Collection of Unpublished Abstracts of the 15th Conference on Computability in Europe

Florin Manea, Barnaby Martin, Daniel Paulusma and Giuseppe Primiero

This booklet contains the abstracts for informal talks as well as some invited talks and special session talks. The LNCS proceedings contains the abstracts and possibly also full papers that do not appear here.

Table of Contents

Invited Talks

Special Sessions

Informal Contributions

Machine-Checked Mathematics

Assia Mahboubi[1]

Abstract. This tutorial will give an overview of formalised and machine-checked mathematics, and discuss the trends and perspectives of this form of computer-aided mathematics.

Keywords: Formal proofs · Proof assistants · Program verification · Formalised mathematics · Logic · Type Theory.

Computers have changed the face of research in mathematics: typography, communication means, experimentation methods, and even the very nature of proofs. For instance, proofs today shall rely in a crucial way on intensive calculations, beyond the capabilities of a human reader. This phenomenon arises in various fields of mathematics: number theory, dynamical systems, combinatorics, etc. Consequently, program verification issues become part of the definition of mathematical rigour. The proof of the Kepler conjecture on sphere packing, by Thomas C. Hales with the help of Samuel Ferguson, and the story of its publication is an emblematic example of this phenomenon [2].

Proof assistants are pieces of software for doing machine-assisted mathematics and for developing digital libraries of formalised mathematics. The first modern proof assistant ever used was the AUTOMATH system, created by Nicolas G. de Bruijn. The foundations, design and implementation of proof assistants has been an active research area ever since. They have been so far mostly used to formalise results related to program verification, logic and to the theory of programming languages: e.g. a verified compiler for the C programming language [5] or a minimal core of operating system [4].

But recently, proof assistants are receiving increased attention from users with a background in mathematics. Large scale endeavours have come to success with the verification of a proof of the Kepler conjecture [2], of a proof of the Odd Order Theorem [1], and more recently that of an ODE solver [3], and the formalisation of the definition of perfectoid spaces[1].

This tutorial will discuss what are formalised mathematics and formal proofs, and describe the architecture of modern proof assistants. It will showcase what proof assistants can be used for today, and what is gained from the activity of formalising mathematics, beyond computer-aided verification.

References

1. Gonthier, G., Asperti, A., Avigad, J., Bertot, Y., Cohen, C., Garillot, F., Le Roux, S., Mahboubi, A., O'Connor, R., Ould Biha, S., Pasca, I., Rideau, L., Solovyev, A., Tassi, E., Théry, L.: A Machine-Checked Proof of the Odd Order Theorem. In: Blazy, S., Paulin, C., Pichardie, D. (eds.) ITP 2013, 4th Conference on Interactive Theorem Proving. LNCS, vol. 7998, pp. 163–179. Springer, Rennes, France (Jul 2013), https://hal.inria.fr/hal-00816699
2. Hales, T., Adams, M., Bauer, G., Dang, T.D., Harrison, J., Hoang, L.T., Kaliszyk, C., Magron, V., McLaughlin, S., Nguyen, T.T., et al.: A formal proof of the Kepler conjecture. Forum of Mathematics, Pi **5** (2017). https://doi.org/10.1017/fmp.2017.1
3. Immler, F.: A verified ODE solver and the lorenz attractor. J. Autom. Reasoning **61**(1-4), 73–111 (2018)
4. Klein, G., Andronick, J., Elphinstone, K., Heiser, G., Cock, D., Derrin, P., Elkaduwe, D., Engelhardt, K., Kolanski, R., Norrish, M., Sewell, T., Tuch, H., Winwood, S.: sel4: formal verification of an operating-system kernel. Commun. ACM **53**(6), 107–115 (2010)
5. Leroy, X.: Formal verification of a realistic compiler. Commun. ACM **52**(7), 107–115 (2009)

[1] https://github.com/leanprover-community/lean-perfectoid-spaces

Journeys in mathematical landscapes: genius or craft?

Ursula Martin

We look at how Anglophone mathematicians have, over the last hundred years or so, presented their activities using metaphors of landscape and journey. We contrast romanticised self-presentations of the isolated genius with ethnographic studies of mathematicians at work, both alone, and in collaboration, looking particularly at on-line collaborations in the *polymath* format. The latter provide more realistic evidence of mathematicians daily practice, consistent with the the *growth mindset* notion of mathematical educators, that mathematical abilities are skills to be developed, rather than fixed traits.

We place our observations in a broader literature on landscape, social space, craft and wayfaring, which combine in the notion of the production of mathematics as crafting the exploration of an unknown landscape. We indicate how *polymath* has a two-fold educational role, enabling participants to develop their skills, and providing a public demonstration of the craft of mathematics in action.

Logic and Computation of Social Behavior

Sonja Smets

Following the recent development in which logical methods can be applied to the formal analysis of social networks, I present work on the use of logic to study social influence and herd behavior in epistemic social networks. In such networks, we first consider agents who adopt a new fashion or behavior depending on whether a "sufficiently large enough group" of their neighbors already has adopted the behavior. We provide different types of models as well as a simple qualitative modal language to reason about the concept of a "strong enough" trigger of influence. Using fixed-point operators in our logic, important results from network theory about the characterization of informational cascades follow immediately and are a straightforward consequence of our logical axioms. Unfolding the influence dynamics in an epistemic social network allows us to characterize the epistemic conditions under which the dynamic diffusion process can speed up or slow down. The results presented in this talk are based on joint work with Alexandru Baltag at the University of Amsterdam and on the paper [1].

References

1. Alexandru Baltag, Zoe Christoff, Rasmus K. Rendsvig, Sonja Smets, Dynamic Epistemic Logics of Diffusion and Prediction in Social Networks *Studia Logica*, June 2019, Volume 107 (3), pp 489–531.

Climbing the hierarchy of completely positive entropy in two-dimensional shifts of finite type

Linda Brown Westrick

A $\mathbb{Z}^d$ shift of finite type (SFT) on alphabet $\mathit{\Lambda}$ is any set $X \subseteq \mathit{\Lambda}^{\mathbb{Z}^d}$ of the form

$$X = \{x \in \mathit{\Lambda}^{\mathbb{Z}^d} : \text{no pattern from } F \text{ appears in } X\}$$

where $F \subseteq \cup_n \mathit{\Lambda}^{[0,n)^d}$ is a finite set of forbidden patterns. Despite the simple definition, there is no algorithm which decides whether a given $\mathbb{Z}^2$-SFT is empty. The reason: an arbitrary Turing computation can be forced to appear in any symbolic tiling of the plane that obeys a precisely crafted finite set F of local restrictions. The presence of computation sometimes (but not always!) allows $\mathbb{Z}^2$-SFTs to mimic the properties of effectively closed subshifts, a strictly larger class. The circumstances under which $\mathbb{Z}^2$-SFTs will behave like effectively closed shifts are not well understood. This talk covers the emergence of another example.

In a recent series of papers, Pavlov [3, 4] and Barbieri and García-Ramos [1] explored the property of topological completely positive entropy (TCPE) in $\mathbb{Z}^d$-SFTs. Defined by Blanchard [2] as a topological analog of the K-property for measurable dynamical systems, TCPE is naively $\mathit{\Pi}^1_1$. However, Pavlov was able to give an arithmetic characterization of TCPE for $\mathbb{Z}$-SFTs. He also introduced two arithmetic properties that a $\mathbb{Z}^d$-SFT X could have, one of which he showed was strictly weaker than TCPE for $\mathbb{Z}^2$-SFTs, the other of which was shown by Barbieri and García-Ramos [1] to be strictly stronger. Generalizing both of these results, we show that there is no arithmetic property that characterizes TCPE in the $\mathbb{Z}^2$-SFTs.

Theorem 1. *The property of TCPE is $\mathit{\Pi}^1_1$-complete in the set of $\mathbb{Z}^2$-SFTs.*

In the course of proving their result, Barbieri and García-Ramos defined an ω_1-length hierarchy within TCPE which stratified TCPE into subclasses. Their explicit counterexample was a $\mathbb{Z}^3$-SFT at level 3 of this hierarchy, and they asked if this could be improved to a $\mathbb{Z}^2$-SFT. We answer in a quite general way. Standard methods of effective descriptive set theory imply that the TCPE rank of any $\mathbb{Z}^2$-SFT must be a computable ordinal. We show that this is the only restriction.

Theorem 2. *For any ordinal $\alpha < \omega_1^{ck}$, there is a $\mathbb{Z}^2$-SFT with TCPE rank α.*

The construction proceeds by first defining a family of effectively closed shifts of all computable TCPE ranks. Then the sofic computation framework of Durand, Romashchenko and Shen is superimposed, allowing the c.e. set of forbidden words to be enforced by embedded computation instead of by fiat. A naive application of this framework destroys the TCPE features of the subshifts in question, but with some tricks the computations can be superimposed transparently.

References

1. Sebastián Barbieri and Felipe García-Ramos. A hierarchy of topological systems with completely positive entropy. Available arXiv:1803.01948.
2. F. Blanchard. Fully positive topological entropy and topological mixing. In *Symbolic dynamics and its applications (New Haven, CT, 1991)*, volume 135 of *Contemp. Math.*, pages 95–105. Amer. Math. Soc., Providence, RI, 1992.
3. Ronnie Pavlov. A characterization of topologically completely positive entropy for shifts of finite type. *Ergodic Theory Dynam. Systems*, 34(6):2054–2065, 2014.
4. Ronnie Pavlov. Topologically completely positive entropy and zero-dimensional topologically completely positive entropy. *Ergodic Theory Dynam. Systems*, 38(5):1894–1922, 2018.

