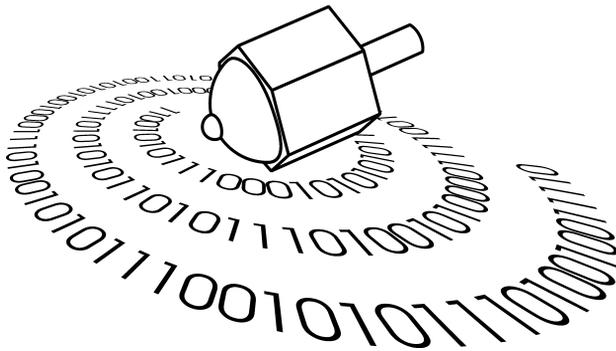Conference on
Logic, Computability and Randomness 2007

January 10 - 13, Buenos Aires, Argentina

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Program Committee

Veronica Becher   Universidad de Buenos Aires, Argentina
Rod Downey   Victoria University, Wellington, New Zealand
Denis Hirschfeldt   University of Chicago, USA

Local Organizers

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Verónica Becher
Santiago Figueira
Daniel Gorín
Sergio Mera
Mariano Pérez Rodríguez

www.dc.uba.ar/logic2007

Sponsors

Conference Address

Fundación YPF
Centro José A. Estenssoro
Echeverría 659
Buenos Aires - Argentina

Contents

Abstracts of invited talks

Abstracts of contributed talks

Arithmetic circuits, real numbers and the counting hierarchy

Eric Allender

Rutgers, the State University of NJ
Department of Computer Science
Piscataway, NJ 08854-8019, USA
allender@cs.rutgers.edu

Arithmetic circuit complexity is the object of intense study in three different subareas of theoretical computer science:

1. **Derandomization.** The problem of determining if two arithmetic circuits compute the same function is known as ACIT (arithmetic circuit identity testing). ACIT is the canonical example of a problem in BPP that is not known to have a deterministic polynomial-time algorithm. Kabanets and Impagliazzo showed that the question of whether or not ACIT is in P very tightly linked to the question of proving circuit size lower bounds [5].

2. **Computation over the Reals.** The Blum-Shub-Smale model of computation over the reals is an algebraic model that has received wide attention [2].

3. **Valiant's Classes VP and VNP.** Valiant characterized the complexity of the permanent in two different ways. Viewed as a function mapping n-bit strings to binary encodings of Natural numbers, the permanent is complete for the class #P [7]. Viewed as an n-variate polynomial, the permanent is complete for the class VNP [6].

The general thrust of these three subareas has been in three different directions, and the questions addressed seem quite different

from those addressed by work in the numerical analysis community, such as that surveyed by Demmel and Koev [4].

This talk will survey some recent work that ties all of these areas together in surprising ways. Most of the results that will be discussed can be found in [1, 3], but I will also discuss some more recent progress.

References

[1] E. Allender, P. Bürgisser, Johann Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. In *Proc. 21st Ann. IEEE Conf. on Computational Complexity (CCC '06)*, pages 331–339, 2006.

[2] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer, 1998.

[3] P. Bürgisser. On defining integers in the counting hierarchy and proving lower bounds in algebraic complexity. Technical Report TR06-113, Electronic Colloquium on Computational Complexity, 2006.

[4] J. Demmel and P. Koev. Accurate and efficient algorithms for floating point computation. In *Proceedings of the 2003 International Congress of Industrial and Applied Mathematics*, 2003.

[5] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. In *Proc. ACM Symp. Theory Comp.*, pages 355–364, 2003.

[6] L. Valiant. Completeness classes in algebra. In *Proc. ACM Symp. Theory Comp.*, pages 249–261, 1979.

[7] L. Valiant. The complexity of computing the Permanent. *Theoret. Comp. Sci.*, 8:189–201, 1979.

An excursion through the algebras of Lukasiewicz infinite-valued logic

Roberto Cignoli

IAM - CONICET, UBA
Argentina
cignoli@dm.uba.ar

J. Lukasiewicz introduced his systems of many-valued logics in the early twenties of the last Century with a strong philosophical motivation. MV-algebras were introduced by C. C. Chang in 1958 to give an algebraic proof of the completeness of certain axioms for Lukasiewicz infinite-valued logic. The aim of this talk is to show some connections of MV-algebras with lattice-ordered abelian groups, the Murray - von Neumann order of projections in operator algebras, Ulam games with lies, toric varieties.

Computably enumerable, strongly jump-traceable reals

Noam Greenberg

School of Mathematics, Statistics and Computer Science
Victoria University of Wellington
New Zealand
der.erlkoenig@gmail.com

Notions of traceability and lowness for randomness have been intertwined since Terwijn and Zambella have shown that a real is low for Schnorr tests iff it is computably traceable. Recently, Figueira, Nies and Stephan introduced the class of *strongly jump-traceable* reals. We show that in the computably enumerable degrees, they form a proper sub-ideal of the K-trivial reals and that none cup over $\mathbf{0}'$ with a Martin-Löf random real. Joint work with Rod Downey and Peter Cholak.

Complexity and programming: the distinct meaning of one-way functions in the continuous world

Joos Heintz

University of Buenos Aires
Argentina and
University of Cantabria
Spain
joos@dm.uba.ar

Joint work with B. Kuijpers, University of Hasselt, Belgium.

This talk is devoted to complexity issues in a simplified model of scientific computation (polynomial equation solving), taking into account the interdependence of symbolic and numeric aspects.

Unlike in classic (bit) complexity theory, efficient encoding of mathematical objects in scientific computing is often *not unique* and the transition of one data structure to another leads generally to deep complexity problems of unknown status. Therefore the corresponding computer programs should make use of rather sophistic (higher type) data types (like circuits) and not only of simple minded (type zero) data structures (like vectors and arrays). This leads to a new model of (*uniform*) computation, which includes specification, and correctness proofs by means of asserted programs. The semantic and syntactic aspects of such computations should be strongly separated.

Inspired by foundational questions of relational database theory, there exist already several attempts to model this situation by means of a (hidden or explicit) concept of computing on structures (see [1, 2, 3, 5, 12, 13]). However these attempts do not reflect the reality of programming and program execution, because they are based on the implicit assumption of a unique encoding of the mathematical objects under consideration. As a consequence of this hidden

assumption (e. g. of the isomorphism postulate of Y. Gurevich´s Abstract State Machines [5]) one obtains a more or less immediate proof that *parametric geometric elimination* requires *exponential sequential time*.

On the other hand there exists an approach to complexity issues with non-unique data structures in a *non-uniform* model (based on vectors and arrays of fixed length). In this context, *Constraint Database* Theory is used in order to specify algorithms. This leads to the notion of *geometric query*. However, there are elimination problems, which can be specified as geometric queries and have *intrinsically exponential complexity* [8].

The Constraint Data Base model is also well suited in order to characterize computational models, which are based on autonomous calculations interleaved with querying inputs (frequently of higher type) or environments (see [5, 7, 10, 11]). As mentioned before, in such models parametric geometric elimination requires *exponential* sequential time.

Recursive algorithms with a priori bounded data swell (in the spirit of the Bellantoni- Cook characterization [4, 7] of the class P) are not expressive enough for elimination tasks. On the other hand, the recursive call of even optimal elimination algorithms leads to uncontrolled data swell. In order to circumvent this difficulty, recursive elimination algorithms have to reduce stepwise their intermediate results to intrinsic geometric data. However it may happen that the expansion of such a reduced intermediate result may become of intrinsic exponential complexity, at least if one requires that the algorithm remains "numerically robust" [6].

Such an instance is given by the robust numerical interpolation of polynomial functions with low approximative arithmetic circuit complexity [9].

This example shows also a substantial difference between discrete and continuous computing: whereas the existence and the exhibition of one-way functions is a fundamental problem in discrete computation with many application, a formal translation of the same question to the continuous world is not too difficult to answer [6, 9].

