Math. Log. Quart. **50**, No. 6, 613 – 627 (2004) / **DOI** 10.1002/malq.200310121 / www.mlq-journal.org

On Schnorr and computable randomness, martingales, and machines

Rod Downey[*1], **Evan Griffiths**[** 1], and **Geoffrey Laforte**[***2]

[1] School of Mathematical and Computing Sciences, Victoria University of Wellington, P. O. Box 600, Wellington, New Zealand

[2] Computer Science Department, University of West Florida, Pensacola, Fl 32571, U. S. A.

Received 16 December 2003, revised 7 April 2004, accepted 2 March 2004
Published online 30 September 2004

Key words Schnorr randomness, martingale, Kolmogorov complexity.
MSC (2000) 68Q30, 03D15, 03D25

We examine the randomness and triviality of reals using notions arising from martingales and prefix-free machines.

1 Introduction

This paper falls within an overall program articulated in Downey, Hirschfeldt, Nies and Terwijn [8], and Downey and Hirschfeldt [4], of trying to calibrate the algorithmic randomness of reals[1)]. There are three basic approaches to algorithmic randomness. They are to characterize randomness in terms of algorithmic predictability ("a random real should have bits that are hard to predict"), algorithmic compressibility ("a random real should have segments that are hard to describe with short programs"), and measure theory ("a random real should pass all reasonable algorithmic statistical tests").

This last intuition was clarified by Martin-Löf who identified "reasonable algorithmic statistical tests" with c. e. open sets and suggested the following rather successful notion of randomness.

Definition 1 A computably enumerable sequence of open sets $\langle U_n : n \in \omega\rangle$ is a *Martin-Löf test* if and only if for every n, $\mu(U_n) \leq 2^n$.

The intersection of the sets forming any particular Martin-Löf test, $\langle U_n : n \in \omega\rangle$, is a set of measure 0, any real $x \notin \bigcup n \in \omega U_n$ is said to *pass* or *withstand* the test. A real is then *Martin-Löf random* or 1-*random* if it passes all Martin-Löf tests. One of the reasons for the success of this definition is that it is relatively satisfying in that there are *equivalent* natural definitions in terms of the other paradigms.

For example, Schnorr proved that a real α is 1-random iff there is a constant c such that for all n, $K(\alpha \restriction n) \geq n - c$ (see [10, p. 238]). That is, using the notion of prefix-free complexity, a real is 1-random iff its initial segments are incompressible. This also allows for a "natural" Martin-Löf random real. Let U be a universal prefix free machine, then $\Omega = \mu(\mathrm{dom}(\mathsf{U})) = \sum_{\mathsf{U}(\sigma)\downarrow} 2^{-|\sigma|}$ is called *Chaitin's Omega* and is 1-random.

* Corresponding author: e-mail: Rod.Downey@mcs.vuw.ac.nz
** e-mail: griffiths@member.ams.org
*** e-mail: glaforte@uvw.edu

1) In this paper "real" will mean a member of Cantor space 2^ω. We write $2^{<\omega}$ for the set of all finite strings of 0s and 1s (sometimes written $\{0,1\}^*$). The Cantor space is equipped with the topology where the basic clopen sets are $[\sigma] = \{\sigma^\frown\alpha : \alpha \in 2^\omega\}$, for each $\sigma \in 2^{<\omega}$. Such clopen sets have measure $2^{-|\sigma|}$. This space is measure-theoretically identical with the rational interval $(0,1)$, without being homeomorphic to it. It is worth mentioning that our results do not depend on the base 2 – any other finite alphabet would give essentially the same notions of randomness and triviality (see, for example, [17]). We assume that the reader is somewhat familiar with basic Kolmogorov complexity, and the notion of a prefix-free machine, that is, a Turing machine M such that for all σ, if $\mathsf{M}(\sigma)\downarrow$, then for all strings τ with $\sigma \prec \tau$, $\mathsf{M}(\tau)\uparrow$. Prefix-free machines are used in the algorithmic information theory of reals. There is a minimal universal such machine U, in the sense that for all M there is a constant c_{M} such that, for all σ, $K_{\mathsf{U}}(\sigma) \leq K_{\mathsf{M}}(\sigma) + c_{\mathsf{M}}$. Here $K_{\mathsf{D}}(\sigma)$ denotes the Kolmogorov complexity of a string σ relative to a machine D. That is the length of shortest string τ with $\mathsf{D}(\tau) = \sigma$, and ∞ if no τ exists. We let $K(\sigma)$ denote $K_{\mathsf{U}}(\sigma)$. Our basic references are per Li-Vitányi [10], or Chaitin [2].

Ω is a *computably enumerable* (c. e.) (or *left computable*) real in that there is a computable sequence of rationals $r_0 < r_1 \cdots$ whose limit is Ω. (r_i is the measure of the domain of U after i stages of some enumeration.) A real is c. e. iff it is the measure of domain of a prefix-free machine and occupy the same distinguished place in algorithmic randomness that c. e. sets do in classical computability theory. Recent work of Kučera and Slaman ([11]) has shown that, in some sense, Ω is essentially the *only* random c. e. real.

Additionally this prefix-free characterization allows us to compare complexities of reals by defining $\alpha \leq_K \beta$ iff there is a c such that for all n, $K(\alpha \upharpoonright n) \leq K(\beta \upharpoonright n) + c$. Although not a "reducibility" in the intuitive sense, this pre-ordering and the degree structure induced by it is a natural object of study. On the c. e. reals, this degree structure is a dense distributive uppersemilattice, with the top degree, that of Ω, join inaccessible, and the join operation induced by arithmetical addition, $[\alpha] \vee [\beta] = [\alpha + \beta]$ (see [6]). Further results on $\leq_K$ can be found in [8].

1-randomness has a lot of very attractive properties. For instance, it is not hard to construct an effective enumeration U_e^j of all Martin-Löf tests. Given such an enumeration, if we let $V_e = \bigcup_{j\in\omega} U_{j+e+1}^j$, then V_e is a *universal* Martin-Löf test: that is, a real $x \in \bigcap_{e\in\omega} V_e$ if and only if there is a j such that $x \in \bigcap_{e\in\omega} U_e^j$. Using a universal Martin-Löf test, it is easy to show that there are c. e. Martin-Löf random reals. Such tests correspond to universal machines.

So far we have examined the measure-theoretic and compression paradigms. However, if you asked most people what they would regard as "random", we think that they would suggest that the sequence should be "unpredictable". Schnorr (and from another point of view Levin) developed this compelling intuition into a notion of randomness. In particular, knowing the first n bits of a real x should make it no easier to guess the $n{+}1$st bit. Formalizing this intuition leads to the notion of an effective martingale:

Definition 2 A *martingale* is a function $f : 2^{<\omega} \longmapsto \mathbb{R}^+ \cup \{0\}$ such that $f(\sigma) = \frac{1}{2}\big(f(\sigma 0) + f(\sigma 1)\big)$ for all $\sigma \in 2^{<\omega}$. We say that the martingale *succeeds* on a real α, if $\limsup_n F(\alpha \upharpoonright n) = \infty$. A martingale f is *effective* if there is a uniformly computable increasing sequence $f(\sigma)[s]$ of rationals such that, for every $\sigma \in 2^{<\omega}$, $\lim_{s\to\infty} f(\sigma)[s] = f(\sigma)$. A martingale f is *computable* if there is in addition a uniformly computable nonincreasing error function e such that for all $\sigma \in 2^{<\omega}$, $\lim_{s\to\infty} e(\sigma)[s] = 0$ and for all s, $f(\sigma) - f(\sigma)[s] \leq e(\sigma)[s]$.

The idea is that a martingale is a betting strategy, and no "effective" betting strategy should result in winning infinite capital. An extension of the basic fairness criteria is the following basic averaging property.

Theorem 1 (Kolmogorov's inequality) *For any martingale* $F : 2^{<\omega} \longrightarrow \mathbb{R}$, *any* $\sigma \in 2^{<\omega}$, *and any* $a \in \mathbb{R}^+$, $\mu([\sigma] \cap \{\, x : \exists m\, F(x \upharpoonright m) > a \,\}) \leq 2^{-|\sigma|} F(\sigma) a^{-1}$.

Schnorr 14] showed that a real x is Martin-Löf random if and only if no computably enumerable[2)] martingale succeeds on x. Thus all three paradigms have versions which coincide on the class of 1-random reals. An extension of the basic fairness criteria is the following basic averaging property.

Of relevance to our investigation is the following weakening of the notion of a martingale. It is related to Zvonkin and Levin's notion of a semimeasure in [20].

Definition 3 A *supermartingale* is a function $f : 2^{<\omega} \longrightarrow \mathbb{R}^+ \cup \{0\}$ such that $f(\sigma) \geq \frac{1}{2}\big(f(\sigma 0) + f(\sigma 1)\big)$ for all $\sigma \in 2^{<\omega}$. We say that the supermartingale *succeeds* on a real α, if $\limsup_n F(\alpha \upharpoonright n) = \infty$.

In fact, however, in the context of betting strategies, the analogue of the notion of Martin-Löf test is that of effective supermartingale. It is not difficult to construct a computable enumeration of all effective supermartingales, $\langle g_i : i \in \omega \rangle$, by simply enumerating all computable real-valued functions on bit strings and stopping the enumeration of any function while it threatens to fail the supermartingale condition. Schnorr (cf. Levin [9]) noted that letting, for all $\sigma \in 2^{<\omega}$, $f(\sigma) = \sum_{i\in\omega} 2^{-i} g_i(\sigma)$ makes f an effective supermartingale such that for all effective supermartingales g, there is a constant c such that for all $\sigma \in 2^{<\omega}$, $cf(\sigma) \geq g(\sigma)$. Such an f is a *multiplicatively optimal effective supermartingale*. Such an optimal martingale is *a fortiori* universal – if g is any effective supermartingale that succeeds on a real x, then f also succeeds on x. Since a function $f(\sigma)$ is a supermartingale if and only if $2^{-|\sigma|} f(\sigma)$ is a semimeasure in the sense of Zvonkin and Levin, the existence of a multiplicatively optimal supermartingale is also a consequence of the existence of the universal semimeasure in [20].

2) A function f is computably enumerable iff it is approximable from below. That is, there is a computable function g such that $\lim_s g(\sigma, s) = f(\sigma)$ and $g(\sigma, s) \leq g(\sigma, s+1)$.

We will prove here that *super*-martingales are necessary here since there is no effective enumeration of all computably enumerable martingales. As well, in spite of the fact that there is a universal effective martingale, we prove that there is no *multiplicatively optimal effective martingale*.

Schnorr [14] pointed out that the fact that 1-randomness was equivalent to a notion involving effective martingales. Since effective martingales correspond to *computably enumerable* betting strategies rather than *computable* betting strategies, Schnorr argued that 1-randomness is too strong to capture the intuitive notion of effective randomness. He suggested two alternative notions

Definition 4 (Schnorr [14])

(i) We say that a real α is *computably random* iff no *computable* martingale[3)] $F : 2^{<\omega} \longrightarrow \mathbb{Q}^+ \cup \{0\}$ succeeds.

