Available at
www.ElsevierMathematics.com
POWERED BY SCIENCE DIRECT®
Annals of Pure and Applied Logic 129 (2004) 163–180
ANNALS OF PURE AND APPLIED LOGIC
www.elsevier.com/locate/apal

The Kolmogorov complexity of random reals☆

Liang Yu[a], Decheng Ding[b], Rodney Downey[a,*]

[a] *Mathematics Department, School of Mathematical and Computing Sciences, Victoria University of Wellington, P.O. Box 600, Wellington, New Zealand*

[b] *Department of Mathematics, Nanjing University, Nanjing, Jiang Su, China*

Received 25 August 2003; received in revised form 9 January 2004; accepted 20 January 2004

Communicated by R.I. Soare

Abstract

We investigate the initial segment complexity of random reals. Let $K(\sigma)$ denote prefix-free Kolmogorov complexity. A natural measure of the relative randomness of two reals α and β is to compare complexity $K(\alpha \upharpoonright n)$ and $K(\beta \upharpoonright n)$. It is well-known that a real α is 1-random iff there is a constant c such that for all n, $K(\alpha \upharpoonright n) \geqslant n - c$. We ask the question, what else can be said about the initial segment complexity of random reals. Thus, we study the fine behaviour of $K(\alpha \upharpoonright n)$ for random α. Following work of Downey, Hirschfeldt and LaForte, we say that $\alpha \leqslant_K \beta$ iff there is a constant $\mathcal{O}(1)$ such that for all n, $K(\alpha \upharpoonright n) \leqslant K(\beta \upharpoonright n) + \mathcal{O}(1)$. We call the equivalence classes under this measure of relative randomness *K-degrees*. We give proofs that there is a random real α so that $\limsup_n K(\alpha \upharpoonright n) - K(\Omega \upharpoonright n) = \infty$ where Ω is Chaitin's random real. One is based upon (unpublished) work of Solovay, and the other exploits a new idea. Further, based on this new idea, we prove there are uncountably many K-degrees of random reals by proving that $\mu(\{\beta : \beta \leqslant_K \alpha\}) = 0$. As a corollary to the proof we can prove there is no largest K-degree. Finally we prove that if $n \neq m$ then the initial segment complexities of the natural n- and m-random sets (namely $\Omega^{\emptyset^{(n-1)}}$ and $\Omega^{\emptyset^{(m-1)}}$) are different. The techniques introduced in this paper have already found a number of other applications.

Keywords: Kolmogorov complexity; Prefix-free; Reducibility; Randomness

☆ Downey is supported by the Marsden Fund for Basic Science in New Zealand. Yu and Ding are supported by NSF of China No.19931020. Additionally, Yu is supported by a postdoctoral fellowship from the New Zealand Institute for Mathematics and its Applications.

* Corresponding author.

E-mail address: downey@math.uuw.ac.nz (R. Downey).

doi:10.1016/j.apal.2004.01.006

1. Introduction

In this paper we will be looking at the algorithmic complexity and relative randomness of reals. There are many settings for such investigations. For definiteness, we will consider reals as elements of Cantor space 2^ω, where the basic open sets are of the form $[\sigma]=\{\sigma\alpha\colon\ \alpha\in 2^\omega\}$. The clopen sets in this topology are finite unions of such basic open sets. The (Lebesgue) measure on this space is induced by $\mu([\sigma])=2^{-|\sigma|}$. This space is not homeomorphic to the real interval $(0,1)$, but is isomorphic in the measure-theoretical sense, and is very convenient for our purposes. One can think of reals an infinite strings or sets by thinking of $\alpha=.A$ in this sense.

There is a long line of reasoning beginning with the work of von Mises [22] seeking to understand the nature of (algorithmic) randomness. A good reference for the delineation of the approaches is van Lambalgen [21]. Our concern in the present paper is one of the most accepted notions of randomness, 1-randomness. This can be defined in several ways. Two celebrated ways are the approaches of Martin-Löf and of Kolmogorov–Solomonoff. Martin-Löf [15] suggested that a real would be random if it passed "effectively presented statistical tests." Consider, for instance, the following consequence of the law of large numbers: If a real $\alpha=.a_1a_2\ldots$ is random then $\lim_n(a_1+\cdots+a_n)/n=\frac{1}{2}$. Then we could consider this a test if we looked at the open set of reals that fail such a test. Martin-Löf dealt with all such tests at once, by saying that a real should be algorithmically random iff it avoided all "effectively given" sets of measure zero. This is formalized as follows.

Definition 1.1 (Martin-Löf [15]). (i) A Martin-Löf test is a computable collection $\{V_n\colon n\in\mathbb{N}\}$ of computably enumerable open sets such that $\mu(V_n)\leqslant 2^{-n}$.

(ii) A real α is said to pass the Martin-Löf test if $\alpha\notin\bigcap_{n\in\mathbb{N}}V_n$.

(iii) Finally, a real is said to be Martin-Löf random if it passes all Martin-Löf tests.

In the same way that computably enumerable sets are just the first level of the arithmetical hierarchy, Martin-Löf random sets can be seen as the first level of a hierarchy of randomness notions. Thus we can replace the V_n by Σ_n sets and we get a notion called n-randomness: a real is n-random iff it passes all Σ_n-Martin-Löf tests. This gives a proper hierarchy 1-random, 2-random, etc. We refer the reader to Downey and Hirschfeldt [6], Kurtz [13], and Kautz [10] for more details. Finally, a real is called *arithmetically* random iff it is n-random for all $n\in\mathbb{N}$. We remark that it is easy to prove that the measure of the set of arithmetically random reals is one. (The n-random reals are, for each n, the complement of the union of countably many sets of measure zero.)

Another fundamental intuition concerning randomness is that a random string should be incompressible. This is the basic intuition of Kolmogorov [11] and Solomonoff [19]. That is, a string σ would be random if, essentially, the only way to generate σ from, say, Turing machine, would be to hardwire σ into the machine. Thus, relative to a universal machine M, the Kolmogorov complexity $C_M(\sigma)$, would be the length of the shortest τ such that $M(\tau)=\sigma$. It is easy to see that one can have a universal M such that for any other $\hat{M}$, $C_M(\sigma)\leqslant C_{\hat{M}}(\sigma)+\mathcal{O}(1)$. Thus we can drop the dependence on M, by fixing such a universal machine. A simple counting argument shows that $C(\sigma) \leqslant |\sigma| + \mathcal{O}(1)$ (for a fixed constant), and for all n there are $\mathcal{O}(2^n)$ strings σ of length n with $C(\sigma) = n$. These are the Kolmogorov random strings.

When this notion is extended to reals one would naturally guess that a real should be random iff all of its initial segments are random as strings. This is more-or-less a good definition, except that one needs to modify the definition of Turing machine to avoid the use of the length of the finite input strings in the programs. (The argument is that on input σ one gets $|\sigma| + \log(|\sigma|)$ much information. This can be used to show that using normal Turing machine Kolmogorov complexity, *no* real has all of initial segments incompressible.)[1] Levin and Chaitin each suggested approaches to circumvent this, the most accessible being Chaitin's notion of a prefix-free machine. A Turing machine U is called prefix-free iff for all v and $\hat{v}$ if $U(v)\downarrow$ and $v \prec \hat{v}$, then $U(\hat{v})\uparrow$. We will let the prefix-free Kolmogorov complexity $K(\sigma)$ be the length of the shortest v such that $U(v) = \sigma$ where U is a universal (minimal) prefix-free Turing machine. Again we can prove fundamental bounds:

Lemma 1.2 (Chaitin [2,3]). (i) $K(\sigma) \leqslant |\sigma| + K(|\sigma|) + \mathcal{O}(1)$.

(ii) $K(x) \leqslant |x| + 2 \log |x| + \mathcal{O}(1)$. (*This is actually a special case of* (i).)

