

# Computability, Complexity and Randomness

Edited by

Verónica Becher<sup>1</sup>, Laurent Bienvenu<sup>2</sup>, Rodney Downey<sup>3</sup>, and  
Elvira Mayordomo<sup>4</sup>

1 University of Buenos Aires, AR, vbecher@dc.uba.ar

2 University Paris-Diderot, FR, laurent.bienvenu@liafa.jussieu.fr

3 Victoria University of Wellington, NZ, Rodney.Downey@vuw.ac.nz

4 University of Zaragoza, ES, elvira@unizar.es

---

## Abstract

Research on the notions of information and randomness has drawn on methods and ideas from computability theory and computational complexity, as well as core mathematical subjects like measure theory and information theory. The Dagstuhl seminar 12021 “Computability, Complexity and Randomness” was aimed to meet people and ideas in these areas to share new results and discuss open problems. This report collects the material presented during the course of the seminar.

**Seminar** 08.–13. January, 2012 – [www.dagstuhl.de/12021](http://www.dagstuhl.de/12021)

**1998 ACM Subject Classification** F.1.3 Complexity Measures and Classes, F.1.1 Computability theory, E.4 Coding and information theory

**Keywords and phrases** algorithmic randomness, computability theory, computational complexity, Kolmogorov complexity, algorithmic information theory

**Digital Object Identifier** 10.4230/DagRep.2.1.19

## 1 Executive Summary

*Verónica Becher*

*Laurent Bienvenu*

*Rodney Downey*

*Elvira Mayordomo*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Verónica Becher, Laurent Bienvenu, Rodney Downey, Elvira Mayordomo

Randomness and information quantity are central notions in computer science that are still undeveloped. Although classical information theory and probability provide formalizations of these notions they do not allow us to measure the information of a specific string or say that a particular real number is random. The definition of the property of randomness and its connection with a measure of information content was obtained in the 1960s and combines different complexity measures.

As witnessed by the three seminars previously organized in Dagstuhl on complexity and randomness (Seminar 9318, *Descriptive complexity: a multidisciplinary perspective* in 1993; Seminar 03181, *Centennial Seminar on Kolmogorov Complexity and Applications* in 2003; and Seminar 06051 *Kolmogorov Complexity and Applications* in 2006) in recent years there has been an upsurge produced by the people in computability theory that resulted in rapid progress in our understanding of even the most basic notions in randomness, and the solution of old open questions. This has changed and is still changing the landscape and opened up



Except where otherwise noted, content of this report is licensed

under a Creative Commons BY-NC-ND 3.0 Unported license

Computability, Complexity and Randomness, *Dagstuhl Reports*, Vol. 2, Issue 1, pp. 19–38

Editors: Verónica Becher, Laurent Bienvenu, Rodney Downey, and Elvira Mayordomo



Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

new avenues of research. An evidence of this activity has been the publication of two new books in the area and the new edition of an already classical one: *Algorithmic Randomness and Complexity*, R. Downey and D. Hirschfeldt, Foundations on Computing, Springer, 2010; *Computability and Randomness*, A. Nies, Oxford University Press, 2009; and *An Introduction to Kolmogorov Complexity and Its Applications*, M. Li and P. Vitanyi, third Edition, Springer Verlag, 2008.

Seminar 12021 has celebrated significant recent research progress. New results connect the theory of algorithmic randomness with computable analysis. We consider them important because they lead to the naturalness of the notions of algorithmic randomness. For instance, Brattka, Miller, and Nies translated the theorem “*every non-decreasing function is almost everywhere differentiable*” to the computable world, by showing that a real  $x$  is computably random if and only if every computable non-decreasing function is differentiable at  $x$  (this work is has not yet appeared as a publication). Similar investigations identified the notions of randomness that correspond to the Lebesgue density and differentiation theorems. J.Franklin and the work of Gács, Hoyrup, and Rojas related Birkhoff’s pointwise ergodic theorem in connection with Schnorr randomness.

Considerable results have been obtained for problems on Kolmogorov complexity and computable enumerable sets, in particular, in the degree structure that arises from comparing the complexity of the initial segments of two reals. Barmaplias announced the solution of the already long standing open problem posed by Downey and Hirschfeldt *Is there a minimal pair of c.e. reals in the K-degrees?* The answer is no.

Since the start of the discipline, the notion of randomness was defined for infinite sequences, or real numbers. The problem posed by Kolmogorov on a notion of randomness of finite objects remains unsolved. This is also the case for arbitrary countable objects. C.Freer made significant progress on the questions *When is a graph random?* and *What is the connection between quasi-random graphs and pseudorandom bit strings?* He pointed to an emerging theory of continuous limits of finite combinatorial structures that connects graph limits, property testing, and exchangeable relations.

There was a general consensus on the fact that there is yet no adequate solution to the fundamental problem that high-quality independent random bits are in very short supply. And there are many practical applications rely on randomness (for instance, assigning keys to users of a public-key crypto-system). Randomness extractors are algorithms developed “extract” high-quality random bits from low-entropy sources. Construction of such algorithms is foreseen to be an active research area.

The aim of Seminar 12021 was to bring together researchers covering this spectrum of relevant areas, to report their advances and to discuss the relevant research open questions. The seminar had 50 participants, including the most recognized senior specialists as well as young researchers. The atmosphere was very stimulating and led to new research contacts and collaborations.

**Concluding remarks and future plans.** The seminar was well received, as witnessed by the high rate of accepted invitations, and the exemplary degree of involvement by the participants. Due to the broad scope and depth of the problems on algorithmic randomness and information quantity that have been discussed in the presentations and informal discussions, the organizers regard the seminar as a great success. The organizers wish to express their gratitude towards the Scientific Directors of the Dagstuhl Center for their support of this seminar. We foresee the proposal of a new seminar focusing in the interplay between algorithmic randomness and computable analysis.

