent of ZFC, even assuming that the Continuum Hypothesis fails.

2. Preliminaries

We begin with a review of the definitions, notation and results that will be used below. A more thorough introduction to effective randomness can be found in the texts of Li and Vitányi [17] or Nies [22], or the upcoming monograph of Downey and Hirschfeldt [6]. By a real, we mean an infinite binary sequence, i.e., a member of 2^ω. Finite binary sequences will be called strings. A set of strings $S \subseteq 2^\omega$ is *prefix-free* if no element of S is a proper prefix of another element of S. A *machine* is a partial computable function from $2^{<\omega}$ to itself, though we will generalize this notion below. A machine is called *prefix-free* if it has prefix-free domain.

A prefix-free machine $U\colon 2^{<\omega} \to 2^{<\omega}$ is *universal* if, for every other prefix-free machine M, there is a prefix $\rho \in 2^{<\omega}$ by which U simulates M. In other words, for all $\sigma \in 2^{<\omega}$, either $U(\rho\sigma) = M(\sigma)$ or both diverge. It is easy to see that a universal prefix-free machine U exists. Furthermore, the universality of U is effective, meaning that from an index for M we can compute the prefix ρ by which U simulates M. This can be exploited, along with the recursion theorem, to let us build a prefix-free machine M as if we knew ρ in advance.

Kolmogorov complexity measures the information content of strings. We restrict our attention to *prefix-free* (*Kolmogorov*) *complexity*, an important variant due to Levin [16] and Chaitin [4]. Given any prefix-free machine M, let $K_M(\sigma) =$

$\min\{|\tau|: M(\tau) = \sigma\}$, i.e., the minimum length of any M-description of σ. The prefix-free complexity of $\sigma \in 2^{<\omega}$ is defined to be $K(\sigma) = K_U(\sigma)$. Note that the universality of U ensures the optimality of K; in other words, for any prefix-free machine M we have $K(\sigma) \leq K_M(\sigma) + O(1)$, where the constant depends on M.

We fix an effective bijection between $2^{<\omega}$ and ω and treat these sets as interchangeable. In particular, we identify $\sigma \in 2^{<\omega}$ with $n \in \omega$ if the binary expansion of $n+1$ is 1σ. This allows us to view K as a function on the natural numbers. It is easy to see that $K(\sigma) \leq |\sigma| + K(|\sigma|) + O(1) \leq 2|\sigma| + O(1)$, hence $K(n) \leq \log n + K(\log n) + O(1) \leq \log n + 2\log\log n + O(1)$.[2] Therefore, for any $\delta > 1$ we have $K(n) \leq \delta \log n + O(1)$, where the constant depends on δ. To see that $K(n)$ is *not* bounded by $\log n + O(1)$, note that the fact that U has prefix-free domain implies that $\sum_{n\in\omega} 2^{-K(n)} = \sum_{\sigma\in 2^{<\omega}} 2^{-K(\sigma)} \leq 1$; this is *Kraft's inequality.* On the other hand, $\sum_{n\in\omega} 2^{-\log n} = \sum_{n\in\omega} 1/n = \infty$, so $\limsup_{n\to\infty} K(n) - \log n = \infty$.

Kraft's inequality has an effective converse, the *Kraft–Chaitin theorem.* A *Kraft–Chaitin set* is a computable sequence of pairs $\{\langle d_n, \sigma_n\rangle\}_{n\in\omega}$ such that $d_n \in \omega$, $\sigma_n \in 2^{<\omega}$ and $\sum_{n\in\omega} 2^{-d_n} \leq 1$. The theorem says that, given a Kraft–Chatin set $\{\langle d_n, \sigma_n\rangle\}_{n\in\omega}$, there is a prefix-free machine M and strings $\{\tau_n\}_{n\in\omega}$ such that $|\tau_n| = d_n$ and $M(\tau_n) = \sigma_n$ for all $n \in \omega$. Then the universality of U implies that $K(\sigma_n) \leq d_n + O(1)$. Our use of the Kraft–Chaitin theorem, particulary in Sections 3 and 4, will be fairly delicate and we should examine the theorem more closely. The proof of the Kraft–Chatin theorem gives a uniform effective procedure to produce M from $\{\langle d_n, \sigma_n\rangle\}_{n\in\omega}$. Furthermore, this procedure is what computer scientists call an *online algorithm*: it produces τ_n after having only seen $\{\langle d_i, \sigma_i\rangle\}_{i\leq n}$. This is relevant in Section 3, where we apply the relativization of the Kraft–Chaitin theorem to an oracle $X \in 2^\omega$. In that case, we have an X-computable sequence $\{\langle d_n, \sigma_n\rangle\}_{n\in\omega}$ from which we produce a prefix-free oracle machine M^X and the corresponding strings $\{\tau_n\}_{n\in\omega}$. Because the construction of M is "online", the use of $M^X(\tau_n) = \sigma_n$ is exactly the part of X required to compute $\{\langle d_i, \sigma_i\rangle\}_{i\leq n}$.

To define *conditional* prefix-free complexity we consider prefix-free machines with a parameter, i.e., partial computable functions $M\colon 2^{<\omega} \times 2^{<\omega} \to 2^{<\omega}$ such that if $\tau \in 2^{<\omega}$ is fixed, then the domain of $M(\cdot, \tau)$ is prefix-free. We can extend U to be universal among such machines (now interpreting $U(\sigma)$ as $U(\sigma, \lambda)$, where λ is the empty string). Define *conditional prefix-free complexity* by $K(\sigma \mid \tau) = \min\{|\nu|: U(\nu, \tau) = \sigma\}$. There is an important relationship between conditional and unconditional complexity. Fix a pairing function, an effective bijection $\langle\cdot,\cdot\rangle\colon \omega \times \omega \to \omega$, and define $K(\sigma, \tau) = K(\langle\sigma, \tau\rangle)$. Let σ^* denote the U-description of σ of length $K(\sigma)$ on which U converges first. This definition ensures that σ^* can be determined from σ and $K(\sigma)$. The *symmetry of algorithmic information*, due to Levin (see Gács [9]) and Chaitin [4], states that $K(\sigma, \tau) = K(\sigma) + K(\tau \mid \sigma^*) + O(1)$.

We say that $A \in 2^\omega$ is 1-*random* if $K(A \restriction n) \geq n - O(1)$. This notion was introduced by Martin-Löf [18], though with a different definition; Schnorr proved the equivalence. It is straightforward to relativize the definition of 1-randomness to an oracle $X \in 2^\omega$. The resulting randomness notion is called X-*randomness.* Of particular importance is 1-randomness relative to $\emptyset'$, the halting problem, which is called 2-*randomness.*

Kučera [15] and Gács [10] proved that every set is computable from a 1-random real. In other words, if $C \in 2^\omega$, then there is a 1-random $X \in 2^\omega$ such that

[2]We exclusively use the logarithm base 2.

$C \leq_T X$. In Section 3, we will need a somewhat stronger form due to Gács. The *use* of $C \leq_T X$ is the least function $u\colon \omega \to \omega$ such that, for all n, the computation of $C(n)$ only examines bits from $X \upharpoonright u(n)$. Gács not only constructed a 1-random X computing C, but ensured that $\lim u(n)/n = 1$. This implies that we can build a reduction of C to X with use exactly $2n$.

We finish with an elementary analytical lemma.

Lemma 2.1. *Assume that* $\sum_{n\in\omega} 2^{-g(n)} < \infty$.

(i) *There is a function* $f \leq_T g$ *such that* f *is majorized by* g, $\limsup_{n\to\infty} g(n) - f(n) = \infty$ *and* $\sum_{n\in\omega} 2^{-f(n)} < \infty$.

(ii) *There is a function* $f \leq_T g'$ *such that* $\lim_{n\to\infty} g(n) - f(n) = \infty$ *and* $\sum_{n\in\omega} 2^{-f(n)} < \infty$.

Proof. (i) For each $m \in \omega$, let $n_m = \min\{n\colon g(n) \geq 2m\}$. Define $f(n_m) = \lfloor g(n_m)/2 \rfloor \geq m$. Let $f(n) = g(n)$ for all other values of n. Then

$$\sum_{n\in\omega} 2^{-f(n)} \leq \sum_{n\in\omega} 2^{-g(n)} + \sum_{m\in\omega} 2^{-m} < \infty.$$

Clearly, f is majorized by g. Also $f \leq_T g$ and $\limsup_{n\to\infty} g(n) - f(n) = \infty$.

(ii) Let $c \geq \sum_{n\in\omega} 2^{-g(n)}$ Note that g' computes an increasing sequence $\{n_i\}_{i\in\omega}$ such that $\sum_{n\geq n_i} 2^{-g(n)} \leq c/2^i$, for all $i \in \omega$. We can assume that $n_0 = 0$. Define $f(n) = g(n) - \lfloor \log |\{i\colon c_i \leq n\}| \rfloor$ (or 0 if this is negative). Then

$$\sum_{n\in\omega} 2^{-f(n)} \leq \sum_{n\in\omega} |\{i\colon n_i \leq n\}|\, 2^{-g(n)} = \sum_{i\in\omega} \sum_{n\geq n_i} 2^{-g(n)} \leq \sum_{i\in\omega} c/2^i = 2c < \infty.$$

Also $f \leq_T g'$ and $\lim_{n\to\infty} g(n) - f(n) = \infty$. □

3. Upward oscillations

In this section we explore the upward oscillations made by the initial segment complexity of 1-random reals. In particular, we characterize the functions g such that for all 1-random reals X, the initial segment complexity $K(X \upharpoonright n)$ infinitely often exceeds $n + g(n)$. These are exactly the functions such that $\sum_{n\in\omega} 2^{-g(n)}$ diverges. One direction of this characterization follows from the ample excess lemma. For the harder direction, we prove:

Theorem 3.1. *If* $\sum_{n\in\omega} 2^{-f(n)} < \infty$, *then there is a* 1*-random* $X \in 2^\omega$ *such that*

$$K(X \upharpoonright n) \leq n + f(n) + O(1).$$

Furthermore, we can ensure that $X \leq_T f \oplus \emptyset'$.