(iii) *For any* k,

$$|\{\sigma : |\sigma| = n \wedge K(\sigma) \leqslant n + K(n) - k\}| \leqslant 2^{n-k+\mathcal{O}(1)}.$$

This leads to a natural definition of randomness:

Definition 1.3 (Levin [14], Zvonkin and Levin [24], Chaitin [2–4], Schnorr [17]). We say a real α is Levin–Chaitin–Schnorr random iff for all n, $K(\alpha \upharpoonright n) \geqslant n - \mathcal{O}(1)$.

The two notions of randomness we have seen are identical.

Theorem 1.4 (Schnorr [17]). *A real α is Chaitin–Schnorr random iff it is Martin-Löf random.*

Notice that if U is a prefix-free machine, then the domain of U is measurable, $\mu(U) = \sum_{U(v)\downarrow} 2^{-|v|}$. Also $\mu(U) \leqslant 1$. Furthermore, the measure of the domain of U is what we call a *left computable*, or *computably enumerable* real: a real α such that $L(\alpha) =_{\text{def}} \{q \in \mathbb{Q}\colon q \leqslant \alpha\}$ is a computable enumerable set of rationals. Such reals are equivalently the limits of computable nondecreasing sequences of rationals. Computably enumerable reals occupy a central position in the study of effective measure and randomness, in the same way as computable enumerable *sets* occupy a central position in classical computability, as we now see.

[1] Specifically, suppose that v is sufficiently long, and take some initial segment τ of v, and suppose that τ is the nth string in the standard length/lexicographic numbering of $2^{<\omega}$. Let σ have length n so that $\tau\sigma \preccurlyeq v$. Then we can construct a machine M which reads input σ, figures out its length, generates τ and outputs $\tau\sigma$ showing that $C(\tau\sigma) \leqslant |\sigma| + \mathcal{O}(1)$.

The most famous example of a computably enumerable set is the halting set $K=\{e: \varphi_e(e)\downarrow\}$. The most famous example of a 1-random computably enumerable real is Chaitin's Ω, the so-called *halting probability*. That is,

$$\Omega = \sum_{U(v)\downarrow} 2^{-|v|},$$

where U is a universal prefix-free machine.

Of course, in classical computability, when we talk about *the* set $K=\{e:\varphi_e(e)\downarrow\}$, we really ought to mention the relevant universal machine. But we do not because we remove the reliance upon the choice of enumeration and universal machine using m-reducibility. Thus $A\leqslant_m B$ iff there is a computable function f, such that for all $x, x\in A$ iff $f(x)\in B$. One of the classical theorems of computability is the result of Myhill that the creative sets are precisely the m-complete sets (i.e. for all c.e. A, $A\leqslant_m B$) and all m-complete sets are the same up to a computable permutation of $\mathbb{N}$. This theorem means that the halting problem is essentially unique up to coding.

Solovay [20] recognized this problem for Ω. He defined the following analytic version of m-reducibility.

Definition 1.5 (Solovay [20]). A real α is called Solovay or domination reducible to β ($\alpha\leqslant_S\beta$) iff there is a constant Q and a partial computable function $\varphi:\mathbb{Q}\mapsto\mathbb{Q}$ such that for all $q<\beta$, $\varphi(q)\downarrow$, $\varphi(q)<\alpha$ and

$$Q(\beta-q) > (\alpha-\varphi(q)).$$

The idea is that however fast I can approximate β I can approximate α just as fast. Solovay called a real *Ω-like* iff $\Omega\leqslant_S\beta$. Calude et al. [1] proved that if a c.e. real is Ω-like, then it is a halting probability of a universal prefix-free machine, and hence a version of Chaitin's Ω.

The present paper falls into the broad agenda of seeking to calibrate randomness of reals. What does it mean for a real to be "more random" than another? What measures should be used, and how do they relate to classical notions of relative complexity, etc. A natural measure suggested by the above is the measure of relative initial segment complexity.

Definition 1.6 (Downey et al. [7]). Let α and β be reals. We say that α is K-reducible[2] to β, $\alpha\leqslant_K\beta$, iff there is a constant $\mathcal{O}(1)$ such that for n,

$$K(\alpha\upharpoonright n) \leqslant K(\beta\upharpoonright n)+\mathcal{O}(1).$$

---

[2] Strictly speaking, it is incorrect to say that this pre-ordering of the reals is a *reducibility* since there is no actual method of generating α from β. But we will abuse terminology and call this ordering a reducibility.

We can also modify the definition above to look at C-reducibility. To do this, we replace K by the non-prefix free C in the definition. As usual we will call the equivalence classes calibrated by a reducibility a *degree*. Clearly, by Schnorr's theorem if a real has higher K-degree than a random real then it is random. Solovay observed that for reals $\alpha \leqslant_S \beta$, $\alpha \leqslant_K \beta$ (and $\alpha \leqslant_K \beta$) so that Solovay reducibility is an example of K-reducibility (and C-reducibility) and hence a measure of relative randomness, at least, as measured by initial segment complexity. Solovay left open the question of whether the analog of Myhill's theorem holds for c.e. reals. This was recently answered by Kucera and Slaman.

Theorem 1.7 (Kucera and Slaman [12]). *Suppose that α is random and c.e. Then for all c.e. reals β, $\beta \leqslant_S \alpha$.*

Thus it follows that there is "only one" c.e. random real (the halting probability of a universal prefix-free Turing machine) in the same way that there is "only one" halting set. The Kucera–Slaman theorem has the following remarkable consequence. If one looks at Lemma 1.2, we see that the initial segment complexity of a real can possibly vary between $n - \mathcal{O}(1)$ and $n + K(n) - \mathcal{O}(1)$. To "qualify" as being random, a real only has to have initial segment complexity above $n - \mathcal{O}(1)$. The Kucera–Slaman Theorem says that all random c.e. reals have "high" complexity (like $n + \log n$) and "low" complexity (like n) at *exactly* the same n's.

The motivating question for this paper is to seek to understand the initial segment complexity for general random reals. To what extent, if any, does the Kucera–Slaman phenomenon hold for all random reals. The point here is that most treatments of randomness are "zero–one" in the sense that all one is concerned with is whether the real in question is random or not. What can be said about the initial segment complexity of random reals? What possible complexities might they have. We will prove the following fundamental theorem.

Theorem 1.8. (i) *For any real α, $\mu(\{\beta\colon \beta \leqslant_K \alpha\}) = 0$.*

(ii) *Consequently since the measure of the set of random reals is* 1, *there are uncountably many K-degrees of random reals.*

The proof that there are, for instance, uncountably many Turing degrees, works by simply observing that $|\{\alpha\colon \alpha \leqslant_T \beta\}| = \aleph_0$, and hence there are $2^{\aleph_0}$ many Turing degrees. This methodology is not available to use here, and we need a measure-theoretical argument, rather than a cardinality one. That is, in spite of the fact that the trivial K-degree (the degree consisting of reals with initial segment complexity identical with $\mathbb{N}$) is countable, there are $2^{\aleph_0}$ many reals $\beta \leqslant_K \Omega$, as we see in this paper.

It is possible to extract from the literature the fact that there are at least two K-degrees containing random sets. The proofs in the literature (such as Solovay [20]) rely upon the fact that, as van Lambalgen [21] remarks, Δ^0_2 sets, being approximable, have different properties than sets in general. We will look at a (new) proof of this fact in Section 2. Some of the material here is due to Solovay, but no proof of

Solovay's material has appeared in the literature, and we include this for completeness, as the proofs are quite short. In Section 3, we will introduce a new technique which allows for more direct control of the initial segment complexity of reals. This technique allows for the construction of uncountably many K-degrees of random reals. Additionally, it allows us to prove that there is *no* greatest K-degree. Again this is not at all obvious, since all of the degrees we construct are uncountable, and there seems no natural join operation in the K-degrees, outside of the c.e. reals. (In the c.e. reals Downey et al. [8] have proven that arithmetical addition, $+$, is a join operator.)

