Using random sets as oracles

Denis R. Hirschfeldt*
Department of Mathematics
University of Chicago

André Nies†
Department of Computer Science
University of Auckland

Frank Stephan‡
Departments of Computer Science and Mathematics
National University of Singapore

Abstract

Let $\mathcal{R}$ be a notion of algorithmic randomness for individual subsets of $\mathbb{N}$. We say B is a *base for $\mathcal{R}$ randomness* if there is a $Z \geqslant_{\mathrm{T}} B$ such that Z is $\mathcal{R}$ random relative to B. We show that the bases for 1-randomness are exactly the K-trivial sets and discuss several consequences of this result. We also show that the bases for computable randomness include every Δ^0_2 set that is not diagonally noncomputable, but no set of PA-degree. As a consequence, we conclude that an n-c.e. set is a base for computable randomness iff it is Turing incomplete.

1 Introduction

The interaction between algorithmic randomness and computability-theoretic notions such as Turing reducibility has received much attention recently (see for instance the survey article [4]). In this paper, we focus on the computational power of a sufficiently random set.

We work in the Cantor space 2^ω, identifying an element of this space with the set of natural numbers of which it is the characteristic function. For finite binary

*Partially supported by the National Science Foundation of the USA, grants DMS-02-00465 and DMS-05-00590; and by the Marsden Fund of New Zealand, grant no. 03-UOA-130.

†Partially supported by the Marsden Fund of New Zealand, grant no. 03-UOA-130.

‡Partially supported by NUS grant R252-000-212-112 and, for a visit to Auckland, by the Marsden Fund of New Zealand, grant no. 03-UOA-130.

2000 Mathematics Subject Classification: 68Q30, 03D80 strings σ and τ, let $\sigma \preccurlyeq \tau$ denote that σ is an initial segment of τ. Similarly, for a set X and a string σ, let $\sigma \prec X$ denote that σ is an initial segment of (the characteristic function of) X.

The space 2^ω is endowed with the tree topology, which has as basic closed-open sets $[\sigma] = \{X \in 2^\omega : \sigma \prec X\}$, where $\sigma \in 2^{<\omega}$. The usual Lebesgue measure μ on 2^ω is induced by giving each basic closed-open set $[\sigma]$ the measure $2^{-|\sigma|}$.

For more on notions of randomness and their relationships to computability theory, see [3, 4, 21], and for basic notions of computability theory used below, see [13, 22, 23, 28].

The starting point of our investigations is the fact that if a set A is not computable, then the sets that compute A are not typical, as witnessed by the following classic theorem.

Theorem 1.1 (de Leeuw, Moore, Shannon, and Shapiro [12]; Sacks [24]). *If A is not computable then $\mu(\{Z : Z \geqslant_T A\}) = 0$.*

However, for any given notion $\mathcal{R}$ of algorithmic randomness for individual subsets of $\mathbb{N}$,[1] it is trivially true that there are noncomputable sets A such that $\{Z : Z \geqslant_{\mathrm{T}} A\}$ contains an $\mathcal{R}$ random set. (This may even be true for all A; see Theorem 1.10 below.) Still, one might expect $\{Z : Z \geqslant_{\mathrm{T}} A\}$ not to contain sets that are $\mathcal{R}$ random *relative to A*. (We will discuss relativization of notions of randomness below.) As we will see, though, if A is sufficiently simple, there may be sets that are $\mathcal{R}$ random relative to A and still manage to compute A.

Definition 1.2. Let $\mathcal{R}$ be a randomness notion. We say B is a *base for $\mathcal{R}$ randomness* if there is a $Z \geqslant_{\mathrm{T}} B$ such that Z is $\mathcal{R}$ random relative to B.

We study bases for two well-known randomness notions, 1-randomness and computable randomness, which we now define.

The first successful notion of randomness for individual sets was introduced by Martin-Löf [16], using an effective measure-theoretic approach, which came from the intuition that a random set should be typical, that is, not have any effectively rare properties. Martin-Löf's idea was to formalize the notion of an effectively null class, and to say that a set is random if it avoids any such class.

Definition 1.3. A *Martin-Löf test* (ML-test) is a uniformly computably enumerable (c.e.) sequence $\{U_i\}_{i\in\mathbb{N}}$ of Σ^0_1-classes such that $\mu(U_i) \leqslant 2^{-i}$. A set $\mathcal{A} \subseteq 2^\omega$ is *Martin-Löf null* (ML-null) if there is an ML-test $\{U_i\}_{i\in\mathbb{N}}$ such that $\mathcal{A} \subseteq \bigcap_i U_i$. A set A is *Martin-Löf random*, or 1-*random*, if $\{A\}$ is not ML-null.

Thus ML-null sets are small in an effective sense and the 1-random sets are those that do not belong to any effectively small set.

[1] Two such notions will be formally defined below.

Another approach to the definition of randomness is through the incompressibility paradigm, as embodied in the concept of Kolmogorov complexity. The idea here is that a random set should be incompressible; that is, its initial segments should not have short descriptions.

For a partial computable function f, we write $f(\sigma)\downarrow$ if $f(\sigma)$ is defined, and $f(\sigma)\uparrow$ otherwise. We say that a partial computable function $f : 2^{<\omega} \to 2^{<\omega}$ is *prefix-free* if the domain of f is an antichain, that is, if whenever $f(\sigma)\downarrow$ and $\sigma \prec \tau$, we have $f(\tau)\uparrow$. A prefix-free partial computable function U is *universal* if for each prefix-free partial computable function f there is a string ρ such that $\forall\sigma\,[U(\rho\sigma) = f(\sigma)]$.

The *prefix-free Kolmogorov complexity* $K(\sigma)$ of $\sigma \in 2^{<\omega}$ is defined to be $\min\{|\tau| : U(\tau) = \sigma\}$. The idea is that $K(\sigma)$ is the length of the shortest description of σ. The value of $K(\sigma)$ is independent of the choice of U, up to an additive constant independent of σ. It is easy to see that the function K can be computably approximated from above. Let $K_s(\sigma)$ be the stage s approximation to $K(\sigma)$. For $n \in \mathbb{N}$, let $K(n) = K(0^n)$. See [15] for more on Kolmogorov complexity, and see [4] for a discussion of why we use prefix-free Kolmogorov complexity (rather than the earlier notion of plain Kolmogorov complexity) to obtain an alternate characterization of 1-randomness.

Theorem 1.4 (Schnorr, see Chaitin [1]). *A set A is 1-random iff there is a constant d such that $K(A \restriction n) > n - d$ for all n.*

Let $\mathbf{R}_d^X = \{\sigma : K^X(\sigma) \leqslant |\sigma| - d\}$, where K^X is prefix-free Kolmogorov complexity relativized to X in the natural way. It is not hard to check that $(\mathbf{R}_d^X)_{d\in\mathbb{N}}$ is an ML-test relative to X. Theorem 1.4 says that $(\mathbf{R}_d^X)_{d\in\mathbb{N}}$ is a *universal* ML-test relative to X, in the sense that Z is 1-random relative to X iff $Z \notin \bigcap_d \mathbf{R}_d^X$. We write $\mathbf{R}_d$ for $\mathbf{R}_d^\emptyset$.