The proof is broken up into two parts. The first part is essentially technical. We would like to be able to code f into a 1-random real in a compact way, but this may not be possible. Instead, we construct a function g such that $(\forall n)\ g(n) \leq f(n)$ and g *can* be coded compactly, meaning that we can use Gács coding to produce a 1-random real X such that $g(n)$ is computable from the first n bits of X, for all n. Furthermore, we ensure that $\sum_{n\in\omega} 2^{-g(n)} < \infty$. The second part of the proof is verifying that X is the desired 1-random real. This is the content of the following result.

Bounding Lemma. *If* $\sum_{n\in\omega} 2^{-g(n)} < \infty$ *and* $g \leq_T X$ *with use* n, *then* $K(X \upharpoonright n) \leq n + g(n) + O(1)$.

Proof. The idea behind this lemma is that if we knew g—in other words, if we had g as an oracle—then by the Kraft–Chaitin theorem we could give every string of length n a description of length $n+g(n)+O(1)$. Furthermore, as was discussed in Section 2, the proof of the Kraft–Chaitin theorem gives an *online algorithm*, so we could decode the description that was given to a string of length n knowing only $g\restriction(n+1)$. Now consider the description σ of length $n+g(n)+O(1)$ given to $X\restriction n$: can we decode σ without knowing g in advance? One might be hopeful, because σ codes $X\restriction n$, from which we can compute $g\restriction(n+1)$ and thus decode σ. But it is as if we have encrypted the decryption key along with our message. We would know how to read the message if only we knew what the message said. The heart of the proof is resolving this circularity.

By the Kraft–Chaitin theorem, there is a prefix-free machine M^X relative to X and a sequence $\{\tau_n\}_{n\in\omega}$ such that $|\tau_n|\leq g(n)+O(1)$ and $(\forall n)\ M^X(\tau_n)=X\restriction n$. We may assume that M is given by an oracle Turing machine (which we also call M) such that:

(i) $M^X(\tau_n)$ has use exactly n, and
(ii) $M^X(\tau_n)$ reads exactly τ_n before halting.

Furthermore, we may assume of M that both its input tape and oracle tape are one-way, read-only, and reading moves the tape one position. These assumptions ensure that we cannot look at the same position of either tape twice. We place no restrictions on the work tapes and, of course, they can be used to store the bits of the input and oracle that we have read, which is why our assumptions do not limit the power of M.

The key step of the proof is to transform M into a Turing machine M° with no oracle. We do this by routing any requests that M makes to *either* its input or oracles tapes to M°'s single input tape. Then M° induces a prefix-free machine (which we also call M°).[3]

Now let us assume that $M^X(\tau)\downarrow=\rho$ with use exactly n. Also assume that M reads all of the bits of τ and only those bits from the input tape. At certain stages of the computation, M asks for the next bit of the input or the next bit of the oracle, and by our assumptions, it cannot see the same bit of either more than once. Now merge the bits of τ and $X\restriction n$ together in exactly the order that they are requested by M; call the resulting string σ. The point is that $M^\circ(\sigma)\downarrow=\rho$ because the computation M° makes on σ is indistinguishable from the computation that M^X makes on τ. Therefore, $K_{M^\circ}(\rho)\leq|\sigma|=n+|\tau|$. Applying this observation to the sequence $\{\tau_n\}_{n\in\omega}$ shows that

$$K(X\restriction n)\leq K_{M^\circ}(X\restriction n)+O(1)\leq n+|\tau_n|+O(1)\leq n+g(n)+O(1),$$

which is the desired conclusion. □

Proof of Theorem 3.1. Assume that we are given a function $f\colon\omega\to\omega$ such that $\sum_{n\in\omega}2^{-f(n)}$ is finite. We want to construct a function g such that $(\forall n)\ g(n)\leq f(n)$ and g can be coded in a compact way. In particular, we require that:

- $g(0)=0$,
- if $n\not\equiv 3 \pmod 4$, then $g(n)=g(n+1)$, and

[3]In particular, we define a partial computable function $M^\circ\colon 2^{<\omega}\to 2^{<\omega}$ so that it converges on τ with output ρ iff the Turing machine M° halts after reading exactly τ on its input tape (no less and no more) and writing ρ on its output tape. In other words, we treat M° as a *self-delimiting* Turing machine, which ensures that M° has prefix-free domain.

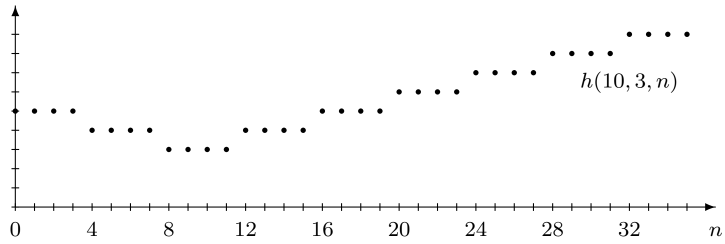

FIGURE 1. The function $h(10, 3, n)$ is the upper bound on the values of g that wold be imposed if $f(10) = 3$.

- $|g(n+1) - g(n)| \leq 1$, for all n.

Define g to be (point-wise) maximal among the functions satisfying these restrictions. It is not hard to see that such a function exists, but a careful examination will help us understand g. Because g is forced to change at a slow rate, the value of $f(n)$ not only bounds the value of $g(n)$, but it also places bounds on all values of g. For example, if $f(10) = 3$, then g is at most 3 on $[8, 11]$, at most 4 on $[4, 7]$ and $[12, 15]$, and so on. Define $h(i, j, n)$ to be the upper bound placed on $g(n)$ by the fact that $f(i) = j$ (see Fig. 1). Now, putting together all of the restrictions on $g(n)$, including the fact that $g(0) = 0$, we have

$$g(n) = \min\{h(0, 0, n), \min_{i\in\omega}\{h(i, f(i), n)\}\}. \tag{1}$$

To verify that $\sum_{n\in\omega} 2^{-g(n)} < \infty$, note that

$$\sum_{n\in\omega} 2^{-h(i,j,n)} \leq 4 \cdot 2^{-j} + 8 \sum_{n>0} 2^{-j-n} = 12 \cdot 2^{-j}.$$

Therefore,

$$\begin{aligned}\sum_{n\in\omega} 2^{-g(n)} &\leq \sum_{n\in\omega} \left(2^{-h(0,0,n)} + \sum_{i\in\omega} 2^{-h(i,f(i),n)}\right) \\ &= \sum_{n\in\omega} 2^{-h(0,0,n)} + \sum_{i\in\omega}\sum_{n\in\omega} 2^{-h(i,f(i),n)} \leq 12 + \sum_{i\in\omega} 12 \cdot 2^{-f(i)} < \infty.\end{aligned}$$

Next we prove that $g \leq_T f$. It is clear that $h \leq_T f$. Although Eq. 1 expresses $g(n)$ as the minimum of an infinite f-computable sequence, it is not hard to see that we can ignore all but finitely many terms. In particular, if $i \geq 2n$, then $h(i, f(i), n) \geq h(i, 0, n) \geq \lfloor n/4 \rfloor = h(0, 0, n)$. Therefore,

$$g(n) = \min\{h(0, 0, n), \min_{i<2n}\{h(i, f(i), n)\}\},$$

so $g \leq_T f$.

The restrictions placed on g allow us to code it compactly into a set $C \in 2^\omega$. It is only necessary, of course, to record the value of $g(n+1) - g(n)$, for all $n \equiv 3 \pmod 4$. Two bits are sufficient to code $g(n+1) - g(n)$ because there are only three possible values. Thus we use the first two bits of C to record $g(4) - g(3)$, the next two for $g(8) - g(7)$, and so on. Note that $g(n)$ can be computed from $C \upharpoonright \lfloor n/2 \rfloor$ (or more precisely, $C \upharpoonright (2\lfloor n/4 \rfloor)$). Of course, $C \leq_T g \leq_T f$.

By the Kučera–Gács theorem, there is a 1-random X such that $C \leq_T X$ and $X \leq_T C \oplus \emptyset' \leq_T f \oplus \emptyset'$. As was mentioned in the preliminaries, the Gács version of the Kučera–Gács theorem produces an X that computes C with use $2n$, meaning that only the first $2n$ bits of X are used to compute $C \restriction n$. Therefore, $g(n)$ is computable from $X \restriction n$, for all n. Hence the bounding lemma implies that $K(X \restriction n) \leq n + g(n) + O(1) \leq n + f(n) + O(1)$, completing the proof. □

Corollary 3.2. *If $h\colon \omega \to \omega$ is unbounded, then there is a 1-random $X \in 2^\omega$ such that $(\exists^\infty n)\ K(X \restriction n) < n + h(n)$.*

Proof. Chose a sequence of distinct natural numbers $\{n_i\}_{i\in\omega}$ such that $h(n_i) \geq 2i$. Define $f\colon \omega \to \omega$ by

$$f(n) = \begin{cases} i, & \text{if } n = n_i \\ n, & \text{otherwise.} \end{cases}$$

We can apply Theorem 3.1 because $\sum_{n\in\omega} 2^{-f(n)} \leq \sum_{i\in\omega} 2^{-i} + \sum_{n\in\omega} 2^{-n} = 4$, so there is a 1-random $X \in 2^\omega$ such that $K(X \restriction n) \leq n + f(n) + O(1)$. Therefore, $K(X \restriction n_i) \leq n_i + f(n_i) + O(1) = n_i + i + O(1) \leq n_i + h(n_i) - i + O(1)$. When $i \in \omega$ is sufficiently large, $K(X \restriction n_i) \leq n_i + h(n_i)$. □

We will want a stronger form of Theorem 3.1 when we study the K-degrees in Chapter 6. It is clear that we can modify the proof above to require that $g(n) = g(n+1)$ whenever $n \not\equiv 7 \pmod 8$. Then g can be coded into C so that $g \leq_T C$ with use $\lfloor n/4 \rfloor$. By Gács coding, there is a 1-random $X \leq_T f \oplus \emptyset'$ such that g is computable from X with use $\lfloor n/2 \rfloor$. This means that if Z is any set, then $g \leq_T X \oplus Z$ with use n. Applying the bounding lemma gives the following result:

Proposition 3.3. *If $\sum_{n\in\omega} 2^{-f(n)} < \infty$, then there is a 1-random $X \leq_T f \oplus \emptyset'$ such that $K((X \oplus Z) \restriction n) \leq n + f(n) + O(1)$, for every $Z \in 2^\omega$.*

We will not use this observation, but it is not hard to see that the constant in the previous result is independent of Y. This is because the constant in the proof of the bounding lemma depends only on the choice of M and, in this particular application, the same M can be used for all Y.