Our notation is relatively standard although we are following one of the traditions by using K for prefix-free Kolmogorov complexity (some authors use H) and C for traditional complexity (whereas some authors use K). We are identifying reals and sets with their characteristic functions. Without loss of generality, all reals are nonrational. We use the notation $\alpha\upharpoonright_n^m$ for the segment of α from lengths n to m inclusive. For other terminology, we refer the reader to Soare [18], Downey and Hirschfeldt [6], and Downey [5]. The classic text for Kolmogorov complexity is Li and Vitanyi [16] and additionally we will refer to van Lambalgen's Thesis [21] and Solovay's notes [20]. These wonderful unpublished notes are often referred to in Li–Vitanyi, especially in the exercises, and the material will be presented in the forthcoming book [6].

We remark that since the writing of this paper, the main result has been used by the first two authors to demonstrate that the number of K-degrees of random reals is $2^{\aleph_0}$. Also the methodology has been used by Yu and Miller to construct a Δ_2^0 real not $\leqslant_K$ below Ω.

2. Random reals, Kolmogorov randomness, Solovay's theorems, and Δ_2^0 reals

Solovay was really the first to propose an analysis of the fine structure of the initial segment complexity of random reals. We remarked that it was already known by Solovay [20] in his studies on the complexity of Ω that there were at least two varieties of random reals in terms of their initial segment complexity. (Explicitly in Solovay's notes it is shown that the K-degrees of Ω and $\Omega^{\emptyset'}$ differ.) This was also noted by van Lambalgen [21]. No proofs have appeared of this fact. For completeness, in this section we give another proof. This short proof is based on unpublished facts from the Solovay material, and a new result on Δ_2^0 reals.

One thing that we did note in the introduction was the fact that no real can have C-complexity $n - \mathcal{O}(1)$ for all n. But there is a natural condition upon initial segments in terms of C-complexity which guarantees Martin-Löf randomness. [3]

[3] Since the submission of the present paper, Miller and Yu have proven that a real α is 1-random iff $\exists^\infty n(C(\alpha\upharpoonright n)>n-K(n)-\mathcal{O}(1))$.

Following [5] we say that a real α is *Kolmogorov random*[4] iff $\exists^{\infty} n(C(\alpha \upharpoonright n) \geqslant n - \mathcal{O}(1))$.

Every Kolmogorov random real is 1-random. As we will see, the measure of the set of Kolmogorov random reals is one. Thus the collection of reals that are Martin-Löf random but not Kolmogorov random is zero. However, Ω is *not* Kolmogorov random. The following proof was suggested by an observation of Fortnow. It counters claims to the contrary in the literature such as Ho [9].

Theorem 2.1. *No Δ_2^0 real (and in particular Ω) is Kolmogorov random.*

Proof. Suppose that $\alpha \leqslant_T \emptyset'$. By the limit lemma, there is a computable function $f(n,s)$ such that $\alpha \upharpoonright n = \lim_s f(n,s)$. Let g be any sufficiently fast growing computable function, such as $g(n) = 2^{2^n}$, say. Let s_n be sufficiently large that $f(g(n),s) = f(g(n),s_n)$ for all $s \geqslant s_n$. Then for $k \geqslant g(n) + s_n$, the following is a short C-program for $\alpha \upharpoonright k$:

The input is n, γ where γ is the part of α of lengths between $g(n)$ and k, which we write as $\gamma = \alpha \upharpoonright_{g(n)}^{k}$. This input has length 2 log n plus $k - g(n)$. Then on this input, we first compute $g(n)$ from n, then scan the length (say t) then calculate $f(g(n),t)$ and output $f(g(n),t)\gamma$, which will equal $\alpha \upharpoonright k$. The length of this program is bounded away from $k - c$ for any c. □

Recall that a real is called n-random iff it passes all Σ_n^0 Martin-Löf tests. Recall that a real is arithmetically random iff it is n-random for all n. The methods of Theorem 2.1 above have been improved recently by Andre' Nies who used a similar argument to show that if α is Kolmogorov random then it is already 2-random. (Specifically, suppose that α is not 2-random. Then for each constant d there is an n such that for some string σ of length less than $n-d$, we have $U^{\emptyset'}(\sigma) = \alpha \upharpoonright n$. Then Nies considers the algorithm which, for sufficiently long input of the form $\sigma\alpha \upharpoonright_n^s$ will output $\alpha \upharpoonright s$ by assuming that $\emptyset'[s]$ is the correct $\emptyset'$-use for $\alpha \upharpoonright n$, and using the fact that U is prefix-free will correctly find σ allowing it to resurrect $\alpha \upharpoonright n$ from some stage onwards.) Nies' result and the one below—that if a real is 3-random then it is Kolmogorov random—lead to the question of clarifying the precise relationships between 3-randomness, Kolmogorov randomness

[4] There are some problems with terminology here. Kolmogorov did not actually construct or even name such reals, but he was the first more or less to define randomness for *strings* via initial segment plain complexity. The first person to actually construct what we are calling Kolmogorov random strings was Martin-Löf, whose name is already associated with 1-randomness. Schnorr was the first person to show that the notions of Kolmogorov randomness and Martin-Löf randomness were distinct. Again we cannot use Schnorr randomness since Schnorr's name is associated with a randomness notion using tests of computable measure. Similar problems occur later with what we call strongly Chaitin random reals. These were never defined by Chaitin, nor constructed by him. They were first constructed by Solovay who has yet another well-known notion of randomness associated with him which is equivalent to 1-randomness. However, again Chaitin *did* look at the associated notion for *finite* strings, where he proved the fundamental lemma that $K(\sigma) \leqslant n + K(|\sigma|) + \mathcal{O}(1)$ which allows for the definition of the reals. It is also known that Loveland in his 1969 ACM paper proposed equivalent notions via uniform Kolmogorov complexity. Again, Loveland's name is commonly associated with yet another notion of complexity Kolmogorov–Loveland stochasticity.

and 2-randomness. In a beautiful recent result, Joe Miller (and, later, independently Nies, Stephan and Terwijn) has proven the other direction from Nies' result to establish that *a real* α *is Kolmogorov random* iff *it is* 2*-random*.

Solovay observed that an arithmetically random real is infinitely often of highest K complexity. We improve this bound to 3. The proof is an analysis of Solovay's.

Lemma 2.2 (After Solovay [20]). (i) *Suppose that* α *is* 3*-random. Then*

$$\exists^{\infty} n(K(\alpha \upharpoonright n) \geqslant n + K(n) - \mathcal{O}(1)).$$

(ii) *Suppose that* $\exists^{\infty} n(K(\alpha \upharpoonright n) \geqslant n + K(n) - \mathcal{O}(1))$. *Then* α *is Kolmogorov random.*

Corollary 2.3. *There exist at least two K-degrees of random sets. Indeed there exists random* α *such that* $\limsup_{n \in \mathbb{N}} (K(\alpha \upharpoonright n) - K(\Omega \upharpoonright n)) = \infty$.

Proof. By the fact that $\mu(\{\alpha : \alpha \text{ is not 3 random}\} = 0$, there is a 3 random set, which is certainly Martin-Löf random. By Theorem 2.1, this cannot have the same K-complexity as Ω, and for such a real the lim sup of the difference will be infinite. □

Proof of Lemma 2.2. (i) We will prove that the natural tests for the property of having infinitely often maximal K-complexity naturally gives rise to a Σ^0_3 Martin-Löf test. This involves a calculation as to the measure of the tests, and an analysis of their definitions. Consider the test $V_c = \{\alpha\colon \exists m \forall n(n \geqslant m) \to K(\alpha \upharpoonright n) \leqslant n + K(n) - c\}$. Now $K \leqslant_T \emptyset'$, and hence V_c is $\Sigma^{\emptyset'}_2$, and hence Σ^0_3. Now we estimate the size of V_c. We show $\mu(V_c) \leqslant \mathcal{O}(2^{-c})$. Let $V_{c,n} = \{\alpha : (\forall m \geqslant n) K(\alpha \upharpoonright m) \leqslant m + K(m) - c\}$. It suffices to get an estimate $\mu(V_{c,n}) = \mathcal{O}(2^{-c})$ uniform in n since $V_c = \bigcup_{n \in \omega} V_{c,n}$. But $\mu(V_{c,n}) \leqslant 2^{-m} |\{\sigma : |\sigma| = m \,\&\, K(\sigma) \leqslant m + K(m) - c\}|$ for any $m \geqslant n$ and, by Chaitin's Theorem 1.2, this last expression is $O(2^{-c})$.