## Description of the seminar topics

### Anti-randomness

The class of sequences with minimal prefix-free Kolmogorov complexity, dubbed K-trivial sequences, were understudied until five years ago. In the seventies, Solovay proved that there is a non computable K-trivial. They are now very well understood, with a number of surprising characterizations and applications. For instance, the “cost function” construction of a K-trivial gives simplest known example of a non computable incomplete computably enumerable set, they also appear in the Kucera-Slaman solution to a well-known question about Turing degrees in Scott sets, also K-triviality has led to a better understanding of the reverse mathematics of the regularity of Lebesgue measure. K-triviality one of the most technically deep subjects in algorithmic randomness, significant questions remain open.

### Resource bounded versions

Classical computational complexity theory comes into play defining resource-bounded versions of Kolmogorov complexity, measure, and dimension. This has led to new characterizations of complexity classes involving efficient reducibility to the set of Kolmogorov random strings. Resource-bounded measure and dimension have been used to gain understanding of properties of complexity classes and their complete sets. For instance, they can be used as a probabilistic methods to prove lower bounds on nonuniform complexity.

### Derandomization and complexity hierarchies

Derandomization is the study of how to replace probabilistic algorithms with deterministic algorithms. Earlier work by Allender et al. showed that the techniques of derandomization could be viewed through the lens of resource-bounded Kolmogorov complexity theory, and gave significant applications. More recently, they proved that every sufficiently dense set in  $NP \cap coNP$  contains strings of low resource-bounded Kolmogorov complexity at every length. In still unpublished work, Allender and his co-authors show that if deterministic and nondeterministic exponential time coincide, this implies a partial collapse of the exponential-time hierarchy, shedding light on a question that has been open for two decades.

### Randomness extractors

Randomness extractors have been used and to derive zero-one laws for the packing dimensions of complexity classes and Turing degrees. Recently it has been shown that the converse direction also holds and Kolmogorov extraction is in fact equivalent to randomness extraction.

### Computational depth

The computational depth of a string is roughly the difference between its time-bounded Kolmogorov complexity, and its (plain) Kolmogorov complexity. Quite recently, Antunes and Fortnow showed that, under a plausible complexity assumption, computational depth is the right notion to present a “universal” poly-time samplable distribution, in the same way that Kolmogorov complexity allows one to define universal computable semi-measures. They derive a new characterization of algorithms that run in polynomial time on average, and give a relation with their worst-case running time.

**Algorithmic randomness and computable analysis**

The most accepted definition of randomness for infinite sequences, or real numbers, is based on constructive measure theory and was given by Martin Lőf, 1965. It coincides with the maximal initial segment complexity. Other notions have been proposed since then, by Schnorr, Demuth, Kurtz and others, either via measure theory, or via martingale theory. Most of these definitions have been very well studied in the space of infinite binary sequences, but less is known for other spaces (although there has been some deep founding work by Levin and Gács). Some natural questions are: for a given randomness notion, to what kind of probability space can this notion be extended? To what extent does the chosen space affect the properties of random objects? Then, for every probability space to which we can extend randomness notions, it is interesting to look at classical theorems from a randomness perspective, and try to convert classical theorems of the form “property  $P$  holds for  $\mu$ -almost every sequence” into “property  $P$  holds for every  $\mu$ -random sequence”. This line of study has recently been investigated in a number of different settings: random closed sets, effective ergodic theory, effective brownian motion, etc.

**Organization of the seminar and activities**

The seminar consisted in nineteen talks, sessions on open questions, and informal discussions among the participants. The organizers selected the talks in order to have comprehensive lectures giving overview of main topics and communications of new research results. Each day consisted of talks and free time for informal gatherings among participants. There were two main sessions on open questions.

## 2 Table of Contents

### Executive Summary

*Verónica Becher, Laurent Bienvenu, Rodney Downey, Elvira Mayordomo* . . . . . 19

### Overview of Talks





The Strange Link between Kolmogorov complexity and computational complexity classes <i>Eric Allender</i> . . . . .	25
Kolmogorov complexity and computably enumerable sets <i>George Barmpalias</i> . . . . .	25
Simple proofs for known inequalities on Kolmogorov complexity using games and symmetry of information <i>Bruno Bauwens</i> . . . . .	26
Connections between ergodic theory and randomness <i>Johanna Franklin</i> . . . . .	26
When is a graph random? <i>Cameron Freer</i> . . . . .	26
Lowness in algorithmic randomness <i>Noam Greenberg</i> . . . . .	27
Normality is equivalent to incompressibility by finite-state automata <i>Pablo A. Heiber</i> . . . . .	27
Communication complexity through the lense of Kolmogorov complexity <i>Michal Koucký</i> . . . . .	27
Constant compression and random weights <i>Wolfgang Merkle</i> . . . . .	28
Randomness and Lebesgue density theorem <i>Joseph S. Miller</i> . . . . .	28
Randomness extraction: a computability perspective <i>Benoit Monin</i> . . . . .	28
Randomness interacts with effective analysis <i>Andre Nies</i> . . . . .	29
Exponential time vs probabilistic polynomial time <i>Sylvain Perifel</i> . . . . .	29
Semi-explicit expanders and extractors and their applications <i>Andrej E. Romashchenko</i> . . . . .	30
Tutorial on randomness extractors <i>Ronen Shaltiel</i> . . . . .	30
Are random axioms useful? <i>Alexander Shen</i> . . . . .	30
The graph reachability problem <i>Vinodchandran Variyam</i> . . . . .	31

Rate-distortion and denoising, of individual sequences by Kolmogorov complexity <i>Paul Vitányi</i> . . . . .	31
<b>Open Problems</b>	
Questions on the link between Kolmogorov complexity and computational complexity classes <i>Eric Allender</i> . . . . .	32
Kolmogorov complexity and computably enumerable sets <i>George Barmpalias</i> . . . . .	32
Normal numbers computable in simple exponential time <i>Verónica Becher</i> . . . . .	33
Relating computability and logical theories <i>Laurent Bienvenu</i> . . . . .	33
Order functions and $K$ -triviality <i>Noam Greenberg</i> . . . . .	34
Questions on $K$ -triviality <i>André Nies</i> . . . . .	34
Questions on higher randomness <i>André Nies</i> . . . . .	34
Extraction of mutual information about two strings <i>Alexander Shen</i> . . . . .	35
Randomness with respect to a semimeasure <i>Alexander Shen</i> . . . . .	35
What do probabilistic methods tell us about the finite sets? <i>Theodore Slaman</i> . . . . .	36
On gales combined with computable exponential order functions <i>Ludwig Staiger</i> . . . . .	36
van Lambalgen-type theorem for time-bounded Kolmogorov complexity <i>Marius Zimand</i> . . . . .	37
Strong extractors for infinite sequences <i>Marius Zimand</i> . . . . .	37
<b>Participants</b> . . . . .	38