Learning to perceive and act in a stochastic environment

Ulrik Beierholm$^{1[0000-0002-7296-7996]}$

Most intelligent systems (biological or not) are able to access data from multiple sources across time and thus faces the problem of how to process this information given its stochastic and/or uncertain origin. Having a bountiful data set is only useful when there is an understanding of what to do with it.

Bayesian statistical inference provides an efficient way of making inferences about a stochastic system while effortlessly combining prior and current information. A large number of studies have shown that human inference in a range of paradigms (including visual, auditory and multisensory perception [1]) is able to utilise Bayesian inference, including the optimal combination of noisy redundant information sources, the use of prior knowledge, causal inference [2] etc.

In a typical experiment a subject is presented with stochastic but potentially redundant information through multiple perceptual stimuli and has to make judgements about properties of the generating environment, relying on current stimuli, prior knowledge, reliability of stimuli etc.

The ability to fully utilise such information relies on an understanding of the causal structure underlying the generation of the stochastic data [3]. It is not well understood how humans are able to learn such structures, to what degree novel structures can be learned or what constraints there are on this learning [4]. Current work is trying to address these problems using a combination of experiments and computational modeling.

These ideas have implications for any learning system that needs to make inferences based on data from a stochastic environment .

References

1. Beierholm, U.R.: Bayesian models of perception, In Encyclopedia of Computational Neuroscience. Springer Verlag (2015).
2. Kording, K.P., Beierholm, U., Ma, W.J., Quartz, S., Tenenbaum, J.B., Shams, L.: Causal inference in multisensory perception. PLoS One. **2**, e943 (2007).
3. Shams, L., Beierholm, U.R.: Causal inference in perception. Trends Cogn. Sci. **14**, 18 (2010).
4. Yildirim, I., Jacobs, R. A.: A Rational Analysis of the Acquisition of Multisensory Representations. Cogn. Sci. 36, 305332 (2011).

Ordinal Regularity

Merlin Carl

1 Ordinal Regularity

Ordinal Computability is commonly concerned with transfinite generalizations of machine models of computability that are classically equivalent to Turing computability; examples are Turing machines, register machines or λ-calculus. Here, we introduce Deterministic Ordinal Automata (DOAs) as generalizations of deterministic finite automata (DFAs) to the transfinite. The absence of a specific limit rule in our setting makes the corresponding notion of regularity extremely liberal, compared e.g. with the approach of Schlicht, Stephan et al., see [KHS].

For a set $\mathcal{A}$, let us write $\mathcal{A}^{**}$ for the set of ordinal strings over $\mathcal{A}$, i.e. the set of functions $f : \alpha \to \mathcal{A}$ where α is an ordinal. In our framework, a DOA $\mathfrak{M}$ on a finite alphabet $\mathcal{A}$ is a set S of states (that can be of any cardinality) together with a partial class function $D : S \times \mathcal{A} \to S$ that satisfies the following 'coherence' or 'forgetfulness' condition: For any $s \in S$ and all $w, w' \in \mathcal{A}^{**}$ such that both $D(s, w)$ and $D(D(s, w), w')$ are defined, $D(s, ww')$ is also defined and equal to $D(D(s, w), w')$ (where ww' denotes the concatenation of w and w'). Moreover, some $s_0 \in S$ is specified as a starting state and some $C \subseteq S$ is specified as the set of accepting states of $\mathfrak{M}$. A subclass $\mathcal{L}$ of $\mathcal{A}^{**}$ is called REG^{∞} if and only if

In spite of this very weak condition on D, we shall see that the basic constructions associated with DFAs, such as the equivalence with NFAs via the power set construction or the theorem of Myhill-Nerode, have straightforward analogues for DOAs.

We then consider connections with space complexity for Ordinal Turing Machines (OTMs), a topic initiated by Löwe in [L] and then further e.g. in [CLR] and [Ca18]. OTMs are transfinite analogues of Turing machines that have the whole class of ordinals available both as the indices of their tape cells and as their working time. A classical theorem in complexity theory is that, if the space usage s of a Turing machine T is such that $2^{2^{s(n)}} \leq c \cdot n$ for some $c \in \mathbb{N}$, then T in fact has a constant bound on its space usage and hence decides a regular language. (See e.g. [Hro] for a proof of this.) We will prove the following ordinal analogue to one direction of this complexity-theoretical characterization of regularity: If P is an OTM-program such that P halts on input s in $<\mathrm{card}(s)$ many steps for any infinite $s \in \mathcal{A}^{**}$ for a finite alphabet $\mathcal{A}$, then the subclass of $\mathcal{A}$ decided by P is REG^{∞}.

Most of the work we will present can be found in the preprint [Ca17].

References

[Ca17] M. Carl. Space-Bounded OTMs and REG^{∞}. Preprint, arXiv:1707.05297v2 (2017)

[Ca18] M. Carl. Some Observations on Infinitary Complexity. In: F. Manea, R. Miller, D. Nowotka (eds.), Sailing Routes in the World of Computation, CiE 2018, Proceedings, LNCS 10936, pp. 118–125 (2018)

[CLR] M. Carl, B. Lwe, B. Rin. Koepke Machines and Satisfiability for Infinitary Propositional Languages. In: J. Kari, F. Manea, I. Petre (eds.), Unveiling Dynamics and Complexity, 13th Conference on Computability in Europe, CiE 2017, Turku, Finland, Proceedings, LNCS 10307, pp. 187-197 (2017)

[Hro] J. Hromkovic. Theoretische Informatik. Springer Vieweg (2011)

[KHS] A. Kartzow, M. Huschenbett, P. Schlicht. Pumping for ordinal automatic structures. Computability 6, 2 (2017), 125-164

[L] B. Lwe. Space bounds for infinitary computation. In: A. Beckmann, U. Berger, B. Lwe, J. V. Tucker (eds.), Logical Approaches to Computational Barriers, CiE 2006, Proceedings, LNCS 3988, pp. 319–329 (2006)

Stability in a probabilistic setting

Thomas Ehrhard

Positive cones were introduced in [4] as a tool for designing a denotational model of higher order quantum computations. Such an object consists of an $\mathbb{R}_{\geq 0}$-semiring P equiped with a *norm* function $\|\_\| : P \to \mathbb{R}_{\geq 0}$ satisfying: $x+y = x'+y \Rightarrow x = x'$, usual axioms for a norm ($\|rx\| = r\|x\|$, $\|x+y\| \leq \|x\| + \|y\|$ and $\|x\| = 0 \Rightarrow x = 0$) as well as $\|x\| \leq \|x+y\|$ which expresses that the elements of P are positive. Then P is equiped with a canonical order relation defined by $x \leq y \Leftrightarrow \exists z\, x + z = y$ and it is also assumed that the unit ball $\mathcal{B}_1$ of P (the set of all $x \in P$ such that $\|x\| \leq 1$) is complete in the sense that any monotonic sequence in $\mathcal{B}_1$ has a lub in $\mathcal{B}_1$. In [3] we showed that exactly the same notion can be used for modeling probabilistic computations. For this purpose we introduced new morphisms between such cones that we called *stable functions*. A stable function $f : P \to Q$, where P and Q are positive cones, is a function $\mathcal{B}_1(P) \to \mathcal{B}_1(Q)$ which satisfies an iterated monotonicity property: whenever it makes sense we have

$$\begin{aligned}
f(x) &\leq f(x+u) \quad \text{(ordinary monotonicity)}\\
f(x+u_1) + f(x+u_2) &\leq f(x+u_1+u_2) + f(x)\\
f(x+u_1+u_2) + f(x+u_2+u_3) + f(x+u_1+u_3) + f(x)&\\
&\leq f(x+u_1+u_2+u_3) + f(x+u_1)\\
&\qquad\qquad + f(x+u_2) + f(x+u_3)\\
&\vdots
\end{aligned}$$

and is Scott-continuous. I will explain that this defines a category which is cartesian closed and has fixed point operators. Then, by considering such cones equiped with an additional *measurability* structure, I will show that the corresponding category provides a model for higher order probabilistic programs dealing with probability distributions on the real line (and other "continuous" types). By transposing this definition of morphisms to coherence spaces I will explain why they are called stable, and I will also mention a result of Raphaëlle Crubillé [1] showing that this semantics is a conservative extension of the model of probabilistic coherence spaces [2].

References

1. Raphaëlle Crubillé. Probabilistic Stable Functions on Discrete Cones are Power Series. In Anuj Dawar and Erich Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 275–284. ACM, 2018.
2. Thomas Ehrhard, Michele Pagani, and Christine Tasson. Full Abstraction for Probabilistic PCF. *Journal of the ACM*, 65(4):23:1–23:44, 2018.
3. Thomas Ehrhard, Michele Pagani, and Christine Tasson. Measurable cones and stable, measurable functions: a model for probabilistic higher-order programming. *PACMPL*, 2(POPL):59:1–59:28, 2018.
4. Peter Selinger. Towards a semantics for higher-order quantum computation. In *Proceedings of the 2nd International Workshop on Quantum Programming Languages, Turku, Finland*, number 33 in TUCS General Publication. Turku Centre for Computer Science, 2004.

Computable Representations of Exchangeable Data

Cameron E. Freer

An array of data is *exchangeable* when its distribution does not depend on the order of the rows/columns. In hand-engineered systems, exchangeability is often exploited to accelerate probabilistic inference, yet few probabilistic programming languages beyond the Church family have any special support for exchangeability. Results in probability theory suggest that no special support would seem to be needed: given exchangeable arrays of data of unbounded size, theorems by de Finetti, Aldous, and Hoover lead to stateless representations of the arrays that expose the key conditional independences and symmetries. However, these results do not take into account computational constraints. In joint work with Ackerman, Avigad, Roy, and Rute, we investigate the computability of the representations, and whether they can themselves be computed given a representation of an exchangeable sequence or array. We give both positive and negative results, and discuss the consequences for the design of probabilistic programming languages.