We see that (ii) follows using Solovay's Theorem 2.5 below. □

The proof of (ii) relies on an unpublished result of Solovay whose proof will appear in [6]. The proof is sufficiently short to be included for completeness. Solovay's proof runs as follows. Let

$$m_C(\sigma) = |\sigma| + c_C - C(\sigma)$$

and

$$m_K(\sigma) = |\sigma| + K(|\sigma|) + c_K - K(\sigma).$$

Here c_C and c_K are the relevant coding constants. The idea is that m_C and m_K reflect the distance that a string from being random: *the randomness deficiency of* σ. Note that if $m_K(\sigma)$ is small, then σ is (strongly) Chaitin random, according to Lemma 1.2, in the sense that its K-complexity is as big as it can be. In the same spirit as for the definition of Kolmogorov random reals, we will call a *real strongly Chaitin random* iff $\exists^{\infty} n(K(\alpha \upharpoonright n) > n + K(n) - \mathcal{O}(1))$.

Theorem 2.4 (Solovay [20]). $m_K(\sigma) \geqslant m_C(\sigma) - \mathcal{O}(\log m_C(\sigma) + 2)$.

The following is a restatement of (ii) of Lemma 2.2.

Corollary 2.5. *Every* (*strongly*) *Chaitin random real is Kolmogorov random.*

Proof. Suppose that α is strongly Chaitin random with constant c. If $\alpha \upharpoonright n = \sigma$ is a strongly Chaitin random string, so that its K-complexity is as high as possible, then $m_K(\sigma) \leqslant c$. Thus $m_C(\sigma) - \mathcal{O}(\log m_C(\sigma) + 2) \leqslant c$ for some fixed $\mathcal{O}$ term. Hence $m_C(\sigma) \leqslant c'$ for some fixed c', and hence α is Kolmogorov random. □

Solovay has shown that there are *strings* which are Kolmogorov random but not strongly Chaitin random. We remark that is still unknown if there is a real which is Kolmogorov random but not strongly Chaitin random, a fascinating open question.

Proof of Theorem 2.4. We know $C(\sigma) = |\sigma| + c_C - m_C(\sigma)$. Thus, $K(C(\sigma)) = K(|\sigma| + c_K - m_k(\sigma)) \leqslant K(|\sigma|) + K(c_C - m_C(\sigma)) \leqslant K(|\sigma|) + \mathcal{O}(\log m_C(\sigma) + 2)$. We will need the following fact also proven by Solovay:

$$K(\sigma) \leqslant C(\sigma) + K(C(\sigma)) + \mathcal{O}(1).$$

To see this let U be a universal prefix-free machine and V a universal machine. We will define a prefix-free machine Q via the following.

On input z, Q first attempts to simulate U. Thus its first halting condition is that an input string must have an initial segment in the domain of U. Hence if $z = z_1 z_2$, then Q will first simulate $U(z_1)$. If U happens to halt on an initial segment z_1 of the input, Q will then read exactly $U(z_1)$ further bits of input, if possible. If this does not use up the input completely then Q will not halt. (Hence Q can only halt on strings of the form $z_1 z_2$ where $z_1 \in \mathrm{dom}(U)$ and z_2 has length $U(z_1)$.) Q will then compute $V(z_2)$, and gives this as its output.

Notice that Q is prefix-free because firstly U is, and if C halts on z, then $z = z_1 z_2$ with $U(z_1)\downarrow$, and $|z| = |z_1| + |U(z_1)|$. Thus all extensions of z_1 upon which Q halts have the same length, and hence cannot be prefixes of other such strings. Let π_Q be the coding constant of Q in U.

Let y_3 be a minimal Kolmogorov program for x, and y_1 a minimal prefix-free program for $|y_3|$. Then $U(\pi_Q y_1 y_3) = Q(y_1 y_3) = V(y_3) = x$. Hence $K(\sigma) \leqslant K(\sigma) + K(C(\sigma)) + |\pi_Q|$. This establishes the claim.

By the claim,

$$K(\sigma) \leqslant |\sigma| + K(|\sigma|) + \mathcal{O}(1) + \mathcal{O}(\log m_C(\sigma) + 2) - m_C(\sigma).$$

Thus $0 \leqslant m_K(\sigma) + \mathcal{O}(\log m_C(\sigma) + 2) - m_C(\sigma)$. Hence,

$$m_K(\sigma) \geqslant m_C(\sigma) - \mathcal{O}(\log m_C(\sigma) + 2). \qquad \square$$

3. The initial segment complexity of random reals

In this section we will introduce new techniques which enable us to more directly control the K-complexity of initial segments of random reals. First we remark that mere cardinality arguments will not suffice to construct uncountably many K-degrees of random reals.

Proposition 3.1. *Suppose that α is 1-random. There are $2^{\aleph_0}$ many reals which are K-reducible to α.*

Proof. Define $\mathscr{A} = \mathscr{P}(\{2^n: n \in \mathbb{N}\})$. Evidently, $|\mathscr{A}| = 2^{\aleph_0}$ (note for every $X \subseteq \mathbb{N}$, there is a set $A \in \mathscr{A}$ so that $X \equiv_T A$). For every set A, define $B(A) = \{n: 2^n \in A\}$. Then for every $A \in \mathscr{A}$ and n,

$$\begin{aligned} K(A \upharpoonright n) &\leqslant K(\log n) + K(B(A) \upharpoonright \log n) + c \\ &\leqslant 2 \log n + 4 \log \log n + c' \\ &\leqslant n + c'' \\ &\leqslant K(\alpha \upharpoonright n) + c'''. \end{aligned}$$

Thus $A \leqslant_K \alpha$ for every $A \in \mathscr{A}$. $\square$

Clearly the above argument can be modified to construct $2^{\aleph_0}$ many α K-below a given β, provided that we have some reasonable insight into the growth rate of $K(\beta \upharpoonright n)$. For instance, it would be enough to have some computable function f monotonically going to ∞, and $K(\beta \upharpoonright m) > K(m) + k$ for all $m \geqslant f(k)$. We know that the trivial K-degree is countable. We ask if any other K-degree is countable. The problem seems hard.

The remainder of this section is devoted to a series of lemmata which will allow us to manipulate the initial segment complexity of random reals.

Our arguments for the main results are concerned with the possible growth rate of the complexity. In 1975, Solovay proved that *if f is any computable function with $\sum_{n\in\mathbb{N}} 2^{-f(n)} = \infty$ (such as $f(n) = \log n$), then there are infinitely many n with* $K(\Omega \upharpoonright n) > n + f(n) - \mathcal{O}(1)$. We will need this result. No proof of Solovay's result has appeared. We give simple proofs of two stronger results here. One is that there are for any computable f with $\sum_{n\in\mathbb{N}} 2^{-f(n)} = \infty$ there is a low c.e. real whose initial segment complexity is infinitely often large. The other is a powerful generalization of Solovay's theorem to *any* function f with $\sum_{n\in\mathbb{N}} 2^{-f(n)} = \infty$. This result is one of Joe Miller, and is included here with his permission. It comes from a new characterization of 1-randomness.

