Lowness for the Class of Random Sets

Antonín Kučera [1]
Department of Computer Science
Charles University
Malostranské náměstí 25
11800 Praha 1
Czech Republic
kucera@ktisun2.ms.mff.cuni.cz

Sebastiaan A. Terwijn [2]
Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands
terwijn@wins.uva.nl

January 2, 1998

Abstract

A positive answer to a question of M. van Lambalgen and D. Zambella whether there exist nonrecursive sets that are low for the class of random sets is obtained. Here a set A is low for the class RAND of random sets if $\mathrm{RAND} = \mathrm{RAND}^A$.

1 Introduction

The present paper is concerned with the notion of randomness as originally defined by P. Martin-Löf in [8]. A set is Martin-Löf-random, or 1-random for short, if it cannot be approximated in measure by recursive means. These sets have played a central role in the study of algorithmic randomness. One can relativize the definition of randomness to an arbitrary oracle. Relativized randomness has been studied by several authors. The intuitive meaning of "A is 1-random relative to B" is that A is independent of B. A justification for this interpretation is given by M. van Lambalgen [7]. In this introduction we review some of the basic properties of sets which are 1-random and we state the main problem. We work in the Cantor space

[1] The first author was supported by the PECO program, grant No. CIPDCT940615.
[2] This work was done during a visit of the second author to Prague in April 1997. The visit was financed by PIONIER-project PGS 22262 of the Netherlands Organization for Scientific Research (NWO).

2^ω of subsets of ω, and we denote the Lebesgue measure on 2^ω by μ. Our notation for recursion theoretic notions is standard and follows [9]. The e-th r.e. set W_e can be both interpreted as a set of numbers $W_e \subseteq \omega$ or a set of initial segments $W_e \subseteq 2^{<\omega}$. In the last case W_e defines the Σ^0_1 class $\mathrm{Ext}(W_e)$ $= \{A \in 2^\omega : (\exists \sigma \in W_e)\, [\sigma \sqsubset A]\}$. The distinction will always be clear from the context. Instead of $\mu(\mathrm{Ext}(W_e))$ we also write $\mu(W_e)$.

Definition 1.1 (Martin-Löf [8], Kautz [3]) A class $\mathcal{A}$ is $\Sigma^{0,A}_1$-*approximable* if there is an A-recursive function f such that for the $\Sigma^{0,A}_1$ classes $W^A_{f(i)}$ it holds that $\mu(W^A_{f(i)}) < 2^{-i}$ and $\mathcal{A} \subseteq \bigcap_i W^A_{f(i)}$. A set C is Martin-Löf-random relative to A, or A-1-*random* for short, if $\{C\}$ is not $\Sigma^{0,A}_1$-approximable. The class of A-1-random sets is denoted by RAND^A. If A is recursive we write RAND instead of RAND^A.

Definition 1.2 A set A is *low for* a class $\mathcal{C}$ if the relativized version $\mathcal{C}^A$ of $\mathcal{C}$ satisfies $\mathcal{C} = \mathcal{C}^A$. The class of sets that are low for $\mathcal{C}$ is denoted by $\mathrm{Low}(\mathcal{C})$.

For example, the ordinary low sets from recursion theory are the sets that are low for the class of T-complete sets, and a set is low for the class of recursive sets if and only if it is recursive. For a class $\mathcal{C}$, the class $\mathrm{Low}(\mathcal{C})$ consists of the oracles that are not 'helpful' for $\mathcal{C}$ in the sense that they do not alter $\mathcal{C}$. A set $A \in \mathrm{Low}(\mathcal{C})$ either contains no information that is useful for $\mathcal{C}$, or the information in it is coded in such a way that elements from $\mathcal{C}$ cannot retrieve it. In this paper we are interested in sets that are low for RAND.