Could computers understand their own programs?

Tony Hoare MA

My answer is yes. To support the positive answer, I give a brief account of the teaching of three famous philosophers, Aristotle, Euclid and Turing.

After a brief reminder of the Aristotelian syllogism and of Euclidian Geometry, I will give examples of the power of computers, which have been programmed to prove major mathematical conjectures like Fermat's last Theorem and the Kepler conjecture.

Computers are now routinely used in the software industry to check the security of their own programs, as well as reporting on deep and shallow errors in all programs that are submitted to them. Industrial and academic research is now concentrated on extending these capabilities.

Finally, I will propose a variant of the well-known Turing test, which is confined to conversations about correct and faulty programs. The participants are the intelligent programmer and the computer. The passing of the test will be that the conversations are actually helpful to practicing programmers.

A Friendly Smoothed Analysis of the Simplex Method

Daniel Dadush[1], *Sophie Huiberts*[1]

The simplex method for linear programming performs much better in practice than theoretical worst-case results would suggest. The bad instances don't seem to occur in practice. In practice, the simplex method takes a number of pivot steps that is roughly linear in $d+n$, where d is the number of variables and n is the number of constraints. The theoretical worst-case performance is at least sub-exponential for all pivot rules that have been analyzed.

The smoothed analysis framework of Spielman and Teng [2] aims to show that difficult instances are unlikely to occur by considering the expected running time under a small perturbation of the input data, and, under this regime, Spielman and Teng managed to prove a smoothed polynomial complexity for a specific simplex method. Their results have been improved in various ways by other authors since. We improve over previous running time bounds in all parameter regimes, with a substantially simpler and more general proof.

Theorem 3. *There is a self-dual simplex method such that, if a linear program* $\max c^{\mathsf{T}} x$ st $Ax \leq b$*, in* d *variables with* n *inequalities, has its constraint vectors* (a_i, b_i) *distributed with* $\|\mathbb{E}[(a_i, b_i)]\| \leq 1$ *and independent Gaussian noise of variance* σ^2 *on every entry of* (A, b)*, the algorithm solves the program in expected time* $O(d^2 \sqrt{\log n}\ \sigma^{-2} + d^3 \log^{3/2} n)$.

Underlying this running time bound is a geometric statement about the expected number of edges of the projection of a polyhedron onto a two-dimensional plane. We proved a better bound on this quantity, as well as a better reduction of algorithmic complexity to it.

Theorem 4. *Let* $W \subset \mathbb{R}^d$ *be a fixed two-dimensional subspace,* $n \geq d \geq 3$ *and let* $a_1, \ldots, a_n \in \mathbb{R}^d$*, be independent Gaussian random vectors with variance* σ^2 *and centers of norm at most* 1*. We write* A *for the matrix with* $a_1, \ldots, a_n$ *as its rows. For* $P := \{x : Ax \leq 1\}$*, the number of edges of the projection polygon* $\pi_W(P)$ *of* P *onto* W *is bounded by*

$$\mathbb{E}[|\mathrm{edges}(\pi_W(P))|] \leq \mathcal{D}_g(n, d, \sigma),$$

where the function $\mathcal{D}_g(d, n, \sigma)$ *is defined as*

$$\mathcal{D}_g(d, n, \sigma) := O(d^2 \sqrt{\log n}\ \sigma^{-2} + d^{2.5} \log n\ \sigma^{-1} + d^{2.5} \log^{1.5} n).$$

References

1. D. Dadush, S. Huiberts, *A Friendly Smoothed Analysis of the Simplex Method*, in *Proceedings of the 50th annual ACM sumposium on Theory of computing* (2018), 390–403. Full version to appear in SICOMP Special Issue.
2. D. Spielman and S-H. Teng. Smoothed Analysis of Algorithms: Why the Simplex Algorithm Usually Takes Polynomial Time. J. ACM, 51(3):385463 (electronic), 2004.

Behaviours and Model Fidelity in Cyber-Physical Systems

Michael Jackson

A cyber-physical system introduces computing equipment into the world to govern its behaviour; dependable behaviour relies on mathematical reasoning from formal models faithful to physical reality. But physical reality cannot provide what mathematical certainty demandstimeless truth, base axioms, atomicity, discrete values, frame conditions, compositionality, and more: at engineering scales, everything in the physical world is recursively contingent. In a cyber-physical system, if the world deviates materially from the model, the system will fail – perhaps catastrophically. This talk presents an approach to behaviour development that can contribute directly to model fidelity – and *ipso facto* to system dependability. A system comprises a bounded world W and a machine M; their interaction evokes the governed behaviour. Both parts are modelled – the software machine by a program text $\underline{M}$, the world by a formal symbolic model $\underline{W}$. The governed behaviour is modelled as a set of traces of phenomena – for example, events and state valuee – denoted by terms in these two interacting models. Requirements are properties, effects and consequences of behaviours. System behaviour is developed – primarily bottom-up – as an assemblage of simple constituent behaviours, each having its own machine M, bounded world W, and models $\underline{M}$ and $\underline{W}$. System operation forms a dynamic tree of concurrent behaviour activations, each instantiated and controlled by its parent. A behaviour may be enacted many times: fidelity is demanded of $\underline{W}$ only on activation and during enactment. If fidelity fails the enactment is pre-emptively terminated. This approach to behaviour contributes to model fidelity in several ways. There is no single model of the physical world. Each $\underline{W}$, further separated into behaviour and requirement models, is simple, and supports sound formalisation – explicit interpretation, multiple granularities, bounded and closed model subjects, wary use of abstraction, and more. Causality is modelled. Causal links are not observable phenomena, but postulated over the physical substratum of domains, entities, states and events: effectuation of each link is attributed to a specific physical domain. In combining and assembling behaviours, potential interferences and conflicts among models are identified and resolved. Explicit design of the enactment tree reveals patterns of behaviour in the large, provides for behaviours to monitor and diagnose the physical context, and prevents avoidable model failure.

Quantitative Separation Logic

Joost-Pieter Katoen

In this talk, we marry two seminal deductive techniques for program verification: weakest pre-expectations and separation logic. Kozen's quantitative analogue of weakest pre-conditions [3], further developed by McIver and Morgan [4], are used to reason about probabilistic effects in randomised algorithms such as coin flipping. Separation logic as originally proposed by Reynolds, O'Hearn and Ishtiaq [2, 5] enables logical reasoning about pointer programs and can deal with aliasing, memory leaks etc. We show that these two different techniques can be combined in a rather natural and elegant manner. This results in *quantitative separation logic* (QSL) [1], a logic for reasoning about pointer programs that use randomisation. In contrast to classical separation logic, QSL employs quantities which evaluate to real numbers instead of predicates which evaluate to Boolean values. The connectives of classical separation logic, separating conjunction and separating implication, are lifted from predicates to quantities.

Main QSL features are: (1) it conservatively extends both weakest pre-expectations and separation logic; in particular, the quantitative analogue of separating conjunction is backward compatible to its classical counterpart and obeys the same laws, e.g. modus ponens and adjointness, (2) QSL's wp-calculus is sound with respect to an intuitive operational semantics based on Markov decision processes, and (3) QSL's wp-calculus preserves O'Hearn's frame rule—the key principle in separation logic enabling local reasoning about heaps.

QSL thus enables to reason about probabilistic programs mutating dynamic data structures in a compositional way purely at the source-code level.

The QSL calculus enables reasoning about quantities such as the probability of terminating with an empty heap in a faulty garbage collection algorithm, the expected length of a list in a lossy list traversal, or the expected length of a path from the root to a leaf in randomised meldable heaps.

References

1. Kevin Batz, Benjamin Lucien Kaminski, Joost-Pieter Katoen, Christoph Matheja, and Thomas Noll. Quantitative separation logic: a logic for reasoning about probabilistic pointer programs. *PACMPL (POPL)*, 3:34:1–34:29, 2019.
2. Samin S. Ishtiaq and Peter W. O'Hearn. BI as an assertion language for mutable data structures. In *POPL*, pages 14–26, 2001.
3. Dexter Kozen. A probabilistic PDL. In *STOC*, pages 291–297, 1983.
4. Annabelle McIver and Carroll Morgan. *Abstraction, Refinement and Proof for Probabilistic Systems.* Monographs in Computer Science. Springer, 2005.
5. John Charles Reynolds. Separation logic: A logic for shared mutable data structures. In *LICS*, pages 55–74. IEEE Computer Society, 2002.

Lowness of the Pigeonhole principle

Benoît Monin, Ludovic Patey

Given a coloring $c : \omega \to \{0,1\}$, there must be, by the Pigeonhole principle, an infinite set X such that c assigns the same color to every element of X. This rather easy theorem is known as the RT^1_2 principle in reverse mathematics : An instance of RT^1_2 is a coloring $c : \omega \to \{0,1\}$, and a solution of this instance is an infinite set X whose every element are assigned the same color via c.

We study the general question of the computational power of RT^1_2: Given a notion of "computational strength", that is, an upward closed class $\mathcal{C}$ in the Turing degree, can we build an instance c of RT^1_2 such that every solution to c is a member of $\mathcal{C}$? The general paradigm is that RT^1_2 has very little computational power. For almost every known natural notion of "computational strength" $\mathcal{C}$, it is known that RT^1_2 is low for this notion : for every instance c of RT^1_2, there is a solution of c which is not a member of $\mathcal{C}$.