A third approach to the definition of randomness is through the unpredictability paradigm, using betting strategies known as martingales. The idea here is that one should not be able to make much money betting on the successive bits of a random set.

Definition 1.5. A *martingale* is a function $M : 2^{<\omega} \to \mathbb{R}^+ \cup \{0\}$ such that $M(\sigma) = \frac{1}{2}(M(\sigma 0) + M(\sigma 1))$ for all σ. It will be convenient to assume that if M is a martingale then $M(\lambda) \leqslant 1$, where λ is the empty string. A martingale M *succeeds* on A if $\limsup_n M(A \restriction n) = \infty$.

A martingale M is *computably enumerable* if the reals $M(\sigma)$ are uniformly c.e. and *computable* if the reals $M(\sigma)$ are uniformly computable. (Here a real is *c.e.* if its left cut is a c.e. set, or, equivalently, if it is approximable from below by a computable sequence of rationals.)

Theorem 1.6 (Schnorr [25]). *A set A is 1-random iff no c.e. martingale succeeds on A.*

We note for future reference that there is a universal c.e. martingale, that is, a c.e. martingale M that succeeds on a set Z iff Z is not 1-random: For $\sigma \in 2^{<\omega}$, let $M(\sigma)$ be the sum of all $2^{|\tau|-K(\tau)}$ where τ is a proper prefix of σ, plus the sum of all $2^{|\sigma|-K(\tau)}$ where σ is a prefix of τ. We can approximate M by the computable martingales M_s, where the sum is taken over all τ of length $\leqslant s$, and we use $K_s(\tau)$ in place of $K(\tau)$. It is not hard to check that $M(\sigma) = \sup_s M_s(\sigma)$ is a universal c.e. martingale.

Given Theorem 1.6, it is natural to consider the effect of replacing c.e. martingales by computable martingales, which leads to the following randomness notion.

Definition 1.7 (Schnorr [25]). A set A is *computably random* if no computable martingale succeeds on A.

Of course, all of the above notions can be relativized to a given set A, yielding definitions of 1-randomness relative to A, computable randomness relative to A, and so forth. For example, we can define a martingale M to be A-computable if the reals $M(\sigma)$ are uniformly computable using A as an oracle, and then define a set B to be computably random relative to A if no A-computable martingale succeeds on B.

One of the most interesting phenomena to arise from recent work on relative algorithmic randomness is an increased understanding of the importance of the class of K-trivial sets, first studied by Chaitin [2] and Solovay [29]. These sets are the ones that have the lowest possible initial segment prefix-free Kolmogorov complexity (up to an additive constant).

Definition 1.8. A set A is *K-trivial* if there is a constant d such that $K(A \upharpoonright n) \leqslant K(n) + d$ for all n.

Relative randomness can also be used to define classes of sets that are computationally weak. For example, for a relativizable randomness notion $\mathcal{R}$, a set A is *low for $\mathcal{R}$ randomness* if every $\mathcal{R}$ random set is $\mathcal{R}$ random relative to A. In 1998, Muchnik defined the class of *low for K* sets, which are those sets A that cannot be used to reduce the prefix-free complexity of any string; that is, there is a constant c such that $\forall \sigma\, [K^A(\sigma) \geqslant K(\sigma) - c]$. It is easy to see that if a set is low for K then it is both K-trivial and low for 1-randomness. Two of the main results in [20] are that every set that is low for 1-randomness is K-trivial and that every K-trivial set is low for K. (For another proof of the first result, see Corollary 3.1 below.) Thus all three classes coincide.

Kučera [9] and Gács [6] showed that every set is computable in some 1-random set. Thus, if 1-randomness implies $\mathcal{R}$ randomness, then every set that is low for

$\mathcal{R}$ randomness is a base for $\mathcal{R}$ randomness. In Theorem 2.1 below, we show that for 1-randomness the converse also holds. That is, every base for 1-randomness is K-trivial and hence low for 1-randomness. This result gives yet another characterization of this natural class of sets that are randomness-theoretically weak. As we discuss below, the situation is quite different for computable randomness.

We note that the proof of Theorem 2.1 can also be modified to show directly that every base for 1-randomness is low for K (see [21]).

The Kučera-Gács Theorem shows that Theorem 1.1 cannot be effectivized, in the sense that $\{Z : Z \geqslant_{\mathrm{T}} A\}$ is never ML-null. However, we might still hope that $\{Z : Z \geqslant_{\mathrm{T}} A\}$ is small in the sense of being ML-null relative to A. It follows from Theorem 2.1 that this is the case iff A is not K-trivial. Thus the K-trivial sets are the ones that are close to being computable, in the sense that many sets compute them. This and other consequences of Theorem 2.1 are discussed in Section 3. Section 4 deals with issues of uniformity in some of these results.

Our characterization of the bases for 1-randomness has already found a surprising application in a different area of computability theory. A *Scott set* is a Turing ideal (i.e., a collection of sets closed downwards under Turing reducibility and closed under joins) $\mathcal{S}$ such that for each infinite binary tree $T \in \mathcal{S}$, there is an infinite path of T in $\mathcal{S}$. Scott sets occur naturally in various contexts, such as the study of models of arithmetic and reverse mathematics. H. Friedman and McAllister independently asked the following question: if $\mathcal{S}$ is a Scott set and $X \in \mathcal{S}$ is not computable, does there necessarily exist a $Y \in \mathcal{S}$ such that $X \mid_{\mathrm{T}} Y$? Kučera and Slaman [10] have recently given a positive answer to this question using Theorem 2.1.

In Section 5, we study bases for computable randomness, and connect them with diagonally noncomputable sets and PA-degrees.

A set A is *diagonally noncomputable* if there is a total function $f \leqslant_{\mathrm{T}} A$ such that $f(n) \neq \Phi_n(n)$ for all n, where Φ_n is the nth partial computable function. A set A has *PA-degree* if it computes a completion of Peano Arithmetic.

We show that the bases for computable randomness include every Δ^0_2 set that is not diagonally noncomputable, but no set of PA-degree. As a consequence, we conclude that an n-c.e. set is a base for computable randomness iff it is Turing incomplete. Nies [20] has shown that the only sets that are low for computable randomness are the computable ones, so the situation here is quite different from the 1-randomness case.

We finish this section with two important tools we will use below, the Kraft-Chaitin Theorem[2] and a strong form of the Kučera-Gács Theorem mentioned above.

[2]We retain the usual terminology "Kraft-Chaitin" for this theorem, which appears in Chaitin [1], and certain associated concepts, but note that it appeared earlier in Levin's dissertation [14].

