Isaac Newton Institute
for Mathematical Sciences

Seventh International Conference on Computability, Complexity and Randomness (CCR 2012)

2 – 6 July 2012,

Cambridge, Great Britain,

Isaac Newton Institute for Mathematical Sciences

ALAN TURING YEAR 2012

CCR 2012 is part of the Alan Turing Year 2012.

Table of Contents

Preface

The *Seventh International Conference on Computability, Complexity and Randomness (CCR 2012)* takes places at the Isaac Newton Institute for Mathematical Sciences in Cambridge from 2 July to 6 July 2012.

The conference CCR 2012 has about 75 registered participants and features 13 invited and 18 contributed talks, hence will be as successful as the previous meeting of the CCR conference series, which took place in Córdoba (2004), Buenos Aires (2007), Nanjing (2008), Luminy (2009), Notre Dame (2010), and Cape Town (2011).

The conference CCR 2012 is the final event of the six-month programme *Semantics and Syntax: a Legacy of Alan Turing*, which is organized and hosted by the Isaac Newton Institute in commemoration of the centenary of Alan Turing's birthday on 23 June 1912.

We would like to acknowledge substantial financial support by the Isaac Newton Institute for all participants of CCR 2012 and support by the Association for Symbolic Logic for student participants. Moreover, we are grateful to all invited speakers, and all authors and co-authors for their contributions and to the members of the Programme Committee for their support.

Rod G. Downey (on behalf of the steering committee of the CCR conference series)
Elvira Mayordomo (on behalf of the programme committee of CCR 2012)
Wolfgang Merkle (on behalf of the programme committee of CCR 2012)

Invited Speakers

George Barmpalias	Chinese Academy of Sciences, Beijing
Vasco Brattka	University of Cape Town
Adam R. Day	University of California, Berkeley
Rod G. Downey	Victoria University of Wellington
John Hitchcock	University of Wyoming
Mathieu Hoyrup	Lorraine Research Laboratory in Computer Science and its Applications
Michal Koucký	Czech Academy of Sciences
Andrew E. M. Lewis	University of Leeds
Jack H. Lutz	Iowa State University
André Nies	University of Auckland
Alexander Shen	Laboratoire d'Informatique Fondamentale de Marseille
Steve Simpson	Pennsylvania State University
Daniel Turetsky	Victoria University of Wellington

Program Committee

Laurent Bienvenu	LIAFA, CNRS & Université Paris 7
Péter Gács	Boston University
Antonín Kučera	Charles University Prague
Elvira Mayordomo	Universidad de Zaragoza
Wolfgang Merkle	Universität Heidelberg
Nikolai Vereshchagin	Lomonosov Moscow State University
Paul Vitányi	CWI & University of Amsterdam

Organizers

Elvira Mayordomo	Universidad de Zaragoza
Wolfgang Merkle	Universität Heidelberg

THE TYPICAL TURING DEGREE

ANDREW E.M. LEWIS

Abstract. Since Turing degrees are tailsets, it follows from Kolmogorov's 0-1 law that for any property which may or may not be satisfied by any given Turing degree, the satisfying class will either be of Lebesgue measure 0 or 1, so long as it is measurable. So either the *typical* degree satisfies the property, or else the typical degree satisfies its negation. Further, there is then some level of randomness sufficient to ensure typicality in this regard. I shall describe a number of results in a largely new programme of research which aims to establish the (order theoretically) definable properties of the typical Turing degree, and the level of randomness required in order to guarantee typicality.

A similar analysis can be made in terms of Baire category, where a standard form of genericity now plays the role that randomness plays in the context of measure. This case has been fairly extensively examined in the previous literature. I shall analyse how our new results for the measure theoretic case contrast with existing results for Baire category, and also provide some new results for the category theoretic analysis.

This is joint work with George Barmpalias and Adam Day.

EXACT PAIRS FOR THE IDEAL OF THE K-TRIVIAL SEQUENCES IN THE TURING DEGREES

GEORGE BARMPALIAS AND ROD G. DOWNEY

Abstract

The algebraic study of the Turing degrees has been a topic of considerable research in computability theory, ever since the establishment of degree theory as a research area in [KP54]. In this study, the ideals of this uppersemilattice are of particular interest. These are downward closed sets of degrees that also closed under the join operator. The recent study of algorithmic information theory by people in computability theory has brought forward a wealth of interactions between the two areas, including the discovery of a new ideal in the Turing degrees: the degrees of sequences with trivial initial segment complexity, the so-called K-trivial sequences. Since this discovery in [DHNS03, Nie05], the study of the K-trivial sequences and degrees have been established as a major area of research in the interface between computability theory and algorithmic information theory.

Issues of definability have been of special interest in the study of ideals in the Turing degrees. Such issues were already present in [KP54], where the notion of exact pairs of ideals was introduced. Two degrees $\mathbf{a}, \mathbf{b}$ form an *exact pair* of an ideal $\mathcal{C}$ in the Turing degrees if they are both upper bounds for the degrees in $\mathcal{C}$ and any degree below both $\mathbf{a}$ and $\mathbf{b}$ is in $\mathcal{C}$. By [KP54, Spe56] every ideal in the Turing degrees has an exact pair. By [Nie05] every K-trivial degree is bounded by a computably enumerable (c.e. for short) K-trivial degree. Hence for the purpose of finding exact pairs for this ideal it suffices to consider its restriction to the c.e. degrees. This turns out to be a Σ^0_3 ideal, in the sense that the index set of its members is Σ^0_3. Moreover by [BN11] it has a c.e. upper bound that is strictly below the degree $\mathbf{0}'$ of the halting problem. By [Sho81], such ideals have an exact pair strictly below $\mathbf{0}'$. However it is well known that such an ideal may or may not have an exact pair in the c.e. degrees (this follows from the existence of branching and non-branching degrees that was established in [Lac66, Yat66]). Hence whether or not such an ideal have an exact pair in the c.e. degrees depends on the specific properties of it. The following question has come into focus.

Key words and phrases. Computably enumerable, Turing degrees, Kolmogorov complexity, K-trivial sets, exact pairs.

This research was partially done whilst the authors were visiting fellows at the Isaac Newton Institute for the Mathematical Sciences, Cambridge U.K., in the programme 'Semantics & Syntax'. Barmpalias was supported by the *Research fund for international young scientists* number 611501-10168 from the National Natural Science Foundation of China, and an *International Young Scientist Fellowship* number 2010-Y2GB03 from the Chinese Academy of Sciences; partial support was also received from the project *Network Algorithms and Digital Information* number ISCAS2010-01 from the Institute of Software, Chinese Academy of Sciences. Downey was supported by a Marsden grant of New Zealand. The authors wish to thank André Nies and Ted Slaman for helpful discussions.

Problem (Question 4.2 in [MN06] and Problem 5.5.8 in [Nie09])**.** *Is there an exact pair for the ideal of the K-trivial sequences in the c.e. degrees?*

The purpose of this work is to give a negative answer to this question.

Theorem. *There exists a K-trivial c.e. degree $\mathbf{d}$ with the following property. For each pair of c.e. degrees $\mathbf{a}, \mathbf{b}$ which are not K-trivial, there exists a c.e. degree $\mathbf{v}$ which is not K-trivial and $\mathbf{v} < \mathbf{a} \cup \mathbf{d}, \mathbf{v} < \mathbf{b} \cup \mathbf{d}$.*

Here $\mathbf{a} \cup \mathbf{d}$ denotes the join (i.e. supremum) of the degrees $\mathbf{a}, \mathbf{d}$. It follows that the ideal of the K-trivial sequences does not have an exact pair of c.e. degrees. The proof of this Theorem rests on a result from [Bar11] which roughly says that any two c.e. sets of nontrivial initial segment complexity must have common lengths in their characteristic sequences where their complexity rises *simultaneously*. We may contrast our main result with the following known fact.

> If $\mathbf{c}$ is a c.e. degree which is not K-trivial then there exist c.e. degrees $\mathbf{a} < \mathbf{c}$ and $\mathbf{b} < \mathbf{c}$ which are not K-trivial and $\mathbf{c} = \mathbf{a} \cup \mathbf{b}$.

Since there exists a Δ^0_2 exact pair for the K-trivial degrees, the phenomenon described our Theorem is specific to c.e. sets.

> There exists a degree $\mathbf{x} < \mathbf{0}'$ which is not K-trivial and for every K-trivial degree $\mathbf{d}$, the only c.e. degrees that are computable from $\mathbf{x} \cup \mathbf{d}$ are also computable from $\mathbf{d}$.

This observation confirms the above intuition from a different angle.

References

[Bar11] George Barmpalias. Universal computably enumerable sets and initial segment prefix-free complexity. Submitted. Available at `http://www.barmpalias.net`, 2011.

[BN11] George Barmpalias and André Nies. Upper bounds on ideals in the computably enumerable turing degrees. *Ann. Pure Appl. Logic*, 162(6):465–473, 2011.

[DHNS03] Rod G. Downey, Denis R. Hirschfeldt, André Nies, and Frank Stephan. Trivial reals. In *Proceedings of the 7th and 8th Asian Logic Conferences*, pages 103–131, Singapore, 2003. Singapore Univ. Press.

[KP54] S.C. Kleene and E. Post. The upper semi-lattice of degrees of recursive unsolvability. *Ann. of Math. (2)*, 59:379–407, 1954.

[Lac66] A. H. Lachlan. Lower bounds for pairs of recursively enumerable degrees. *Proc. London Math. Soc. (3)*, 16:537–569, 1966.

[MN06] Joseph S. Miller and André Nies. Randomness and computability: open questions. *Bull. Symbolic Logic*, 12(3):390–410, 2006.

[Nie05] André Nies. Lowness properties and randomness. *Adv. Math.*, 197(1):274–305, 2005.

[Nie09] André Nies. *Computability and Randomness*. Oxford University Press, 2009.

[Sho81] Richard A. Shore. The theory of the degrees below $0'$. *J. London Math. Soc.*, 24:1–14, 1981.

[Spe56] C. Spector. On the degrees of recursive unsolvability. *Ann. of Math. (2)*, 64:581–592, 1956.

[Yat66] C. E. M. Yates. A minimal pair of recursively enumerable degrees. *J. Symbolic Logic*, 31:159–168, 1966.

George Barmpalias: State Key Lab of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.O. Box 8718, China.

E-mail address: `barmpalias@gmail.com`

URL: `http://www.barmpalias.net`

Rod G. Downey: School of Mathematics, Statistics and Operations Research, Victoria University, P.O. Box 600, Wellington, New Zealand.

E-mail address: `rod.downey@vuw.ac.nz`

RESOLUTE SETS AND INITIAL SEGMENT COMPLEXITY

ROD DOWNEY

Abstract. Notions of triviality have been remarkably productive in algorithmic randomness,with K-triviality being the most notable. Of course, ever since the original characterization of Martin-Löf randomenss by initial segment complexity, there has been a longstanding interplay between initial segment complexity and calibrations of randomness, as witnessed by concepts such as autocomplexity, and the like.

In this talk I wish to discuss recent work with George Barmpalias on a triviality notion we call *resoluteness*. Resoluteness is defined in terms of computable shifts by is intimately related to a notion we call weak resoluteness where A is weakly resolute iff for all computable orders h, $K(A \upharpoonright n) \geq^+ K(A \upharpoonright h(n))$, for all n. It is not difficult to see that K-trivials have this property but it turns out that there are uncountablly many degrees which are completely K-resolute, and there are c.e. degrees also with this property.

These degrees seem related to Lathrop-Lutz *ultracompressible* degrees.

Our investigations are only just beginning and I will report on our progress.

Joint work with George Barmpalias.

ON THE COMPUTATIONAL CONTENT OF THE BAIRE CATEGORY THEOREM

VASCO BRATTKA

Abstract. We present results on the classification of the computational content of the Baire Category Theorem in the Weihrauch lattice. The Baire Category Theorem can be seen as a pigeonhole principle that states that a large (= complete) metric space cannot be decomposed into a countable number of small (= nowhere dense) pieces (= closed sets). The difficulty of the corresponding computational task depends on the logical form of the statement as well as on the information that is provided. In the first logical form the task is to find a point in the space that is left out by a given decomposition of the space that consists of small pieces. In the contrapositive form the task is to find a piece that is not small in a decomposition that exhausts the entire space. In both cases pieces can be given by descriptions in negative or positive form. We present a complete classification of the complexity of the Baire Category Theorem in all four cases and for certain types of spaces. The results are based on joint work with Guido Gherardi and Alberto Marcone, on the one hand, and Matthew Hendtlass and Alexander Kreuzer, on the other hand. One obtains a refinement of what is known in reverse mathematics in this way.

References

[BG11a] Vasco Brattka and Guido Gherardi. Effective choice and boundedness principles in computable analysis. *The Bulletin of Symbolic Logic*, 17(1):73–117, 2011.

[BG11b] Vasco Brattka and Guido Gherardi. Weihrauch degrees, omniscience principles and weak computability. *The Journal of Symbolic Logic*, 76(1):143–176, 2011.

[BGM12] Vasco Brattka, Guido Gherardi, and Alberto Marcone. The Bolzano-Weierstrass theorem is the jump of weak Kőnig's lemma. *Annals of Pure and Applied Logic*, 163:623–655, 2012.

[BHK12] Vasco Brattka, Matthew Hendtlass, and Alexander P. Kreuzer. On the Weihrauch complexity of computability theory. *unpublished notes*, 2012.

[Bra01] Vasco Brattka. Computable versions of Baire's category theorem. In Jiří Sgall, Aleš Pultr, and Petr Kolman, editors, *Mathematical Foundations of Computer Science 2001*, volume 2136 of *Lecture Notes in Computer Science*, pages 224–235, Berlin, 2001. Springer. 26th International Symposium, MFCS 2001, Mariánské Lázně, Czech Republic, August 27-31, 2001.

[BS93] Douglas K. Brown and Stephen G. Simpson. The Baire category theorem in weak subsystems of second order arithmetic. *The Journal of Symbolic Logic*, 58:557–578, 1993.

CUPPING WITH RANDOM SETS

ADAM R. DAY

Joint work with Joseph S. Miller (University of Wisconsin-Madison).