Theorem 3.2 (J. Miller, unpublished). *A real α is 1-random iff $\sum_{n\in\mathbb{N}} 2^{n-K(\alpha\upharpoonright n)} < \infty$.*

Proof. One direction is easy. Suppose that α is not 1-random.Then we know that for all c, for infinitely many n, $K(\alpha \upharpoonright n) < n - c$. This means that $\sum_{n\in\mathbb{N}} 2^{n-K(\alpha\upharpoonright n)} = \infty$.

Now for the nontrivial direction. For the other direction, note that, for any $m \in \mathbb{N}$,

$$\sum_{\sigma \in 2^m} \sum_{n \leqslant m} 2^{n-K(\sigma \upharpoonright n)} = \sum_{\sigma \in 2^m} \sum_{\tau \prec \sigma} 2^{|\tau|-K(\tau)}$$
$$= \sum_{\tau \in 2^{\leqslant m}} 2^{m-|\tau|} 2^{|\tau|-K(\tau)} = 2^m \sum_{\tau \in 2^{\leqslant m}} 2^{-K(\tau)} \leqslant 2^m,$$

where the inequality is Kraft's. Therefore, for any $p \in \mathbb{N}$, there are at most $2^m/p$ strings $\sigma \in 2^m$ for which $\sum_{n \leqslant m} 2^{n-K(\sigma \upharpoonright n)} \geqslant p$. This implies that $\mu(\{\alpha \in 2^\omega : \sum_{n \leqslant m} 2^{n-K(\alpha \upharpoonright n)} \geqslant p\}) \leqslant 1/p$. Define $\mathscr{I}_p = \{\alpha \in 2^\omega : \sum_{n \in \mathbb{N}} 2^{n-K(\alpha \upharpoonright n)} \geqslant p\}$. We can express $\mathscr{I}_p$ as a nested union $\bigcup_{m \in \mathbb{N}} \{\alpha \in 2^\omega \mid \sum_{n \leqslant m} 2^{n-K(\alpha \upharpoonright n)} \geqslant p\}$. Each member of the nested union has measure at most $1/p$, so $\mu(\mathscr{I}_p) \leqslant 1/p$. Also note that $\mathscr{I}_p$ is a Σ^0_1 class. Therefore, $\mathscr{I} = \bigcap_{k \in \mathbb{N}} \mathscr{I}_{2^k}$ is a Martin-Löf test. Finally, note that $\alpha \in \mathscr{I}$ iff $\sum_{n \in \mathbb{N}} 2^{n-K(\alpha \upharpoonright n)} = \infty$. Now assume that $\alpha \in 2^\omega$ is 1-random. Then $\alpha \notin \mathscr{I}$, because it misses all Martin-Löf tests, so $\sum_{n \in \mathbb{N}} 2^{n-K(\alpha \upharpoonright n)}$ is finite. □

Corollary 3.3 (Miller, unpublished). *Suppose that f is an arbitrary function with $\sum_{m \in \mathbb{N}} 2^{-f(m)} = \infty$. Suppose that α is* 1*-random. Then there are infinitely many m with $K(\alpha \upharpoonright m) > m + f(m) - \mathcal{O}(1)$.*

Proof. Suppose that for all $m > n_0$, we have $K(\alpha \upharpoonright m) \leqslant m + f(m) - \mathcal{O}(1)$. Fix $m > n_0$. Then $n - K(\alpha \upharpoonright m) \geqslant m - (m - f(m) - \mathcal{O}(1)) = -f(m) + \mathcal{O}(1)$. Hence $\sum_{m \in \mathbb{N}} 2^{m-K(\alpha \upharpoonright m)} \geqslant \sum_{m \in \mathbb{N}} 2^{(-f(m)+\mathcal{O}(1))} = \infty$, a contradiction. □

Note that Miller's result says that there are low reals with $K(\alpha \upharpoonright n) > n + f(n) - \mathcal{O}(1)$ infinitely often for any f with $\sum_{n \in \mathbb{N}} 2^{-f(n)} = \infty$. This follows since there are low random reals. The following improves this result for c.e. reals, but only for computable functions f.

Lemma 3.4. *Let f be any computable function such that $\sum_{m \in \mathbb{N}} 2^{-f(m)} = \infty$. Then there is a c.e. real of low Turing degree $\alpha = .A$ such that $K(\alpha \upharpoonright m) \geqslant m + f(m) - \mathcal{O}(1)$, infinitely often.*

Proof. It suffices to construct a c.e. real $\alpha = .A$ to meet for all e the requirements:

N_e $(\exists^\infty s)(\{e\}_s^{A_s}(e)\downarrow) \Rightarrow \{e\}^A(e)\downarrow$,
P_e There exists an interval $I_e = \lim_s I_e^s$ and a number $m_e \in I_e$ so that $K(A \upharpoonright m_e) \geqslant m_e + f(m_e)$.

We give a priority ordering $P_0, N_0, P_1, \ldots$. We use the usual apparatus of modern computability theory. The phrase "initialize" means that all parameters associated with a particular requirement become undefined and a currently satisfied requirement becomes unsatisfied. Also from stage-to-stage uninitialized requirements retain their parameters. The argument is finite injury. We say a requirement $R \in \{N_e, P_e\}$ *requires attention* at stage $s+1$ if

Case 1: $R = N_e$. N_e is currently unsatisfied and s is a stage so that $\{e\}_s^{A_s}(e)\downarrow$.

Case 2: $R = P_e$. Either

(i) there is no interval I_e^s currently defined at stage s for P_e or,
(ii) for every number $q \in I_e^s$, $K_s(A \upharpoonright q) < q + f(q)$.

Construction

Stage 0: Let $A_0 = \emptyset$.

Stage $s+1$: As usual, the highest priority requirement to require attention acts at this stage. Lower priority ones are initialized. Choose the appropriate case below.

Case 1: The requirement is N_e. Declare N_e as satisfied.

Case 2: The requirement is P_e.

Subcase 1: If I_e^s is undefined, select a fresh number (i.e. as usual, bigger than the current stage number, and any previously seen numbers) and let this be $m_{e,s}^0$. Define $m_{e,s}^1$ to be the least number so that $\sum_{m_{e,s}^0 \leqslant x \leqslant m_{e,s}^1} 2^{-f(x)-m_{e,s}^0} > 1$. Let $I_e^s = [m_{e,s}^0, m_{e,s}^1]$.

Subcase 2: If I_e^s is defined, put the largest number $x \in I_e^s$ not in A_s into A_{s+1}. Extract all of the numbers larger than x from A_s. We say that P_e *requires attention at length x and stage s.*

Verification: Define $\alpha = .A = \lim_{s \geqslant 0} A_s$. Since the sequence $.A_s$ as $s \to \infty$ is a non-decreasing sequence of rationals, α is a c.e. real. For every requirement e, we can prove that every requirement require attention at most finitely many times by induction on e, and is met.

There is nothing much to argue for a N_e requirement. Once it has priority, and (hence) all of the earlier requirements cease activity, it will initialize all lower priority requirements when it receives attention. This will protect the $\{e\}^{A_s}(e)\downarrow$ computations forever and hence N_e will be met, and never again receive attention.

For P_e-requirement, go to the least stage s so that it has priority, all the earlier requirements have ceased activity, and hence P_e will never been initialized thereafter. If P_e fails to be met it will require attention too many times. Select the first stage $t \geqslant s$ where it has priority and receives attention. Then lower priority requirements are initialized and the interval $I_e = I_e^t = [m^0(e,t), m^1(e,t)] = [m^0, m^1]$ is defined. If P_e fails to be met, we eventually enumerate every $x \in I_e$ into A. Note that for fixed number $x \in [m^0, m^1]$ there are at least 2^{x-m^0} different strings with a stage $s > t$ and $\sigma = A_s \upharpoonright q$ with $|\sigma| = q$ and $K(\sigma) \leqslant q + f(q)$ (namely the stages at which P_e requires attention at length q).

