Publishers' page

Publishers' page

Publishers' page

Publishers' page

CONTENTS

FOREWORD

a foreword

PREFACE

a preface

LOWNESS FOR COMPUTABLE MACHINES

Rod Downey
School of Mathematics, Statistics and Computer Science, Victoria University, P.O. Box 600, Wellington, New Zealand
E-mail: Rod.Downey@vuw.ac.nz

Noam Greenberg
School of Mathematics, Statistics and Computer Science, Victoria University, P.O. Box 600, Wellington, New Zealand
E-mail: greenberg@mcs.vuw.ac.nz

Nenad Mihailović
Mathematical Institute, University of Heidelberg, Im Neuenheimer Feld 294, 69120 Heidelberg, Germany
E-mail: mihailovic@math.uni-heidelberg.de

André Nies
Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand
E-mail: andre@cs.auckland.ac.nz

Two lowness notions in the setting of Schnorr randomness have been studied (lowness for Schnorr randomness and tests, by Terwijn and Zambella [19], and by Kjos-Hanssen, Stephan, and Nies [7]; and Schnorr triviality, by Downey, Griffiths and LaForte [3, 4] and Franklin [6]). We introduce lowness for computable machines, which by results of Downey and Griffiths [3] is an analog of lowness for K. We show that the reals

The first, second and fourth authors are partially supported by the New Zealand Marsden Fund for basic research. This work was carried out while Mihailović was visiting Victoria University and was also partially supported by the Marsden Fund and by a "Doktorandenstipendium" from the DAAD (German Academic Exchange Service).

that are low for computable machines are exactly the computably traceable ones, and so this notion coincides with that of lowness for Schnorr randomness and for Schnorr tests.

Contents

1. Introduction

A central set of results in the theory of algorithmic randomness were established by Nies and his co-authors. They prove the coincidence of a number of natural "anti-randomness" classes associated with prefix-free Kolmogorov complexity. Recall that A is called *low for K* if for all x, $K^A(x) \geq K(x) - O(1)$,[a] A is called *K-trivial* if for all n, $K(A \upharpoonright n) \leq K(n) + O(1)$, and A is called *low for Martin-Löf randomness* if the collection of reals Martin-Löf random relative to A is the same as the collection of Martin-Löf random reals. We have the following.

Theorem 1.1: (Nies, Hirschfeldt, [12, 13]) *For every real A, the following are equivalent.*

(i) A is low for K.
(ii) A is K-trivial.
(iii) A is low for Martin-Löf randomness.

The situation for other notions of randomness is less clear. In this paper we look at the situation for Schnorr randomness. Recall that a real A is said to be *Schnorr random* iff for all Schnorr tests $\{U_n : n \in \mathbb{N}\}$, $A \notin \cap_n U_n$, where a Schnorr test is a Martin Löf test such that $\mu(U_n) = 2^{-n}$ for all n. (Of course 2^{-n} is a convenience. As Schnorr [16] observed, any uniformly computable sequence of reals with effective limit 0 would do.)

The reader might note that there are two possible lowness notions associated with Schnorr randomness. A real A is *low for Schnorr randomness*

[a]In this paper K will denote prefix-free Kolmogorov complexity and we will refer to members $A = a_0 a_1 \ldots$ of Cantor space as *reals*, with $A \upharpoonright n$ being the first n bits of A. We assume that the reader is familiar with the theory of algorithmic randomness. For details we refer to the monographs of Li and Vitányi [10], of Downey and Hirschfeldt [5], and of Nies [14].

if no Schnorr random real becomes non-Schnorr-random relative to A. But since there is no universal Schnorr test, we can also define the stronger (and more technical) notion of lowness for *tests*; a real A is *low for Schnorr tests* if for every A-Schnorr test $\{U_n^A : n \in \mathbb{N}\}$, there is a Schnorr test $\{V_n : n \in \mathbb{N}\}$ such that $\cap_n U_n^A \subseteq \cap_n V_n$.

Terwijn and Zambella [19] proved that there are reals that are low for Schnorr tests. In fact, they classified the collection of reals which are low for Schnorr tests.

For any n, we let D_n denote the nth canonical finite set.

Definition 1.2: (Terwijn and Zambella [19]) We say that a real A is *computably traceable* if there is a computable function $h(x)$ such that for all functions $g \leq_T A$, there is a computable collection of canonical finite sets $D_{r(x)}$ with $|D_{r(x)}| \leq h(x)$ and such that $g(x) \in D_{r(x)}$.

