Workshop on Computability Theory and Foundations of Mathematics 2018

Surugadai Campus, Meiji University, Tokyo, Japan.

13–15 September, 2018

Updated on September 9, 2018

Contents

Local Organizers:
Akitoshi Kawamura (kawamura@inf.kyushu-u.ac.jp),
Kenshi Miyabe (research@kenshi.miyabe.name)

1 Programme

Thursday 13

10:00–12:00 Fujiwara-Kawai, Kjos-Hanssen

12:00–13:30 Lunch Break

13:30–17:00 Suzuki, Pelupessy, Nakabayashi-Tanaka-Li, Miyabe

Friday 14

10:00–12:00 Mizusawa, Yu

12:00–13:30 Lunch Break

13:30–17:00 Barmpalias, Miyabe, de Brecht, Yokoyama

Saturday 15

10:00–12:00 Hamamoto-Kawamura-Ziegler, Miyaji

12:00–13:30 Lunch Break

13:30–15:30 Potapov, Kawamura-Steinberg-Thies

2 Abstracts

Permutations of the integers induce only the trivial automorphism of the Turing degrees

Bjorn Kjos-Hanssen (University of Hawaii at Manoa)

Is there a nontrivial automorphism of the Turing degrees? It is a major open problem of computability theory. Past results have limited how nontrivial automorphisms could possibly be. Here we consider instead how an automorphism might be induced by a function on reals, or even by a function on integers. We show that a permutation of ω cannot induce any nontrivial automorphism of the Turing degrees of members of 2^ω, and in fact any permutation that induces the trivial automorphism must be computable. A main idea of the proof is to consider the members of 2^ω to be probabilities, and use statistics: from random outcomes from a distribution we can compute that distribution, but not much more. In the second part of the talk, we answer a question of Schweber from 2013 by giving an explicit example is given of a countable group that is not isomorphic to the automorphism group of the Turing degrees $\mathrm{Aut}(\mathcal{D}_T)$. This is obtained by showing that $\mathrm{Aut}(\mathcal{D}_T)$ has a presentation recursive in Kleene's $\mathcal{O}$. We also show that $\mathrm{Aut}(\mathcal{D}_T)$ is a subgroup of a Δ^0_{19}-presentable group.

Chaitin's number as a function

Yu Liang (Nanjing University)

Abstract: TBA

Monotonous betting strategies in warped casinos

George Barmpalias (Chinese Academy of Sciences)

Suppose that you know the casino roulette is rigged and there is an imbalance of red/black outcomes, at least in the limit. Then there is a strategy which only bets on red or only bets on black, which guarantees you unbounded profit. More generally, suppose that you have the restriction that you cannot bet the dollars you earn by betting on red, to bet on black and vice-versa. In the same casino there is a successful strategy of this kind, which does not depend on where the bias is (red or black) or even the degree of the bias (ie how far from 1/2 each outcome frequency can get in the limit).

Sometimes casinos are rigged in more subtle ways, while satisfying all commonly used laws of large numbers like the relative frequency limit of each outcome tending to 1/2. Then are there simple winning strategies? We study this question from an algorithmic perspective, which is a natural approach since it is reasonable to expect that a strategy is programmable in a computer. We show that in the case of programmable strategies the answer is positive while in the case of countable mixtures of programmable strategies the answer is negative.

This talk is based on the following joint work with Fang Nan and Andy Lewis-Pye:
`https://arxiv.org/pdf/1807.04635.pdf`

Continuous valuations on quasi-Polish spaces

Matthew de Brecht (Kyoto University)

Quasi-Polish spaces are a class of countably based topological spaces which generalize both Polish spaces (which are important in analysis and measure theory) and ω-continuous domains (which are important in theoretical computer science and algebra). A valuation is a particular kind of mapping from the open subsets of a topological space to the real numbers, which shares many properties of a measure.

In this talk, we will give a brief introduction to quasi-Polish spaces and present some basic results concerning continuous valuations on quasi-Polish spaces. Every Borel measure restricts to a continuous valuation, and conversely every (locally finite) continuous valuation on a quasi-Polish space extends (uniquely) to a Borel measure. Furthermore, the space of continuous valuations on a quasi-Polish space is again a quasi-Polish space when given the weak topology.