Posner and Robinson proved that any non-computable set that is Turing below $\emptyset'$ can be cupped to $\emptyset'$ with a 1-generic set [8]. In 2004, Kučera asked which sets below $\emptyset'$ can be cupped to $\emptyset'$ with an incomplete Martin-Löf random [7]. In other words, does the Posner-Robinson theorem hold if we replace Baire category with Lebesgue measure, and if not, for which sets does it fail?

The basic definitions are the following. The prefix-free complexity of a string σ is denoted by $K(\sigma)$. A set R is *Martin-Löf random* if there exists some constant c such that for all n, $K(R \upharpoonright n) > n - c$. The definition of a Martin-Löf random set can be relativized to any oracle A. We call a set A, *low for Martin-Löf randomness* if every Martin-Löf random set is also Martin-Löf random relative to A. A set A is *K-trivial* if for some constant c, for all n we have that $K(A \upharpoonright n) \leq K(n) + c$ (where $K(n)$ is defined to be $K(1^n)$). Hence, a K-trivial set is indistinguishable from a computable set in terms of K complexity. (The existence of non-computable K-trivial sets was first established by Solovay in an unpublished manuscript [2]. Later, Zambella constructed a non-computable K-trivial c.e. set [10].) A set A is *weakly ML-cuppable* if $A \oplus X \geq_T \emptyset'$ for some incomplete Martin-Löf random set X. A is *ML-cuppable* if one can choose $X <_T \emptyset'$.

Kučera conjectured that the weakly ML-cuppable sets might be exactly the sets that are not K-trivial. Nies showed that there exists a non-computable K-trivial c.e. set that is not weakly ML-cuppable providing evidence for this conjecture [7]. We prove this conjecture showing that the K-trivial sets are precisely those sets that cannot be joined above $\emptyset'$ with an incomplete random. We also show that all sets below $\emptyset'$ that are not K-trivial, can be joined to $\emptyset'$ with a low random.

There are two directions to this proof. The first is that no K-trivial is weakly ML-cuppable. This direction uses the equivalence of the K-trivial sets and the low for Martin-Löf randomness sets, a result of Nies [6]. It also builds on work of Franklin and Ng, and Bienvenu, Hölzl, Miller and Nies. Franklin and Ng characterized the incomplete Martin-Löf random sets in terms of tests formed by taking the difference of two c.e. sets [3]. Recently, Bienvenu, Hölzl, Miller and Nies showed that the incomplete Martin-Löf random sets are exactly those Martin-Löf random sets for which a particular density property fails [1]. Our proof combines this density property with the fact that if A is a K-trivial set and W_A is a bounded set of strings c.e. in A, then there exists a bounded c.e. set of strings W such that $W_A \subseteq W$. (A set of finite strings S is *bounded* if $\sum_{\sigma \in S} 2^{-|\sigma|} < \infty$.) This fact was first explicitly stated, in an even stronger form, by Simpson [9]. It is also implied by work of Miller, Kjos-Hanssen and Solomon [4].

The second direction is that every set that is not K-trivial is ML-cuppable. This proof of this direction is an oracle construction using Π^0_1 classes of positive

measure. This construction makes use of a result of Kučera that any Π^0_1 class of positive measure contains a tail of every Martin-Löf random [5].

References

[1] Laurent Bienvenu, Rupert Hölzl, Joseph S. Miller, and André Nies. The Denjoy alternative for computable functions. *preprint*.

[2] Rod G. Downey and Denis R. Hirschfeldt. *Algorithmic Randomness and Complexity*. Springer-Verlag, 2010.

[3] Johanna N. Y. Franklin and Keng Meng Ng. Difference randomness. *Proc. Amer. Math. Soc.*, 139(1):345–360, 2011.

[4] Bjørn Kjos-Hansen, Joseph S. Miller, and Solomon Reed. Lowness notions, measure and domination. *London Mathematical Society*, to appear.

[5] Antonín Kučera. Measure, Π^0_1 classes and complete extensions of PA. In H. D. Ebbinghaus, G. H. Müller, and G. E. Sacks, editors, *Recursion Theory Week. Proceedings of the Conference Held at the Mathematisches Forschungsinstitut in Oberwolfach, April 15-21, 1984*, volume 1141 of *Lecture Notes in Mathematics*, pages 245–259, Berlin, 1985. Springer.

[6] André Nies. Lowness properties and randomness. *Advances in Mathematics*, 197(1):274 – 305, 2005.

[7] André Nies. Non-cupping and randomness. *Proc. Amer. Math. Soc.*, 135(3):837–844, 2007.

[8] David B. Posner and Robert W. Robinson. Degrees joining to $\mathbf{0}'$. *J. Symbolic Logic*, 46(4):714–722, 1981.

[9] Stephen G. Simpson. Almost everywhere domination and superhighness. *MLQ Math. Log. Q.*, 53(4-5):462–482, 2007.

[10] Domenico Zambella. On sequences with simple initial segments. Technical Report ML-1990-05, The Institute for Logic, Language and Computation (ILLC), University of Amsterdam, 1990.

Department of Mathematics, University of California, Berkeley, CA 94720-3840.

SJT-HARDNESS AND PSEUDO-JUMP INVERSION

DANIEL TURETSKY, VICTORIA UNIVERSITY OF WELLINGTON

(JOINT WITH DAVID DIAMONDSTONE, ROD DOWNEY AND NOAM GREENBERG)

Jockusch and Shore [6] introduced the notion of a *pseudo-jump operator*, which is a map $J : 2^\omega \to 2^\omega$ with $J(A) = W_e^A$ for some e and $J(A) \geq_T A$ for A. The original example of a pseudo-jump operator is the Turing jump, which sends a set A to A'. However, nearly any construction of a c.e. set produces a pseudo-jump operator by defining $J(A)$ to be the result of the construction relativized to A (to ensure that $J(A) \geq_T A$, we can join the result with A).

Jockusch and Shore [6] proved the following result, known as *pseudo-jump inversion*:

Theorem 1. *For any pseudo-jump operator J, there is a non-computable c.e. set A with $J(A) \equiv_T \emptyset'$.*

A pseudo-jump operator is *increasing* if for all A, $J(A) >_T A$. Coles, Downey, Jockusch and LaForte [2] considered what other constructions were compatible with pseudo-jump inversion for increasing operators. They showed that any increasing pseudo-jump operator could be inverted to incomparable c.e. sets; that is, for any increasing pseudo-jump operator J, there are Turing incomparable c.e. sets A and B with $J(A) \equiv_T J(B) \equiv_T \emptyset'$.

Coles et al. then asked if pseudo-jump inversion was compatible with cone avoidance; that is, for any increasing pseudo-jump operator J, and any non-computable c.e. set C, is there an $A \not\geq_T C$ with $J(A) \equiv_T \emptyset'$? Downey and Greenberg [3] answered this question in the negative, using a natural pseudo-jump operator obtained from randomness involving tracing.

Tracing was introduced to computability theory by Terwijn and Zambella [8], who used it to characterize the degrees which are low for Schnorr randomness. Zambella observed that tracing also has a relationship to K-triviality, which was strengthened by Nies [7] and then later others [5, 1].

Definition 1. A *trace* for a partial function $f : \omega \to \omega$ is a sequence $\langle T_z \rangle_{z \in \omega}$ of finite sets with $f(z) \in T_z$ for all $z \in \mathrm{dom}(f)$.

A trace $\langle T_z \rangle_{z \in \omega}$ is c.e. if the T_z are uniformly c.e. sets.

Definition 2. An *order function* is a total, nondecreasing, unbounded function h with $h(0) > 0$.

If h is an order, $\langle T_z \rangle_{z \in \omega}$ is an *h-trace* if $|T_z| \leq h(z)$ for all z.

Definition 3 (Figuiera, Nies and Stephan [4])**.** A set A is called *jump-traceable (JT)* if every partial A-computable function has a c.e. h-trace for some computable order h.

For a computable order h, a set A is called *h-jump-traceable (h-JT)* if every partial A-computable function has a c.e. h-trace.

A set A is called *strongly jump-traceable (SJT)* if it is h-JT for every computable order h.

Figuiera et al. constructed a non-computable c.e. set which is SJT. This gives a natural pseudo-jump operator, which is the operator Downey and Greenberg used. Pseudo-jump inverting this SJT-operator gives a set A such that $\emptyset'$ looks SJT relative to A:

Definition 4. For a computable order h, a set A is *h-JT-hard* if every partial $\emptyset'$-computable function has an h-trace which is c.e. relative to A.

A set A is *SJT-hard* if it is h-JT-hard for every computable order h.

Downey and Greenberg showed that there is a non-computable c.e. set E which is computable from every c.e. SJT-hard set. Thus the SJT-operator cannot be pseudo-jump inverted outside of the cone above E. We strengthen this result, showing that there is a high c.e. set which is computable from every c.e. SJT-hard. In fact, for every computable order h, there is an h-JT hard c.e. set which is computable from every SJT-hard c.e. set.

References

[1] Peter Cholak, Rod Downey and Noam Greenberg. Strong jump-traceability. I. The computably enumerable case. *Adv. Math.*, 217(5):2045–2074, 2008.

[2] R. Cole, R. Downey, C. Jockusch and G. LaForte. Completing psudojump operators. *Ann. Pure Appl. Logic*, 136(3):297–333, 2005.

[3] R. Downey and N. Greenberg. Pseudo-jump inversion and SJT-hard sets. *Submitted.*

[4] Santiago Figueira, André Nies and Frank Stephan. Lowness properties and approximations of the jump. *Ann. Pure Appl. Logic*, 152(1-3):51–66, 2008.

[5] Rupert Hölzl, Thorsten Kräling and Wolfgang Merkle. Time-bounded Kolmogorov complexity and Solovay functions. Lecture Notes in Comput. Sci., 5734:392–402, 2009.

[6] Carl Jockusch Jr. and Richard Shore. Pseudojump operators. I. The r.e. case. *Trans. Amer. Math. Soc.*, 275(2):599–609, 1983.

[7] André Nies. Lowness properties and randomness. *Adv. Math.*, 197(1):274–305, 2005.

[8] Sebastiaan Terwijn and Domenico Zabella. Computational randomness and lowness. *J. Symbolic Logic*, 66(3):1199–1205, 2001.

ON THE INVERSION OF COMPUTABLE FUNCTIONS

MATHIEU HOYRUP

Abstract. Ergodic shift-invariant measures inherit many effective properties of the uniform measure: for instance, the frequency of 1's in a typical sequence converge effectively, hence it converges at every Schnorr random sequence; the convergence is robust to small violations of randomness [4]; every Martin-Löf random sequence has a tail in every effective closed set of positive measure ([1]). These properties are generally not satisfied by a non-ergodic measure, unless its (unique) decomposition into a combination of ergodic measures is effective. V'yugin [3] constructed a computable non-ergodic measure whose decomposition is not effective. This measure is a countable combination of ergodic measures. What happens for finite combinations? Is there a finitely but non-effectively decomposable measure?

We prove that the answer is positive: there exist two non-computable ergodic measures P and Q such that $P + Q$ is computable. Moreover, the set of pairs (P, Q) such that neither P nor Q is computable from $P + Q$ is large in the sense of Baire category.

This result can be generalized into a theorem about the inversion of computable functions, which gives sufficient conditions on a one-to-one computable function f that entail the existence of a non-computable x such that $f(x)$ is computable.

We also establish a stronger result ensuring the existence of a "sufficiently generic" x such that $f(x)$ is computable, in the spirit of Ingrassia's notion of p-genericity [2].

References

[1] Laurent Bienvenu, Adam Day, Ilya Mezhirov, and Alexander Shen. Ergodic-type characterizations of algorithmic randomness. In *Computability in Europe (CIE 2010)*, volume 6158 of *LNCS*, pages 49–58. Springer, 2010.

[2] M.A. Ingrassia. *P-genericity for Recursively Enumerable Sets*. University of Illinois at Urbana-Champaign, 1981.

[3] Vladimir V. V'yugin. Effective convergence in probability and an ergodic theorem for individual random sequences. *SIAM Theory of Probability and Its Applications*, 42(1):39–50, 1997.

[4] Vladimir V. V'yugin. Non-robustness property of the individual ergodic theorem. *Problems of Information Transmission*, 37(2):27–39, 2001.

THE STORY OF SUPERCONCENTRATORS – THE MISSING LINK

MICHAL KOUCKÝ

Abstract

In 60's and 70's directed graphs with strong connectivity property were linked to proving lower bounds on complexity of solving various computational problems. Graphs with strongest such property were named *superconcentrators* by Valiant [5]. An n-superconcentrator is a directed acyclic graph with n designated input nodes and n designated output nodes such that for any subset X of input nodes and any equal-sized set Y of output nodes there are $|X|$ vertex disjoint paths connecting the sets. Contrary to previous conjectures Valiant showed that there are n-superconcentrators with $O(n)$ edges thus killing the hope of using them to prove lower bounds on computation. His n-superconcentrators have depth $O(\log n)$.

Despite this setback, superconcentrators found their way into lower bounds in the setting of bounded-depth circuits. A bounded-depth circuit is a circuit where each gate (node) has an arbitrary fan-in (the number of incoming edges) and computes an arbitrary Boolean function of the incoming values; the depth of the circuit is bounded by a constant when one considers a family of such circuits for various input lengths. Chandra, Fortune and Lipton [1] used the then recent non-linear lower bounds of Dolev et al. [2] on the number of edges in *relaxed* superconcentrators of bounded-depth to prove non-linear lower bounds on the number of wires in bounded-depth circuits computing functions like addition of two integers represented in binary. A *relaxed* n-superconcentrator differs from the n-superconcentrator in that one requires at least $\delta \cdot |X|$ vertex disjoint paths on average between any two randomly chosen equal-sized sets X and Y of inputs and outputs, respectively. Here, δ is any constant such that $0 < \delta \leq 1$.

Both superconcentrators and relaxed superconcentrators were studied further to obtain optimal bounds on their size for all possible depth $d \geq 1$. Table 1 summarizes these bounds.

This could be the end of the story but one can naturally or at least formally consider graphs, that satisfy a connectivity property in-between superconcentrators and relaxed superconcentrators. Namely, one can require at least $\delta \cdot |X|$ vertex disjoint paths on average between *any* set X of inputs and an equal-sized *random* set Y of outputs, for a fixed constant $0 < \delta \leq 1$. Do graphs satisfying such connectivity property occur in nature? In our recent joint work with A. Gál, K. Hansen, P. Pudlák and E. Viola [3] we show that such connectivity property is required by circuits computing asymptotically good error-correcting codes. Thus similarly to relaxed superconcentrators there are natural functions that correspond to this definition.