6

References

[1] S. Abiteboul, C. H. Papadimitriou, V. Vianu. The Power of Reflective Relational Machines. Logic in Computer Science (1994) 230-240

[2] S. Abiteboul, C. H. Papadimitriou, V. Vianu . Reflective Relational Machines. Information and Computation, 143 (2) (1998) 110-136

[3] S. Abiteboul, V. Vianu. Computing on Structures. In Proceedings of the 20th international Colloquium on Automata, Languages and Programming. A. Lingas, R. G. Karlsson, and S. Carlsson, Eds. Springer LNCS 700 (1993) 606-620

[4] S. Bellantoni, S. Cook. A new recursion-theoretic characterization of the polytime functions. Comput. Complex. 2 (2) (1992) 97-110

[5] A. Blass, Y. Gurevich. Ordinary interactive small-step algorithms, I. ACM Trans. Comput. Logic 7 (2) (2006), 363-419

[6] D. Castro, M. Giusti, J. Heintz, G. Matera, L. M. Pardo. The hardness of polynomial equation solving. Foundations of Computational Mathematics 3 (2003) 1-74

[7] P. Clote. Computational Models and Function Algebras. In Selected Papers From the international Workshop on Logical and Computational Complexity. D. Leivant, Ed. Springer LNCS 960 (1994) 98-130.

[8] M. Giusti, J. Heintz, B. Kuijpers. The evaluation of geometric queries: constraint databases and quantifier Elimination. Manuscript Hasselt University (2006)

[9] J. Heintz, B. Kuijpers. Constraint data bases, data structures and efficient query elimination. Constraint Databases. Proceedings of the 1st International Symposium Applications of Constraint Databases (CDB'04), B. Kuijpers, P. Revesz, eds., Springer LNCS 3074 (2004) 1-24.

7

[10] B. Kapron, S. A. Cook. A new characterization of Mehlhorn's polynomial time functionals. 32nd Annual Symposium on Foundations of Computer Science (1991) 342-347

[11] K. Mehlhorn. Polynomial and abstract subrecursive classes. Proceedings of the Sixth Annual ACM Symposium on theory of Computing STOC '74. ACM Press (1974) 96-109

[12] Y. Moschovakis. What Is an Algorithm? Björn Engquist and Wilfried Schmid, Eds. Mathematics Unlimited – 2001 and Beyond. Springer Verlag (2001)

[13] Y. Moschovakis. On founding the theory of algorithms. Truth in mathematics H. G. Dales and G. Oliveri, Eds., Clarendon Press, Oxford (1998) 71-104.

Countable Π_1^0 classes, strong degree spectra and Kolmogorov complexity

Carl G. Jockusch

University of Illinois at Urbana-Champaign
USA
jockusch@math.uiuc.edu

This is joint work with John Chisholm, Jennifer Chubb, Valentina Harizanov, Denis Hirschfeldt, Timothy McNicholl, and Sarah Pingrey.

We study the weak truth-table spectra of relations on computable models. A basic result is that K is not wtt-reducible to the ω-part of any computable linear ordering of order-type $\omega + \omega^*$. Further, we show that there is a low c.e. set C which is not wtt-reducible to any element of any countable Π_1^0 subset of 2^ω, and hence is not wtt-reducible to any initial segment of any scattered computable linear order. Kolmogorov complexity is used to greatly simplify the original proof of this result.

Low upper bounds of ideals

Antonin Kučera

Charles University
Prague, Czech Republic
kucera@ktisun2.ms.mff.cuni.cz

This is a joint project with T. Slaman.

We show that there is a low upper bound for the class $\mathcal{K}$, i.e. the class of K-trivial sets. The result can be strengthened to a more general characterization of ideals of r.e. sets for which there is a low upper bound. Coding into Π_1^0-classes plays an important role here, as well as in some other applications.

Dimensions of points on lines and curves

Steffen Lempp

Department of Mathematics
University of Wisconsin
USA
lempp@math.wisc.edu

This is a joint work with Jack Lutz. I will present recent new results on the (constructive Hausdorff) dimensions of individual points on lines and curves in Euclidean space.

Traceability and Kolmogorov complexity

Wolfgang Merkle

Workgroup for Mathematical Logic and Theoretical Computer Science
University of Heidelberg
Germany
merkle@math.uni-heidelberg.de

We review known and recent results about the relations between variants of traceability and concepts defined in terms of Kolmogorov complexity such as autoreducibility or lowness for Kolmogorov complexity.

Randomness, lowness notions, measure and domination

Joseph S. Miller

Department of Mathematics
University of Connecticut
USA
joseph.miller@math.uconn.edu

An oracle A is low for a given computability theoretic class if relativizing to A does not change the class. The oracles that are low for Martin-Löf randomness are a particularly interesting example. They were introduced by Zambella in 1990 and several characterizations were given in papers of Nies, Hirschfeldt, Stephan and others. Recently, Downey, Nies, Weber and Yu proved that every oracle low for weak 2-randomness is low for ML-randomness. We see that the reverse is also true.

This work is related to two domination properties introduced by Dobrinen and Simpson: almost everywhere domination and its uniform variant. Following up on work of Kjos-Hanssen, we explain how lowness properties relate to measure regularity properties and thus to domination properties. We can use this relationship to prove that the domination properties of Dobrinen and Simpson are equivalent.

Profinite topologies on words

Jean-Éric Pin

LIAFA, Université Paris VII and CNRS
Case 7014, 2 Place Jussieu
75251 Paris Cedex 05, France
Jean-Eric.Pin@liafa.jussieu.fr

Profinite topologies were introduced by M. Hall Jr, originally for the free group. Over the past twenty years, they found surprising applications in the theory of finite automata. In this survey lecture, I shall introduce the main definitions, give several examples and present some of the main results of this theory.

Effectively closed sets of measures and randomness

Jan Reimann

Visiting Assistant Professor
Department of Mathematics
University of California at Berkeley
USA
reimann@math.berkeley.edu

We study effectively closed sets of measures under the weak topology. These have been used by Levin to prove results on the existence of uniform tests of randomness or neutral measures. We show how to use standard techniques concerning Π_1^0 classes, such as basis theorems, to obtain results concerning the relation between randomness for Hausdorff and probability measures, as well as give new, information theoretic proofs of fundamental results in geometric measure theory.

Pseudorandom generators, a survey

Claus-Peter Schnorr

Department of Mathematics/Computer Science
Johann Wolfgang Goethe-University
Frankfurt am Main, Germany
schnorr@mi.informatik.uni-frankfurt.de

Pseudorandom numbers play an important role in many modern applications. In particular, public and private key cryptographic schemes use pseudorandom numbers for encryption, authentication and digital signatures. The corresponding pseudorandom number generation must be both efficient and provably secure.

We survey highlights of the development of pseudorandom generators since their invention due to Yao and Blum-Micali in 1982. We focus on practical generators that are provably secure under reasonable complexity assumptions such as the complexity of integer factorization, the complexity of the discrete logarithm and the complexity of lattice problems.

While the hardness of factoring integers gives rise to the elegant modular squaring generator of Blum-Blum-Shub the discrete logarithm problem has the advantage of being harder, in particular for generic groups like elliptic curves. However, if quantum computers can be build the complexity of factoring and of the discrete logarithm break down. For this case it seems best to construct pseudorandom generators based on NP-hard problems. NP-hard lattice problems are particular appropriate.

The theories of Turing degree structures

Richard A. Shore[1]

Department of Mathematics
Cornell University
Ithaca NY 14853, USA
shore@math.cornell.edu

This talk will primarily be an exposition of the general approaches to proving that the theories of various Turing degree structures are undecidable or even as complicated as full first or second order arithmetic. The methods that we shall consider are all, from a methodological point of view, ones proceeding by the interpretation of some standard theory such as that of partial orderings or a finitely axiomatized version of arithmetic. For each structure considered, specific methods and set constructions will be described that implement the desired interpretations. We will consider the structures $\mathcal{D}$, the Turing degrees of all sets; $\mathcal{D}(\leq \mathbf{0}')$, the Turing degrees of the sets computable from the Halting problem; and $\mathcal{R}$, the Turing degrees of the recursively enumerable sets. We also expect to describe some new joint work with Ted Slaman giving results along these lines for the structures $\mathcal{R}_n$, the Turing degrees of the n-r.e. sets.