Motivated by the work in [6], M. van Lambalgen and D. Zambella formulated the question whether there exist nontrivial examples of sets A such that every random set is already random relative to A. (The question is first explicitly stated in Zambella [11].) This question was raised in the context of a comparison between randomness properties in classical dynamic systems (specifically, Bernoulli sequences) and recursion theoretic randomness. A famous result of Kamae [2] showed that the infinite binary sequences that have no information about Bernoulli sequences (normal sequences) are precisely the sequences with zero entropy. The question was whether a similar characterization exists for sets that have no information about Martin-Löf random sequences. This motivates the question whether every element of Low(RAND) has to be recursive.

First, it is not immediately clear that there is a 1-random set that has a nonrecursive set Turing-below it in which it is 1-random. That this situation can occur was proved by Kučera in [5] by consideration of diagonally nonrecursive functions. He also proved that if a nonrecursive set A admits an A-1-random set above it (which is the case when $A \in \mathrm{Low(RAND)}$, cf. the proof of Corollary 3.2) then A is not too complex in the sense that A is generalized low (GL_1), i.e. $A \oplus \emptyset' \equiv_T A'$. In Section 2 we prove that indeed the class Low(RAND) contains nonrecursive sets, thereby answering the above question.

Next we prove some facts that will be useful later. A recursive sequence of Σ^0_1 classes such as in Definition 1.1 is called a *sequential test*. The next theorem shows that there are sequential tests that are *universal* in the sense that they cover all the sets that are covered by some sequential test.

THEOREM 1.3 (Martin-Löf [8]) *There exists a universal sequential test. That is, there is a recursive sequence of Σ^0_1 classes $\mathcal{U}_0, \mathcal{U}_1, \ldots$ such that*

- $\mathcal{U}_0 \supseteq \mathcal{U}_1 \supseteq \ldots$
- $\forall n\, (\mu(\mathcal{U}_n) < 2^{-n})$
- *for any Σ^0_1-approximable class $\mathcal{A}$ we have $\mathcal{A} \subseteq \bigcap_n \mathcal{U}_n$.*

We sketch the proof of Theorem 1.3. For every n construct an r.e. set $U_n \subseteq 2^{<\omega}$ as follows. For every $e > n$, U_n enumerates all the elements of $W_{\{e\}(e)}$ (where we take this set to be empty if $\{e\}(e)$ is undefined) as long as $\mu(W_{\{e\}(e)}) < 2^{-e}$. Define $\mathcal{U}_n = \mathrm{Ext}(U_n)$. Then $\mu(\mathcal{U}_n) < \sum_{e>n} 2^{-e} = 2^{-n}$, and if $\{e\}$ defines a sequential test then for every n there exists by padding $i \in \omega$ (in fact, infinitely many i) such that $W_{\{e\}(i)} \subseteq \mathcal{U}_n$, so $\bigcap_i W_{\{e\}(i)} \subseteq \bigcap_n \mathcal{U}_n$.

DEFINITION 1.4 For every n, denote by $\mathcal{U}_n$ the Σ^0_1 class from the above proof. Define $\mathcal{P}_n$ to be the complement of $\mathcal{U}_n$.

Define the *left shift* $T : 2^\omega \to 2^\omega$ by $T(C)(n) = C(n+1)$. Let T^k denote the k-iteration of T.

LEMMA 1.5 *For every $C \in \mathrm{RAND}$ there exists $k \in \omega$ such that $T^k(C) \in \mathcal{P}_0$.*

Proof. For a set of initial segments Σ and a class $\mathcal{A}$ define $\Sigma\hat{\ }\mathcal{A} = \{\sigma\hat{\ }A : \sigma \in \Sigma \wedge A \in \mathcal{A}\}$, where $\sigma\hat{\ }A$ denotes the concatenation of σ with the characteristic sequence of A. Fix an r.e. set U_0 that defines the Σ^0_1 class $\mathcal{U}_0$. By induction define $\mathcal{U}^1_0 = \mathcal{U}_0$ and $\mathcal{U}^{k+1}_0 = U_0\hat{\ }\mathcal{U}^k_0$.