### 3 Overview of Talks

#### 3.1 The Strange Link between Kolmogorov complexity and computational complexity classes

*Eric Allender (Rutgers University – Piscataway, US)*

License     Creative Commons BY-NC-ND 3.0 Unported license  
© Eric Allender

This talk will survey a body of work that has developed over the last decade, that has led some researchers to suspect that certain important computational complexity classes can be better understood, by studying the computational power of the set of Kolmogorov-random strings.

More specifically, let  $R$  denote the set of Kolmogorov-random strings. Let BPP denote the class of problems that can be solved with negligible error by probabilistic polynomial-time computations, and let NEXP denote the class of problems solvable in nondeterministic exponential time.





Conjecture 1:  $\text{NEXP} = \text{NP}^R$ .

Conjecture 2: BPP is the class of problems non-adaptively polynomial-time reducible to  $R$ .

These are not only bold conjectures; they are obviously false!  $R$  is not a decidable set, and thus it is absurd to suggest that the class of problems reducible to it constitutes a complexity class. The absurdity fades if, for example, we interpret “ $\text{NP}^R$ ” to be “the class of problems that are NP-Turing reducible to  $R$ , no matter which universal machine we use in defining Kolmogorov complexity”. We are not yet able to prove that either conjecture (suitably interpreted) is true, but some recent theorems approach this goal. The lecture will highlight several problems that seem ripe for a fruitful blending of techniques from computability theory and complexity theory.

#### 3.2 Kolmogorov complexity and computably enumerable sets

*George Barmpalias (Chinese Academy of Sciences, CN)*


License     Creative Commons BY-NC-ND 3.0 Unported license  
© George Barmpalias

I will start with reporting a solution to a problem of Downey and Hirschfeldt from 2006 as well as further progress that I made on problems on the topic of Kolmogorov complexity of c.e. sets (in particular the structure of the c.e. K-degrees).

After this I will motivate this topic with several open questions which I find natural, yet I haven’t been able to solve.

### 3.3 Simple proofs for known inequalities on Kolmogorov complexity using games and symmetry of information

*Bruno Bauwens (Universidade do Porto, PT)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Bruno Bauwens

First we provide a remarkably simple game-proof that for every  $n$ , there is an  $x$  of length  $n$  such that  $C(C(x)|x) \geq \log n - O(1)$  and  $C(x) \geq n/2$ , slightly improving a result of Gacs and solving a conjecture of Chaitin and Solovay.

As an intermezzo we state symmetry of information for plain complexity as:


$$C(a, b) = K(a|C(a, b)) + C(b|a, C(a, b)),$$

which has two interesting known corollaries: Levin's formula  $C(a) = K(a|C(a))$  (taking  $b = C(a)$ ), and every infinitely often C-random real is 2-random.

Finally, we provide a short proof for Solovay's result (a bit improved) stating that for some strings plain complexity can be maximal but prefix-free complexity not. More precise: infinitely many strings  $x$  have  $C(x) = |x| - O(1)$  and  $K(x) = |x| + K(|x|) - \log \log |x| \pm O(1)$ . The proof only uses symmetry of information of prefix-free complexity, and Levin's and Gács' results (see above).

### 3.4 Connections between ergodic theory and randomness

*Johanna Franklin (Univ. Of Connecticut, US)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Johanna Franklin

Since randomness can be defined in terms of measure theory as well as Kolmogorov complexity, it is not surprising that it is related to other areas of mathematics where this concept is fundamental. In this talk, I will introduce the basic principles of ergodic theory, which is the study of the behavior of certain measure-preserving transformations over time, and explain the relationship between ergodic theory and randomness.

### 3.5 When is a graph random?

*Cameron Freer (MIT – Cambridge, US)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Cameron Freer

Joint work of Ackerman, Nate; Freer, Cameron; Patel, Rehana; Roy, Daniel


What is the connection between quasi-random graphs and pseudorandom bit strings? Can this be used to develop a useful theory of resource-bounded complexity for discrete structures? In the first half of the talk, we will describe the translation by Trevisan between notions in additive combinatorics and computational indistinguishability, and also highlight the emerging theory of continuous limits of finite combinatorial structures that connects graph limits, property testing, and exchangeable relations.



When is a countably infinite graph algorithmically random? In some cases, there is a natural probabilistic construction of the graph that gives rise to an obvious candidate for randomness, but in other cases this is not so clear. In the second half of the talk, we will discuss invariant measures concentrated on a given countable structure, which induces a notion of an algorithmically random copy of that structure.

### 3.6 Lowness in algorithmic randomness


Noam Greenberg (Victoria University of Wellington, NZ)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Noam Greenberg

I will give a survey of the project of understanding lowness for notions of effective randomness, and pass through some related topics. Characterising a notion of lowness *usually* involves traceability, and is obtained by forcing with an adequate class of closed sets. This, however, fails for the most familiar notion of randomness, namely Martin-Löf's. In this case lowness is inherently enumerable – the opposite of being obtained by forcing. Instead, weakness as an oracle can be measured by interaction with the Turing degrees of random sets (à la Day and Miller, for example).

### 3.7 Normality is equivalent to incompressibility by finite-state automata


Pablo A. Heiber (University of Buenos Aires, AR)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Pablo A. Heiber

Recall that an infinite sequence over a finite alphabet  $\Sigma$  is *normal* if for any given  $n$ , all possible patterns of length  $n$  appear in the sequence with equal frequency. We will present a direct and elementary proof of the following fact: an infinite sequence is normal if and only if it cannot be compressed by a finite-state compressor (injective finite state transducer).