Institute of Mathematics, The Academy of Science of the Czech Republic, Prague. Email: koucky@math.cas.cz.

In that work we also provide tight asymptotic bounds on the size of depth d graphs having this property. These bounds are different for depth $d = 2$ for all three connectivity properties. For larger depths they are asymptotically identical. The next table summarizes these bounds.

depth	$d = 2$	$d = 3$	$d = 2k$ or $d = 2k + 1$
superconc.	$\Theta(n(\log n)^2/\log\log n)$	$\Theta(n\log\log n)$	$\Theta(n\lambda_k(n))$
missing link	$\Theta(n(\log n/\log\log n)^2)$	$\Theta(n\log\log n)$	$\Theta(n\lambda_k(n))$
relaxed superconc.	$\Theta(n\log n)$	$\Theta(n\log\log n)$	$\Theta(n\lambda_k(n))$

TABLE 1. The number of edges in depth d superconcentrators. Here, $\lambda_1(n) = \lceil \log n \rceil$, $\lambda_{i+1}(n) = \lambda_i^*(n)$, and the $*$ operation gives how many times one has to iterate the function λ_i to reach a value at most 1 from the argument n.

The talk will provide an exposition of this area.

REFERENCES

[1] A. K. Chandra, S. Fortune, and R. J. Lipton. Lower bounds for constant depth circuits for prefix problems. In *10th Colloquium on Automata, Languages and Programming (ICALP'83)*, volume 154 of *LNCS*, pages 109–117. Springer, 1983.

[2] D. Dolev, C. Dwork, N. Pippenger, and A. Wigderson. Superconcentrators, generalizers and generalized connectors with limited depth. In *15th Annual ACM Symposium on Theory of Computing (STOC'83)*, pages 42–51. ACM Press, 1983.

[3] A. Gál, K.A. Hansen, M. Koucký, P. Pudlák, and E. Viola. Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates. In *44th Annual ACM Symposium on Theory of Computing (STOC'12)*, pages 479–494. ACM Press, 2012.

[4] P. Pudlák. Communication in bounded depth circuits. *Combinatorica*, 14(2):203–216, 1994.

[5] L. Valiant. On non-linear lower bounds in computational complexity. In *7th Annual ACM Symposium on Theory of Computing (STOC'75)*, pages 45–53. ACM Press, 1975.

ALAN TURING IN THE TWENTY-FIRST CENTURY: NORMAL NUMBERS, RANDOMNESS, AND FINITE AUTOMATA

JACK H. LUTZ
DEPARTMENT OF COMPUTER SCIENCE
IOWA STATE UNIVERSITY
AMES, IA 50014 USA

We discuss ways in which Turing's then-unpublished "A Note on Normal Numbers" foreshadows and can still guide research in our time.

This research was supported in part by NSF Grant 0652569. Part of the work was done while the author was on sabbatical at Caltech and the Isaac Newton Institute for Mathematical Sciences at the University of Cambridge.

DEMUTH RANDOMNESS AND ITS VARIANTS

ANDRÉ NIES
UNIVERSITY OF AUCKLAND, NEW ZEALAND

A Demuth test is like a Martin-Löf test with the passing condition to be out of infinitely many components; the strength of the test is enhanced by the possibility to exchange the n-th component of the test a computably bounded number of times. Demuth introduced Demuth randomness of reals in 1982, and showed that the Denjoy alternative for Markov computable functions holds at any such real. In [2] we proved that Demuth's hypothesis is in fact too strong: difference randomness (i.e., ML-randomness together with incompleteness) of the real already suffices. However, Demuth randomness now plays an important role in the interaction of computability and randomness. The basic relevant fact here is that a Demuth random set can be below the halting problem.

In [1] we characterized lowness for Demuth randomness by a property called BLR-traceability, in conjunction with being computably dominated. The low for Demuth random sets form a proper subclass of the computably traceable sets used by Terwijn and Zambella to characterize lowness for Schnorr randomness.

The covering problem asks whether each K-trivial set A is Turing below a difference random set Y. Combining work of Kucera and Nies [3] with results of Downey, Diamondstone, Greenberg and Turetsky gives an affirmative answer to an analogous question: a set A is strongly jump traceable if and only if it is below a Demuth random set Y.

In recent work, Bienvenu, Greenberg, Kucera, Nies, and Turetsky introduced a weakening of Demuth randomness called Oberwolfach randomness. They used it to build a "smart" K-trivial set A: it is difficult to cover in that any Martin-Löf random set Y above A must be LR-hard.

References

[1] Bienvenu, Downey, Greenberg, Nies, and Turetsky. Characterizing lowness for Demuth Randomness. Submitted.

[2] Bienvenu, Hoelzl, Miller, and Nies. The Denjoy alternative for computable functions. Proceedings of STACS 2012.

[3] Kucera, A. and Nies, A. Demuth randomness and computational complexity. Annals of Pure and Applied Logic 162 (2011) 504-513.

TOPOLOGICAL ARGUMENTS FOR KOLMOGOROV COMPLEXITY

ALEXANDER SHEN

Let us start with an example. Consider a string x that has complexity n (we consider plain complexity $C(x)$, but this does not matter for now). We want to find a string y such that $C(x|y) \approx n/2$. This can be done as follows: consider the shortest description p of x; it has length n; let y be the first half of this description. Then it is easy to check that $C(x|y) = n/2 + O(\log n)$.

However, if we want $C(x|y)$ to be close to $n/2$ with (maximal possible) precision $O(1)$, one needs a different argument, and it is not difficult to find one. Let us start with $y = x$ (when $C(x|y) \approx 0$) and delete bits (say, at the end) one by one until we get $y = \Lambda$ (empty string) with $C(x|y) \approx n$). When the last bit of y is deleted, the conditional complexity $C(x|y)$ changes by at most $O(1)$, so it cannot cross the threshold $n/2$ without visiting $O(1)$-neighborhood of $n/2$.

Topological arguments of this type can be used in two (and more) dimensions, though they become less trivial: one needs to replace the indermediate value theorem by some other topological fact (the non-triviality of the n-th homotopy group of n-dimensional sphere). We provide two examples.

1. Vyugin's result and its extensions

M. Vyugin [1] has shown that for every n and for every string x with $C(x) \geq 2n + O(1)$ one can find a string y such that both conditional complexities $C(x|y)$ and $C(y|x)$ are equal to $n + O(1)$. This is proved with a (rather ingenious) game argument. As we shall see in this paper, the condition $C(x) \geq 2n$ is stronger than necessary; it is enough to assume that $C(x) \geq n + c\log n$ for some c. This can be shown (unless $C(x)$ is not very large) by a simple topological argument. (The game argument still seems to be necessary if $C(x)$ is really big compared to n.)

Similar reasoning allows us to construct y such that both complexities $C(x|y)$ and $C(y|x)$ has prescibed values with $O(1)$-precision, even if those values are different. (This question was discussed in Vyugin's paper [1], but no positive result of this type is given there except for the already mentioned case $m = n + O(1)$.) Again we need some restrictions that guarantee that prescribed values are not unreasonable large or small. Here is the exact statement.

Theorem 1. *Let P be some polynomial. There exists a constant c such that for every string x and for every integers m, n such that*

- $n + c\log n \leq C(x) \leq P(n)$;
- $c\log n \leq m \leq P(n)$,

there exists a string y such that $|C(x|y) - n| \leq c$ and $|C(y|x) - m| \leq c$.

LIRMM, CNRS and University of Montpellier 2, France. On leave from IITP RAS, Moscow. Supported by ANR NAFIT-008 grant.

(Since $C(x|y)$ does not exceed $C(x)$, we need $C(x)$ to be greater than n; the "safety margin" of size $O(\log n)$ is assumed in the statement. We also require m and $C(x)$ to be polynomially bounded.)

2. Decreasing complexity by using an oracle

Let a and b be two strings. They have some complexities $C(a)$ and $C(b)$. If a third string t is given, we can consider the conditional complexities $C(a|y)$ and $C(b|y)$ which are (in general) smaller that $C(a)$ and $C(b)$. Now the question: can we describe the pairs $(C(a|y), C(b|y))$ that can be obtained by choosing an appropriate value of y? We answer this question for the case when a and b have small mutual information, and the answer is simple: we can get an arbitrary pair (α, β) such that $0 \le \alpha \le C(a)$ and $0 \le \beta \le C(b)$ and α, β are not too close to the endpoints of the corresponding intervals (the distance is big compared to the logarithms of complexities and to the mutual information).

Theorem 2. *For some constant c the following statement holds: for every two strings a, b and for every integers α, β such that*

- $\alpha, \beta \ge c(\log C(a) + \log C(b) + I(a:b))$;
- $\alpha \le C(a) - c(\log C(a) + \log C(b) + I(a:b))$;
- $\beta \le C(b) - c(\log C(a) + \log C(b) + I(a:b))$,

there exists a string y such that $|C(a|y) - \alpha| \le c$ and $|C(b|y) - \beta| \le c$.

Note that this statement is evidently true if instead of $O(1)$-precision we are satisfied with $O(\log C(a) + \log C(b) + I(a:b))$-precision. Indeed, we can consider the shortest descriptions p and q for a and b and then let $y = (p', q')$ where p' is p without α last bits, q' is q without β last bits; the information distance between a, p and between b, q is logarithmic, p' and q' are independent with our precision, etc.

Acknowledgements. The author is grateful to Laurent Bienvenu who suggested to write down this simple argument, Tarik Kaced, Andrei Romashchenko and all the colleagues in Escape/NAFIT/Kolmogorov seminar team.

References

[1] M. Vyugin, Information distances and conditional complexities, *Theoretical Computer Science*, **271**(1–2): 145–150 (2002).

Propagation of partial randomness

Stephen G. Simpson
Department of Mathematics
Pennsylvania State University
http://www.math.psu.edu/simpson/

May 6, 2012

Let X be an infinite sequence of 0's and 1's, i.e., $X \in \{0,1\}^{\mathbb{N}}$. Even if X is not Martin-Löf random, we can nevertheless quantify the amount of *partial randomness* which is inherent in X. Many researchers including Calude, Hudelson, Kjos-Hanssen, Merkle, Miller, Reimann, Staiger, Tadaki, and Terwijn have studied partial randomness. We now present some new results due to Higuchi, Hudelson, Simpson and Yokoyama concerning *propagation of partial randomness.* Our results say that if X has a specific amount of partial randomness, then X has an equal amount of partial randomness relative to certain Turing oracles. More precisely, let KA denote a priori Kolmogorov complexity, i.e., $\mathrm{KA}(\sigma) = -\log_2 m(\sigma)$ where m is Levin's universal left-r.e. semimeasure. Note that KA is similar but not identical to the more familiar prefix-free Kolmogorov complexity. Given a computable function $f : \{0,1\}^* \to [0,\infty)$, we say that $X \in \{0,1\}^{\mathbb{N}}$ is strongly f-random if $\exists c \forall n\, (\mathrm{KA}(X{\restriction}\{1,\ldots,n\}) > f(X{\restriction}\{1,\ldots,n\}) - c)$. Two of our results read as follows. Theorem 1. Assume that X is strongly f-random and Turing reducible to Y where Y is Martin-Löf random relative to Z. Then X is strongly f-random relative to Z. Theorem 2. Assume that $\forall i\, (X_i$ is strongly f_i-random). Then, we can find a PA-oracle Z such that $\forall i\, (X_i$ is strongly f_i-random relative to $Z)$. We also show that Theorems 1 and 2 fail badly with KA replaced by KP = prefix-free complexity.

PREFIX AND PLAIN KOLMOGOROV COMPLEXITY CHARACTERIZATIONS OF 2-RANDOMNESS: SIMPLE PROOFS

BRUNO BAUWENS

Joseph Miller [3] and independently Andre Nies, Frank Stephan and Sebastian Terwijn [5] gave a complexity characterization of 2-random sequences in terms of plain Kolmogorov complexity $C(\cdot)$: they are sequences that have infinitely many initial segments with $O(1)$-maximal plain complexity (among the strings of the same length).

Later Miller [4] (see also [2]) showed that prefix complexity $K(\cdot)$ can be also used in a similar way: a sequence is 2-random if and only if it has infinitely many initial segments with $O(1)$-maximal *prefix* complexity (which is $n + K(n)$ for strings of length n).

The known proofs of these results are quite involved; we provide simple direct proofs for both of them.

In [3] Miller also gave a quantitative version of the first result: the $0'$-randomness deficiency of a sequence ω equals $\liminf_n [n - C(\omega_1 \ldots \omega_n)] + O(1)$. (Our simplified proof also can be used to prove this quantitative version.) We show (and this seems to be a new result) that a similar quantitative result is true also for prefix complexity: $0'$-randomness deficiency $d^{0'}(\omega)$ equals also $\liminf_n [n + K(n) - K(\omega_1 \ldots \omega_n)] + O(1)$. This completes the picture:

$$\begin{aligned} d^{0'}(\omega) &= \sup_n \left[n - K^{0'}(\omega_1 \ldots \omega_n) \right] + O(1) \\ &= \liminf_n \, [n - C(\omega_1 \ldots \omega_n)] + O(1) \\ &= \liminf_n \, [n + K(n) - K(\omega_1 \ldots \omega_n)] + O(1) \,. \end{aligned}$$

References

[1] L. Bienvenue, A. Muchnik, A. Shen, and N. Vereshchagin. Limit complexities revisited [once more]. *ArXiv e-prints*, April 2012.

[2] R.G. Downey and D.R. Hirschfeldt. *Algorithmic Randomness and Complexity*. Theory and Applications of Computability. Springer, 2010.

[3] J.S. Miller. Every 2-random real is Kolmogorov random. *Journal of Symbolic Logic*, 69(3):907–913, 2004.

[4] J.S. Miller. The K-degrees, low for K-degrees, and weakly low for K sets. *Notre Dame Journal of Formal Logic*, 50(4):381–391, 2009.

[5] A. Nies, F. Stephan, and S.A. Terwijn. Randomness, relativization and turing degrees. *The Journal of Symbolic Logic*, 70(2), 2005.

Date: June 4, 2012.