One of the first of these result is that for any non computable set X and any instance c of RT^1_2, one solution of c does not compute X (Dzhafarov and Jockusch). To show this, the authors designed a special forcing notion : the computable Mathias forcing, with which one can control the truth of Σ^0_1 statements. Last year, Monin and Patey designed in the article "Pigeons do not jump high", a new forcing notion, that builds upon computable Mathias forcing, in order to control the truth of Σ^0_2 statements. This lead to the following result : for every instance c of RT^1_2, there is a solution of c which is not of high degree, that is whose jump does not compute the double jump.

Oddly enough, this new forcing could not be iterated in order to control the truth of Σ^0_n statement, not even Σ^0_3. The difficulty behind such an iteration have recently been overcome : A general forcing notion have been found, allowing to show that for every instance c of RT^1_2, there is a solution of c whose n-th jump does not compute the $(n+1)$-th jump. This lead to knew results, such as preservation of arithmetical and hyperarithmetical reductions, for RT^1_2.

The computational strength of points in function spaces

Takayuki Kihara[1], *Keng Meng Ng*[2]

The study of computability in analysis has a rich history, and is still very much an active and ongoing program. In this work we focus on the computational strength of points in topological spaces. Each point in an effective second countable space can be associated with an enumeration degree, and one can use this to compare the "computational strength" between different topological spaces. A well-known example of this is the class of continuous degrees introduced by Miller. We give a survey of different results, emphasizing on the use of enumeration degrees in understanding the computational content of (the points in) a second countable space.

We take this work further and consider the use of computability in defining the computational strength of points in function spaces. As this requires a notion of countability, we follow the approach of Kleene in his work on higher type computations. We launch a systematic study into the computability of points in function spaces and compare the strength of various spaces in this way.

Future Directions in Transfinite Complexity

Benjamin Rin

Transfinite complexity theory is the analogue of classical complexity theory lifted to the transfinite case. As one may expect, the idea is to study what is computable by transfinite machines under given resource constraints. For instance, in the mid-2000s, a few papers considered the capabilities and limits of infinite time Turing machines (ITTMs) with constraints on run time ([4], [2], [3]). Among other results, an infinitary analogue of $\mathsf{P} \neq \mathsf{NP}$ was found. Interest arose about a decade later in complexity theory for Ordinal Turing Machines (OTMs), whereby it was found, for example, that ∞-SAT—the satisfiability problem for infinitary propositional logic $\mathcal{L}_{\infty,0}$—is ∞-NP-complete (that is, complete for nondeterministic ordinal polynomial-time computations on OTMs) (see [1]). A few other works exist, but the literature so far is still small. Little is known at the present early stage about complexity theory for other transfinite machines outside of ITTMs and OTMs—e.g., ordinal register machines, ordinal Blum-Shub-Smale machines, or α-ITTMs.

In this talk, we will first briefly outline the current state of the art in transfinite complexity theory. We will then examine a variety of possible directions that the future of this subject may take. The most straightforward among these is to consider infinitary decision problems relating to infinitary logics, algebra, graph theory, and other domains, and then identify the transfinite resources necessary to compute them. But we will also discuss the possible viability and challenges of taking other sub-disciplines within finite complexity—for instance, descriptive complexity theory—and importing them to the transfinite setting. Further seemingly promising links between transfinite complexity and logic will also be discussed. As this subject is still young and extremely wide open, a number of open questions will be raised throughout the talk.

References

1. Carl, M., Löwe, B., Rin, B.: Koepke Machines and Satisfiability for Infinitary Propositional Languages. In: J., K., F., M., I., P. (eds.) Unveiling Dynamics and Complexity. CiE 2017. LNCS, vol. 10307. Springer, Cham (2017)
2. Deolalikar, V., Hamkins, J.D., Schindler, R.: $\mathbf{P} \neq \mathbf{NP} \cap \mathbf{co}\text{-}\mathbf{NP}$ for infinite time Turing machines. J. Log. Comput. **15**(5), 577–592 (2005)
3. Hamkins, J.D., Welch, P.D.: $\mathbf{P}^f \neq \mathbf{NP}^f$ for almost all f. Math. Log. Q. **49**(5), 536–540 (2003)
4. Schindler, R.: $\mathbf{P} \neq \mathbf{NP}$ infinite time Turing machines. Monatsh. Math. **139**, 335–340 (2003)

The Smoothed Number of Pareto-optimal Solutions in Non-integer Bicriteria Optimization*

Heiko Röglin, Clemens Rösner

Optimization problems that arise from real-world applications often come with multiple objective functions. Since there is usually no solution that optimizes all objectives simultaneously, trade-offs have to be made. One of the most important solution concept in multi-objective optimization is that of *Pareto-optimal solutions*, where a solution is called Pareto-optimal if there does not exist another solution that is simultaneously equal or better in every objective and strictly better in at least one objective. Intuitively Pareto-optimal solutions represent the reasonable trade-offs between the different objectives, and it is a common approach to compute the set of Pareto-optimal solutions to filter out all unreasonable trade-offs. For many multi-objective optimization problems there exist algorithms that compute the set of Pareto-optimal solutions in polynomial time with respect to the input size and the number of Pareto-optimal solutions. These algorithms are not efficient in the worst case because for almost every problem with two or more objectives there exist instances with an exponential number of Pareto-optimal solutions. This however does not reflect experimental results, where the number of Pareto-optimal solutions is usually small. To reconcile theory and practice, the number of Pareto-optimal solutions has been analyzed in the framework of smoothed analysis, and it has been shown that the expected value of this number is polynomially bounded for linear integer optimization problems. We make the first step towards extending the existing results to non-integer optimization problems. Given a finite set of solution vectors for a linear bicriteria optimization problem, we define two interdependent parameters connected to the number of different values and the smallest Euclidean distance between different solutions. We show an upper bound on the smoothed number of Pareto-optimal solutions, which depends polynomially on these two parameters and the dimension of the problem. Furthermore, we improve the previously known analysis of the smoothed number of Pareto-optimal solutions in bicriteria integer optimization slightly to match its known lower bound.

*This research was supported by ERC Starting Grant 306465 (BeyondWorstCase).

Multielectrode-array applications to investigate retinal function in health and disease

Evelyne Sernagor

Vision begins with photoreceptors converting light from different parts of the visual scene into electrical signals, compressing our visual world into a parsimonious code of spikes at the retinal output level, the retinal ganglion cells (RGCs). The brain then recreates images from interpreting these highly compressed barcodes or trains of spikes. RGCs reside in a monolayer, the innermost cellular layer of the retina. This two-dimensional configuration is particularly amenable to recordings using planar multielectrode arrays (MEAs) which come in direct contact with the RGC layer, allowing us to undertake population recordings of the retinal output to the brain. This talk will introduce various projects from our group investigating RGC function using large-scale, high density MEA recordings. We use the active pixel sensor (APS) MEA, consisting of 4,096 electrodes arranged in a 64x64 configuration to record from the RGC layer in the mouse retina. The array covers a substantial proportion of the RGC layer, allowing us to undertake large population (100s to 1,000s of cells) recordings that reveal important network properties that cannot be deciphered when done at lower spatiotemporal resolution. Assigning spikes to individual RGCs is a challenging task in high density recording systems because activity from the same cell can be detected on several neighbouring electrodes. We use a novel approach for accurate spike clustering. The method takes advantage of that multiple sampling, using the x,y coordinates of current sources combined with principal component analysis. Spontaneous waves of activity spread across the RGC layer in the neonatal retina. These waves are important for guiding the development of visual connectivity both at the level of the retina and in retinal central projections. Thanks to the high spatiotemporal resolution of the APS MEA, we were able to characterise profound developmental changes in wave dynamics during the critical period for wiring the visual system, providing important novel insights about the possible role of these waves in consolidating connectivity while the visual system develops. RGCs come in an astonishing functional variety, each class conveying a different aspect of the visual scene to the brain visual areas. RGC functional classification is a challenging task. We are using an interdisciplinary approach to characterise novel RGC classes. It is based on pharmacogenetics to characterise RGCs sharing gene expression, using a combination of MEA electrophysiology, neuroanatomy and modelling. We use a non-parametric computational approach for functional clustering, based on comparing spike distances between spike trains. Thanks to large-scale recordings from 100s to 1,000s of RGCs, we were also able to determine that RGCs use a population approach to decode visual stimuli, including complex visual scenes, and that their performance improves when images undergo transformations, an important issue for the development of retinal prosthetics.

Brains and Bayes Nets: Inferring Neural Information Flow

V. Anne Smith[0000−0002−0487−2469]

2 Overview

Understanding how information flows in the brain or other neural systems – often know as functional connectivity – is of great interest for elucidating many aspects of behaviour. In this talk, I will provide an overview of our work on using a probabilistic graphical model, dynamic Bayesian networks, to infer neural information flow. Bayesian networks are well-suited for inference of biological networks in general: their probabilistic framework easily models the stochastic nature of biological systems as well as noise in measurement; they are capable of handling simultaneous interactions of multiple forms, such as linear, non-linear, non-monotonic, and combinatoric [1, 2]. Neuroscience in particular is especially amenable to their application. Neural recordings can easily amass tens of thousands or even hundreds of thousands of samples, feeding Bayesian networks' famously data-hungry algorithms [3], and the neuronal system itself is hypothesised to be inherently Bayesian [4].

I will cover material ranging from our original validation of inferred neural information flow with known anatomy [5], to developing a new score for single unit recordings [6], to recent work inferring networks from live imaging data, showing the power of dynamic Bayesian networks for neuroscience.