### 3.8 Communication complexity through the lense of Kolmogorov complexity


Michal Koucký (Academy of Sciences – Prague, CZ)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Michal Koucký

In this talk I will survey recent developments in communication complexity related to the notion of information cost and privacy. This development raises interesting questions in the context of Kolmogorov complexity.

### 3.9 Constant compression and random weights


Wolfgang Merkle (*Universität Heidelberg, DE*)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Wolfgang Merkle

We introduce a new characterization of left recursively enumerable (left-r.e.) Martin-Löf random reals: a real is Martin-Löf random and recursively approximable from below if and only if it equals the weight of the compressible strings for some universal prefix-free machine. For sufficiently large intervals  $[a; b)$ , the weight of strings which are  $a$ -compressible strings but not  $b$ -compressible is a left-r.e. Martin-Löf random real, and in fact we can use finite intervals of compressibility to characterize the left-r.e. Martin-Löf randoms as well.

### 3.10 Randomness and Lebesgue density theorem

Joseph S. Miller (*University of Wisconsin – Madison, US*)


License  Creative Commons BY-NC-ND 3.0 Unported license  
© Joseph S. Miller

Joint work of Bienvenu, Laurent; Day, Adam; Hölzl, Rupert; Miller, Joseph S.; Nies, André

In this talk we will present several recent results on the interactions between effective randomness a Lebesgue differentiability theorem. In joint work with Bienvenu, Hölzl and Nies, we show that a real  $x$  is a point of positive density in every  $\Pi_1^0$  class it belongs to *if and only* it is Martin-Löf random and Turing incomplete (also known as *difference random*). In subsequent joint work with Day, this lead to a solution of a longstanding open question, namely, we prove that a real  $x$  is  $K$ -trivial if and only if for every incomplete random  $z$ ,  $x \oplus z$  is incomplete.

### 3.11 Randomness extraction: a computability perspective


Benoit Monin (*University Paris Diderot, FR*)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Benoit Monin

Suppose you want to generate a random sequence of zeros and ones and all you have at your disposal is a coin which you suspect to be biased (but do not know the bias). Can “perfect” randomness be produced with this coin? The answer is positive, thanks to a little trick discovered by von Neumann. We will present a generalization of this question: if we have access to a source of bits produced according to some probability measure in a given class of measures, and suppose we know the class but not the measure, can perfect randomness be produced? We will give a positive answer for a large class of probability measures. (as Bernoulli measures or Markov measures). Furthermore, this work naturally has some interesting connections with the Kjos-Hanssen’s concept of Hippocratic randomness. We will actually provide another interesting characterisation of (some) classes of measures for which Hippocratic randomness and Martin-Löf randomness are equivalent.

### 3.12 Randomness interacts with effective analysis

*Andre Nies (University of Auckland, NZ)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Andre Nies

**Joint work of** Bienvenu, Laurent; Brattka, Vasco; Freer, Cameron; Hoelzl, Rupert; Kjos-Hanssen, Bjørn; Kucera, Antonin; Miller, Joseph S.; Nies, André

We seek connections between algorithmic randomness and computable analysis. Tests correspond to computable functions on the unit interval. A real passes a test if and only if the corresponding function is differentiable at the real. In this way, for instance we characterize computable randomness and Schnorr randomness via differentiability of effective Lipschitz functions ([1, 2]; also work of Pathak-Rojas-Simpson, and Rute). We include a historical perspective [3]. The constructivist Osvald Demuth, working on differentiability of effective functions, anticipated major algorithmic randomness notions in the 1970s and 1980. He introduced Demuth randomness which is in the focus of present-day research on lowness properties of oracles. However, in [4] we show that the weaker notion of difference randomness, due to Franklin and Ng already suffices for the application to constructive analysis Demuth had in mind.


We also discuss algorithmic versions of the ergodic theorem. Finally we mention the interaction of higher randomness and differentiability of hyperarithmetical functions.

#### References

- 1 Brattka, Miller, and Nies. Randomness and differentiability. Submitted.
- 2 Freer, Kjos-Hanssen and Nies. Effective aspects of Lipschitz functions. In preparation.
- 3 Kucera and Nies. Demuth's path to randomness. To appear.
- 4 Bienvenu, Hoelzl, Miller and Nies. The Denjoy alternative for computable functions. Submitted.

### 3.13 Exponential time vs probabilistic polynomial time


*Sylvain Perifel (University Paris-Diderot, FR)*

**License**  Creative Commons BY-NC-ND 3.0 Unported license  
© Sylvain Perifel

People usually believe that probabilistic algorithms can be derandomized, meaning that randomness would not give additional power to polynomial-time algorithms. However our current knowledge is despairingly limited, not even ruling out the possibility that incredibly big complexity classes have polynomial probabilistic algorithms. More precisely, we don't know how to separate nondeterministic exponential time NEXP from probabilistic polynomial time BPP, even if we believe that  $BPP=P$  (!). After presenting the state of the art, we shall discuss some attempts and strategies to resolve these questions and related circuit lower bounds. The tools will range from resource-bounded Kolmogorov complexity to interactive protocols.

### 3.14 Semi-explicit expanders and extractors and their applications


*Andrej E. Romashchenko (CNRS, Université Montpellier II, FR)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Andrej E. Romashchenko

Explicit constructions of graphs with some “random” properties (e.g., expanders and extractors) are known to be a mighty tool in computer science. Despite an impressive progress in this area, the known effective constructions of such graphs still do not always match the parameters achievable by truly random graphs. We are going to discuss constructions of extractors and expanders where the combinatorial parameters are made better while the conventional requirement of “explicitness” is somehow relaxed, e.g., a graph should be constructed in polynomial space but not in polynomial time, or the property of expansion/randomness extraction should hold only for a tiny family of sets of vertices, or a construction may involve some reduced (but not negligible) random seed. We illustrate these methods with several applications: a version of Muchnik’s conditional complexity theorem (for space bounded Kolmogorov complexity), the optimal compression of sets in PSPACE, nearly optimal bit-probe schemes for membership problem (by recent papers of D.Musatov, A.Shen, M.Zimand and A.R.).