Computer-assisted proofs via interval arithmetic: introduction and applications

Tomoyuki Miyaji (Meiji University)

In this talk, computer-assisted proofs using floating-point arithmetic are discussed from a viewpoint of applied analysis. A basic strategy of the proof is to verify the existence of the true solution near an approximate solution which is computed by a usual numerical method. Interval arithmetic plays a fundamental role in the verification method. It returns an interval which encloses the true value of arithmetic operation, taking all the rounding errors into account. One can use computer to test whether a sufficient condition of some fixed-point theorem is satisfied. Such verification methods are applied to many problems arising in dynamical systems, partial differential equations, computational geometry, etc. This talk consists of two parts. In Part 1, a brief overview of studies of verification methods based on interval arithmetic is provided, and some techniques of solving finite dimensional problems are explained. For instance, the interval Newton method is a standard method for solving nonlinear equations, and Lohner's method is applied to an initial value problem of ordinary differential equations. In Part 2, an application to a problem arising from mathematical fluid dynamics is presented. Some boundary value problem for ordinary differential equations is solved via the shooting method with the verification method.

Decision Problems in Matrix Semigroups: algorithmic decidability and computational complexity

Igor Potapov (University of Liverpool)

The abstracts of Potapov's talk and the contributed talks are added from the next page.

Decision Problems in Matrix Semigroups:

algorithmic decidability and computational complexity

Igor Potapov *

A large number of naturally defined matrix problems are still unanswered despite the long history of matrix theory. Originally in Arthur Cayley's "A Memoir on the Theory of Matrices" in 1858, the notion of a matrix arises naturally from abbreviated notations for a set of linear equations where he also defined associated operation of multiplication, notions of determinant, inverse matrices, etc. Nowadays questions on matrices and matrix problems emerge in much larger context as they appear in the analysis of various digital processes, verification problems [18], in the context of control theory questions [2]. Moreover problems on matrix products have been associated with several long standing open problems in algebraic number theory and transcendence theory, Nash equilibria, in the theory of joint spectral radius and its applications [9, 14, 18, 19].

Many simply formulated and elementary problems for matrices are inherently difficult to solve even in dimension two, and most of these problems become undecidable in general starting from dimension three or four [6, 4, 7, 9, 10, 20]. Only few decidability results are known so far, see for example [1, 12, 5, 11, 13, 21, 22, 23].

Let us given a finite set of square matrices (known as a generator) which is forming a multiplicative semigroup S. The classical computational problems for matrix semigroups are:

- Membership (Decide whether a given matrix M belong to a semigroup S) and two special cases such as: Identity (i.e. if M is the identity matrix) and Mortality (i.e. if M is the zero matrix) problems
- Vector reachability (Decide for a given vectors u and v whether exist a matrix M in S such that $M \cdot u = v$)
- Scalar reachability (Decide for a given vectors u, v and a scalar L whether exist a matrix M in S such that $u \cdot M \cdot v{=}L$)
- Freeness (Decide whether every matrix product in S is unique, i.e. whether it is a code) and some variants of the freeness such as finite freeness problem, the recurrent matrix problem, the unique

*Department of Computer Science, University of Liverpool, Email: potapov@liverpool.ac.uk.

- factorizability problem, vector freeness problem, vector ambiguity problems, etc.

The undecidability proofs in matrix semigroups are mainly based on various techniques and methods for embedding universal computations into matrix products. The case of dimension two is the most intriguing since there is some evidence that if these problems are undecidable, then this cannot be proved directly using previously known constructions. Due to a severe lack of methods and techniques the status of decision problems for 2×2 matrices (like membership, vector reachability, freeness) is remaining to be a long standing open problem not only for matrices over algebraic, complex, rational numbers but also for integer matrices.

Recently, a new approach of translating numerical problems of 2×2 integer matrices into variety of combinatorial and computational problems on words and automata over group alphabet and studying their transformations as specific rewriting systems [11, 13] have led to a few results on decidability and complexity for some subclasses:

- The membership problem for 2×2 nonsingular integer matrices is decidable [23]. The algorithm relies on a translation of numerical problems on matrices into combinatorial problems on words. It also makes use of some algebraic properties of well-known subgroups of $GL(2, \mathbb{Z})$ and various new techniques and constructions that help to convert matrix equations into the emptiness problem for intersection of regular languages.

- The Identity problem in $SL(2, \mathbb{Z})$ is NP-complete [8, 5]. Our NP algorithm is based on various new techniques that allow us to operate with compressed word representations of matrices without explicit exponential expansion.

- The vector reachability problem over a finitely generated semigroup of matrices from $SL(2, \mathbb{Z})$ and the point to point reachability (over rational numbers) for fractional linear transformations, where associated matrices are from $SL(2, \mathbb{Z})$ are decidable [21].