Now by $q = \mu(\mathcal{U}_0) < 1$ there is an $l \in \omega$ such that $q^l < 1/2$, so $\mu(\mathcal{U}_0^{kl}) = q^{kl} < 2^{-k}$. It follows that the sequence

$$\mathcal{U}_0,\ \mathcal{U}_0^l,\ \mathcal{U}_0^{2l},\ \ldots$$

constitutes a sequential test. Therefore, if $C \in$ RAND then either $C \notin \mathcal{U}_0$, i.e. $C \in \mathcal{P}_0$ and we are done, or for some $k > 0$ we have $C \in \mathcal{U}_0^{kl}$ and $C \notin \mathcal{U}_0^{(k+1)l}$. But the latter means that $T^{k'}(C) \notin \mathcal{U}_0$ for some k', so $T^{k'}(C) \in \mathcal{P}_0$. $\square$

When we relativize the concept of a sequential test to an oracle A it makes no difference if we relativize the function that gives the indices of the levels of the test or not, as the following standard lemma shows.

LEMMA 1.6 *Let f be an A-recursive function. Then there is a recursive function g such that $W^A_{f(n)} = W^A_{g(n)}$ for every n.*

2 A NONRECURSIVE SET THAT IS LOW FOR THE RANDOM SETS

A set which is low for RAND is computationally weak in the sense that it cannot detect any regularity in any 1-random sequence. Clearly every recursive set is in Low(RAND). This section is devoted to a proof that also nontrivial examples of such sets exist.

THEOREM 2.1 *There exists a nonrecursive r.e. set A that is low for* RAND.

Proof. We make A simple to guarantee nonrecursiveness. That is, during the construction we want to satisfy the requirements

$$R_z : \quad W_z \text{ is infinite } \Rightarrow\ W_z \cap A \neq \emptyset.$$

By Theorem 1.3 and Lemma 1.6, let f be a recursive function that defines the universal sequential test relative to X for any set X. That is, for every i, $f(i)$ is an index of the i-th level $W^X_{f(i)}$ of the universal sequential test relative to X. So for every oracle X and every i it holds that $\mu(W^X_{f(i)}) < 2^{-i}$. Simultaneously with A we describe a program coded by e ($e > 0$) such that

$$W_{\{e\}(e)} \supseteq W^A_{f(e+1)} \tag{1}$$

and such that $\mu(W_{\{e\}(e)}) < 2^{-e}$. By the recursion theorem we may assume that we know the number e in advance. Note that by construction of the first level $\mathcal{U}_0$ of the universal sequential test (see above) the equation (1) implies that the $(e+1)$-st level of the universal sequential test relative to A is included in $\mathcal{U}_0$. In particular $\mathrm{RAND}^A \supseteq \mathcal{P}_0$. So if $C \in \mathrm{RAND}$, then $T^k(C)$ is in $\mathcal{P}_0$ for some k by Lemma 1.5, hence $T^k(C) \in \mathrm{RAND}^A$, and therefore $C \in \mathrm{RAND}^A$. So (1) guarantees that A is low for RAND.