Note: There is a common framework in which one can define the three proper substructures of $\mathcal{D}$ that we will consider. We say that $f(x, s)$ is an approximation to a set A if for every x, $f(x, 0)$, $\lim_s f(x, s) = 1 \Leftrightarrow x \in A$ and $\lim_s f(x, s) = 0 \Leftrightarrow x \notin A$. By definition, for each x, the set $\{s | f(x, s) \neq f(x, s + 1)\}$ of stages at which an approximation f changes its value at x is finite. In this setting, we note that A is computable from $0'$ if and only if it has a recursive approximation. A is r.e. if and only if it has a recursive approximation that, for each x, changes its value at x at most once. A is n-r.e. if and only if it has a recursive approximation that, for each x, changes its value at x at most n many times.

Moduli of computation

Theodore Slaman

Theodore A. Slaman Department of Mathematics
The University of California
USA
slaman@math.berkeley.edu

In this talk, we will discuss joint work with Marcia Groszek, Dartmouth College, in which we examine sets recursive in all sufficiently-quickly growing functions. We say that $X \subset \omega$ has a modulus (of computation) $f : \omega \to \omega$ if and only if every function g which dominates f pointwise computes X. If f is recursive in X, then we say that X has a self-modulus.

By a theorem of Solovay, every set which has a modulus is Δ^1_1. We show that if X has a self-modulus then either X is Δ^0_2 or X computes a 1-generic. We give examples to show that these cases are nondegenerate. In particular, there is a nonrecursive set X with a self-modulus which does not compute any nonrecursive Δ^0_2 set.

Other connections between rates of growth and genericity will be discussed as time allows.

Incomputability in games, wars and economics – inductive inference in hostile environments

Ray Solomonoff

Royal Holloway
University of London
U.K.
trovaxo@yahoo.com

We know that the very best probability evaluation functions are incomputable. We also know that for any computable approximation to such functions, there exist hostile environments in which this approximation is catastrophically bad.

One way of dealing with environments of this sort is to have larger computation resources than the hostile environment and/or use our resources more efficiently. We will consider the problem of getting the very best probability estimates using whatever resources we happen to have.

For resource bounds of this kind, a variant of Levin's Search Procedure is able to give near optimum predictions – but with certain restrictions. We will examine these restrictions and propose techniques to transcend them.

Intervals in the Medvedev lattice

Sebastiaan A. Terwijn

Institute of Discrete Mathematics and Geometry
Technical University of Vienna
Austria
terwijn@few.vu.nl

The Medvedev lattice is a structure from computability theory with ties to constructive logic. We will briefly describe this connection and the relation to structures such as the Turing degrees. We will then discuss structural properties of the Medvedev lattice, in particular, the size of its intervals. We prove that every interval in the lattice is either finite, in which case it is isomorphic to a finite Boolean algebra, or contains an antichain of size $2^{2^{\aleph_0}}$, the size of the lattice itself. We also prove that it is consistent that the lattice has chains of this size, and in fact that these big chains occur in every interval that has a big antichain. We also study embeddings of lattices and algebras. We show that large Boolean algebras can be embedded into the Medvedev lattice as upper semilattices, but that a Boolean algebra can be embedded as a lattice only if it is countable. Finally we discuss which of these results hold for the closely related Muchnik lattice.

Genericity theory from the randomness

Liang Yu

Institute of Mathematical Science
Nanjing University
Nanjing, JiangSu province 210093
P. R. of China
yuliang.nju@gmail.com

I shall survey recent results about genericity in the light of randomness theory. It is well known that there are many analogies between category and measure theory. So it is natural compare genericity theory with randomness theory. In particular, we focus on the lowness properties for genericity and obtain a complete description. We also compare n-genericity with n-randomness in the both recursion theory and set theory aspects.

Randomness, lowness and degrees

George Barmpalias

School of Mathematics
University of Leeds
Leeds, LS2 9JT, U.K.
barmpalias@yahoo.co.uk

Say that $A \leq_{LR} B$ if every B-random is A-random. This reducibility was introduced by Nies and has turned out to be a very interesting relativisation of the notion of 'low for random' (although a straightforward relativisation gives a different reducibility). We study the structure of LR degrees globally and locally (i.e. restricted to computably enumerable degrees) and their relationship with the Turing degrees. Among other results we show that every generalized superhigh degree bounds $2^{\aleph_0}$ degrees and we give sample results which demonstrate how various techniques from the theory of c.e. degrees can be used to prove results about the c.e. LR degrees. Following is a sample of our results.

Theorem 1 *If H is (generalized) superhigh then in the LR degrees the degree of H bounds $2^{\aleph_0}$ degrees.*

Theorem 2 *If W is an incomplete c.e. set, i.e. $\emptyset' \not\leq_T W$, then (uniformly in W) there is a c.e. set B such that $B \leq_{LR} W$ and $B \not\leq_T W$.*

Theorem 3 *If A is c.e. and not low for random then there are c.e. B, C such that*

- *$B \cap C = \emptyset$*

- *$B \cup C = A$*

- *$B \not\leq_{LR} C$ and $C \not\leq_{LR} B$.*

Most of this work is joint with Andy Lewis and Mariya Soskova.

Algorithmic information transfer and its practical use

Bruno Bauwens, Luc Boullart

Department of Electrical Energy, Systems and Automation
Ghent University
Technologiepark 913, B-9052
Ghent, Belgium

Patrick Santens

Department of Neurology
Ghent University
De Pintelaan 185, B-9000
Ghent, Belgium

Bruno.Bauwens@UGent.be
Luc.Boullart@UGent.be
Patrick.Santens@UGent.be

Algorithmic complexity is the most fundamental absolute measure of information. However a definition of information flow between measured signals is often necessary. Investigating the functioning of complex systems, one tries to forecast what the influence will be of changing a component or cutting pathways to other parts of the system. When only the activity of a limited number of components in the system is visible, an analytical solution or a simulation is not possible. One tries to model the system using the measured signals from the components which are visible and to calculate the information transfer rate in order to conclude whether there is communication or not.

We introduce the time conditional Kolmogorov complexity $K(x|y \uparrow)$ of string $x = x_{1..n}$ and $y = y_{1..n}$ as the length of the shortest program p that writes x_n on the output tape when the first $n-1$ elements

of x and y are presented on the input tape.

$$K(x|y \uparrow) \quad = \quad \min\{|p| : \forall k = 1..n; U(p, x_{1..k-1}, y_{1..k-1}) = x_k\}$$

The information transfer is defined as:

$$IT(x \leftarrow y) = K(x) - K((|x \uparrow))$$

The mutual information $I(x : y)$ can now be decomposed in three parts: information transfer from y to x, from x to y, and information coming from a common source.

The information transfer rate is not an enumerable function because it's the difference of two non-recursive functions. However, there exists a c such that for any recursive distribution and a fraction ϵ there exists a halting program of length $-c \log(\epsilon) + c_P$ which equals the information transfer with probability $1 - \epsilon$. c_P is a constant depending on the probability distribution P.

In practice we distinguish 2 types of methods for inducing causality: Both types fit a model $\mathcal{M}$ to data (x, y).

1. Type 1: Calculates the information transfer using $\mathcal{M}$ as below:

$$IT(x \leftarrow y|\mathcal{M}) = K(x|\mathcal{M}) - K(x| \uparrow y, \mathcal{M})$$

2. Type 2: Uses only the model $\mathcal{M}$ to measure 'information transfer' by using Shannon Mutual information on estimated probability distributions.