Similar techniques have been applied to show that the freeness problem is co-NP-hard [16] as well as to study the complexity of other freeness problems such as finite freeness problem, the recurrent matrix problem, the unique factorizability problem, vector freeness problem, vector ambiguity problems, etc [15].

Currently we focus on decidability of matrix problems in the Special Linear Group in dimension three, 3×3 matrices with determinant one. In the seminal paper of Paterson in 1970 [20], an injective morphism from pairs of words into 3×3 integral matrices was used to prove the undecidability of the mortality problem, and later led to many undecidability results of matrix problems in dimension three. In [17] it was shown that there is no embedding from pairs of words into 3×3 integral matrices with determinant one, i.e., into $SL(3, \mathbb{Z})$, which provides strong evidence that computational problems in $SL(3, \mathbb{Z})$ may be

decidable, as all known undecidability techniques for low-dimensional matrices are based on encoding of Turing machine computations via Post's Correspondence Problem (PCP), which cannot be applied in $SL(3,\mathbb{Z})$ following the results of [17]. In the case of the PCP encoding, matrix products extended by right multiplication correspond to a Turing machine simulation, and the only known proof alternatives rely on recursively enumerable sets and Hilbert's Tenth Problem, but provide undecidability for matrix equations of very high dimensions. [3].

References

[1] László Babai, Robert Beals, Jin-yi Cai, Gábor Ivanyos, and Eugene M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '96, pages 498–507, Philadelphia, PA, USA, 1996. Society for Industrial and Applied Mathematics.

[2] Vincent D. Blondel, John N. Tsitsiklis. A survey of computational complexity results in systems and control. Automatica 36(9): 1249-1274 (2000)

[3] Paul Bell, Vesa Halava, Tero Harju, Juhani Karhumki, Igor Potapov: Matrix Equations and Hilbert's Tenth Problem. IJAC 18(8): 1231-1241 (2008)

[4] Paul C. Bell, Mika Hirvensalo, and Igor Potapov. Mortality for 2x2 matrices is NP-hard. In Branislav Rovan, Vladimiro Sassone, and Peter Widmayer, editors, *Mathematical Foundations of Computer Science 2012*, volume 7464 of *Lecture Notes in Computer Science*, pages 148–159. Springer Berlin Heidelberg, 2012.

[5] Paul C. Bell, Mika Hirvensalo, and Igor Potapov. The Identity Problem for Matrix Semigroups in SL2(Z) is NP-complete. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, pages 187-206, 2017.

[6] Paul Bell and Igor Potapov. On undecidability bounds for matrix decision problems. *Theoretical Computer Science*, 391(1-2):3–13, 2008.

[7] Paul C. Bell and Igor Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *Int. J. Found. Comput. Sci.*, 21(6):963–978, 2010.

[8] Paul C. Bell and Igor Potapov. On the computational complexity of matrix semigroup problems. *Fundam. Inf.*, 116(1-4):1–13, January 2012.

[9] Vincent D. Blondel, Emmanuel Jeandel, Pascal Koiran, and Natacha Portier. Decidable and undecidable problems about quantum automata. *SIAM J. Comput.*, 34(6):1464–1473, June 2005.

[10] Julien Cassaigne, Vesa Halava, Tero Harju, and François Nicolas. Tighter undecidability bounds for matrix mortality, zero-in-the-corner problems, and more. *CoRR*, abs/1404.0644, 2014.

[11] Christian Choffrut and Juhani Karhumaki. Some decision problems on integer matrices. *RAIRO-Theor. Inf. Appl.*, 39(1):125–131, 2005.

[12] Esther Galby, Joël Ouaknine, and James Worrell. On Matrix Powering in Low Dimensions. In Ernst W. Mayr and Nicolas Ollinger, editors, *32nd International Symposium on Theoretical Aspects of Computer Science (STACS 2015)*, volume 30 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 329–340, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[13] Yuri Gurevich and Paul Schupp. Membership problem for the modular group. *SIAM J. Comput.*, 37(2):425–459, May 2007.

[14] Raphael Jungers. The Joint Spectral Radius. Theory and Applications, Lecture Notes in Control and Information Sciences, Springer, 146pp, 2009

[15] Sang-Ki Ko, and Igor Potapov Vector Ambiguity and Freeness Problems in SL(2,Z), Theory and Applications of Models of Computation: 14th Annual Conference, TAMC 2017, Bern, Switzerland, April 20-22, 2017, Proceedings, 2017, LNCS Springer, 373–388.