We finish with the result promised at the start of this section.

Theorem 3.4. *The following are equivalent for a function g:*

(i) *$\sum_{n\in\omega} 2^{-g(n)}$ diverges.*
(ii) *For every 1-random real $X \in 2^\omega$, $(\exists^\infty n)\ K(X \restriction n) > n + g(n)$.*

Proof. (i) $\Longrightarrow$ (ii): We prove the contrapositive. Assume that X is 1-random and that there is an $m \in \omega$ such that $(\forall n \geq m)\ K(X \restriction n) \leq n + g(n)$. This implies that $\sum_{n\geq m} 2^{n-K(X\restriction n)} \geq \sum_{n\geq m} 2^{-g(n)}$. The first sum is finite by the ample excess lemma, so $\sum_{n\in\omega} 2^{-g(n)}$ converges.

(ii) $\Longrightarrow$ (i): Again we prove the contrapositive. Assume that $\sum_{n\in\omega} 2^{-g(n)}$ converges. By Lemma 2.1(ii), there is a function f such that $\lim_{n\to\infty} g(n) - f(n) = \infty$ and $\sum_{n\in\omega} 2^{-f(n)} < \infty$. Hence by Theorem 3.1, there is a 1-random X such that $K(X \restriction n) \leq n + f(n) + O(1)$. This together with the fact that $\lim_{n\to\infty} g(n) - f(n) = \infty$ implies that $(\forall^\infty n)\ K(X \restriction n) \leq n + g(n)$. □

4. The improved counting theorem

Before we turn out attention to downward oscillations, we present a result that will be important for that investigation. Chaitin proved that there are at most $2^{n-m+O(1)}$ strings $\sigma \in 2^n$ for which $K(\sigma) < n + K(n) - m$ (see [5, Lemma I3][4]). This result has been called Chaitin's Counting Theorem. In this section, we improve the upper bound in Chaitin's theorem and show that our new upper bound is tight.

Improved Counting Theorem.

$$|\{\sigma \in 2^n \colon K(\sigma) < n + K(n) - m\}| \leq 2^{n-m-K(m \mid n^*)+O(1)}.$$

Our proof will use the same basic technique as in Chaitin [5]: exploiting the minimality of K among information content measures. Levin and Zvonkin [28] introduced information content measures, although the name comes from Chaitin [5]. Call a function $\widehat{K} \colon \omega \to \mathbb{R} \cup \{\infty\}$ an *information content measure* if

(i) $\sum_{n\in\omega} 2^{-\widehat{K}(n)} \leq 1$ (where $2^{-\infty} = 0$).
(ii) $\{\langle k, n\rangle \colon \widehat{K}(n) < k\}$ is computable enumerable.

(This definition differs superficially from the one given in the companion paper [21].) Note that K is an information content measure (when viewed as a function of ω); (i) is Kraft's inequality and (ii) is clear. In fact, Levin [16] proved that K is the minimal information content measure. To see this, let $\widehat{K}$ be another information content measure. Consider the c.e. set $W = \{\langle k+1, n\rangle \colon \widehat{K}(n) < k\} = \{\langle h+2, n\rangle \colon \lfloor \widehat{K}(n)\rfloor \leq h\}$. Note that

$$\sum_{\langle d,\sigma\rangle\in W} 2^{-d} = \sum_{n\in\omega} \sum_{h\geq\lfloor\widehat{K}(n)\rfloor} 2^{-(h+2)} = \sum_{n\in\omega} 2^{-\lfloor\widehat{K}(n)\rfloor-1} \leq \sum_{n\in\omega} 2^{-\widehat{K}(n)} \leq 1.$$

Therefore, W is a Kraft–Chaitin set. By the Kraft–Chaitin theorem, there is a prefix-free machine M such that $\langle d, \sigma\rangle \in W$ implies $K_M(\sigma) \leq d$. It follows from the definition of W that $K_M(n) \leq \lfloor\widehat{K}(n)\rfloor + 2 \leq \widehat{K}(n) + 2$. Assume that K simulates M with a prefix ρ. Then $K(n) \leq K_M(n) + |\rho| \leq \widehat{K}(n) + 2 + |\rho|$. In other words, if $\widehat{K}$ is any information content measure, then $K(n) \leq \widehat{K}(n) + O(1)$.

The reason for proving the minimality of K in such detail is that we want to generalize it to the case of conditional complexity using the uniformity of the Kraft–Chaitin theorem. Consider a function $\widehat{K} \colon \omega \times 2^{<\omega} \to \mathbb{R} \cup \{\infty\}$ such that $\{\langle k, n\rangle \colon \widehat{K}(n \mid \tau) < k\}$ is c.e., uniformly in τ. Build a family of c.e. sets W_τ by putting $\langle k+1, n\rangle$ into W_τ whenever we find that $\widehat{K}(n \mid \tau) < k$, but only if W_τ would remain a Kraft–Chaitin set. This produces, by fiat, a uniform family of Kraft–Chaitin sets, one for each $\tau \in 2^{<\omega}$. By the uniformity of the Kraft–Chaitin theorem, there is a partial computable function $M \colon 2^{<\omega} \times 2^{<\omega} \to \omega$ such that

- $M(\cdot, \tau)$ is prefix-free for each $\tau \in 2^{<\omega}$, and
- $\langle d, \sigma\rangle \in W_\tau$ implies $K_M(\sigma \mid \tau) \leq d$.

Now assume that K simulates M with a prefix ρ. If $\sum_{n\in\omega} 2^{-\widehat{K}(n \mid \tau)} \leq 1$ for *some* τ, then by the same calculation as before, $\{\langle k+1, n\rangle \colon \widehat{K}(n \mid \tau) < k\}$ is a Kraft–Chaitin set. Thus our construction guarantees that $W_\tau = \{\langle k+1, n\rangle \colon \widehat{K}(n \mid \tau) < k\}$. So again we have $K_M(n \mid \tau) \leq \lfloor\widehat{K}(n \mid \tau)\rfloor + 2 \leq \widehat{K}(n \mid \tau) + 2$. But then

$$K(n \mid \tau) \leq K_M(n \mid \tau) + |\rho| \leq \widehat{K}(n \mid \tau) + 2 + |\rho| = \widehat{K}(n \mid \tau) + O(1).$$

[4]The result is stated much earlier in [4, Theorem 4.2(b)], but the proof given there is flawed.

A crucial observation is that the constant term does not depend on τ; with this in mind, we are ready to prove our theorem.

Proof of the improved counting theorem. Let $\widehat{K}(n) = -\log\left(\sum_{\sigma\in 2^n} 2^{-K(\sigma)}\right)$. Note that

$$\sum_{n\in\omega} 2^{-\widehat{K}(n)} = \sum_{n\in\omega}\sum_{\sigma\in 2^n} 2^{-K(\sigma)} = \sum_{\sigma\in 2^{<\omega}} 2^{-K(\sigma)} \leq 1,$$

where the inequality is Kraft's. Furthermore, $\{\langle k,n\rangle : \widehat{K}(n) < k\}$ is a c.e. set, so $\widehat{K}$ is an information content measure. By the minimality of K, there is a $c\in\omega$ such that $(\forall n)\ K(n) \leq \widehat{K}(n) + c$. Hence, for all n,

$$2^{-K(n)+c} \geq \sum_{\sigma\in 2^n} 2^{-K(\sigma)}. \tag{2}$$

Up to this point we have followed Chaitin [5], whose proof of the counting theorem finishes with the inequality above.

Now let

$$\widehat{K}(m \mid \tau) = \begin{cases} n + c - m - \log\left(|\{\sigma\in 2^n : K(\sigma) < n + |\tau| - m\}|\right), & \text{if } U(\tau)\downarrow = n \\ \infty, & \text{otherwise.}\end{cases}$$

Note that $\{\langle k,m\rangle : \widehat{K}(m \mid \tau) < k\}$ is c.e., uniformly in τ. Furthermore,

$$\begin{aligned}\sum_{m\in\omega} 2^{-\widehat{K}(m \mid n^*)} &= 2^{-n-c}\sum_{m\in\omega} 2^m |\{\sigma\in 2^n : K(\sigma) < n + K(n) - m\}| \\ &= 2^{-n-c}\sum_{\sigma\in 2^n}\sum_{m<n+K(n)-K(\sigma)} 2^m \leq 2^{-n-c}\sum_{\sigma\in 2^n} 2^{n+K(n)-K(\sigma)} \\ &= 2^{K(n)-c}\sum_{\sigma\in 2^n} 2^{-K(\sigma)} \leq 1,\end{aligned}$$

where the last inequality follows from (2). Therefore, the discussion above implies that there is a $d\in\omega$ such that $(\forall n)(\forall m)\ K(m \mid n^*) \leq \widehat{K}(m \mid n^*) + d$. So for all n and m,

$$2^{-K(m \mid n^*)} \geq 2^{-\widehat{K}(m \mid n^*)-d} = 2^{-n+m-c-d}\ |\{\sigma\in 2^n : K(\sigma) < n + K(n) - m\}|.$$

Multiplying both sides by $2^{n-m+c+d}$ completes the proof. □

The improved counting theorem is tight, up to a multiplicative constant. This follows from the next lemma, which will also be useful in the next section.

Lemma 4.1. *There is a $c\in\omega$ such that if $\delta\in 2^n$ ends in at least $m+K(m \mid n^*)+c$ zeros, then $K(\delta) < n + K(n) - m$.*

Proof. We define a prefix-free machine M. By the recursion theorem, we may assume that we know in advance the prefix ρ by which U simulates M. Set $c = |\rho| + 1$. The domain of M consists of strings $\sigma\tau\nu$ for which there are $n, m\in\omega$ such that $U(\sigma)\downarrow = n$, $U(\tau \mid \sigma)\downarrow = m$, and $|\nu| = n - m - |\tau| - c$. Note that the set of all such strings is prefix-free. For $\sigma\tau\nu$, n and m as above, define $M(\sigma\tau\nu) = \nu 0^{n-|\nu|}$.

