CDMTCS
Research
Report
Series

Randomness, Relativization and Turing Degrees

A. Nies[1], F. Stephan[2], S.A. Terwijn[3]

[1]University of Auckland

[2]University of New South Wales, Australia

[2]Technical University of Vienna, Austria

CDMTCS-234
February 2004

Centre for Discrete Mathematics and
Theoretical Computer Science

Randomness, relativization, and Turing degrees

André Nies, Frank Stephan and Sebastiaan A. Terwijn

Abstract. We compare various notions of algorithmic randomness. First we consider relativized randomness. A set is n-random if it is Martin-Löf random relative to $\emptyset^{(n-1)}$. We show that a set is 2-random if and only if there is a constant c such that infinitely many initial segments x of the set are c-incompressible: $C(x) \geq |x| - c$. The 'only if' direction was obtained independently by Joseph Miller. This characterization can be extended to the case of time-bounded C-complexity.

Next we prove some results on lowness. Among other things, we characterize the 2-random sets as those 1-random sets that are low for Chaitin's Ω. Also, 2-random sets form minimal pairs with 2-generic sets. The r.e. low for Ω sets coincide with the r.e. K-trivial ones.

Finally we show that the notions of Martin-Löf randomness, recursive randomness, and Schnorr randomness can be separated in every high degree while the same notions coincide in every non-high degree. We make some remarks about hyperimmune-free and PA-complete degrees.

Mathematical Subject Classification: 68Q30, 03D15, 03D28, 03D80, 28E15.

1. Introduction

The study of algorithmic randomness received a strong impulse when Martin-Löf [**19**] defined his notion of randomness of infinite strings based on constructive measure theory. Especially the strong connections with the theory of randomness for finite objects made this notion very popular, see e.g. [**17**], to name only one of the many references that the reader can consult for this. Another landmark in the theory of randomness is Schnorr's book [**26**], containing a thorough discussion (and criticism) of several of the randomness notions used in this paper, in particular

A. Nies: Department of Computer Science, University of Auckland, 38 Princes St, New Zealand, anie010@cs.auckland.ac.nz.

F. Stephan: National ICT Australia LTD, Sydney Research Laboratory at Kensington, The University of New South Wales, Sydney NSW 2052, Australia, fstephan@cse.unsw.edu.au. National ICT Australia is funded by the Australian Government's Department of Communications, Information Technology and the Arts and the Australian Research Council through Backing Australia's Ability and the ICT Centre of Excellence Program.

S. A. Terwijn: Institute for Algebra and Computational Mathematics, Technische Universität Wien, Wiedner Hauptstrasse 8–10/E118, A-1040 Vienna, Austria, terwijn@logic.at. Supported by the Austrian Research Fund (Lise Meitner grant M699-N05).

Martin-Löf randomness, recursive randomness, and what is now called Schnorr randomness. Since all of these notions are defined in terms of basic recursion theory, it comes as no surprise that they are often best analyzed in the context of that same theory. In particular, there has been a clear interest in the interplay of the various randomness notions and relative computability, or Turing reducibility. The reader can e.g. consult the recent survey paper by Ambos-Spies and Kučera [**1**]. In the present paper we prove some new results on randomness relating to both Turing reducibility and Kolmogorov complexity.

The outline of the paper is as follows. In Section 2 we consider relativized randomness and Kolmogorov complexity. Ding, Downey, and Yu [**7**] call a set X *Kolmogorov random* if

$$(\exists b)(\exists^\infty n)\big[\,C(X\restriction n) \geq n - b\,\big],$$

where C is the plain Kolmogorov complexity. This notion was studied earlier in several equivalent forms by Loveland, Schnorr, Daley and others, see section 2. Martin-Löf [**20**] proved that there are no sets X such that $(\exists b)(\forall n)\big[\,C(X\restriction n) \geq n - b\,\big]$ and he also showed that Kolmogorov randomness implies Martin-Löf randomness. We give a simple proof of this last fact in Proposition 2.4. We then compare Kolmogorov randomness with relativized Martin-Löf randomness. A set is n-random if it is Martin-Löf random relative to $\emptyset^{(n-1)}$. So it is 1-random if it is Martin-Löf random, 2-random if it is Martin-Löf random relative to $\emptyset'$, etc. Ding, Downey, and Yu [**7**] proved that each 3-random set is Kolmogorov random. Indeed we can push the result by one level and show that *Kolmogorov randomness coincides with 2-randomness* (Theorem 2.8). This had been conjectured by C. Calude (personal communication to André Nies, Auckland, June 2003). That 2-randomness implies Kolmogorov randomness was proved independently (and earlier) by Miller [**22**]. Note that Martin-Löf randomness was characterized by Schnorr in terms of the *prefix-free* Kolmogorov complexity K, whereas the above characterization is in terms of the *plain* Kolmogorov complexity C. It is remarkable that such a "high-level" notion of randomness as 2-randomness can be thus characterized by a "low-level" notion as C-complexity. Like the characterization of Martin-Löf randomness, this is a new connection between the theory of randomness of finite and that of infinite objects. It also revindicates the notion of C-complexity as more than a mere "historical accident" (Chaitin [**4**, p. 87]). We extend the characterization by showing that 2-randomness is also equivalent to *time-bounded* Kolmogorov randomness. This notion is defined in the same way, using C^g instead of C, where $C^g(x)$ is the plain Kolmogorov complexity of x with time bound g. The particular choice of g does not matter for our results. Although in this paper we are mainly concerned with *infinite* random sequences, Section 2 also contains some relevant material about finite random strings.

In Section 3 we discuss lowness for Chaitin's Ω. Note that we can interpret every set like Ω also as the real number $\sum_{n\in\Omega} 2^{-n-1}$. Fixing a universal prefix-free machine U, Ω is that number which represents the halting probability of U, that is, the probability that an infinitely chosen sequence of 0s and 1s extends a program p such that $U(p)$ halts. The main reason for being interested in Ω is that Ω is a natural example for a left-r.e. random set and in a certain sense the only one: Kučera and Slaman [**14**] showed that all random left-r.e. sets are Ω-numbers, that is, represent the halting probability of some universal prefix-free machine.

At the beginning of Section 3 we discuss lowness for random sets and we prove a restriction on the complexity of sets that are low for Ω. We show that on the r.e. sets "low for Ω" is equivalent to being K-trivial. Since a set is K-trivial precisely when it is low for the Martin-Löf random sets, this means that, for r.e. A, when Ω is A-random then all random sets are A-random.

We then characterize the 2-random sets as those 1-random sets that are low for Ω (Theorem 3.10). This may be counterintuitive at first sight, since 2-random sets are "more random" than 1-random sets, but "low for Ω" is a *restriction* rather than a strengthening. One way of understanding this is that computational power and randomness are in fact orthogonal to each other. Another example of this is that 2-random sets are GL_1, i.e. satisfy $A' \leq_T A \oplus \emptyset'$ (Corollary 3.12).

At the end of Section 3 we discuss the relation between 2-generic and 2-random sets. From an earlier result of Demuth and Kučera it was known that a 2-generic cannot reduce to a 2-random set. We show that the converse is also true. In fact every 2-random set forms a *minimal pair* with every 2-generic set. This even holds for sets that are low for Ω (Theorem 3.14).

In Section 4 we discuss the separation of the notions of Martin-Löf randomness, recursive randomness, and Schnorr randomness. It was known that all of these notions are different (see Schnorr [**26**] and Wang [**34**]). Here we indicate precisely what computational resources are needed to separate them: we show that the three notions can be separated in every high degree, and conversely that if a set separates any two of these notions then this set must be high (Theorem 4.2). Moreover, if the high degree is r.e. then the notions can be separated by a left-r.e. set. Hereby a set is called *left-r.e.* if the set of all finite strings at the left of the characteristic function with respect to length-lexicographic order is recursively enumerable. Downey and Griffiths [**8**] independently proved that Schnorr randomness and recursive randomness can be separated by a left-r.e. set. At the end of Section 4 we make some remarks on Kurtz-randomness, hyperimmune-free degrees, and PA-complete degrees.

We now list the preliminaries and notation for this paper.

Our notation for Kolmogorov complexity follows Li and Vitányi [**17**]. Thus C denotes the plain Kolmogorov complexity function and K the prefix complexity. Usually, we use V to denote a universal plain machine (for the definition of C) and U to denote a universal prefix-free machine (for K). Our recursion theoretic notation is standard and follows [**25, 28**]. As usual, subsets $A \subseteq \mathbb{N}$ can be identified with infinite binary sequences and sometimes we interpret an $A \subseteq \mathbb{N}$ as the real number $\sum_{n \in A} 2^{-n-1}$. $A{\upharpoonright}n$ is the initial segment of A of length n and $\sigma \prec A$ denotes that σ is a finite initial segment of A. $\sigma \cdot \tau$ denotes string concatenation, $\{0,1\}^*$ is the set of finite binary strings and λ is the empty string.

As mentioned above, a set A is *left-r.e.* if the set of finite strings lexicographically left (= below) of A is an r.e. set. Equivalently one can define that the real number defined by A is approximable from below by a recursive sequence of rationals. Another straightforward characterization is that $\{q \in \mathbb{Q} : q < A\}$ is an r.e. set.