A *Kraft-Chaitin set* (KC-set) is a c.e. set of pairs $\{\langle d_i, \tau_i\rangle : i \in \mathbb{N}\}$ (which we call *axioms*), with $d_i \in \mathbb{N}$ and $\tau_i \in 2^{<\omega}$, such that $\sum_i 2^{-d_i} \leqslant 1$. We say that 2^{-d_i} is the *weight* of the axiom $\langle d_i, \tau_i\rangle$.

Theorem 1.9 (Kraft-Chaitin Theorem; Levin [14]). *Let $S = \{\langle d_i, \tau_i\rangle : i \in \mathbb{N}\}$ be a Kraft-Chaitin set. Then there is a constant c, which can be obtained effectively from an index for S, such that $K(\tau_i) \leqslant d_i + c$ for all i.*

Theorem 1.10 (Kučera-Gács Theorem [6], [9]). *Let $c \in \mathbb{N}$. There is a functional Θ such that for each A there is a $Z \notin \mathbf{R}_c$ for which $\Theta^Z = A$ with use function bounded by $2n$.*

See Merkle and Mihailović [17] for a proof of this result (and an improvement of the bound on the use of Θ).

2 K-triviality and Bases for 1-randomness

As discussed above, every K-trivial set is a base for 1-randomness. We now prove the converse. As we show in Corollary 3.2, this result implies that the K-trivial sets are exactly those sets A that are too weak to compute a null set containing $\{Z : Z \geqslant_{\mathrm{T}} A\}$.

Theorem 2.1. *Every base for 1-randomness is K-trivial.*

Proof. Suppose that A is a base for 1-randomness, that is, there are a Z and a Φ such that $\Phi^Z = A$ and Z is 1-random relative to A. We will enumerate a Kraft-Chaitin set L_d for each $d \in \mathbb{N}$. We want to ensure that there is a d such that L_d contains an axiom $\langle K(|\tau|) + d + 2, \tau\rangle$ for each $\tau \prec A$. The idea is to build sets $C_d^\tau \subseteq 2^\omega$ for $d \in \mathbb{N}$ and $\tau \in 2^{<\omega}$ with the following properties.

- The C_d^τ are uniformly c.e.
- For each fixed d, the C_d^τ are pairwise disjoint.
- If we let $U_d = \bigcup_{\tau \prec A} C_d^\tau$, then the following hold.
  - $(U_d)_{d\in\mathbb{N}}$ is a Martin-Löf test relative to A.
  - If $Z \notin U_d$ then $\mu(C_d^\tau) = 2^{-K(|\tau|)-d}$ for all $\tau \prec A$.

We then define L_d by enumerating an axiom $\langle K_s(|\tau|)+d+2, \tau\rangle$ at stage s whenever we have not previously enumerated such an axiom and $\mu(C_d^\tau[s]) \geqslant 2^{-K_s(|\tau|)-d-1}$. Since the C_d^τ are pairwise disjoint, this is a KC-set. Since Z is 1-random relative to A, we have $Z \notin U_d$ for some d and hence $\mu(C_d^\tau) = 2^{-K(|\tau|)-d}$ for all $\tau \prec A$, which implies that $\langle K(|\tau|) + d + 2, \tau\rangle \in L_d$ for all $\tau \prec A$, as desired.

To build the C_d^τ, as long as $\mu(C_d^\tau) < 2^{-K_s(|\tau|)-d}$, we look for strings σ such that $\tau \preccurlyeq \Phi^\sigma$ and $\mu(C_d^\tau) + 2^{-|\sigma|} \leqslant 2^{-K_s(|\tau|)-d}$, and put $[\sigma]$ into C_d^τ. To keep our sets pairwise disjoint, we then ensure that no $[\sigma']$ such that σ' is compatible with σ is later put into any C_d^ν. If $Z \notin U_d$, then no $[\sigma]$ with $\sigma \prec Z$ is ever put into any C_d^τ, which means that the measure of each C_d^τ with $\tau \prec A = \Phi^Z$ must eventually exceed $2^{-K(|\tau|)-d-1}$.

We now give the formal details of the construction. For each $d \in \mathbb{N}$, we have a separate procedure, which acts as follows. Initially, all strings are *unused*. Each stage s has 2^s many substages, one for each σ with $|\sigma| = s$. Let $C_{d,\sigma}^\tau$ denote the approximation to C_d^τ at the beginning of the substage corresponding to σ. For each σ with $|\sigma| = s$ in turn, if σ is not used and $\Phi^\sigma[s]\downarrow$, then look for the shortest $\tau \preccurlyeq \Phi^\sigma[s]$ such that $\mu(C_{d,\sigma}^\tau) + 2^{-s} \leqslant 2^{-K_s(|\tau|)-d}$. If there is such a τ, then put $[\sigma]$ in C_d^τ and declare every extension of σ to be *used*.

Note that, for a fixed d, the C_d^τ are pairwise disjoint, as we only enumerate unused strings of length s at stage s.

Let $C_d = \bigcup_{\tau \prec A} C_d^\tau$. The sets C_d are uniformly A-c.e., and

$$\mu(C_d) = \sum_{\tau \prec A} \mu(C_d^\tau) \leqslant \sum_{\tau \prec A} 2^{-K(|\tau|)-d} < 2^{-d},$$

so $(C_d)_{d \in \mathbb{N}}$ is a Martin-Löf test relative to A. Since Z is 1-random relative to A, there must be a d such that $Z \notin C_d$.

We claim that for such a d we have $\mu(C_d^\tau) = 2^{-K(|\tau|)-d}$ for all $\tau \prec A$. To establish this claim, suppose that $\mu(C_d^\tau) < 2^{-K(|\tau|)-d}$ for some $\tau \prec A$. Let s be a stage such that

- $K(|\tau|) = K_s(|\tau|)$,
- $\mu(C_d^\tau) + 2^{-s} \leqslant 2^{-K(|\tau|)-d}$, and
- $\Phi^Z \upharpoonright (|\tau| + 1)[s]\downarrow$.

Then $[Z \upharpoonright (s+1)]$ must enter C_d^τ at the substage corresponding to $Z \upharpoonright (s+1)$ unless it enters some other $C_d^{\tau'}$ or is already used. In any case, there is a ν and an n such that $[Z \upharpoonright n]$ is in C_d^ν. But then we must have $\nu \preccurlyeq \Phi^{Z \upharpoonright n} \prec \Phi^Z = A$, so $[Z \upharpoonright n]$ is in C_d, and hence $Z \in C_d$, contrary to our choice of d. This establishes the claim.