(ii) A real α is a *Schnorr random* iff it passes all Schnorr tests, where a Schnorr test is a Martin-Löf test $\{U_n : n \in \mathbb{N}\}$, but with $\mu(U_n) = 2^{-n}$.

Whilst Lutz and others have used miniaturizations of these notions in computational complexity theory, our understanding of these notions remains relatively poor. A major goal of the present paper is to add to this understanding.

Many basic questions remain. It was a longstanding open question of van Lambalgen and others, for instance, to give a machine characterization of Schnorr or of computable randomness. In [3], Downey and Griffiths gave the first machine characterization of Schnorr randomness.

Theorem 2 (Downey and Griffiths [3]) *We say that a prefix-free machine* M *is computable, if* $\mu(\mathrm{dom}(\mathsf{M}))$ *is a computable real. Then a real* α *is Schnorr random iff for all computable machines* M, $K_{\mathsf{M}}(\alpha \upharpoonright n) > n - O(1)$.

In the same way as for 1-randomness, this allows us to compare the Schnorr complexity of reals. $\alpha \leq_{\mathrm{Sch}} \beta$ iff for all computable machines M there is a computable machine $\widehat{\mathsf{M}}$ such that $K_{\widehat{\mathsf{M}}}(\alpha \upharpoonright n) \leq K_{\mathsf{M}}(\beta \upharpoonright n) + O(1)$, where we regard the right hand side as infinite if some initial segment of β is not in the range of M.

In this paper, we give a the first test characterization of computable randomness, which could be turned into a machine one also. This solves an open problem from Ambos-Spies and Kučera [1]. The characterization is roughly, that a real is computably random iff it passes all "computably graded" tests, which are Martin-Löf tests with kind of a road map to the maximum measure in them.

Next we turn to looking at the interesting notion of *triviality* for Schnorr complexity. Recall that a real is called K*-trivial* if for all n, $K(\alpha \upharpoonright n) \leq K(n) + O(1)$. Solovay [16] showed that noncomputable K-trivial reals exist. Downey, Hirschfeldt, Nies and Stephan [7] gave a simple construction of such reals, and proved that the K-trivial reals gave a natural requirement free solution to Post's problem. Nies has later shown that the Turing degrees of K-trivial reals form a Σ^0_3 ideal in the degrees, and are all low.

In [3], Downey and Griffiths began the study of *Schnorr trivial reals*, where now we ask that $\alpha \leq_{\mathrm{Sch}} 1^\infty$. Downey and Griffiths proved that noncomputable Schnorr trivials exist.

We prove the following: No Schnorr trivial c. e. real is wtt-complete. Schnorr trivials can be Turing complete. If $\alpha \leq_{\mathrm{tt}} \beta$ and β is Schnorr trivial, then α is too, and additionally, the tt-degrees of Schnorr trivials form an ideal in the tt-degrees. Finally, we construct a c. e. Turing degree which contains no Schnorr trivial reals.

The relationship between Turing reducibility and Schnorr triviality remains murky. For one thing, we do not even know whether a Schnorr trivial real must be Δ^0_2. (This is the case for K-trivial reals, since they are all low.) We conjecture that this is false: that in fact every real that is *low for Schnorr* is Schnorr trivial. It would then follow from a result of Terwijn and Zambella [18] that there are 2^ω distinct Schnorr trivials. We can prove that for every low for Schnorr real α there is an infinite increasing sequence $\{\, n_j : j \in \omega \,\}$ on which the real is trivial. In other words, for every computable M, there exists a computable M' and a number c such that that for all j, $K_{\mathsf{M}'}(\alpha \upharpoonright n_j) \leq K_{\mathsf{M}}(1^{n_j}) + c$. For K-triviality, this would be enough: since universal prefix-free machines exist, there is an essentially machine-independent notion of K-complexity. Given any universal prefix-free machine M, for any such sequence, there exist constants c_1, c_2, c_3 such that for every $j \in \omega$,

$$K_{\mathsf{M}}(\alpha \upharpoonright j) \leq K_{\mathsf{M}}(\alpha \upharpoonright n_j) + c_1 \leq K_{\mathsf{M}}(1^{n_j}) + c_2 \leq K_{\mathsf{M}}(1^j) + c_3,$$

3) It is also possible to consider f's that map to the computable reals, but this gives rise to the same notion, a fact established by Schnorr.

and this would make α K-trivial. In the present context, this is not sufficient – in fact, there can be no universal computable machine. We therefore leave the question of there being any arithmetical bound for Schnorr trivials open.

In an earlier draft of the present paper, we had proven that every high c. e. degree contains a Schnorr random real, and, effectivizing a construction of Wang [19], that there were c. e. reals that were Schnorr random but not computably random. Both of these results have been improved by Nies, Stephan and Terwijn [13] who constructed Schnorr but not computably random c. e. reals in every high c. e. degree, and showed that every high c. e. degree contains a computable random c. e. real.

Notation is standard and follows Soare [15].

2 Optimal and universal effective martingales

Above, we referred to Schnorr's construction of a multiplicatively optimal universal effective super-linebreak martingale. It is possible to construct a *universal effective martingale*, i. e., an effective martingale F such that for every real x, $\lim_{n\to\infty} F(x \upharpoonright n) = \infty$ if and only if there exists an effective martingale f such that $\lim_{n\to\infty} f(x \upharpoonright n) = \infty$. We describe the construction, also due to Schnorr. Let $\{ V_e : e \in \omega \}$ be a universal

Martin-Löf test. Each V_e can be approximated by a computable enumeration $V_e[s]$ of finite sets of prefix-free strings, so that $V_e[s] \subseteq V_e[s{+}1] \subseteq V_e$. For convenience, assume that at each stage s there is at most one e such that $V_e[s] \neq V_e[s{+}1]$.

To construct an effective martingale F from $\{ V_e : e \in \omega \}$, we begin with $F(\sigma)[0] = 0$ for all $\sigma \in 2^{<\omega}$. At stage $s+1$, for every σ such that $\sigma \in V_e[s{+}1] - V_e[s]$, we let, for all $\tau \supseteq \sigma$, $F(\tau)[s{+}1] = F(\sigma)[s] + 1$, and, for all $\tau \subset \sigma$, we let $F(\tau)[s{+}1] = F(\sigma)[s] + 2^{|\tau|-|\sigma|}$. It is straightforward to show that F is a martingale, and, clearly, for every real x, $\lim_{n\to\infty} F(x \upharpoonright n) = \infty$ if and only if $x \in \bigcup_{e\in\omega} V_e$.

Given an effective martingale, f, we can form a sequence of sets, $U_e^f = \bigcup\{ [\sigma] : f(\sigma) > 2^e \}$. This is a Martin-Löf test by Kolmogorov's inequality. Suppose $U^f = U^j$ in our enumeration of all effective martingales. Suppose $f(\sigma) > 2^{j+1}$. Choose e largest so that $f(\sigma) > 2^{j+e+1}$. Then $j{+}e{+}2 > \log f(\sigma)$. Also, for all e' with $0 \leq e' \leq e$, $[\sigma] \subset U^j_{j+e'+1}$. This implies $F(\sigma) \geq e{+}1 > \log f(\sigma) - j - 1$. Of course, this implies that F is a universal effective martingale. We can describe F as being *logarithmically optimal* since if f is an effective martingale, there exists a c such that for all $\sigma \in 2^{<\omega}$, $\log f(\sigma) < F(\sigma) + c$.

Recall that the construction of a multiplicatively optimal effective supermartingale depended on the existence of an computable enumeration of all effective supermartingales. It is not hard to show that there can be no computable enumeration of all effective martingales. (We have seen statements to the contrary in the literature, and we can find no proof of the following result but suspect that it might have been known.)

Proposition 3 *There is no effective enumeration of all effective martingales.*

P r o o f. This is a straightforward diagonalization argument. Suppose $\hat{M}_i$, $i \in \omega$, is an effective enumeration of all c. e. martingales, with or without repetition. We can effectively eliminate all martingales that are the constant-zero function to produce an enumeration M_i, $i \in \omega$, of the not-everywhere-zero c. e. martingales in this list. We simply list $\hat{M}_0(\lambda)[0]$, then $\hat{M}_0(\lambda)[s], \ldots, \hat{M}_s(\lambda)[s]$ for increasing values of s and select the least i such that $\hat{M}_i(\lambda)[s] > 0$, and i has not yet been chosen, to appear next in our new enumeration.

We now derive a contradiction by defining a (nowhere-zero) effective martingale N such that for all $i \in \omega$ there exists $\sigma \in 2^{<\omega}$ such that $|\sigma| = i$ and $N(\sigma) \neq M_i(\sigma)$. In fact N will be computable map from $2^{<\omega}$ to $\mathbb{Q}$. If $|\sigma| > 0$, we write σ^c for the string formed from σ by changing only the last bit from 0 to 1 or vice versa. For any string $\tau \neq \lambda$ we set $\tau^- = \tau \upharpoonright (|\tau| - 1)$, that is, the string formed by removing the last bit of τ.

S t a g e 0. Find t such that $M_0(\lambda)[t] = q_0 > 0$ and set $N(\lambda)[0] = q_0/2$.

S t a g e $s + 1$. Find t such that for some string σ of length $s{+}1$ we see $M_{s+1}(\sigma)[t] = q_{n+1} > 0$. Let $N(\sigma)[s{+}1] = \min(N(\sigma^-)[s], q_{n+1}/2)$. Set $N(\sigma^c)[s{+}1] = 2N(\sigma^-)[s] - N(\sigma)[s{+}1]$; notice this value is strictly positive. Set $N(\tau)[s{+}1] = N(\tau^-)[s] > 0$ for all other strings τ of length $s{+}1$.

For every nonempty $\sigma \in 2^{<\omega}$, $N(\sigma^-) = (N(\sigma) + N(\sigma^c))/2$. Clearly, N is a strictly positive c. e. martingale that is not equal to M_i for any i, giving the contradiction. □

In fact, the logarithmically optimal effective martingale is essentially the best one can do: Schnorr's result showing the existence of a multiplicatively optimal supermartingale fails for martingales. So, in fact, Proposition 3 follows from this stronger result.

Theorem 4 (Levin) *There is no multiplicatively optimal effective martingale.*

Proof. Suppose $F : 2^{<\omega} \longrightarrow \mathbb{R}$ is an effective martingale. We build a single martingale G such that for all $i \in \omega$ there exists σ such that $F(\sigma) \not> i/G(\sigma)$. So F, an arbitrary martingale, cannot be optimal.

At stage 0, we set $G(\lambda) = 1$ and $G(1^n) = 1$ for all $n \in \omega$, and also $G(1^n 0) = 1$ for all n. The idea is that on some extension τ of $1^n 0$ we will ensure $F(\tau) \leq G(\tau)/(n+1)$.