For any model $\mathcal{M}$ we have:

$$IT(x \leftarrow y|\mathcal{M}) < IT(x \leftarrow y) + c$$

This inequality has an important consequence: fitting a model and using the model to forecast x from the past of y will always result in an information transfer which is lower than building a model for only forecasting x for the past of y. Overfitting the model in the first case results in a lower information transfer but not for the last case.

One the other side, overfitting in type 2 transfer measures using Shannon mutual information, leads to a too high estimation of information transfer. This can be fixed using actual data compression ratios.

We argue that [3] and all methods based on Granger causality can be considered as type 1 methods and [1] and [2] can be seen as a type 2 methods.

We have implemented this new approach using the Lempel-Ziff compression algorithm. Denote $K^{LZ}(x)$ as the length of the Lempel-Ziff code for x. The LZ algorithm $K^{LZ}(x|y)$ receives a natural definition after a little modification to guarantee that $K^{LZ}(x|y\uparrow) < K^{LZ}(x)$. In the simulations we used a basic LZ-algorithm. The resulting estimation method has an equal performance compared to existing methods for calculating the directionality index $\frac{IT(x\leftarrow y)-IT(y\leftarrow x)}{IT(x\leftarrow y)+IT(y\leftarrow x)}$. The advantages are:

- Any improvement of the LZ-algorithm reflects to an improved estimate.

- No data dependent parameters need to be tuned by the (inexperienced) user.

References

[1] A. Stefanovska M. Palus. Direction of coupling from phases of interacting oscillators: an information theoretic approach. *Physical Review E Rapid Communications*, 67:055201(R), 2003.

[2] T. Schreiber. Measuring information transfer. *Physical Review Letters*, 85(2), 2000.

[3] J. Bhattacharya U. Feldmann. Predictability improvement as an asymmetrical measure of interdependence in bivariate time series. *International Journal of Bifurcation and Chaos*, 14:505–514, 2004.

Algorithmic randomness and decidable machines

Laurent Bienvenu

Laboratoire d'Informatique Fondamentale
Université de Provence
Marseille, France
laurent.bienvenu@lif.univ-mrs.fr

Wolfgang Merkle

Institut für Informatik
Ruprecht-Karls-Universität
Heidelberg, Germany
merkle@math.uni-heidelberg.de

We study several concepts of algorithmic randomness in the light of decidable notions. We define the class of decidable Turing machines, which we use to give machine characterizations for Martin-Löf randomness, Schnorr randomness and Kurtz randomness. Some applications of these results are given, such as a new proof of the Miller-Yu theorem which characterizes Martin-Löf randomness by the plain Kolmogorov complexity of the initial segments, new characterizations of computable dimension, and equivalence results between computable martingales and computable martingale processes in the definition of Schnorr randomness, Kurtz randomness and computable dimension.

Random sets and functions

Paul Brodhead

Department of Mathematics
University of Florida
USA
brodhead@math.ufl.edu

I will discuss recent joint work related to the study of random closed subsets of 2^ω and random continous functions on 2^ω. In each instance a probability measure is given and a version of the Martin-Löf test for randomness is defined. Douglas Cenzer, and Seyyed Dashti, and I jointly studied the notion of a random closed set. We showed that Π_2^0 random closed sets exist but there are no random Π_1^0 closed sets. Additionally, a random closed set is perfect, has measure zero, and has no computable elements. Now a closed subset of 2^ω may be defined as a set of infinite paths through a tree. Therefore we also explored the problem of compressibility of trees, leading to some results on a Chaitin-style notion of randomness for closed sets.

Continuing from the work on random closed sets, Douglas Cenzer, Jeffrey Remmel, and I studied random continuous functions. We showed that random Δ_2^0 continuous functions exist, but no computable function can be random. Additionally, a random function maps any computable real to a random real and the image of a random continuous function is always a perfect set. Furthermore any element of 2^ω is always contained in the image of some random continuous function. Hence the image of a random continuous function need not be a random closed set.

I will highlight these and other recent results.

Robinson consistency property for Lukasiewicz propositional logic

Manuela Busaniche

FIQ- IMAL
Universidad Nacional del Litoral- CONICET
Argentina
manuelabusaniche@yahoo.com.ar

For all unexplained notions about MV-algebras and Lukasiewicz (always propositional in the present talk) logic: we refer to [1]. For X an arbitrary set of variables, L_X denotes the set of formulas ψ whose variables are in X. Any such ψ is said to be an L_X-*formula*. The definition is the same for boolean logic and for many-valued logic. A proper subset Θ of L_X is called a *theory* (or, an L_X-theory if necessary) if

(i) Θ contains all L_X-tautologies of Lukasiewicz infinite-valued propositional logic, and

(ii) Θ is closed under modus ponens.

Theories are in one-one correspondence with ideals of free MV-algebras. An L_X-theory Θ is said to be *prime* (also called "complete" in Hájek's monograph [2]) if for any L_X-formulas φ and ψ either $\varphi \to \psi$ or $\psi \to \varphi$ belongs to Θ. Prime theories are in one-one correspondence with prime ideals of free MV-algebras. Every prime theory Θ has a unique *maximally consistent* completion Θ'. In other words, $L_X \supseteq \Theta' \supseteq \Theta$ and there is no theory $\Theta'' \subseteq L_X$ properly extending Θ'. By contrast with boolean logic Θ' generally does not coincide with Θ. Maximally consistent theories are in one-one correspondence with maximal ideals of free MV-algebras. The *Robinson consistency property* for boolean, as well for Lukasiewicz logic, can be stated as follows:

Suppose Θ is a prime L_X-theory, and Ψ is a prime L_Y-theory. Let $L_Z = L_X \cap L_Y$ and $L_W = L_X \cup L_Y$. If $\Theta \cap L_Z = \Psi \cap L_Z$ then there is a prime L_W-theory Φ such that $\Theta = \Phi \cap L_X$ and $\Psi = \Phi \cap L_Y$.

We give a proof of the Robinson consistency property for Lukasiewicz propositional logic. As a corollary we obtain a new proof of the amalgamation property for MV-algebras. For the proof of our main results we make no use of lattice-ordered groups and the Γ functor. Rather, we make use of geometric tools naturally arising from the rich theory of MV-algebras, such as McNaughton's representation of free MV-algebras via $[0,1]$-valued piecewise linear functions, unimodular triangulations of the n-cube, and the classification of spectral spaces of free MV-algebras via bases in euclidean space.

References

[1] R. Cignoli, I. M. L. D'Ottaviano, D. Mundici, *Algebraic Foundations of Many-Valued Reasoning*, Kluwer, Dordrecht, 2000.

[2] P. Hájek, *Metamathematics of Fuzzy Logic*, Kluwer, Dordrecht, 1998.

Congruences and compatible functions by Priestley duality

Leonardo M. Cabrer and Marta S. Sagastume

U.N.C.P.B.A.- U.N.L.P
CC 172, 1900 La Plata - Buenos Aires - Argentina

lcabrer@exa.unicen.edu.ar
marta@mate.unlp.edu.ar

In [5] Sofronie-Strokkermans develop a Priestley duality for distributive lattices with some operations called *join-hemimorphisms* or *meet-hemimorphisms*. This duality generalizes previous results obtained by many authors as Petrovich in [4] or Celani in [2, 3]. In these papers the congruences of each structure are studied using the mentioned duality. In this work we obtain a topological characterization of congruences of lattices with operations of the type mentioned above that generalizes previous results.

We use this characterization to describe simple and subdirectly irreducible algebras of the form $\langle L, f \rangle$, where L is a distributive lattice and f is an n-ary operation defined on L. Finally we obtain necessary and sufficient conditions for some kind of operations to be compatible functions in Heyting algebras. These conditions are closely related to the more general ones obtained by Cignoli and Caicedo in [1], but in some cases, e.g. for negations and modal operators, they allow us to prove stronger characterizations.

References

[1] Caicedo, X. and Cignoli, R. *An algebraic approach to intuitionistic connectives.* The Journal of Symbolic Logic **66** (2001), 1620-1636

[2] Celani, S. *Distributive Lattices with a Negation Operator.* Mathematical Logic Quarterly **45** (1999) 2, 209-218.