### 3.15 Tutorial on randomness extractors


*Ronen Shaltiel (University of Haifa, IL)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Ronen Shaltiel

We give an introduction to the area of “randomness extraction” and survey the main concepts of this area: deterministic extractors, seeded extractors and multiple sources extractors. For each one we briefly discuss background, definitions, explicit constructions and applications.

### 3.16 Are random axioms useful?

*Alexander Shen (Université de Provence, FR)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Alexander Shen


The famous Gödel incompleteness theorem says that for every sufficiently rich formal theory there exist true unprovable statements. Such statements would be natural candidates for being added as axioms, but how can we obtain them? One classical (and well studied) approach is to add (to some theory  $T$ ) an axiom that claims the consistency of  $T$ .

Here we discuss another approach (motivated by Chaitin’s version of the Gödel theorem) where axioms claiming randomness (incompressibility) of some strings are added, and show that it is not really useful (in the sense that it does not help us to prove new interesting theorems). This result answers a question recently asked by Lipton. However, the situation changes if we take into account the size of the proofs: randomly chosen axioms may help to make proofs much shorter (unless  $NP=PSPACE$ ). This result (partially) answers the question asked a while ago by Shen. We also study what can be achieved by adding axioms of type

“complexity of  $x$  exceeds  $n$ ” for some strings  $x$  and numbers  $n$ . We show that by adding all true statements of this type, we obtain a theory that proves all true universal statements. Moreover, it is enough to add one statement of this type for each  $n$  (or even for infinitely many  $n$ ) if strings are chosen in a special way. On the other hand, one may add statements of this type for most  $x$  of length  $n$  (for every  $n$ ) still having a weaker theory. Finally, we consider a theory that claims Martin-Löf randomness of a given infinite binary sequence. This claim can be formalized in different ways. We show that different formalizations are closely related but not equivalent, and study their properties.

### 3.17 The graph reachability problem

*Vinodchandran Variyam (University of Nebraska – Lincoln, US)*


License  Creative Commons BY-NC-ND 3.0 Unported license  
© Vinodchandran Variyam

The graph reachability problem, the computational problem of deciding whether there is a path between two given vertices in a graph, is the canonical problem while studying space bounded computations.

Different variations of this problem characterize various important space bounded complexity classes. Understanding the complexity of the reachability problem is a central concern of computational complexity theory. In this talk I will revisit some well known open problems regarding the space complexity of the reachability problem and discuss certain approaches toward them.

### 3.18 Rate-distortion and denoising, of individual sequences by Kolmogorov complexity

*Paul Vitanyi (CWI – Amsterdam, NL)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Paul Vitanyi


Joint work of de Rooij, Steven; Vereshchagin, Nikolay K.; Vitanyi, Paul

The canonical rate-distortion function of a single string is related to the more standard rate-distortion function of Shannon for the given distortion measure. Examples are Hamming distortion, List distortion, and Euclidean distortion. The rate-distortion function for individual sequences can and does assume a wide class of shapes (unlike Shannon’s). Low algorithmic mutual information is related to low Kolmogorov complexity. Destination words having lower distortion to the source word have more properties in common with the source word (hard or impossible to formalize in Shannon’s theory) and this suggests an approach to denoising.

## 4 Open Problems

### 4.1 Questions on the link between Kolmogorov complexity and computational complexity classes

*Eric Allender (Rutgers University – Piscataway, US)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Eric Allender

Recall  $\Delta_1^0 \cap \bigcap_U P_{dt}^{R_{C_U}} = P$ , where  $R_{C_U}$  is the set of random strings using universal machine  $U$ :  $R_{C_U} = \{x : C_U(x) \geq |x|\}$ . We know that it is necessary to take the intersection over all universal machines  $U$ ; however, it is not obvious that the other intersection is necessary. This motivates the first two questions below:

**Question 1:** Does it hold that  $\bigcap_U P_{dt}^{R_{C_U}} \subseteq \Delta_1^0$ ?

**Question 2:** Do there exist machines  $U_1, U_2$  such that the two sets  $R_{K_{U_1}}, R_{K_{U_2}}$  are minimal pairs with respect to  $\leq_{tt}$  or  $\leq_{wtt}$ ?

**Question 3:** Recall that there exists  $U$  such that the Halting problem  $H$  is not in  $NP^{R_{K_U}}$ . (This is not true if we consider plain Kolmogorov complexity  $C$  instead of prefix-free complexity  $K$ .) Show that this holds for *every*  $U$ .

**Question 4:** We know that, for all  $U$  and for all  $t \ll 2^n$ ,  $H \not\leq_{dt}^{Dtime(t)} R_{C_U}$ . We also know that, for *some*  $U$ ,  $H$  is dtt-reducible to  $R_{C_U}$  in doubly-exponential time. Close this gap between exponential and doubly-exponential time.

**Question 5:** Hitchcock has shown that the exponential time class E contains sets that are not poly-time dtt-reducible to  $R$  (no matter which universal machine one uses). Does this hold for small time bounds as well? That is, is it true for every superpolynomial  $t(n)$ , that  $Dtime(t(n)) - P_{dt}^R \neq \emptyset$ ?

**Question 6:** We know that, for every decidable set  $A$  outside PSPACE, there is some  $U$  such that  $A \notin P_{tt}^{R_{K_U}}$ ; thus in particular  $H \notin P_{tt}^{R_{K_U}}$ . Show that this holds for  $C$ -complexity as well. That is, show there is a  $U$  such that  $H \notin P_{tt}^{R_{C_U}}$ . [Then try to show that this is true for *every*  $U$ .]