We will now list very briefly some preliminaries from effective measure theory. More discussion on these notions can be found e.g. in [**1, 32**]. We also refer there for complete references and suppress these in the following. A *martingale* is a function

$M : \{0,1\}^* \to \mathbb{R}^+$ that satisfies for every $\sigma \in \{0,1\}^*$ the averaging condition

$$2M(\sigma) = M(\sigma 0) + M(\sigma 1).$$

A martingale M *succeeds on* a set A if $\limsup_{n\to\infty} M(A{\restriction}n) = \infty$, and M succeeds on a class $\mathcal{A}$ of subsets of $\mathbb{N}$ if M succeeds on every $A \in \mathcal{A}$. The *success class* $S[M]$ of M is the class of all sets on which M succeeds. The basic theorem of Ville is that a class has Lebesgue measure zero if and only if it is included in a set of the form $S[M]$.

We now use effective martingales to introduce the three basic notions of randomness. A martingale M is r.e. if it is recursively approximable from below. An r.e. martingale is recursive if and only if $M(\lambda)$ is a recursive real number. In those cases where recursive martingales are needed, one can without loss of generality assume that $M(\lambda) = 1$ and that M outputs a rational number [**26**].

Definition 1.1. *Let A be any subset of the natural numbers.*

- *A is* Martin-Löf random *if there is no r.e. martingale M such that $A \in S[M]$.*
- *A is* recursively random *if there is no recursive martingale M such that $A \in S[M]$.*
- *A is* Schnorr random *if there is no recursive martingale M and no recursive non-decreasing and unbounded function r such that $M(A \restriction n) > r(n)$ for infinitely many n.*

In the remainder of this section we discuss a number of equivalent definitions that will be used throughout the paper.

Discussion 1.2. A *test* is a sequence of open classes $T_n \subseteq \{0,1\}^\infty$ such that the T_n are uniformly Σ_1. Here the T_n are uniformly in Σ_1 if there is a recursively enumerable array $\sigma_{n,m}$ of strings with

$$(\forall n)\left[A \in T_n \Leftrightarrow (\exists m)\left[\sigma_{n,m} \preceq A\right]\right].$$

The following statements are equivalent and characterize Martin-Löf randomness.

- A is not Martin-Löf random.
- There is a Σ_1-test $T_0, T_1, \ldots$ such that, for all n, $A \in T_n$ and $\mu(T_n) \leq 2^{-n}$.
- There is a Σ_1-test $T_0, T_1, \ldots$ such that $(\exists^\infty n)\,[A \in T_n]$ and $(\forall n)\,[\mu(T_n) \leq 2^{-n}]$.
- $(\forall c)(\exists x \prec A)[\,K(x) < |x| - c\,]$.

In the case of Schnorr randomness there are besides the test characterization and the standard martingale characterization some further martingale characterizations. The following statements are equivalent and characterize Schnorr randomness.

- A is not Schnorr random.
- A is covered by a Schnorr test. That is, there is a test $T_0, T_1, \ldots$ such that for all n, $A \in T_n$ and $\mu(T_n) = 2^{-n}$.
- For every recursive function r, there is a recursive martingale M and a recursive function h such that $(\exists^\infty n)\,[M(A \restriction h(n)) > r(n)]$.
- For every recursive function r, there is a recursive martingale M and a recursive function h such that $(\exists^\infty n)\,[M(A \restriction h(n)) > r(n)]$ and $M(x) \leq M(xy) + 1$ for all $x, y \in \{0,1\}^*$.

The last condition in the last statement says that the martingale never looses more than the amount 1. That is, if a gambler is betting according to the strategy of this martingale then he knows that after accumulating sufficient wealth he will never be poor again. The price the gambler pays for this strategy is that the growth-rate of the capital may be logarithmic compared to the growth rate of less reliable martingales. We refer to Schnorr's book [**26**] for further information about tests. Proofs of the various equivalences mentioned here can be found there, as well as in [**32, 34**].

2. Relativized randomness and Kolmogorov complexity

In this section we compare sequences that have infinitely often high C-complexity with relativized Martin-Löf random sequences. We start off with some observations about the complexity of finite strings. The method used to prove the following inequality goes back to Solovay's manuscript [**29**], and was further used in [**7**].

Proposition 2.1. *For all strings x and y, $C(xy) \leq K(x) + C(y) + O(1)$.*

Proof. Recall that V is the universal machine for C and U is the universal prefix-free machine for K. Define a plain machine L as follows. On input p, L first looks for $\sigma \preceq p$ such that $U(\sigma) \downarrow= x$. Then it tries to compute $V(z) = y$ where z is the rest of σ, i.e. $\sigma z = p$. In that case, it outputs xy. Now it is clear that $C(xy) \leq K(x) + C_L(y)$. □

As a consequence, we show that each substring of a finite C-random string is K-random. By Proposition 2.1 let c be a constant so that for each x, y, $C(xy) \leq K(x) + |y| + c$.

Proposition 2.2. *For each d and each string z, if $C(z) \geq |z| + c - d$, then $K(x) \geq |x| - d$ for each $x \preceq z$*

Proof. For $z \succeq x$, if $K(x) \leq |x| - d$ then $C(z) \leq K(x) + |z| - |x| + c \leq |z| + c - d$. □

Definition 2.3. (Ding, Downey, and Yu [**7**]) *A set X is* Kolmogorov random *if* $(\exists b)(\exists^\infty n)\big[C(X\restriction n) \geq n - b\big]$.

This notion was studied earlier in several forms, see Schnorr [**27**], Loveland [**18**], Daley [**5**]. E.g. Daley [**5**] proved that a set A is Kolmogorov random if and only if $(\exists b)(\exists^\infty n)\big[C(X\restriction n|n) \geq n - b\big]$, where $C(\sigma|n)$ is the complexity of σ *given* n.

We now give a simple proof of [**17**, Theorem 2.14 (I)] that each Kolmogorov random set is Martin-Löf random. Later we will strengthen this considerably.

Proposition 2.4. (Martin-Löf [**20**]) *Each Kolmogorov random set is Martin-Löf random.*

Proof. We only need the consequence of Proposition 2.1 that $C(xy) \leq K(x)+|y|+c$ for an appropriate constant c. If X is not Martin-Löf random, then for each d, there is an initial segment x of X such that $K(x) \leq |x| - d$. So for $z \succeq x$, $C(z) \leq K(x) + |z| - |x| + c \leq |z| + c - d$. Hence X is not Kolmogorov random. □

Schnorr [**26, 27**] proved that the converse direction of Proposition 2.4 does not hold.

An argument similar to the one in Proposition 2.1 can be used to answer a question of Calude e.a. [**2**] for each infinite recursive R, if Z has high prefix complexity on all initial segments whose length is in R, then Z is Martin-Löf random. This was independently proved by Lance Fortnow.

Proposition 2.5. *Suppose that the recursive set R is infinite. If there is b such that $(\forall r \in R)\,[K(Z{\upharpoonright}r) \geq r - b]$, then Z is Martin-Löf random.*

Proof. This time L is a prefix machine. As before, on input p L first looks for $\sigma \preceq p$ such that $U(\sigma)\downarrow= x$. Next, if $\sigma z = p$, it sees whether $|x| + |z|$ is the least number in R which is $\geq |x|$. In this case it outputs xz.

Clearly L is a prefix machine. Moreover, if $K(x) \leq |x| - d$, then for each extension w of x whose length is the least number in R which is $\geq |x|$, $K_L(w) \leq |w| - d$. Hence if Z is not Martin-Löf random, the hypothesis of the proposition fails. □

Of course, since every infinite r.e. set contains an infinite recursive subset, Proposition 2.5 also holds for infinite r.e. sets R. One can show that the proposition fails for some infinite Π^0_1 set R.

Next we compare Kolmogorov randomness with relativized randomness. We recall the following definition:

Definition 2.6. *A set A is n-random if and only if A is Martin-Löf random for the notion relativized to the oracle $\emptyset^{(n-1)}$.*

For the comparison of the randomness notions it will be useful to consider time-bounded C-complexity (see e.g. [**17**]). For any computable g such that $g(n) \geq n$, let

$$C^g(x) = \min\big\{\, |p| \ : V(p) = x \text{ in } g(|x|) \text{ steps} \,\big\},$$

where V is any universal plain machine. We may choose V such that V simulates all other machines with at most a logarithmic slowdown ([**17**, page 378], [**25**, Vol. 2, page 74]): If M is a machine working in time t then there is a constant c such that V simulates M in time $ct(n)\log(t(n))$. We will use this in the proof of Theorem 2.8.

Definition 2.7. (Time bounded Kolmogorov randomness) *We say that a set Z is* Kolmogorov random with time bound g *if* $(\exists b)(\exists^\infty n)\big[\,C^g(Z{\upharpoonright}n) \geq n - b\,\big]$.