At stage $s > 0$ we work on strategies for $n < s$. Fix $n < s$. The strategy to defeat F with $1/(n+1)$ depends on which of finitely many states the strategy lies in at stage s. Let $\sigma_0 = 1^n 0$. Initially, when the strategy is in state 0, if $F(\sigma_0)[s] < 1/(n+1)$, we define $G(\sigma_0 0^k) = 2^k$ for $k = 1{+}s{-}n$, and $G(\tau) = 0$ for all other extensions of σ_0 of length $s{+}1$. At the first stage s where $F(\sigma_0)[s] \geq 1/(n+1)$, we fix $k_0 = s{-}n$ and wait until $\sum_{\tau \in T_0} F(\tau)[s] \geq 2^{k_0+1}/(n+1)$, where T_0 is the set of strings of length $n{+}k_0{+}2$ extending σ_0. This wait is finite since F is a martingale and $F(\sigma_0) \geq 1/(n+1)$. At this stage $G(\sigma_0 0^{k_0}) = 2^{k_0}$. Choose σ_1 to be whichever of $\sigma_0 0^{k_0+1}$ and $\sigma_0 0^{k_0} 1$ gives the smaller value on F at stage s. In other words, $F(\sigma_1)[s] \leq F(\sigma_1^c)[s]$, where τ^c is the string that results from switching the last bit of τ to the opposite value. Then set $G(\sigma_1) = 2^{k_0+1}$, and let $G(\tau)[s] = 0$ for all other extensions τ of $\sigma_0 0^{k_0}$ of length $n{+}k_0{+}1$. Note that $\sum_{\tau \in T_0} F(\tau)[s] - F(\sigma_1)[s] \geq 2^{k_0}/(n{+}1)$. Inasmuch as any $F(\tau)[t]$ can only grow as t increases, if $F(\sigma_1) > G(\sigma_1)/(n{+}1) = 2^{k_0+1}/(n{+}1)$, then $\sum_{\tau \in T_0} F(\tau) \geq 3 \cdot \dfrac{2^{k_0}}{n+1} \cdot F(\sigma_0 0^{k_0}) > \dfrac{2^{k_0+1}}{n{+}1}$. This implies $F(\sigma_0) > \dfrac{3}{2(n+1)}$.

The strategy now enters state 1, and repeats the process, with extensions of σ_1 rather than extensions of σ_0. In general, at stage s in state m, if $F(\sigma_0) \leq \dfrac{2m{+}1}{2} \cdot \dfrac{1}{n{+}1}$, we define $G(\sigma_m 0^k) = 2^{k_{m-1}+l+1}$ for $l \leq s{-}k_{m-1}$, and $G(\tau) = 0$ for all other previously undefined values on extensions of σ_0 of length $\leq s{+}1$. At the first stage s where $F(\sigma_0) > \dfrac{2m{+}1}{2} \cdot \dfrac{1}{n{+}1}$, we let $k_m = s{-}n$ and wait until $\sum_{\tau \in T_m} F(\tau)[t] \geq \dfrac{2m{+}1}{2} \cdot \dfrac{2^{k_m+1}}{n{+}1}$, where T_m is the set of strings of length $n{+}k_m{+}2$ extending σ_0. As before, this wait is finite since F is a martingale and $F(\sigma_0) \geq \dfrac{2m{+}1}{2} \cdot \dfrac{1}{n{+}1}$. At this stage $G(\sigma_m 0^{k_m}) = 2^{k_m}$. Choose σ_{m+1} to be whichever of $\sigma_m 0^{k_m+1}$ and $\sigma_m 0^{k_m} 1$ gives the smaller value on F at stage s. Then set $G(\sigma_{m+1}) = 2^{k_m+1}$, and and let $G(\tau)[s] = 0$ for all other extensions τ of $\sigma_m 0^{k_m}$ of length $n{+}k_m{+}1$. Note that $\sum_{\tau \in T_m} F(\tau)[s] - F(\sigma_{m+1})[s] \geq \dfrac{1}{2} \dfrac{2m{+}1}{2} \dfrac{2^{k_m+1}}{n{+}1}$. Hence, if $F(\sigma_{m+1}) > G(\sigma_{m+1})/(n+1) = 2^{k_m+1}/(n+1)$, then

$$\textstyle\sum_{\tau \in T_m} F(\tau) \geq \dfrac{2^{k_m+1}}{n{+}1} + \dfrac{1}{2} \dfrac{2m{+}1}{2} \dfrac{2^{k_m+1}}{n{+}1} > \dfrac{2(m{+}1){+}1}{2} \dfrac{2^{k_m}}{n{+}1}.$$

Since $|\sigma_{m+1}| - |\sigma_0| = k_m$, this would imply $F(\sigma_0) > (2(m+1)+1)/2(n+1)$.

Since $F(\sigma_0)$ is finite, there must be some least m so that $F(\sigma_0) \leq (2(m+1)+1)/2(n+1)$. We have, therefore, by the above argument, $F(\sigma_{m+1}) \leq G(\sigma_{m+1})/(n+1)$, as required. □

3 Computable randomness and computably graded tests

Schnorr, in [14], argues that because effective martingales can map to any c. e. values, Martin-Löf randomness should be replaced by a wider notion, one obtained by substituting the notion of computability for computable enumerability. Because Martin-Löf randomness can be characterized in terms of either martingales or test sets, this can be done in two ways. The first is to define a real x to be *computably random* if no computable martingale succeeds on x. With some work, this notion can be seen as involving the real passing all the members of a more restricted class of test sets.

Definition 5 A Martin-Löf test $\{V_n\}$ is *computably graded* if there is a computable map $f : 2^{<\omega} \times \omega \longrightarrow \mathbb{R}$ such that, for any $n \in \omega$, $\sigma \in 2^{<\omega}$, and any finite prefix-free set of strings $\{\sigma_i\}_{i \leq I}$ with $\bigcup_{i=0}^{I}[\sigma_i] \subseteq [\tau]$, the following conditions are satisfied:

1. $\mu(V_n \cap [\sigma]) \leq f(\sigma, n)$;
2. $\Sigma_{i=0}^{I} f(\sigma_i, n) \leq 2^{-n}$;
3. $\Sigma_{i=0}^{I} f(\sigma_i, n) \leq f(\tau, n)$;

By combining conditions 1. and 2. it is immediately apparent that $\mu(V_n) \leq 2^{-n}$ for all n. Further, if condition 2. holds for any *finite* prefix free set $\{\sigma_i\}$, then it also holds for any infinite prefix free set of strings: the infinite sum is just the supremum of the associated finite sums, so is also no greater than 2^{-n}. Similarly, since 3. holds for finite prefix free sets it also holds for infinite prefix free sets. If $\bigcup_i [\sigma_i] = [\tau]$, then we can summarize conditions 1.–3. in Definition 5 by the following:

$$\mu(V_n \cap [\tau]) \leq \textstyle\sum_{i=0}^{I} f(\sigma_i, n) \leq f(\tau, n) \leq 2^{-n}.$$

A real x withstands a computably graded test iff $x \notin \bigcap_n V_n$. The computably graded tests give an alternative to the martingale characterization of the notion *computably random*.

Theorem 5 *A real x is computably random if and only if it withstands all computably graded tests.*

The equivalence follows immediately from the following:

Theorem 6

(i) *From a computable martingale $G : 2^{<\omega} \longrightarrow \mathbb{Q}$ we can effectively define a computably graded test (V_n, f) such that for every real x, if $\limsup_j G(x \restriction j) = \infty$, then $x \in \bigcap_n V_n$.*

(ii) *From a computably graded test (V_n, f) we can effectively define a computable martingale $G : 2^{<\omega} \longrightarrow \mathbb{Q}$ such that for every real x, if $x \in \bigcap_n V_n$, then $\limsup_j G(x \restriction j) = \infty$.*

Proof. Showing (i) is relatively simple. Given martingale G we may assume without loss of generality that $G(\lambda) = 1$. Define test sets V_n via $V_n = \{[\sigma] : G(\sigma) \geq 2^n\}$.

Not only does V_n satisfy the property $\mu(V_n) \leq 2^{-n}$ but also $\mu(V_n \cap [\sigma])/\mu(\sigma) \leq G(\sigma)/2^n$. That is, the proportion of $[\sigma]$ that intersects with V_n, which is the proportion for which the martingale G exceeds 2^n, is no greater than $G(\sigma)/2^n$ (a consequence of Kolmogorov's inequality, Theorem 1). If we define a computable function $f : 2^{<\omega} \times \omega \longrightarrow \mathbb{Q}$ by $f(\sigma, n) = G(\sigma)\mu(\sigma)2^{-n}$, then the inequality can be rewritten as $\mu(V_n \cap [\sigma]) \leq f(\sigma, n)$. We also note that for any prefix-free set of strings $\{\sigma_i\}$, $\sum_i f(\sigma_i, n) \leq 2^{-n}$, since $\sum_i f(\sigma_i, n) = 2^{-n} \sum_i G(\sigma_i)\mu(\sigma_i) \leq 2^{-n}$. This inequality on G follows from the fact that the average of G, weighted by $\mu(\sigma_i)$, is $G(\lambda) = 1$, if the strings σ_i partition the entire unit interval. This is clear if the strings σ_i represent all 2^l strings of a fixed length l, the general case follows from this restricted case.

The function f satisfies condition 3. in Definition 5 as a consequence of $G(\bigcup_i \sigma_i) = \sum_i G(\sigma_i)\mu(\sigma_i)$.

Thus V_n and f satisfy 1., 2. and 3. in Definition 5, and furthermore if $\limsup_j G(x \restriction j) = \infty$, then $x \in \bigcap_n V_n$ since, for all n, if $G(x \restriction k_n) \geq 2^n$, then $[x \restriction k_n] \subseteq V_n$.

Establishing (ii) is more involved. We need a preliminary definition:

Definition 6 A function $f : X \longrightarrow \mathbb{R}$ is *co-c. e.* if there exists a computable approximation $f : X \times \omega \longrightarrow \mathbb{Q}$ such that for all $x \in X$, $\lim_{s \to \infty} f(x)[s] = f(x)$ and, for all $s \in \omega$, $f(x)[s] \geq f(x)[s+1]$.

Without loss of generality we may assume, for all n, that $V_{n+1} \subseteq V_n$. Given V_n and f we define the computable martingale $G : 2^{<\omega} \longrightarrow \mathbb{Q}$ via two intermediate functions: $h : 2^{<\omega} \times \omega \longrightarrow \mathbb{R}$, a co-c. e. map, and $J : 2^{<\omega} \longrightarrow \mathbb{R}$, a co-c. e. martingale.

Lemma 3.1 (Schnorr [14]) *From a co-c. e. martingale $J : 2^{<\omega} \longrightarrow \mathbb{R}$ we can effectively find a computable martingale $G : 2^{<\omega} \longrightarrow \mathbb{Q}$ such that for all strings σ, $G(\sigma) \geq J(\sigma)$.*

For a proof in English, see Downey and Hirschfeldt [4].

Thus once we construct our co-c. e. martingale $J : 2^{<\omega} \longrightarrow \mathbb{R}$, such that for every real x, if $x \in \bigcap_n V_n$, then $\limsup_j J(x \restriction j) = \infty$, we are assured of the existence of the necessary effective martingale G.