References

1. Friedman, N.: Inferring cellular networks using probabilistic graphical models. Science **303**, 799–805 (2004)
2. Heckerman, D., Geiger, D., Chickering, D. M.: Learning Bayesian networks: The combination of knowledge and statistical data. Mach. Learn. **20**, 197–243 (1995)
3. Smith, V. A.: Revealing structure of complex biological systems using Bayesian networks. In: Estrada, E., Fox, M., Higham, D. J., Oppo, G.-L. (eds) Network Science: Complexity in Nature and Technology, pp. 185–204. Springer-Verlag, London (2010)
4. Rao, R. P. N.: Bayesian computation in neural circuits. Neural Comput. **16**, 1–38 (2004)
5. Smith, V. A., Yu, J., Smulders, T. V., Hartemink, A. J., Jarvis, E, D.: Computational inference of neural information flow networks. PLoS Comp. Biol. **2**, e161 (2006)
6. Echtermeyer, C., Smulders, T. V., Smith, V. A.: Causal pattern recovery from neural spike train data using the Snap Shot Score. J. Comp. Neurosci. **29**, 231–252 (2010)

Semantic models of probability with higher order functions[⋆]

Sam Staton[1]

Higher order functions arise in several ways in probabilistic programming.

- One way is as regression problems: given some data points, what is the chance that they were generated by one function or another? A solution to a Bayesian regression problem is a distribution over a space of functions.
- Another is in a probabilistic treatment of fresh name generation, such as Lisp's gensym or, more formally, the ν-calculus of Pitts and Stark [2]. Although name generation is an aspect of traditional programming, it also seems important in Bayesian non-parametrics.

In this talk I will discuss issues regarding the combination of higher-order functions and continuous probability distributions, drawing on mathematical frameworks such as measure theory (e.g. [1]), domain theory (e.g. [4]), and quasi-Borel spaces [3].

The talk will be partly based on work and discussions with Nate Ackerman, Cameron Freer, Chris Heunen, Ohad Kammar, Gordon Plotkin, Dan Roy, Dario Stein, Matthijs Vákár, Hongseok Yang, and others.

References

1. Aumann, R.J.: Borel structures for function spaces. Illinois J. Math. **5**:614-630. 1961.
2. Pitts, A.M., Stark, I.D.B.: Observable properties of higher order functions that dynamically create local names, or: What's new?. Proc. MFCS 1993.
3. Heunen, C., Kammar, O., Staton, S., Yang, H.: A convenient category for higher-order probability theory. Proc. LICS 2017.
4. Tix, R., Keimel, K., Plotkin, P.: Semantic Domains for Combining Probability and Non-Determinism. Electr. Notes. Theoret. Comput. Sci. 222. 2009.

[⋆] Supported by Royal Society University Research Fellowship.

Effective Dimension of Planar Lines and Fractal Geometry

D. M. Stull[1]

Keywords: Effective dimension · Fractal geometry · Kolmogorov complexity

This talk is concerned with the algorithmic dimension of points on a given line in the Euclidean plane. The most well-studied algorithmic dimensions for a point $x \in \mathbb{R}^n$ are the effective Hausdorff dimension, $dim(x)$, and its dual, the effective packing dimension, $Dim(x)$. In this talk we investigate the (effective) dimension spectra of lines in the Euclidean plane. The dimension spectrum of a line $L_{a,b}$, $sp(L_{a,b})$, with slope a and intercept b is the set

$$sp(L_{a,b}) = \{dim(x, ax + b) \,|\, x \in \mathbb{R}\},$$

i.e., the set of all effective dimensions of the points on $L_{a,b}$. It has been recently shown that, for every a and b with effective dimension less than 1, the dimension spectrum of $L_{a,b}$ contains an interval. Our first main theorem shows that this holds for every line. Moreover, when the effective dimension of a and b is at least 1, $sp(L)$ contains a unit interval. Our second main theorem gives lower bounds on the dimension spectra of lines. In particular, we show that for every $\alpha \in [0, 1]$, with the exception of a set of Hausdorff dimension at most α, the effective dimension of $(x, ax+b)$ is at least $\alpha + \frac{dim(a,b)}{2}$. As a consequence of this theorem, using a recent characterization of Hausdorff dimension using effective dimension, we give a new proof of a result by Molter and Rela on the Hausdorff dimension of Furstenberg sets. We will conclude with examples of lines whose dimension spectrum is interesting. These examples are derived from classical constructions showing upper bounds for Furstenberg sets.

Dual-Pivot Quicksort and Beyond*

Sebastian Wild[1][0000–0002–6061–9177]

Quicksort is one of most well-understood algorithms – both in terms of theoretically performance guarantees and practical running time. An implementation of quicksort is part of almost every programming library. After excessive experimenting and engineering in the 1970s, the tuning efforts seemed to have converged to a stable state; but now, there is again excitement within the algorithms community, triggered by the success of a new dual-pivot quicksort used in the Java 7 runtime library.

I will introduce the new algorithm and present analytical evidence for my hypothesis why (a) dual-pivot quicksort is faster than the previously used (standard) quicksort and (b) why this basic improvement was not already found much earlier. We will then explore the potential of using even more pivots. In passing, I try to give the intuition behind my favorite mathematical tools for the probabilistic analysis of algorithms.

*This work was supported by the Natural Sciences and Engineering Research Council of Canada and the Canada Research Chairs Programme.

Phylomemetics of a Mathematical Folk Tale

Andrew Aberdein

One of the most memorable items of mathematical folklore is Paul Erdős's tale of The Book: a divine book of the best mathematical proofs [1]. However, this narrative exists in multiple versions. The present paper reports on research conducted with a corpus of fifty different versions of the story: five directly sourced to Erdős; the rest recounted by other mathematicians (all but two with Erdős number ≤ 4). Specifically, it applies to this corpus computational techniques devised to work with phylogenetic data in biological systematics, an approach that has come to be called "phylomemetics" [2]. For example, Fig. 1 comprises two neighbour-nets produced by the SplitsTree package [3]. Fig. 1(a) exhibits the relationships across the corpus as a whole. Perhaps unsurprisingly, Erdős's own versions of the narrative are quite tightly clustered (upper right). But several other groupings can be discerned. Fig. 1(b) is derived solely from the adjectives ascribed to Book proofs. (Hence there are fewer distinct narratives, since some use identical sets of adjectives.) The upper right grouping (which includes all of Erdős's versions) contains most narratives in which the Book proofs are characterized as "best", "elegant", or "simple"; the lower left grouping contains most narratives in which the Book proofs are characterized as "beautiful" or "perfect". This comports with earlier empirical work in mathematical aesthetics that suggests that beauty and simplicity do not necessarily coincide; however, it departs from that work in suggesting a clear distinction between beauty and elegance [4, 5, 6]. This and other implications of the corpus for aesthetics of mathematics will be explored.

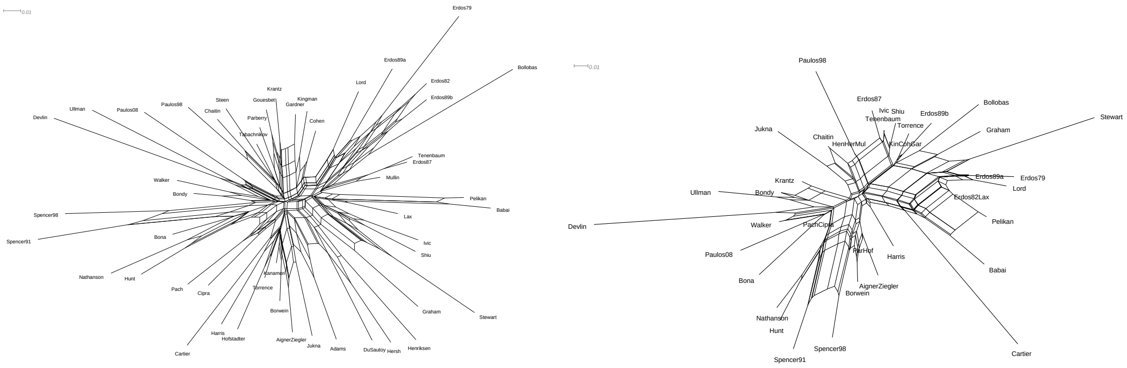

Fig. 1. (a) A neighbour-net constructed from 78 features present or absent in the 50 narratives in the corpus (left); **(b)** A neighbour-net constructed from the 30 distinct adjectives ascribed to Book proofs in 37 distinct combinations (right).