Now fix $n, m\in\omega$ and let $\delta = \nu 0^{m+K(m \mid n^*)+c}$ be a string of length n. Let $\sigma = n^*$ and let τ be a minimal program for m given n^*. Note that $|\nu| = n - m - |\tau| - c$, so we have $M(\sigma\tau\nu) = \nu 0^{n-|\nu|} = \delta$. Therefore, $K(\delta) \leq |\sigma\tau\nu| + c - 1 = K(n) + |\tau| + (n - m - |\tau| - c) + c - 1 = n + K(n) - m - 1$, as required. □

Proposition 4.2. $|\{\sigma \in 2^n : K(\sigma) < n + K(n) - m\}| \geq \lfloor 2^{n-m-K(m\,|\,n^*)-O(1)} \rfloor$.

Proof. Let c be the constant from the previous lemma. The lemma guarantees that there are $2^{n-m-K(m\,|\,n^*)-c}$ distinct strings of length n with complexity less than $n + K(n) - m$ (assuming that $n - m - K(m\,|\,n^*) - c \geq 0$). □

5. Downward oscillations

The main theorem in this section gives a necessary and sufficient condition on a function f to ensure that for almost all $X \in 2^\omega$ the initial segment complexity $K(X \upharpoonright n)$ infinitely often drops below $n + K(n) - f(n)$.

Theorem 5.1.

(i) *If* $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)} < \infty$*, then* $(\forall^\infty n)\ K(X \upharpoonright n) \geq n + K(n) - f(n)$ *for almost every* $X \in 2^\omega$.

(ii) *If* $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)} = \infty$*, then* $(\exists^\infty n)\ K(X \upharpoonright n) < n + K(n) - f(n)$ *for almost every* $X \in 2^\omega$.

The proof of (i) uses the first Borel–Cantelli Lemma. We state both lemmas.

Borell–Cantelli Lemmas. *Let* $\langle E_n \rangle$ *be a sequence of events in a probability space.*

(1) *If* $\sum_{n\in\omega} \Pr(E_n) < \infty$*, then the probability that infinitely many* E_n *occur is* 0.

(2) *If* $\sum_{n\in\omega} \Pr(E_n) = \infty$ *and* E_n *are independent events, then the probability that infinitely many* E_n *occur is* 1.

Proof of Theorem 5.1(i). The events we consider are

$$E_n : K(X \upharpoonright n) < n + K(n) - f(n).$$

Note that

$$\begin{aligned}\Pr(E_n) &= \frac{|\{\sigma \in 2^n : K(\sigma) < n + K(n) - f(n)\}|}{2^n} \\ &\leq \frac{2^{n-f(n)-K(f(n)\,|\,n^*)+O(1)}}{2^n} = 2^{-f(n)-K(f(n)\,|\,n^*)+O(1)},\end{aligned}$$

where the inequality follows from the improved counting theorem. Therefore, if $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)} < \infty$, then by the first Borel–Cantelli Lemma, the probability that $(\exists^\infty n)\ K(X \upharpoonright n) < n + K(n) - f(n)$ is zero. In other words, $(\forall^\infty n)\ K(X \upharpoonright n) \geq n + K(n) - f(n)$ for almost every $X \in 2^\omega$. □

For the proof of Theorem 5.1(ii), we require the following purely analytical lemma. It states that if $\sum_{n\in\omega} 2^{-g(n)}$ diverges, then with probability one a real has a run of $g(n)$ zeros ending at position n, for infinitely many $n \in \omega$. The lemma would follow from the second Borel–Cantelli lemma if "$X \upharpoonright n$ ends in at least $g(n)$ zeros" were independent events for different n.[5] Because they are not, we give a direct proof.

Lemma 5.2. *If* $\sum_{n\in\omega} 2^{-g(n)}$ *diverges, then for almost all* $X \in 2^\omega$

$$(\exists^\infty n)\ X \upharpoonright n \text{ ends in at least } g(n) \text{ zeros.}$$

[5]Indeed, Chaitin [5] used the second Borel–Cantelli lemma to derive a similar theorem—in a more restricted context—about runs of zeros in (the binary expansion of) Ω, the halting probability of U.

Proof. Fix $v \in \omega$. We will prove that for almost every $X \in 2^\omega$ there is an $n \geq v$ such that $X \upharpoonright n$ ends in at least $g(n)$ zeros. Because v is arbitrary, the lemma follows.

First, it will be convenient to restrict g to a subset of its domain. Define $P = \{n \geq v \colon g(n) \leq n\}$. Note that $\sum_{n<v} 2^{-g(n)} + \sum_{n\in P} 2^{-g(n)} + \sum_{n\in\omega} 2^{-n} \geq \sum_{n\in\omega} 2^{-g(n)} = \infty$. Because the first and third series are finite, $\sum_{n\in P} 2^{-g(n)} = \infty$. Now define $Q = \{n \in P \colon (\forall m < n)\ m - g(m) < n - g(n)\}$. It is not hard to see that if $n \in P \smallsetminus Q$, then there is an $m \in Q$ such that $m < n$ and $m - g(m) \geq n - g(n)$. In that case, $g(n) \geq n - m + g(m)$. This means that $\sum_{n\in P} 2^{-g(n)} \leq \sum_{m\in Q} \sum_{n\geq m} 2^{-n+m-g(m)} = 2\sum_{m\in Q} 2^{-g(m)}$. Therefore, $\sum_{m\in Q} 2^{-g(m)}$ also diverges.

Let $S(m) = \{\sigma \in 2^m \colon (\forall n \leq m)\ n \in Q \implies \sigma \cap [n - g(n), n) \neq \emptyset\}$, for each $m \in \omega$. Define $s(m) = |S(m)|$. Note that every element of $S(m+1)$ extends an element of $S(m)$, hence $s(m+1) \leq 2s(m)$ and $m \mapsto s(m)/2^m$ is nonincreasing. Therefore, $d = \lim_{m\to\infty} s(m)/2^m$ exists. If $d = 0$, then for almost every X there is an $n \in Q$ (hence $n \geq v$) such that $X \upharpoonright n$ ends in at least $g(n)$ zeros. Assume for a contradiction that $d > 0$.

Consider $n \in Q$. If $\tau \in S(n - g(n) - 1)$, then $\tau 10^{g(n)-1} \in S(n-1)$. Otherwise, there would be an $m < n$ in Q such that $m - g(m) \geq n - g(n)$, contradicting the definition of Q. But clearly $\tau 10^{g(n)} \notin S(n)$, so $s(n) \leq 2s(n-1) - s(n - g(n) - 1)$. Thus if $n \in Q$, then

$$\begin{aligned}\frac{s(n)}{2^n} &\leq \frac{s(n-1)}{2^{n-1}} - \frac{s(n-g(n)-1)}{2^n} \\ &= \frac{s(n-1)}{2^{n-1}} - \frac{s(n-g(n)-1)}{2^{n-g(n)-1}} 2^{-g(n)-1} \leq \frac{s(n-1)}{2^{n-1}} - \frac{d}{2} 2^{-g(n)}.\end{aligned}$$

As was already mentioned, $s(n)/2^n \leq s(n-1)/2^{n-1}$ for any $n \in \omega$. So by induction, $d = \lim_{n\to\infty} s(n)/2^n \leq s(0) - d/2 \sum_{m\in Q} 2^{-g(m)} = -\infty$. This is a contradiction, which completes the proof. □

Combining the previous result with Lemma 4.1 yields Theorem 5.1(ii).

Proof of Theorem 5.1(ii). Let c be the constant from Lemma 4.1. Assume that $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)}$ diverges. Then $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)-c}$ also diverges. So by Lemma 5.2, for almost every $X \in 2^\omega$ there are infinitely many n such that $X \upharpoonright n$ ends in at least $f(n) + K(f(n)\,|\,n^*) + c$ zeros. But for such an n, Lemma 4.1 guarantees that $K(X \upharpoonright n) < n + K(n) - f(n)$. □

If f is computable, then $K(f(n)\,|\,n^*)$ is $O(1)$. So by Theorem 5.1(ii), the divergence of $\sum_{n\in\omega} 2^{-f(n)}$ implies that $(\exists^\infty n)\ K(X \upharpoonright n) < n + K(n) - f(n)$ for almost all $X \in 2^\omega$. Using a different proof, we will show that this actually holds for *all* X. This result is sketched by Li and Vitányi [17] using an analogous result of Martin-Löf for plain Kolmogorov complexity [19]. It can also be seen as a generalization of a result of Van Lambalgen [25, Corollary 5.4.2.6]; he proved that if X is 1-random and $f(n) = a \log n$, where $a \in (0,1)$ is computable, then $(\exists^\infty n)\ K(X \upharpoonright n) < n + K(n) - f(n)$.

Theorem 5.3 (Li and Vitányi [17, Exercise 3.6.3(a)])**.** *If f is computable and $\sum_{n\in\omega} 2^{-f(n)} = \infty$, then $(\exists^\infty n)\ K(X \upharpoonright n) < n + K(n) - f(n)$ for all $X \in 2^\omega$.*

Proof. We build a prefix-free machine M using the Kraft–Chaitin theorem. In other words, we build a Kraft–Chaitin set W and let M be the corresponding machine.

By the recursion theorem, we may assume that we know in advance the prefix ρ by which U simulates M. Let $c = |\rho| + 1$. Similar to the proof of Lemma 5.2, define $P = \{n \in \omega\colon f(n) \leq n - c - 1\}$. Note that $\sum_{n\in P} 2^{-f(n)} + \sum_{n\in\omega} 2^{-n+c+1} \geq \sum_{n\in\omega} 2^{-f(n)} = \infty$. Because the second series converges, $\sum_{n\in P} 2^{-f(n)} = \infty$.

We build W in stages. At stage $s+1$ we will work with lengths in $[n_s, n_{s+1})$.

Stage 0. Let $n_0 = 0$.

Stage $s+1$. Let n_{s+1} be the least number such that $\sum_{n\in P\cap[n_s,n_{s+1})} 2^{-f(n)-c-1} \geq 1$. For each $n \in P \cap [n_s, n_{s+1})$, take $S_n \subseteq 2^n$ such that the measure of the set of reals with a prefix in S_n is $2^{-f(n)-c-1}$ (in other words, $|S_n| = 2^{n-f(n)-c-1}$, justifying our restriction to P). Furthermore, choose the sets S_n such that every real has a prefix in $\bigcup_{n\in P\cap[n_s,n_{s+1})} S_n$. This is possible by the choice of n_{s+1}. Finally, for each $n \in P \cap [n_s, n_{s+1})$, each $\sigma \in S_n$, and each $m \in \omega$, enumerate $\langle n + K(n) + m - f(n) - c, \sigma\rangle$ into W. (The purpose of m is to make this a c.e. set of pairs.)