[16] Sang-Ki Ko, and Igor Potapov. Matrix Semigroup Freeness Problems in SL(2,Z). SOFSEM 2017: Theory and Practice of Computer Science: 43rd International Conference on Current Trends in Theory and Practice of Computer Science, 2017, LNCS Springer, 268–279.

[17] Sang-Ki Ko, Reino Niskanen, Igor Potapov: On the Identity Problem for the Special Linear Group and the Heisenberg Group. ICALP 2018: 132:1-132:15

[18] Joël Ouaknine, João Sousa Pinto, and James Worrell. On termination of integer linear loops. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '15, pages 957–969. SIAM, 2015.

[19] Joël Ouaknine and James Worrell. On the positivity problem for simple linear recurrence sequences,. In *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, pages 318–329, 2014.

[20] M. S. Paterson. Unsolvability in 3x3 matrices. *Studies in Applied Mathematics*, 49(1):pp.105–107, 1970.

[21] Igor Potapov and Pavel Semukhin. Vector reachability problem in SL(2, Z). MFCS 2016. 84:1-84:14, LIPICS, 2016

[22] Igor Potapov, Pavel Semukhin: Membership Problem in GL(2, Z) Extended by Singular Matrices. MFCS 2017: 44:1-44:13

[23] Igor Potapov and Pavel Semukhin. Decidability of the membership problem for 2 x 2 integer matrices. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, pages 170–186, 2017.

Bar induction and bar recursion with respect to continuity on Baire space

Makoto Fujiwara
Waseda Institute for Advanced Study, Waseda University

Bar induction is originally discussed by L. E. J. Brouwer under the name of "bar theorem" in his intuitionistic mathematics but first formalized by S. C. Kleene probably in late 1950's. On the other hand, in his posthumously published paper [1], C. Spector introduced a principle so-called "bar recursion" and gave a consistency proof of classical analysis by extending K. Gödel's consistency proof of Peano arithmetic by using the so-called Dialectica interpretation. As already mentioned in [1], bar recursion is an analogue of bar induction in the sense that bar recursion is a principle of definition and bar induction is a corresponding principle of proof. In particular, bar induction of type $\mathbb{N}$ (namely, formalized Brouwer's bar theorem) is briefly compared with bar recursion in an intuitionistic setting (namely, in the presence of continuity principle) in [1, Section 6 with footnote 5 and 6 written by G. Kreisel]. However, the exact relation between them from the purely constructive point of view is still unknown.

In this talk, we systematically study the relation between several forms of bar induction of type $\mathbb{N}$ and bar recursion for continuous functions of type $\mathbb{N}^{\mathbb{N}} \to \mathbb{N}$, which is classically valid while bar recursion in general is not so. Among other things, we show that the existence of bar recursor for continuous functions with continuous modulus of type $\mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ is derived from the decidable bar induction of type $\mathbb{N}$ over the extensional versions of intuitionistic arithmetic in all finite types with the axiom scheme of countable choice. In addition, the converse is also the case over that system augmented with the characteristic principles of the Dialectica interpretation.

This is a joint work with Tatsuji Kawai (Japan Advanced Institute of Science and Technology).

References

[1] C. Spector, Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles in current intuitionistic mathematics. In F. D. E. Dekker, editor, Recursive Function Theory: Proceedings of Symposia in Pure Mathematics, volume 5, pp. 1–27. American Mathematical Society, Providence, Rhode Island, 1962.

Independent distributions on a multi-branching AND-OR tree of height 2

(a joint work with Mika Shigemizu and Koki Usami)

Toshio Suzuki*[a]

[a] *Tokyo Metropolitan University, Japan*

We investigate an AND-OR tree T of height h and a probability distribution d on the truth assignments to the leaves. The *cost* denotes the expected number of leaves probed during the comuptation. If an algorithm is a minimizer of the cost among all algorithms being considerd then it is called an *optimal* algorithm (with respect to d). The following is a known result.

- (Tarsi,*J.ACM*, 1983) If d is an independent and identical distribution (IID) such that the probability of a leaf having value $0 \neq 0, 1$ then (under a certain assumptions) there exists an optimal algorithm that is depth-first.

Depth-first algorithms have an advantage that they are compatible with induction on subtrees. We investigate the case where d is an independent distribution (ID) and the probability depends on each leaf. The following are known results.