References

1. Aigner, M., Ziegler, G.M.: Proofs from THE BOOK. Springer, Berlin, 5th edn. (2014)
2. Howe, C.J., Windram, H.F.: Phylomemetics—evolutionary analysis beyond the gene. PLoS Biology **9**(5), e1001069 (2011)
3. Huson, D.H., Bryant, D.: Application of phylogenetic networks in evolutionary studies. Molecular Biology and Evolution **23**(2), 254–267 (2005)
4. Inglis, M., Aberdein, A.: Beauty is not simplicity: An analysis of mathematicians' proof appraisals. Philosophia Mathematica **23**(1), 87–109 (2015)
5. Inglis, M., Aberdein, A.: Diversity in proof appraisal. In: Larvor, B. (ed.) Mathematical Cultures: The London Meetings 2012–2014, pp. 163–179. Birkhäuser, Basel (2016)
6. Johnson, S.G., Steinerberger, S.: Intuitions about mathematical beauty: A case study in the aesthetic experience of ideas. Cognition **189**, 242–259 (2019)

Feasibility in Nonstandard Heyting Arithmetic

Péter Battyányi

In this talk, we intend to examine first-order arithmetic together with the axioms for all recursive functions equipped with intuitionistic predicate logic in the background, which is called Heyting arithmetic (HA). It was proved as early as the 1930s by Skolem that, if we augment the theory with the axioms $n < c$ for all natural numbers n, then we get a consistent extension of HA named HA^c. Though no first order formula characterizes in any model exactly the standard natural numbers, it could be interesting to extend arithmetic with a first-order predicate expressing feasibility. Following , we define a feasibility relation F in HA^c by the axioms below:

1. $F(0)$
2. $\forall x \forall y (F(x) \wedge y < x \supset F(y))$
3. $\forall x (F(x) \supset x < c)$
4. $\forall x_1 ... \forall x_n (F(x_1) \wedge ... \wedge F(x_n) \supset F(g(x_1, ..., x_n)))$, for each symbol g standing for a primitive recursive function
5. $A(0) \wedge \forall^f x (A(x) \supset A(Sx)) \supset \forall^f x A(x)$, where $A(x)$ does not contain F and $\forall^f x A(x)$ means $\forall x (F(x) \supset A(x))$.

We preserve only the last axiom as induction scheme for HA^c. The new theory will be referred to as HAF^f. induction scheme with restricted quantifiers. It turns out, however, that the notion of feasibility is not far away from its intended meaning. Reviewing a former presentation given in 2004 [1], the author proves by a reformulation of Kleene's realizability method [3] the following result on the feasibility predicate:

Theorem 1: Let us suppose $HAF^f \vdash F(t)$ for some term t. Then there exists a natural number n, such that $HAF^f \vdash t = \underline{n}$.

That is, if a term is feasible, it is provably equal to a natural number n.

References

1. Battyányi, P.: On some nonstandard extensions of Heyting Arithmetic. In: Proceedings of the 6th International Conference on Applied Informatics Eger, Hungary (2004)
2. Dragalin, A. G.: Explicit algebraic models for constructive and classical theories with non-standard elements. Studia Logica, **55**(1), 33-61 (1995)
3. Kleene, S. C.: Introduction to Metamathematics. North Holand, Amsterdam (1952)
4. Troelstra, A. S., van Dalen, D.: Constructivism in Mathematics. Vol. I.-II., North-Holland (1988)

Weihrauch goes Brouwerian

Vasco Brattka[1,2], *Guido Gherardi*[3]

We prove that the Weihrauch lattice can be transformed into a Brouwer algebra by the consecutive application of two closure operators in the appropriate order: first completion and then parallelization. The closure operator of completion is a new closure operator that we introduce. It transforms any problem into a total problem on the completion of the respective types, where we allow any value outside of the original domain of the problem. This closure operator is of interest by itself, as it generates a total version of Weihrauch reducibility that is defined like the usual version of Weihrauch reducibility, but in terms of total realizers. From a logical perspective completion can be seen as a way to make problems independent of their premises. Alongside with the completion operator and total Weihrauch reducibility we need to study precomplete representations that are required to describe these concepts. In order to show that the parallelized total Weihrauch lattice forms a Brouwer algebra, we introduce a new multiplicative version of an implication. While the parallelized total Weihrauch lattice forms a Brouwer algebra with this implication, the total Weihrauch lattice fails to be a model of intuitionistic linear logic in two different ways. In order to pinpoint the algebraic reasons for this failure, we introduce the concept of a Weihrauch algebra that allows us to formulate the failure in precise and neat terms. Finally, we show that the Medvedev Brouwer algebra can be embedded into our Brouwer algebra, which also implies that the theory of our Brouwer algebra is Jankov logic.

All details can be found in [2], some background information is available in [3, 1].

References

1. Brattka, V., Gherardi, G.: Weihrauch degrees, omniscience principles and weak computability. The Journal of Symbolic Logic **76**(1), 143–176 (2011). https://doi.org/10.2178/jsl/1294170993, http://dx.doi.org/10.2178/jsl/1294170993
2. Brattka, V., Gherardi, G.: Weihrauch goes Brouwerian. arXiv 1809.00380 (2018), https://arxiv.org/abs/1809.00380
3. Brattka, V., Gherardi, G., Pauly, A.: Weihrauch complexity in computable analysis. arXiv 1707.03202 (2017), https://arxiv.org/abs/1707.03202

Novel Ways of Using Quantum Annealing[⋆]

Nicholas Chancellor[1]

Quantum annealing, a technique of computing using physical systems which realize quantum Ising models and used quantum physics to find low energy states, have proven to be applicable to a number of diverse fields. A Canadian company, D-Wave Systems Inc. currently produce quantum annealers with around 2000 qubits. In this presentation, I discuss several experimental results related to techniques on D-Wave devices which go beyond just using them for simple monolithic optimisation algorithms, and discuss several different ways in which physical effects on these devices can be used algorithmically.

Firstly, I discuss how the thermal nature of the output of these devices can be used to perform statistical inference. I review the results of [1] which demonstrate that for a simple classical error correcting code, maximum entropy decoding on a real device can out perform even perfect decoding using the more traditional maximum likelihood method. I then unpublished work on extending to more realistic codes.

Next, I discuss *reverse annealing*, a new technique which allows for a rich variety of hybrid quantum-classical algorithms, and briefly review [2], a paper which pioneered the use of the technique. I then present some unpublished experimental results which demonstrate that reverse annealing does indeed perform the predicted algorithmic task.

Finally, I discuss unpublished experimental work on how reverse annealing can be combined with another advanced feature known as *anneal offsets* to trade off between more optimal solutions and solutions which are more robust to changes in the problem definition.

I conclude with an outlook on the future development of quantum annealing algorithms and techniques.

References

1. Chancellor, N., Szoke, S., Vinci, W., Aeppli, G., Warburton, P.A.: Maximum–entropy inference with a programmable annealer. Scientific Reports **6**(22318) (2016). https://doi.org/doi:10.1038/srep22318
2. Chancellor, N.: Modernizing quantum annealing using local searches. New Journal of Physics **19**(2), 023024 (feb 2017). https://doi.org/10.1088/1367-2630/aa59c4,

[⋆] Portions of the work presented here supported by EPSRC, BP, NASA, and Lockheed Martin

Poincaré, Weyl and a predicative concept of set

Laura Crosilla

In this talk, I discuss a constructive concept of set and analyse its origins in the late Poincaré [2, 3] and in Weyl's "Das Kontinuum" [4]. Predicativity made its appearance at the turn of the 20th century in a remarkable exchange between Poincaré and Russell, prompted by the discovery of the set-theoretic paradoxes. According to a well-known characterisation of predicativity, a definition is impredicative if it defines an entity by reference to (e.g. generalization over) a totality to which the entity itself belongs, and is predicative otherwise. Compliance with predicativity directly affects the concept of set, as it rules out all those sets which can only be defined impredicatively. Substantial technical work has clarified this notion of predicativity, as witnessed by Russell's ramified type theory and an influential proof-theoretic analysis that saw fundamental contributions by Kreisel, Feferman and Schütte.

Predicativity also prominently figures in foundational systems for constructive mathematics such as Martin-Löf type theory. I argue that a different characterisation of predicativity proposed by the late Poincaré [2, 3] better suits the notion of predicativity that we find in constructive type theory. I analyse this second characterisation of predicativity and highlight its relation to Poincaré's criticism of actual infinity. I note similarities with views expressed in Weyl's "Das Kontinuum", which contains a distinctive, precise characterisation of predicativity, without resorting to ramification. At the heart of Weyl's predicative analysis is the delineation of a predicative concept of set as extensions of an arithmetical property. I finally argue that Poincaré and Weyl's concept of predicative set may help clarify important aspects of a contemporary constructive concept of set.

References

1. Martin-Löf, P.: An intuitionistic theory of types: predicative part. In eds. Rose, H. E. and Shepherdson, J. C. *LOGIC COLLOQUIUM 1973*, North–Holland, Amsterdam (1975).
2. Poincaré, H.: La logique de l'infini. Revue de Métaphysique et Morale **17**, 461–482 (1909).
3. Poincaré, H.: La logique de l'infini. Scientia **12**, 1–11 (1912).
4. Weyl, H.: Das Kontinuum. Kritische Untersuchungen über die Grundlagen der Analysis. Veit, Leipzig (1918).

Graph Isomorphism for (H_1, H_2)-free Graphs: An Almost Complete Dichotomy*

Marthe Bonamy[1], *Konrad K. Dabrowski*[2], *Matthew Johnson*[2], *Daniël Paulusma*[2]

The Graph Isomorphism problem, which is that of deciding whether two given graphs are isomorphic, is a central problem in algorithmic graph theory. Babai [1] recently proved that the problem can be solved in quasi-polynomial time, but it is not known if this can be improved to polynomial-time on general graphs.

We consider the Graph Isomorphism problem restricted to classes of graphs characterized by two forbidden induced subgraphs H_1 and H_2. The study of the problem on such classes was initiated by Kratsch and Schweitzer [4]. Later, Schweitzer [5] combined old and new results to settle the computational complexity (polynomial-time solvable or GI-complete) of this problem restricted to (H_1, H_2)-free graphs for all but a finite number of pairs (H_1, H_2), but without explicitly giving the number of open cases. Grohe and Schweitzer [3] proved that Graph Isomorphism is polynomial-time solvable on graph classes of bounded clique-width. By combining previously known results for Graph Isomorphism with known results for boundedness of clique-width, we reduce the number of open cases to 14. By proving a number of new polynomial-time and GI-completeness results, we then further reduce this number to seven.