[3] Celani, S. *Bounded Distributive Lattices with Fussion and Implication.* Southeast Asian Bulletin of Mathematics **28** (2004), 999-1010.

[4] Petrovich A. *Distributive Lattices with an Operator.* Studia Logica **59** (1996) 1/2, 205-224.

[5] Sofronie-Strokkermans, V. *Representation theorems and the semantics of non classical logics, and applications to automated theorem proving.* Physica, Heidelberg **114** (2003), 59-100

Axiomatizability of classes closed under intersection of submodels

Miguel Campercholi and Diego Vaggione

Facultad de Matematica Astronomía y Física
Universidad Nacional de Córdoba
Argentina

vaggione@mate.uncor.edu
mcampercholi@yahoo.com

We prove the following:

Theorem 4 *Let* $\mathbf{A}$ *be a finite model of a first order language without one-element submodels. Then every* $\mathcal{C} \subseteq S(\mathbf{A})$ *which is closed under intersection of submodels is axiomatizable by* $\forall\exists!$*-sentences (relative to* $S(\mathbf{A})$*) if and only if*

(1) *no two distinct submodels of* $\mathbf{A}$ *are isomorphic and*

(2) *for* $\mathbf{B} \leq \mathbf{A}$ *and* $f, g \in Aut(\mathbf{B})$*, if* $f(b) = g(b)$ *for some* $b \in B$ *then* $f = g$.

Some applications to discriminator varieties will be given.

Distribution of the average external depth for tries in dynamical sources context

Eda Cesaratto

CNRS UMR 6072
GREYC, Université de Caen
Caen, France and
Facultad de Ingeneria
Universidad de Buenos Aires
Argentina
ecesara@fi.uba.ar

Brigitte Vallée

CNRS UMR 6072
GREYC, Université de Caen, F-14032
Caen, France
brigitte.vallee@info.unicaen.fr

A trie is a tree structure which is used as a dictionary. It is based on a splitting according to symbols encountered in strings. If X is a set of strings, and $\mathcal{M} = \{m_1, \ldots, m_r\}$ is the alphabet (possibly infinite), then the trie associated to X is defined recursively by the rule: $\mathrm{trie}(X) = \langle \mathrm{trie}(X \setminus m_1), ..., \mathrm{trie}(X \setminus m_r) \rangle$ where $X \setminus m$ means the subset of X consisting of strings that start with the symbol m stripped of their initial symbol m ; recursion is halted as soon as X contains less than 2 elements. Various applications, as partial match queries and text processing tasks, justify considering the trie structure as one of the central general purpose data structures of Computer Science.

The complexity of many algorithms on strings can be expressed with various parameters of tries, for instance the average external depth. The (average) external depth is the number of nodes in a path

from the root to a (uniformly randomly selected) leaf. This work aims studying the average external depth of a random trie. More precisely, we assume that the set X is formed with n infinite independently chosen strings drawn from a given source. For classical sources, namely memoryless sources (where the symbols are independently drawn) or Markov chains (where the dependency between symbols is bounded), this parameter is well known: its mean value is of order $\log n$, and its distribution is proven to be asymptotically gaussian. These results on tries are now classical (see, for instance, [5] and [7]).

In the last decade, dynamical sources were introduced by Vallée [8]. These sources, built from dynamical systems (with strongly expanding maps of the interval), provide a quite general model of sources, where the dependency between symbols may be unbounded. This model encompasses classical sources (memoryless sources and Markov chains) and can be precisely studied, via transfer operators which generalize the transfer operators introduced by Ruelle [6]. The analysis of the main parameters of a trie built on a dynamical source was done by Clément, Flajolet and Vallée [2]: the authors studied three main parameters: the path length, the size, and the height. Our parameter of interest, the average external depth, was precisely analyzed by Flajolet and Vallée [4], in the case of the source related to the Continued Fraction System: the authors exhibited the mean value of this parameter and related it to some classical constants...together to the Riemann hypothesis.

In all these previous studies, the distribution of the parameters cannot be reached. There was a change in 2004, when Baladi and Vallée designed a general method for obtaining distribution results on the Euclid Algorithm. They proved that the main parameters of the algorithm follow asymptotic gaussian laws. Their results are obtained by sharpening results due to Dolgopyat [3], and they are based on the existence of a strip free of poles for the transfer operator.

Here, we adapt this framework to dynamical sources: we extend the Baladi-Vallée result to the generalized operator associated to a dynamical source, and this extension is possible provided that the dynamical system does not resemble too much to a memoryless system: this is the UNI Condition of Dologopyat (UNI = Uniform Non Integrability). We extend also some ideas of [4] to our general context,

and we obtain the following result:

Theorem. *Consider a dynamical source which satisfies the UNI Condition. The average external depth of a trie built on n words produced by this dynamical source is asymptotically Gaussian, with an expectation and a variance of order $\log n$ and a speed of convergence of order $1/\sqrt{\log n}$. The constants which appear in the main terms of the mean and the variance are expressed in terms of the spectral objects of transfer operators and they are computable.*

References

[1] V. Baladi, B. Vallée, *Euclidean algorithms are Gaussian*, J. Number Theory **110** (2005), 331–386.

[2] J. Clément, Ph. Flajolet; B. Vallée, *Dynamical Sources in Information Theory: A General Analysis of Trie Structures*, Algorithmica, Vol 29, (2001) 307-369

[3] D. DOLGOPYAT, *On decay of correlations in Anosov flows*, Ann. of Math. 147 (1998) 357-390.

[4] Ph. Flajolet, B. Vallée, *Continued Franctions, Comparison Algorithms, and fine structure constants*, Canadian Mathematical Society, Conference Proceedings, Vol 27, (2000) 53-81.

[5] H. Mahmoud, *Evolution of Random Search Trees*, John Wiley, New York, 1992.

[6] D. Ruelle, *Thermodynamic formalism*, Addison Wesley, 1978.

[7] W. Szpankowski, *Average Case Analysis of Algorithms on Sequences*, John Wiley, New York, 2001.

[8] B. Vallée, *Dynamical Sources in Information Theory: Fundamental Intervals and Words Prefixes*, Algorithmica, Vol 29, No 1/2 (2001) 262-306.

Quantifying knowledge

Fouad B. Chedid

Department of Computer Science
Notre Dame University
P.O.Box: 72 Zouk Mikael
Zouk Mosbeh, Lebanon
fchedid@ndu.edu.lb

While the information contents of a binary string x can be measured by its prefix Kolmogorov complexity $K(x)$ (the length of a shortest prefix-free binary program that computes x), it is not clear how to measure the knowledge stored in x. In this talk, we argue that the knowledge contained by a string x is relative to the hypothesis assumed to compute x. So, if H is the hypothesis used to explain x, then we suggest to measure the knowledge in x by $K(H)$. The absolute knowledge in x is $K(H_0)$, where H_0 is the simplest model capable of explaining x. Using Bayes's rule and Solomonoff's universal semi-measure, we obtain

$$K(H) = K(H \mid x) - (K(x \mid H) - K(x)).$$

Here, $K(x \mid H)$ is the ideal code length for describing x given H. Such prefix code length can be achieved by the Shannon-Fano code. Also, one would expect $K(H \mid x)$ to be minimal. So, if we discard that term and rewrite the above equation, we obtain $K(x) = K(H) + K(x \mid H)$. We interpret $K(H)$ as the knowledge part in x and $K(x \mid H)$ as the random aspect (accidental information) in x following the hypothesis H.

   Astonishingly, our above simple observation is similar to Kolmogorov's 1974 result in which he proposed to found statistical theory on finite combinatorial and computational principles independent of probabilistic assumptions, as the relation between the individual

data and its explanation (model), expressed by Kolmogorov's structure function. The basic approach as formalized by Kolmogorov is as follows. To each constructive object x corresponds a function $\phi_x(k)$ of a natural number k - the log of minimal cardinality of x-containing sets that allow definitions of complexity at most k. Kolmogorov called an object positively probabilistically random only when function ϕ having taken the value ϕ_0 at a relatively small $k = k_0$, then changes approximately as

$$\phi_x(k) = \phi_0 - (k - k_0).$$

We explain how Kolmogorov's structure function relates to our definition of knowledge.