Instituto de Telecomunicações, Faculdade de Ciência da Universidade do Porto. Supported by the Portuguese science foundation FCT (SFRH/BPD/75129/2010); partially supported by CSI^2 (PTDC/EIA-CCO/099951/2008) and NAFIT ANR-08-EMER-008-01 projects.
E-mail: `Brbauwens (a) gmail dot com`. The simple proof for the C-characterization is given in [1] and was much inspired by the simplified proofs of Nikolay (Kolia) Vereshchagin and Laurent Bienvenu. The author is also grateful to Alexander (Sasha) Shen for useful discussions.

NORMALITY AND DIFFERENTIABILITY

VERÓNICA BECHER AND PABLO ARIEL HEIBER

We translate to the world of functions computable by finite automata the classical theorem of numerical analysis establishing that every non-decreasing real valued continuous function is almost everywhere differentiable. We obtain a characterization of *normality to a given base* in terms of differentiability of non-decreasing functions computable by injective finite-state transducers (finite automata with input and output). Our theorem was motivated by the recent work of Brattka, Miller and Nies [2] who proved the counterpart result for real valued functions computable by Turing machines, yielding a characterization of the property of computable randomness.

Let us recall that Borel's original definition of normality [3] is equivalent to the following simpler one [4].

Definition. A real number r is *simply normal to a given base* b if each digit in $\{0, 1, ..., b-1\}$ occurs with the same limiting frequency $1/b$ in the expansion of r in base b. A number is *normal to base* b if it is simply normal to the each base b^i, for every positive integer i.

We write $\mathbf{b} = \{0, ..., b-1\}$ for the set of digits in base b. $\mathbf{b}^*$ and $\mathbf{b}^\omega$ denote, respectively, the set of finite and infinite sequences of digits in base b. Let $\mathrm{conv}_b : \mathbf{b}^\omega \to [0,1]$ and $\mathrm{conv}_b^{-1} : [0,1] \to \mathbf{b}^\omega$ be the usual maps between reals and their expansions in base b, $\mathrm{conv}_b(x) = \sum_{n=1}^{n} b^{-n} x[n]$ and $\mathrm{conv}_b^{-1}(x) = \prod_{n=1}^{n} \lfloor b^n x \rfloor - b\lfloor b^{n-1} x \rfloor$, where $\prod$ stands for concatenation.

Definition. (1) A *finite-state transducer* is a 5-uple $C = \langle b, \mathcal{Q}, q_0, \delta, o \rangle$, where $\mathcal{Q}$ is a finite set of states, $q_0 \in \mathcal{Q}$ is the initial state, $\delta : \mathcal{Q} \times \mathbf{b} \to \mathcal{Q}$ is the transition function and $o : \mathcal{Q} \times \mathbf{b} \to \mathbf{b}^*$ is the output function. A finite-state transducer processes the input digits according to the current state q. When a digit $d \in \mathbf{b}$ is read, the automaton moves to state $\delta(q, d)$ and outputs $o(q, d)$. The extension of δ and o to process strings are $\delta^* : \mathcal{Q} \times \mathbf{b}^* \to \mathcal{Q}$ and $o^* : \mathcal{Q} \times \mathbf{b}^* \to \mathbf{b}^*$ such that, for $d \in \mathbf{b}$, $s \in \mathbf{b}^*$ and λ the empty string, $\delta^*(q, \lambda) = q$, $\delta^*(q, ds) = \delta^*(\delta(q, d), s)$, and $o^*(q, \lambda) = \lambda$, $o^*(q, ds) = o(q, d) o^*(\delta(q, d), s)$. The extension of o to infinite sequences $o^\omega : \mathcal{Q} \times \mathbf{b}^\omega \to \mathbf{b}^\omega$ is $o^\omega(q, dx) = o(q, d) o^\omega(\delta(q, d), x)$.

(2) The function $f_C : \mathbf{b}^\omega \to \mathbf{b}^\omega$ computed by $C = \langle b, \mathcal{Q}, q_0, \delta, o \rangle$ is $f_C(x) = o^\omega(q_0, x)$.

(3) A function $f : \mathbf{b}^\omega \to \mathbf{b}^\omega$ is *finite-state computable* when $f = f_C$ for some finite-state transducer C. A function $f : \mathbf{b}^\omega \to [0,1]$ is finite-state computable when $f = \mathrm{conv}_b \circ f_C$ for some finite-state transducer C. A function $f : [0,1] \to [0,1]$ is *finite-state computable in base* b if $f = \mathrm{conv}_b \circ f_C \circ \mathrm{conv}_b^{-1}$ for some finite-state transducer C such that for each $s \in \mathbf{b}^*$, $\mathrm{conv}_b(f_C(s01^\omega)) = \mathrm{conv}_b(f_C(s10^\omega))$.

vbecher@dc.uba.ar, pheiber@dc.uba.ar, Universidad de Buenos Aires, Argentina.

From the above definition it follows that every finite-state computable function is continuous for the usual topologies on $\mathbf{b}^\omega$ and $\mathbb{R}$.

We consider the lexicographical ordering of infinite sequences in $\mathbf{b}^\omega$ and define a natural notion of differential for non-decreasing functions $\mathbf{b}^\omega \to \mathbf{b}^\omega$. For each string $s \in \mathbf{b}^*$, we write $A_s = \{sx : x \in \mathbf{b}^\omega\}$ for the set of infinite sequences that start with s.

Definition. The differential of a non-decreasing function $f : \mathbf{b}^\omega \to \mathbf{b}^\omega$ at x is

$$Df(x) = \lim_{n\to\infty} \frac{\mu(f(A_{x\restriction n}))}{\mu(A_{x\restriction n})} = \lim_{n\to\infty} b^n \mu(f(A_{x\restriction n})).$$

We say that f is differentiable at x if the limit $Df(x)$ converges to a finite value.

The differential of a non-decreasing finite-state computable function bounds how many initial digits of the input fix the initial digits of the output.

Proposition. *Let $f : \mathbf{b}^\omega \to \mathbf{b}^\omega$ be a non-decreasing finite-state computable function differentiable at x. If $Df(x) \neq 0$ then, for sufficiently large n, $f(A_{x\restriction n}) \subseteq A_{f(x)\restriction n - \log Df(x)}$. If $Df(x) = 0$ then, for each $c \in \mathbb{N}$ and sufficiently large n, $f(A_{x\restriction n}) \subseteq A_{f(x)\restriction n+c}$.*

Now we can formulate the announced result.

Theorem. *For a real $r \in [0,1]$, the following are equivalent:*

(1) *r is normal to base b.*
(2) *Every non-decreasing function $f : \mathbf{b}^\omega \to \mathbf{b}^\omega$ finite-state computable is differentiable at the expansion of r in base b.*
(3) *Every non-decreasing function $f : [0,1] \to [0,1]$ finite-state computable in base b is differentiable at r.*

The proof uses the characterization of normal sequences as those incompressible by injective finite-state transducers (lossless finite-state compressors) [7, 6, 5, 1]. Substantial adaptation is needed to deal with the non-decreasing condition.

References

[1] Becher, V., Heiber, P. 2012. Normal Numbers and Finite Automata. *Submitted.*

[2] Brattka, V., Miller, J.S. and Nies, A. 2011. Randomness and differentiability. *Submitted.* Available at `http://arxiv.org/abs/1104.4465`

[3] Borel, Émile. 1909. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27:247–271.

[4] Bugeaud, Yann. 2012. *Distribution Modulo One and Diophantine Approximation.* Cambridge University Press.

[5] Bourke, C., Hitchcock, J., Vinodchandran, N. 2005. Entropy rates and finite-state dimension. *Theoretical Computer Science*, 349 (3): 392–406.

[6] Dai, L., J., Lutz, J., Mayordomo, E. 2004. Finite-state dimension. *Theoretical Computer Science*, 310:1–33.

[7] Schnorr, Claus-Peter, Stimm, H. 1972. Endliche Automaten und Zufallsfolgen. *Acta Informatica* 1: 345–359.

COMPUTABLY ENUMERABLE PARTIAL ORDERS

PETER A. CHOLAK, DAMIR D. DZHAFAROV, NOAH SCHWEBER,
AND RICHARD A. SHORE

Abstract. We study the degree spectra and reverse-mathematical applications of computably enumerable and co-computably enumerable partial orders. We formulate versions of the chain/antichain principle and ascending/descending sequence principle for such orders, and show that the latter is strictly stronger than the latter. We then show that every $\emptyset'$-computable structure (or even just of c.e. degree) has the same degree spectrum as some computably enumerable (co-c.e.) partial order, and hence that there is a c.e. (co-c.e.) partial order with spectrum equal to the set of nonzero degrees. A copy of the submitted paper can be found at http://www.nd.edu/~cholak/papers/ceorderings.pdf.

Department of Mathematics, University of Notre Dame, Notre Dame, Indiana 46556 U.S.A.
E-mail address: cholak@nd.edu

Department of Mathematics, University of Notre Dame, Notre Dame, Indiana 46556 U.S.A.
E-mail address: ddzhafar@nd.edu

Department of Mathematics, University of California, Berkeley, California 94720 U.S.A.,
E-mail address: schweber@math.berkeley.edu

Department of Mathematics, Cornell University, Ithaca, NY 14853 U.S.A.,
E-mail address: shore@math.cornell.edu

The authors are grateful to Julia Knight for helpful comments. This research was partly conducted while Dzhafarov and Shore were visiting the Institute for Mathematical Sciences at the National University of Singapore in 2011, with funding from the John Templeton Foundation. Cholak was partially supported by NSF grant DMS-0800198, Dzhafarov by an NSF Postdoctoral Fellowship, and Shore by NSF grant DMS-0852811.

TRANSLATING THE CANTOR SET BY A RANDOM

JASON TEUTSCH

I will discuss the constructive dimension of points in random translates of the Cantor set. The Cantor set "cancels randomness" in the sense that some of its members, when added to Martin-Löf random reals, identify a point with lower constructive dimension than the random itself. In particular, we find the Hausdorff dimension of the set of points in a Cantor set translate with a given constructive dimension.

More specifically, let $\mathcal{C}$ denote the standard middle third Cantor set, and for each real α let $\mathcal{E}_\alpha$ consist of all real numbers with constructive dimension α. Our result is the following.

Theorem. *If $1 - \log 2/\log 3 \leq \alpha \leq 1$ and r is a Martin-Löf random real, then the Hausdorff dimension of the set $(\mathcal{C} + r) \cap \mathcal{E}_\alpha$ is $\alpha - (1 - \log 2/\log 3)$.*

From this theorem we obtain a simple relation between the effective and classical Hausdorff dimensions of this set; the difference is exactly 1 minus the dimension of the Cantor set. We conclude that many points in the Cantor set additively cancel randomness.

On the surface, the theorem above describes a connection between algorithmic randomness and classical fractal geometry. Less obvious is its relationship to additive number theory. In 1954, G. G. Lorentz proved the following statement.

Lorentz's Lemma. *There exists a constant c such that for any integer k, if $A \subseteq [0, k)$ is a set of integers with $|A| \geq \ell \geq 2$, then there exists a set of integers $B \subseteq (-k, k)$ such that $A + B \supseteq [0, k)$ with $|B| \leq ck\frac{\log \ell}{\ell}$.*

Given a Martin-Löf random real r, I will show how Lorentz's Lemma can be used to identify a point $x \in \mathcal{C}$ such that the constructive dimension of $x + r$ is close to $1 - \log 2/\log 3$, which is as small as it can possibly be.

This talk is based on joint work with Randy Dougherty, Jack Lutz, and Dan Mauldin.

Penn State University, teutsch@cse.psu.edu .

KOLMOGOROV COMPLEXITY AND FOURIER ASPECTS OF BROWNIAN MOTION

WILLEM L. FOUCHÉ
DEPARTMENT OF DECISION SCIENCES,
SCHOOL OF ECONOMICAL SCIENCES
UNIVERSITY OF SOUTH AFRICA, PO BOX 392, 0003 PRETORIA, SOUTH AFRICA
FOUCHWL@GMAIL.COM

Abstract

It is well-known that the notion of randomness, suitably refined, goes a a long way in dealing with the tension between the "incompatability of shortest descriptions and of effecting the most-economical algorithmical processing" Manin(2006). In this work, we continue to explore this interplay between short descriptions and randomness in the context of Brownian motion and its associated geometry. In this way one sees how random phenomena associated with the geometry of Brownian motion, are implicitly enfolded in each real number which is complex in the sense of Kolmogorov. These random phenomena range from fractal geometry, Fourier analysis and non-classical noises in quantum physics.

Countable dense random sets arise naturally in the theory of Brownian motion, in non-classical noises and the understanding of percolation phenomena in statistical physics. It is an interesting fact that the study of countable dense random sets quite naturally brings one in contact with studying random processes over spaces which are not even Polish. One has to do probability theory over orbit spaces under the action of the group S_∞, which is the symmetry group of a countable set, on the space of all injections of $\mathbb{N}$ into the unit interval. These are examples of what Kechris (1999) referred to as singular spaces of Borel cardinality F_2.

In 2006 Tsirelson developed a very powerful approach to random processes over these singular spaces and his results imply that the Kechris-singularity manifests in very concrete and interesting statistical properties of countable dense random sets and new aspects of Brownian motion.

Tsirelson shows that the minimizers of a Browian motion are instances of so-called stationary local random dense countable sets over the white noise and that they play a pivotal role in the understanding of non-classical noises.

This work suggested to the author the problem of constructing the minimizers of Brownian motion directly from an unbiased coin-tossing experiment. This can be seen as an extension of my work (2000) where a generic Brownian motion was constructed from a generic point in the unit interval. We shall again adopt the viewpoint of Kolmogorov complexity to define what we mean by the word generic. In this way, we shall be able to find Σ^0_3 definitions, within the arithmetical hierarchy, for countable dense random sets, which can be considered to be "generic" countable dense sets of reals and moreover symmetrically random over white noise. We provide an explicit computable enumeration of the elements of such sets relative to

Kolmogorov-Chaitin-Martin-Löf random real numbers. This opens the way to relate certain non-classical noises to Kolmogorov complexity. For example, the work of the present work enables one to represent Warren's splitting noise directly in terms of infinite binary strings which are Kolmogorov-Chaitin-Martin-Löf random.