We remark that (as noticed by Terwijn and Zambella) if A is computably traceable then for the witnessing function h we can choose any computable, non-decreasing and unbounded function.

Terwijn and Zambella proved the following attractive result.

Theorem 1.3: (Terwijn and Zambella [19]) *A is low for Schnorr tests iff A is computably traceable.*

We remark that while all K-trivials are Δ_2^0 by a result of Chaitin [1], the computably traceable reals are all hyperimmune-free, and there are $2^{\aleph_0}$ many of them.

Subsequently, Kjos-Hanssen, Stephan, and Nies [7] proved that A is low for Schnorr randomness iff A is low for Schnorr tests.

The reader might wonder about analogs of the other results for K. The other members of the coincidence involve K-triviality and lowness for K. What about the Schnorr situation? We want some analog of the characterization of Martin-Löf randomness in terms of prefix-free complexity. (R is Martin-Löf random iff for all n, $K(R \upharpoonright n) \geq n - O(1)$.) Such a characterization was discovered by Downey and Griffiths [3]. They define a prefix-free Turing machine M to be *computable* if the domain of M has computable measure, that is, $\sum_{\{\sigma : M(\sigma)\downarrow\}} 2^{-|\sigma|}$ is a computable real. They then establish the following:

Theorem 1.4: (Downey and Griffiths [3]) *R is Schnorr random iff for all computable machines M, for all n, $K_M(R \upharpoonright n) \geq n - O(1)$.*[b]

The quantification over machines is necessary because (as in the situation for Schnorr tests), there is no universal computable machine. With this result we are in a position to define a real A to be *Schnorr trivial* if for every computable machine N there is a computable machine M such that for all n, $K_M(A \upharpoonright n) \leq K_N(n) + O(1)$. This notion was initially explored by Downey and Griffiths [3] and Downey, Griffiths and LaForte [4], who showed that this class does not coincide with the reals that are low for Schnorr randomness. For instance, there are Turing complete Schnorr trivial reals. Johanna Franklin [6] established the following.

Theorem 1.5: (Franklin [6])

(i) There is a perfect set of Schnorr trivials.
(ii) Every degree above $\mathbf{0}'$ contains a Schnorr trivial.
(iii) Every real that is low for Schnorr randomness is also Schnorr trivial. [c]

Thus the relationship between lowness for Schnorr randomness and Schnorr triviality is quite different from the analogous situation for Martin-Löf randomness.

The last piece of the puzzle is the analog for lowness for K. Armed with the machine characterization of Schnorr randomness, we give the following definition.

Definition 1.6: A real A is *low for computable machines* iff for all A-computable machines M there is a computable machine N such that for all x,

$$K_M^A(x) \geq K_N(x) - O(1).$$

[b]Note that since the range of M need not be all of $2^{<\omega}$, we need to let $K_M(x) = \infty$ for all strings x not in the range of M.

[c]Interestingly, Franklin also showed that the reals that are low for Schnorr randomness are not closed under join. The referee points out that a proof from Lerman [9] can be used to establish Franklin's result. To wit, the minimal degrees generate the Turing degrees under meet and join, and the referee points out that the proof (in [9]) also shows that such degrees can be chosen computably traceable, in the same way that the standard construction of a minimal degree is automatically computably traceable.

The reader might be concerned about whether for an A-computable machine M^A as in the definition above, M^B is B-computable for other oracles B. However, given a such a machine, we can obtain another oracle machine $\widetilde{M}$ such that $M^A = \widetilde{M}^A$, and such that $\widetilde{M}^B$ is prefix-free and B-computable for every oracle B. [d]

A relativized version of the Kraft-Chaitin Theorem (Lemma 2.1) can be used to show that Theorem 1.4 relativizes. Namely, we have that R is A-Schnorr random iff for all A-computable machines M, for all n, $K_M^A(R \upharpoonright n) \geq n - O(1)$. Therefore, every real A that is low for computable machines is low for Schnorr randomness, and by the results quoted above it follows further that A is low for Schnorr tests and thus is computably traceable. In this paper we show that unlike the situation for triviality, the coincidence of the reals low for Martin-Löf randomness and the low for K ones carries over to the Schnorr case:

Theorem 1.7: *A real A is low for computable machines iff A is computably traceable.*

We remark that part (iii) of Theorem 1.5 above is a consequence of Theorem 1.7, since every real A that is low for computable machines is Schnorr trivial. For let N be a computable machine. Let L be an A-computable machine such that for all n, $K_L^A(A \upharpoonright n) = K_N(n)$ (for all x, if $N(x) = n$ then let $L(x) = A \upharpoonright n$.) Then there is some computable machine M such that for all x, $K_M(x) \leq K_L^A(x) + O(1)$; M is as required to witness that A is trivial.