- (S.,2018) If $h \geq 3$ then Tarsi-type result does not hold.
- (S.,2018) If T is complete binary and $h = 2$ then Tarsi-type result holds.

We ask whether Tarsi-type result holds in the case of $h = 2$. Here, a child node of the root is either an OR-gate or a leaf: The number of child nodes of an internal node is arbitrary, and depends on an internal node.

- (Main result) If $h = 2$ then Tarsi-type result holds.

Our strategy of the proof is to reduce the problem to the case of directional algorithms. We discuss why our proof does not apply to height 3 trees.

References

[1] Mika Shigemizu, Toshio Suzuki and Koki Usami. Independent distributions on a multi-branching AND-OR tree of height 2. Preprint, arXiv:1804.06601[cs.DS] (2018).

[2] Toshio Suzuki. Non-Depth-First Search against an Independent Distribution on a Balanced AND-OR Tree. To appear in: *Inform. Process. Lett.*, 139 (2018) 13–17.

*E-mail: toshio-suzuki@tmu.ac.jp Partially supported by JSPS KAKENHI 16K05255.

Reverse mathematics of the finite downwards closed subsets of $\mathbb{N}^k$ ordered by inclusion

Florian Pelupessy

The following was conjectured by Hatzikiriakou and Simpson in Remark 6.2 in [1].

Definition 1 *We order k-tuples coordinatewise.*

Theorem 2 RCA_0 *proves that the following are equivalent:*

1. ω^{ω^ω} *is well founded,*
2. *For every k: the finite downwards closed subsets of $\mathbb{N}^k$, ordered by inclusion, are a well partial order.*

We confirm that this is the case, also with RCA_0^* as base theory.

References

[1] K. Hatzikiriakou and S. G. Simpson, *Reverse mathematics, Young diagrams, and the ascending chain condition*, Journal of Symbolic Logic **82** (2017): 576-589.

[2] F. Pelupessy, *Reverse mathematics of the finite downwards closed subsets of $\mathbb{N}^k$ ordered by inclusion and adjacent Ramsey for fixed dimension*, Mathematical Logic Quarterly **64**: 178-182.

On one-variable modal μ-calculus

Misato Nakabayashi*

A Joint work with Wenjuan Li†and Kazuyuki Tanaka‡

Modal μ-calculus, introduced by Kozen, is an extension of modal propositional logic by adding a greatest fixpoint operator μ and a least fixpoint operators ν. It is well suited for specifying properties of transition systems, and closely related to tree automata and parity games.

A fundamental issue on modal μ-calculus is the strictness of *alternation hierarchy* of the L_μ-formulas, which are classified by their *alternation depth*, namely, the number of alternating blocks of μ and ν. Roughly speaking, the class $\Sigma_0^\mu = \Pi_0^\mu$ is the class of L_μ-formulas with no fixed-point operations; Σ_{n+1}^μ (resp. Π_{n+1}^μ) is the closure of Σ_n^μ and Π_n^μ under the composition (i.e., substitution) and μ (resp. ν). A classical result by Rabin implies that $\Delta_2^\mu (= \Sigma_2^\mu \cap \Pi_2^\mu)$ is equal to the compositions of Σ_1^μ and Π_1^μ, which may also be represented by one-variable formulas.

In this talk, we first show the relationship between one-variable L_μ-formulas and weak alternating tree automata. An alternating tree automaton $\mathcal{A} = (A, Q, q_I, \delta, \Omega)$ with a priority function $\Omega : Q \to \{0, \ldots, n\}$ is said to be *weak* if δ has the following additional property:

$$\text{for all } q \in Q \text{ and } a \in A, \text{ if } q' \text{ occurs in } \delta(q, a), \text{ then } \Omega(q') \leq \Omega(q).$$

Then, we have

Theorem There is an effective translation procedure between a one-variable L_μ-formula φ and a weak alternating tree automaton $\mathcal{A}$ so that for all finitely branching transition system $(\mathcal{S}, s)$,

$$(\mathcal{S}, s) \models \varphi \Longleftrightarrow (\mathcal{S}, s) \in L(\mathcal{A}).$$

Furthermore, the alternation depth of a one-variable L_μ-formula φ corresponds to the number of the priorities of the associated automaton $\mathcal{A}$. Therefore, we conclude the strictness of the alternation hierarchy of one-variable L_μ-formulas within Δ_2^μ from the strictness of the hierarchy of weak alternating tree automata first proved by Mostowski.