Note that every Kolmogorov random set is Kolmogorov random with time bound g, for every recursive g. As noted above, a set A is Kolmogorov random if and only if $(\exists b)(\exists^\infty n)\big[\,C(X{\upharpoonright}n|n) \geq n - b\,\big]$. Terwijn [**31, 32**] showed that a similar equivalence holds for time-bounded Kolmogorov complexity.

The next theorem shows that 2-randomness is characterized by Kolmogorov randomness, as well as by its time-bounded version. Miller [**22**] obtained the implication from (I) to (II) independently of us. Ding, Downey, and Yu [**7**] proved that each 3-random set is Kolmogorov random. We modified this proof in Proposition 2.11 in order to get our proof for the direction from (I) to (II). Furthermore, Ding, Downey, and Yu [**7**] observed that no Kolmogorov random set is in Δ^0_2. This is also implied by Theorem 2.8 since 2-random sets cannot be Δ^0_2.

Theorem 2.8. *Let g be a computable time bound such that $g(n) \geq n^2 + O(1)$. The following are equivalent for any set Z:*

(I) *Z is 2-random*
(II) *Z is Kolmogorov random*
(III) *Z is Kolmogorov random with time bound g.*

Proof. (I) $\Longrightarrow$ (II) We introduce a concept which is of independent interest.

Definition 2.9. *We call a function $F : \{0,1\}^* \to \{0,1\}^*$ a* compression function *if $(\forall x)\left[|F(x)| \leq C(x)\right]$ and F is one-one. We say that a set Z is* Kolmogorov random with respect to *F if there is a constant b such that $|F(Z \restriction n)| \geq n - b$ for infinitely many n. Below we write $C_F(\sigma) = |F(\sigma)|$.*

Lemma 2.10. *There is a compression function F such that $F' \leq_T \emptyset'$.*

Proof. Consider the Π^0_1 class of graphs of partial functions extending the plain universal machine U. By the low basis theorem (see e.g. [**25**, Vol. 1, Theorem V.5.32]) there is a low path A which is the graph of some extension $\tilde{U}$ of U. Now let $F(x)$ be the first p with respect to length-lexicographic such that $\langle p, x\rangle \in A$, that is, $\tilde{U}(p) = x$. Since for every x there is a q with $U(q) = x$, the function F is total. Furthermore the p found satisfies $|p| \leq |q|$ by the length-lexicographic search constraint and $|F(x)| \leq C(x)$. So F is a compression function. Since $x = \tilde{U}(F(x))$ for all x, F is one-one. □

Lemma 2.11. *Let F be a compression-function. If Z is 2-random relative to the oracle given by the graph of F, then Z is Kolmogorov random with respect to F.*

Proof. Suppose Z is not Kolmogorov random for F. We produce an F'-recursive Martin-Löf test $\{T_b\}_{b\in\mathbb{N}}$ that covers Z. Note that $Z \in \bigcap_b V_b$, where $V_b = \bigcup_t P_{b,t}$, and

$$P_{b,t} = \big\{X : (\forall n \geq t)[\, C_F(X\restriction n) < n - b\,]\big\}.$$

$P_{b,t}$ is a Π^0_1-class relative to F and $\mu(P_{b,t}) \leq 2^{-b}$ because as F is 1-1, for every n there are less than 2^{n-b} strings σ of length n such that $C_F(\sigma) < n - b$. As $P_{b,t} \subseteq P_{b,t+1}$, this implies $\mu(V_b) \leq 2^{-b}$. Let

$$R_{b,t,k} = \big\{X : (\forall n)[\, t \leq n \leq k \;\rightarrow\; C_F(X\restriction n) < n - b\,]\big\}.$$

For each t, F' can compute $k(t)$ such that

$$\mu(R_{b,t,k(t)} - P_{b,t}) \leq 2^{-(b+t+1)}.$$

Let $T_b = \bigcup_t R_{b,t,k(t)}$. Then the T_b are open sets that are Σ^0_2 relative to F, uniformly in b. Moreover, $V_b \subseteq T_b$ and $\mu(T_b - V_b) \leq 2^{-b}$, so $\mu(T_b) \leq 2 \cdot 2^{-b}$. Hence $\{T_b\}_{b\in\mathbb{N}}$ is indeed an F'-recursive test that covers Z. □

Choose a low compression function F. If Z is 2-random, then Z is 2-random relative to F (since F is low). By Proposition 2.11 Z is Kolmogorov random with respect to F. Since it holds for every x that $|F(x)|$ is shorter than the smallest program for x it follows that Z is Kolmogorov random.

(II) $\Longrightarrow$ (III): This is immediate from the definitions.

(III) $\Longrightarrow$ (I): We begin with a fact about finite strings.

Definition 2.12. *For $b \in \mathbb{N}$ we say that x is a b-*root *if*

$$(\exists t_0)(\forall w \succeq x)\big[\,|w| \geq t_0 \;\rightarrow\; C(w) \leq |w| - b\,\big].$$

*Similarly, for g as above we say x is a b-*root with time bound *g if the above holds even with $C^g(w)$.*

$K^{\emptyset'}(x)$ denotes the prefix complexity with oracle $\emptyset'$.

Lemma 2.13. *For some constant c^*, the following holds. Let g be a time bound with $g(n) \geq n^2 + O(1)$. If $K^{\emptyset'}(x) \leq |x| - b - c^*$, then x is a b-root with time bound g.*

Proof. Let $U^{\emptyset'}$ be the universal prefix machine with oracle $\emptyset'$. $U^{\emptyset'}(\sigma)[s]$ denotes the approximation of $U^{\emptyset'}(\sigma)$ at the end of stage s.

We plan to adapt the argument of Proposition 2.1 to $U^{\emptyset'}$. Let c^* be a coding constant to be determined later. If $K^{\emptyset'}(x) \leq |x| - b - c^*$ via a computation $U^{\emptyset'}(\sigma) = x, |\sigma| \leq |x| - b - c^*$, then the idea is to compress all extensions w of x for $|w| \geq t_0$, where the computation $U^{\emptyset'}(\sigma)$ is stable from t_0 on. Since we do not know t_0, we have to define a machine L which works for each possible t_0.

Definition of the plain machine L. Given an input p of length t, carry out *cycles s* for $s = 0, 1, \ldots$ until t steps have been used.

Cycle s. For each $n \leq s$ see if $U^{\emptyset'}(p\restriction n)[s]$ gives an output, x say. Choose n where the use of the computation is smallest. If n exists, let $\rho = p\restriction n$.

If s is greatest such that cycle s has been completed and values ρ, x have been obtained, and $p = \rho z$, output the string xz.

Note that L uses no more than $2t + O(1)$ steps, t for the cycles and t for copying z.

Claim 2.14. *Suppose that the computation $U^{\emptyset'}(\sigma)[s] = x$ is stable from $s = s_0$ onwards. Then there is t_0 such that for all $p = \sigma z$, if $t = |p| \geq t_0$, then $L(p) = xz$ in at most $2t + O(1)$ steps.*

Proof. To prove the Claim 2.14, pick t_0 so that for each p as above, L on input p passes cycle s_0. Then, for all cycles $s \geq s_0$, the value ρ obtained equals σ. Namely, the use of any computation $U^{\emptyset'}(p\restriction n)[s]$, $n \neq |\sigma|$ must be greater than the use of $U^{\emptyset'}(\sigma)[s]$, for if the use would be smaller this computation would be stable as well, contradicting that $U^{\emptyset'}$ is a prefix machine. But if the use of the computation for $p\restriction n$ is greater than that for σ then σ is chosen over $p\restriction n$ in cycle s. This proves Claim 2.14. □

Let c^* be the coding constant for L. Suppose $K^{\emptyset'}(x) \leq |x| - b - c^*$ via a computation $U^{\emptyset'}(\sigma) = x$, $|\sigma| \leq |x| - b - c^*$. Let s_0 be a stage from which on this computation is stable. Choose t_0 as in Claim 2.14. Then for each $w = xz$ of length $\geq t_0 + |x|$, $L(p) = w$ in at most $2|w|$ steps where $p = \sigma z$. Hence $C(w) \leq C_L(w) + c^* \leq |x| - b + |z| = |w| - b$ and in fact $C^g(w) \leq |w| - b$ since $g(n) \geq n^2 + O(1)$. □

We note that the existence of b-roots contrasts with the case of prefix complexity, where each string x has an extension w such that $K(w) > |w| - b$, for instance because one can extend x to a Martin-Löf random set X, which always satisfy $\lim_{n\to\infty} K(X\restriction n) - n = \infty$.

To complete the proof of (III) $\Longrightarrow$ (I), suppose Z is not 2-random. Given b and the constant c^* from Lemma 2.13, choose $x \prec Z$ such that $K^{\emptyset'}(x) \leq |x| - b - c^*$, so that by Lemma 2.13 x is a b-root with time bound g. Let t_0 be a number as in the definition of b-root. Then for each $n \geq t_0$, $C^g(Z\restriction n) \leq n - b$. Hence Z is not Kolmogorov random with time bound g. □

In the following we study the frequency of initial segments with high C-complexity for a 2-random set. Given a time bound g as above and a number b, for each set Z consider the function

$$f = f^Z_{g,b}(m) = (\mu n)(\exists p_0, \ldots, p_m \leq n)(\forall i \leq m)\big[C^g(Z\restriction p_i) \geq p_i - b\big],$$

where μn denotes the least n satisfying the condition. If Z is 2-random and hence time-bounded Kolmogorov random with some constant b, then the corresponding function f is total and $f \leq_T Z$. We show that f infinitely often exceeds each recursive function.