2. The proof

We note that if we enumerate a Kraft-Chaitin set with a computable sum then the machine produced is computable:

Lemma 2.1: (Kraft-Chaitin) *Let $\langle d_0, \tau_0 \rangle, \langle d_1, \tau_1 \rangle, \ldots$ be a computable list of pairs consisting of a natural number and a string. Suppose that*

---

[d] Indeed, define the machine $\widetilde{M}$ as follows. First, we may assume that for every oracle B, M^B is prefix-free. Now let F be a computable functional such $F(A)$ is total and the measure of the set $\{x \leq F(A,n) \colon M^A(x)$ is defined after $F(A,n)$ steps$\}$ approximates $\mu(M^A)$ to within 2^{-n}. Define $\widetilde{M}^B$ inductively: at stage n, first wait for $F(B,n)$ to halt (in the meantime, no new $\widetilde{M}^B$-computations are recognised.) Next, allow M^B to run for $F(B,n)$ many steps and accept new computations as $\widetilde{M}^B$-computations; if at a later stage we see that $\mu(M^B) > \mu(M^B)[F(B,n)] + 2^{-n}$ then we stop accepting new $\widetilde{M}^B$-computations altogether. Then move to stage $n+1$. Note that the construction is uniform in M, F but not in M alone.

$\sum_{i<\omega} 2^{-d_i}$ *is a computable real (in particular, is finite). Then there is a* computable *machine N such that for all i, $K_N(\tau_i) \leq d_i + O(1)$.*

(See Downey [2] for a proof of the Kraft-Chaitin theorem; the fact that we get a computable machine is immediate from the proof.)

To prove Theorem 1.7 we need to show that every computably traceable set A is low for computable machines. So let A be a computably traceable set and let M be an oracle machine such that M^A is A-computable. The idea (somewhat following Terwijn and Zambella) is to "break up" the machine M^A into small and finite pieces which we trace. We view M^A as a function from strings to strings. We will partition M^A into finite pieces $g, f_0, f_1, f_2, \dots$ where for $n < \omega$, the measure of the domain of f_n is smaller than some small rational ε_n. We then trace the sequence $\langle f_n \rangle$; so for every n, we get $h(n)$ many candidates for f_n, each with domain with measure smaller than ε_n. If we keep $\sum_n h(n)\varepsilon_n$ finite, the union of all of the candidates can be translated into a Kraft-Chaitin set that produces the machine we want.

Let h be the computable function given by Definition 1.2 (again we remark that we can pick any reasonable function; it doesn't matter for this proof.) Fix a computable, decreasing sequence of positive rationals $\varepsilon_0, \varepsilon_1, \dots$ such that $\sum_{n<\omega} h(n)\varepsilon_n$ is finite; moreover, we want the convergence to be quick, say for every $m < \omega$,

$$\sum_{n \geq m} h(n)\varepsilon_n \; < \; 2^{-m}.$$

Let $\langle (\sigma_i, \tau_i) \rangle_{i<\omega}$ be an A-computable enumeration of M^A. We let M^A_s, the machine M^A at stage s, be $\{(\sigma_i, \tau_i) \,:\, i < s\}$, and similarly let $M^A_{\geq s} = M^A \setminus M^A_s = \{(\sigma_i, \tau_i) \,:\, i \geq s\}$, and for $s < t$, $M^A_{[s,t)} = M^A_t \setminus M^A_s$.

Let t_n be the least stage t such that $\mu(\operatorname{dom} M^A_{\geq t}) < \varepsilon_n$. We let $g = M^A_{t_0}$; for $n < \omega$, we let $f_n = M^A_{[t_n, t_{n+1})}$. The point is that the sequence $\langle t_n \rangle$, and so the sequence $\langle f_n \rangle$, are A-computable, as $\mu(\operatorname{dom} M^A_{\geq t}) = \mu(\operatorname{dom} M^A) - \mu(\operatorname{dom} M^A_t)$; the first number is A-computable by assumption, and the latter a rational, computable from the sequence $\langle (\sigma_i, \tau_i) \rangle$ and so from A. For all $n < \omega$, $\mu(\operatorname{dom} f_n) < \varepsilon_n$.