But $\sum_{|\sigma| \in I_e} 2^{-K(\sigma)} = \sum_{q \in I_e^t} \sum_{|\sigma| = q} 2^{-K(\sigma)} \geqslant \sum_{q \in I_e} 2^{q-m^0} \cdot 2^{-q-f(q)} = \sum_{m^0 \leqslant x \leqslant m^1} 2^{-f(q)-m^0} > 1$, a contradiction. So P_e cannot use up the whole interval and is met, since it receives attention whenever it needs to. It follows that for some final $m_e \in I_e^t$, $K(A \upharpoonright m_e) \geqslant m_e + f(m_e)$. $\square$

We are now ready to begin our proofs concerning the possible initial segment complexity of random reals. The main idea in the following is this: Suppose that α is any given random real. We *know* its length n complexity is at least $n - \mathcal{O}(1)$, *but* it could be as high as $n + K(n) - \mathcal{O}(1)$. Our idea is that

(i) first we argue, as in the C-complexity case, that there must be complexity oscillations where the complexity of α oscillates *downwards* towards n;
(ii) second, we will build a Martin-Löf test *avoiding* the places where the complexity of α oscillates downwards. To do this, we will choose a collection of lengths where we can calculate the measure of the reals avoiding this downward oscillation, allowing us to define a D-Martin-Löf test [5] for infinitely many such avoidances. Since a random real will leave the Martin-Löf test, we can conclude that the real will, infinitely often, have higher K-complexity then the given one.

We will illustrate this with a new proof of Corollary 2.3. In the following section, we will prove that there are uncountably many K-degrees amongst the random reals. Thus the following Lemma is the key. It says that in a relatively controllable way, every so often the complexity of a real will oscillate downwards. This lemma is an analog of the fact that for any real α the C-complexity of $\alpha \upharpoonright n$ will go below n. It will be applied for certain computable f, for the m's of Corollary 3.3.

Lemma 3.5. *For every A and every m, define $n(m)=n$ if $A \upharpoonright m$ is the nth string under the standard length/lexicographic order. Then $K(A \upharpoonright n(m)) \leqslant n(m) + \log(n(m)) + c$ for some constant c.*

Proof. For every $m \in \mathbb{N}$, $A \upharpoonright m$ is the $n(m)$th string under standard lexicographic order. Then $m = \lfloor \log n(m) \rfloor$. [6] Hence, given $n(m)$, we can calculate m with a K-program e.

Thus we claim that $K(A \upharpoonright n(m)) \leqslant K(A \upharpoonright_{m+1}^{n(m)}) + m + c$.

To see this, consider the prefix-free machine M which works as follows. M emulates the universal machine U. When it sees $U(\sigma)\downarrow = \tau$ for some σ, it assumes that this is $\tau = B \upharpoonright_{m+1}^{n(m)}$ for some real B. (This uses the advise of what m is, which takes $\log n(m)$ many bits.) On this assumption, if possible, M calculates $n(m)$ and m. If τ is not of the correct form then $M(\sigma)\uparrow$. M then decodes m as a string v. The output of M, if any, on input σ, will be $v\tau$. Notice that if $U(\sigma) = A \upharpoonright_{m+1}^{n(m)}$ then $M(\sigma) = A \upharpoonright n(m)$.

As a consequence, we see that $K(A \upharpoonright n(m)) \leqslant K(A \upharpoonright_{m+1}^{n(m)}) \leqslant n(m) - m - 1 + 2\log(n(m) - m - 1) + c$ (by Lemma 1.2(ii)) $= n(m) - \log n(m) - 1 + 2\log(n(m) - m - 1) + c \leqslant n(m) - \log n(m) + 2\log(n(m) + c = n(m) + \log n(m) + \mathcal{O}(1)$. □

The fundamental idea we now pursue is that we can build a random real whose complexity is infinitely often up in the places where the complexity of a given real (such as Ω) is down. There *will* be places where the complexity is down as Lemma 3.5 shows. Now how to build a random real to do this. The answer is that we need to build a D-Martin-Löf test *avoiding* the places where the complexity is down. We need some method of controlling the measure of the potential D-Martin-Löf test and this is where we will use Corollary 3.3. That is, we will use m's where Ω's complexity is up.

[5] That is, a Martin-Löf test relative to some oracle D.

[6] Henceforth, we will write $\log q$ whenever we mean $\lfloor \log q \rfloor$, for ease of notation, as this will be clear from the context.

Definition 3.6. Define $\mathscr{D}=\{n$: there is a m so that $\Omega\upharpoonright m$ is the nth string under the standard lexicographic order and $K(\Omega\upharpoonright m)>m+\log m+\log\log m\}$.

Notice that we have used Corollary 3.3, to know that there are infinitely many m with $K(\Omega\upharpoonright m)>m+\log m+\log\log m$. Hence $|\mathscr{D}|=\infty$. By Lemma 3.5, for every $n\in\mathscr{D}$, $K(\Omega\upharpoonright n)\leqslant n+\log n+c$. Note $K(n(m))=K(\Omega\upharpoonright m)-c>m+\log m+\log\log m-c=\log n+\log\log n+\log\log\log n-c'$ for some fixed c'. We now will use a sparse subset of $\mathscr{D}$, allowing us to estimate the size of sets constituting our D-Martin-Löf test.

Lemma 3.7. *There is an infinite set* $\mathscr{D}'\subseteq\mathscr{D}$ *so that* $\sum_{n\in\mathscr{D}'}2^{-\log\log\log n}\leqslant\frac{1}{2}$.

Proof. Define intervals $I_k=(2^{2^{2^k}},2^{2^{2^{k+1}}}](k\geqslant 2)$ and set

$$\mathscr{D}'=\{n_k:n_k=\min(\mathscr{D}\cap I_k)\}\text{ for }\mathscr{D}\cap I_k\neq\emptyset\}.$$

So $\sum_{n\in\mathscr{D}'}2^{-\log\log\log n}\leqslant\sum_{k\geqslant 2}2^{-\log\log\log 2^{2^{2^k}}}=\sum_{k\geqslant 2}2^{-k}=\frac{1}{2}$ and $|\mathscr{D}'|=\infty$. □

Define $U_k=\{y:(\exists n\in\mathscr{D}')[K(y\upharpoonright n)\leqslant n+\log n+\log\log n-k]\}$. Clearly, $U_k\supseteq U_{k+1}$ for every $k\in\mathbb{N}$.

Lemma 3.8. *There is a constant* C *so that* $\mu(U_k)\leqslant C\cdot 2^{-k}$ *for every* k.

Proof.

$$\begin{aligned}\mu(U_k)&=\mu(\{y:(\exists n\in\mathscr{D}')[K(y\upharpoonright n)\leqslant n+\log n+\log\log n-k\})\\&\leqslant\sum_{n\in\mathscr{D}'}\mu(\{y:K(y\upharpoonright n)\leqslant n+\log n+\log\log n-k\})\\&\leqslant\sum_{n\in\mathscr{D}'}C\cdot 2^{-K(n)+\log n+\log\log n-k}\ \text{(by Lemma 1.2(iii))}\\&\leqslant\sum_{n\in\mathscr{D}'}C\cdot 2^{-\log\log\log n-k}\ \text{(by the definition of }\mathscr{D}')\\&\leqslant C\cdot 2^{-k-1}\ \text{(by the definition of }\mathscr{D}).\qquad\square\end{aligned}$$

Thus $\{U_k\colon k\in\mathbb{N}\}$ is a $\mathscr{D}'$-Martin-Löf test. Unraveling the definition of $\mathscr{D}'$, we see that $\{U_k\colon k\in\mathbb{N}\}$ is a Ω-Martin-Löf test and hence a $\emptyset'$-Martin-Löf test. This allows us to give a new proof of 2.3 that there is a random real x so that $\limsup_n K(x\upharpoonright n)-K(\Omega\upharpoonright n)=\infty$. In fact it sharpens the result to make the real x any 2-random real.