Proposition 2.15. *If Z is Kolmogorov random with time bound g and constant b, then $f = f^Z_{g,b}$ is not dominated by a recursive function.*

Proof. Suppose h dominates f. Consider the recursive tree

$$T = \big\{\sigma : (\forall m)\big[\,|\sigma| \geq h(m) \to (\exists p_0, \ldots, p_m \leq |\sigma|)(\forall i \leq m)[\,C^g(\sigma\restriction p_i) \geq p_i - b\,]\big]\big\}.$$

Since h dominates f, Z is a path on T. Moreover, each path is time-bounded Kolmogorov random and hence 2-random by Theorem 2.8. However, the leftmost path in T is Δ^0_2 and hence not 2-random, a contradiction. □

Corollary 2.16 (Kurtz). *Each 2-random set has hyperimmune Turing degree.*

Remark 2.17. *Let $f^Z_b(m) = (\mu n)(\exists p_0, \ldots p_m \leq n)(\forall i \leq m)\big[C(Z\restriction p_i) \geq p_i - b\big]$. We have shown that there is a single $p \leq_T \emptyset'$ such that p dominates f^Z_b, for each 2-random Z and b sufficiently large.*

3. Low for Ω

Let $\mathcal{C}$ be a class that relativizes to $\mathcal{C}^X$ for an oracle X. A set A is called *low* for $\mathcal{C}$ if $\mathcal{C} = \mathcal{C}^A$. Several authors have studied the Turing degrees of sets that are low for classes of random sets.

- (Kučera and Terwijn [**15**]) There is a nonrecursive r.e. set that is low for the Martin-Löf random sets. Every such set must be in Δ^0_2 by Nies [**24**].
- (Nies [**24**]) A set is low for the recursively random sets if and only if it is recursive.
- (Terwijn and Zambella [**33**]) There are uncountably many sets that are low for the Schnorr random sets. These all have hyperimmune-free degree, hence *cannot* be in Δ^0_2.

In this section we study lowness for an individual random set, namely Chaitin's Ω [**3**]. Following a tradition of Chaitin, we denote by the symbol Ω not only the set but also the real number $\sum_{n \in \Omega} 2^{-n-1}$ represented by the set. Fixing a universal prefix-free machine U, Ω is the halting probability of U and satisfies the equation

$$\Omega = \sum_{\sigma \in dom(U)} 2^{-|\sigma|}.$$

Note that the definition of Ω depends on the choice of U. We can choose U also such that $U = U^{\emptyset}$ for the oracle $\emptyset$ and U^A is a universal prefix-free machine relative to A. Then Ω^A is the set representing the halting-probability of U^A. Every set Ω^A is left-r.e. relative to A and Martin-Löf random relativized to A. Note that for most oracles A, Ω^A is not left-r.e. (unrelativized). Furthermore, we might write Ω_V instead of Ω if we use the prefix machine V instead of U.

Definition 3.1. *A is* low for Ω *if Ω is Martin-Löf random relative to A.*

Note that this property does not depend on the particular universal machine U: If V is a further universal prefix machine, then Ω_U is equivalent to Ω_V under Solovay reducibility. Relativizing the main result of Kučera and Slaman [**14**], for sets X which are left-r.e. relative to A, one has that X is Martin-Löf random relative to A if and only if X is complete for Solovay reducibility relativized to A. Thus Ω_U is A-random if and only if Ω_V is.

We first prove that each low for Ω set is generalized low. Then we see that for r.e. sets, the restriction to Ω instead of all Martin-Löf-random sets does not matter, since here low for Ω coincides with K-trivial and hence with low for the Martin-Löf random sets by [**24**]. However, this is not true for sets in general, since all 2-random sets are low for Ω, so this class has in fact measure 1!

The following proof is similar to the one of Kučera [**13**] that all sets which are low for Martin-Löf randomness are in the class GL_1.

Theorem 3.2. *Let A be low for Ω. Then A is generalized low: $A' \leq_T A \oplus \emptyset'$.*

Proof. Let ψ^A be an A-recursive function with A' as domain, and for any $x \in A$ let $\Psi^A(x)$ be the time it takes for x to be enumerated into A'. Let Ω_s be the approximation to Ω at stage s. Each class

$$T_n^A = \bigcup_{x \in A'} (\Omega_{\Psi^A(x)} \restriction x + n + 1) \cdot \{0,1\}^{\infty}$$

has at most measure $\sum_x 2^{-x-n-1} = 2^{-n}$ and hence these classes form a Σ_1^A-test. Since A is low for Ω, there is an n such that $\Omega \notin T_n$. Thus, for all $x \in A'$, $c_\Omega(x+n) > \Psi^A(x)$, where $c_\Omega(z)$ is the least s such that $\Omega_s \restriction z = \Omega \restriction z$. So we have that $x \in A'$ if and only if x is enumerated into A' within $c_\Omega(x+n)$ many steps, hence $A' \leq_T A \oplus \Omega$. □

Definition 3.3 ([**9**]). *A is K-trivial if $K(X \restriction n) \leq K(n) + O(1)$ for every n.*

Definition 3.4. *An r.e. set $W \subseteq \mathbb{N} \times \{0,1\}^*$ is a* Kraft-Chaitin set (KC set) *if*

$$\sum_{\langle r,y \rangle \in W} 2^{-r} \leq 1.$$

The pairs enumerated into W are called axioms. *For any W, the* weight *of W is* $\mathrm{weight}(W) = \sum\{2^{-r} : \langle r,y \rangle \in W\}$.

Theorem 3.5. (Chaitin [**3**, Theorem 3.2]) *From a Kraft-Chaitin set W one can effectively obtain a machine M with prefix-free domain such that*

$$(\forall \langle r, y\rangle \in W)(\exists w)\left[\,|w| = r \;\wedge\; M(w) = y\,\right].$$

We say that M is a prefix machine for *W.*

Theorem 3.6. *An r.e. set is low for Ω if and only if it is K-trivial.*

Proof. Each K-trivial set is low for the Martin-Löf random sets by [**24**, Corollary 5.2], and hence low for Ω. For the converse direction, let A be an r.e. set which is low for Ω. We enumerate a Martin-Löf test $\{R_d^A\}_{d\in\mathbb{N}}$ relative to A. Then there is d such that $\Omega \notin R_d^A$. This will be used to define a Kraft-Chaitin set L_d showing that A is K-trivial: for each n there will be an axiom $\langle r, A\restriction n\rangle \in L_d$ where $r \le K(n) + d + 1$.

L_d is a union $S \cup \widetilde{L}_d$, where S supplies a new axiom when $K(n)$ decreases, and $\widetilde{L}_d$ does when $A\restriction n$ changes (after some delay). Let $S = \{\langle K_s(n) + 2, A_s\restriction n\rangle : K_s(n) < K_{s-1}(n)\}$. Then S is a KC set of weight $\le \Omega/2$. (Namely, for every n it holds that $\sum\left\{2^{-K_s(n)} : s \in \mathbb{N} \wedge K_s(n) < K_{s-1}(n)\right\} \le \sum_{r\ge K(n)} 2^{-r} = 2\cdot 2^{-K(n)}$, so $\mathrm{weight}(S) \le \frac{1}{4}\sum_n 2\cdot 2^{-K(n)} = \Omega/2$.) Next, when k enters A at stage s, we want to enumerate axioms $\langle K_s(n) + d + 1, A_s\restriction n\rangle$ into $\widetilde{L}_d$ for each n, $k < n \le s$. We ensure $\widetilde{L}_d$ is a KC set of weight at most $1/2$, so that $L_d = \widetilde{L}_d \cup S$ is a KC set. To do so, we "force" Ω to increase by $2^{-(K_s(n)+d)}$ before we put the axiom into $\widetilde{L}_d$. Thus, enumeration into $\widetilde{L}_d$ is charged against increases of Ω. The increase is achieved by putting at subsequent stages s an interval $\left[\Omega_s, \Omega_s + 2^{-K_s(n)-d}\right]$ into R_d^A with an appropriate A-use. Either A changes (and we do not need the new axiom anymore), or Ω has to move out of the interval. Note that this construction shares elements with the one in [**14**] showing that each random left-r.e. set is Solovay complete.

Construction of R_d^A and $\widetilde{L}_d$. For each parameter d simultaneously, perform the following. At every stage $s > 0$ a unique procedure P_n, $n = n_s$, is running, which was started at a stage $t \le s$ and has the goal $\Omega \ge \Omega_t + 2^{-K_t(n)-d}$. Let $n_0 = 0$.

Stage $s > 0$.