We now build the KC-sets L_d as described above. To build L_d, we enumerate an axiom $\langle K_s(|\tau|) + d + 2, \tau \rangle$ at stage s whenever we have not previously enumerated this axiom and $\mu(C_d^\tau[s]) \geqslant 2^{-K_s(|\tau|)-d-1}$. For a fixed τ, there is at most one axiom per length, so all axioms $\langle r, \tau \rangle$ together contribute at most twice the weight of the one with smallest r. Thus the total weight of our axioms is bounded by $\sum_\tau \mu(C_d^\tau)$, which is less than or equal to 1, since the C_d^τ are pairwise disjoint. If d is such that $Z \notin C_d$, then $\mu(C_d^\tau) = 2^{-K(|\tau|)-d}$ for all $\tau \prec A$, so we eventually enumerate $\langle K(|\tau|) + d + 2, \tau \rangle$ into L_d. This shows that A is K-trivial. $\square$

3 Further connections between K-triviality and 1-randomness

We now discuss consequences of our main result, and give conditions under which we can replace 1-randomness relative to A by unrelativized 1-randomness. More precisely, we show that if A is c.e., $Z \geqslant_{\mathrm{T}} A$, and $Z \not\geqslant_{\mathrm{T}} \emptyset'$, then to ensure that A is K-trivial it is enough to assume that Z is 1-random. We also include two open questions related to our main result, both of which have been the subject of intense recent research.

The following corollary to Theorem 2.1 was first proved by different means in [20]. The more complex proof there is via martingales, and yields the stronger result that a set A is K-trivial if each 1-random set is computably random relative to A.

Corollary 3.1. *Every set that is low for* 1*-randomness is* K*-trivial.*

Proof. Let A be low for 1-randomness. By the Kučera-Gács Theorem, there is a 1-random $Z \geqslant_{\mathrm{T}} A$. Since Z is also 1-random relative to A, it follows that A is a base for 1-randomness, and hence K-trivial. $\square$

Since there is a universal ML-test, a set A is a base for 1-randomness iff $\{Z : A \leqslant_{\mathrm{T}} Z\}$ is not ML-null relative to A. So we have the following consequence of Theorem 2.1.

Corollary 3.2. *A set A is not K-trivial iff $\{Z : A \leqslant_{T} Z\}$ is ML-null relative to A.*

As a byproduct of the method of the proof of Theorem 2.1, we obtain another, related characterization of the K-trivial sets, which also says that a Turing functional can almost be viewed as a special kind of oracle Martin-Löf test.

Proposition 3.3. *A set A is not K-trivial iff for each Turing functional Φ, there is an oracle ML-test $(C_d^X)_{d\in\mathbb{N}}$ such that $\{Z : A = \Phi^Z\} = \bigcap_d C_d^A$.*

Proof. If A is K-trivial then there are a Φ and a Z such that $\Phi^Z = A$ and Z is 1-random relative to A. (Indeed, by the Kučera-Gács Theorem, there is a single Φ that works for all K-trivial sets.) So $\{X : A = \Phi^X\}$ is not ML-null relative to A.

Now suppose that A is not K-trivial. For a given functional Φ, define the sets C_d^τ as in the proof of Theorem 2.1, but with the minor change that for each d

only C_d^τ with $|\tau| \geqslant d$ are built. Let $C_d^X = \bigcup_{\tau \prec X,\ |\tau| \geqslant d} C_d^\tau$. Then, as shown in the proof of Theorem 2.1, $(C_d^X)_{d\in\mathbb{N}}$ is an oracle ML-test, and, since A is not K-trivial, $\{Z : A = \Phi^Z\} \subseteq \bigcap_d C_d^A$. But if $\Phi^Z \neq A$ then there is a d such that $A \upharpoonright d \not\prec \Phi^Z$, and hence $Z \notin C_d^A$. So $\{Z : A = \Phi^Z\} = \bigcap_d C_d^A$. □

If $A \oplus B$ is 1-random then we would intuitively expect that A and B share very little common information. Indeed, van Lambalgen [11] showed that in this case A and B are 1-random relative to each other. On the other hand, Kučera [9] proved that no two Δ^0_2 1-random (or even diagonally noncomputable) sets form a minimal pair. However, using Theorem 2.1, we can show that our intuition is essentially correct, in the following sense.

Corollary 3.4. *If $A \oplus B$ is 1-random, then any $X \leqslant_T A, B$ is K-trivial.*

Proof. As mentioned above, A is 1-random relative to B, and hence relative to X. So X is a base for 1-randomness, and thus is K-trivial. □

We next wish to establish a corollary relating the notions of K-triviality and unrelativized 1-randomness. We first prove a lemma saying that if A is c.e., and a 1-random set Z is not too complex, then Z is 1-random relative to A.

Lemma 3.5. *Let A be c.e., and let Z be 1-random and such that $\emptyset' \nleqslant_T A \oplus Z$. Then Z is 1-random relative to A.*

Proof. Suppose Z is not 1-random relative to A. Thus $Z \in \bigcap_d \mathbf{R}_d^A$.

The idea of the proof is the following. Since $A \oplus Z \ngeqslant_{\mathrm{T}} \emptyset'$, infinitely many x enter $\emptyset'$ after (some initial segment of) Z enters $\mathbf{R}_x^A$, with A correct on the use. This allows us to convert $(\mathbf{R}_d^A)_{d\in\mathbb{N}}$ into an unrelativized ML-test for Z.

We now give the details. Let $\mathbf{R}_d^A[s] = \mathbf{R}_{d,s}^{A_s}$ be the approximation at stage s of the dth set in the universal ML-test with oracle A_s. We may assume that $\mu(\mathbf{R}_d^A[s]) \leqslant 2^{-d}$ for all s. Each enumeration of a string σ into $\mathbf{R}_d^Y$ corresponds to a convergent computation with oracle Y, and hence has an associated use on this oracle. The following function is computable in $A \oplus Z$:

$$f(x) = \mu s\, \exists k\, [Z \upharpoonright k \in \mathbf{R}_x^A[s] \text{ with use } u \,\wedge\, A_s \upharpoonright u = A \upharpoonright u].$$

If k and s are as in the definition of $f(x)$, then, because $A_s \upharpoonright u$ is stable, $Z \upharpoonright k \in \mathbf{R}_x^A[t]$ for all $t \geqslant s$. (Here we need that A is c.e., not merely Δ^0_2.) Let $m(x) \simeq \mu s\, [x \in \emptyset'_s]$ (i.e., $m(x)$ is defined only if the right side is). Then $\exists^\infty x \in \emptyset'\, [m(x) \geqslant f(x)]$, since otherwise we could compute $\emptyset'$ from $A \oplus Z$ because, for almost all x, we would have $x \in \emptyset' \Leftrightarrow x \in \emptyset'_{f(x)}$.