Next, we consider infinitely branching transition systems, or especially recursively presented transition systems (RPTS). Bradfield [1] adapted Lubarsky's alternation hierarchy of arithmetic μ-calculus ($\Sigma_n^{A\mu}$, $\Pi_n^{A\mu}$) to show that for L_μ-formula $\varphi \in \Sigma_n^\mu$, the denotation $||\varphi||$ in any RPTS is a $\Sigma_n^{A\mu}$ definable set of integers, and conversely, for any arithmetic μ-calculus formula $\Phi \in \Sigma_n^{A\mu}$, there is an RPTS $\mathcal{R}$ and an L_μ-formula $\varphi \in \Sigma_n^\mu$ such that $||\Phi||$ is definable by φ over $\mathcal{R}$. Thus, Δ_2^μ in RPTS's corresponds to the class of sets S of integers such that both S and its complement are definable by a Σ_1^1-monotone operator. Therefore, in RPTS's, Δ_2^μ is not equal to the compositions of Σ_1^μ and Π_1^μ, which corresponds to the compositions of Π_1^1 and Σ_1^1 in integers.

Finally, we introduce the transfinite extension of the hierarchy of one-variable modal μ-calculus, and show that it exhausts Δ_2^μ in RPTS's.

References

[1] J.C. Bradfield, The modal μ-calculus hierarchy is strict. *Theoret. Comput. Sci.* **195** (1998), 133-153.

*Mathematical Institute, Tohoku University. E-mail: misato.nakabayashi@gmail.com

†School of Mathematics, Nanyang Technological University. E-mail: wenjuan.li1701@gmail.com

‡Mathematical Institute, Tohoku University. E-mail: tanaka.math@tohoku.ac.jp

A TUTORIAL ON GAME-THEORETIC PROBABILITY AND ALGORITHMIC RANDOMNESS

KENSHI MIYABE

I will give a tutorial on game-theoretic probability and algorithmic randomness.

Probability is a strange notion, and its formulation and interpretation is still ongoing. A mathematical formulation of the notion of probability has been given by Kolmogorov, which we call *measure-theoretic probability theory*. According to the theory, probability is something with which some axioms hold. There are some alternatives such as the theory of collectives by von Mises and algorithmic probability by Solomonoff. In both theories, random sequences are essential notions.

The most well-known notion of randomness is by Martin-Löf. An infinite binary sequence is ML-random if it is a *typical* sequence and it avoids all effective null sets. ML-randomness can be characterized by *unpredictability*, say, random if any effective betting strategy does not succeed along the sequence. Also by *incompressibility*, random if every initial segment does not have short descriptions. We have intuition that random if typical, unpredictable, or complex. One of interesting things about the theory of randomness is that we can mathematically prove such things.

The theory of randomness has a strong relation with computability theory. Chaitin's Ω is a left-c.e. real, which means it has a computable approximation from below, and is ML-random at the same time. Solovay reducibility is a notion to compare two left-c.e. reals in the sense of approximability. The top element of Solovay degrees in left-c.e. reals is exactly the class of left-c.e. ML-random reals. There are many statements about the relation between randomness and computability, which one can not state in the measure-theoretic probability.

Game-probability probability has another interpretation of probability, and it interacts with the theory of randomness. Suppose one flips a coin $(2n+1)$-times. Then, by symmetry, the event that the number of heads is larger than or equal to $n+1$ has probability $\frac{1}{2}$. In measure-theoretic probability, this is because the number of possible equally-likely outcomes is 2^n and the number of the desirable outcomes is exactly a half of it. Ville showed that there is a betting strategy such that one can double their capital when the desirable event occurs. The one should keep their capital non-negative along any outcome. The ratio of the final capital and the initial capital is nothing but game-theoretic probability.

Any theorem in measure-theoretic probability should have a game-theoretic counterpart proof, which roughly saying uses only martingales. Rewriting proofs via martingales makes it easy to analyze computability of martingales. Roughly saying, we can separate the proof into computability part and probability part. One such example will be given in my another talk.

(K. Miyabe) Meiji University, Japan
E-mail address: research@kenshi.miyabe.name

Some results of pS-reducibility

(a joint work with Toshio Suzuki and Masahiro Kumabe)

YUKI MIZUSAWA*[a]

[a] *Tokyo Metropolitan University, Japan*

Solovay reducibility is well-known notion in theory of algorithmic randomness.We define pS-reducibility as a generalization of Solovay reducibility.