- If the procedure $P_{n_{s-1}}$ has ended at stage $s-1$ then let $k = 1$, else $k = 0$. Let $n = n_s = \min(\{n_{s-1} + k\} \cup (A_s - A_{s-1}))$.
- If $n_s \ne n_{s-1}$ we say that P_n is *started at* s, and we enumerate the interval
$$I_{n,s} = \left[\Omega_s, \Omega_s + 2^{-K_s(n)-d}\right]$$
into $R_d^{A_s}$ with use n. (We are slightly abusing notation here, by identifying intervals in the unit interval $[0,1]$ with intervals of the same measure in Cantor space $\{0,1\}^\infty$, using dyadic expansions.)
- If P_n has last been started at stage t and $\Omega_s \notin I_{n,t}$ then we say that P_n *ends* and we put the axiom $\langle K_t(n) + d + 1, A\restriction n\rangle$ into $\widetilde{L}_d$.

Claim 3.7. $(\forall d)[\mu(R_d^A) \le 2^{-d}]$*, hence R_d^A is a Martin-Löf test relative to A.*

Proof. For, if an interval $I_{n,s}$ is added to $R_d^{A_s}$ at stage s, then since this was done so with use n this interval is not in R_d^A unless also $A_s\restriction n = A\restriction n$. P_n is started at most once after $A_s\restriction n = A\restriction n$ and hence can contribute at most $2^{-K_s(n)-d}$ to $\mu(R_d^A)$. Hence $\mu(R_d^A) \le 2^{-d}$. □

Claim 3.8. *$\widetilde{L}_d$ is a KC set of weight $\leq 1/2$.*

Proof. For when P_n ends and contributes an axiom $\langle r+1, y\rangle$, then Ω has increased by 2^{-r} since the stage when this run of P_n was started. As only one procedure runs at each stage, this implies the claim. □

Claim 3.9. *A is K-trivial.*

Proof. Let d be such that $\Omega \notin R^A_d$, which exists since by the first claim R^A_d is an A-test and Ω is A-random. We show that for each n there is an axiom $\langle K(n) + c, A\restriction n\rangle \in L_d$ where $c \leq d + 1$. If $A \restriction n = 0^n$ the required axiom is in S. Else suppose s is greatest such that some $u' < n$ is in $A_s - A_{s-1}$. Then some P_u is running by the end of stage s, $u \leq u'$. Say this run was started at $t \leq s$. Since P_u is still running at s, $A_t\restriction u = A_s\restriction u = A\restriction u$, hence $I_{u,t}$ is in R^A_d. As $\Omega \notin R^A_d$, P_u ends. Since $A_s\restriction n = A\restriction n$, by the same reasoning the subsequently started procedures $P_{u+1}, \ldots, P_n$ end as well. When P_n ends, we put an axiom $\langle K_t(n) + d + 1, A\restriction n\rangle$ into $\widetilde{L}_d$. This is the required axiom unless $K(n) < K_t(n)$, in which case the axiom is in S. □

With these claims, also the proof of Theorem 3.6 is completed. □

By [**24**], a K-trivial set A is in fact low for K, namely $K(x) \leq K^A(x) + O(1)$ for all x. The proof of Theorem 3.6 could be modified in order to reach this conclusion directly.

We next give a further characterization of 2-randomness.

Theorem 3.10. *A set A is 2-random if and only if A is 1-random and low for Ω.*

Proof. M. van Lambalgen [**16**] showed that for any two sets A and B, $A \oplus B$ is Martin-Löf random if and only if B is Martin-Löf random and A is Martin-Löf random relative to B. Thus, for any 1-random set A it holds that A is 2-random $\Leftrightarrow$ A is 1-random relative to Ω $\Leftrightarrow$ $A \oplus \Omega$ is 1-random $\Leftrightarrow$ Ω is 1-random relative to A $\Leftrightarrow$ A is low for Ω. Since any 2-random set A is 1-random the equivalence follows. □

Every PA-complete set A bounds a 1-random set B. If the PA-complete set has hyperimmune-free or Δ^0_2 Turing degree, then B is not 1-random and thus not low for Ω. It follows that in this cases, A is also not low for Ω. So one has the following corollary.

Corollary 3.11. *No PA-complete set of hyperimmune-free Turing degree and no PA-complete set below $\emptyset'$ is low for Ω.*

Theorems 3.2 and 3.10 give the following result immediately, which according to Kautz [**11**, Theorem IV.2.4 (III)] is due to Sacks and Stillwell.

Corollary 3.12 (Sacks and Stillwell). *Every 2-random set A is* GL_1*, i.e. satisfies $A' \leq_T A \oplus \emptyset'$.*

An interesting example is $A = \Omega^{\emptyset'}$, which is 2-random and hence GL_1, but also high, as $\emptyset'' \equiv_T A \oplus \emptyset' \leq_T A'$.

By Nies [**24**] every set that is low for the Martin-Löf random sets is in Δ^0_2, hence has hyperimmune degree. The question remains whether Corollary 2.16 can be strengthened, namely,

Question 3.13. *Does every set that is low for Ω have hyperimmune Turing degree?*

Demuth and Kučera [**6**] proved that no 1-random set is below a 1-generic set, which implies that no 2-random set is below a 2-generic set. The next theorem shows that the conversely no 2-generic set is below a 2-random set. In fact, every such two sets build a minimal pair. This even holds when we weaken "2-random" to "low for Ω". Since every 2-random set is above a 1-generic set [**11**, Theorem IV.2.4 (V)], the result cannot be strengthened to minimal pairs between 2-random and 1-generic sets. In particular, many 1-generic sets are low for Ω.

Theorem 3.14. *Let A be 2-generic and let B be low for Ω. Then A and B form a minimal pair.*

Proof. Suppose that Ψ is a Turing reduction and that $D = \Psi^A$ is nonrecursive. We have to prove that $D \not\leq_T B$. For this it suffices to show that D is not low for Ω, which we do by showing that there is a D-computable martingale M^D that succeeds on Ω.

For every $\sigma \in \{0,1\}^*$ we recursively define a function $g(\sigma) = \bigcup_s g_s(\sigma)$ as follows. At stage 0 we define $g_0(\sigma) = \sigma$. Given $g_s(\sigma)$ at stage s, we search for an extension $\tau \succ g_s(\sigma)$ such that Ψ^τ is defined on strictly more numbers than $\Psi^{g_s(\sigma)}$. If τ is found, define $g_{s+1}(\sigma) = \tau$ and let $g_{s+1}(\sigma)$ be undefined otherwise.

Now for every σ there are two possibilities:

(a) $g(\sigma)$ is total and $\Psi^{g(\sigma)}$ is a recursive set, or
(b) $g(\sigma)$ is finite and there is no total extension h of $g(\sigma)$ such that Ψ^h is total.

We first show that case (b) never obtains. Define the $\emptyset'$-recursive function G by

$$G(\sigma) = \begin{cases} g(\sigma) & \text{if } g(\sigma) \text{ is finite,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

(G simulates g and uses the oracle $\emptyset'$ to see whether the definition of g has terminated or not.) Since Ψ^A is total, for every $\sigma \prec A$ we have that $G(\sigma)$ is either undefined or incomparable to A. By 2-genericity there is a $\tau \prec A$ such that $G(\sigma)$ is undefined for all $\sigma \succeq \tau$. For the rest of the proof, there is no loss of generality if we assume that τ is the empty string. Hence $g(\sigma)$ is total for all $\sigma \in \{0,1\}^*$ and case (a) above always obtains.

Now we define a D-recursive function F^D by

$$F^D(x) = (\mu y)(\forall \sigma \in \{0,1\}^x)(\exists z < y)\big[\Psi^{g(\sigma)}_y(z)\!\downarrow \neq D(z)\big].$$

Since all $\Psi^{g(\sigma)}$ are total and recursive, they all differ from the nonrecursive set D. Hence F^D is total and recursive in D.

Next we show that F^D is fast-growing. Recall that $c_\Omega(z)$ is the least s such that $\Omega_s{\restriction}z = \Omega{\restriction}z$. Define $H(\sigma) \prec g(\sigma)$ to be so long that $\Psi^{H(\sigma)}(z)$ is defined for all

$z \leq c_\Omega(3|\sigma|)$. H is $\emptyset'$-recursive because c_Ω is. By 2-genericity of A there are infinitely many $\sigma \prec A$ such that $H(\sigma) \prec A$. For these σ it holds that

$$F^D(|\sigma|) > c_\Omega(3|\sigma|). \tag{1}$$

Finally we show how D can use F^D to cover Ω. Let M^D be the D-recursive martingale that on input σ of length n bets half its capital that the next bit is $b = \Omega_{F(n)}(n)$: $M^D(\sigma b) = (3/2)M^D(\sigma)$ and $M^D(\sigma(1-b)) = (1/2)M^D(\sigma)$. Now if σ satisfies (1) then $\Omega_{F(n)}\restriction 3n = \Omega\restriction 3n$, so $M^D(\Omega\restriction 3n) \geq (1/2)^n(3/2)^{2n} = (9/8)^n$. Since there are infinitely many σ satisfying (1) it follows that M^D succeeds on Ω. (It follows even that Ω is not Schnorr random relative to D.) □

Remark 3.15. We note that neither part of the hypothesis in Theorem 3.14 can be weakened. Namely:

- There are many 1-generic sets that are low for Ω. Since the sets which are low for Ω are closed downward under Turing reductions, it is enough to consider the fact that the following examples of sets which are low for Ω bound a 1-generic set.
  - Every 2-random set: These are low for Ω by Theorem 3.10 and they bound a 1-generic set by [**11**, Theorem IV.2.4 (V)].
  - Every nonrecursive r.e. K-trivial set: Note that such a set exists [**15, 24**]. It is low for Ω by Theorem 3.6. It bounds a 1-generic set because every nonrecursive r.e. set does [**25**, Vol. 2, Proposition XI.2.10].