Let

$$S_d = \bigcup_{x>d,\ x\in\emptyset'} \mathbf{R}_x^A[m(x)].$$

Then the sequence $(S_d)_{d\in\mathbb{N}}$ is uniformly c.e., and $\mu(S_d) \leqslant 2^{-d}$. Moreover, $Z \in \bigcap_d S_d$, because $m(x) \geqslant f(x)$ for infinitely many x. Since Z is 1-random, this is a contradiction. □

Corollary 3.6. *Suppose A is c.e. and Z is a 1-random set such that $A \leqslant_T Z$ and $\emptyset' \nleqslant_T Z$. Then A is K-trivial.*

Proof. Suppose $Z \geqslant_{\mathrm{T}} A$ is 1-random. If A is not K-trivial, then by Theorem 2.1, Z is not 1-random relative to A. So, by Lemma 3.5, $\emptyset' \leqslant_{\mathrm{T}} A \oplus Z \equiv_{\mathrm{T}} Z$. □

Stephan [30] showed that if Z is a 1-random set such that $\emptyset' \nleqslant_{\mathrm{T}} Z$, then Z does not have PA-degree. Corollary 3.6 is further evidence that the 1-random sets not above $\emptyset'$ are computationally weak, and hence very different from the 1-random sets above $\emptyset'$.

We do not know at present whether Corollary 3.6 is in fact a characterization of K-triviality for c.e. sets. This is Question 4.6 in [18].

Question 3.7. If A is K-trivial, must there be a 1-random $Z \geqslant_{\mathrm{T}} A$ such that $\emptyset' \nleqslant_{\mathrm{T}} Z$?

It would not alter the question to restrict attention to c.e. K-trivial sets, since Nies [20] showed that every K-trivial set is computable in some c.e. K-trivial set.

Recall that the proof of Corollary 3.6 can be adapted to show that A is low for K. Thus an affirmative answer to Question 3.7 would also give a new proof of the result in [20] that every K-trivial set is low for K.

Remark 3.8. Corollary 3.6 can also be proved directly, by combining the proofs of Theorem 2.1 and Lemma 3.5. Suppose that A is c.e. and not K-trivial, $\Phi^Z = A$, and $\emptyset' \nleqslant_{\mathrm{T}} Z$. We will show that Z is not 1-random by building an ML-test $(E_i)_{i\in\mathbb{N}}$ such that $Z \in \bigcap_i E_i$.

Define C_d^τ as in the proof of Theorem 2.1. For each d, the KC-set L_d fails to show that A is K-trivial, so we must have $\mu(C_d^\tau) < 2^{-K_s(|\tau|)-d}$ for some $\tau \prec A$. So after $K_s(|\tau|)$ has settled, C_d^τ keeps requesting strings. Thus for each d there is an n such that $Z \upharpoonright n \in C_d^\tau$ for some $\tau \prec A$. Now let $g(d)$ be the least stage s such that $Z \upharpoonright n$ is in $C_{d,s}^\tau$ for some n and τ with $\tau \prec A$ and $\tau \prec A_s$.

The function g is computable in Z, so if we let m be as in the proof of Lemma 3.5, then there are infinitely many d such that $m(d) > g(d)$. Now define

$$E_i = \bigcup_{d>i,\ d\in\emptyset'} \ \bigcup_{\tau\prec A_{m(d)}} C_{d,m(d)}^\tau.$$

Then the sets E_i are uniformly c.e. and $\mu(E_i) \leqslant \sum_{d>i} 2^{-d} = 2^{-i}$, so $(E_i)_{i\in\mathbb{N}}$ is an ML-test. Furthermore, for each i there is a $d > i$ such that $m(d) > g(d)$. For such a d, there is an n such that $Z \upharpoonright n$ is in C_d^τ for some $\tau \prec A_{m(d)}$, so $Z \upharpoonright n$ is in E_i. Thus $Z \in \bigcap_i E_i$, and hence Z is not 1-random.

We finish this section with an application of Theorem 2.1 noted by Kučera. Let us say that A is *weakly ML-cuppable* if $A \oplus Z \geqslant_{\mathrm{T}} \emptyset'$ for some 1-random $Z \ngeqslant_{\mathrm{T}} \emptyset'$, and that A is *ML-cuppable* if one can choose $Z <_{\mathrm{T}} \emptyset'$.

Question 3.9 (Kučera, see [18]). Which Δ^0_2 sets are (weakly) ML-cuppable? Is one of the notions equivalent to not being K-trivial?

Fix a prefix-free oracle machine U such that U^A is universal for all oracles A, and let Ω^A be the halting probability of U^A, that is, $\sum_{U^A(\sigma)\downarrow} 2^{-|\sigma|}$. (For more on such Omega operators, see [5].)

If $A \leqslant_{\mathrm{T}} \emptyset'$ is not K-trivial, then $\Omega^A \ngeqslant_{\mathrm{T}} \emptyset'$ by Theorem 2.1. Since $\emptyset' \leqslant_{\mathrm{T}} A' \equiv_{\mathrm{T}} A \oplus \Omega^A$, it follows that A is ML-cuppable. If A is low then in fact $\Omega^A <_{\mathrm{T}} \emptyset'$, so every Δ^0_2 set that computes a low non-K-trivial set is ML-cuppable. Such sets include: (1) any Δ^0_2 1-random set A, since $A \cap 2\mathbb{N}$ is low [5, Thm. 3.4]; (2) any non-low$_2$ or c.e.a. set, as each such set is the supremum of a pair of 1-generic sets (see [13, Ex. IV.3.15] for the first case); (3) any c.e. non-K-trivial set A, because A is a disjoint union of c.e. low sets A_0, A_1, and at least one of these is not K-trivial.

Nies has shown that there is a (necessarily K-trivial) noncomputable c.e. set that is not weakly ML-cuppable.

4 Uniformity

It is not hard to see that the proof of Theorem 2.1 is uniform, in the sense that if Z is 1-random and $\Phi^Z = A$, then a constant b such that A is K-trivial via b can be obtained effectively from an index for Φ and a constant c such that $Z \notin \mathbf{R}_c$. On the other hand, Corollary 3.6 is necessarily nonuniform. It is not hard to see why the particular construction in Remark 3.8 is nonuniform. From a c such that $Z \notin \mathbf{R}_c$, one can compute an i such that $Z \notin E_i$, but that is not enough, since we would now need $\emptyset'$ to determine which KC-set L_d shows that A is not K-trivial, namely the one where $d > i$ is least such that $m(d) > g(d)$. The following proposition shows that this nonuniformity cannot be avoided. In fact, even if Z is low and we are also given a lowness index for Z, we cannot effectively determine a constant for the K-triviality of A.

Proposition 4.1. *There is no computable function $f(c, e, i, p)$ such that, if $A = W_e = \Phi^Z_i$, where $Z' = \Phi^{\emptyset'}_p$, and $Z \notin \mathbf{R}_c$, then A is K-trivial via $b = f(c, e, i, p)$.*

Proof. Let $f(c, e, i, p)$ be computable. Fix $c \in \mathbb{N}$. We effectively build a c.e. set A (which will in fact be finite) and reductions Φ and Ψ such that there is a $Z \notin \mathbf{R}_c$ with $\Phi^Z = A$ and $\Psi^{\emptyset'} = Z'$. By the Recursion Theorem, we may assume we know indices e, i and p such that $A = W_e = \Phi^Z_i$ and $\Phi^{\emptyset'}_p = Z'$. We will ensure that A is not K-trivial via $b = f(c, e, i, p)$.