Let A_s denote the (finite) set of elements of A enumerated by the end of stage s. To be able to satisfy (1) we want to make sure that whenever y enters A at stage s for the sake of R_z, the 'mistake' we have made, that is, the amount of measure enumerated up to stage s on the basis of '$A(y) = 0$', is small, so that we can correct it without danger of enumerating too much in total. Given y and s, let M_y^s be the set of all strings $\sigma \in \bigcup_{t<s} W_{f(e+1),t}^{A_t}$ such that for some $t < s$ with $y \notin A_t$ the computation $\{f(e+1)\}_t^{A_t}(\sigma)$ converges and has use bigger than y, and such that there is no $\tau \sqsubseteq \sigma$ such that $(\exists t < s)[\mathrm{use}(\{f(e+1)\}_t^{A_t}(\tau)\downarrow) < y]$. That is, M_y^s is the set of strings σ that contribute to the measure of $W_{\{e\}(e)}$ (this set will be defined below) on the basis of '$A(y) = 0$', and that were not yet enumerated (or implicitly enumerated because some initial segment was enumerated) on the basis of some other computation before stage s that did not use the bit $A(y)$. We think of M_y^s as the potential mistake we make, which may become a real mistake when we enumerate y into A, thereby changing the bit $A(y)$ from 0 to 1. Note that we do not require different mistakes to be disjoint and that mistakes may be counted more than once. The (finite) set M_y^s defines a Σ_1^0 class of which we can compute the measure.

We say that R_z *requires attention* at stage s if

$$(\exists y \leq s)\, [y \in W_{z,s} \,\wedge\, y \geq 2z \,\wedge\, W_{z,s} \cap A_s = \emptyset \,\wedge\, \mu(M_y^s) \leq 2^{-z-e-2}]. \quad (2)$$

The construction of A is now easily described:

Stage $s = 0$. Define $A_0 = \emptyset$.

Stage $s > 0$. For every $z \leq s$ such that R_z requires attention at s, pick some y witnessing this, say the smallest y satisfying (2), and enumerate y into A_s.

The number $\{e\}(e)$ is defined to be an index of a Σ_1^0 class such that whenever σ is enumerated into $W_{f(e+1),s}^{A_s}$ then σ is enumerated into $W_{\{e\}(e)}$, i.e., $W_{\{e\}(e)}$ is defined as

$$W_{\{e\}(e)} = \bigcup_{s \in \omega} W_{f(e+1),s}^{A_s}\ .$$

Note that when the oracle A changes, say because y enters A at stage s, no further string is enumerated into $W_{\{e\}(e)}$ using the 'wrong' bit $A(y) = 0$ because of the 's' occurring in the subscript.

LEMMA 1 $\mu(W_{\{e\}(e)}) < 2^{-e}$.

PROOF. The measure of $W_{\{e\}(e)}$ is by definition equal to the measure of $W^A_{f(e+1)}$ plus the amounts of measure $\mu(M^s_y)$ enumerated by 'mistake' because the approximation to A was changed. Because the approximation to A is only changed for the sake of R_z if this mistake is not bigger than 2^{-z-e-2} and every R_z requires attention at most once we have

$$\mu(W_{\{e\}(e)}) < 2^{-(e+1)} + \sum_{z\in\omega} 2^{-z} \cdot 2^{-e-2} = 2^{-e}$$

$\square$ Lemma 1

LEMMA 2 *R_z is satisfied for every z.*

PROOF. Suppose W_z is infinite and that for all $y \geq 2z$ with $y \in W_{z,s}$ it holds that $\mu(M^s_y) > 2^{-z} \cdot 2^{-e-2}$. First observe that for every y and s there exist $y' > y$ and $s' > s$ such that for every $v \geq y'$ and every $t \geq s'$ we have $\mathrm{Ext}(M^t_v) \cap \mathrm{Ext}(M^s_y) = \emptyset$. To see that y' and s' exist, define the downward closure

$$\mathrm{downcl}(M^s_y) = \{\tau \in 2^{<\omega} : \exists \sigma \in M^s_y(\tau \sqsubseteq \sigma)\}.$$

Let $t_0 \in \omega$ be so large that

$$\{\tau \in \mathrm{downcl}(M^s_y) : \exists t(\{f(e+1)\}^{A_t}_t(\tau)\downarrow)\} =$$
$$\{\tau \in \mathrm{downcl}(M^s_y) : \exists t \leq t_0(\{f(e+1)\}^{A_t}_t(\tau)\downarrow)\}.$$