Let $P_{\sigma,s}$ be the collection of all finite partitions of σ into a finite prefix-free set of strings of length at most $|\sigma| + s$ (for example, $\{\sigma 00, \sigma 01, \sigma 1\} \in P_{\sigma,2}$). Then $P_\sigma = \bigcup_{s\in\omega} P_{\sigma,s}$ is the collection of all finite partitions of σ into a finite prefix-free set of strings. We use an infimum over all partitions $\{\sigma_i : i \in I\}$ in $P_{\sigma,s}$ to define h: Let $h(\sigma, n)[s] = 2^{|\sigma|} \inf_{\{\sigma_i\,:\,i\in I\}\in P_{\sigma,s}} \sum_{i\in I} f(\sigma_i, n)$. Then with $h(\sigma, n) = \lim_{s\to\infty} h(\sigma, n)[s]$, we have a co-c. e. function and $h(\sigma, n)[s] = 2^{|\sigma|} \inf_{\{\sigma_i\,:\,i\in I\}\in P_\sigma} \sum_{i\in I} f(\sigma_i, n)$.

First, note that $2^{|\sigma|}\mu(V_n \cap [\sigma]) \leq h(\sigma, n) \leq 2^{|\sigma|}2^{-n}$ as f satisfies conditions 1. and 2. Each partition of σ into a finite prefix-free set, other than the singleton $\{\sigma\}$, is union of a partition of $\sigma 0$ and a partition of $\sigma 1$. Thus the infimum in the definition of h gives us that, for each n,

$$h(\sigma, n) = \min\big(\tfrac{1}{2}\big(h(\sigma 0, n) + h(\sigma 1, n)\big), 2^{|\sigma|} f(\sigma, n)\big).$$

We claim that $2^{|\sigma|} f(\sigma, n) \geq \frac{1}{2}\big(h(\sigma 0, n) + h(\sigma 1, n)\big)$. Otherwise, dividing both sides by $2^{|\sigma|}$, we would have for all partitions $\{\, \sigma_i : i \in I \,\}$ of σ (other than $\{\sigma\}$) the inequality $f(\sigma, n) < \sum_{i\in I} f(\sigma_i, n)$. But this is not possible by condition 3. on f. Thus, for each n, $h(\sigma, n) = [h(\sigma 0, n) + h(\sigma 1, n)]/2$, so that the function $\lambda\sigma \,.\, h(\sigma, n)$ is a martingale. Hence, we have $0 \leq 2^{|\sigma|}\mu(V_n \cap [\sigma]) \leq h(\sigma, n) \leq 2^{|\sigma|} f(\sigma, n) \leq 2^{|\sigma|}2^{-n}$.

Let $J(\sigma) = \sum_{n=0}^{\infty} h(\sigma, n)$. Clearly $J(\sigma) \leq 2^{|\sigma|}\sum_{n=0}^{\infty} 2^{-n} = 2^{|\sigma|+1}$. J, being a sum of martingales, is obviously a martingale. Let $\sigma = x \restriction k$, and suppose $[\sigma] \subset V_n$. Then

$$J(\sigma) \geq \textstyle\sum_{j=0}^{n} h(\sigma, j) \geq 2^{|\sigma|}\sum_{j=0}^{n} \mu(V_j \cap [\sigma]) = 2^{|\sigma|}(n+1)2^{-|\sigma|} = n + 1.$$

Then since $x \in \bigcap_n V_n$ iff such a σ exists for all n, we have that $x \in \bigcap_n V_n$ implies $\limsup_j J(x \restriction j) = \infty$.

To see that J is co-c. e., we must have an effective way of approximating J from above. Let

$$J(\sigma)[s] = \textstyle\sum_{p=0}^{s} h(\sigma, p)[s] \,+\, \sum_{p=s+1}^{\infty} 2^{|\sigma|}2^{-p}.$$

This is computable as the first sum is a finite sum of computable rational numbers, and the second sum is simply $2^{|\sigma|}2^{-s}$. Since $h(\sigma, p)[s+1] \geq h(\sigma, p)[s]$, and $h(\sigma, s+1)[s+1] \leq 2^{|\sigma|}2^{-(s+1)}$, $J(\sigma)[s+1] \leq J(\sigma)[s]$. Thus J is co-c. e., as required. □

4 Schnorr trivial reals

A change in the notion of randomness that goes further than the shift from Martin-Löf randomness to computable randomness involves a further restriction of the class of allowable test sets, leading to the notion of Schnorr randomness. It was shown in Downey and Griffiths [3] that Schnorr randomness is closely related to another pre-theoretic notion of randomness: one involving the difficulty of describing initial segments of a random real via prefix-free machines with a computable domain. If M is a prefix-free machine, then $\mu(\mathsf{M}) = \sum_{\mathsf{M}(\sigma)\downarrow} 2^{-|\sigma|}$ is a c. e. real. A fundamental result involving such machines is the Kraft-Chaitin inequality, which says not only that such a sum $\sum_{\mathsf{M}(\sigma)\downarrow} 2^{-|\sigma|} \leq 1$ but also that any c. e. sequence of pairs $\langle n_0, \tau_0\rangle, \langle n_1, \tau_1\rangle, \dots$ with the property that $\sum_{i\in\omega} 2^{-i} \leq 1$ can be used to define a prefix-free machine M and a prefix-free set $\{\, \sigma_i : i \in \omega \,\}$ such that for all i, $|\sigma_i| = n_i$ and $\mathsf{M}(\sigma_i) = \tau_i$. If M is a prefix-free machine, then we define the M-*complexity* of a string τ, $K_{\mathsf{M}}(\tau)$, to be the length of the shortest σ such that $\mathsf{M}(\sigma)\downarrow = \tau$. (If τ is not in the range of M, then its M-complexity is ∞.) Schnorr and Chaitin showed that a real x is Martin-Löf random if and only if there is no way for any prefix-free machine to describe its initial segments succinctly: for every prefix-free machine M there is a c such that for every n, $K_{\mathsf{M}}(x \restriction n) > n - c$. Downey and Griffiths [3] showed requiring the measure of the domain of a prefix-free machine to be a computable real leads to an alternative characterization of Schnorr randomness. Notice that no universal prefix-free machine can be computable, since such a machine must have measure equal to a Martin-Löf random real, which must have degree $\mathbf{0}'$. Computable machines can be total, however, in the sense that they can give every string as an output. We have an upper bound on the complexity required of such machines:

Proposition 7 *There is a computable machine,* M*, and a constant* $c \in \omega$ *such that for all finite strings* σ*,* $K_{\mathsf{M}}(\sigma) \leq |\sigma| + 2\log(|\sigma|) + c$

Proof. We describe the machine M and then we check that its domain is a computable real. We should like M to be as close to the identity function as is possible for a prefix-free machine. M maps the string $l(\sigma)^\frown\sigma$ to σ, where $l(\sigma)$ is a special prefix-free coding of $|\sigma|$, consisting of the binary representation of $|x|$ but with every bit repeated, and then the 'end indicator' bits 01. For example, if $\sigma = 1001$, then $|\sigma| = 4$ and $l(\sigma) = 11000001$. So $l(\sigma)\sigma = 110000011001$ and $\mathsf{M}(l(\sigma)\sigma) = \sigma$. The length of $l(\sigma)$ is of the order $2\log(|\sigma|)$, so M maps a string of length order $|\sigma| + 2\log(|\sigma|)$ to σ, and its range is $2^{<\omega}$. The domain of M is prefix-free because the set $L = \{\, l(\sigma) : \sigma \in 2^{<\omega} \,\}$ is prefix-free.

This machine M gives the result, provided $\mu(\mathsf{M})$ is a computable real. Consider all strings σ with $|\sigma| = n$. The the domain of M contains all possible extensions of $l(\sigma)$ of length $|l(\sigma)| + n$, so their combined measure is $2^n 2^{-|l(\sigma)|+n} = 2^{-|l(\sigma)|}$. Hence $\mu(\mathsf{M}) = \sum_{\tau \in L} 2^{-|\tau|}$. There are two strings of length 4 in L (0001 and 1101). There are two strings of length 6 (110001 and 111101) and four strings of length 8. Generally there are 2^i strings of length $2(i+2)$ for each $i \geq 2$. Thus $\mu(\mathsf{M}) = 2^{-3} + 2.2^{-6} + 2^2 \cdot 2^{-8} + 2^3 \cdot 2^{-10} + \cdots = 2^{-3} + 2^{-5} + 2^{-6} + 2^{-7} + \cdots = 2^{-3} + 2^{-4} = 3/16$. □

Machine characterizations of randomness are interesting partly because they allow one to introduce natural reducibilities between reals. These reducibilities can then be used to describe notions of extreme nonrandomness, or triviality. In essence, triviality means there is always a (uniform) shorter way to describe initial segments of x. The machine characterization of Schnorr randomness yields a natural reducibility and notion of triviality that is different from the notions of K-reducibility and K-triviality given by considering all prefix-free machines.

Definition 7 $x \leq_{\mathrm{Sch}} y$ if and only if for every computable machine M there exists a computable machine M' and a constant c such that for every n, $K_{\mathsf{M}'}(x \upharpoonright n) \leq K_{\mathsf{M}}(y \upharpoonright n) + c$. A real x is *Schnorr trivial* if $x \leq_{\mathrm{Sch}} 1^\infty$.

Unlike K-trivial reals, Schnorr trivial reals are not limited in the high-low hierarchy, a fact that follows from the even stronger result below.

Theorem 8 *There is a c. e. complete Schnorr trivial real.*

Proof. As pointed out in [3], any computable machine M is equivalent to some machine M' such that $\mu(\mathsf{M}') = 1$. This fact helps to simplify the proof. We call a computable machine M *total* if $\mu(\mathsf{M}) = 1$ and $\{\, 1^n : n \in \omega \,\} \subset \mathrm{ran}(\mathsf{M})$. It is not hard to approximate whether or not a machine is total in a Π^0_2 manner. To prove the result, we build a c. e. set A and function $g \leq_{\mathrm{T}} A$ satisfying the following two sequences of requirements

R_e : if M_e is a total machine, then there exist a computable machine M'_e and a c such that for all n, $K_{\mathsf{M}'_e}(A \upharpoonright n) \leq K_{\mathsf{M}}(1^n) + c$,

K_i if $i \in K$, then $g(i) \in A$,

where $\langle \mathsf{M}_e : e \in \mathbb{N} \rangle$ is a computable enumeration of all Turing machines with $\mu(\mathsf{M}_e) \leq 1$. This clearly suffices to establish the result.

For general background and notation involving priority arguments, we refer the reader to Soare [15]. The requirement R_e is essentially negative, since the main problem faced in ensuring it is to control the growth of $\mu(\mathsf{M}'_e)$. The main conflict involved in the construction is that arising between a negative requirement R_e and the infinitely many coding markers $g(i)$ used by the K_i for $i \geq e$. The idea is to progressively move each such $g(i)$ to a number large enough to guarantee that $\sum_{j \geq i} K_{\mathsf{M}_e}(1^{g(j)})$ is so small that the total measure that must be added to M'_e for the sake of keeping track of the different membership possibilities for all the $g(j)$ is less than 2^{-i}. What makes this possible is that, if M_e is a computable machine, one can wait for a stage such that $1 - \mu(\mathsf{M}_e)$ is very small, so that one has a very tight estimate on $\sum\{\, K_{\mathsf{M}_e}(1^k) : \mathsf{M}_e$ has not yet produced the string $1^k \,\}$. At such a point, it is easy to move $g(j)$ for $j \geq i$ to these large numbers and ensure thereby that for all $j \geq i$ with $g(j)$ so defined, $\sum_{j \geq i} K_{\mathsf{M}_e} 1^{g(j)}$ is small enough to allow future changes in $\mu(\mathsf{M}')$ to be computably bounded.