  In particular, our "natural examples" for sets which are low for Ω do not build a minimal pair with every 1-generic set.
- Above every set there is a 1-random set by Kučera [**12**]. In particular, no 2-generic set builds a minimal pair with every 1-random set.

4. Separating randomness notions in Turing degrees

In this section we show that the notions of Martin-Löf randomness, recursive randomness, and Schnorr randomness coincide in every non-high Turing degree and can be separated in every high Turing degree. Furthermore, they can be separated by left-r.e. sets. if the high degree happens to be an r.e. degree. That Schnorr randomness and recursive randomness can be separated by left-r.e. set was independently proven by Downey and Griffiths [**8**].

Recall that a set A is high if and only if $A' \geq_T \emptyset''$. Martin [**28**, Theorem XI.1.3] showed that a set A is high if and only if there is an A-recursive function which dominates every recursive function.

Proposition 4.1. *If a Schnorr-random set does not have high Turing degree then it is Martin-Löf random.*

Proof. Let A be a set that does not have high Turing degree and that is not Martin-Löf random, say A is covered by Martin-Löf test $T = \{T_i\}_{i\in\mathbb{N}}$. We show that A is not Schnorr random. Let f be an A-recursive function that computes when A is covered by U. That is, f computes for every n how long we have to enumerate T_n to include A. Since f is computable relative to a non-high oracle, there is a recursive function g such that $g(n) > f(n)$ for infinitely many n. Now consider the Schnorr test V where V_n contains all sets Z which are enumerated into V within $g(n)$ steps. Then every V_n is finite. So V is a Schnorr test and A is in V_n for infinitely many n. As mentioned in Discussion 1.2, this implies that A is not Schnorr random. □

Theorem 4.2. *For every set A, the following are equivalent.*

(I) *A is high.*
(II) *$\exists B \equiv_T A$, B is recursively random but not Martin-Löf random.*
(III) *$\exists C \equiv_T A$, C is Schnorr random but not recursively random.*

Furthermore, the same equivalence holds is one considers left-r.e. sets.

Proof. (III) ⇒ (I) and (II) ⇒ (I): These implications follow immediately from Proposition 4.1.

(I) ⇒ (II): Given A, the set B is constructed in two steps as follows. First a set F is constructed which contains information about A and partial information about the behaviour of recursive martingales – this information will then be exploited to define a partial recursive martingale that witnesses that the finally constructed recursively random set B is not Martin-Löf random. The sets A and F will be Turing equivalent and the sets B and F will be wtt-equivalent.

Let $\langle \cdot\,, \cdot\rangle$ be Cantor's pairing function $\langle x, y\rangle = \frac{1}{2}\cdot(x+y)\cdot(x+y+1)+y$. Furthermore, the natural numbers can be split into disjoint and successive intervals of the form $\{z_0\}, I_0, \{z_1\}, I_1, \ldots$ such that the following holds.

- The intervals $\{z_k\}$ contain the single element z_k.
- The intervals I_k are so long that for every $\sigma \in \{0,1\}^{z_k+1}$ and every partial martingale M defined on all extensions $\tau \in \sigma \cdot \{0,1\}^*$ with $|\tau| \leq |\sigma| + |I_k|$ there are two extensions $\tau_{\sigma,0,M}, \tau_{\sigma,1,M}$ of length $|\sigma| + |I_k|$ such that M does not grow beyond $M(\sigma) \cdot (1 + 2^{-k})$ within I_k. These extensions can be computed from M. Without loss of generality it holds that $\tau_{\sigma,0,M} <_{lex} \tau_{\sigma,1,M}$.
- The partition of the natural numbers in the intervals $\{z_0\}, I_0, \{z_1\}, I_1, \ldots$ is computable. This can be done since one can compute from k a length for which an I_k of this length with the properties in the previous item exist [**21**, Remark 9], see also [**26, 34**].

Let $M_0, M_1, \ldots$ be a recursive list of all partial recursive martingales. That is, the enumeration satisfies the following conditions:

- The uniform domain $\{(i, \sigma) : M_i(\sigma) \text{ is defined}\}$ is a recursively enumerable set.
- If $M_i(\sigma\tau)$ is defined for some non-empty string τ, then $M_i(\sigma)$, $M_i(\sigma 0)$, $M_i(\sigma 1)$ are also defined and their values are positive rational numbers.
- If $M_i(\sigma 0), M_i(\sigma 1)$ are defined, then $M_i(\sigma 0) + M_i(\sigma 1) = 2M_i(\sigma)$.

Now a partial recursive martingale M is defined inductively as follows. The goal is to let M multiplicatively dominate all recursive martingales on its domain of definition (i.e. for every recursive martingale N there is a constant c such that for all σ, if $M(\sigma)\downarrow$ then $N(\sigma) \leq c \cdot M(\sigma)$), while M does not succeed on a set B

constructed below. This then ensures that B is recursively random. Furthermore, a set $F \equiv_T A$ is constructed such that

- $F(k)$ is coded into $B \upharpoonright z_{k+1}$ where "most" of the coding into B is done on the interval I_k.
- $F(\langle i,j \rangle)$ for $i \neq 0$ tells whether M_i is defined on all strings up to the length of $z_{\langle i,j+1 \rangle +1}$. This is necessary to know since on each length M will be the weighted sum of some M_i's and only M_i's which are defined on all relevant inputs should be considered.
- M can decode $F(k')$ for all $k' < k$ from $B \upharpoonright z_k$. This information permits to compute M on all τ with $B \upharpoonright z_k \preceq \tau$ and $|\tau| \leq z_{k+1}$. If a set $\tilde{B} \neq B$ is considered, it might be impossible to retrieve F and therefore, $M(\tilde{B} \upharpoonright q)$ might be undefined for some q. Thus, M is a partial recursive and not a total recursive martingale.

Now the details of the constructions just outlined are given. First we give the definition of M. Although M will only be partial, $M(B \upharpoonright x)$ will be defined for all x. For each k and $\eta \in \{0,1\}^{z_k}$ where $M(\eta)$ is already defined, we will try to define $M(\tau)$ for all $\tau \in \eta \cdot \{0,1\}^*$ with $|\tau| \leq z_{k+1}$.

(1) $M(\lambda) = r_\lambda$ and $r_\lambda = 1$.

(2) Assume that $|\eta| = z_k$, $M(\eta)$, r_η are already defined and for all $l < k$ there are values a_l and strings $\sigma_l = \eta \upharpoonright z_l + 1$ such that $\tau_{\sigma_l, a_l, M}$ are defined and prefixes of η. Then

  (2.1) Compute $E = \big\{ i : \langle i,0 \rangle < k \wedge (\forall j)[\, \langle i,j \rangle < k \rightarrow a_{\langle i,j \rangle} = 1 \,] \big\}$.

  (2.2) Let $D = \{\tau \in \eta \cdot \{0,1\}^* : |\eta| < |\tau| \leq z_{k+1}\}$.

  (2.3) Compute for all $e \in E$ and $\tau \in D$ the value $M_e(\tau)$.

(3) If the algorithm has gone through step (2.3) and all the computations there have terminated then

$$(\forall \tau \in D)\Big[\, M(\tau) = r_\tau + \sum_{e \in E} 2^{-2z_{\langle e,0 \rangle +1} - 1} M_e(\tau) \,\Big]$$

where the sum is 0 for the case that $E = \emptyset$ and r_τ is defined inductively such that the conditions

$$M(\tau' 0) + M(\tau' 1) = 2M(\tau') \text{ and } r_{\tau' 0} = r_{\tau' 1}$$

are kept for all $\tau' \prec \tau$.

If the algorithm did not go through step (2.3), then $M(\tau)$, r_τ are undefined for all proper extensions τ of η.

The r_τ are necessary since at every level z_k, some M_i might be dropped from the sum and at most one new M_i is added. This new martingale is added if $k = 1 + \langle i,0 \rangle$ and $a_{\langle i,0 \rangle} = 1$. Furthermore, it is added with the factor $2^{-2z_k - 1}$ which guarantees that $M_e(\eta)$ is at most $2^{-z_k - 1}$ for all $\eta \in \{0,1\}^{z_k}$. But this increases the sum by at most $2^{-z_k - 1}$ and therefore can be compensated by r_τ: At every level, $r_\tau \geq 2^{-|\tau|}$ and at most $2^{-|\tau| - 1}$ of this capital is lost in order to maintain the martingale property of M.

By highness of A, let f^A be an A-recursive function which dominates all recursive functions. Now define the set F as follows.