We have following results

1. Solovay reducible ⇒ pS-reducible
2. ¬ [pS-reducible ⇒ Solovay reducible]
3. pS-reducible ⇒ wtt-reducible
4. ¬ [wtt-reducible ⇒ pS-reducible]
5. pS-reducibility is standard reducibility.

We also study relationship between reducibility and continuity in analytics and have some results.

References

[1] Rodney G. Downey and Denis R. Hirschfeldt. Algorithmic Randomness and Complexity,Theory and Applications of Computability. Springer-Verlag New York,2010.

*E-mail: houji6@gmail.com

ERDÖS-FELLER-KOLMOGOROV-PETROWSKY LAW OF THE ITERATED LOGARITHM

KENSHI MIYABE

A fundamental results in measure-theoretic probability is the *strong law of large numbers* (SLLN) shown by Borel (1901). Let X_i be i.i.d. random variables with $P(X_i = 1) = P(X_i = -1) = \frac{1}{2}$. Let $S_n = \sum_{i=1}^{n} X_i$. Then, $\frac{S_n}{n} \to 0$ almost surely.

A more precise version was given by Khintchine (1924). With the same assumption, we have

$$\limsup_{n\to\infty} \frac{S_n}{\sqrt{2n \ln \ln n}} = 1$$

almost surely. This is called the *law of the iterated logarithm* (LIL).

Further precise version was also known as the *Erdös-Feller-Kolmogorov-Petrowsky law of the iterated logarithm* (EFKP-LIL). Let ψ be a positive increasing function. Let

$$I(\psi) = \int_1^\infty \frac{\psi(\lambda)}{\lambda} \exp(-\psi(\lambda)^2/2) d\lambda$$

If $I(\psi) < \infty$, then

$$S_n < \sqrt{n}\psi(n)$$

for almost all n almost surely. If $I(\psi) = \infty$, then

$$S_n > \sqrt{n}\psi(n)$$

for infinitely many n almost surely. We call the former the *validity*, and the latter *sharpness*.

We restrict ψ to be computable. Notice that $I(\psi)$ may not be computable even if it converges, and $I(\psi)$ can grow more slowly than any computable function. The main claim in this talk is that computable randomness is sufficient to hold EFKP-LIL, but Schnorr randomness is not sufficient. In fact, the speed of divergence or convergence of $I(\psi)$ exactly corresponds to the bound of the speed of divergence of martingales.

The known proofs of EFKP-LIL for fair-coin tossing are fairy complicated. The EFKP-LIL also holds for Brownian motion, whose proof uses the Ornstein-Uhlenbeck process and its scale function. The proof can be naturally converted to a game-theoretic proof. Finally, we construct a computable function ψ and a Schnorr random sequence with some properties as usual in the theory of randomness.

(K. Miyabe) Meiji University, Japan
E-mail address: research@kenshi.miyabe.name

Approaching the first-order strength of Hindman's theorem

Keita Yokoyama*

Japan Advanced Institute of Science and Technology
y-keita@jaist.ac.jp

The reverse mathematical study of Hindman's theorem is initiated by Blass, Hirst and Simpson [1]. They showed that Hindman's theorem is provable from $\mathsf{ACA}_0{}^+$, and it implies ACA_0 over RCA_0. Since then, many people tried to decide the exact strength with many different approaches, but it is still open whether Hindman's theorem is equivalent to one of them or strictly in between. In this talk, we will try to calibrate the first-order strength of HIndman's theorem. Hindman's theorem is a Ramsey type theorem, and thus its first-order part can be approximated by some density style statement as in [2, 3]. We will give a characterization of the first-order part of Hindman's theorem with this idea, and then examine what is needed to prove the density style variation of Hindman's theorem. This is a joint work with Paul-Elliot Anglès d'Auriac.

References

1. Andreas R. Blass, Jeffry L. Hirst, and Stephen G. Simpson. Logical analysis of some theorems of combinatorics and topological dynamics. In *Logic and combinatorics (Arcata, Calif., 1985)*, volume 65 of *Contemp. Math.*, pages 125–156. Amer. Math. Soc., Providence, RI, 1987.
2. Andrey Bovykin and Andreas Weiermann. The strength of infinitary Ramseyan principles can be accessed by their densities. *Ann. Pure Appl. Logic*, 168(9):1700–1709, 2017.
3. Ludovic Patey and Keita Yokoyama. The proof-theoretic strength of Ramsey's theorem for pairs and two colors. *Adv. Math.*, 330:1034–1070, 2018.