Construction.

A number is *fresh at stage s* if it is larger than the length of any string in the range of any Turing machine at stage s. It is also helpful to normalize each machine M so that if $1^n \in \mathrm{ran}(M)[s]$, then for all $k < n$, $1^k \in \mathrm{ran}(\mathsf{M})[s]$. Since we are only interested in total machines, this makes no difference to the satisfaction of any requirement. We use the priority tree $2^{<\omega}$ to control the construction.

Stage 0. $A[0] = \emptyset$, for all k, $g(k)[0] = k$, and all other functionals are undefined.

Stage $s+1$. We define an *approximation to the true path*, $f[s]$, of length $s{+}1$ consisting of the nodes accessible at stage $s{+}1$. For each $e < s$ we perform the following pair of actions:

First, to satisfy K_e, if $e \in K[s{+}1] - K[s]$, we enumerate $g(e)[s] \in A$.

Next, we allow $\alpha = f \restriction e[s]$ to act if necessary as follows: If $s{+}1$ is the first stage since α was last initialized, we declare all $m \leq s$ to be stable for α, let $j^\alpha[s{+}1] = 1$, and immediately end stage $s{+}1$. Let k be the least number that is not stable for α at s. If

(a) $0 \leq 1 - \mu(\mathsf{M}_e)[s] < 2^{-2j^\alpha[s]-3}$,

(b) for all β such that $\beta 0 \subseteq \alpha$, k is stable for β at s, and

(c) $1^{g(k)[s]} \in \operatorname{ran}(\mathsf{M}_e)$,

then enumerate $g(k)[s] \in A[s{+}1]$ and choose, for all $m \geq k$, fresh numbers $g(m)[s{+}1]$ in increasing order. Declare k *stable for* α, set $j^\alpha[s{+}1] = j^\alpha[s]{+}1$, and let $f(n)[s] = 0$, so that $\alpha 0$ is accessible at stage $s{+}1$. Otherwise, take no action for α, and let $f(n)[s] = 1$, so that $\alpha 1$ is accessible at $s{+}1$.

Verification.

First, note that for all k, $g(k)[s]$ is only moved finitely often. There are only a finite number of $\alpha \in 2^{<\omega}$ that are accessible before stage k, and only such α will ever move k. For each such α, there is at most one stage s at which k is the least number that is not yet stable for α and at which $g(k)[s]$ is enumerated into $A[s{+}1]$ by the α-strategy. Hence each such α moves $g(k)[s]$ only finitely often, and so $g(k)[s]$ eventually stops moving. Since $g(k)[s{+}1] \neq g(k)[s]$ implies $g(k)[s] \in A[s{+}1]$, the action taken at the beginning of each stage guarantees that $K \leq_{\mathrm{T}} A$.

Let $f = \liminf_{s\to\infty} f[s]$. Fix e, let $\alpha = f \restriction e$, and let s_0 be the least stage at which α is accessible and is never again initialized . If $\beta 0 \subseteq \alpha$, then eventually each number $k > s_0$ must become stable for β. Also, eventually, each $g(k)[s]$ never changes value. Hence, if $\alpha 1 \subset f$, then either $\mu(\mathsf{M}_e) \neq 1$ or $\{\, 1^n : n \in \omega \,\} \not\subseteq \operatorname{ran}(\mathsf{M}_e)$, so that the requirement is immediately satisfied. So, we may assume $\alpha 0 \subset f$. So, for every $j > 0$ there is a stage $s(j)$ such that $j^\alpha[s] = j$ and $j^\alpha[s{+}1] = j + 1$. At each stage $s(j)$,

(a) $1 - \mu(\mathsf{M}_e)[s(j)] < 2^{-2j-3}$,

(b) $g(s_0 + j)[s(j)] \in A[s(j) + 1]$,

(c) for all $m < g(s_0 + j)[s]$, $1^m \in \operatorname{ran}(\mathsf{M}_e[s])$,

(d) for all $k \geq s_0 + j$, $1^{g(k)[s(j)+1]} \notin \operatorname{ran}(\mathsf{M}_e[s])$, and

(e) for all $k \geq s_0 + j$ and for all $s > s(j)$, $g(k)[s] \neq g(k)[s(j)]$.

For each $m \in \operatorname{ran}(\mathsf{M}_e)[s]$, let $\sigma_m[s]$ be the shortest, lexicographically least string such that $\mathsf{M}_e(\sigma_n)[s] = 1^m$. Clearly, $\lim_{s\to\infty}|\sigma_m[s]| = K_{\mathsf{M}_e}(1^n)$. We will use the Kraft-Chaitin theorem to construct a computable machine M' satisfying the requirement, by enumerating pairs $\langle s, \sigma\rangle$ into a c. e. set R. $g(s_0{+}1)[s(1){+}1]$ is the least number that we have to worry about. So, let $\tau^- = A \restriction (g(s_0{+}1)[s(1){+}1])$, and, for each $m \leq |\tau^-]$, enumerate $\langle K_{\mathsf{M}_e}(1^m) + 2, A \restriction m\rangle$ into $R[s(1)]$. Notice that this adds at most 2^{-2} to the measure of M', since $\mu(\mathsf{M}_e) = 1$. Let $m_1 = |\tau^-|$, and for each $j > 1$, let $m_j = \max\{\, m : 1^m \in \operatorname{ran}(\mathsf{M}[s(j)]) \,\}$. Notice that

$$g(s_0{+}j)[s(j)] \leq m_j < g(s_0{+}j)[s(j){+}1].$$

For each bit string σ with $|\sigma| < j$, let $\tau_\sigma[s(j){+}1]$ be defined by $\tau_\sigma(g(s_0 + k))[s{+}1] = \sigma(k)$ for all $k < j$ and $\tau_\sigma(m)[s(j){+}1] = A(m)$ for all other $m \leq m_j$.

For each $m \leq m_j$, if $\langle |\sigma_m[s(j)]| + 3, \tau_\sigma[s(j){+}1] \restriction m\rangle \notin R[s(j)]$, then enumerate it into $R[s(j){+}1]$. Note that for each $m \leq m_j$, $\langle |\sigma_m[s(j)]| + 3, A[s(j){+}1] \restriction m\rangle \in R[s(j){+}1]$. Since $\lim_{j\to\infty} m_j = \infty$, this shows that for all m, $K_{\mathsf{M}'}(A \restriction m) \leq K_{\mathsf{M}_e}(1^m){+}3$. If $m \leq m_{j-1}$, then $\langle |\sigma_m[s(j)]| + 3, \tau_\sigma[s(j){+}1] \restriction m\rangle$ is enumerated into $R[s(j){+}1]$ only if $\sigma_m[s(j-1)] \neq \sigma_m[s(j)]$. If $m_{j-1} < m \leq m_j$, then $1^m \notin \operatorname{ran}(\mathsf{M}[s(j-1)])$. Hence, if $S = \{\, m : \langle |\sigma_m[s(j)]| + 3, \tau_\sigma[s(j){+}1] \restriction m\rangle$ is enumerated into $R[s(j){+}1] \,\}$, then $\sum_{m\in S} 2^{-|\sigma_m|-3} < 2^{-2(j-1)-6}$. Since there are only 2^j bit strings of length j, this means that the measure of the machine M' is increased by at most at most $2^j \cdot 2^{-2(j-1)-6} = 2^{-j-4}$ at stage $s(j){+}1$. This shows M' is computable. So M' satisfies the requirement. □

Because both complete Schnorr trivial reals exist, and computable Schnorr trivial reals exist, one might wonder whether every c. e. degree contains a Schnorr trivial real. The following theorem yields a negative answer to this question.

Theorem 9 *There exists a c. e. set A such that for all sets B if $B \equiv_{\mathrm{T}} A$, then there exists a computable machine M' such that for all c. e. machines M and numbers c there is an n such that $K_{\mathsf{M}}(B \restriction n) > K_{\mathsf{M}'}(1^n) + c$.*

Proof. We must build a c. e. set satisfying the following sequence of requirements:

$\mathrm{R}_{\Phi,\Psi}$: if $\Psi(\Phi(A)) = A$, then there exists a computable machine M' such that for each machine M and each c there exists an n such that $K_{\mathsf{M}}(\Phi(A) \restriction n) > K_{\mathsf{M}'}(1^n) + c$.

The strategy for a requirement $\mathrm{R}_{\Phi,\Psi}$ is composed of an infinite sequence of strategies for subrequirements

$\mathrm{S}_{\Phi,\Psi,i}$: $K_{\mathsf{M}_i}(\Phi(A) \restriction n) > K_{\mathsf{M}'}(1^n) + i$,

that are only allowed to act on a sequence of stages at which $\Psi(\Phi(A)) = A$ appears more and more likely to be the case. Each such substrategy has a large number m associated to it and picks a sequence of witnesses $x_1, \dots, x_m \notin A$ such that for every $1 \le i < m$, $\psi(\Phi(A); x_i) < x_{i+1}$. Once these witnesses have been chosen, we enumerate the pair $\langle \log m{-}i{-}1, 1^{\psi(\Phi(A);x_m)}\rangle$ into a c. e. set defining M'. If there is no stage s and string σ such that $|\sigma| \le \log m{+}i$ and $\mathsf{M}_i(\sigma) = \Phi(A) \restriction \psi(\Phi(A); x_m)$, then there is no need to ever take further action. At any stage s where there is a string σ such that $|\sigma| \le \log m{+}i$ and $\mathsf{M}_i(\sigma) = \Phi(A) \restriction \psi(\Phi(A); x_m)$, we enumerate the greatest $x_j \notin A[s]$ into $A[s{+}1]$. If $\Psi(\Phi(A)) = A$, $\Phi(A)$ must change on $\psi(\Phi(A); x_j)$, so that M_i will be forced to converge on at least $m{+}1$ different strings of length less than or equal to $\log m{-}i$, thereby adding $(m{+}1) \cdot 2^{-\log m - i} > 2^{i+1} \ge 2$ to the measure of M_i. By Kraft's inequality, $\mu(\mathsf{M}_i) \le 1$, so this is not a possibility.

The priority organization of the requirements involves interleaving the subrequirements needed for strategies of type R, a task that is straightforward, although a little involved.

Construction.

We use the tree of strategies $2^{<\omega}$ to control the construction, and adopt the convention that all uses with c. e. oracles are nondecreasing in the stage and increasing in the argument. The priority arrangement of the requirements is accomplished by a list function L, defined recursively on the nodes in $2^{<\omega}$ and the natural numbers. For all $n \in \omega$, $L(\lambda, n) = \mathrm{R}_{\Phi,\Psi}$, where $n\langle\Phi, \Psi\rangle$ under some standard enumeration of pairs of computable functionals. For any $\sigma \in 2^{<\omega}$, if $L(\sigma, 0) = \mathrm{R}_{\Phi,\Psi}$ for some Φ and Ψ, then for every $n \in \omega$, $L(\sigma 1, n) = L(\sigma, n{+}1)$, $L(\sigma 0, 2n) = L(\sigma, n{+}1)$, and $L(\sigma 0, 2n{+}1) = \mathrm{S}_{\Phi,\Psi,n}$. Otherwise, $L(\sigma 0, n) = L(\sigma 1, n) = L(\sigma, n{+}1)$. For each $\sigma \in 2^{<\omega}$, σ has requirement $L(\sigma, 0)$ assigned to it.