First, we must check that W is a Kraft–Chaitin set. The total contribution to the weight of W for any $n \in P$ is

$$|S_n| \sum_{m\in\omega} 2^{-n-K(n)-m+f(n)+c} = 2^{n-f(n)-c-1} 2^{-n-K(n)+f(n)+c+1} = 2^{-K(n)}.$$

If $n \notin P$, then it contributes nothing to W. So $\sum_{\langle d,\sigma\rangle\in W} 2^{-d} = \sum_{n\in P} 2^{-K(n)} \leq 1$, by Kraft's inequality. Therefore W is a Kraft–Chaitin set.

Now if $\sigma \in S_n$, then $\langle n + K(n) - f(n) - c, \sigma\rangle \in W$. Hence $K(\sigma) < K_M(\sigma) + c \leq n + K(n) - f(n)$. But the construction guarantees that for any $X \in 2^\omega$, there are infinitely many n such that $X \upharpoonright n \in S_n$. Indeed, there is such an $n \in P \cap [n_s, n_{s+1})$ for every s. Therefore, $(\exists^\infty n)\ K(X \upharpoonright n) < n + K(n) - f(n)$. □

Considering the complexity of the divergence condition on f in Theorem 5.1(ii), one might hope for a simplification. In particular, is it enough to assume that $\sum_{n\in\omega} 2^{-f(n)}$ diverges, as in Theorem 5.3? The following proposition allows us to rule out this possibility.

Proposition 5.4. *There is a function f such that $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)} < \infty$ but $\sum_{n\in\omega} 2^{-f(n)}$ diverges.*

Proof. We define f in stages. At stage $s+1$ we will define f on an interval $[n_s, n_{s+1})$.

Stage 0. Let $n_0 = 0$.

Stage $s+1$. For each n, there is an $m_s(n) \in [0, 2^s)$ such that $K(m_s(n)\,|\,n^*) \geq s$. Choose n_{s+1} to be the least number such that $\sum_{n\in[n_s,n_{s+1})} 2^{-m_s(n)} \geq 1$. Let $f(n) = m_s(n)$ for all $n \in [n_s, n_{s+1})$.

It is clear that $\sum_{n\in\omega} 2^{-f(n)} = \sum_{s\in\omega} \sum_{n\in[n_s,n_{s+1})} 2^{-f(n)} \geq \sum_{s\in\omega} 1 = \infty$. On the other hand, the minimality of n_{s+1} implies that $\sum_{n\in[n_s,n_{s+1})} 2^{-m_s(n)} \leq 2$. Therefore, $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)} = \sum_{s\in\omega} \sum_{n\in[n_s,n_{s+1})} 2^{-f(n)-K(f(n)\,|\,n^*)} \leq \sum_{s\in\omega} \sum_{n\in[n_s,n_{s+1})} 2^{-f(n)-s} = \sum_{s\in\omega} 2^{-s} \sum_{n\in[n_s,n_{s+1})} 2^{-f(n)} \leq \sum_{s\in\omega} 2^{-s} \cdot 2 = 4$. So f has the desired properties. □

Corollary 5.5. *There is an f such that $\sum_{n\in\omega} 2^{-f(n)} = \infty$ but $(\forall^\infty n)\ K(X \upharpoonright n) \geq n + K(n) - f(n)$ for almost every $X \in 2^\omega$.*

Proof. Immediate from the previous proposition and Theorem 5.1(i). □

The theorems in this section have thus far been stated in terms of the distance between $K(X \restriction n)$ and the upper bound $n+K(n)$. We will now restate Theorem 5.1 in terms of the distance between $K(X \restriction n)$ and n, as in Theorem 3.4. The translation is simple; we essentially take $g(n) = K(n) - f(n)$ and state Theorem 5.1 in terms of $g(n)$. The details are unfortunately somewhat tedious.

Corollary 5.6. *The following are equivalent:*

(i) $\sum_{n\in\omega} 2^{g(n)-K(n,g(n))}$ *diverges.*
(ii) $(\exists^\infty n)\ K(X \restriction n) < n + g(n)$ *with nonzero measure.*
(iii) $(\exists^\infty n)\ K(X \restriction n) < n + g(n)$ *for almost every* $X \in 2^\omega$*.*

Proof. Let $f(n) = \max\{K(n) - g(n), 0\}$. First assume that $g(n) > K(n)$ only finitely often. So for almost all n, we have $K(f(n) \mid n^*) = K(K(n) - g(n) \mid n^*) = K(g(n) \mid n^*) + O(1)$, where the last holds because $K(n) = |n^*|$ can be determined from n^*. Using the symmetry of information, $-f(n) - K(f(n) \mid n^*) = K(n) - f(n) - K(n) - K(g(n) \mid n^*) + O(1) = g(n) - K(n, g(n)) + O(1)$ with finitely many exceptions. So $\sum_{n\in\omega} 2^{g(n)-K(n,g(n))}$ diverges iff $\sum_{n\in\omega} 2^{-f(n)-K(f(n) \mid n^*)}$ diverges. The fact that $g(n) = K(n) - f(n)$ for almost all n implies that $(\exists^\infty n)\ K(X \restriction n) < n + g(n)$ iff $(\exists^\infty n)\ K(X \restriction n) < n + K(n) - f(n)$. It now follows from Theorem 5.1(ii) that (i) implies (iii). Similarly, the contrapositive of Theorem 5.1(ii) gives (ii) implies (i). Finally, (iii) obviously implies (ii). Therefore, the three conditions are equivalent under the assumption that $g(n) > K(n)$ only finitely often.

We must now deal with the case when $g(n) > K(n)$ for infinitely many $n \in \omega$. If this holds, then $f(n) = 0$ infinitely often. But then $f(n) + K(f(n) \mid n^*)$ infinitely often takes the same value, so $\sum_{n\in\omega} 2^{-f(n)-K(f(n) \mid n^*)}$ diverges. Therefore, Theorem 5.1(ii) implies that $(\exists^\infty n)\ K(X \restriction n) < n + K(n) - f(n)$ for almost every X. But $g(n) \geq K(n) - f(n)$, so $(\exists^\infty n)\ K(X \restriction n) < n + g(n)$ for almost every X. Hence (iii) and, *a fortiori*, (ii) hold. We must also show that (i) holds in this case. If $g(n) > K(n)$, then $g(n) - K(n, g(n)) = g(n) - K(n) - K(g(n) \mid n^*) + O(1) = g(n) - K(n) - K(g(n) - K(n) \mid n^*) + O(1) \geq g(n) - K(n) - 2\log(g(n) - K(n)) + O(1) \geq O(1)$. This is true infinitely often, hence $\sum_{n\in\omega} 2^{g(n)-K(n,g(n))}$ diverges. □

The series in Corollary 5.6(i) is no easier to understand than its counterpart in Theorem 5.1. It may not be at all clear for a given g whether $\sum_{n\in\omega} 2^{g(n)-K(n,g(n))}$ diverges. By the following result, it is sufficient to prove that $\sum_{n\in\omega} 2^{-g(n)}$ converges, which should often be easier to determine.

Proposition 5.7. $\sum_{n\in\omega} 2^{g(n)-K(n,g(n))}$ *and* $\sum_{n\in\omega} 2^{-g(n)}$ *cannot both converge.*

Proof. Assume that both series converge. Because $K(n, g(n)) \leq K(n) + K(g(n)) + O(1)$ and $K(g(n)) \leq 2\log(g(n)) + O(1) \leq g(n)/2 + O(1)$, there is a c such that $g(n) - K(n, g(n)) + c \geq g(n)/2 - K(n)$. Therefore,

$$\sum_{n\in\omega} 2^{g(n)/2-K(n)} \leq \sum_{n\in\omega} 2^{g(n)-K(n,g(n))+c} < \infty$$

It follows from the monotonicity of exponentiation that $2^a + 2^b \geq 2^{(2/3)a+(1/3)b}$, for all $a, b \in \mathbb{R}$.[6] Thus,

$$\sum_{n\in\omega} 2^{-(2/3)K(n)} \leq \sum_{n\in\omega} 2^{g(n)/2-K(n)} + \sum_{n\in\omega} 2^{-g(n)} < \infty.$$

[6] In fact, the convexity of the exponential function implies that $(2/3)2^a + (1/3)2^b \geq 2^{(2/3)a+(1/3)b}$, but this tighter inequality is unnecessary here.

But this gives us a contradiction: there is a c such that $K(n) \leq (3/2)\log n + c$, which implies that $\sum_{n\in\omega} 2^{-(2/3)K(n)} \geq \sum_{n\in\omega} 2^{-\log n - c} = \infty$. $\square$

Corollary 5.8. *If $\sum_{n\in\omega} 2^{-g(n)}$ converges, then $(\exists^\infty n)\ K(X\restriction n) < n + g(n)$ for almost every $X \in 2^\omega$.*

Proof. Immediate from Proposition 5.7 and Corollary 5.6. $\square$

It is not difficult to refute the converse of this corollary. Consider $g(n) = \log n$. On the one hand, $\sum_{n\in\omega} 2^{-g(n)}$ diverges. But $g(n) - K(n, g(n)) \geq \log n - 2\log n - O(1) = -\log n - O(1)$, so $\sum_{n\in\omega} 2^{g(n)-K(n,g(n))}$ also diverges. Hence by Corollary 5.6(iii), $(\exists^\infty n)\ K(X\restriction n) < n + g(n)$ for almost every X. To some extent this example is misleadingly specific; if g is *any* unbounded computable function, then $\limsup_{n\to\infty} g(n) - K(n) = \infty$ and hence $(\exists^\infty n)\ K(X\restriction n) < n + g(n)$ for *all* X. Thus any unbounded computable function g for which $\sum_{n\in\omega} 2^{-g(n)}$ diverges is sufficient to refute the converse of Corollary 5.8.

Several of the results in this section are stated for *almost every* $X \in 2^\omega$. It is natural to ask if they hold for every 1-random, which would better match Theorem 3.4 on upward oscillations. The answer in every case is *no*. For example, it is not hard to prove that for any 1-random $X \in 2^\omega$, there exists a function f such that $\sum_{n\in\omega} 2^{-f(n)-K(f(n)\,|\,n^*)}$ converges—in fact, even $\sum_{n\in\omega} 2^{-f(n)}$ converges—but $(\exists^\infty n)\ K(X\restriction n) < n + K(n) - f(n)$. This proves that the conclusion of Theorem 5.1(i) does not necessarily hold for all 1-random reals. Instead of showing this in detail, we will derive the analogous fact for Corollary 5.6.