We discuss the images of certain Π^0_2 perfect sets of Hausdorff dimension zero under a complex oscillation (which is also known as an algorithmically random Brownian motion). We have given a sketch in the extended abstract in (2009) of a proof that there are instances of such sets where such images under complex oscillations have elements all of which are linearly independent over the field of rational numbers. In Fourier analysis, these sets are called sets of independence. We shall discuss a generalisation of this result and show in fact that one can obtain sets via complex oscillations which are linearly independent over the field of recursive real numbers. Moreover, all the elements in these images are non-computable.

ERGODIC THEORY AND STRONG RANDOMNESS NOTIONS

JOHANNA N.Y. FRANKLIN AND HENRY TOWSNER
DEPARTMENT OF MATHEMATICS
196 AUDITORIUM ROAD
UNIVERSITY OF CONNECTICUT, U-3009
STORRS, CT 06269-3009
USA
JOHANNA.FRANKLIN@UCONN.EDU, HENRY.TOWSNER@UCONN.EDU

There has been a great deal of interest recently in the connection between algorithmic randomness and ergodic theory, which naturally leads to the question of how much one can say if the transformations in question need not be ergodic. We have essentially reversed a result of V'yugin and shown that if an element of the Cantor space is not Martin-Löf random, then there is a computable function f and a computable transformation $T : 2^\omega \to 2^\omega$ for which this element is not typical with respect to the ergodic theorem. More recently, we have shown that every weakly 2-random element of the Cantor space is typical with respect to the ergodic theorem for every lower semicomputable function f and computable transformation $T : 2^\omega \to 2^\omega$. I will explain the proof of the latter result and discuss the technical difficulties present in producing a full characterization.

(ALMOST) LOWNESS FOR K AND FINITE SELF-INFORMATION

IAN HERBERT

The prefix-free Kolmogorov complexity K of a finite string σ is the length of the shortest program that outputs σ, and can be used as a measure of the information content of σ. The mutual information of two finite strings, σ and τ, can be given by $K(\sigma) + K(\tau) - K(\sigma, \tau)$, where $K(\sigma, \tau) = K(\langle \sigma, \tau \rangle)$ for some standard pairing function $\langle \cdot\ ,\ \cdot \rangle$. Levin [1] has proposed an extension of this concept to the infinite case: for $A,\ B \in 2^\omega$ the mutual information of A and B is

$$I(A : B) = \log_2 \sum_{\sigma,\tau \in 2^{<\omega}} 2^{K(\sigma) - K^A(\sigma) + K(\tau) - K^B(\tau) - K(\sigma,\tau)},$$

where $K^A(\sigma)$ and $K^B(\tau)$ are the prefix-free Kolmogorov complexities of σ and τ relative to A and B, respectively. In the case where A and B are finite, this coincides up to an additive constant with the previous definition. One way of thinking of this definition is to treat $K(\sigma) - K^A(\sigma)$ as a measure of how much A 'knows' about σ; if σ has 10 bits of information, but A thinks σ has only 7 bits of information, then A has 3 bits of information about σ. Similarly, we can think of $K(\tau) - K^B(\tau)$ as a measure of how much B 'knows' about τ and $K(\sigma, \tau)$ as a measure of how far σ is from τ. Then each term of this sum measures how much information A has about σ and B has about τ, giving more weight to pairs (σ, τ) that are closely related.

A real A is said to have *finite self-information* if $I(A : A) < \infty$. It is clear that any low for K real (which has $K(\sigma) \leq K^A(\sigma) + c$ for all σ and some c independent of σ) has finite self-information, and relatively easy to show that any real that computes $0'$ does not. Levin posed the question as to whether the lows for K were exactly the reals with finite self-information, and Hirschfeldt and Weber [2] showed that there is a non-low-for-K real with finite self-information. There remained the question of how 'close' these two concepts were. The reals that are low for K are all Δ^0_2 and they form a countable ideal. We show that there is a perfect Π^0_1 class of reals with finite self-information, so there are uncountably many and thus they are not all Δ^0_2. Moreover, the Π^0_1 class can be constructed so that any real above $0'$ is Turing-equivalent to the join of two reals from the class, so they do not form an ideal.

The technique used to construct the Π^0_1 class is more general and in fact, given any Δ^0_2 order $f : 2^{<\omega} \to \mathbb{N}$ (i.e nondecreasing and unbounded with respect to the $\preceq$ partial order on $2^{<\omega}$), it can be used to construct a similar perfect Π^0_1 class of reals A all satisfying $K(\sigma) \leq K^A(\sigma) + f(\sigma) + c$ for all σ and some constant c (so reals that are low for K 'up to' f). Different choices of f can be used to give perfect classes of interesting types of reals. For example, $f(\sigma) = \log |\sigma|$ gives such a perfect Π^0_1 class of reals that are low for both effective Hausdorff and effective packing dimensions. Note that it follows from a result of Baartse and Barmpalias [3] that there is a Δ^0_3 order function $g : 2^{<\omega} \to \mathbb{N}$ such that any A with $K(\sigma) \leq^+ K^A(\sigma) + g(\sigma)$ for all σ

is in fact low for K, so it is not possible in general to get perfect classes for more complicated orders.

Another interesting aspect of the 'almost' lowness for K notion is that the classical equivalence between lowness for K and K-triviality (a real A is K-trivial if $K(A\restriction_n) \leq K(n) + c$ for all $n \in \mathbb{N}$ and some c independent of n) breaks down in the 'almost' case. In particular, there is a recursive order $f : 2^{<\omega} \to \mathbb{N}$ and a real A such that for all Δ^0_2 orders $g : \mathbb{N} \to \mathbb{N}$, $K(A\restriction_n) \leq^+ K(n) + g(n)$ (here the constant obviously depends on g) but $\forall\sigma\ K(\sigma) \leq^+ K^A(\sigma) + f(\sigma)$ fails to hold. That is, A is K-trivial 'up to' any Δ^0_2 order g but not low for K 'up to' f, which is only recursive.

On a philosophical note, the existence of so many reals with finite self-information that do not have finite information in the traditional sense (i.e. are not low for K) might be seen as evidence that this definition of mutual information is not the right one. However, we would argue that self-information should not be thought of as capturing the actual information content of a real, but rather the second-order notion of the information that a real has about itself (or its own information). Given that in general a real cannot effectively find the strings about which it has information, it seems reasonable for there to be reals with infinite information but only finitely much information about that information.

References

[1] Levin, L. A. Laws on the conservation (zero increase) of information, and questions on the foundations of probability theory. *Problemy Peredači Informacii 10*, 3 (1974), 30–35.

[2] Hirschfeldt, D. R., and Weber, R. Finite self-information. To appear.

[3] Baartse, M., and Barmpalias, G. On the gap between trivial and nontrivial initial segment prefix-free complexity. To appear.

SCHNORR TRIVIALITY IS EQUIVALENT TO BEING A BASIS FOR SCHNORR RANDOMNESS

KENSHI MIYABE

We present some new characterizations of Schnorr triviality. The well-known notion of K-triviality is defined using complexity K via a prefix-free machine, with which Martin-Löf randomness has a characterization. In a similar manner, Schnorr triviality is defined using complexity via a computable measure machine, with which Schnorr randomness has a characterization. Further, we have a characterization of Schnorr randomness via decidable prefix-free machine. Hence, we should also have a characterization of Schnorr triviality using complexity via a decidable prefix-free machine.

Definition 1. *A set $A \in 2^\omega$ is called* weakly decidable prefix-free machine reducible *to a set $B \in 2^\omega$ (denoted by $A \leq_{\mathrm{wdm}} B$) if for each decidable prefix-free machine M and a computable order g, there exists a decidable prefix-free machine N such that*

$$(\exists d)(\forall n) K_N(A \upharpoonright n) \leq K_M(B \upharpoonright n) + g(n) + d.$$

It can be clearly observed that the relation $\leq_{\mathrm{wdm}}$ is reflexive and transitive. This reducibility has a strong connection with Schnorr randomness.

Theorem 2 (Bienvenu and Merkle [1])**.** *A set X is Schnorr random iff*

$$(\exists d)(\forall n) K_M(X \upharpoonright n) \geq n - g(n) - d$$

for all decidable prefix-free machines M and all computable orders g.

Theorem 3. *If a set A is Schnorr random and $A \leq_{\mathrm{wdm}} B$, then B is Schnorr random.*

Definition 4. *We say that a set A is* weakly trivial for decidable prefix-free machines *if A is weakly decidable prefix-free machine reducible to $\emptyset$.*

Theorem 5. *A set is Schnorr trivial iff it is weakly trivial for decidable prefix-free machines.*

It should be noted that numerous characterizations of Schnorr triviality have the following form: for any computable object, there exists another computable object such that the real is in some object. By defining a basis for Schnorr randomness in a similar manner, we can show the equivalence to Schnorr triviality while Franklin and Stephan [2] showed that there exists a Schnorr trivial set that is not truth-table reducible to any Schnorr random set. Further, it should be noted that Franklin, Stephan and Yu [3] studied a base for Schnorr randomness, which is however a notion different from the one considered in this study.

At the same time, we also consider a basis for tt-reducible randomness. For the definition of tt-reducible randomness, refer to [4].

Research Institute for Mathematical Sciences, Kyoto University, kmiyabe@kurims.kyoto-u.ac.jp.

Definition 6. *Let d be a tt-reducible martingale. Then, a set X is A-tt-reducible random for d if*

$$(\exists d)(\forall n) d^A(X \upharpoonright n) \leq d.$$

Further, a set X is A-tt-Schnorr random for d if for each computable order g,

$$(\exists d)(\forall n) d^A(X \upharpoonright n) \leq h(n) + d.$$

Definition 7. *A set A is a basis fot tt-reducible randomness if, for each tt-reducible martingale d, there exists a set X such that $A \leq_{\mathrm{tt}} X$ and X is A-tt-reducible random for d.*

A set A is a basis fot tt-Schnorr randomness if, for each tt-reducible martingale d, there exists a set X such that $A \leq_{\mathrm{tt}} X$ and X is A-tt-Schnorr random for d.

Theorem 8. *The following are equivalent for a set A:*

(i) *A is Schnorr trivial,*
(ii) *A is a basis for tt-reducible randomness,*
(iii) *A is a basis for tt-Schnorr randomness.*

References

[1] L. Bienvenu and W. Merkle. Reconciling data compression and Kolmogorov complexity. In L. Arge, C. Cachin, T. Jurdziński, and A. Tarlecki, editors, *Automata, Languages and Programming*, volume 4596 of *Lecture Notes in Computer Science*, pages 643–654, Berlin, 2007. Springer.

[2] J. N. Y. Franklin and F. Stephan. Schnorr trivial sets and truth-table reducibility. *Journal of Symbolic Logic*, 75(2):501–521, 2010.

[3] J. N. Y. Franklin, F. Stephan, and L. Yu. Relativizations of randomness and genericity notions. *Bulletin of the London Mathematical Society*, 43(4):721–733, 2011.

[4] K. Miyabe. Truth-table Schnorr randomness and truth-table reducible randomness. *Mathematical Logic Quarterly*, 57(3):323–338, 2011.

AUTOREDUCIBILITY FOR NEXP

DUNG T. NGUYEN AND ALAN L. SELMAN

Autoreducibility was first introduced by Trakhtenbrot [Tra70] in a recursion theoretic setting. A set A is autoreducible if there is an oracle Turing machine M such that $A = L(M^A)$ and M never queries x on input x. Ambos-Spies [AS84] introduced the polynomial-time variant of autoreducibility, where we require the oracle Turing machine to run in polynomial time.

The question of whether complete sets for various classes are polynomial-time autoreducible has been studied extensively. In some cases, it turns out that resolving autoreducibility can result in interesting complexity class separations. Glaßer et al. [GOP$^+$09] showed that all m-complete sets of the following complexity classes are many-one autoreducible: NP, PSPACE, EXP, NEXP, Σ_k^P, Π_k^P, and Δ_{k+1}^P for $k \geq 1$. For Turing autoreducibility, Beigel and Feigenbaum [BF92] showed that Turing complete sets for the classes that form the polynomial-time hierarchy, Σ_k^P, Π_k^P, and Δ_k^P, are Turing autoreducible. Also, all Turing complete sets for NP are Turing autoreducible. However, the above proof can be applied to any complexity class that has a complete language that is length-decreasing self-reducible. Since every self-reducible language belongs to PSPACE, that proof idea does not work for classes such as EXP and NEXP. Nevertheless, Buhrman et al. [BFvMT00] showed that all Turing complete sets for EXP are Turing autoreducible.

One question that remains open is whether all Turing complete sets for NEXP are Turing autoreducible. An important separation may result when solving the autoreducibility for NEXP; if there is one Turing complete set of NEXP that is not Turing autoreducible, then EXP is different from NEXP. We do not know whether proving all Turing complete sets of NEXP are Turing autoreducible yields any separation results [GOP$^+$09]. Moreover, Buhrman et al. [BFvMT00] showed that all Turing complete sets for NEXP are nonuniform Turing autoreducible. Thus it is conceivable that all Turing complete sets for NEXP are Turing autoreducible.

Buhrman et al. [BFvMT00] showed that all $\leq^p_{2\text{-}tt}$-complete sets for EXP are $\leq^p_{2\text{-}tt}$-autoreducible. This proof technique exploits the fact that EXP is closed under exponential-time reductions that only ask one query that is smaller in length. Difficulties arise when we want to prove that the above result holds for NEXP, because we do not know whether this property still holds for NEXP. To resolve that difficulty, we use a nondeterministic technique that applies to NEXP.

Theorem 1. *Every $\leq^p_{2\text{-}tt}$-complete set for* NEXP *is $\leq^p_{2\text{-}tt}$-autoreducible.*

The proof involves an analysis of all two truth-table reductions and uses a subtle diagonalization. Using similar techniques, we also obtain the following results for disjunctive and conjunctive truth-table autoreducibility:

Theorem 2. *Every $\leq^p_{dtt}$-complete set for* NEXP *is $\leq^p_{dtt}$-autoreducible.*

Department of Computer Science and Engineering, University at Buffalo. Email: dtn3@buffalo.edu, selman@buffalo.edu.