(In more detail, we use Smullyan's extension of the Recursion Theorem (see [28]), with parameter c and three arguments e, i, p. We build a c.e. set $A = W_{f(e,i,p)}$, and Turing functionals $\Phi_{g(e,i,p)}$ and $\Phi_{h(e,i,p)}$ such that $\Phi^{\emptyset'}_{h(e,i,p)}$ is of the form Z' where $\Phi^{Z}_{g(e,i,p)} = A$. By Smullyan's Theorem, we may assume that $A = W_i$, that $\Phi_{g(e,i,p)} = \Phi_e$ and that $\Phi_{h(e,i,p)} = \Phi_p$, where the latter equalities hold for all oracles.)

There is a constant d such that $K(2^m) \leqslant 2\log m + d$ for all m. Let N be of the form 2^m and such that $N > 2^{2\log\log N + d + b + 1}$. We build A by putting a number less than N into A at stage s whenever $K_s(A_s \upharpoonright N) \leqslant 2\log\log N + d + b$. Since there are fewer than N many strings σ of length N such that $K(\sigma) \leqslant 2\log\log N + d + b$, this procedure ensures that $K(A \upharpoonright N) > 2\log\log N + d + b \geqslant K(N) + b$. Thus A is not K-trivial via b.

The idea now is to find a string σ of length $2N$ such that $[\sigma] \nsubseteq \mathbf{R}_c$ and σ computes $A \upharpoonright N$ via the functional Θ from the Kučera-Gács Theorem (Theorem 1.10). We then extend σ to a low set Z by applying the Low Basis Theorem [8].

In more detail, since $\emptyset'$ can compute $K(\tau)$ for every τ, there is a $\emptyset'$-computable procedure $\Gamma^{\emptyset'}$ for determining a σ of length $2N$ such that $[\sigma] \nsubseteq \mathbf{R}_c$ and $\Theta^{\sigma} \upharpoonright N = A \upharpoonright N$, where N is as above (so that $A \subseteq [0, N)$).

Since the complement of $\mathbf{R}_c$ is a Π^0_1 class, the Low Basis Theorem implies that given a string τ, we can effectively find an index l_τ such that if $[\tau] \nsubseteq \mathbf{R}_c$ then $\Phi^{\emptyset'}_{l}$ is the jump of a low set $Z \notin \mathbf{R}_c$ such that $\tau \prec Z$.

Now we define Ψ^X as follows: Run Γ^X until it returns a string τ of length $2N$. If that happens, then determine l_τ as above and simulate $\Phi^X_{l_\tau}$.

Then $\Psi^{\emptyset'} = \Phi^{\emptyset'}_{l_\sigma}$ is the jump of a low set $Z \notin \mathbf{R}_c$ such that $\sigma \prec Z$.

Finally, define the reduction Φ as follows: $\Phi^X(k) = \Theta^X(k)$ if $k < N$, and $\Phi^X(k) = 0$ otherwise. Then $\Phi^Z \upharpoonright N = \Theta^Z \upharpoonright N = \Theta^\sigma \upharpoonright N = A \upharpoonright N$. Since $A \subseteq [0, N)$, this means that $\Phi^Z = A$. $\square$

5 Bases for computable randomness

In this section, we show that the bases for computable randomness include every Δ^0_2 set that is not diagonally noncomputable, but no set of PA degree. As a consequence, we conclude that an n-c.e. set is a base for computable randomness iff it is Turing incomplete. We begin with a couple of lemmas that will be useful below.

Lemma 5.1. *If $B' \geqslant_T A''$ and $B \geqslant_T A$, then there is a B-computable martingale M^B that dominates all A-computable martingales, in the sense that, for each A-computable martingale D, there is a k such that $kM^B(\sigma) > D(\sigma)$ for all σ.*

Proof. It is enough to produce a uniformly B-computable sequence of martingales $M^B_0, M^B_1, \ldots$ containing all A-computable martingales, since we can then let $M^B =$

$\sum_n 2^{-n-1} M_n^B$. (Recall that we are assuming that $M(\lambda) \leqslant 1$ for every martingale M.)

To obtain such a list, we begin with an effective list $\Psi_0^A, \Psi_1^A, \dots$ of all partial A-computable martingales and use the fact that, since $B' \geqslant_{\mathrm{T}} A''$, there is a B-computable function f that dominates all A-computable functions. Let $g_0, g_1, \dots$ be a uniformly B-computable sequence consisting of all functions that are eventually equal to f (that is, $\exists n \, \forall m > n \, [f(m) = g_e(m)]$). Note that each A-computable function is majorized by some g_e.

For $n = \langle i, e \rangle$, define M_n^B as follows. If $\Psi_i^A(\lambda)[g_e(0)] \downarrow$, then let $M_n^B(\lambda) = \Psi_i^A(\lambda)$. Otherwise, let $M_n^B(\sigma) = 1$ for all σ. If $M_n^B(\sigma)$ has been defined and $M_n^B(\sigma 0)$ and $M_n^B(\sigma 1)$ have not yet been defined, then define them as follows. If $\Psi_i^A(\sigma j)[g_e(|\sigma| + 1)] \downarrow$ for $j = 0, 1$, then let $M_n^B(\sigma j) = \Psi_i^A(\sigma j)$ for $j = 0, 1$. Otherwise, let $M_n^B(\tau) = M_n^B(\sigma)$ for all $\tau \succ \sigma$.

It is easy to see that the M_n^B are uniformly B-computable martingales. Furthermore, if Ψ_i^A is total then there is an e such that $\Psi_i^A(\sigma)[g_e(|\sigma|)] \downarrow$ for all σ. For $n = \langle i, e \rangle$, we have $M_n^B = \Psi_i^A$. $\square$

Recall that G is 1-*generic relative to* A if for every A-c.e. $S \subseteq 2^{<\omega}$ there is a $\sigma \prec G$ such that either $\sigma \in S$ or S contains no extension of σ.

Lemma 5.2. *If A is not diagonally noncomputable and G is 1-generic relative to A, then $A \oplus G$ is not diagonally noncomputable.*

Proof. Let $e \in \mathbb{N}$ be such that $\Phi_e^{A \oplus G}$ is total. We need to show that there is an n such that $\Phi_e^{A \oplus G}(n) \downarrow = \Phi_n(n) \downarrow$.