Fix a 1-random $X \in 2^\omega$. Consider the function $g(n) = \max\{K(X\restriction n) - n, 0\}$. By the ample excess lemma, $\sum_{n\in\omega} 2^{-g(n)}$ converges. So Proposition 5.7 implies that g satisfies Corollary 5.6(i). For all but finitely many values of n, we have $n + g(n) = K(X\restriction n)$. Therefore, it is not true that $(\exists^\infty n)\ K(X\restriction n) < n + g(n)$. So Corollary 5.6(iii) fails for the 1-random real X. For a more satisfying counterexample, apply Lemma 2.1(ii) to get another function h such that $\lim_{n\to\infty} g(n) - h(n) = \infty$ and $\sum_{n\in\omega} 2^{-h(n)}$ still converges. Again, Proposition 5.7 implies that h satisfies Corollary 5.6(i). And yet, $(\forall^\infty n)\ K(X\restriction n) \geq n + h(n) + c$ for every $c \in \omega$.

So we see that it is not, in general, enough for X to be 1-random for it to satisfy the conclusions of the theorems in this section. However, some degree of randomness (depending on the function involved) will be sufficient. The following result illustrates this phenomenon for Corollaries 5.6 and 5.8. We leave the proof to the reader.

Proposition 5.9. *If $(\exists^\infty n)\ K(X\restriction n) < n + g(n)$ for almost every $X \in 2^\omega$, then this holds for every X that is 1-random relative to g.*

6. Applications to the K-degrees

The results of Section 3 have several interesting consequences in the K-degrees. In particular, they let us easily produce comparable 1-random K-degrees, which is non-trivial. In fact, no other method is known.

Theorem 6.1. *For every 1-random $A \in 2^\omega$, there is a 1-random $B \leq_T A \oplus \emptyset'$ such that $B <_K A$.*

Proof. Let $g(n) = K(A\restriction n) - n$ and note that $g \leq_T A \oplus \emptyset'$. By Lemma 2.1(i), there is a function f majorized by g such that $\sum_{n\in\omega} 2^{-f(n)} < \infty$ and $\limsup_{n\to\infty} g(n) -$

$f(n) = \infty$. Furthermore, $f \leq_T g \leq_T A \oplus \emptyset'$. Applying Theorem 3.1 to f produces a 1-random real $B \leq_T f \oplus \emptyset' \leq_T A \oplus \emptyset'$ such that $K(B \upharpoonright n) \leq n + f(n) + O(1)$. But then $K(B \upharpoonright n) \leq n + f(n) + O(1) \leq n + g(n) + O(1) = K(A \upharpoonright n) + O(1)$ for all n. In other words, $B \leq_K A$. Finally, note that $\limsup_{n\to\infty} K(A \upharpoonright n) - K(B \upharpoonright n) \geq \limsup_{n\to\infty} K(A \upharpoonright n) - n - f(n) - O(1) \geq \limsup_{n\to\infty} g(n) - f(n) - O(1) = \infty$. Therefore, $A \not\leq_K B$. □

Corollary 6.2. *For every Δ^0_2 1-random $A \in 2^\omega$ there is a Δ^0_2 1-random real B such that $B <_K A$.*

By weakening the complexity restriction on B in Theorem 6.1, we can replace $<_K$ with what *appears to be* a much stronger relation.

Definition 6.3. For $A, B \in 2^\omega$, we write $B \ll_K A$ to mean that $\lim_{n\in\omega} K(A \upharpoonright n) - K(B \upharpoonright n) = \infty$. We say that B is *strongly K-below* A.

Clearly $B \ll_K A$ implies $B <_K A$; the converse is open.

Theorem 6.4. *For every 1-random $A \in 2^\omega$, there is a 1-random $B \leq_T A'$ such that $B \ll_K A$.*

Proof. First, we wish to find a function g such that $\sum_{n\in\omega} 2^{-g(n)}$ converges and $(\forall n)\ g(n) \leq K(A \upharpoonright n) - n$. In order to control the complexity of B, we also require g to be low over A (otherwise, we could simply let $g(n) = K(A \upharpoonright n) - n$). By the ample excess lemma, there is a $c \in \omega$ such that $\sum_{n\in\omega} 2^{n-K(A\upharpoonright n)} \leq c$. Define a $\Pi^0_1[A]$ class $\mathcal{S} \subseteq \omega^\omega$ by

$$\mathcal{S} = \Big\{ g \in \omega^\omega \colon \sum_{n\in\omega} 2^{-g(n)} \leq c \text{ and } (\forall n)\ g(n) \leq K(A \upharpoonright n) - n \Big\}.$$

Note that $\mathcal{S}$ is computably bounded (meaning that there is a computable function majorizing every member of $\mathcal{S}$) because $K(A \upharpoonright n) - n \leq K(n) + O(1) \leq 2\log n + O(1)$, for all n. Therefore, by the low basis theorem [13] relativized to A, there is a function $g \in \mathcal{S}$ such that $g' \leq_T A'$.

By Lemma 2.1(ii), there is a function f such that $\sum_{n\in\omega} 2^{-f(n)}$ converges and $\lim_{n\to\infty} g(n) - f(n) = \infty$. Furthermore, $f \leq_T g' \leq_T A'$. Finally, apply Theorem 3.1 to f; this produces a 1-random real $B \leq_T f \oplus \emptyset' \leq_T A' \oplus \emptyset' \leq_T A'$ such that $K(B \upharpoonright n) \leq n + f(n) + O(1)$. To complete the proof, note that $\lim_{n\to\infty} K(A \upharpoonright n) - K(B \upharpoonright n) \geq \lim_{n\to\infty} K(A \upharpoonright n) - n - f(n) - O(1) \geq \lim_{n\to\infty} g(n) - f(n) - O(1) = \infty$. □

Now take $A \in 2^\omega$ to be a low 1-random. Then $B \leq_T A' \equiv_T \emptyset'$, which gives us the following result.

Corollary 6.5. *There are Δ^0_2 1-random reals $A, B \in 2^\omega$ such that $B \ll_K A$.*

In the appendix that follows this section we will see that, even in the absence of the Continuum Hypothesis (CH), it is consistent that there are collections of 1-random reals of size $\aleph_1$ with no 1-random lower bound in the K-degrees. The following result shows that any countable collection does have a lower bound.

Proposition 6.6. *There is a 1-random K-degree strongly below every countable collection of 1-random K-degrees.*

Proof. Let $\{A_i\}_{i\in\omega}$ be a sequence of 1-random real numbers. Applying the ample excess lemma and Lemma 2.1(ii), there is a sequence of functions $\{f_i\}_{i\in\omega}$ such that $\sum_{n\in\omega} 2^{-f_i(n)}$ converges and $\lim_{n\to\infty} K(A_i\restriction n) - n - f_i(n) = \infty$. For each i, define $m_i \in \omega$ such that $\sum_{n\geq m_i} 2^{-f_i(n)} \leq 2^{-i}$. Define a function f by $f(n) = \min\{f_i(n) \colon n \geq m_i\}$. Then

$$\sum_{n\in\omega} 2^{-f(n)} \leq \sum_{i\in\omega}\sum_{n\geq m_i} 2^{-f_i(n)} \leq \sum_{i\in\omega} 2^{-i} = 2 < \infty.$$

By Theorem 3.1, there is a 1-random real B such that $K(B\restriction n) \leq n + f(n) + O(1)$. But then,

$$K(A_i\restriction n) - K(B\restriction n) \geq K(A_i\restriction n) - n - f(n) - O(1) \geq K(A_i\restriction n) - n - f_i(n) - O(1),$$

for all $i \in \omega$ and $n \geq m_i$. Therefore, $\lim_{n\to\infty} K(A_i\restriction n) - K(B\restriction n) = \infty$. □

The remaining results in this section explore upper and lower cones in the 1-random K-degrees. First we show that every 1-random is strongly K-above continuum many 1-random reals, and in fact, strongly K-bounds an antichain of size continuum in the 1-random K-degrees.

Lemma 6.7. *For every* 1*-random* $A \in 2^\omega$*, there is another* 1*-random* $B \leq_T A'$ *such that* $B \oplus Z \ll_K A$*, for every* $Z \in 2^\omega$*.*

Proof. As in the proof of Theorem 6.4, there is a function $f \leq_T A'$ such that $\sum_{n\in\omega} 2^{-f(n)}$ converges and $\lim_{n\to\infty} K(A\restriction n) - n - f(n) = \infty$. By Theorem 3.3, there is a 1-random real $B \leq_T f \oplus \emptyset' \leq_T A'$ such that $K((B \oplus Z)\restriction n) \leq n + f(n) + O(1)$, for every $Z \in 2^\omega$. Then $\lim_{n\to\infty} K(A\restriction n) - K((B\oplus Z)\restriction n) \geq \lim_{n\to\infty} K(A\restriction n) - n - f(n) - O(1) = \infty$, so $B \oplus Z \ll_K A$. □

Van Lambalgen [26] proved that if B is 1-random, then $B \oplus Z$ is 1-random iff Z is B-random. Since almost every real is B-random, the lemma implies that there are continuum many 1-random reals strongly K-below A, as promised. We claim that 1-random K-degrees are countable, from which it follows that there are continuum many 1-random K-degrees strongly below A. First, in [21] it is shown that if $X, Y \in 2^\omega$ are 1-random, then $X \leq_K Y$ implies that $Y \leq_{LR} X$, which means that every X-random real is Y-random.[7] Kjos-Hanssen, Miller and Solomon [14] prove that $\leq_{LR}$ is equivalent to another relation, $\leq_{LK}$, which was shown to induce countable equivalence classes by Nies [23]; in particular, he proved that $X \equiv_{LK} Y$ implies $X' \equiv_{tt} Y'$. Putting it all together, 1-random K-degrees are countable and every 1-random $A \in 2^\omega$ strongly bounds continuum many 1-random K-degrees. The next result improves this by giving us an antichain below A.