Theorem 3. *Every $\leq^p_{ctt}$-complete set for* NEXP *is $\leq^p_{ctt}$-autoreducible.*

Also we have the following negative results for NEXP:

Theorem 4. *There is a $\leq^p_{tt}$-complete set for* NEXP *that is not $\leq^p_{btt}$ autoreducible.*

Theorem 5. *There is a Turing complete set for* NEXP *that is not $\leq^p_{bT}$ autoreducible.*

Theorem 6. *There is a $\leq^p_{2\text{-}T}$-complete set for* NEXP *that is not $\leq^p_{2\text{-}tt}$-autoreducible.*

In the relativized world, we obtain the following negative result for NEXP:

Theorem 7. *Relative to some oracle, there is a $\leq^p_{2\text{-}T}$-complete set for* NEXP *that is not Turing autoreducible.*

References

[AS84] K. Ambos-Spies. P-mitotic sets. In E. Börger, G. Hasenjäger, and D. Roding, editors, *Logic and Machines, Lecture Notes in Computer Science 177*, pages 1-23. Springer-Verlag, 1984.

[BF92] R. Beigel and J. Feigenbaum. On being incoherent without being very hard. *Computational Complexity*, 2:1-17, 1992.

[BFvMT00] H. Buhrman, L. Fortnow, D. van Melkebeek, and L. Torenvliet. Using autoreducibility to separate complexity classes. *SIAM Journal on Computing*, 29(5):1497-1520, 2000.

[GOP+09] C. Glaßer, M. Ogihara, A. Pavan, A. Selman, and L. Zhang. Autoreducibility and mitoticity. *SIGACT News*, 2009.

[Tra70] B. Trahtenbrot. On autoreducibility. *Dokl. Akad. Nauk SSSR*, 192, 1970. Translation in Soviet Math. Dokl. 11: 814-817, 1970.

[Wat87] Osamu Watanabe. A comparison of polynomial time completeness notions. *Theoretical Computer Science*, 54:249-265, 1987.

TWO BETTING STRATEGIES THAT PREDICT ALL COMPRESSIBLE SEQUENCES

TOMISLAV PETROVIĆ
ZELENI TRG 1, ZAGREB, CROATIA
TOMEEPX@GMAIL.COM

Abstract. A new type of betting games that charaterize Martin-Löf randomness is introduced. These betting games can be compared to martingale processes of Hitchcock and Lutz as well as non-monotonic betting strategies. Sequence-set betting is defined as successive betting on prefix-free sets that contain a finite number of words. In each iteration we start with an initial prefix-free set P and an initial capital c, then we divide P into two prefix-free sets P_0 and P_1 of equal size and wager some amount of capital on one of the sets, let's say P_0. If the infinite sequence we are betting on has a prefix in P_0 then in the next iteration the initial set is P_0 and the wagered amount is doubled. If the infinite sequence we are betting on does not have a prefix in P_0 then in the next iteration the initial set is P_1 and the wagered amount is lost. In the first iteration the initial prefix-free set contains the empty string. The player succeeds on the infinite sequence if the series of bets increases capital unboundedly. Non-monotonic betting can be viewed as sequence-set betting with an additional requirement that the initial prefix-free set is divided into two prefix-free sets such that sequences in one set have at some position bit 0 and in the other have at that same position bit 1. On the other hand if the requirement that the initial prefix-free set P is divided into two prefix-free sets of equal size is removed, and we allow that P_0 may have a different size from P_1 we have a betting game that is equivalent to martingale processes in the sense that for each martingale process there is a betting strategy that succeeds on the same sequences as martingale process and for each betting strategy a martingale process exists that succeeds on the the same sequences as the betting strategy. It is shown that, unlike martingale processes, for any computable sequence-set betting strategy there is an infinite sequence on which betting strategy doesn't succeed and which is not Martin-Löf random. Furthermore it is shown that there is an algorithm that constructs two sets of betting decisions for two sequence-set betting strategies such that for any sequence that is not Martin-Löf random at least one of them succeeds on that sequence.

Date: April, 2012.

TRIVIAL MEASURES ARE NOT SO TRIVIAL

CHRISTOPHER P. PORTER

Although algorithmic randomness with respect to various biased computable measures is well-studied, little attention has been paid to algorithmic randomness with respect to computable *trivial* measures, where a measure μ on 2^ω is trivial if the support of μ consists of a countable collection of sequences. In this talk, I will show that there is much more structure to trivial measures than has been previously suspected. In particular, I will outline the construction of

(i) a trivial measure μ such that every sequence that is Martin-Löf random with respect to μ is an atom of μ (i.e., μ assigns positive probability to such a sequence), while there are sequences that are Schnorr random with respect to μ that are not atoms of μ (thus yielding a counterexample to a result claimed by Schnorr), and

(ii) a trivial measure μ such that (a) the collection of sequences that are Martin-Löf random with respect to μ are not all atoms of μ and (b) every sequence that is Martin-Löf random with respect to μ and is not an atom of μ is also not weakly 2-random with respect to μ.

Lastly, I will show that, if we consider the class of LR-degrees associated with a trivial measure μ (generalizing the standard definition of the LR-degrees), then for every finite distributive lattice $\mathscr{L} = (L, \leq)$, there is a trivial measure μ such that the the collection of LR-degrees with respect to μ is a finite distributive lattice that is isomorphic to $\mathscr{L}$.

COMPUTABLE RANDOMNESS AND ITS PROPERTIES

JASON RUTE

Computable randomness at first does not seem as natural of a randomness notion as Schnorr and Martin-Löf randomness. However, recently Brattka, Miller, and Nies [1] have shown that computable randomness is closely linked to differentiability. Why is this so? What are the chances that, say, computable randomness will also be linked to the ergodic theorem? In this talk I will explain how computable randomness is similar to and how it is different from other notions of randomness.

Unlike other notions of randomness, computable randomness is closely linked to the Borel sigma-algebra of a space. This has a number of interesting implications: (1) Computable randomness can be extended to other computable probability spaces, but this extension is more complicated to describe [2]. (2) Computable randomness is invariant under isomorphisms, but not morphisms (a.e.-computable measure-preserving maps) [2]. (3) Computable randomness is connected more with differentiability than with the ergodic theorem. (4) Dyadic martingales and martingales whose filtration converges to a "computable" sigma-algebra characterize computable randomness, while more general computable betting strategies do not.

However, this line of research still leaves many open questions about the nature of computable randomness and the nature of randomness in general. I believe the tools used to explore computable randomness may have other applications to algorithmic randomness and computable analysis.

References

[1] Vasco Brattka, Joseph S. Miller, and André Nies. Randomness and differentiability. Submitted.
[2] Jason Rute. Computable randomness and betting for computable probability spaces. In preparation.

INTEGRATION OF IDEAS AND METHODS OF KOLMOGOROV COMPLEXITY AND CLASSICAL MATHEMATICAL STATISTICS

BORIS RYABKO AND ZHANNA REZNIKOVA

Abstract. A new approach is suggested which allows to combine the advantages of methods based on Kolmogorov complexity with classical methods of testing of statistical hypotheses. As distinct from other approaches to analysis of different sequences by means of Kolmogorov complexity, we stay within the framework of mathematical statistics. As examples, we consider behavioural sequences of animals (ethological "texts") testing the hypotheses whether the complexity of hunting behaviour in ants and rodents depends on the age of an individual.

The idea of quantitative evaluation of complexity of sequences of symbols from a finite alphabet (or "texts") is important for many scientific fields, including molecular biology, linguistics, zoosemiotics, and ethology. The degree of complexity of a "text" could be estimated by its Kolmogorov complexity. Although Kolmogorov complexity is not algorithmically computable, it can be, in a certain sense, estimated by means of data compressors. This simple observation has been a basis of many applications of Kolmogorov complexity to comparative analysis of many literary, musical and biological texts; see [2] for review. However, this approach does not give a possibility to use methods of mathematical statistics and, in particular, hypothesis testing. This presents significant limitations for the applicability of ideas of Kolmogorov complexity to natural sciences, in particular, to biological studies, because, since Fishers classical works, mathematical statistics and, in particular, hypothesis testing became the main method of quantitative analysis of biological data.

We suggest an approach which allows to combine the advantages of methods based on Kolmogorov complexity with classical methods of testing statistical hypotheses. The goal here is to estimate the complexity of sequences of different kinds and to use these estimates to test hypotheses. This gives the possibility to make decisions on the basis of standard statistical tests. For example, two sets of sequences could be DNA of two different species (say, viruses or bacteria), and the problem is to compare complexities of these sequences. Similar problems arise in many fields of biology and other sciences.

First we describe the scheme of the suggested approach. Let there be a sequence $x = x_1...x_t$, $t > 0$, of letters from a finite alphabet A and let φ be a data compressor. We denote the compressed sequence by $\varphi(x)$, its length by $|\varphi(x)|$ and define the complexity (per letter) as follows:

$$K_\varphi(x_1...x_t) = |\varphi(x_1...x_t)| \,/\, t.$$

Generally speaking, we suggest to use $K_\varphi(x)$ for hypothesis testing.

boris@ryabko.net, zhanna@reznikova.net.

It turns out that, under certain conditions, the proposed approach can be used to evaluate hypotheses about the Kolmogorov complexity of the considered sequences; see Theorem 1 below (even though it is impossible to calculate Kolmogorov complexity). These conditions are as follows: first, the considered sequences are generated by stationary ergodic sources, and second, the data compressor φ is a universal code. Informally, a universal code can "compress" a sequence $x_1...x_t$ up to its Shannon entropy (per letter) if the sequence is generated by a stationary ergodic source (a formal definition and description such a code can be found, for ex. in [1]). The following theorem gives a theoretical basis for the suggested approach:

Theorem 1. *Let there be a stationary ergodic source generated letters from a finite alphabet and a universal code φ. Then, with the probability 1,* $\lim_{t\to\infty} t^{-1}(|\varphi(x_1...x_t)| = \lim_{t\to\infty} t^{-1}K(x_1...x_t)$ *, where $x_1...x_t$ is generated by the source and $K(x_1...x_t)$ is the Kolmogorov complexity.*

Nowadays there are many efficient universal codes, which are described in numerous papers. It is important for practical applications that the modern data compressors (or archivers) are based on the universal codes and, hence, the main properties of universal codes are valid for them (as far as asymptotic properties can be valid for a real computer program).

The main idea of the suggested approach is very simple and can be formulated as follows: Apply some universal code φ to estimate the Kolmogorov complexity of a word $x_1...x_t$. Then, use (consistent) statistical tests to study $\varphi(x_1...x_t)/t$ $(= K_\varphi(x_1...x_t)\,)$ in the same manner as one would study any other natural parameter, such as the weight, length, speed, etc. For example, suppose that one wants to compare complexities of DNA sequences of viruses and bacteria. In such a case one can consider two corresponding set of sequences (say, $V = \{v_1, ..., v_n\}$ and $B = \{b_1, ..., b_m\}$) and apply any statistical test to the sets V and B.

Our goal is to find a statistical test that can distinguish between the following two hypotheses: $H_0 = \{$**the sequences from both sets are generated by one source**$\}$ and $H_1 = \{$**the sequences from the different sets are generated by stationary and ergodic sources with different Kolmogorov complexities (per letter of generated sequences)**$\}$. In order to construct the test for H_0 against H_1 we consider an auxiliary hypothesis $H_1^* = \{$**the estimation of the average complexity $K_\varphi()$ is not equally large for sequences from different sets V, B**$\}$. The suggested test $T_\varphi^{'}$ for H_0 against H_1 (not H_1^* !) uses a universal code φ and a consistent test T for assessing whether two independent samples of observations have equally large values (say, the Mann–Whitney–Wilcoxon U test). The test $T_\varphi^{'}$ is as follows: First, calculate $K_\varphi()$ for all sequences from V, B and then apply T for testing H_0 against H_1^* based on the new sets $\{K_\varphi(x), x \in V\}$ and $\{K_\varphi(x), x \in B\}$. The following Theorem describes properties of $T_\varphi^{'}$:

Theorem 2. *The Type I error of the test $T_\varphi^{'}$ is not greater than α and, if* $\min(|B|, |V|) \to \infty$ *and* $\min(|v|, |b|,\ v \in V, b \in B, \to \infty$*, the probability to accept H_0 instead of* $H_1 = \{$**the sequences from the different sets are generated by stationary and ergodic sources with different Kolmogorov complexities (per letter)**$\}$ *goes to 0.*

References

[1] B. Ryabko. Applications of Universal Source Coding to Statistical Analysis of Time Series. *In: Isaac Woungang, Sudip Misra, Subhas Chandra Misra (Eds.), "Selected Topics in Information and Coding Theory", Edited Book, Series on Coding and Cryptology,* World Scientific Publishing, 2010.

[2] P.M.B. Vitanyi. Compression-based Similarity. *In Proc. IEEE 1st Int. Conf. Data Compression, Communication and Processing,* Palurno, Italy, June 21-24, 2011, 111–118.

LIMIT CAPACITY OF NON-STOCHASTIC STEGANOGRAPHIC SYSTEMS AND HAUSDORFF DIMENSION

BORIS RYABKO AND DANIIL RYABKO

Abstract. It was shown recently that the limit capacity of perfect steganography systems for i.i.d. and Markov sources equals the Shannon entropy of the "cover" process. Here we address the problem of limit capacity of general perfect steganographic systems. We show that this value asymptotically equals the Hausdorff dimension of the set of possible cover messages.

The goal of steganography is as follows. Alice and Bob can exchange messages of a certain kind (called *covertexts*) over a public channel, which is open to Eve. The covertexts can be, for example, a sequence of photographic images, videos, text emails and so on. Alice wants to pass some secret information to Bob so that Eve cannot notice that any hidden information was passed. Thus, Alice should use the covertexts to hide the secret text. We assume that Eve does not attempt to disrupt communication between Alice and Bob, but only tries to determine whether secret information is being passed.

Several formalizations of this problem are possible.