- $F(\langle i,0 \rangle) = A(i)$ for all i.

- $F(\langle i,j\rangle) = 1$ if $F(\langle i,j'\rangle) = 1$ for all $j' < j$ and $M_i(\tau)$ is computed within $f^A(i+j)$ many steps for all $\tau \in \{0,1\}^*$ with $|\tau| \leq z_{\langle i+j+1,i+j+1\rangle}$. Otherwise $F(\langle i,j\rangle) = 0$.

Clearly $F \equiv_T A$. The set B is defined inductively.

(k.0) Assume that exactly $B\restriction z_k$ is defined.
Let $B(z_k) = 0$ if $M(B\restriction z_k \cdot 0) \leq M(B\restriction z_k \cdot 1)$
and $B(z_k) = 1$ otherwise.

(k.1) Assume that exactly $B\restriction z_k + 1$ is defined.
Let $\eta = B\restriction z_k + 1$ and $B\restriction z_{k+1} = \tau_{\eta,F(k),M}$.

We now need to show that the inductive definition of B goes through for all k. Note that the $a_{\langle i,j\rangle}$ in the construction of M always exist for $\eta \prec B$ and that they are just the bits $F(\langle i,j\rangle)$. So the decoding at the beginning of step (2) is possible. Furthermore, for all $i \in E$ with $i > 0$, $\langle i,j\rangle \in F$ for $j = 0,1,\ldots,j'$ where j' is the maximal j'' with $\langle i,j''\rangle < k$. Note that $j' \geq 0$ and thus M_i is defined on all strings of length up to z_{k+1}. Thus the computations in step (2.3) all terminate. So M is defined on all extensions of $B\restriction z_k$ of length up to z_{k+1}. It follows that B is defined up to z_{k+1} and $F(k)$ is coded into B.

Note that coding gives $F \leq_{wtt} B$. Furthermore, one can compute for each k the string $B\restriction z_k$ using information obtained from $F\restriction z_k$. So $B \leq_{wtt} F$. Since A and F are Turing equivalent, one has $B \equiv_T A$.

To see that B is not Martin-Löf random, it suffices to observe that $B(z_k)$ is computed from $B\restriction z_k$. Thus one can build a partial recursive martingale N which ignores the behaviour of B on all intervals I_k but always bets all its capital on $B(z_k)$ which is computed from the previous values. This martingale N clearly succeeds on B.

To see that B is recursively random, note first that M does not go to infinity on B: On z_k, M does not gain any new capital by the choice of $B(z_k)$. By choice of I_k, M can increase its capital on I_k at most by a factor $1 + 2^{-k}$. Since the sum over all 2^{-k} converges, the infinite product $\prod_k (1 + 2^{-k})$ also converges to some real number r and M never exceeds r. Now given any recursive martingale M' there are infinitely many programs i for M' which all compute M' with the same amount of time. Since f^A dominates every recursive function, there is a program i for M' such that for all j, $f^A(i+j)$ is greater than the number of steps to compute $M_i(\tau)$ for any string $\tau \in \{0,1\}^*$ with $|\tau| \leq z_{\langle i+j+1,i+j+1\rangle+1}$. It follows that $M_i(\eta) \leq 2^{2z_{\langle i,0\rangle+1}+1} \cdot M(\eta) \leq 2^{2z_{\langle i,0\rangle+1}+1} \cdot r$ for all $\eta \preceq B$. Thus B is recursively random.

(I) $\Rightarrow$ (II), r.e. case: If A is a r.e. as a set then one can choose f^A such that f^A is approximable from below. Therefore also F is r.e. and the set B can be approximated lexicographically from the left: In step (k.0) the value $B(z_k)$ is computed from the prefix before it and in step (k.1) one first assumes that $B\restriction z_{k+1}$ is given by $\tau_{B\restriction z_k+1,0,M}$ and later changes to $\tau_{B\restriction z_k+1,1,M}$ in the case that k is enumerated into F.

(I) $\Rightarrow$ (III): The construction of C is similar to the one of B above, with one exception: there will be a thin set of k's such that $B(z_k)$ is not chosen according to the condition (k.0) given above but $B(z_k) = 0$. These guaranteed 0's will be distributed in such a way that on the one hand they appear so rarely that the Schnorr bound cannot be kept while on the other hand they still permit a recursive winning strategy for the martingale. Now let

$$\psi(e,x) = z_{\langle\langle e,\Phi_e(x)\rangle,x\rangle+1}$$

for the case that $\varphi_e(x)$ is defined and uses $\Phi_e(x)$ many computation steps to converge, otherwise $\psi(e,x)$ is undefined. Note that ψ is one-one, has a recursive range and satisfies $\psi(e,x) \geq z_{x+1} > x$ for all (e,x) in its domain. Furthermore, let

$$p(x) = \begin{cases} p(y)+1 & \text{if } (\exists e \leq \log p(y))\,[\psi(e,y) = x\,] \text{ for some } y < x, \\ x+4 & \text{otherwise.} \end{cases}$$

The function p is computable, unbounded and takes every value only finitely often. Assume without loss of generality that φ_0 is total and let

$$g^A(x) = \max\{\psi(e,x) : \psi(e,x)\!\downarrow\, \leq f^A(x) \wedge e < \log(p(x)) - 1\}.$$

The set C is defined by the same procedure as B with one exception: namely $C(z_k) = 0$ if $z_k = g^A(x)$ for some $x < z_k$. So having F as above, the overall definition of C is the following:

(k.0) Assume that exactly $C{\restriction}z_k$ is defined.
Let $C(z_k) = 0$ if $M(C{\restriction}z_k \cdot 0) \leq M(C{\restriction}z_k \cdot 1) \vee z_k \in \mathrm{range}(g^A)$
and $C(z_k) = 1$ otherwise.

(k.1) Assume that exactly $C{\restriction}z_k + 1$ is defined.
Let $\eta = C{\restriction}z_k + 1$ and $C{\restriction}z_{k+1} = \tau_{\eta,F(k),M}$.

The proof that $C \equiv_T A$ is the same as the proof that $B \equiv_T A$ except that one has to use the additional fact that g^A is recursive relative to A.

To see that C is not recursively random, consider the following betting strategy for a recursive martingale N. For every x, let $G_x = \{\psi(e,x) : \psi(e,x)\downarrow \wedge\, e < \log(p(x)) - 1\}$. Since ψ is one-one, these sets are all disjoint and every G_x contains a number z_k such that $C(z_k) = 0$. (Choose some small code e such that φ_e is total.) Starting with $x = z_0$, the martingale N adopts for every G_x a St. Petersburg - like strategy to gain the amount $1/p(x)$ on it, using the knowledge that G_x contains some z_k. For this purpose, N sets aside one dollar of its capital. More precisely: If the next point y to bet on is not in the current G_x, N does not bet. If $y \in G_x$ and N has lost m times while betting on points in G_x, then N bets $2^m/p(x)$ of its capital on $C(y) = 0$. In case of failure, N stays with x and waits for the next element of G_x without betting intermediately. In case of success, N has gained on the points of G_x in total the amount $1/p(x)$ and updates x to the current value of y and m to 0. Because $|G_x| < \log(p(x)) - 1$ this strategy never goes broke. Note that $p(y) = p(x) + 1$ (because N switches from G_x to G_y on some z_k). Thus one can verify inductively that – in the limit – N gains the amount $1/(z_0 + 4) + 1/(z_0 + 5) + 1/(z_0 + 6) + \ldots$, that is, goes to infinity. Thus N succeeds on C and C is not recursively random.

To see that C is not Schnorr random, assume by way of contradiction that for M_i and a recursive bound h we would have that $M_i(C{\restriction}h(m)) > m$ for infinitely many m. But for almost all m, $g^A(\log\log(m)) > h(m)$. An upper bound for M on C is then given by $M(C{\restriction}h(m)) \leq \log(m) \cdot r$ since M can increase its capital on any interval I_k only by $1 + 2^{-k}$ and furthermore only on those z_k which are in the range of g^A. But of the latter there are only $\log\log(m)$ many below $h(m)$. Since $\log(m) \cdot r \cdot 2^{2^{z_{\langle i,0\rangle+1}+1}} < m$ for almost all m, one has that $M_i(C{\upharpoonright}h(m)) < m$ for almost all m. Thus C is not Schnorr random.

(I) $\Rightarrow$ (III), r.e. case: If A is an r.e. set and f^A approximable from below, then g^A is also approximable from below; let g_s be this approximation. Now one verifies that C is left-r.e. due to the following approximation C_s obtained from the definition of C where the approximation C_s is defined from below by going up the stages $(k.0), (k.1)$ iteratively until the procedure is explicitly terminated.

(k.0) Assume that exactly $C_s{\upharpoonright}z_k$ is defined.
If $M_s(\sigma)$ is undefined for some $\sigma \in \{C_s{\upharpoonright}z_k \cdot 0, C_s{\upharpoonright}z_k \cdot 1\}$ then terminate the procedure to define C_s by going to (ter).
If $M(C{\upharpoonright}z_k \cdot 0) \leq M(C{\upharpoonright}z_k \cdot 1)$ or there is an $x < z_k$ such that $z_k = \psi(e,x)$ for some $x < z_k$ and $e < \log(p(x) - 1)$ and $g_s(p(x)) \leq z_k$
then $C_s(z_k) = 0$ else $C_s(z_k) = 1$.