### 4.2 Kolmogorov complexity and computably enumerable sets

*George Barmpalias (Chinese Academy of Sciences, CN)*

License  Creative Commons BY-NC-ND 3.0 Unported license  
© George Barmpalias

**Question:** Is there a pair of sequences  $x, y$  which are not  $K$ -trivial and

$$\min(K(x \upharpoonright n), K(y \upharpoonright n)) \leq K(n) + c?$$

**Question:** Is there a c.e. set where the initial segment complexity is maximal amongst the c.e. sets? The same question holds for the global structure of  $\leq_K$  (Miller and Yu).





Also the same question holds for the set of non random strings.

**Question:** What is the algorithmic independence of c.e. sets? Compare with the work of Levin, Calude and Zimmand on algorithmic independence.

**Question:** Recall that an order is a strictly increasing computable function  $f : \mathbb{N} \rightarrow \mathbb{N}$ . Let  $X_f = \{f(n) \mid n \in X\}$ .  $X$  is  $K$ -invariant under  $f$  if  $X \equiv_K X_f$ . Characterize their degrees (called  $K$ -resolute sequences).

### 4.3 Normal numbers computable in simple exponential time

Verónica Becher (*Universidad de Buenos Aires, AR*)

License     Creative Commons BY-NC-ND 3.0 Unported license  
© Verónica Becher

It is fair to say that Borel's question on providing an example of an absolutely normal number (normal to every integer base) is still unresolved because the few known instances are not completely satisfactory: it is desirable that the number be easily computable, we would like to exhibit the number explicitly.





Turing's algorithm and the computable reformulation of Sierpiński's work are the only known constructions of computable normal numbers. Unfortunately, they both require double exponentially many steps to produce a next digit of the expansion of a constructed number. The existence of normal numbers computable in simple exponential time is ensured by a theorem of Strauss in [1]; however, no specific instances have yet been identified.

#### References

- 1 Strauss, Martin, 1997. Normal numbers and sources for BPP. *Theoretical Computer Science* 178, 155-169.

### 4.4 Relating computability and logical theories

Laurent Bienvenu (*Université Paris-Diderot, FR*)

License     Creative Commons BY-NC-ND 3.0 Unported license  
© Laurent Bienvenu

Following A. Shen's talk, here are some interesting open questions about the axiomatic power of Kolmogorov complexity:

**Question:** Is it possible to find an example when some information about Kolmogorov complexity gives us the power to compute  $\emptyset'$ , yet not allowing us, on a proof-theoretic level, to prove all true  $\Pi_1^0$ -statements ?


**Question:** We know from Chaitin's theorem that one can only prove finitely many statements of type " $C(x) > n$ ". How about statements of type " $C(x) \notin [n_1, n_2]$ " ?

**Question:** Can one give a characterization of the sequences  $(x_n)$  of strings such that  $x_n \in 2^n$  and  $C(x_n) \geq n$  such that, adding for each  $n$  the axiom " $C(x_n) \geq n$ " for each  $n$ , we can prove all true  $\Pi_1^0$ -statements?

**Question:** Is there a sequence  $(x_n)$  of strings such that  $x_n \in 2^n$  and  $C(x_n) \geq n$  such that, adding for each  $n$  the axiom " $C(x_n) \geq n/2$ " for each  $n$ , we can prove all true  $\Pi_1^0$ -statements?

## 4.5 Order functions and $K$ -triviality

Noam Greenberg (Victoria University of Wellington, NZ)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Noam Greenberg


The goal is to find a combinatorial (or discrete) characterisation of  $K$ -triviality. That is, one that does not mention measure, Kolmogorov complexity, or randomness. Such dual characterisations are available for example for lowness for Schnorr randomness and for strong jump-traceability.

One possible approach is via traceability. Let  $h$  be an order function (a computable, non-decreasing, and unbounded function from  $\omega$  to  $\omega - \{0\}$ ). Recall that a Turing degree  $\mathbf{a}$  is  $h$ -jump-traceable if every  $\mathbf{a}$ -partial computable function has a c.e. trace bounded by  $h$ . The aim is to identify a collection  $\mathcal{H}$  of order functions such that a degree is  $K$ -trivial if and only if it is  $h$ -jump-traceable for all  $h \in \mathcal{H}$ . We have some approximations of such a result. For example, it is known that if  $\mathbf{a}$  is  $\sqrt{\log n}/9$ -jump-traceable then it is  $K$ -trivial; and that every  $K$ -trivial degree is  $O(h)$ -jump-traceable for any summable order function  $h$  ( $\sum 2^{-h(n)} < \infty$ ). The latter result comes from a characterisation of  $K$ -triviality (by Hölzl, Kräling and Merkle) using jump-traceability with respect to a collection of bounds which is defined using Solovay functions and Kolmogorov complexity  $K$ .

The dividing line may be some constant multiple of the logarithm function. Here we have a related result: if every  $K$ -trivial degree is  $(\log n)/10$ -jump-traceable, then there is no minimal pair of LR-hard c.e. degrees.

## 4.6 Questions on $K$ -trivials

André Nies (University of Auckland, NZ)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© André Nies

**Question** (open since 2005): Let  $A$  be  $K$ -trivial. Is there a  $T$ -incomplete Martin Löf random  $Z$  such that  $Z \geq_T A$ ?

**Question** (open since 2006): Let  $\mathcal{K}$  be the ideal of  $K$ -trivial degrees. Are there c.e.  $\mathbf{a}, \mathbf{b}$  such that  $\mathcal{K} = [\mathbf{0}, \mathbf{a}] \cap [\mathbf{0}, \mathbf{b}]$ ?

**Question** (open since 2011): A function  $f : \omega \rightarrow \omega$  is  $K$ -trivial if there is  $c$  such that  $\forall n [K(f \upharpoonright n) \leq K(0^n) + c]$ . Can we compute, from a  $K$ -trivial constant from the graph of  $f$  (as a set) a  $K$ -trivial constant for  $f$ ?

## 4.7 Questions on higher randomness

André Nies (University of Auckland, NZ)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© André Nies

Recall the definitions:

$Z$  is  $\Pi_1^1$ -random if  $Z$  is in no null  $\Pi_1^1$  set.