* This work is partially supported by JSPS KAKENHI (grant numbers 16K17640 and 15H03634) and JSPS Core-to-Core Program (A. Advanced Research Networks).

On proving parameterized polynomial time computability of compositions of fundamental functions

Hiromichi Hamamoto, Akitoshi Kawamura, Martin Ziegler

In a standard formulation of real complexity theory [1], the complexity of real functions is discussed in oracle machine model and is measured in terms of the required precision n. This notion of complexity can only be applied to functions whose domain is compact, because the time for reading its arguments must be finite.

To differentiate more accurately the complexity of reading or outputting and the computing procedure itself, parametrized complexity has been recently introduced [2]. In this framework, the domain of a real function is a set of tuples of real numbers $\boldsymbol{x}$ and integer parameters $\boldsymbol{k}$, for example $\{(x,k) \in \mathbb{R} \times \mathbb{N} \mid x \in [-2^k, 2^k]\}$, and the complexity is measured in terms of n and $\boldsymbol{k}$. As an important theorem, the closure property of parameterized polynomial time computable functions under composition is proved by simply connecting Turing machines computing each subfunction. Moreover, fundamental functions, such as addition, multiplication, exponential and reciprocal, are proved to be parameterized polynomial time computable on appropriate domains.

Then as a natural interest, we want to prove parameterized polynomial time computability of functions, such as $f(x) = 1/e^x$, which can be expressed as composition of reciprocal and exponential functions. To grasp accurately parameterized polynomial time computability of such a function, each subfunction and their composition must be defined more carefully. In this talk, first I will give a sound definition of composition of parameterized real functions. Then after proving some properties and theorems about those functions, I will introduce output-sensitive polynomial time computability in order to more accurately characterize parameterized polynomial time computability of composition of reciprocal.

Reference

[1] Ker-I Ko. Complexity Theory of Real Functions. Birkhäuser Boston, 1991.
[2] Akitoshi Kawamura, Martin Ziegler. Invitation to Real Complexity Theory: Algorithmic Foundations to Reliable Numerics with Bit-Costs. In WAAC, 2015.

Computable analysis and computability in linear time

Akitoshi Kawamura[1], Florian Steinberg[2], and Holger Thies[3]

[1]Kyushu University [2]INRIA [3]University of Tokyo

For many applications, such as for instance computable analysis [5], one is interested in computing functions where input and output are not finite strings but functions themselves. That is, computing operators of type $\mathcal{B} \to \mathcal{B}$ where $\mathcal{B}$ denotes the Baire space of all total functions $\varphi\colon \{0,1\}^* \to \{0,1\}^*$ on finite binary strings. The accepted computational model for such type-2 computations are oracle machines or equivalent models.

Computational complexity theory deals with how efficiently a problem can be solved in terms of resources such as time and space. The computationally feasible functions are identified with those functions whose run-time can be bounded by a polynomial. For computations at type level two the class of basic feasible functionals is widely accepted as the natural class of feasible operations [3, 2].

Instead of only considering feasibility, one is often interested in which operations can be performed *efficiently*. A possible notion for efficient computation is computability in *linear time*. Already in classical complexity theory, robustness of linear-time computability under reasonable changes in the computational model is not given [1]. Nonetheless, proofs of linear-time computability are considered highly desirable in applications and there is a well-developed theory for the model of multi-tape Turing machines [4].

In this work, we put forward a complexity class of type-two linear-time. For this definition to be meaningful, a detailed protocol for oracle interactions has to be fixed. This includes some choices the defined class is sensible to and we carefully discuss our choices and their implications. We further discuss some properties and examples of linear-time and almost linear-time computable operators and applications to computable analysis.

References

[1] Gurevich, Y., and Shelah, S. Nearly linear time. In *International Symposium on Logical Foundations of Computer Science* (1989), Springer, pp. 108–118.

[2] Kapron, B. M., and Cook, S. A. A new characterization of type-2 feasibility. *SIAM Journal on Computing 25*, 1 (1996), 117–132.

[3] Mehlhorn, K. Polynomial and abstract subrecursive classes. In *Proceedings of the sixth annual ACM symposium on Theory of computing* (1974), ACM, pp. 96–109.

[4] Regan, K. W. Machine models and linear time complexity. *ACM SIGACT News 24*, 3 (1993), 5–15.

[5] Weihrauch, K. *Computable Analysis*. Springer, Berlin/Heidelberg, 2000.