In the *information-theoretic* framework, the source of covertexts is modelled as a probabilistic source. Alice uses this source to generate covertexts and transmits possibly different covertexts that code her secret message; her goal is that *the distribution of the output is the same as the distribution of the input.* It was shown in [3] that this goal is achievable if the source of covertexts has a finite memory (the distribution of the source does not have to be known). The idea of the proposed method can be illustrated with the following simple example of a stegosystem for memoryless sources of covertexts. Suppose that Alice wants to pass a single bit, and assume that the source of covertexts is i.i.d., but its distribution is unknown. Alice reads two symbols from the source, say ab. She knows that (since the source is i.i.d.) the probability of ba is the same. So if Alice's secret bit to pass is 0 she transmits ab and if she needs to pass 1 then she transmits ba. However, if the source has generated aa then Alice cannot pass her secret bit, but she has to transmit aa anyway, to preserve the probabilistic characteristics of the source. It is easy to see that this system is perfect simply because sequences with and without hidden information beyond the same distribution. This construction can be generalized for a case of any word length and the obtained system will have the asymptotically maximal speed, if the word length grows. The limit capacity of such a stegosystem equals the Shannon entropy of the source of covertexts.

However, practically interesting sources of covertexts, such as human-written texts or photographic images, cannot be realistically modelled by finite-memory sources, or, more generally, by some stochastic sources with simple probabilistic characteristics.

{boris,daniil}@ryabko.net.

Therefore, a non-stochastic (or combinatorial) model of the problem is of interest. In early works on steganography, the following simple method is considered (see, e.g., [1]), known as *hash-based steganography*. Alice has a (possibly infinite) set of covertexts (a *cover set*) and a secret message she wants to transmit. Any element of the set of covertexts is considered legitimate, in the sense that Eve cannot say that it contains a secrete message. Alice picks a covertext, applies to it a certain hash function (known to Bob), and if the output *coincides exactly* with her message, then she transmits the covertext to Bob; otherwise, she picks another covertext and repeats. While such a stegosystem may not be practical in general, it is viable for short secret messages.

In this work we consider the problem of finding the limit speed of transmission of hidden information for non-stochastic (combinatorial) sources. The following two models are considered. First, we suppose that any procedure for selecting covertexts from the set of available covertexts is admissible. In this case we show that the limiting speed equals the Hausdorff dimension of the cover set. In the second model we consider only those stegosystems that can be realized on a Turing machine. In this case the limit speed of transmission of the hidden information can be expressed in terms of Kolmogorov complexity of the covertexts.

Let us give some definitions. Consider a finite alphabet A and, without lose of generality, suppose that $A = \{0, 1, ..., |A|-1\}$. The cover source I is a subset of A^∞. For any subset $I \subset A^\infty$ we define a set $I' \subset [0, 1]$ as follows: a point $0.x_1x_2...$, $x_i \in \{0, 1, ...|A| - 1\}$, belongs to I' iff $x_1x_2... \in I$. We denote the Hausdorff dimension of the set I' by $\dim(I)$.

Theorem 1. *Let $I \subset A^\infty$ be a cover set. Then there exists a stegosystem φ whose speed of transmission of the hidden information equals* $\dim(I) \log_2 |A|$. *On the other hand, the speed of transmission of the hidden information of any stegosystem ψ is not larger than* $\dim(I) \log_2 |A|$.

Proof. Let φ be an optimal code for the set I, described in [2] and let $s = s_1s_2...$ be a binary sequence that should be hidden. Alice decodes s and obtains a sequence $x = x_1x_2... = \varphi^{-1}(s)$. Then she sends it to Bob. Bob decodes the sequence x and obtains the hidden message s. It is important to note that the encoding and decoding can be done step-by-step (i.e. without infinite delay) and there exists such an optimal code that for any $s \in \{0, 1\}^\infty$ the sequence $\varphi^{-1}(s)$ exists, see [2]. The proof of the second statement immediately follows from [2, Theorem 1]. More precisely, it is shown in [2] that $\dim(I)$ is an upper bound for the speed of information transmission. Hence, the speed of transmission of hidden information cannot be larger than this limit. □

References

[1] C. Cachin. An information-theoretic model for steganography. *Information and Computation*, 192:41–56, 2004.

[2] B. Ryabko. Noiseless coding of combinatorial sources, Hausdorff dimension, and Kolmogorov complexity. *Problems of Information Transmission*, 22:170-179, 1986.

[3] B. Ryabko and D. Ryabko. Constructing perfect steganographic systems. *Information and Computation*, 209(9):1223–1230, 2011.

NONSTANDARD ANALYSIS: A NEW WAY TO COMPUTE

SAM SANDERS

Abstract. Constructive Analysis was introduced by Errett Bishop to identify the 'computational meaning' of mathematics. In the spirit of intuitionistic mathematics, notions like *algorithm*, *explicit computation*, and *finite procedure* are central. The exact meaning of these vague terms was left open, to ensure the compatibility of Constructive Analysis with several traditions in mathematics. Constructive Reverse Mathematics (CRM) is a spin-off of Harvey Friedman's famous Reverse Mathematics program, based on Constructive Analysis. Here, we introduce 'Ω-invariance': a simple and elegant definition of finite procedure in (classical) Nonstandard Analysis. Using an intuitive interpretation, we obtain many results from CRM, thus showing that Ω-invariance is quite close to Bishop's notion of algorithm.

1. Introduction

1.1. **Nonstandard Analysis and Computability.** Around 1960, Abraham Robinson introduced *Nonstandard Analysis*, providing a formalization of the calculus with infinitesimals [4]. In Nonstandard Analysis, the set $\mathbb{N}$ is extended with new elements which are larger than all $n \in \mathbb{N}$. The resulting set is called ${}^*\mathbb{N}$ and any $\omega \in \Omega := {}^*\mathbb{N} \setminus \mathbb{N}$ is called *infinite*. In contrast, any $n \in \mathbb{N}$ is called *finite*. The following notion is meant to correspond to *algorithm* and *finite procedure*.

1. **Definition.** [Ω-invariance] For $\psi(n,m) \in \Delta_0$, the formula $\psi(n,\omega)$ is Ω-invariant if $(\forall n \in \mathbb{N})(\forall \omega' \in \Omega)(\psi(n,\omega) \leftrightarrow \psi(n,\omega'))$.

Hence, an Ω-invariant formula does not depend on the *choice* of the infinite number $\omega \in \Omega$. The following theorem states that the properties of an Ω-invariant set are determined at some *finite* number. It is called 'modulus lemma' as it bears a resemblance to the modulus lemma from Recursion Theory [6, 3.2]. This observation suggests that Ω-invariance models the notion of *finite procedure* quite well.

2. **Theorem** (Modulus lemma)**.** *For every Ω-invariant formula $\psi(n,\omega)$, we have*

$$(\forall n \in \mathbb{N})(\exists m_0 \in \mathbb{N})(\forall m \in {}^*\mathbb{N})[m \geq m_0 \to \psi(n,m) \leftrightarrow \psi(n,\omega)],$$

and the number m_0 can be computed by an Ω-invariant function.

1.2. **Constructive Analysis and Ω-invariance.** In Errett Bishop's *Constructive Analysis*, the notion of (constructive) *algorithm* is central. This already becomes clear from the definition of disjunction ([1, 2]).

3. **Definition.** [Disjunction] $P \vee Q$: we have an algorithm that outputs either P or Q, together with a proof of the chosen disjunct.

In Nonstandard Analysis, we have the following similar definition, where the role of 'algorithm' is played by Ω-invariance.

This research is generously sponsored by the John Templeton Foundation as part of the project *Philosophical Frontiers in Reverse Mathematics*.

4. **Definition.** [Hyperdisjunction] For formulas P, Q the formula $P \mathbb{V} Q$ is the statement: *There is an Ω-invariant formula ψ such that*

$$(\forall n \in \mathbb{N})(\psi(n,\omega) \to P(n) \wedge \neg\psi(n,\omega) \to Q(n).$$

Given the formula $P \mathbb{V} Q$, there is an Ω-invariant procedure, provided by $\psi(n,\omega)$, to determine which disjunct of $P(n) \vee Q(n)$ makes it true. Thus, we observe that the meaning of the hyperdisjunction '$\mathbb{V}$' is quite close to its intuitionistic counterpart '$\vee$' from Definition 3. The other intuitionistic connectives may be translated analogously. The translation of $\to$ (resp. $\neg$) will be denoted $\Rrightarrow$ (resp. $\sim$). As for disjunction, the meaning of the intuitionistic connectives is quite close to that of the hyperconnectives. These new connectives provide a translation of Constructive Analysis (aka 'BISH') into Nonstandard Analysis. As it turns out, this translation preserves the many equivalences from *Constructive Reverse Mathematics* ([3]). For instance, compare the following theorems.

5. **Theorem.** *In* BISH*, the following are equivalent.*

(1) LPO*:* $P \vee \neg P \qquad (P \in \Sigma_1)$.
(2) PR: $(\forall x \in \mathbb{R})(x > 0 \vee \neg(x > 0))$.
(3) MC: (*The monotone convergence theorem*)
(4) CIT: (*The Cantor intersection theorem*).

6. **Theorem.** *In* BISH*, the following are equivalent.*

(1) LLPO: $\neg(P \wedge Q) \to \neg P \vee \neg Q \quad (P, Q \in \Sigma_1)$.
(2) LLPR: $(\forall x \in \mathbb{R})[\neg(x > 0) \vee \neg(x < 0)]$.
(3) NIL: $(\forall x, y \in \mathbb{R})(xy = 0 \to x = 0 \vee y = 0)$.
(4) CLO: *For all $x, y \in \mathbb{R}$ with $\neg(x < y)$, $\{x, y\}$ is a closed set.*
(5) IVT: *a version of the intermediate value theorem.*
(6) WEI: *a version of the Weierstraß extremum theorem.*

7. **Theorem.** *In Nonstandard Analysis, the following are equivalent.*

(1) $\mathbb{LPO}$*:* $P \mathbb{V} \sim P \qquad (P \in \Sigma_1)$.
(2) $\mathbb{PR}$: $(\forall x \in \mathbb{R})(x > 0 \mathbb{V} \sim(x > 0))$.
(3) $\mathbb{MC}$: (*The monotone convergence theorem*)
(4) $\mathbb{CIT}$: (*The Cantor intersection theorem*).
(5) *Universal Transfer: For all $\varphi \in \Delta_0$, $(\forall n \in \mathbb{N})\varphi(n) \to (\forall n \in {}^*\mathbb{N})\varphi(n)$.*

8. **Theorem.** *In Nonstandard Analysis, the following are equivalent.*

(1) $\mathbb{LLPO}$: $\sim(P \wedge Q) \Rrightarrow \sim P \mathbb{V} \sim Q \quad (P, Q \in \Sigma_1)$.
(2) $\mathbb{LLPR}$: $(\forall x \in \mathbb{R})[\sim(x > 0) \mathbb{V} \sim(x < 0)]$.
(3) $\mathbb{NIL}$: $(\forall x, y \in \mathbb{R})(xy = 0 \Rrightarrow x = 0 \mathbb{V} y = 0)$.
(4) $\mathbb{CLO}$: *For all $x, y \in \mathbb{R}$ with $\sim(x < y)$, $\{x, y\}$ is a closed set.*
(5) $\mathbb{IVT}$: *a version of the intermediate value theorem.*
(6) $\mathbb{WEI}$: *a version of the Weierstraß extremum theorem.*

In [5], we show that most equivalences from Constructive Reverse Mathematics (e.g. those for LPO, LLPO, WLPO, MP, $\mathrm{MP}^{\vee}$, BD-N, FAN_{Δ} and WMP) can be translated to Nonstandard Analysis. Hence, we observe that Ω-invariance must be close to Bishop's notion of (constructive) algorithm, as it gives rise to exactly the same kind of Reverse Mathematics results.

References

[1] Errett Bishop, *Foundations of constructive analysis*, McGraw-Hill Book Co., New York, 1967.

[2] Douglas S. Bridges, *Constructive mathematics: a foundation for computable analysis*, Theoret. Comput. Sci. **219** (1999), no. 1-2, 95–109.

[3] Hajime Ishihara, *Reverse mathematics in Bishop's constructive mathematics*, Philosophia Scientiae (Cahier Spécial) **6** (2006), 43-59.

[4] Abraham Robinson, *Non-standard analysis*, North-Holland Publishing Co., Amsterdam, 1966.

[5] Sam Sanders, *On the notion of algorithm in Nonstandard Analysis*, Submitted (2012).

[6] Robert I. Soare, *Recursively enumerable sets and degrees*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1987.

Ghent University, Department of Mathematics, Krijgslaan 281, 9000 Gent (Belgium)
E-mail address: `sasander@cage.ugent.be, http://cage.ugent.be/∼sasander`

CRYPTOGRAPHY AND ALGORITHMIC RANDOMNESS

KOHTARO TADAKI AND NORIHISA DOI

Key words: cryptography, random oracle model, provable security, instantiation, cryptographic hash function, algorithmic randomness, random real, Schnorr randomness

In this talk, we apply the concepts and methods of algorithmic randomness to cryptography. In particular, we investigate the problem of instantiation of the random oracle in *the random oracle methodology* [1] from the point of view of algorithmic randomness.

In modern cryptography, *the random oracle model* is widely used as an *imaginary* framework in which the security of a cryptographic scheme is discussed. In the random oracle model, the cryptographic hash function used in a cryptographic scheme is formulated as a random variable uniformly distributed over all possibility of the function, called *the random oracle*, and the legitimate users and the adversary against the scheme are modeled so as to get the values of the hash function not by evaluating it in their own but by querying the random oracle [1]. Since the random oracle is an imaginary object, even if the security of a cryptographic scheme is proved in the random oracle model, the random oracle has to be instantiated using a concrete cryptographic hash function such as the SHA hash functions if we want to use the scheme in the real world. In fact, the instantiations of the random oracle by concrete cryptographic hash functions are widely used in modern cryptography to produce efficient cryptographic schemes. Once the random oracle is instantiated, however, the original security proof in the random oracle model is spoiled and goes back to square one. Actually, it is not clear how much the instantiation can maintain the security originally proved in the random oracle model, nor is it clear whether the random oracle can be instantiated somehow while keeping the original security. (For the detail of the random oracle methodology, see e.g. Katz and Lindell [6, Chapter 13].)

In the present talk we investigate this problem using concepts and methods of algorithmic randomness. Here, *algorithmic randomness* is a research field in which the notion of random real plays a central role. A *random real* is an individual infinite binary sequence which is classified as "random", and not a random variable such as the random oracle. Algorithmic randomness enables us to classify an individual infinite binary sequence into random or not. The contributions of this talk are as follows:

(i) We investigate the instantiation of the random oracle by a random real in a scheme already proved secure in the random oracle model. We present equivalent conditions for a specific oracle instantiating the random oracle to keep a cryptographic scheme secure, using a concept of algorithmic randomness, i.e., a variant of Schnorr randomness where the class of Schnorr

tests is restricted appropriately. Based on this, in particular we show that the security proved in the random oracle model is firmly maintained after instantiating the random oracle by any Schnorr random real.