$Z$  is higher weakly 2-random if  $Z$  passes all  $\Pi_1^1$  weak 2-tests (i.e.,  $Z \notin \bigcap_m G_m$ , where “ $[\sigma] \subseteq G_m$ ” is  $\Pi_1^1$ , and  $\lim_{m \rightarrow \infty} \lambda G_m = 0$ ).

**Question** (open since 2005): Is there a non hyperimmune set that is low for  $\Pi_1^1$ -random?




**Question** (posed in Chapter 9, *Computability and Randomness*, A. Nies, Oxford University Press, 2009): Show the properness of these implications.

$\Pi_1^1$ -random  $\Rightarrow$  higher weakly 2-random  $\Rightarrow$   $\Pi_1^1$ -Martin Lőf random.

The last implication was recently announced by Yu Liang.

## 4.8 Extraction of mutual information about two strings

Alexander Shen (*Université de Provence, FR*)

License     Creative Commons BY-NC-ND 3.0 Unported license  
© Alexander Shen





Let  $A_1, \dots, A_n$  be a tuple of strings. If  $X$  is a random oracle, with high probability it does not change significantly the complexities of  $A_i$ , of pairs  $(A_i, A_j)$ , etc. The question is whether the same is true for other properties expressed in terms of complexity.

**A specific question:** assume that for a random  $X$  the strings  $A_1, A_2$  have common information (extractable mutual information): there exists a string  $B$  such that  $C(B|A_1, X) \approx 0$ ,  $C(B|A_2, X) \approx 0$ , and  $C(B|X) \approx I(A_1 : A_2|X)$ . Is the same true without an oracle?

**Another question** about oracles and tuples of strings: is it always possible for given  $A_1, \dots, A_n$  to find some oracle  $X$  such that  $C(A_i|X) \approx 0.5 C(A_i)$ ?

## 4.9 Randomness with respect to a semimeasure

Alexander Shen (*Université de Provence, FR*)


License     Creative Commons BY-NC-ND 3.0 Unported license  
© Alexander Shen

Let  $L$  be some probabilistic machine that uses the internal random bits generator to produce a sequence of output bits. Such a machine  $L$  has an output distribution which corresponds to a semimeasure:  $l(x)$  equals the probability that the output of  $L$  has  $x$  as a prefix. In this way we can obtain all semimeasures on the binary tree (lower semicomputable functions on finite strings with nonnegative values such that  $l(\Lambda) = 1$  for the empty string  $\Lambda$  and  $l(x) \geq l(x0) + l(x1)$  for every string  $x$ ). Now consider the infinite outputs of  $L$  for all Martin-Löf random sequences used as random bits.

**Question:** is this set of sequences determined by  $l$  or different machines with the same output distributions can lead to different sets? (If determined by  $l$ , this set can be considered as the set of random sequences with respect to a semimeasure  $l$ . This would extend the Martin-Löf definition of randomness to semimeasures.)

## 4.10 What do probabilistic methods tell us about the finite sets?

Theodore Slaman (University of California – Berkeley, US)

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Theodore Slaman

I would like to propose an investigation of the heuristic question, “What do probabilistic methods tell us about the finite sets?” For this, we would like both lower bounds, saying that certain properties  $P$  of the finite sets can be established by probabilistic methods, and upper bounds, saying that any theorem about the finite sets established probabilistically has an alternate proof from purely number-theoretic properties  $Q$ . Still speaking informally, we would like to know the power of and limitations on probabilistic methods as applied to number-theoretic questions.

For example, we might express a version of this question using the formalism of second-order arithmetic, in which one has the language appropriate to express properties of the natural numbers  $n$  with addition, multiplication, and order, and also to refer to subsets  $X$  of the natural numbers with the relation “element of” allowing formulas of the form “ $n$  is an element of  $X$ .” It is standard to use the theory  $RCA_0$  to formalize computable methods, where  $RCA_0$  includes the basic properties of  $+$  and  $\times$  ( $P-$ ), the principle of induction for  $\Sigma_1^0$  sets of numbers (to allow for the definition of total computable functions by recursion), and the property that the sets of numbers are closed under relative computation.

Now consider augmenting  $RCA_0$  by postulating the existence of relative random reals. Let 1 –  $RAN$  be the formal statement that for every set  $X$  there is a set  $R$  which is Martin-Löf relative to  $X$ . Let 2 –  $RAN$  be the analogous statement for 2-randoms. Applying a theorem of Harrington, if  $\varphi$  is an arithmetic sentence which is provable from “ $RCA_0 + 1 - RAN$ ,” then  $\varphi$  is provable from  $RCA_0$ . In other words, the use of randomness can be eliminated.


Recent results with Conidis, show that there is an arithmetic sentence which is provable from “ $RCA_0 + 2 - RAN$ ” and not provable from  $RCA_0$ . So, this use of randomness cannot be eliminated. However, if  $\varphi$  is an arithmetic sentence which is provable from “ $RCA_0 + 2 - RAN$ ,” then  $\varphi$  is provable from “ $RCA_0 + B - \Sigma_2^0$ .” Here,  $B - \Sigma_2$  is the assertion that if  $F$  is a finite set and  $\psi$  is a  $\Sigma_2^0$  formula relative to the set  $X$  such that  $\psi$  holds for every number in  $F$ , then there is a bound on the existential witnesses needed to verify  $\psi$  on  $F$ .

**Specific question:** It is also known that  $B - \Sigma_2$  is not provable from “ $RCA_0 + 2 - RAN$ ”, and it would be very interesting to obtain a natural number-theoretic axiomatization of the number-theoretic consequences of “ $RCA_0 + 2 - RAN$ .” The same is true for “ $RCA_0 + k - RAN$ ”, for larger values of  $k$ .

**Heuristic question.** Identify the natural contexts, beyond purely computable, in which randomness is used to shed light on the finite and determine in which cases the arguments based on concepts of measure and randomness cannot be removed.