Theorem 3.9. *Suppose that* x *is* 2-*random. Then* $\limsup_{n\in\mathbb{N}}K(x\upharpoonright n)-K(\Omega\upharpoonright n)=\infty$.

Proof. We have seen that the collection $\{U_k\colon k\in\mathbb{N}\}$ is a $\emptyset'$-Martin-Löf test. If x is 2-random, $x\notin\bigcap_{k\in\mathbb{N}}U_k$. Hence for almost all $n\in\mathscr{D}'$, for some fixed k, we have $K(x\upharpoonright n)>n+\log n+\log\log n-k$. But for every $n\in\mathscr{D}'$, $K(\Omega\upharpoonright n)\leqslant n+\log n$ and $|\mathscr{D}'|=\infty$. $\square$

Here is another application of the idea showing that for $p\neq q$ the K-degrees of $\Omega^{\emptyset(p)}$ and $\Omega^{\emptyset(q)}$, the "natural" random sets, differ. For ease of notation let $\Omega^d=_{\text{def}}\Omega^{\emptyset(d)}$. Now the method is completely analogous. We define $\mathscr{D}^p=\{n$: there is a m so that $\Omega^p\upharpoonright m$ is the nth string under the standard lexicographic order and $K(\Omega^p\upharpoonright m)>m+\log m+\log\log m\}$. We can then use exactly the same method to refine $\mathscr{D}^p$ to a sparse version $\mathscr{D}^{p'}$, and then define an $\emptyset^{(p)}$-Martin-Löf test. (That is, define $U_k=\{y:(\exists n\in\mathscr{D}^{p'})[K^{\emptyset^{(p)}}(y\upharpoonright n)\leqslant n+\log n+\log\log n-k]\}$, as before.) Then if $q>p$, $\Omega^{(q)}$, will avoid such a Martin-Löf test. This gives the corollary

Corollary 3.10 (with Denis Hirschfeldt). *Suppose that* $p<q$. *Then* $\limsup_{n\in\mathbb{N}}(K(\Omega^q\upharpoonright n)-K(\Omega^p\upharpoonright n))=\infty$.

The methods also show the following.

Corollary 3.11. *Suppose that* α *is* p*-random and* β *is* p-α*-random. Then* $\limsup_{n\in\mathbb{N}}(K(\beta\upharpoonright n)-K(\alpha\upharpoonright n))=\infty$.

Proof. Use the same proof, observing that replacing Ω^p by α results in a $\emptyset^{(p)}\oplus\alpha$ test. Note that $\emptyset^{(p)}\oplus\alpha\leqslant_T\alpha^{(p)}$, giving the result. $\square$

The proof of Theorem 3.9 contains most of ingredients used in the proof of Theorem 4.4.

4. The number of *K*-degrees of random reals

We begin by modifying the definition of $\mathscr{D}$ of the previous section.

Definition 4.1. For $i\geqslant 2$, define
$\mathscr{D}_i=\{n$: there is a m so that $\Omega\upharpoonright m$ is the nth string under the standard length/lexicographic order and $K(\Omega\upharpoonright m)>\sum_{0\leqslant j\leqslant i}\log^{(j)}m\}$.

Again we have that $|\mathscr{D}_i|=\infty$ by Solovay's Theorem 3.3, and for every $n\in\mathscr{D}_i$, $K(\Omega\upharpoonright n)\leqslant n+\log n+c$ by Proposition 3.5.

Note $K(n)=K(\Omega\upharpoonright m)-c>\sum_{0\leqslant j\leqslant i}\log^{(j)}m-c=\sum_{1\leqslant j\leqslant i+1}\log^{(j)}n-c'$ for some fixed c'.

Lemma 4.2. *For every* $i\geqslant 2$, *there is a infinite set* $\mathscr{D}_i'\subseteq\mathscr{D}_i$ *so that* $\sum_{n\in\mathscr{D}_i'}2^{-\log^{(i+1)}n}\leqslant\frac{1}{2}$.

Proof. Define $h(1,k)=2^{2^k}$, $h(i+1,k)=2^{h(i,k)}$ and intervals $I_{i,k}=(h(i,k),h(i,k+1)]$ $(i,k\geqslant 2)$. Set $\mathscr{D}'_i=\{n_{i,k}\colon n_{i,k}=\min(\mathscr{D}_i\cap I_{i,k})$ (if $\mathscr{D}\cap I_{i,k}\neq\emptyset$; otherwise, undefined)$\}$.

So $\sum_{n\in\mathscr{D}'_i} 2^{-\log^{(i+1)} n}\leqslant\sum_{k\geqslant 2} 2^{-\log^{(i+1)} h(i,k)}=\sum_{k\geqslant 2} 2^{-k}=\frac{1}{2}$ and $|\mathscr{D}'_i|=\infty$. □

Define $U_{i,k}=\{y:(\exists n\in\mathscr{D}')[K(y\restriction n)\leqslant\sum_{0\leqslant j\leqslant i}\log^{(j)} n-k]\}$ $(i\geqslant 2)$. We see that $U_{i,k}\supseteq U_{i,k+1}$ for every $k\in\mathbb{N}$.

Lemma 4.3. *For every $i\geqslant 2$, there is a constant C_i so that $\mu(U_{i,k})\leqslant C_i\cdot 2^{-k}$ for every k.*

Proof.

$$
\begin{aligned}
\mu(U_{i,k}) &= \mu\left(\left\{y:(\exists n\in\mathscr{D}')\left[K(y\restriction n)\leqslant\sum_{0\leqslant j\leqslant i}\log^{(j)} n-k\right]\right\}\right)\\
&\leqslant \sum_{n\in\mathscr{D}'_i}\mu\left(\left\{y:K(y\restriction n)\leqslant\sum_{0\leqslant j\leqslant i}\log^{(j)} n-k\right\}\right)\\
&\leqslant \sum_{n\in\mathscr{D}'_i} C_i\cdot 2^{-K(n)+\sum_{1\leqslant j\leqslant i}\log^{(j)} n-k} \quad \text{(by Lemma 1.2)}\\
&\leqslant \sum_{n\in\mathscr{D}'_i} C_i\cdot 2^{-\log^{(i+1)} n-k} \quad \text{(by the definition of } \mathscr{D}'_i)\\
&\leqslant C_i\cdot 2^{-k-1} \quad \text{(by the definition of } \mathscr{D}_i). \qquad \square
\end{aligned}
$$

Define $U_i=\bigcap_k U_{i,k}$, then $\mu(U_i)=0$. Define $U=\bigcup_i U_i$, then $\mu(U)=0$. Thus for every $x\in 2^\omega-U$ and every $i\in\mathbb{N}$ with $i\geqslant 2$, there is a constant $c_{x,i}$ so that $K(x\restriction n)>\sum_{0\leqslant j\leqslant i}\log^{(j)} n-c_{x,i}$ for every $n\in\mathscr{D}'_i$. Define $V=\mathit{Random}\cap(2^\omega-U)$, where *Random* denotes the collection of Martin-Löf random reals, then $\mu(V)=1$ and $x\in V$ iff for every $i\in\mathbb{N}$ with $i\geqslant 2$, there is a constant $k_{x,i}$ so that $K(x\restriction n)>\sum_{0\leqslant j\leqslant i}\log^{(j)} n-k_{x,i}$ for infinitely $n\in\mathbb{N}$.

Theorem 4.4. *There are at least $\aleph_1$ many K-degrees in V.*

Proof. We construct $\aleph_1$ many K-degrees by induction on the ordinals $\alpha<\omega_1$.

Suppose we have constructed random reals $\{x_i\}_{i<\alpha}$ and there are no $i\neq j$ so that $x_i\equiv_K x_j$.

We define a bijection $f:\{x_i\}_{i<\alpha}\to\omega$ and define $y_i=f^{-1}(i)$. It suffices to construct real $z\in V$ so that $\limsup_n K(z\restriction n)-K(y_i\restriction n)=\infty$ for every i.