A node is initialized by having all its associated parameters undefined and associated sets set to $\emptyset$. A node α with a requirement $\mathrm{R}_{\Phi,\Psi}$ assigned to it has a machine M^α assigned to it that is built by enumerating pairs $\langle k, \tau\rangle$ into a c. e. set W^α. By the Kraft-Chaitin theorem, if $\sum_{\langle k,\tau\rangle \in W^\alpha} 2^{-k} \le 1$, this defines a prefix-free machine M^α such that for every $\langle k, \tau\rangle \in W^\alpha$, there is a string σ with $|\sigma| = k$ such that $\mathsf{M}^\alpha(\sigma) \downarrow = \tau$. A node α with a requirement $\mathrm{S}_{\Phi,\Psi,i}$ assigned to it has parameter for a *starting number* $s^\alpha[s]$, and a sequence of witness parameters $x(\alpha, 1)[s], \dots, x(\alpha, 2^{s^\alpha + i + 1})[s]$. The construction of A and the necessary machines proceeds in stages.

Stage 0. We initialize all nodes in $2^{<\omega}$.

Stage $s{+}1$. We define an *approximation to the true path*, $f[s]$, of length at most s and allow each node $\alpha \subset f[s]$ to act. If $\alpha \subset f[s]$, then we call s an *α-stage*. Let $n = |\alpha|$. Let s^- be the most recent stage at which $\alpha \subset f[s^-]$, or the most recent stage at which α was initialized, whichever is greater.

Suppose α has requirement $\mathrm{R}_{\Phi,\Psi}$. In this case, we define the length-of-agreement function

$$l^\alpha[s] = \max\{\, y \,:\, (\forall\, x < y)\,(\Psi(\Phi(A); x) = A(x))[s] \,\}.$$

Let s_0 be the stage at which α was last initialized.

A stage s is α-expansionary if $l^\alpha[s] > \max\{\, l^\alpha[t] \,:\, s_0 < t < s$ and t is an α stage$\,\}$.

If s is not α-expansionary, then initialize all nodes β such that $\alpha 1 <_L \beta$ and let $f(n)[s] = 1$, so that $\alpha 1$ is accessible at stage $s{+}1$. If s is α-expansionary, then we let $\alpha 0$ be accessible at stage $s{+}1$ and initialize all nodes β such that $\alpha 0 <_L \beta$.

Suppose α has requirement $\mathrm{S}_{\Phi,\Psi,i}$ assigned to it. If there exists a node $\alpha' \subset \alpha$ such that α' has requirement $\mathrm{S}_{\Phi',\Psi',i'}$ for some Φ', Ψ', and i', and β is the longest node such that $\beta 0 \subset \alpha'$ and β has requirement $\mathrm{R}_{\varphi',\Psi'}$ assigned to it, and $(\langle s^\alpha, 1^{\psi(\Phi(A);x(\alpha',2^{s^{\alpha'}+i+1})}\rangle \notin W^\beta)[s]$, then immediately end stage $s{+}1$ and initialize all $\gamma \geq \alpha$.

Otherwise there are several cases to consider. Let β be the longest node with requirement $\mathrm{R}_{\Phi,\Psi}$ assigned to it such that $\beta 0 \subseteq \alpha$. If $x(\alpha,1) \uparrow [s]$, then let $s^\alpha[s] = x(\alpha,1)[s] = s$. If there exists some least $j \leq 2^{s^\alpha[s]+i+1}$ such that $x(\alpha,j) \uparrow [s]$ and $(x(\alpha,j{-}1) < l^\beta)[s]$, then let

$$x(\alpha,j)[s] = \max\{\, \varphi(A;y)[s] \,:\, y < \psi(\Phi(A);x(\alpha,j{-}1))[s]\,\}{+}1.$$

Immediately end stage $s{+}1$ and initialize all $\gamma \geq \alpha$.

Suppose $x(\alpha,j) \downarrow [s]$ for all $j \leq 2^{s^\alpha+i+1}$. If $l^\beta[s] > x(\alpha,2^{s^\alpha+i+1})$ but $l^\beta[s^-] \leq x(\alpha,2^{s^\alpha+i+1})$, then enumerate $\langle s^\alpha[s], 1^{\psi(\Phi(A);x(\alpha,2^{s^\alpha+i+1}))[s]}\rangle$ into $W^\beta[s{+}1]$. Immediately end stage $s{+}1$ and initialize all $\gamma \geq \alpha$. If there exists σ such that $\big(\mathsf{M}_i(\sigma) = \Phi(A) \restriction \psi(\Phi(A);x(\alpha,2^{s^\alpha+i+1}))\big)[s]$ and $|\sigma| < s^\alpha[s]{+}i$, and j is greatest such that $(x(\alpha,j) \notin A)[s]$, then let $(x(\alpha,j) \in A)[s{+}1]$. Immediately end stage $s{+}1$ and initialize all $\gamma \geq \alpha$.

This completes the construction.

Verification.

Let the *true path* f be $\liminf_{s\to\infty} f[s]$. Each $\alpha \subset f$ has some stage after which $\alpha \leq f[s]$ for every subsequent s. Once a node chooses a sequence of witnesses and is never again initialized, it only acts to change A or initialize other nodes a finite number of times. It follows, therefore, by a straightforward induction, that every $\alpha \subset f$ is initialized only finitely often.

Lemma 4.1 *Suppose $\alpha \subset f$ and there exist Φ, Ψ, and i such that α has requirement $\mathrm{S}_{\Phi,\Psi,i}$ assigned to it, and β is the longest node such that $\beta 0 \subset \alpha'$ and β has requirement $\mathrm{R}_{\varphi',\Psi'}$ assigned to it, Then there is some stage t such that for all $s \geq t$ and $j \leq 2^{|\alpha|+i+1}$, $x(\alpha,j) \downarrow [t] = x(\alpha,j)[s]$, and $(\langle s^\alpha, 1^{\psi(\Phi(A);x(\alpha,2^{s^\alpha+i+1})}\rangle \in W^\beta)[s]$.*

Proof. By induction on $|\alpha|$, for all $\gamma \subset \alpha$ and Φ', Ψ', i' such that $\mathrm{S}_{\Phi',\Psi',i'}$ is assigned to γ, there is some stage after which $x(\gamma,j)\downarrow$ with the same value for every $j \leq 2^{|\gamma|+i'+1}$. Let t_0 be the either this stage or the last stage at which α is initialized. The requirement $\mathrm{S}_{\Phi,\Psi,i}$ can only be assigned to a node extending some $\beta 0$ such that β has requirement $\mathrm{R}_{\Phi,Psi}$ assigned to it. For such a $\beta \subset f$, $\limsup_{s\to\infty} l^\beta[s] = \infty$. Hence, after t_0, nothing can prevent α from choosing all its witnesses $x(\alpha,1)$, $x(\alpha,2)$, etc., and nothing can cause these witnesses to later diverge, once chosen. □

Naturally, we just write s^α and $x(\alpha,j)$ without reference to the stage for these final values. Note that for any $\gamma \subset \alpha \subset f$ and j' and j, $x(\gamma,j') < x(\alpha,j)$.

By Lemma 4.1, the true path is infinite, and it follows, again by a straightforward induction, that every requirement $\mathrm{R}_{\Phi,\Psi}$ is assigned to some node along it. It remains to be shown that all these requirements are satisfied by the strategies of the associated nodes on the true path.

Suppose $\beta \subset f$ with requirement $\mathrm{R}_{\Phi,\Psi}$ assigned to it. If it is not the case that $\Psi(\Phi(A)) = A$, then there is nothing to prove, so suppose that this is the case. In this case, $\beta 0 \subset f$. Since requirements are only added to a list $L(\gamma,\cdot)$ when $L(\gamma 0,\cdot)$ and $L(\gamma 1,\cdot)$ are defined, each subrequirement $\mathrm{S}_{\Phi,\Psi,i}$ is assigned to some node included in f. The following lemmas about β verify that the requirement is satisfied.

Lemma 4.2 *$\mu(\mathsf{M}^\beta)$ is a computable real.*

Proof. Clearly $\mu(\mathsf{M}^\beta)$ is c.e. We show that there is a nonincreasing computable function $e^\beta[s]$ such that $\lim_{s\to\infty} e^\beta[s] = 0$ and for all s, $\mu(\mathsf{M}^\beta) - \mu(\mathsf{M}^\beta)[s] < e^\beta[s]$. If W^β is finite, then there is nothing to prove. Otherwise, set $e^\beta[0] = 1$. Given $s > 0$, we wait for the next stage $t > s$ such that a new element is enumerated into $W^\beta[t+1]$. Since at each $t' > s$ such that a new element is enumerated into $W^\beta[t'+1]$, all subsequent enumerations into W^β individually add some unique number less than $2^{-t'}$ to $\mu(\mathsf{M}^\beta)$, it follows that $\mu(\mathsf{M}^\beta) - \mu(\mathsf{M}^\beta)[s] < \sum_{t'>t} 2^{-t'} = 2^{-t}$. Hence setting $e^\beta[t'] = e^\beta(s-1)$ for all t' with $s \leq t' \leq t$ and $e^\beta(t{+}1) = 2^{-t}$ works as claimed. Notice that this also shows that $\mu(\mathsf{M}^\beta) < 2^0 = 1$, so that M^β is a well-defined prefix-free machine. This suffices to prove the lemma. □

Lemma 4.3 *If* M *is a prefix-free machine, then for all* c *there is a* k *such that* $K_{\mathsf{M}}(\Phi(A) \upharpoonright k) > K_{\mathsf{M}^\beta}(1^k) + c$

Proof. By a suitable version of the padding lemma, there exist infinitely many i such that M is equivalent to M_i. Choose such an $i \geq c$. Let $\alpha \supset \beta 0$ be the unique node included in f such that $\mathrm{S}_{\Phi,\Psi,i}$ is assigned to α. Suppose we have passed the stage after which α is last initialized, so that only strategies assigned to node $\gamma \geq \alpha$ act at any later stage. We show that

$$K_{\mathsf{M}}(\Phi(A) \upharpoonright \psi(\Phi(A); x(\alpha, 2^{s^\alpha+i+1}))) > s^\alpha + i \geq K_{\mathsf{M}^\beta}(1^{\psi(\Phi(A);x(\alpha,2^{s^\alpha+i+1}))}) + i.$$

If there exists a witness $x(\alpha, j)$ such that $x(\alpha, j) \notin A$, then suppose $x(\alpha, j)$ is added to A at stage $s{+}1$. Note that $x(\alpha, j) > \max\{\, \varphi(A; y)[s] \,:\, y < \psi(\Phi(A); x(\alpha, j{-}1))[s]\,\}$, and all nodes $\gamma > \alpha$ are initialized at $s{+}1$. Hence if s^+ is any subsequent β-expansionary stage before $x(\alpha, j{-}1)$ is added to A, we must have

$$\Phi(A)[s^+] \upharpoonright 1^{\psi(\Phi(A);x(\alpha,j-1)))}[s] = \Phi(A)[s] \upharpoonright \psi(\Phi(x(\alpha, j{-}1))).$$