Consider the maximum

$$\max\{\mathrm{use}(\{f(e+1)\}^{A_t}_t(\tau)) : t \leq t_0 \wedge \tau \in \mathrm{downcl}(M^s_y)\}.$$

Note that this maximum exists because the set $\mathrm{downcl}(M^s_y)$ is finite. Now if y' is chosen above this maximum and $s' > t_0$ then for every $v \geq y'$ and $t \geq s'$ we have $M^t_v \cap \mathrm{downcl}(M^s_y) = \emptyset$ and $M^s_y \cap \mathrm{downcl}(M^t_v) = \emptyset$, so $\mathrm{Ext}(M^t_v) \cap \mathrm{Ext}(M^s_y) = \emptyset$. It follows from our assumption and from the above that there are infinitely many pairs y and s such that $y \in W_{z,s}$ with $\mu(M^s_y) > 2^{-z-e-2}$ and such that all the Σ^0_1 classes $\mathrm{Ext}(M^s_y)$ are disjoint. Because for every y and s it holds that $M^s_y \subseteq W_{\{e\}(e)}$ we then have $\mu(W_{\{e\}(e)}) = \infty$, a contradiction. So the assumption from the beginning of our proof cannot be true, and it follows with (2) that for infinite W_z, R_z requires attention at some stage and is satisfied at that same stage. (For finite W_z the requirement R_z is vacuously satisfied.) $\square$ Lemma 2

From the construction we see that the set A is r.e. By the clause '$y \geq 2z$' in (2) it has infinite complement and by Lemma 2 it intersects every infinite r.e. set, so A is simple. By Lemma 1 and the definition of $\mathcal{U}_0$ we have the inclusion $W^A_{f(e+1)} \subseteq W_{\{e\}(e)} \subseteq \mathcal{U}_0$, so (1) is satisfied. This concludes the proof of Theorem 2.1. $\square$

We conclude this section with some remarks. Zambella (private communication) has shown that the use of the recursion theorem in the above proof is not essential. It is unknown exactly how complex sets in Low(RAND) can be. The nonrecursive example constructed above is still r.e. Are there sets in Low(RAND) that are outside of Δ^0_2? And if so, are there uncountably many such sets? Recently, Terwijn and Zambella [10] proved that there are uncountably many nonrecursive sets that are low for the class of Schnorr random sequences. They also showed that these sets are *all* outside of Δ^0_2. This contrasts the situation for the 1-random sequences above.

3 Some limitations

In this section we make some remarks on the complexity of sets that are low for RAND. Since every nonrecursive r.e. set bounds a 1-generic set we immediately have the existence of 1-generic sets that are low for RAND. However, if $A \in \text{Low(RAND)}$ then A cannot be 1-random, since this would imply that A is A-1-random, which is impossible. Another limitation comes from the next theorem.

Theorem 3.1 (Kučera [5]) *If $A \leq_T B$ and B is A-1-random then $A \in \mathrm{GL}_1$.*

Corollary 3.2 *If A is low for* RAND *then $A \in \mathrm{GL}_1$.*

Proof. Since every set has a 1-random set above it ([4, 1]), if A is low for RAND then in particular A has a set above it that is A-1-random, and the corollary immediately follows from Theorem 3.1. $\square$

Next we prove a limitation that shows that all (partial) functions that are of degree that is low for RAND can be uniformly dominated by a function recursive in $\emptyset'$. First we give two definitions. We say that a function g *dominates* a partial function f if there is a $k \in \omega$ such that whenever $f(n)$ is defined for some $n \geq k$ it holds that $g(n) \geq f(n)$. For strings τ and σ we say that τ is *to the left* of σ, denoted $\tau <_{\mathrm{L}} \sigma$, if there is a string ρ such that $\rho\hat{\ }0 \sqsubseteq \tau$ and $\rho\hat{\ }1 \sqsubseteq \sigma$.