Let $S = \{\tau \in 2^{<\omega} : \exists n \, [\Phi_e^{A \oplus \tau}(n) \downarrow = \Phi_n(n) \downarrow]\}$. If S contains an initial segment of G then $\Phi_e^{A \oplus G}(n) \downarrow = \Phi_n(n) \downarrow$ for some n. Otherwise, since S is c.e. relative to A, there is a $\sigma \prec G$ such that S contains no extension of σ. Since $\Phi_e^{A \oplus G}$ is total, for each n we can A-computably find a $\tau_n \succ \sigma$ such that $\Phi_e^{A \oplus \tau_n}(n) \downarrow$. Since $\tau_n \notin S$, we have $\Phi_e^{A \oplus \tau_n}(n) \neq \Phi_n(n)$. So the function f defined by $f(n) = \Phi_e^{A \oplus \tau_n}(n)$ is a total A-computable function such that $f(n) \neq \Phi_n(n)$ for all n, which contradicts the assumption that A is not diagonally noncomputable. $\square$

We are now ready to show that every Δ_2^0 set that is not diagonally noncomputable is a base for computable randomness.

Theorem 5.3. *If $A \leqslant_{\mathrm{T}} \emptyset'$ is not diagonally noncomputable, then A is a base for computable randomness, and indeed there is a $Z \geqslant_{\mathrm{T}} A$ such that $Z \ngeqslant_{\mathrm{T}} \emptyset'$ and Z is computably random relative to A.*

Proof. Let $A \leqslant_{\mathrm{T}} \emptyset'$ be not diagonally noncomputable. Then $A <_{\mathrm{T}} \emptyset'$. The relativized form of the Shoenfield Jump Inversion Theorem [26] (see also [13, 22, 23]) allows us to obtain sets B and G such that

- G is 1-generic relative to A,
- $B = A \oplus G$, and
- $B' \equiv_{\mathrm{T}} A''$.

Since G is 1-generic relative to A and $\emptyset'$ is c.e. but not computable in A, we also have that $B \not\geqslant_{\mathrm{T}} \emptyset'$ (see Proposition XI.2.3 in [23]). We will build a set Z that is computably random relative to A and such that $A \leqslant_{\mathrm{T}} Z \leqslant_{\mathrm{T}} B$.

Since $B' \equiv_{\mathrm{T}} A''$, there is a B-computable martingale M^B that dominates all A-computable martingales, in the sense of Lemma 5.1.

There is a computable ascending sequence $0 = k_0 < k_1 < \cdots$ such that for every $i > 0$ and every σ of length k_{i-1}, there are at least 2 extensions $\tau \succ \sigma$ of length k_i such that $M^B(\tau) < M^B(\sigma) + 2^{-i}$ (see Merkle and Mihailović [17]).

We define $\sigma_0 \prec \sigma_1 \prec \cdots$ with $|\sigma_i| = k_i$ by recursion, using the oracle B. We then let $Z = \bigcup_i \sigma_i$. Let c_A be the convergence modulus of A as defined by Miller and Martin [19]:

$$c_A(x) = \min\{s \geqslant x : \forall y \leqslant x \, [A_s(y) = A(y)]\}.$$

Let σ_0 be the empty string. For $i > 0$, given σ_{i-1}, we can choose an extension σ_i of σ_{i-1} such that

- $|\sigma_i| = k_i$,
- $M^B(\sigma_i) < M^B(\sigma_{i-1}) + 2^{-i}$, and
- if $\Phi_i(i)[c_A(k_i)]\downarrow$ then $\sigma_i \neq \Phi_i(i)$ (where we identify binary strings with natural numbers in some effective way).

Clearly, M^B does not succeed on Z, so Z is computably random relative to A, by the choice of M^B. Furthermore, $Z \leqslant_{\mathrm{T}} B$, and therefore $Z \not\geqslant_{\mathrm{T}} \emptyset'$.

We now show that $A \leqslant_{\mathrm{T}} Z$. Note that $A \leqslant_{\mathrm{T}} Z$ iff some Z-computable function f majorizes c_A. (The reason for the if direction is that A is the only infinite branch of the Z-computable binary tree containing all σ such that for every $\tau \preccurlyeq \sigma$ there is an s with $|\tau| \leqslant s \leqslant f(|\tau|)$ and $\tau \preccurlyeq A_s$.)

The function $i \mapsto \sigma_i$ is computable in $B = A \oplus G$. By Lemma 5.2, $A \oplus G$ is not diagonally noncomputable, so there are infinitely many i such that $\Phi_i(i)\downarrow = \sigma_i$. Thus the function f defined as follows is a total Z-computable function: $f(x)$ is the least t such that there is an i with $x < k_i$ and $\Phi_i(i)[t]\downarrow = \sigma_i = Z \upharpoonright k_i$. We claim that f majorizes c_A. To show this, suppose that x is such that $f(x) < c_A(x)$, and let i be as in the definition of $f(x)$. Then $f(x) < c_A(x) \leqslant c_A(k_i)$ and $\Phi_i(i)[f(x)]\downarrow$, so we see the convergent computation $\Phi_i(i) = \tau$ at step i of the definition of Z. Hence we define σ_i to be distinct from $\Phi_i(i)[f(x)]$, contradicting the definition of f. Thus f majorizes c_A, and hence $A \leqslant_{\mathrm{T}} Z$. $\square$

A set A has *PA-degree relative to B* if it computes a completion of Peano Arithmetic with an extra unary predicate symbol R and axioms $R(\mathbf{n})$ for all $n \in B$ and $\neg R(\mathbf{n})$ for all $n \notin B$ (where $\mathbf{n}$ is the formal numeral corresponding to the natural number n). An equivalent definition (see [27]), which is the one we use below, is that every B-computable infinite binary tree has an A-computable infinite path.

In showing that no set of PA-degree is a base for computable randomness, we use the following lemma.

Lemma 5.4. *If A has PA-degree relative to B and Z is computably random relative to A, then Z is 1-random relative to B.*

Proof. Let M be a universal c.e. martingale relative to B; that is, M is c.e. and succeeds on a set Z iff Z is not 1-random relative to B. We will define an A-computable martingale N that majorizes M, in the sense that $\forall \sigma \in 2^{<\omega}\, [M(\sigma) \leqslant N(\sigma)]$.

For a martingale N, the *undergraph* $U(N)$ is $\{(\sigma, q) : \sigma \in 2^{<\omega} \wedge q \in \mathbb{Q}^+ \wedge q < N(\sigma)\}$. By definition,

$$N \leqslant_{\mathrm{T}} A \Leftrightarrow U(N) \leqslant_{\mathrm{T}} A.$$

Furthermore, $U(M)$ is c.e. in B. Fix a bijection from the natural numbers to $2^{<\omega} \times \mathbb{Q}^+$. We define the Π^0_1 class $\mathcal{C}$ relative to B of all martingales N such that $X = U(N)$ is a superset of $U(M)$. This class is given by the following conditions on X (where p, q range over $\mathbb{Q}^+$ and σ ranges over $2^{<\omega}$):

(i) $\forall p \geqslant 1\, [(\lambda, p) \notin X]$;

(ii) $\forall \sigma\, \forall p, q\, [p < q \wedge (\sigma, q) \in X \Rightarrow (\sigma, p) \in X]$;

(iii) $\forall \sigma\, \forall p, q\, [(\sigma 0, p) \in X \wedge (\sigma 1, q) \in X \Rightarrow (\sigma, \frac{p+q}{2}) \in X]$;

(iv) $\forall \sigma\, \forall p, q\, [(\sigma, \frac{p+q}{2}) \in X \Rightarrow (\sigma 0, p) \in X \vee (\sigma 1, q) \in X]$;

(v) $\forall \sigma\, \forall p\, \forall s\, [(\sigma, p) \in U(M_s) \Rightarrow (\sigma, p) \in X]$.