Thus if $s_1 < s < 2 < \cdots < s_{2^{s^\alpha+i+1}}$ is the sequence of stages such that $x(\alpha, j) \in A[s_j{+}1] - A[s_j]$, there must be a sequence of distinct strings $\sigma_0, \sigma_2, \ldots, \sigma_{2^{s^\alpha+i+1}}$ such that for each j,

$$\mathsf{M}(\sigma_j) \downarrow = \Phi(A)[s_j] \upharpoonright \psi(\Phi(A); x(\alpha, 2^{s^\alpha+i+1}))$$

and $|\sigma_j| \leq s^\alpha + i$. But then $\mu(\mathsf{M}) \geq 2^{s^\alpha+i+1} \cdot 2^{-s^\alpha-i} \geq 2^1 > 1$, a contradiction. Hence not all witnesses can be added, so that $K_{\mathsf{M}}(\Phi(A) \upharpoonright \psi(\Phi(A); x(\alpha, 2^{s^\alpha+i+1}))) > s^\alpha + i \geq K_{\mathsf{M}^\beta}(1^{\psi(\Phi(A);x(\alpha,2^{s^\alpha+i+1}))}) + i$. □

The last two lemmas establish the result. □

The following two corollaries are immediate:

Corollary 10 *There is a c. e. degree containing no* K*-trivial real.*

Corollary 11 *There is a c. e. degree containing no Schnorr trivial real.*

5 Schnorr reducibility and strong reducibilities

Theorem 12 *No c. e. real* α *can be both wtt-complete and Schnorr trivial.*

Proof. Suppose α is wtt-complete. We will construct a c. e. set D that forces α to change too often to be Schnorr trivial. Using the method of standard proofs of Lachlan's Non-diamond Theorem (see Soare [15, Chapter IX]) we can assume that a wtt-reduction Γ such that $\Gamma(\alpha) = D$ is given in advance. More precisely, we define an infinite sequence of constructions of c. e. sets D_e, each one using a p. c. functional Φ_e. Because for each c. e. D_e, D_e is uniformly m-reducible to $K \leq_{\mathrm{wtt}} A$, we have a computable index $g(e)$ for a p. c. functional $\varphi_{g(e)}$ such that $\varphi_{g(e)}(A) = D_e$. By the Recursion Theorem, for some e, $\varphi_e = \varphi_{g(e)}$, so that we can take $\varphi_{g(e)} = \Gamma$.

We must satisfy, for all $e \in \omega$, the following sequence of requirements

R_e : there exists x such that $K_{\mathsf{M}_e}(\alpha \upharpoonright x) \geq K_{\mathsf{M}}(1^x){+}e$.

The strategy is straightforward: we choose some (large) number m, and followers $x_1 < x_2 < \cdots < x_m$ to use in satisfying this requirement. We then enumerate $\langle -e{+}\log m, 1^{\gamma(x_m)+1}\rangle$ into a c. e. set defining M at some stage s_{m+1}. In general, given s_k, we wait for a stage s such that $s > s_k$ at which some σ_m appears with $|\sigma_m| < \log m$ such that $(\mathsf{M}_e(\sigma) = \alpha \upharpoonright \gamma(x_m){+}1)[s]$, then we enumerate x_{k-1} into D. In order for $\Gamma(\alpha; y)[s]$ to change value on a $y \leq x_m$, $\alpha[s]$ must change on some $z < \gamma(x_m)$. Now, since $\Gamma(\alpha) = D$, we must have some $s_{k-1} > s$ such that $\alpha \upharpoonright \gamma(x_{k-1}{+}1)[s] \neq \alpha \upharpoonright \gamma(x_{k-1}){+}1)[s_{k-1})]$. Since α is c. e., this means the approximation to α must increase by some amount greater than $2^{-\gamma(x,m)}$. Hence, if $K_{\mathsf{M}_e}(\alpha \upharpoonright \gamma(x_m){+}1) < K_{\mathsf{M}}(1^{\gamma(x_m)+1}){+}e = \log m$, there must exist a sequence $\sigma_m, \ldots, \sigma_1$ of distinct strings of length less than $\log m$ such that for all k, $\mathsf{M}_e(\sigma_k)\downarrow$. But then $\mu(\mathsf{M}_e) > m2^{\log m} = 1$. This contradicts M_e being a prefix-free machine.

The only difficulty involves choosing m and the witnesses $x_1 \ldots, x_m$ so that strategies for different requirements don't interfere with each other. We use a finite-injury priority argument to achieve this.

Stage 0. We let $m^0[0] = 1$, $x^0_1[0] = 0$, $x^0_2 = 1$.

Stage $s{+}1$. First, choose e least so that $m^e \downarrow [s]$, $x^e_{m^e} \downarrow [s]$, $s^e \downarrow [s]$, $\Gamma(\alpha; x^e_{m^e}) \downarrow [s]$, and there exists some $\sigma \in 2^{<\omega}$ such that $|\sigma| < \log m^e[s]$, $(\mathsf{M}_e(\sigma) = \alpha \restriction \gamma(x^e_{m^e}){+}1)[s]$, and $\mu(\mathsf{M}_e)[s] \le 1$. If k is greatest such that $x^e_{k-1} \notin D[s]$, then let $x^e_{k-1)} \in D[s{+}1]$. For all $e' > e$, undefine all functionals and parameters associated to the strategy for $\mathrm{R}_{e'}$.

Next, choose e least so that $m^e \downarrow [s]$, $x^e_{m^e} \downarrow [s]$, $\Gamma(\alpha; x^e_{m^e}) \downarrow [s]$, but $s^e \uparrow [s]$. Then enumerate the pair $\langle -e{+}\log m^e, 1^{\gamma(x^e_m)+1}\rangle$ into the c. e. set defining machine M. Set $s^e \downarrow [s] = s{+}1$.

Finally, choose e least so that $m^e \uparrow [s]$. Let $m_e \downarrow [s]$ with value the least number greater than or equal to 2^{s+e} that has never yet been a value $m^{e'}[s']$ for any e' and $s' \le s$. Let b be the least number greater than any yet mentioned in the construction. For all j with $1 \le j \le m^e[s]$, let $x^e_j \downarrow [s] = b{+}j$.

This completes the construction.

Notice first that M is a computable machine, since at stage s, the set $\{\, e : m^e \downarrow [s]\,\}$ is finite. All values $m^e[s']$ that are defined after stage s are greater than 2^s, and they are all distinct. If we wait for a stage $t > s$ such that for all such e, either $m^e[s] \ne m^e[t]$, or $\langle -e{+}\log m^e, 1^{\gamma(x^e_m)+1}\rangle$ is in the c. e. set that defines M, then, $\mu(\mathsf{M}) - \mu(\mathsf{M})[s] \le \sum_{m>s} 2^{-m} = 2^{-s}$. This gives a computable nonincreasing function with limit 0 that bounds the error, so that $\mu(\mathsf{M})$ is computable.

Consider a fixed requirement R_e and suppose that for all $e' < e$, $\mathrm{R}_{e'}$ is satisfied, and the strategy for $\mathrm{R}_{e'}$ only changes D and M finitely often. Once no strategy for any such $\mathrm{R}_{e'}$ ever acts again, the functionals and parameters for R_e are, once defined, defined permanently. Thus the actions taken in the third phase of the construction at stage $s{+}1$ guarantee that $m^e \downarrow$, $s^e \downarrow$, and for all j with $1 \le j \le m^e$, $x^e_j \downarrow$ with final values. At stage s^e, $x^e_j \notin D$ for all $j \le m$. Now, $m^e > 2^{e+1}$, $-e{+}\log m^e > 1$, and Γ is a total function. Hence, the action in the second phase of the construction guarantees that $K_{\mathsf{M}}(1^{\gamma(x^e_m)+1}) \le -e{+}\log m^e$. There can exist only m^e different stages after this point at which D is changed for the sake of the R_e-strategy. As pointed out before the description of the construction, if $K_{\mathsf{M}_e}(\alpha \restriction \gamma(x^e_m){+}1) < K_{\mathsf{M}}(1^{\gamma(x^e_m)+1}){+}e$, then the action taken in the first phase of the construction at stage $s{+}1$ guarantees that there must exist a sequence $\sigma_m, \dots, \sigma_1$ of distinct strings of length less than $\log m^e$ such that for all k, $\mathsf{M}_e(\sigma_k) \downarrow$. But then $\mu(\mathsf{M}_e) > m^e(2^{\log m^e}) = 1$. By the Chaitin-Kraft inequality, this is a contradiction since M_e is a prefix-free machine. □

A reducibility more closely related to randomness than wtt-reducibility is strong weak-truth-table reducibility, studied in [5].

Definition 8 A is *strongly weak-truth-table reducible to* B, written $A \le_{\mathrm{sw}} B$, if there exists a p. c. functional Γ and a constant c such that $\Gamma(B) = A$ and, for all n, the use $\gamma(n) \le x + c$.

If $A \le_{\mathrm{sw}} B$, then $A \le_{\mathrm{K}} B$ (see [5]). This fails for Schnorr reducibility.

Theorem 13 *There are c. e. sets A and B such that $B \le_{\mathrm{sw}} A$, but $B \not\le_{\mathrm{Sch}} A$.*

Proof. As usual, we need only consider prefix-free machines M_e such that $\mu(\mathsf{M}_e) = 1$, since any computable machine is equivalent to such a one. We therefore build a computable machine M, and c. e. sets A, B, to satisfy the requirements

$$\mathrm{R}_e : \quad \text{if } \mu(\mathsf{M}_e) = 1, \text{ then there exists an } n \text{ such that } K_{\mathsf{M}}(A \restriction n) < K_{\mathsf{M}_e}(B \restriction n) - e.$$

To satisfy requirement R_e, we will set aside a block of numbers $\{n, n{+}1, \dots, n{+}d\}$, where d is some number greater than 2^{e+2}. Note that $2 < 2^{e+2}$, so that $d^2 < 2^{d+2} - 2$. Of the numbers in the block $\{n, \dots, n{+}d\}$, we will allow no $n{+}j$ for $j > 0$ to ever enter A, but we may possibly put n itself into A. Thus we enumerate two axioms of the form $\langle 2{+}\log d, \tau\rangle$, one for each of the two possibilities for $\tau = A \restriction n + j{+}1$ with $j \le d$. This adds $2(d{+}1)2^{-2-\log d} \le 2^{-1} + 2^{-1-\log d} < 1$ to $\mu(\mathsf{M})$. We now wait for a stage s such that $1 - \mu(\mathsf{M}_e)[s] < 2^{-e-2-\log d}$. Since $\mu(\mathsf{M}_e) \le 1$, there can be at most $d \cdot 2^{e+2} \le d^2 < 2^{d+2} - 2$ strings of length less than or equal to $e{+}2{+}\log d$ on which M_e converges. However, the number of axioms required by M_e to cover all possibilities of members of the block $\{n, \dots, n+d\}$ being in or out of B, for the $d{+}1$ strings, $B \restriction n, \dots, B \restriction (n+d)$ is $2^1 + 2^2 + \dots + 2^{d+1} = 2^{d+2} - 2$. Hence, at least one possibility is not in the range of M_e restricted to strings in its domain of length less than or equal to $e{+}2{+}\log d$. At this point, we choose such a combination of elements of $\{n, \dots, n+d\}$ and enumerate them into $B[s{+}1]$, simultaneously enumerating n into $A[s{+}1]$. Any new axioms for M_e must cause convergence on strings of length greater than $e+2+\log d$. Since $K_{\mathsf{M}}(n+j) = 2+\log d$ for every $j \leq d$, the requirement is satisfied. Also, the membership of all elements of $\{n, \ldots, n+d\}$ in B can be calculated just by checking whether or not $n \in A$, so $B \leq_{\text{sw}} A$. Not also that $\mu(\mathsf{M})$ is computable, since the enumeration of its axioms do not depend on waiting for any condition to be satisfied.