Also, we mention that building on the notion of Kolmogorov's structure function, Vitanyi and Vereshchargin [1, 2] have recently reached a definition of knowledge (called meaningful information there) similar to ours. However, the work in [1, 2] follows a much more complicated argument where a program that computes a string is assumed to be divisible into two parts: the model part and the data-to-model part, a very difficult task to do. Moreover, many of the results derived in [1, 2] are straightforward using our definition of knowledge.

References

[1] Vereshchargin, N., Vitanyi, P.M.B., Kolmogorov's Structure Functions and Model Selection. IEEE Trans. on Information Theory, **50:12** (2004) 3265–3290

[2] Vitanyi, P., Meaningful Information. url=www.cwi.nl/~paulv/kolmocompl.html

Complexity of logical inferences in Martin-Löf's type theory. Part 1

Gohar Marikyan

Empire State College,
325 Hudson Street,
New York, NY 10013, USA
Gohar.Marikyan@esc.edu

In [1] and [2] Per Martin-Löf has introduced his Type Theory (hereafter MLTT). To characterize the complexity of inferences in MLTT we need to compare complexity of inferences in Martin-Löf's Type Theory with complexity of inferences in other formal systems. One of the systems is MLTT0 which is Martin-Löf's Theory of Small Types [2] enriched with one more postulate. The second system is the Hilbert-type System (hereafter H) [4]. As a third system I have defined a formal system G that is a Gentzen-type system [3]. All three systems are formalizations of arithmetic. In order to compare complexity of inferences in these three systems, in part 1 I have built three methods of complexity measurements universal for all three systems. In ensuing parts I will show the results of the comparison of complexity of inferences in these three systems. [1] Per Martin-Löf. Constructive mathematics and computer programming. Sixth International Congress for Logic, Methodology, and Philosophy of Science. North–Holland, Amsterdam, 1982, pages 153–175. [2] Per Martin-Löf. An Intuitionistic Theory of Types: Predicative Part. Logic Colloquium '73, H. E. Rose and J. C. Shepherdson. North–Holland, Amsterdam, 1973, pages 73–118. [3] Stephen C. Kleene. Introduction to Metamathematics (Bibliotheca Mathematica, Vol 1) [4] Stephen C. Kleene. Mathematical Logic (John Wiley & Sons, Inc.)

References

[1] Per Martin-Löf. Constructive mathematics and computer programming. *Sixth International Congress for Logic, Methodology, and Philosophy of Science.* North–Holland, Amsterdam, 1982, pages 153–175.

[2] Martin-Löf. An Intuitionistic Theory of Types: Predicative Part. *Logic Colloquium '73*, H. E. Rose and J. C. Shepherdson. North–Holland, Amsterdam, 1973, pages 73–118.

[3] Stephen C. Kleene. *Introduction to Metamathematics* (Bibliotheca Mathematica, Vol 1)

[4] Stephen C. Kleene. *Mathematical Logic* (John Wiley & Sons, Inc.)

Hybrid logics with concrete domains

Sergio Mera

Computer Science Department, FCEyN
University of Buenos Aires
Argenitna
smera@dc.uba.ar

In this paper we present the hybrid logic $\mathcal{HL}_\mathcal{C}(@, \downarrow)$, an extension of $\mathcal{HL}(@, \downarrow)$, whose models have a concrete domain (such as the natural or real numbers). This logic extends the language of $\mathcal{HL}(@, \downarrow)$ including terms with equality to deal with concrete domain values. Similar languages have already been investigated in other areas like knowledge representation (e.g., description logics with concrete domains) and languages for verification (e.g., half-order logic). Our main result is a sound and complete axiomatization for $\mathcal{HL}_\mathcal{C}(@, \downarrow)$. We also present an embedding of description logics with concrete domains and half-order logic within our framework.

Thermodynamic cost in reversible Turing machines

José Orlicki

Computer Science Department, FCEyN
University of Buenos Aires
Argentina
jio@fibertel.com.ar

Bennett and Vitanyi introduce the notion of *thermodynamic cost* as the cost of transforming an input x into an output y using a reversible Turing machine. This cost is given by the size of the garbage that appears on the output after a computation. Their thesis is that this thermodynamic cost equals the amount of irreversible operations that have to be performed in a classical and optimal Turing machine that transforms x into y (with no garbage).

The class of reversible Turing machines is a subclass of the partial recursive injective maps. As it is well known, although this class is recursively enumerable, it lacks a universal function. We argue that to give an appropriate definition of *minimal thermodynamic cost* an adequate definition of optimal reversible machine is needed. We make a thorough review of Bennett and Vitanyi's work and we provide the missing formal developments regarding this notion.

We also briefly consider the relation between reversible computations and one-way functions.

Bounded genericity

Ludwig Staiger

Martin-Luther-Universität Halle-Wittenberg
Germany
staiger@informatik.uni-halle.de

Many diagonalisation arguments in computability theory and in computational complexity theory can be phrased in terms of the finite extension method. In a finite extension argument a sequence ξ of letters is inductively defined by specifying longer and longer initial segments of ξ. The goal of the construction is to ensure that the sequence ξ has a certain property. For a more detailed discussion see [AB03].

In this paper we generalise the automatic genericity concept of [AB03] to extension strategies not necessarily defined by finite automata but we focus also on those finite extension arguments which require extensions of constant length.

It turns out that the hierarchy result of [AB03] on weakly k-reggeneric sets does not depend on the fact that the underlying extension strategy is defined by a finite automaton.

We consider, for an alphabet X of cardinality $r := |X| \geq 2$, the set X^ω of all sequences (ω-words) and the set $X^* = \bigcup_{n=0}^{\infty} X^n$ of finite words over X.

Next we briefly recall some definitions from [AB03]. For $k \geq 2$ a k-bounded[1] extension function over X is a function $f : X^* \to X^k$. We say that f meets a $\xi \in X^\omega$ iff $w \cdot f(w)$ is a prefix of ξ (short: $w \cdot f(w) \sqsubset \xi$). Moreover, let $M_f := \{\xi : f \text{ meets } \xi\} = \bigcup_{w \in X^*} w \cdot f(w) \cdot X^\omega$ and $F_f := X^\omega \setminus M_f$. For a countable family of extension functions, $\mathcal{F}$, we define $M_\mathcal{F} := \bigcap_{f \in \mathcal{F}} M_f$ and likewise $F_\mathcal{F} := \bigcup_{f \in \mathcal{F}} F_f$.

Our aim is to show a hierarchy result of the following form.

---

[1] The case $k = 1$ is trivial.

Theorem 5 *Let $\mathcal{F}$ be a countable family of k-bounded extension functions and let $f : X^* \to X^{k+1}$ be an extension function.*

If $|X| \geq 3$ then $M_{\mathcal{F}} \not\subset M_f$, and if $|X| = 2$, there are $(k+1)$-bounded extension functions f such that $M_{\mathcal{F}} \not\subset M_f$.