Proposition 6.8. *For every* 1*-random* $A \in 2^\omega$*, there is an antichain of size continuum in the* 1*-random* K*-degrees strongly below* A*.*

Proof. Let B be the 1-random from Lemma 6.7. Recursively construct an uncountable sequence $\{Z_\alpha \colon \alpha < \omega_1\}$ of 1-random reals such that Z_α is $B \oplus Z_\beta$-random whenever $\beta < \alpha$. Applying Van Lambalgen's theorem (relativized to B) twice, it follows that Z_β is $B \oplus Z_\alpha$-random whenever $\beta < \alpha$.

[7] In the notation of [21], what is actually proved is that $X \leq_K Y$ implies $X \leq_{vL} Y$. But if X and Y are 1-random, then $X \leq_{vL} Y$ is equivalent to $Y \leq_{LR} X$.

Now assume $\alpha \neq \beta$ are countable ordinals. Then Z_α is $B \oplus Z_\beta$-random, but not $B \oplus Z_\alpha$-random, so $B \oplus Z_\alpha \not\leq_{LR} B \oplus Z_\beta$. Similarly, $B \oplus Z_\beta \not\leq_{LR} B \oplus Z_\alpha$. Therefore, $B \oplus Z_\alpha \mid_{LR} B \oplus Z_\beta$, from which it follows that $B \oplus Z_\alpha \mid_K B \oplus Z_\beta$, as we mentioned above [21]. Hence, there is an uncountable antichain of 1-random K-degrees strongly below A. Since the relation $\leq_K$ is a Borel partial order, it follows from a result of Harrington and Shelah (see [11, Corollary 5.2]) that there must be an antichain of size continuum in the 1-random K-degrees strongly below A. □

The situation with upper cones in the K-degrees is somewhat different than that of lower cones. It is even possible, given what we currently know, that there is a maximal 1-random K-degree. We know that upper cones are almost always small; the first author has shown that the cone above a 2-random real is countable [20]. On the other hand, it is possible for the cone above a 1-random in the K-degrees to have size continuum.

Proposition 6.9. *If $\mathcal{S} \subseteq 2^\omega$ is a perfect class of* 1*-random reals, then there is a nonempty perfect subclass $\mathcal{S}' \subseteq \mathcal{S}$ and a* 1*-random $A \in 2^\omega$ such that $A \ll_K Z$ for all $Z \in \mathcal{S}'$.*

Proof. Note that given a perfect class $\mathcal{S}$ of 1-random reals, the statement "there is a nonempty perfect subclass $\mathcal{S}' \subseteq \mathcal{S}$ and a 1-random $A \in 2^\omega$ such that $A \ll_K Z$ for all $Z \in \mathcal{S}'$" is $\mathbf{\Sigma}^1_2$. So by Shoenfiled's absoluteness theorem, we may assume that Martin's Axiom holds and $2^{\aleph_0} > \aleph_1$.

For any $\mathcal{A} \subseteq \mathcal{S}$ of size $\aleph_1$, Theorem 7.4 gives us a 1-random set A such that $A \ll_K X$ for every $X \in \mathcal{A}$. Thus the set $\{Z \in 2^\omega \colon A \ll_K Z \text{ and } Z \in \mathcal{S}\}$ is an uncountable Borel set, hence it contains a perfect subset $\mathcal{S}'$. □

As was mentioned above, if $X, Y \in 2^\omega$ are 1-random, then $X \leq_K Y$ implies that $Y \leq_{LR} X$ [21]. So the previous result implies that there are lower cones of size continuum in the LR-degrees. Barmpalias, Lewis and Soskova [1] show this directly and for a fairly large class of degrees.

Section 5 also has consequences in the K-degrees, but they are modest and are superseded by the authors' earlier results [21].

7. Appendix: Chains of 1-random K-degrees

This section is somewhat independent of the others, except for the proof of Proposition 6.9. Readers having no interest in set theory may skip it. We consider the statement:

($\star$) *Every chain of* 1*-random K-degrees of size less than $2^{\aleph_0}$ has a lower bound in the* 1*-random K-degrees.*

If we assume the Continuum Hypothesis (CH), then ($\star$) follows from Proposition 6.6. We can do better than this; we prove that the statement follows from Martin's Axiom.[8] We also show that it is consistent with ZFC that ($\star$) fails, so it is independent of ZFC.

Since the section is about set theory, we follow set theorists' notation. We use x, y, z to denote reals and A, E, F to denote sets of reals. Define

$$\mathcal{C} = \Big\{ f \in \omega^\omega \colon \sum_{i \in \omega} 2^{-f(i)} \leq 1 \Big\}.$$

[8]For more information about Martin's Axiom, see [12].

We write $f \leq g$ if $f(n) \leq g(n)$ for all but finitely many $n \in \omega$. We will use this notation both for functions in ω^ω and $(\mathbb{Q} \cap [0,1])^\omega$.

7.1. **The positive answer.** In this subsection, we show that Martin's Axiom (MA) implies ($\star$). Define a forcing notation $\mathbb{P} = \langle P, \leq \rangle$ as follows. Let

$$P = \Big\{ \langle n, f \rangle \in \omega \times \omega^\omega \colon \sum_{i<n} 2^{-f(i)} + 2 \sum_{i \geq n} 2^{-f(i)} < 1 \Big\}.$$

We define $\langle n, f \rangle \leq \langle m, g \rangle$ if $n \geq m$, $f \upharpoonright m = g \upharpoonright m$, and g majorizes f, i.e., $(\forall n)\ f(n) \leq g(n)$. It is clear that $\leq$ is a partial order on P.

Lemma 7.1. *$\mathbb{P}$ is a c.c.c. forcing notation.*

Proof. We prove that if $\langle n, f \rangle, \langle n, g \rangle \in P$ and $f \upharpoonright n = g \upharpoonright n$, then $\langle n, f \rangle$ and $\langle n, g \rangle$ are compatible. This implies that any antichain in $\mathbb{P}$ must be countable. Let $h(i) = \min\{f(i), g(i)\}$ for all $i \in \omega$. Without loss of generality, we may assume that $\sum_{i \geq n} 2^{-g(i)} \leq \sum_{i \geq n} 2^{-f(i)}$. So

$$\sum_{i \in \omega} 2^{-h(i)} \leq \sum_{i<n} 2^{-f(i)} + \sum_{i \geq n} 2^{-f(i)} + \sum_{i \geq n} 2^{-g(i)} \leq \sum_{i<n} 2^{-f(i)} + 2 \sum_{i \geq n} 2^{-f(i)} < 1.$$

So we can take $m \geq n$ large enough that $\sum_{i<m} 2^{-h(i)} + 2 \sum_{i \geq m} 2^{-h(i)} < 1$. Thus $\langle m, h \rangle$ is a valid forcing condition. It clearly refines both $\langle n, f \rangle$ and $\langle n, g \rangle$. $\square$

For $g \in \omega^\omega$, let $D_g = \{\langle n, f \rangle \in P \colon f \leq g\}$.

Lemma 7.2. *If $g \in \mathcal{C}$, then D_g is dense.*

Proof. Fix $g \in \mathcal{C}$ and $\langle n, f \rangle \in P$. Since $\sum_{i \in \omega} 2^{-g(i)}$ converges and $\sum_{i \in \omega} 2^{-f(i)} < 1$, we can chose $m \geq n$ large enough that

$$\sum_{i<m} 2^{-f(i)} + 2 \sum_{i \geq m} 2^{-f(i)} + 2 \sum_{i \geq m} 2^{-g(i)} < 1.$$

Let $h(i) = f(i)$ if $i < m$; otherwise let $h(i) = \min\{f(i), g(i)\}$. Then $\langle m, h \rangle$ is a valid condition refining $\langle n, f \rangle$. The definition of h ensures that $h \leq g$, so $\langle m, h \rangle \in D_g$. $\square$

Lemma 7.3. *Assume* MA. *For any $A \subseteq \mathcal{C}$ with $|A| < 2^{\aleph_0}$, there is a function $g \in \mathcal{C}$ such that $(\forall f \in A)\ g \leq f$.*

Proof. By Lemma 7.1, $\mathbb{P}$ is a c.c.c. forcing notation. Lemma 7.2 ensures that D_f is dense for every $f \in A$. By Martin's Axiom, there is a generic set G meeting all of these dense sets. Define $g = \bigcup_{\langle n,h \rangle \in G} h \upharpoonright n$. This is clearly well-defined and total. For any $m \in \omega$, there is a $\langle n, h \rangle \in G$ with $n \geq m$. Since $g \upharpoonright m = h \upharpoonright m$, we have $\sum_{i<m} 2^{-g(i)} = \sum_{i<m} 2^{-h(i)} < 1$. Therefore $\sum_{i \in \omega} 2^{-g(i)} \leq 1$, so $g \in \mathcal{C}$. Finally, take $f \in A$. Since G meets D_f, there is a $\langle n, h \rangle \in G$ such that $h \leq f$. But the definition of g ensures that h majorizes g, so $g \leq f$. $\square$

Now we can prove that ($\star$) follows from Martin's Axiom.

Theorem 7.4. *Assume* MA. *There is a 1-random strongly below every set of size less than $2^{\aleph_0}$ in the 1-random K-degrees.*

Proof. Suppose that $X \subseteq 2^\omega$ is a set of 1-random reals with $|X| < 2^{\aleph_0}$. For each $x \in X$, let $f_x(n) = K(x \upharpoonright n) - n + c_x$, where $c_x \in \omega$ is large enough to ensure that $f_x \in \mathcal{C}$. (This is possible by the ample excess lemma.) Define $A = \{f_x : x \in X\}$. By Lemma 7.3, there is a function $g \in \mathcal{C}$ such that $(\forall x \in X)\ g \leq f_x$. In fact, by Lemma 2.1(ii), we may assume that $\lim_{n\to\infty} f_x(n) - g(n) = \infty$ for all $x \in X$. By Theorem 3.1, there is a 1-random real z so that $K(z \upharpoonright n) \leq n + g(n) + O(1)$. So for any $x \in X$ we have $\lim_{n\to\infty} K(x \upharpoonright n) - K(z \upharpoonright n) \geq \lim_{n\to\infty} n + f_x(n) - n - g(n) + O(1) = \infty$. In other words, the K-degree of z is strongly below each $x \in X$. □

7.2. **The negative answer.** In this subsection, we show that $(\star)$ cannot be proved in ZFC. To do this, we start from a model M that satisfies ZFC + CH. In M, every maximal chain of 1-random K-degrees has size $\aleph_1$. The idea is to extend M by adding lots of reals to destroy CH, while simultaneously ensuring that there is no lower bound in the new model for any maximal chain from M. To do the latter, we extend M to a new model N so that every function in $\mathcal{C} \cap N$ has a lower bound in $\mathcal{C} \cap M$. Recall that Sacks forcing is:

$$\mathbb{S} = \langle \{T : T \text{ is a perfect tree in } 2^{<\omega}\}, \leq \rangle,$$

where $T \leq S$ iff $T \subseteq S$. For more information about Sacks forcing, please see [12]. We use the countable support iterated Sacks forcing of length ω_2, $\mathbb{S}_{\omega_2} = \langle \mathbb{S}_\alpha, \mathbb{S} : \alpha < \omega_2 \rangle$, as in [3].