Each f_n is a finite function (and so has a natural number code.) We can thus computably trace the sequence $\langle f_n \rangle$; there is a computable sequence of finite sets $\langle X_n \rangle_{n<\omega}$ (i.e. $X_n = D_{r(n)}$ where r is computable) such that for each n, $|X_n| \leq h(n)$, and for each n, (the code for) $f_n \in X_n$. By weeding out elements, we may assume that for each $n < \omega$, every element of X_n

is a code for a finite function f from strings to strings whose domain is prefix-free and has measure at most ε_n.

Enumerate a Kraft-Chaitin set L as follows. Let $\langle d, \tau \rangle \in L$ if there is some σ such that $|\sigma| = d$, and one of the following holds:

- $(\sigma, \tau) \in g$;
- For some n and for some $f \in X_n$, $(\sigma, \tau) \in f$.

The set L is computably enumerable. Further, the total of the requests $s = \sum_{(d,\tau) \in L} 2^{-d}$ is a finite, computable real, as we know that for any m,

$$\sum \{2^{-|\sigma|} \colon (\exists n \geq m)(\exists f \in X_n)[\sigma \in \operatorname{dom} f]\} \;\leq\; \sum_{n \geq m} h(n)\varepsilon_n \;\leq\; 2^{-m}.$$

From the "computable" Kraft-Chaitin theorem we get a computable machine N such that for some constant c, if $(d, \tau) \in L$, then $K_N(\tau) \leq d + c$. On the other hand, we know that if τ is in the range of M^A then $(K_M^A(\tau), \tau) \in L$ because $f_n \in X_n$ for all n. Thus N is as required.

References

1. Chaitin, G., *Information-theoretical characterizations of recursive infinite strings,* Theoretical Computer Science, Vol. 2 (1976), 45–48.
2. Downey, R., *Five lectures on algorithmic randomness,* this volume.
3. Downey, R. and E. Griffiths, *On Schnorr randomness*, Journal of Symbolic Logic, Vol. 69, No. 2 (2004), 533–554.
4. Downey, R., E. Griffiths, and G. LaForte, *On Schnorr and computable randomness, martingales, and machines*, Mathematical Logic Quarterly, Vol. 50, No. 6 (2004), 613–627.
5. Downey, R. and D. Hirschfeldt, *Algorithmic Randomness and Complexity,* Springer-Verlag Monographs in Computer Science, to appear (preliminary version `www.mcs.vuw.ac.nz/~downey`).
6. Franklin, J., Ph.D. Dissertation, University of California at Berkeley, in preparation.
7. Kjos-Hanssen, B., F. Stephan, and A. Nies. *Lowness for the class of Schnorr random reals,* SIAM Journal on Computing, Vol. 35, No. 3 (2006), 647–657.
8. Kučera, A. and S. Terwijn, *Lowness for the class of random sets,* Journal of Symbolic Logic, Vol. 64 (1999), 1396–1402.
9. Lerman, M., *Degrees of Unsolvability,* Springer-Verlag Berlin Heidelberg, 1983.
10. Li, M. and P.M.B. Vitányi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, New York, second edition, 1997.
11. Martin-Löf, P., *The definition of random sequences*, Information and Control, Vol. 9 (1966), 602–619.
12. Nies, A., *Reals which compute little*, to appear, *Proceedings of CL 2002.*

13. Nies, A., *Lowness properties and randomness*, Advances in Mathematics 197, Vol. 1 (2005), 274–305.
14. Nies, A., *Computability and Randomness,* monograph in preparation.
15. Schnorr, C. P., *A unified approach to the definition of a random sequence,* Mathematical Systems Theory, Vol. 5 (1971), 246–258.
16. Schnorr, C. P., *Zufälligkeit und Wahrscheinlichkeit*, Lecture Notes in Mathematics, Vol. 218, 1971, Springer-Verlag, New York.
17. Terwijn, S. A., *Computability and Measure*, Ph.D. Thesis, University of Amsterdam, 1998.
18. Terwijn, S. A., *Complexity and Randomness,* Notes for a course given at the University of Auckland, March 2003. Published as research report CDMTCS-212, University of Auckland.
19. Terwijn, S. A. and D. Zambella, *Computational randomness and lowness*, Journal of Symbolic Logic, Vol. 66, No. 3 (2001), 1199–1205.