We can combine all strategies by assigning them intervals $\{x_0, \ldots, x_0+d_0\}$, $\{x_1, \ldots, x_1+d_1\}, \ldots$, where $x_0 = 0$ and $x_{i+1} = x_i + d_i + 1$. Since for each i, any combination of the values x_j for $j < i$ could show up in A, we must in general use 2^{i+1} axioms of the form $\langle m, \tau \rangle$, 2^i for each of the two possibilities for $\tau = A \upharpoonright x_i+j+1$ with $j \leq d_i$. This means we must enumerate axioms of the form $\langle 2+2i+\log d_i, \tau \rangle$ into M. In this case, the axioms enumerated into M for the sake of requirement R_i will add exactly

$$2^i(d_i+1)2^{-2-2i-\log d_i} \leq 2^{-i-2} + 2^{-i-2-\log d_i} \leq 2 \cdot 2^{-i-2} < 2^{-i-1}$$

to the measure of M, so that $\mu(\mathsf{M}) = \sum_{i \geq 0} 2^{-i-1} = 1$, as required for a computable machine. In order to satisfy the requirement, we can therefore choose d_i to be the least number greater than 2^{2+3i}. Note again that $d_i^2 < 2^{d_i+2} - 2$, since $d_i \geq 2$. Then there can be at most $d \cdot 2^{2+3i} \leq d^2 < 2^{d_i+2} - 2$ strings of length less than or equal to $2+3i+\log d_i$ on which M_e converges. We take action for R_i at the first stage s such that $1 - \mu(\mathsf{M}_i)[s] < 2^{-2-3i-\log d_i}$, enumerating the elements of an appropriate subset of $\{x_i, \ldots, x_i+d_i\}$ into $B[s+1]$ and enumerating x_i into $A[s+1$. This satisfies requirement R_i permanently, which suffices to prove the result. □

Recall that A is truth-table reducible to B ($A \leq_{\text{tt}} B$) if and only if $A \leq_{\text{wtt}} B$ via a reduction Γ such that $\Gamma(\sigma, n) \downarrow$ for all $\sigma \in 2^{<\omega}$ and $n \in \omega$. It turns out that tt-reducibility is related to Schnorr-reducibility somewhat as wtt-reducibility is to K-reducibility. This is not surprising, since the essential difference between a tt-reduction and an ordinary wtt-reduction is that the former has a computable domain, and this is what distinguishes a computable machine from an ordinary prefix-free machine.

Theorem 14 *If y is Schnorr trivial and $x \leq_{\text{tt}} y$, then x is Schnorr trivial.*

Proof. We must show that for any computable machine M, there exists some computable machine M_x and a constant c such that for every $n \in \omega$, $K_{\mathsf{M}_x}(x \upharpoonright n) \leq K_{\mathsf{M}}(1^n) + c$.

Suppose that the truth-table reduction is given by $x = \Gamma^y$ with use bounded by the strictly increasing recursive function $\gamma(n)$. Given any computable machine M we first define another computable machine M_u such that for all n, $K_{\mathsf{M}_u}(1^{u(n)}) \leq K_{\mathsf{M}}(1^n)$. To define M_u simply follow the enumeration of axioms into M. Every time $\langle \sigma, \tau \rangle$ enters M, then put the same axiom into M_u unless $\tau = 1^k$ for some k. In that case put $\langle \sigma, 1^{\gamma(k)} \rangle$ into M_u. $\mu(\mathsf{M}_u) = \mu(\mathsf{M})$, so that M_u is also a computable machine. Evidently, M_u is as required.

Now as y is Schnorr trivial, there exists a computable machine M_y and a constant c such that for all k, $K_{\mathsf{M}_y}(y \upharpoonright k) \leq K_{\mathsf{M}_u}(1^k) + c$. In particular, for all n, $K_{\mathsf{M}_y}(y \upharpoonright \gamma(n)) \leq K_{\mathsf{M}_u}(1^{\gamma(n)}) + c \leq K_{\mathsf{M}}(1^n) + c$.

Now we define a machine M_x with the same domain as M_y to show that x is Schnorr trivial. If $\mathsf{M}_y(\sigma) = \tau$, then let $\mathsf{M}_x(\sigma) = (\Gamma^{\tau \upharpoonright \gamma(\hat{n})} \upharpoonright \hat{n})$ for the largest $\hat{n}$ with $\gamma(\hat{n}) \leq |\tau|$. Then, if $\mathsf{M}_y(\sigma) = y \upharpoonright \gamma(n)$, we have $\mathsf{M}_x(\sigma) = (\Gamma^{y \upharpoonright \gamma(n)} \upharpoonright n) = x \upharpoonright n$, so that $K_{\mathsf{M}_x}(x \upharpoonright n) = K_{\mathsf{M}_y}(y \upharpoonright \gamma(n)) \leq K_{\mathsf{M}_u}(1^{\gamma(n)}) + c \leq K_{\mathsf{M}}(1^n) + c$. Since the tt-reduction converges with any string as an oracle, $\mu(\mathsf{M}_x) = \mu(\mathsf{M}_y)$, and so M_x is a computable machine. □

We would like to show that the Schnorr trivials form an ideal in the tt-degrees. All we need is the following simple fact.

Question *Suppose x and y are Schnorr trivial reals. Is $x \oplus y$ Schnorr trivial ?*

The result that K-degrees are closed downward under sw-reducibility has an analogous tt-version as well:

Definition 9 A is *strongly truth-table reducible to* B (written $A \leq_{\text{st}} B$) if and only if $A \leq_{\text{tt}} B$ via a truth table reduction Γ with a constant c such that for all n, the use $\gamma(n) \leq n+c$.

Theorem 15 *If $A \leq_{\text{st}} B$, then $A \leq_{\text{Sch}} B$.*

Proof. Let $A \leq_{\text{st}} B$ via some st reduction Γ with use $\gamma(n)$ bounded by $n+c$. Let $\zeta_0, \ldots, \zeta_{2^c-1}$ be the 2^c different elements of $2^{<\omega}$ of length c. Let M be any computable prefix-free machine. For every σ and τ such that

$\mathsf{M}(\sigma) = \tau$, add $\langle |\sigma| + c, \Gamma^{\tau^\frown \zeta_j} \upharpoonright |\tau| \rangle$ for each $j < 2^c$ to a c. e. set, thereby defining a machine M' via the Kraft-Chaitin Theorem. Since Γ is a tt-reduction, all these computations converge, and so this adds $2^c \cdot 2^{-|\sigma|-c} = 2^{-|\sigma|}$ to $\mu(\mathsf{M}')$. Hence, $\mu(\mathsf{M}') = \mu(\mathsf{M})$, making M' a computable machine. Then, if $\mathsf{M}(\sigma) = B \upharpoonright n$, we have, for some string σ' of length $|\sigma|+c$, $\mathsf{M}'(\sigma') = (\Gamma^{B \upharpoonright (n+c)} \upharpoonright n) = A \upharpoonright n$, so that $K_{\mathsf{M}'}(A \upharpoonright n) = K_{\mathsf{M}}(B \upharpoonright n)+c$. □

References

[1] K. Ambos-Spies and A. Kučera, Randomness in computability theory. In: Computability Theory: Current Trends and Open Problems (P. Cholak et al., eds.), Contemporary Mathematics 257 (2000), pp. 1 – 14 (American Math. Society, Reading (MA) 2000).

[2] G. J. Chaitin, Algorithmic Information Theory (Cambridge University Press, Cambridge 1987).

[3] R. G. Downey and E. Griffiths, Schnorr randomness. J. Symbolic Logic **69**, 533 – 554 (2004).

[4] R. Downey and D. Hirschfeldt, Algorithmic Randomness and Complexity (Springer-Verlag, Berlin et al., to appear).

[5] R. Downey, D. Hirschfeldt, and G. LaForte, Randomness and reducibility. J. Computer and System Sciences **68**, 96 – 114 (2004).

[6] R. Downey, D. Hirschfeldt, and A. Nies, Randomness, computability, and density. SIAM J. Comput. **31**, 1169 – 1183 (2002). An extended abstract appeared in: Symposium for Theoretical Aspects of Computer Science, STACS'01, January, 2001 (A. Ferriera and H. Reichel, eds.), Lecture Notes in Computer Science, pp. 195 – 201 (Springer-Verlag, Berlin et al. 2001).

[7] R. G. Downey, D. R. Hirschfeldt, A. Nies, and F. Stephan, Trivial reals. In: Electronic Notes in Theoretical Computer Science (ENTCS), 2002. The final version appears in Proceedings Asian Logic Conferences (R. G. Downey et al., eds.), pp. 103 – 131 (World Scientific, 2003).

[8] R. G. Downey, D. R. Hirschfeldt, A. Nies, and S. Terwijn, Calibrating randomness. In preparation.

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

[10] M. Li and P. Vitányi, An Introduction to Kolmogorov Complexity and its Applications (Springer-Verlag, Berlin et al. 1993).

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

[12] A. Nies, Reals which compute little. To appear.

[13] A. Nies, F. Stephan, and S. Terwijn, Randomness, relativization, and Turing degrees. In preparation.

[14] C.-P. Schnorr, Zufälligkeit und Wahrscheinlichkeit. Lecture Notes in Mathematics **218** (Springer-Verlag, Berlin-Heidelberg 1971).

[15] R. I. Soare, Recursively Enumerable Sets and Degrees. Perspectives in Mathematical Logic, Omega Series (Springer-Verlag, Berlin-Heidelberg-New York-Tokyo 1987).

[16] R. Solovay, Draft of a paper (or series of papers) on Chaitin's work. Unpublished manuscript (IBM Thomas J. Watson Research Center, New York, May 1975, 215 pp.).

[17] L. Staiger, The Kolmogorov complexity of real numbers. Theoretical Computer Science **284**, 455 – 466 (2002)

[18] S. A. Terwijn and D. Zambella, Computational randomness and lowness. J. Symbolic Logic **66**, 1199 – 1205 (2001).

[19] Y. Wang, Randomness and Complexity. PhD Diss., University of Heidelberg 1996.

[20] A. K. Zvonkin and L. A. Levin, The complexity of finite objects and the development of concepts of information and randomness by the theory of algorithms. Russian Math. Surveys **25**, 83 – 124 (1970).