By exploiting the strong relationship between Graph Isomorphism and clique-width, we simultaneously reduce the number of open cases for boundedness of clique-width for (H_1, H_2)-free graphs to five.

References

1. L. Babai. Graph isomorphism in quasipolynomial time [extended abstract]. *Proc. STOC 2016*, pages 684–697, 2016.
2. M. Bonamy, K.K. Dabrowski, M. Johnson and D. Paulusma Graph Isomorphism for (H_1, H_2)-free Graphs: An Almost Complete Dichotomy *LNCS Proc. WADS 2019*, (to appear)
3. M. Grohe and P. Schweitzer. Isomorphism testing for graphs of bounded rank width. *Proc. FOCS 2015*, pages 1010–1029, 2015.
4. S. Kratsch and P. Schweitzer. Graph isomorphism for graph classes characterized by two forbidden induced subgraphs. *Discrete Applied Mathematics*, 216, Part 1:240–253, 2017.
5. P. Schweitzer. Towards an isomorphism dichotomy for hereditary graph classes. *Theory of Computing Systems*, 61(4):1084–1127, 2017.

*This paper has been accepted for publication in the proceedings of WADS 2019 [2].

Reverse mathematics of a theorem about posets of finite width

Marta Fiori Carones

(Joint work with Alberto Marcone, Paul Shafer and Giovanni Sold).

In 1980 Ivan Rival and Bill Sands [1] proved that for each infinite poset P with finite width (i.e. such that there is a fixed finite bound on the size of antichains in P) there is an infinite chain $C \subseteq P$ such that each vertex of P is comparable to none or to infinitely many vertices of C. We are interested in analysing the strength of this statement, which we denote RS-po, restricted to countable posets, from the viewpoint of reverse mathematics.

Despite the fact that the original proof makes essential use of Π^1_1-CA_0, we give a proof of RS-po which goes through in ACA_0. Moreover, we obtain a sharper result when restricting to partial orders of width three. In fact, we prove that RS-po restricted to partial orders of width three is equivalent to ADS over the base theory RCA_0. ADS is the statement that each countable linear order has an infinite ascending or an infinite descending chain. Very few principles are known to be equivalent to ADS and among them there are no theorems of ordinary mathematics, as far as we know. Thus the equivalence between RS-po restricted to partial orders of width three and ADS is, to the best of our knowledge, an interesting novelty in the field.

We suspect that ADS is also equivalent to RS-po for posets of width n, for each standard $n \geq 3$. However, it is likely that the combinatorial complexity of the proof grows with n. On the other hand, RS-po for posets of width two is strictly weaker than ADS, but not computably true since it implies SADS, which is ADS restricted to posets of order type ω, ω^* or $\omega + \omega^*$.

References

1. Rival, Ivan and Sands, Bill, *On the adjacency of vertices to the vertices of an infinite subgraph*, ***Journal of the London Mathematical Society***, vol. 2 (1980), no. 3, pp. 393–400.

Quantum Random Self-Modifiable Computation

Michael Stephen Fiske[0000−0001−6236−6903]

Among the fundamental questions in computer science, at least two have a deep impact on mathematics. What can computation compute? How many steps does a computation require to solve an instance of the 3-SAT problem? Our work addresses the first question, by introducing a new model called the *ex-machine* [3]. The ex-machine executes Turing machine instructions and two special types of instructions. *Quantum random instructions* are physically realizable with a quantum random number generator [4, 6]. *Meta instructions* can add new states and add new instructions to the ex-machine.

A countable set of ex-machines is constructed, each with a finite number of states and instructions; each ex-machine can compute a Turing incomputable language, whenever the quantum randomness measurements behave like unbiased Bernoulli trials. In 1936, Alan Turing posed the halting problem for Turing machines and proved that this problem is unsolvable for Turing machines. Consider an enumeration $\mathcal{E}_a(i) = (\mathfrak{M}_i, T_i)$ of all Turing machines $\mathfrak{M}_i$ and initial tapes T_i, each containing a finite number of non-blank symbols. Does there exist an ex-machine $\mathfrak{X}$ that has at least one evolutionary path $\mathfrak{X} \to \mathfrak{X}_1 \to \mathfrak{X}_2 \to \dots \to \mathfrak{X}_m$, so at the mth stage ex-machine $\mathfrak{X}_m$ can correctly determine for $0 \le i \le m$ whether $\mathfrak{M}_i$'s execution on tape T_i eventually halts? We construct an ex-machine $\mathfrak{Q}(x)$ that has one such evolutionary halting path.

The existence of this path suggests that David Hilbert [5] may not have been misguided to propose that mathematicians search for finite methods to help construct mathematical proofs. Our refinement is that we cannot use a fixed computer program that behaves according to a fixed set of mechanical rules. We must pursue computational methods that exploit randomness and self-modification [1, 2] so that the complexity of the program can increase as it computes.

References

1. Michael S. Fiske. Turing Incomputable Computation. *Turing-100 Proceedings. Alan Turing Centenary.* EasyChair, **10**, 2012, pp. 66-91.
2. Michael S. Fiske. Quantum Random Active Element Machine. *Unconventional Computation and Natural Computation.* LNCS 7956. Springer, 2013, pp. 252-254.
3. Michael S. Fiske. Quantum Random Self-Modifiable Computation. 2018, pp. 1-50. https://arxiv.org/abs/1807.01369.
4. Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics.* **89**(1), 015004, APS, Feb. 22, 2017.
5. David Hilbert. Mathematische Probleme. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematische-Physikalische Klasse.* **3**, 1900, pp. 253-297.
6. A. Kulikov, M. Jerger, A. Potočnik, A. Wallraff, and A. Fedorov. Realization of a Quantum Random Generator Certified with the Kochen-Specker Theorem. *Physical Review Letter.* **119**, 240501, Dec. 11, 2017.

Computable type of certain polyhedra[⋆]

Zvonko Iljazović

A compact subset S of Euclidean space $\mathbb{R}^n$ is computable if S can be effectively approximated by finitely many rational points with any given precision. More general than computable are semicomputable sets: a compact set $S \subseteq \mathbb{R}^n$ is semicomputable if $S = f^{-1}(\{0\})$ for some computable function $f : \mathbb{R}^n \to \mathbb{R}$.

In general, a semicomputable set need not be computable. However, under certain conditions semicomputability of a set implies its computability. It turns out that topology plays an important role in this regard.

The notions of a semicomputable and a computable set can be naturally defined in a computable topological space and the general question is: under what conditions a semicomputable set in a computable topological space is computable?

If $\varDelta$ is a topological space and $\varSigma$ is a subspace of $\varDelta$, we say that the pair $(\varDelta, \varSigma)$ has computable type if the following holds: whenever X is a computable topological space and $f : \varDelta \to X$ a topological embedding such that $f(\varDelta)$ and $f(\varSigma)$ are semicomputable in X, then $f(\varDelta)$ is computable in X. We say that a topological space $\varDelta$ has computable type if the pair $(\varDelta, \emptyset)$ has computable type. For example, $[0, 1]$ does not have computable type, but $([0, 1], \{0, 1\})$ has computable type. On the other hand, the unit circle in the plane has computable type and in fact any sphere in $\mathbb{R}^n$ has computable type. More generally, if M is a compact manifold with boundary, then $(M, \partial M)$ has computable type. Furthermore, if G is a topological graph and E the set of its endpoints, then (G, E) has computable type.

We consider topological spaces P which have topological type of a polyhedron and we examine under what conditions P or (P, E) has computable type, where E is some subspace of P. We prove the following: P has computable type if P is the wedge of two spheres, i.e. $P = S_1 \wedge S_2$, where S_1 is a sphere in $\mathbb{R}^n$ and S_2 is a sphere in $\mathbb{R}^m$.

If $\varDelta_1$ and $\varDelta_2$ are topological spaces which have computable type, does $\varDelta_1 \times \varDelta_2$ have computable type? A more general question is: if $(\varDelta_1, \varSigma_1)$ and $(\varDelta_2, \varSigma_2)$ have computable types, does $(\varDelta_1 \times \varDelta_2, \varDelta_1 \times \varSigma_2 \cup \varSigma_1 \times \varDelta_2)$ have computable type? We prove that the the answer to the latter question is affirmative in the following case: $\varDelta_1$ is a triode, $\varSigma_1$ is the set of all endpoints of $\varDelta_1$, $\varDelta_2 = [0, 1]$ and $\varSigma_2 = \{0, 1\}$.

[⋆] Supported by the Croatian Science Foundation under project 7459 CompStruct

Formalizing Probabilistic Quantum Security Protocols in the Isabelle Infrastructure Framework*

Florian Kammüller[1,2][0000−0001−5839−5488]

3 Extended Abstract

In this informal talk, we present a first step towards a formalisation of the Quantum Key Distribution (QKD) algorithm in Isabelle. We focus on the formalisation of the main probabilistic argument why Bob cannot be certain about the key bit sent by Alice before he doesn't have the chance to compare the chosen polarization scheme. This means that any adversary Eve is in the same position as Bob and cannot be certain about the transmitted keybits.

We formalise the necessary basic probability theory in the Isabelle Infrastructure framework, present a graphical depiction of the protocol steps and their probabilities, and finally how this is translated into a formal proof of the security argument. A more detailed description of this formalisation experiment is available [3].

The motivation for this simple experiment is to find the minimum requirements for expressing probabilistic properties for security protocols in the Isabelle Infrastructure framework. This framework, built in the interactive theorem prover Isabelle, supports the proof of Security and Privacy properties for IoT system specifications including actors and policies. It formalises a generic notion of state transitions over Kripke structures. The temporal logic CTL is used to provide a formal semantics of Attack Trees [1]. A stepwise formal refinement process interleaves risk analysis with attack trees with property preserving refinement steps. This is illustrated on an IoT healthcare application from the context of the SUCCESS project [2].