(ii) We introduce the notion of *effective security*, which is a constructive strengthening of normal (non-constructive) notions of security. We show that, for any effectively secure cryptographic scheme in the random oracle model, there exists a specific *computable* function which can instantiate the random oracle while keeping the security originally proved in the random oracle model. We demonstrate that the effective security is a natural alternative to the normal security notions in modern cryptography by reconsidering the security notions required in modern cryptography.

Our results use the general form of definitions of security notions for cryptographic schemes in modern cryptography, and depend neither on specific schemes nor on specific security notions.

Acknowledgments. This work was supported by the Ministry of Economy, Trade and Industry of Japan. The first author was also supported by KAKENHI (23340020), KAKENHI (70188291), and KAKENHI (24540142).

References

[1] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," Proceedings of the 1st ACM Conference on Computer and Communications Security, ACM, pp.62–73, 1993.

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

[3] R. G. Downey and D. R. Hirschfeldt, *Algorithmic Randomness and Complexity*. Springer-Verlag, New York, 2010.

[4] O. Goldreich, *Foundations of Cryptography: Volume 1 – Basic Tools*. Cambridge University Press, New York, 2001.

[5] O. Goldreich, *Foundations of Cryptography: Volume 2 – Basic Applications*. Cambridge University Press, New York, 2004.

[6] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, 2007.

[7] A. Nies, *Computability and Randomness*. Oxford University Press, Inc., New York, 2009.

Research and Development Initiative, Chuo University, 1–13–27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan, E-mail: tadaki@kc.chuo-u.ac.jp, doi@doi.ics.keio.ac.jp, WWW: http://www2.odn.ne.jp/tadaki/

ALGORITHMIC RANDOMNESS AND STOCHASTIC SELECTION FUNCTION

HAYATO TAKAHASHI

Let S and Ω be the set of finite binary strings and the set of binary sequences, respectively. Let $\mathcal{B}$ be the σ-algebra generated by $\{\Delta(s)\}_{s\in S}$, where $\Delta(s) = \{sx \mid x \in \Omega\}$. For a computable probability P on $(\Omega, \mathcal{B})$, let $P(s) := P(\Delta(s)), s \in S$ and $\mathcal{R}^P$ be the set of Martin-Löf random sequences w.r.t. P. For $x = x_1x_2\cdots, y = y_1y_2\cdots \in \Omega$, let $x^n := x_1\cdots x_n$ and $x/y := x_{\tau(1)}x_{\tau(2)}\cdots$ where $\{i \mid y_i = 1\} = \{\tau(1) < \tau(2) < \cdots\}$.

Let u be the uniform measure on Ω and v be a computable probability such that $\forall s \in S\ v(s0^\infty) = 0$, where 0^∞ is the sequence of 0's. In [7], it is shown that (i) if $x \in \mathcal{R}^u$ then $v\{y \mid x/y \in \mathcal{R}^u\} = 1$ and (ii) $\{(x, y) \mid x/y \notin \mathcal{R}^u\}$ is a Martin-Löf test of $u \times v$, i.e.,

$$\mathcal{R}^{u\times v} \subseteq \{(x, y) \mid x/y \in \mathcal{R}^u\}.$$

Our problem is to find a finite set of selection functions such that $x \in \mathcal{R}^u$ when subsequences selected by them are in $\mathcal{R}^u$. This is trivial if we allow $y = s1^\infty$ for $s \in S$, where 1^∞ is the sequence of 1's. It is possible that x is not random w.r.t. uniform probability even if x/y is random for all $y \in \mathcal{R}^v$ and for some computable v, e.g., $x = 0101\cdots$ (repetition of 01) then $x/y \in \mathcal{R}^u$ for all $y \in \mathcal{R}^v$, where $\forall n\ v(x_1\cdots x_{2n}) = 2^{-n}, x_{2i-1}x_{2i} = 01$ or $10, 1 \le i \le n$. In the following, we say that a selection function is non-trivial if it contains infinitely many 1's and 0's.

Proposition 1. *The following two statements are equivalent.*
(i) $x \in \mathcal{R}^u$.
(ii) $\exists$ *computable* w $\ x \in \mathcal{R}^w$ *and* $x/y_i(w, x) \in \mathcal{R}^u$ *for* $i = 1, 2, \ldots, 6,$ *where* $\{y_1(w, x), \ldots, y_6(w, x)\}$ *consists of non-trivial selection functions and depends on* w *and* x.

In the above proposition, selection functions $\{y_1(w, x), \ldots, y_6(w, x)\} \subset \Omega$ need not be computable. We can show that $\lim_n w(x_i\cdots x_j \mid x_{j+1}\cdots x_{j+n})$ exists for all $i < j$ and $x \in \mathcal{R}^w$, see [4]. The selection functions in the above proposition depend on the convergence rate of these conditional probabilities and if they are uniformly computable for all $i < j$ then we can choose computable selection functions. It is possible that the convergence rate of conditional probability is not computable, see [1]

The author do not know whether we can replace (ii) with $x/y \in R^u$ for $y \in Y^x$ where Y^x consists of non-trivial selection functions and depends on x.

In [3], it is shown that x is normal number iff for all $q \in (0, 1)$,

$$u_q\{y \mid x/y \text{ is normal number}\} = 1,$$

The Institute of Statistical Mathematics, 190-8562 Japan. Present address: The university of Electro-Communications, Japan, hayato.takahashi@ieee.org.

where u_q is the binary i.i.d. process with parameter q. We have an algorithmic analogy for this result.

Proposition 2. *Let w be a computable probability such that*
(a) $\forall y \in \mathcal{R}^w,\ \lim_n K(y^n)/n = 0$, *(b)* $\lim_n \sum_{1 \le i \le n} y_i/n$ *exists for* $y \in \mathcal{R}^w$, *and (c)* $\forall \epsilon > 0 \exists y \in \mathcal{R}^w \lim_n \sum_{1 \le i \le n} y_i/n > 1 - \epsilon$.
Then the following two statements are equivalent.
(i) $\lim_{n \to \infty} \frac{1}{n} K(x^n) = 1$.
(ii) $\lim_{n \to \infty} \frac{1}{|x^n/y^n|} K(x^n/y^n) = 1$ *for* $y \in \mathcal{R}^w$.

For example, $w = \int P_\rho d\rho$, where P_ρ is a probability derived from irrational rotation with parameter ρ, satisfies the condition of Prop. 2, see [6].

There are similar algorithmic analogies for Kamae's theorem [2], see [5].

References

[1] N. L. Ackerman, C. E. Freer, and D. M. Roy. Noncomputable conditional probabilities. In *2011 IEEE 26th Annual Symposium on Logic in computer science*. IEEE, 2011.

[2] T. Kamae. Subsequences of normal numbers. *Israel J. Math.*, 16:121–149, 1973.

[3] H. Steinhaus. Les probabilités dénombrables et leur rapport à la théorie de la meésure. *Fund. Math.*, 4:286–310, 1922.

[4] H. Takahashi. On a definition of random sequences with respect to conditional probability. *Inform. and Compt.*, 206:1375–1382, 2008.

[5] H. Takahashi. Algorithmic analogies to Kamae-Weiss theorem on normal numbers. In *Solomonoff 85th memorial conference*. To appear in LNAI.

[6] H. Takahashi and K. Aihara. Algorithmic analysis of irrational rotations in a sigle neuron model. *J. Complexity*, 19:132–152, 2003.

[7] M. van Lambalgen. *Random sequences*. PhD thesis, Universiteit van Amsterdam, 1987.

LANGUAGE COMPRESSION FOR SETS IN P/POLY

MARIUS ZIMAND

Recently, some techniques based on the theory of pseudo-randomness in computational complexity have been used to obtain interesting results in polynomial-time-bounded Kolmogorov complexity. Antunes and Fortnow [AF09] have shown that, under a certain reasonable hardness assumption, $2^{-C^p(x)}$ dominates all P-samplable distributions (where $C^p(x)$ is the length of the shortest program that generates x within time $p(|x|)$). Using a similar assumption, the paper [Zim11] has shown that sets in PSPACE can be compressed optimally and has discussed similar results for sets in P and in NP.

In this work, we revisit the language compression problem. We present a related but more direct method than the one in [Zim11] suggested by Vinodchandran [Vin11] and show how it can be used to obtain results regarding the optimal compression of sets in P/poly (and also in P, NP, and in general in the polynomial hierarchy), under weaker hardness assumptions than in [Zim11].

The language compression problem. If we consider a finite set A, it is desirable to represent every $x \in A$ by another shorter string $compressed(x)$ such that $compressed(x)$ describes unambigously the initial x. Regarding the compression rate, ideally, one would like to achieve the information-theoretical bound $|compressed(x)| \approx \log(|A|)$, for all $x \in A$. This optimal rate is achievable for c.e. (and also co-c.e.) sets A, because for such a set $C(x) \leq \log(|A^{=n}|) + O(\log n)$ ($C(x)$ is the Kolmogorov complexity of string x and n is the length of x). In the time-bounded setting, we would like to have a polynomial-time type of unambiguous description. The relevant concept is the time-bounded distinguishing complexity, $\mathrm{CD^t}(\cdot)$, introduced by Sipser [Sip83]. The t-time bounded distinguishing complexity of x conditioned by y, denoted $\mathrm{CD^t(x \mid y)}$ is the length of the shortest program p that accepts x and only x within time $t(|x|)$. Formaly, $\mathrm{CD^t(x \mid y)}$ is the length of the shortest program p such that (1) $U(p, x)$ accepts, (2) $U(p, v)$ rejects for all $v \neq x$, (3) $U(p, v)$ halts in at most $t(|v|)$ steps for all v. Here U is the type of universal Turing machine typically used for time-bounded Kolmogorov complexity. If U is an oracle machine, we define in the similar way $\mathrm{CD^{t,A}(x)}$, by allowing U to query the oracle A.

Buhrman, Fortnow, and Laplante [BFL01] show that for some polynomial p, for every set A, and every string $x \in B^{=n}$, $\mathrm{CD^{p,A^{=n}}(x) \leq 2\log(|A^{=n}|) + O(\log n)}$. This is not optimal compression because of the factor 2, but Buhrman, Laplante, and Miltersen [BLM00] show that, for some sets A, the factor 2 is necessary. As mentioned, for sets in P, NP, PSPACE, optimal compression can be achieved, using some reasonable hardness assumptions [Zim11]. We show that this also holds for sets in P/poly, i.e., for sets computable by polynomial-size circuits. Furthermore,

Department of Computer and Information Sciences, Towson University, Baltimore, MD.; email: mzimand@towson.edu; http://triton.towson.edu/~mzimand. This work has been supported by NSF grant CCF 1016158.

we use a different proof method (even though some key elements are common), which needs a weaker hardness assumption.

The hardness assumption is that there exists a function f computable in E (where $E = \bigcup_c \mathrm{DTIME}[2^{cn}]$) that, for some $\epsilon > 0$, cannot be computed by circuits of size $2^{\epsilon n}$ that also have SAT gates (in addition to the standard logical gates). More formally let us denote by $C_f^{\mathrm{SAT}}(n)$ the size of the smallest circuit with SAT gates that computes the function f for inputs of length n.

Assumption H: There exists a function f in E such that, for some $\epsilon > 0$, $C_f^{\mathrm{SAT}}(n) > 2^{\epsilon n}$.

Klivans and van Melkebeek [KvM02], generalizing the work of Nisan and Wigderson [NW94] and Impagliazzo and Wigderson [IW97], have shown that, under assumption H, for every k, there is a pseudo-random generator $g : \{0,1\}^{c \log n} \to \{0,1\}^n$ that fools all n^k-size circuits with SAT gates.

Theorem 0.1. *Assume H holds. Then for every A in P/poly, there exists a polynomial p such that, for all $x \in A^{=n}$,* $\mathrm{CD^{p,A}(x) \leq \log |A^{=n}| + O(\log n)}$.

The same result holds for sets in P and NP too (for a set A in P, the oracle A can, of course, be dropped). In general, the following result for sets in the polynomial hierarchy, and even for sets in the polynomial hierarchy with polynomial advice, holds.

Theorem 0.2. *Assume that there exists a function f in E such that, for some $\epsilon > 0$, $C_f^{\Sigma_k^p}(n) \geq 2^{\epsilon n}$, where k is a natural number.*

Then for every A in Σ_k^P/poly, there exists a polynomial p such that, for all $x \in A^{=n}$, $\mathrm{CD^{p,A}(x) \leq \log |A^{=n}| + O(\log n)}$.

References

[AF09] L. Antunes and L. Fortnow. Worst-case running times for average-case algorithms. In *Proceedings of the 24th Conference in Computational Complexity Conference*, pages 598–303. IEEE Computer Society Press, 2009.

[BFL01] Harry Buhrman, Lance Fortnow, and Sophie Laplante. Resource-bounded Kolmogorov complexity revisited. *SIAM J. Comput.*, 31(3):887–905, 2001.

[BLM00] Harry Buhrman, Sophie Laplante, and Peter Bro Miltersen. New bounds for the language compression problem. In *IEEE Conference on Computational Complexity*, pages 126–130, 2000.

[IW97] R. Impagliazzo and A. Wigderson. P = BPP if E requires exponential circuits: Derandomizing the XOR lemma. In *Proceedings of the 29th Annual ACM Symposium on the Theory of Computing (STOC '97)*, pages 220–229, New York, May 1997. Association for Computing Machinery.

[KvM02] Adam Klivans and Dieter van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM J. Comput.*, 31(5):1501–1526, 2002.

[NW94] N. Nisan and A. Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49:149–167, 1994.

[Sip83] M. Sipser. A complexity theoretic approach to randomness. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, pages 330–335, 1983.

[Vin11] N. V. Vinodchandran. Personal communication, 2011.

[Zim11] Marius Zimand. On the optimal compression of sets in pspace. In Olaf Owe, Martin Steffen, and Jan Arne Telle, editors, *FCT*, volume 6914 of *Lecture Notes in Computer Science*, pages 65–77. Springer, 2011.

Author Index