Lemma 7.5 (Baumgartner and Laver [3])**.** *Assume* CH.

(i) $\mathbb{S}_{\omega_2}$ *preserves cardinals.*
(ii) $\Vdash_{\mathbb{S}_{\omega_2}} 2^{\aleph_0} = \aleph_2$.

Let $\Delta = \{f \in (\mathbb{Q} \cap [0,1])^\omega : \sum_{n\in\omega} f(n) < 1\}$. Bartoszyński and Judah [2, page 302] showed that $\mathbb{S}_{\omega_2}$ has the so-called Δ-*bounding* property. What this means is that $\Vdash_{\mathbb{S}_{\omega_2}} (\forall f \in \Delta)(\exists h \in M \cap \Delta)\ h$ majorizes f. It is not hard to translate this into the property we need. For every $g \in \omega^\omega$, define $h_g(n) = 2^{-g(n)-1}$ for all $n \in \omega$. We have the following lemma.

Lemma 7.6. $(\forall f \in \Delta)(\exists g \in \mathcal{C})\ h_g \geq f$.

Proof. For $f \in \Delta$, define $g \in \omega^\omega$ by

$$g(n) = \begin{cases} m, & \text{where } 2^{-m-2} < f(n) \leq 2^{-m-1} \\ n, & \text{if } f(n) = 0 \text{ or } f(n) > 1/2. \end{cases}$$

Since $f(n) > 1/2$ for only finitely many $n \in \omega$, we have $h_g \geq f$. Note that if the value of $g(n)$ is determined by the first case, then $2^{-g(n)-2} < f(n)$, so $2^{-g(n)} < 4f(n)$. Thus,

$$\sum_{n\in\omega} 2^{-g(n)} \leq \sum_{n\in\omega} 4f(n) + \sum_{n\in\omega} 2^{-n} < 4 + 2 < \infty.$$

It is easy to change finitely many values of g so that $g \in \mathcal{C}$. □

Together with the fact that $\mathbb{S}_{\omega_2}$ has the Δ-*bounding* property, we have:

Lemma 7.7. $\Vdash_{\mathbb{S}_{\omega_2}} (\forall f \in \mathcal{C})(\exists g \in M \cap \mathcal{C})\ g \leq f$.

Proof. Suppose that $p \Vdash \sum_{n\in\omega} 2^{-f(n)} \leq 1$. Then $p \Vdash h_f \in \Delta$, so there is a function $h \in M \cap \Delta$ such that $p \Vdash h$ majorizes h_f. Since $h \in M \cap \Delta$, by Lemma 7.6, there is a function $g \in M \cap \mathcal{C}$ such that $h_g \geq h$. So $h_g \in \Delta$ and $p \Vdash h_g \geq h_f$. Thus $p \Vdash g \leq f$. □

Although we do not need the next result, it illustrates the method we will use in the proof of Theorem 7.9 without reference to the K-degrees.

Lemma 7.8. $\mathrm{ZFC} + \mathrm{Con}(\mathrm{ZFC}) \vdash \mathrm{Con}(\mathrm{ZFC} + \neg\mathrm{CH} + (\exists A \subseteq \mathcal{C})[A$ *is a chain,* $|A| = \aleph_1$ *and* $(\forall f \in \mathcal{C})(\exists g \in A)\ f \not\leq g])$.

Proof. Suppose that $M \models \mathrm{CH} + \mathrm{ZFC}$. By Lemma 7.5(ii), $\Vdash_{\mathbb{S}_{\omega_2}} 2^{\aleph_0} = \aleph_2$. Select a maximal chain A in $M \cap \mathcal{C}$. Then $|A| = \aleph_1$. Note that A is a chain in $M[G]$, for any generic set G, and $|A|^{M[G]} = \aleph_1$, since $\mathbb{S}_{\omega_2}$ preserves cardinals by Lemma 7.5(i). Assume, for a contradiction, that there is an $f \in M[G] \cap \mathcal{C}$ such that $f \leq g$ for every $g \in A$. By Lemma 7.7, there is an $h \in M \cap \mathcal{C}$ such that $h \leq f$. Together with Lemma 2.1, this contradicts the maximality of A. Therefore, there is a $g \in A$ such that $f \not\leq g$. □

Finally, we see that ZFC does not prove ($\star$).

Theorem 7.9. ZFC *does not prove that "Every chain of* 1*-random K-degrees of size less than* $2^{\aleph_0}$ *has a lower bound in the* 1*-random K-degrees."*

Proof. As in the proof of Lemma 7.8, suppose that $M \models \mathrm{ZFC} + \mathrm{CH}$. Select a maximal chain $A \in M$ of 1-random K-degrees. As before, if G is a generic set, then A is a chain in $M[G]$ of size $\aleph_1$. Assume that z is a 1-random real in $M[G]$ such that $z \leq_K x$ for all $x \in A$. By the ample excess lemma, there is a function $f_z(n) = K(z \restriction n) - n + O(1)$ such that $f_z \in M[G] \cap \mathcal{C}$. Then Lemma 7.7 gives us an $h \in M \cap \mathcal{C}$ such that $h \leq f_z$. By Theorem 3.1, there is a 1-random real $y \in M$ such that $K(y \restriction n) \leq n + h(n) + O(1)$. This means that $y \leq_K x$ for all $x \in A$, but no maximal chain in the 1-random K-degrees can have a lower bound by Theorem 6.1. □

References

[1] George Barmpalias, Andrew E. M. Lewis, and Mariya Soskova. Randomness, Lowness and Degrees. *J. of Symbolic Logic*, 73(2):559–577, 2008.
[2] Tomek Bartoszyński and Haim Judah. *Set theory.* A K Peters Ltd., Wellesley, MA, 1995. On the structure of the real line.
[3] James E. Baumgartner and Richard Laver. Iterated perfect-set forcing. *Ann. Math. Logic*, 17(3):271–288, 1979.
[4] Gregory J. Chaitin. A theory of program size formally identical to information theory. *J. Assoc. Comput. Mach.*, 22:329–340, 1975.
[5] Gregory J. Chaitin. Incompleteness theorems for random reals. *Adv. in Appl. Math.*, 8(2):119–146, 1987.
[6] R. Downey and D. Hirschfeldt. *Algorithmic randomness and complexity.* Springer-Verlag, Berlin. To appear.
[7] Rod G. Downey, Denis R. Hirschfeldt, and Geoff LaForte. Randomness and reducibility (extended abstract). In *Mathematical foundations of computer science, 2001 (Mariánské Lázně)*, volume 2136 of *Lecture Notes in Comput. Sci.*, pages 316–327. Springer, Berlin, 2001.
[8] Rod G. Downey, Denis R. Hirschfeldt, and Geoff LaForte. Randomness and reducibility. *J. Comput. System Sci.*, 68(1):96–114, 2004. See [7] for an extended abstract.
[9] Péter Gács. The symmetry of algorithmic information. *Dokl. Akad. Nauk SSSR*, 218:1265–1267, 1974.

[10] Péter Gács. Every sequence is reducible to a random one. *Inform. and Control*, 70(2-3):186–192, 1986.
[11] Leo Harrington, David Marker, and Saharon Shelah. Borel orderings. *Trans. Amer. Math. Soc.*, 310(1):293–302, 1988.
[12] Thomas Jech. *Set theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. The third millennium edition, revised and expanded.
[13] Carl G. Jockusch, Jr. and Robert I. Soare. Π^0_1 classes and degrees of theories. *Trans. Amer. Math. Soc.*, 173:33–56, 1972.
[14] B. Kjos-Hanssen, J. Miller, and R. Solomon. Lowness notions, measure, and domination. In preparation, 20xx.
[15] Antonín Kučera. Measure, Π^0_1-classes and complete extensions of PA. In *Recursion theory week (Oberwolfach, 1984)*, volume 1141 of *Lecture Notes in Math.*, pages 245–259. Springer, Berlin, 1985.
[16] 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.
[17] M. Li and P. Vitányi. *An introduction to Kolmogorov complexity and its applications*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993.
[18] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.
[19] Per Martin-Löf. Complexity oscillations in infinite binary sequences. *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, 19:225–230, 1971.
[20] Joseph S. Miller. The K-degrees, low for K degrees, and weakly low for K sets. In preparation.
[21] Joseph S. Miller and Liang Yu. On initial segment complexity and degrees of randomness. *Trans. Amer. Math. Soc.*, 360(6):3193–3210, 2008.
[22] A. Nies. *Computability and randomness*. Oxford University Press. To appear in the series Oxford Logic Guides.
[23] André Nies. Lowness properties and randomness. *Adv. Math.*, 197(1):274–305, 2005.
[24] Robert M. Solovay. Draft of paper (or series of papers) on Chaitin's work. May 1975. Unpublished notes, 215 pages.
[25] M. van Lambalgen. *Random sequences*. Ph.D. Dissertation, University of Amsterdam, 1987.
[26] Michiel van Lambalgen. The axiomatization of randomness. *J. Symbolic Logic*, 55(3):1143–1167, 1990.
[27] Liang Yu, Decheng Ding, and Rod G. Downey. The Kolmogorov complexity of random reals. *Ann. Pure Appl. Logic*, 129(1-3):163–180, 2004.
[28] A. K. Zvonkin and L. A. Levin. The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms. *Russian Math. Surveys*, 25(6):83–124, 1970.

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

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

Liang Yu, Institute of Mathematical Sciences, Nanjing University, Nanjing, Jiangsu Province 210093, P. R. of China

E-mail address: yuliang.nju@gmail.com