The class $\mathcal{C}$ is nonempty, as it contains $U(M)$. Conditions (i), (ii), and (iii) ensure that X is the undergraph of some function N with $N(\lambda) \leqslant 1$. Conditions (iii) and (iv) guarantee the equation

$$\forall \sigma \in 2^{<\omega}\, [N(\sigma) = \tfrac{1}{2}(N(\sigma 0) + N(\sigma 1))]$$

and the last condition says that $U(M) \subseteq X$, and hence implies that N majorizes M. Since $B \leqslant_{\mathrm{T}} A$ and A has PA-degree relative to B, there is an $N \leqslant_{\mathrm{T}} A$ such that $U(N)$ is a member of $\mathcal{C}$. If N does not succeed on a set Z, then M also fails to succeed on Z, and hence Z is 1-random relative to B. $\square$

Theorem 5.5. *No set of PA-degree is a base for computable randomness.*

Proof. Let A have PA-degree. By Theorem 6.5 in Simpson [27], there is a set $B \leqslant_{\mathrm{T}} A$ such that B has PA-degree and A has PA-degree relative to B. If B has PA-degree, then B is not K-trivial, since every set of PA-degree computes a 1-random set and the K-trivial sets are closed downwards under Turing reducibility [20]. On the other hand, if $Z \geqslant_{\mathrm{T}} A$ is computably random relative to A, then Z is 1-random relative to B, by Lemma 5.4, so B is K-trivial, by Theorem 2.1. Thus A is not a base for computable randomness. $\square$

Theorems 5.3 and 5.5 provide an exact characterization of the n-c.e. bases for computable randomness.

Corollary 5.6. *An n-c.e. set is a base for computable randomness iff it is Turing incomplete.*

Proof. Let A be n-c.e. If A is Turing incomplete then A is not diagonally noncomputable, by Jockusch, Lerman, Soare, and Solovay [7] (which extends Arslanov's Completeness Criterion). So, by Theorem 5.3, A is a base for computable randomness.

If A is Turing complete then A has PA-degree. So, by Theorem 5.5, A is not a base for computable randomness. $\square$

References

[1] Gregory J. Chaitin, *A theory of program size formally identical to information theory*, Journal of the Association for Computing Machinery 22 (1975), 329–340.

[2] Gregory J. Chaitin, *Algorithmic information theory*, IBM Journal of Research and Development 21 (1977), 350–359, 496.

[3] Rodney Downey and Denis R. Hirschfeldt, *Algorithmic Randomness and Complexity*, to be published by Springer-Verlag.

[4] Rodney Downey, Denis R. Hirschfeldt, André Nies, and Sebastiaan A. Terwijn, *Calibrating randomness*, The Bulletin of Symbolic Logic 12 (2006), 411–491.

[5] Rodney Downey, Denis R. Hirschfeldt, Joseph S. Miller, and André Nies, *Relativizing Chaitin's halting probability*, Journal of Mathematical Logic 5 (2005), 167–192.

[6] Péter Gács, *Every sequence is reducible to a random one*, Information and Control 70 (1986), 186–192.

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

[8] Carl G. Jockusch, Jr. and Robert I. Soare, Π^0_1 *classes and degrees of theories*, Transactions of the American Mathematical Society 173 (1972), 33–56.

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

[10] Antonín Kučera and Theodore A. Slaman, *Turing incomparability in Scott sets*, to appear in Proceedings of the American Mathematical Society.

[11] Miechiel van Lambalgen, *Random Sequences*, PhD Dissertation, University of Amsterdam, 1987.

[12] Karel de Leeuw, Edward F. Moore, Claude F. Shannon, and Norman Shapiro, *Computability by probabilistic machines*, in *Automata Studies*, Annals of Mathematics Studies 34, Princeton University Press, 1956, 183–212.

[13] Manuel Lerman, *Degrees of Unsolvability*, Perspectives in Mathematical Logic, Springer-Verlag, 1983.

[14] Leonid A. Levin, *Some Theorems on the Algorithmic Approach to Probability Theory and Information Theory*, Dissertation in Mathematics, Moscow, 1971.

[15] Ming Li and Paul Vitányi, *An Introduction to Kolmogorov Complexity and its Applications*, 2nd ed., Graduate Texts in Computer Science, Springer-Verlag, 1997.

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

[17] Wolfgang Merkle and Nenad Mihailović, *On the construction of effectively random sets*, The Journal of Symbolic Logic 69 (2004), 862–878.

[18] Joseph Miller and André Nies, *Randomness and computability: open questions*, The Bulletin Symbolic Logic 12 (2006), 390–410.

[19] Webb Miller and Donald A. Martin, *The degree of hyperimmune sets*, Zeitschrift für Mathematische Logik und Grundlagen der Mathematik 14 (1968), 159–166.

[20] André Nies, *Lowness properties and randomness*, Advances in Mathematics 197 (2005), 274–305.

[21] André Nies, *Computability and Randomness*, to appear.

[22] Piergiorgio Odifreddi, *Classical Recursion Theory, Vol. 1*, Studies in Logic and the Foundations of Mathematics 125, North-Holland, 1989.

[23] Piergiorgio Odifreddi, *Classical Recursion Theory, Vol. 2*, Studies in Logic and the Foundations of Mathematics 143, Elsevier, 1999.

[24] Gerald E. Sacks, *Degrees of Unsolvability*, Annals of Mathematics Studies 55, Princeton University Press, 1963.

[25] Claus-Peter Schnorr, *Zufälligkeit und Wahrscheinlichkeit*, Lect. Notes in Math. 218, Springer-Verlag, 1971.

[26] Joseph R. Shoenfield, *On degrees of unsolvability*, Annals of Mathematics 69 (1959), 644–653.

[27] Steven G. Simpson, *Degrees of unsolvability: a survey of results*, in *Handbook of Mathematical Logic* (J. Barwise, ed.), North-Holland, Amsterdam, 1977, 631–652.

[28] Robert I. Soare, *Recursively Enumerable Sets and Degrees*, Perspectives in Mathematical Logic, Springer-Verlag, 1987.

[29] Robert 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.

[30] Frank Stephan, *Martin-Löf random and PA-complete sets*, Logic Colloquium 2002, Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic and the Colloquium Logicum, held in Münster, Germany, August 3–11, 2002. Lecture Notes in Logic 27 (2006), 342–348.