(k.1) Assume that exactly $C_s{\upharpoonright}z_k + 1$ is defined.
Let $\eta = C_s{\upharpoonright}z_k + 1$. If $M_s(\sigma)$ is undefined for some $\sigma \in \{C_s{\upharpoonright}z_k + 1 \cdot \tau : |\tau| \leq |I_k|\}$ then terminate the procedure to define C_s by going to (ter).
Let $\eta = C{\upharpoonright}z_k + 1$ and $C{\upharpoonright}z_{k+1} = \tau_{\eta,F_s(k),M}$.

(ter) If the inductive definition above is terminated with $C_s = \eta$ for some string η, then one defines that C_s is the set with the characteristic function $\eta 0^\infty$.

Now consider different sets C_s and C_{s+1}. There is a first stage (k.a) in which the construction behaves differently for C_s and C_{s+1}. There are three cases:

Case 1. The difference is due to one but not both procedures terminates in stage (k.a). Since this termination is due to $M_s(\sigma)$ or $M_{s+1}(\sigma)$ being undefined for the same string σ in both cases, it follows that the procedure for C_s terminates but that for C_{s+1} not. Since C_s is extended by zeroes only, it holds that so $C_s \leq_{lex} C_{s+1}$.

Case 2. The procedure does not terminate for C_s, C_{s+1} at this stage and the stage is of the form (k.0). Then the only difference between the construction this stage for C_s, C_{s+1} can come from the case that $g_s(x) \leq z_k$ and $g_{s+1}(x) > z_k$. In this case $C_s(z_k) = 0$ and $C_{s+1}(z_k) = 1$, so $C_s <_{lex} C_{s+1}$.

Case 3. The procedure does not terminate for C_s, C_{s+1} at this stage and the stage is of the form (k.1). Then the only possible reason is that $k \in F_{s+1} - F_s$. Recall that $\eta = C_s{\upharpoonright}z_k + 1 = C_{s+1}{\upharpoonright}z_k + 1$. It follows that $C_s <_{lex} C_{s+1}$ by $\tau_{\eta,0,M} <_{lex} \tau_{\eta,1,M}$.

This case distinction gives $C_0 \leq_{lex} C_1 \leq_{lex} \ldots$ and so the approximation witnesses that C is a left-r.e. set. □

If A has hyperimmune-free degree, then one can even show that A is Kurtz-random if and only if A is Schnorr random. The reason is that one can choose g such that g dominates f.

Theorem 4.3. *A degree contains a set which is Kurtz-random but not Schnorr random if and only if the degree is hyperimmune. On the hyperimmune-free degrees, all considered notions of randomness coincide.*

Stephan [**30**] investigated the connection between PA-completeness and Martin-Löf randomness. He showed that no PA-complete set $A \not\geq_T K$ is in the Turing degree of a Martin-Löf random set. This result is somewhat surprising since such sets A exist and there are always Turing degrees of Martin-Löf random sets below A and above A.

Theorem 4.4. (Stephan [**30**]) *Every PA-complete Martin-Löf random set is above the halting problem* $\emptyset'$.

In Theorem 4.2 the following was shown for every set R which does not have high Turing degree: R is Schnorr random if and only if R is recursively random if and only if R is Martin-Löf random. Thus one can obtain the following corollary where "above K" is replaced by "having high Turing degree".

Corollary 4.5. *Every PA-complete Schnorr random set and every PA-complete recursively random set has high Turing degree.*

Acknowledgment. The second and third authors wish to thank Bakhadyr Khoussainov and the Marsden Fund for enabling them to visit the University of Auckland.

References

[1] Klaus Ambos-Spies and Antonín Kučera, *Randomness in computability theory*, in: P. Cholak et al., Computability Theory: Current Trends and Open Problems, Contemporary Mathematics 257 (2000) 1–14, American Mathematical Society.

[2] C. Calude, L. Staiger, K. Svozil, *Randomness relative to Cantor expansions*, CDMTCS Research Report 213, The University of Auckland, 2003.

[3] Gregory J. Chaitin, *A theory of program size formally identical to information theory*, Journal of the ACM 22 (1975) 329–340.

[4] Gregory J. Chaitin, *The Unknowable*, Springer Verlag, 1999.

[5] Robert P. Daley, *Complexity and randomness*, in: R. Rustin (ed.), Computational Complexity, Algorithmics Press (1971) 113–122.

[6] Osvald Demuth and Antonín Kučera, *Remarks on 1-genericity, semigenericity and related concepts*, Commentationes Mathematicae Universitatis Carolinae 28 (1987) 85–94.

[7] Decheng Ding, Rod Downey, and Liang Yu, *The complexity of the random reals*, to appear.

[8] Rod Downey and Evan Griffiths, personal communication, Wellington, March 28, 2003.

[9] Rod G. Downey, Denis R. Hirschfeldt, André Nies, and Frank Stephan, *Trivial reals*, Proceedings of the 7th and 8th Asian Logic Conferences (7th Conference: Hsi-Tou, Taiwan 6 – 10 June 1999, 8th Conference: Chongqing, China 29 August – 2 September 2002), World Scientific (2003) 103–131.

[10] Carl G. Jockusch, jr., Manuel Lerman, Robert I. Soare, and Robert M. Solovay, *Recursively enumerable sets modulo iterated jumps and extensions of Arslanov's completeness criterion*, The Journal of Symbolic Logic 54(4) (1989) 1288–1323.

[11] Steven M. Kautz, *Degrees of random sets*, PhD thesis, Cornell University, August 1991.

[12] Antonín Kučera, *Measure, Π^0_1-classes and complete extensions of PA*, in: H.-D. Ebbinghaus, G. H. Müller, and G. E. Sacks (eds), Recursion theory week, Springer Lecture Notes in Mathematics 1141 (1985) 245–259.

[13] Antonín Kučera, *On relative randomness*, Annals of Pure and Applied Logic 63 (1993) 61–67.

[14] Antonín Kučera and Theodore A. Slaman, *Randomness and recursive enumerability*, SIAM Journal on Computing 31 (2001) 199–211.

[15] Antonín Kučera and Sebastiaan A. Terwijn, *Lowness for the class of random sets*, The Journal of Symbolic Logic 64(4) (1999) 1396–1402.

[16] Michiel van Lambalgen, *The axiomatization of randomness*, The Journal of Symbolic Logic 55(3) (1990) 1143–1167.

[17] Ming Li and Paul Vitányi, *An introduction to Kolmogorov complexity and its applications*, first edition, Springer-Verlag, 1993. (Second edition 1997.)

[18] Donald W. Loveland, *On minimal program complexity measures*, in Proceedings 1st ACM Symposium on Theory of Computing (1969) 61–66.

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

[20] Per Martin-Löf, *Complexity oscillations in infinite binary sequences*, Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete 19 (1971) 225–230.

[21] Wolfgang Merkle and Nenad Mihailović, *On the construction of effective random sets*, Mathematical Foundations of Computer Science 2002, Springer LNCS 2420 (2002) 568-580.

[22] Joseph S. Miller, *Kolmogorov random reals are 2-random*, to appear.

[23] André Nies, *Each Low*(*CR*) *set is computable*, Manuscript, January 2003.

[24] André Nies, *Lowness properties and randomness*, to appear.

[25] Piergiorgio G. Odifreddi, *Classical recursion theory*, North-Holland, 1989 (Vol. 1) and Elsevier, 1999 (Vol. 2).

[26] Claus-Peter Schnorr, *Zufälligkeit und Wahrscheinlichkeit*, Springer Lecture Notes in Mathematics 218, Springer, 1971.

[27] Claus-Peter Schnorr, *A unified approach to the definition of random sequences*, Mathematical Systems Theory 5 (1971) 246–258.

[28] Robert I. Soare, *Recursively Enumerable Sets and Degrees*, Springer-Verlag, Heidelberg 1987.

[29] Robert M. Solovay, *Draft of a paper* (*or series of papers*) *on Chaitin's work.* Manuscript, IBM Thomas J. Watson Research Center, New York, May 1975.

[30] Frank Stephan, *Martin-Löf random and PA-complete sets*, Forschungsberichte Mathematische Logik 58 / 2002, Universität Heidelberg, 2002.

[31] Sebastiaan A. Terwijn, *Computability and measure*, PhD thesis, University of Amsterdam/ILLC, 1998.

[32] Sebastiaan A. Terwijn, *Complexity and randomness*, Report CDMTCS-212, The University of Auckland, March 2003. http://www.logic.at/people/terwijn/auckland.ps.

[33] Sebastiaan A. Terwijn and Domenico Zambella, *Computational randomness and lowness*, The Journal of Symbolic Logic 66(3) (2001) 1199–1205.

[34] Yongge Wang, *Randomness and complexity*, PhD Thesis, University of Heidelberg, 1996.