To achieve this goal it is useful to investigate the Hausdorff and upper box-counting dimensions of the sets F_f, the complements of M_f. The sets F_f are known to be nowhere dense in the Cantor topology of X^ω, in fact even porous (for porosity see [Za87, CS05]). Thus dimension inequalities lead to the above non-inclusion results. The dimension results follow from arguments counting the number of prefixes of length n of ω-words in F_f, $\mathsf{s}_{F_f}(n)$. It holds that

$$\underline{\mathsf{s}}_k(n) \leq \mathsf{s}_{F_f}(n) \leq \mathsf{s}_k(n) \tag{1}$$

for any k-bounded extension function f. Here $\underline{\mathsf{s}}_k$ and s_k are the functions defined by the initial conditions

$$\begin{array}{llll}
\mathsf{s}_k(n) & = & \underline{\mathsf{s}}_k(n) & = & r^n & \text{, if } 0 \leq n < k \text{ and} \\
\mathsf{s}_k(k) & = & \underline{\mathsf{s}}_k(k) & = & r^k - 1 & ,
\end{array} \tag{2}$$

and the recurrences

$$\begin{array}{lll}
\underline{\mathsf{s}}_k(n) & = & r \cdot \underline{\mathsf{s}}_k(n-1) - \underline{\mathsf{s}}_k(n-k) \quad \text{, if } n > k \\
\mathsf{s}_k(n) & = & (r-1) \cdot \sum_{i=1}^{k} \mathsf{s}_k(n-i) \quad \text{, if } n > k
\end{array} \tag{3}$$

We call an extension function $f : X^* \to X^k$ *minimal* iff $\mathsf{s}_{F_f} = \underline{\mathsf{s}}_k$, and we call f *maximal* iff $\mathsf{s}_{F_f} = \mathsf{s}_k$.

The main result concerning dimensions can be expressed in a single equation; it turns out that for a k-bounded extension function f the following holds.

$$\log_r \underline{\lambda}_k \leq \dim_H F_f \leq \overline{\dim}_B F_f \leq \log_r \lambda_k \tag{4}$$

Moreover, using results of [St89] we have the following.

Lemma 6 *If an extension function $f : X^* \to X^k$ is minimal then $\log_r \underline{\lambda}_k = \dim_H F_f = \overline{\dim}_B F_f$, and if f is maximal then $\log_r \lambda_k = \dim_H F_f = \overline{\dim}_B F_f$.*

Here $\dim_H F_f$ and $\overline{\dim}_B F_f$ are the Hausdorff and upper box-counting dimensions of the sets F_f, respectively, and $\underline{\lambda}_k$ and λ_k are the maximum roots of the polynomials $\underline{p}_k(z) = z^k - r \cdot z^{k-1} + 1$ or $p_k(z) = z^k - \sum_{i=0}^{k-1} (r-1) \cdot z^i$, respectively [2].

¿From Eq. (4) we obtain a theorem from which Theorem 5 follows using the stability properties of the Hausdorff dimension.

Theorem 7 *If f is a k-bounded extension function and f' is a $(k+1)$-bounded extension function over X then $F_f \neq F_{f'}$ and $\dim_H F_f \leq \dim_H F_{f'}$. Equality of Hausdorff dimension can hold only if $|X| = 2$ and f and f' satisfy a certain property.*

In any case $F_f \not\supseteq F_{f'}$.

The proof of the first part is easily obtained from Eq. (4), since for the maximum roots of $\underline{p}_{k+1}(z)$ and $p_k(z)$, $\underline{\lambda}_{k+1}$ and λ_k it holds $\underline{\lambda}_{k+1} > \lambda_k$ whenever $r \geq 3$ (if $r = 2$ we have $\underline{p}_{k+1}(z) = (z-1) \cdot p_k(z)$ and thus $\underline{\lambda}_{k+1} = \lambda_k$).

The proof of the second part follows from the inequality $\dim_H F_f < \dim_H F_{f'}$ if if $|X| \geq 3$ or the fact that $\underline{s}_{k+1}(n) > s_k(n)$ for $n \geq k$ and $|X| = 2$.

As an illustration we consider the class of constant extension functions. Here we have $F_f = X^\omega \setminus X^* \cdot f(a) \cdot X^\omega$ where $a \in X$. In this case the dimension of F_f depends on the combinatorial structure of the word $w = f(a)$. We have the following hierarchy result known from [Vo53].

Theorem 8 ([Vo53]) *Let $k \geq 2$, $a, b \in X, a \neq b$ and $w \in X^k$. Then*

$$
\begin{array}{rclcl}
\log_r \underline{\lambda}_k & = & \dim_H X^\omega \setminus X^* \cdot ba^{k-1} \cdot X^\omega & \leq & \dim_H X^\omega \setminus X^* \cdot w \cdot X^\omega \\
& \leq & \dim_H X^\omega \setminus X^* \cdot a^k \cdot X^\omega & = & \log_r \lambda_k \, .
\end{array}
$$

Moreover, $\dim_H X^\omega \setminus X^* \cdot w \cdot X^\omega = \log_r \underline{\lambda}_k$ if and only if w is overlap-free [3], and $\dim_H X^\omega \setminus X^* \cdot w \cdot X^\omega = \log_r \lambda_k$ if and only if w is of the form $w = x^k$ for some $x \in X$.

¿From this result one can also conclude the hierarchy result of [AB03] for automatic extension functions.

---

[2] It is easy to see that $\underline{\lambda}_k < \lambda_k$.

[3] A word w is *overlap-free* iff no proper prefix of w is a suffix of w.

The final lemma deals with the asymptotic lower Kolmogorov complexity (or constructive dimension) $\underline{\kappa}(\xi)$ of ω-words in F_f (see [Hi05, St98]).

Lemma 9 *If $\mathcal{F}$ is a family of recursive k-bounded extension functions then $\underline{\kappa}(\xi) \leq \log_r \lambda_k$ for every $\xi \in \bigcup_{f \in \mathcal{F}} F_f$.*

References

[AB03] K. Ambos-Spies and E. Busse, Automatic Forcing and Genericity: On the Diagonalization Strength of Finite Automata. in: *Calude, C. S.* (ed.) et al., Discrete Mathematics and Theoretical Computer Science, DMTCS 2003, Springer-Verlag, Berlin 2003, Lect. Notes Comput. Sci. **2731**, 97-108.

[CS05] C.S. Calude and L. Staiger, Generalisations of Disjunctive Sequences, Math. Log. Quart. **51,** (2005) 120-128.

[Hi05] J.M. Hitchcock, Correspondence principles for effective dimension. Theory Comput. Systems **38** (2005), 559-571.

[St89] L. Staiger, Combinatorial properties of the Hausdorff dimension. J. Statist. Plann. Inference **23** (1989), 95 - 100.

[St98] L. Staiger, A tight upper bound on Kolmogorov complexity and uniformly optimal prediction, Theory Comput. Systems **31** (1998), 215-229.

[Vo53] B. Volkmann, Über Hausdorffsche Dimensionen von Mengen, die durch Zifferneigenschaften charakterisiert sind III. Math. Zeitschr. **59** (1953), 259-270.

[Za87] L. Zajîček, Porosity amd σ-Porosity, Real Exchange Analysis **13** (1987-88), 314-350.

On randomness of the Bernoulli parameter

Vladimir V'yugin

Institute for Information Transmission Problems
Russian Academy of Sciences, Bol'shoi Karetnyi per. 19
Moscow GSP-4, 127994, Russia
vyugin@iitp.ru

1 Introduction

We study statistical properties of the parameter in the Bernoulli family using algorithmic randomness theory. In particular, for the case of biased coin, we show that for any θ the Levin's a priory semicomputable measure of the set of all random θ-Bernoulli sequences is positive if and only if the parameter θ is a computable real number; θ-Bernoulli sequences with noncomputable random θ can be generated by computable Bayesian measures. We also show that the Bayesian approach is insufficient: a probabilistic machine can be constructed, which with probability close to one outputs a random θ-Bernoulli sequence, where the parameter θ is not random with respect to each computable probability distribution.

2 Preliminaries

Let Ξ be the set of all finite binary sequences, Ω be the set of all infinite binary sequences. We write $x \subseteq y$ if a sequence y is an extension of a sequence x. A real-valued function $P(x)$, where $x \in \Xi$, is called semimeasure if

$$P(\Lambda) \leq 1,$$
$$P(x0) + P(x1) \leq P(x) \tag{1}$$

for all x, and the function P is semicomputable from below; this means that the set $\{(r, x) : r < P(x)\}$, where r is a rational number, is recursively enumerable. A definition of upper semicomputability is analogous.