Theorem 3.3 *There exists a function $g \leq_T \emptyset'$ that dominates every function in the class of partial functions $\{\{e\}^A : A \in \text{Low(RAND)}\}$.*

Proof. Let R be the leftmost path in $\mathcal{P}_0$, $\mathcal{P}_0$ as defined in Definition 1.4. Then R is 1-random, being an element of $\mathcal{P}_0$, and it is easy to see that $R \leq_T \emptyset'$ (even $R \leq_{tt} \emptyset'$). Denote by V the set of strings to the left of R, i.e.

$$V = \bigcup_{i \in \omega} \{\tau \in 2^{<\omega} : \tau <_{\mathrm{L}} R{\restriction}i\}.$$

Note that V is an r.e. set since $\mathcal{U}_0$ is Σ^0_1. Let $\{V_s\}_{s\in\omega}$ be a recursive enumeration of V. To every set $A \in 2^\omega$ and every partial A-recursive function $\{e\}^A$ we can assign an A-recursive sequential test $\{\mathcal{B}_i^{e,A}\}_{i\in\omega}$ as follows. If $\{e\}^A(i)\downarrow$ let τ be the first string of length i to the right of the rightmost (in the sense of the ordering $<_L$ defined above) string of length i in $V_{\{e\}^A(i)}$ if such a string exists, and let τ be 0^i otherwise. Now let $\mathcal{C}_i^{e,A}$ be the basic open set defined by the string τ, i.e. $\mathcal{C}_i^{e,A} = \{B : \tau \sqsubset B\}$. If $\{e\}^A(i)\uparrow$ let $\mathcal{C}_i^{e,A}$ be empty. Finally, let

$$\mathcal{B}_i^{e,A} = \bigcup_{j>i} \mathcal{C}_j^{e,A}.$$

Now define

$$g(i) = (\text{least } s)(\forall \tau <_{\mathrm{L}} R{\restriction}i)[|\tau| = i \rightarrow \tau \in V_s].$$

We claim that g satisfies the statement of the theorem. Clearly we have $g \leq_T R \leq_T \emptyset'$. Let $A \in \mathrm{Low(RAND)}$. Suppose that there are infinitely many $i \in \omega$ such that $\{e\}^A(i)$ is defined and bigger than or equal to $g(i)$. For every such i it holds that $R \in \mathcal{B}_i^{e,A}$. It follows that R is not A-1-random. Since $A \in \mathrm{Low(RAND)}$ we then also have that R is not 1-random, a contradiction. $\square$

Zambella (private communication) has shown, using ideas of a totally different nature, that Theorem 3.3 can be improved. Namely, the values of the functions that are partial recursive in a set in Low(RAND) can be uniformly approximated by an r.e. set in such a way that the number of approximating values is small.

Acknowledgments. The second author would like to thank Klaus Ambos-Spies, Michiel van Lambalgen, and Domenico Zambella for helpful discussions.

References

[1] P. Gács, *Every sequence is reducible to a random one*, Inform. and Control 70 (1986) 186–192.

[2] T. Kamae, *Subsequences of normal sequences*, Israel J. Math. 16 (1973) 121–149.

[3] S. M. Kautz, *Degrees of random sets*, PhD Thesis, Cornell University (1991).

[4] A. 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 1984, Lect. Notes in Math. 1141 (1985) 245–259.

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

[6] M. van Lambalgen, *Random sequences*, PhD Thesis, University of Amsterdam, 1987.

[7] M. van Lambalgen, *The axiomatization of randomness*, J. Symbolic Logic 55 (3), 1990, 1143–1167

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

[9] R. I. Soare, *Recursively enumerable sets and degrees*, Springer-Verlag, 1987.

[10] S. A. Terwijn and D. Zambella, *Algorithmic randomness and lowness*, ILLC technical report ML-1997-07, University of Amsterdam, 1997.

[11] D. Zambella, *On sequences with simple initial segments*, ILLC technical report ML-1990-05, University of Amsterdam, 1990.