## 4.11 On gales combined with computable exponential order functions

Ludwig Staiger (Martin-Luther-Universität Halle-Wittenberg, DE))

License  Creative Commons BY-NC-ND 3.0 Unported license  
© Ludwig Staiger





Lutz’s  $s$ -(super-)gales are (super-)martingales combined with exponential order functions. They are mainly considered as computable or left-computable functions having a (weakly) com-

putable value of  $s$ . This corresponds to computable or left-computable (super-)martingales combined with (weakly) computable exponential order functions.

**Question:** Are there computable or left-computable  $s$ -(super-)gales for non-(weakly) computable values of  $s$  which are not  $s'$ -(super-)gales for a value  $s' < s$ ?

## 4.12 van Lambalgen-type theorem for time-bounded Kolmogorov complexity

Marius Zimand (Towson University, US)





License     Creative Commons BY-NC-ND 3.0 Unported license  
© Marius Zimand

For unrestricted Kolmogorov complexity, it holds that if we put together two sequences (or strings) such that each one of them is random given the other one the result is random. More precisely if  $x \in \{0, 1\}^\omega$  is (Martin-Löf, Schnorr, computable) random conditioned by  $y$ , and  $y \in \{0, 1\}^\omega$  is random conditioned by  $x$ , then  $x \oplus y$  is random (van Lambalgen Theorem). The same holds for finite strings  $x$  and  $y$  that are  $c$ -random conditioned by each other (meaning  $C(x | y) \geq |x| - c$ ,  $C(y | x) \geq |y| - c$ , and also if we replace  $C$  by  $K$ ). For time-bounded Kolmogorov complexity this question is open. More precisely, the question is:

**Question:** Let  $x, y$  be  $n$ -bit strings such that for some constant  $c$  and some polynomial-time bound  $p(n)$ ,  $C^{p(n)}(x | y) \geq n - c$  and  $C^{p(n)}(y | x) \geq n - c$ . What can we say about the  $C^{poly(n)}(xy)$ ? (Perhaps, under some computational complexity assumption, one can show that it is  $\ll 2n$ .)

## 4.13 Strong extractors for infinite sequences

Marius Zimand (Towson University, US)

License     Creative Commons BY-NC-ND 3.0 Unported license  
© Marius Zimand

It is known that Kolmogorov extractors for two independent sequences exist. For example there exists a Turing reduction (even truth-table reduction) such that for each sequences  $x$  and  $y$  that have each effective dimension, say  $1/2$ , and are independent, it holds that that  $f^{x \oplus y}$  has effective dimension 1.

**Question:** Is it possible to have a Turing-reduction  $f$  such that for all  $x$  and  $y$  as above, computes a sequence that has effective dimension 1 even conditioned by  $x$ , and also conditioned by  $y$ ?

For  $x$  and  $y$  finite strings (or finite distributions) the corresponding  $f$  exists and is called strong Kolmogorov extractor (and respectively strong extractor).

## Participants

- Eric Allender  
Rutgers Univ. – Piscataway, US
- Klaus Ambos-Spies  
Universität Heidelberg, DE
- George Barmpalias  
Chinese Academy of Sciences, CN
- Bruno Bauwens  
Universidade do Porto, PT
- Verónica Becher  
University of Buenos Aires, AR
- Laurent Bienvenu  
University Paris-Diderot, FR
- Harry Buhrman  
CWI – Amsterdam, NL
- Douglas Cenzer  
University of Florida –  
Gainesville, US
- Chris J. Conidis  
University of Waterloo, CA
- Quinn Culver  
Univ. of Notre Dame, US
- David Diamondstone  
Victoria Univ. of Wellington, NZ
- Rodney Downey  
Victoria Univ. of Wellington, NZ
- Lance Fortnow  
Northwestern University –  
Evanston, US
- Johanna N. Y. Franklin  
Univ. Of Connecticut, US
- Cameron Freer  
MIT – Cambridge, US
- Noam Greenberg  
Victoria Univ. of Wellington, NZ
- Serge Grigorieff  
University Paris-Diderot, FR
- Pablo A. Heiber  
University of Buenos Aires, AR
- John Hitchcock  
University of Wyoming, US
- Rupert Hölzl  
University Paris-Diderot, FR
- Michal Koucký  
Academy of Sciences –  
Prague, CZ
- Thorsten Kräling  
Universität Heidelberg, DE
- Antonin Kucera  
Charles University – Prague, CZ
- Sophie Laplante  
INRIA Saclay – Orsay, FR
- Andrew Lewis  
University of Leeds, GB
- Bruno Loff  
CWI – Amsterdam, NL
- Elvira Mayordomo  
University of Zaragoza, ES
- Wolfgang Merkle  
Universität Heidelberg, DE
- Joseph S. Miller  
University of Wisconsin –  
Madison, US
- Benoit Monin  
University Paris-Diderot, FR
- Philippe Moser  
Nat. University of Ireland, IE
- Satyadev Nandakumar  
Indian Inst. of Technology –  
Kanpur, IN
- Andre Nies  
University of Auckland, NZ
- Sylvain Perifel  
University Paris-Diderot, FR
- Christopher P. Porter  
Univ. of Notre Dame, US
- Robert Rettinger  
FernUniversität in Hagen, DE
- Andrej E. Romashchenko  
CNRS, Univ. Montpellier II, FR
- Ronen Shaltiel  
University of Haifa, IL
- Alexander Shen  
Université de Provence, FR
- Theodore A. Slaman  
University of California –  
Berkeley, US
- Ludwig Staiger  
Martin-Luther-Universität  
Halle-Wittenberg, DE
- Antoine Tavenaux  
University Paris-Diderot, FR
- Leen Torenvliet  
University of Amsterdam, NL
- Daniel Turetsky  
Victoria Univ. of Wellington, NZ
- Vinodchandran N. Variyam  
Univ. of Nebraska – Lincoln, US
- Stijn Vermeeren  
University of Leeds, GB
- Paul M. B. Vitanyi  
CWI – Amsterdam, NL
- Vladimir Viyugin  
IITP – Moscow, RU
- Osamu Watanabe  
Tokyo Institute of Technology, JP
- Marius Zimand  
Towson University, US