Solomonoff proposed ideas for defining the *a priori* probability distribution on the basis of the general theory of algorithms. Levin [8] gives a precise form of Solomonoff ideas in a concept of a maximal semimeasure semicomputable from below (see also [4], Section 4.5). Levin proved that there exists a maximal to within a multiplicative positive constant factor semimeasure M semicomputable from below, i.e. for every semimeasure P semicomputable from below a positive constant c exists such that the inequality

$$cM(x) \geq P(x) \tag{2}$$

holds for all x.

A function P is a measure if (1) holds, where both inequality signs $\leq$ are replaced on $=$. Any function P satisfying (1) (with equalities) can be extended to all Borel subsets of Ω if we define $P(\Gamma_x) = P(x)$ in Ω, where $x \in \Xi$ and $\Gamma_x = \{\omega \in \Omega : x \subseteq \omega\}$; after that, we use the standard method for extending P to all Borel subsets of Ω.

A measure P is computable if it is, at one time, lower and upper semicomputable. In [8] any semimeasure P is considered as a measure in the set $\Xi \cup \Omega$ of all finite and infinite binary sequences. By this reason, we call M the a priory (universal) measure. Then by (2) $cM(A) \geq P(A)$ for every Borel set A.

Levin [2, 3, 8] considered combinations of probabilistic and deterministic processes as the most general class of processes for generating data. With any probabilistic process some computable probability distribution can be assigned. Any deterministic process is realized by means of an algorithm. Algorithmic processes transform sequences generated by probabilistic processes into new sequences. More precise, a probabilistic computer is a pair (P, F), where P is a computable probability distribution, and F is a Turing machine supplied with an additional input tape. In the process of computation this machine reads on this tape a sequence ω distributed according to P and produces a sequence $\omega' = F(\omega)$. So we can compute the probability

$$Q(x) = P\{\omega : x \subseteq F(\omega)\}$$

47

of that the result $F(\omega)$ of the computation begins with a finite sequence x. It is easy to see that $Q(x)$ is semicomputable from below.

Strictly speaking, Q is not a probability distribution in Ω, since $F(\omega)$ may be finite for an infinite ω; however, it can be considered as a measure in $\Xi \cup \Omega$. The converse result is proved in [8]: for every semimeasure $Q(x)$ semicomputable from below a probabilistic computer (L, F) exists such that

$$P(x) = L\{\omega | x \subseteq F(\omega)\},$$

for all x, where $L(x) = 2^{-l(x)}$ is the uniform probability distribution in the set of all binary sequences, $l(x)$ is the length of a sequence x.

Therefore, by (2) $M(x)$ is an universal upper bound of the probability of generating x by probabilistic computers.

3   Results

We consider the standard definition of a random sequence in terms of universal probability. Let P be some computable measure in Ω. The deficiency of randomness of a sequence $\omega \in \Omega$ with respect to P is defined as

$$d(\omega | P) = \sup_n \frac{M(\omega^n)}{P(\omega^n)}, \tag{3}$$

where $\omega^n = \omega_1 \omega_2 \ldots \omega_n$. This definition leads to the same class of random sequences as the original Martin-Löf [5] definition (for the proof see [4]). Let R_P be the set of all infinite binary sequences random with respect to a measure P: $R_P = \{\omega \in \Omega : d(\omega | P) < \infty\}$.

For any $\theta \in [0, 1]$, let $B_\theta(x) = \theta^k (1-\theta)^{n-k}$, where n is the length of x and k is the number of ones in it, be the Bernoulli measure.

We associate with a binary sequence $\theta_1 \theta_2 \ldots$ the real number $0.\theta_1 \theta_2 \ldots$. When the sequence $\theta_1 \theta_2 \ldots$ is computable or random with respect some measure we say that the number $0.\theta_1 \theta_2 \ldots$ is computable or random with respect to the corresponding measure in $[0, 1]$.

The corresponding definition of randomness with respect to B_θ is obtained by relativization of (3) with respect to θ

$$d_\theta(\omega) = \sup_n \frac{M_\theta(\omega^n)}{B_\theta(\omega^n)}$$

(see also [1]). The relativization means, that all algorithms in the definitions given above use in their work the binary expansion of the parameter θ. For any θ let

$$I_\theta = \{\omega \in \Omega : d_\theta(\omega) < \infty\}$$

be the set of all infinite binary sequences random with respect to the measure B_θ. We call elements of this set θ-Bernoulli sequences.

The following theorem shows that, from the point of view of Levin's philosophy explained above, θ-Bernoulli sequences with a pre-specified noncomputable parameter θ can not be obtained in any combinations of stochastic and deterministic processes; in other words, these θ-Bernoulli sequences can not be "realizable in the physical world".

Theorem 10 *For any $\theta \in [0, 1]$ it holds $M(I_\theta) > 0$ if and only if θ is computable.*

Let Q be a computable probability distribution in the set Ω. Then the Bayesian measure

$$P(x) = \int B_\theta(x) dQ(\theta)$$

is also computable. Obviously, $P(\cup_{\theta \in R_Q} I_\theta) = 1$. Moreover, it follows from Corollary 4 of Vovk and V'yugin [6]

Theorem 11 *For any computable measure Q a sequence ω is random with respect to the measure P if and only if ω is random with respect to a measure B_θ for some θ random with respect to the measure Q; in other words,*

$$R_P = \cup_{\theta \in R_Q} I_\theta.$$

The following theorem is some generalization of Theorem 10.

Theorem 12 *For any $\Theta \subseteq \Omega$ it holds $M(\cup\{I_\theta : \theta \in \Theta\}) > 0$ if and only if $M(\Theta) > 0$.*

Let $\mathcal{C}$ be the set of all computable measures in Ω, and let

$$S = \Omega \setminus \cup_{P \in \mathcal{C}} R_P$$

49

be the set of all "nonstochastic" sequences. By definition, any $\omega \in S$ is not random with respect each computable measure. We prove in V'yugin [7] that $M(S) > 0$.

We show that an analogous result holds for parameters of the Bernoulli sequences.

Theorem 13 $M(\cup\{I_\theta : \theta \in S\}) > 0$. *In terms of probabilistic computers, this means that for any $\epsilon > 0$ a probabilistic machine (L, F) can be constructed, which generates with probability $\geq 1 - \epsilon$ an θ-Bernoulli sequence, where $\theta \in S$ (θ is nonstochastic).*

We also prove in [7] that $M(\Omega \setminus \overline{R}_L) > 0$, where $\overline{R}_L$ is the set of all sequences Turing reducible to sequences random with respect to the uniform measure L. By [8] it holds $S \subseteq \overline{R}_L$. The corresponding strengthening of the Theorem 13 is: $M(\cup\{I_\theta : \theta \in \overline{R}_L\}) > 0$.

References

[1] Levin, L.A., On the notion of random sequence, Soviet Math. Dokl., 1973, **14**, 1413-1416.

[2] Levin, L.A., Laws of information conservation (non-growth) and aspects of the foundation of probability theory, Problems Inform. Transmission, 1974, **10**, 206-210.

[3] Levin, L.A., Randomness conservation inequalities; information and independence in mathematical theories, Inform. and Contr., 1984, **61**, 15-37.

[4] Li, M., Vitányi, P. An Introduction to Kolmogorov Complexity and Its Applications, 2nd ed. New York: Springer-Verlag. 1997.

[5] Martin-Löf, P., The definition of random sequences, Inform. and Contr., 1966, **9**, No.6, 602-619.

[6] Vovk, V.G. and V'yugin, V.V., On the empirical validity of the Bayesian rule, J. R. Statist. Soc. B, 1993, **55**, 317-351.

[7] V'yugin, V.V., On Turing invariant sets, Soviet Math. Dokl., 1976, **17**, No.4, 1090-1094.

[8] Zvonkin, A.K. and Levin, L.A., The complexity of finite objects and the algorithmic concepts of information and randomness, Russ. Math. Surv., 1973, **25**, 83-124.

Author Index