By Lemma 3.5, for every i and every m, if $y_i\restriction m$ is the nth string under standard lexicographic order then $K(\chi_{y_i}\restriction n)\leqslant n+\log(n)+c_i$ for some constant c_i. Define $\mathscr{F}_i=\{n\colon$ There is a m so that $y_i\restriction m$ is the nth string under standard lexicographic order and $K(y_i\restriction m)>m+\log m+\log\log m\}$. It is clear $|\mathscr{F}_i|=\infty$ and for every $n\in\mathscr{F}_i$, $K(y_i\restriction n)\leqslant n+\log n+c_i$ since $y_i\in V$.

Note $K(n)=K(y_i\upharpoonright m)-c>m+\log m+\log\log m-c=\log n+\log\log n+\log\log\log n-c'$ for some fixed c'_i.

As in Lemma 3.7, there is a set $\mathscr{F}'_i\subseteq\mathscr{F}_i$ with $\sum_{n\in\mathscr{F}'_i}2^{-\log\log\log n}\leqslant\frac{1}{2}$ and $|\mathscr{F}'_i|=\infty$ (because $y_i\in V$ and we can replace this condition for Lemma 3.3).

Define $U_{i,k}=\{y:(\exists n\in\mathscr{F}'_i)[K(y\upharpoonright n)\leqslant n+\log n+\log\log n-k]\}$. Again, $U_{i,k}\supseteq U_{i,k+1}$ for every $k\in\mathbb{N}$ and for every i, there is a constant C so that $\mu(U_{i,k})\leqslant C\cdot 2^{-k}$ for every k as the proof in Lemma 3.8. Set $U_i=\bigcap_k U_{i,k}$ and $U=\bigcup_i U_i$, then $\mu(U_i)=0$ for every i and so $\mu(U)=0$. Thus there is a real say $z\in V-U$. In other words, for every $\beta<\alpha$, $\limsup_n K(z\upharpoonright n)-K(x_\beta\upharpoonright n)=\infty$. Define $x_\alpha=z$. Thus there are at least $\aleph_1$ many K-degrees in V. $\square$

An interesting corollary is an equivalent form of Theorem 4.4.

Corollary 4.5. *There is no largest K-degree. Further, for every real x,* $\mu(\{y:y\leqslant_K x\})=0$.

Proof. Given a real x, if $x\notin V$, then it is clear $\mu(\{y:y\leqslant_K x\})=0$ by the definition of V and the fact that $\mu(V)=1$. Otherwise, by the proof of Theorem 4.4, there is a set U with $\mu(U)=0$ so that if $y\notin U$ then $\limsup_n K(y\upharpoonright n)-K(x\upharpoonright n)=\infty$. Thus $\mu(\{y:y\leqslant_K x\})\leqslant\mu(U)=0$. $\square$

Corollary 4.5 in some sense means that there are no "genuine" random reals.

5. Some questions and consequences

In the original version of the present paper, we asked if there are $2^{\aleph_0}$ many K-degrees of random reals. Yu and Ding [23] used Corollary 4.5 to answer this affirmatively constructing $2^{\aleph_0}$ K-incomparable random reals. We do not know of any examples of *comparable* random reals!

Question 5.1. *Are there random reals x and y with* $x<_K y$?

There might even be *maximal* K-degrees of (random) reals. The following is a weaker form of this possibility.

Question 5.2. *Given a real x, is* $\mu(\{y:x\leqslant_K y\})=0$?

Question 5.3. *What can be said about the K-degrees of* Δ^0_2 *random reals*?

Miller and Yu have shown that there are Δ^0_2 reals $\alpha\nleqslant_K\Omega$. It is unknown if such α can be random but this seems reasonable to conjecture.

Question 5.4. *Can there be pseudo-minimal random reals? That is random* α *such that* $\beta<_K\alpha$ *implies* β *is not random.*

Question 5.5. *We can define $\leqslant_C$ using plain Kolmogorov complexity in place of the prefix-free version. It is known that there are reals $\alpha \leqslant_K \beta$ with $\alpha \not\leqslant_C \beta$. Is the reverse possible or does $\leqslant_C$ imply $\leqslant_K$? What about for c.e. reals.*

References

[1] C. Calude, P. Hertling, B. Khoussainov, Y. Wang, Recursively enumerable reals and Chaitin's Ω number, in: STACS'98, Lecture Notes in Computer Science, vol. 1373, Springer, Berlin, 1998, pp. 596–606.

[2] G.J. Chaitin, A theory of program size formally identical to information theory, J. Assoc. Comput. Mach. 22 (1975) 329–340.

[3] G.J. Chaitin, Incompleteness theorems for random reals, Adv. in Appl. Math. 8 (1987) 119–146.

[4] G.J. Chaitin, Algorithmic Information Theory, Cambridge University Press, Cambridge, 1987.

[5] R.G. Downey, Some computability-theoretical aspects of reals and randomness, in: P. Cholak (Ed.), Lecture Notes in Logic, to appear.

[6] R.G. Downey, D. Hirschfeldt, Algorithmic Randomness and Complexity, Monographs in Computer Science, Springer, Berlin, in preparation.

[7] R. Downey, D. Hirschfeldt, G. Laforte, Randomness and reducibility, J. Comput. Systems Sci. 68 (2004) 96–114 [Extended abstract appeared in: J. Sgall, A. Pultr, P. Kolman (Eds.), Mathematical Foundations of Computer Science, 2001, Lecture Notes in Computer Science, vol. 2136, Springer, Berlin, 2001, pp. 316–327].

[8] R.G. Downey, D.R. Hirschfeldt, A. Nies, F. Stephan, Trivial reals, in: Downey, et al. (Eds.), Proc. of the 7th and 8th Asian Logic Conf., World Scientific, Singapore, 2003, pp. 103–132.

[9] Kejia Ho, Kolmogorov complexity, strong reducibilities, and computably enumerable sets, Ph.D. Thesis, University of Illinois at Urbana-Champaign, 2000.

[10] S. Kautz, Degrees of random sets, Ph.D. Dissertation, Cornell University, 1991.

[11] A.N. Kolmogorov, Three approaches to the quantitative definition of information, Problems of Information Transmission (Problemy Peredachi Informatsii) 1 (1965) 1–7.

[12] A. Kucera, T.A. Slaman, Randomness and recursive enumerability, SIAM J. Comput. 31 (2001) 199–211.

[13] S. Kurtz, Randomness and genericity in the degrees of unsolvability, Ph.D. Dissertation, University of Illinois, Urbana, 1981.

[14] L.A. Levin, On the notion of a random sequence, Soviet Math. Dokl. 14 (1973) 1413–1416.

[15] P. Martin-Löf, The definition of random sequences, Inform. and Control 9 (1966) 602–619.

[16] Ming Li, P. Vitanyi, Kolmogorov Complexity and its Applications, Springer, Heidelberg, 1993.

[17] C.P. Schnorr, Zufälligkeit und Wahrscheinlichkeit, Lecture Notes in Mathematics, vol. 218, Springer, New York, 1971.

[18] R.I. Soare, Recursively Enumerable Sets and Degrees, Springer, Heidelberg, 1987.

[19] R. Solomonoff, A formal theory of inductive inference, part 1 and part 2, Inform. and Control 7 (1964) 224–254.

[20] R.M. Solovay, Draft of paper (or series of papers) on Chaitin's work, unpublished notes, May, 1975, 215pp.

[21] M. van Lambalgen, Random sequences, Ph.D. Dissertation, University of Amsterdam, 1987.

[22] R. von Mises, Grundlagen der Wahrscheinlichkeitsrechnung, Math. Z. 5 (1919) 52–99.

[23] Yu Liang, Ding Decheng, The initial segment complexity of random reals, Proc. Amer. Math. Soc., to appear.

[24] A.K. Zvonkin, 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) (1970) 83–124.