The application to the QKD protocol serves as a requirements analysis to understand to what extent probabilistic temporal reasoning needs to be added to the Isabelle Infrastructure framework to enable probabilistic arguments for security protocols. Adding probabilistic features onto this logical framework with actors, their environment, and policies over those within the logical model promises to enable proofs of less abstract Quantum security properties that are closer to physical implementations.

References

1. Kammüller, F.: Attack trees in isabelle. In: 20th International Conference on Information and Communications Security, ICICS2018. LNCS, vol. 11149. Springer (2018)
2. Kammüller, F.: Combining secure system design with risk assessment for iot healthcare systems. In: Workshop on Security, Privacy, and Trust in the IoT, SPTIoT19, colocated with IEEE PerCom. IEEE (2019)
3. Kammüller, F.: Qkd in isabelle bayesian calculation. CoRR **submit/2673210** (2019), `https://arxiv.org`

*Supported by CHIST-ERA project102112

Continuous-time quantum computing[⋆]

Viv Kendon[0000−0002−6551−3056]

Until recently, computation by continuous-time quantum walk (QW) [1], adiabatic quantum computing (AQC) [2], and special purpose quantum simulators have been treated as different approaches to quantum computing. While quantum annealing [3, 4] is related to adiabatic quantum computing, it is also distinct in how it harnesses open quantum system effects. All except some special purpose quantum simulators are universal for quantum computation, in the sense that they can be mapped to the circuit model of quantum computing with at most a polynomial overhead in resources [5]. However, they all share a key feature: evolving the initial quantum state to the final quantum state using a continuous-time process. This is a natural way to compute with quantum systems.

In the setting of the quantum search algorithm, interpolating between AQC and QW computation [6] provides a family of continuous-time quantum algorithms. While QW is optimal under ideal conditions for large systems, hybrid strategies are better for certain types of noise and problem misspecification. The structure of correlations can be exploited by choosing the encoding to match, providing further advantages [7] for realistic problems.

Continuous-time quantum computing is a realistic short- to medium-term goal that is applicable to a wide range of hardware and problem types. Quantum annealing is already known to be well-suited to a very wide range of optimisation and sampling problems of importance to industry and commerce, especially finance, big data, scheduling, and networks. Any particular physical implementation of continuous-time quantum computing will have its own strengths, making it more suitable for particular types of problems. Special-purpose quantum simulation hardware already under development will likely be able to solve other problems, and thus be significantly more useful than originally envisaged. This suggests that the benefits of following multiple hardware paths will be fruitful in many directions, rather than needing to pick one winner from the pack.

References

1. E Farhi and S Gutmann. *Phys. Rev. A*, 58:915–928, 1998.
2. E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser. Arχiv:quant-ph/0001106.
3. A. B. Finilla, et al, *Chem. Phys. Lett.*, 219:343, 1994.
4. T. Kadowaki & H. Nishimori. *Phys. Rev. E*, 58:5355, 1998.
5. Andrew M. Childs. *Phys. Rev. Lett.*, 102:180501, 2009.
6. J. G. Morley, N. Chancellor, S. Bose, and V. Kendon. *Phys. Rev. A*, 99:022339, 2019. Arχiv:1709.00371.
7. A. Callison, N. Chancellor, F. Mintert, and V. Kendon. Arχiv:1903.05003.

[⋆] Supported by UK EPSRC Fellowship EP/L022303/1.

Is Brownian Motion Computable?[⋆]

Hyunwoo Lee, Sewon Park, Martin Ziegler

1D *Brownian Motion* (aka Wiener Process) is a probability distribution on the space $\mathcal{C}[0;1]$ of continuous functions $f:[0;1]\to\mathbb{R}$ with $f(0)=0$. Although the pointwise and correlated distibution of $\big(f(t_1),\ldots f(t_N)\big)$ at any finite choice of arguments $0<t_1<\ldots<t_N$ is just a multivariate Gaussian distribution [Gal16, Corollary 2.4], the question of whether f itself is computable remains open [DF13]. Recall the Wiener and Donsker and Lévy representation $f(t)\ =$

$$=\ \xi_0\cdot t+\sqrt{2}\sum_n \xi_n\sin(n\pi t)/(n\pi)\ =\ \lim_N\sum_{n\le Nt}\xi_n/\sqrt{N}\ =\ \sum_N\sum_{n=0}^{2^N-1}\xi_{n+2^N}h_{N,n}(t)$$

with independent standard normally distributed random variables ξ_n and 'hat' functions $h_{N,n}$ of height $2^{-N/2}$ and support $\big[n/2^N;(n+1)/2^N\big]$: none of the limits converges uniformly with probability 1, hence fail to yield the required *computable* continuity [Grz57]. The reader may try to spot and fill the gap in the proof sketch of [Col15, Theorem 58]; and avoid confusing computing a random function with probabilistically computing a function [Bos08, BGH15]. We discuss several approaches to settingly the conjecture positively, and for each point out the corresponding key property to prove.

References

[BGH15] Vasco Brattka, Guido Gherardi, and Rupert Hölzl. Probabilistic computability and choice. *Information and Computation*, 242:249–286, 2015.

[Bos08] Volker Bosserhoff. Notions of probabilistic computability on represented spaces. In Ruth Dillhage, Tanja Grubba, Andrea Sorbi, Klaus Weihrauch, and Ning Zhong, editors, *Proceedings of the Fourth International Conference on Computability and Complexity in Analysis (CCA 2007)*, volume 202 of *Electronic Notes in Theoretical Computer Science*, pages 137–170. Elsevier, 2008. CCA 2007, Siena, Italy, June 16–18, 2007.

[Col15] Pieter Collins. Computable stochastic processes. *arXiv*, 1409.4667v2, 2015.

[DF13] George Davie and Willem L. Fouché. On the computability of a construction of Brownian motion. *Mathematical Structures in Computer Science*, 23:1257–1265, 12 2013.

[Gal16] Jean-François Le Gall. *Brownian Motion, Martingales, and Stochastic Calculus*, volume 274 of *GTM.* Springer, 2016.

[Grz57] Andrzej Grzegorczyk. On the definitions of computable real continuous functions. *Fundamenta Mathematicae*, 44:61–71, 1957.

[⋆] Supported by the National Research Foundation of Korea (grant NRF-2017R1E1A1A03071032) and the International Research & Development Program of the Korean Ministry of Science and ICT (grant NRF-2016K1A3A7A03950702).

Graph and String Parameters: Connections Between Pathwidth, Cutwidth and the Locality Number

K. Casel[1], *J. Day*[2], *P. Fleischmann*[3], *T. Kociumaka*[4], *F. Manea*[3], *and M. Schmid*[5]

Abstract. We investigate the locality number, a recently introduced structural parameter for strings (with applications in pattern matching with variables), and its connection to two important graph-parameters, cutwidth and pathwidth. These connections allow us to show that computing the locality number is NP-hard but fixed parameter tractable (when the locality number or the alphabet size is treated as a parameter), and can be approximated with ratio $O(\sqrt{\log \mathrm{opt}} \log n)$. As a by-product, we also relate cutwidth via the locality number to pathwidth, which is of independent interest, since it improves the currently best known approximation algorithm for cutwidth. In addition to these main results, we also consider the possibility of greedy-based approximation algorithms for the locality number.
The paper on which this presentation is based will appear in the proceedings of ICALP 2019, and it is available on Arxiv [1].

References

1. Katrin Casel, Joel D. Day, Pamela Fleischmann, Tomasz Kociumaka, Florin Manea, and Markus L. Schmid. Graph and string parameters: Connections between pathwidth, cutwidth and the locality number. *CoRR*, abs/1902.10983, 2019.

Luzin's (N) and randomness reflection

Arno Pauly[1][0000−0002−0173−3295], *Linda Brown Westrick*[2], *Liang Yu*[3]

We consider some notions and results from classic analysis (along the line of Saks [4]) in the light of (higher) randomness. Specifically, we are exploring Luzin's (N) property:

Definition 1. *A function $f : \mathbb{R} \to \mathbb{R}$ has Luzin's (N), if for every null set A also $f[A]$ is null.*

It is well-known that effectivization of results from analysis replaces *null set* with some form of *non-random point*. This could be taken as *definition* of what a randomness notion is – but it is remarkable that a few specific randomness notions appear over and over. Usually, these are randomness notions from lower levels. Here, however, a higher randomness notion appears. Our main result is:

Theorem 5. *For an effectively Borel measurable $f : \mathbb{R} \to \mathbb{R}$ the following are equivalent:*

1. *f has Luzin's (N)*
2. *If $f(x)$ is $\Delta^1_1(\mathcal{O})$-random, then so is x.*

Our proof involves obtaining a higher randomness analogue to results from [3], and invokes Martin's solution to Friedman's conjecture. As a consequence of the proof we obtain an effective strengthening of a result by Banach that if a function has Luzin's (N), then almost all its fibers are countable.

By drawing on results from [2] and [1], we can show that replacing $\Delta^1_1(\mathcal{O})$-random with various other randomness notions makes the theorem fail. A notable exception to this is Δ^1_1-randomness – whether reflecting Δ^1_1-randomness is equivalent to Luzin's (N) is left as an open question.

References

1. Bienvenu, L., Merkle, W.: Constructive equivalence relations on computable probability measures. Annals of Pure and Applied Logic **160**(3), 238 – 254 (2009). https://doi.org/j.apal.2009.01.002, http://www.sciencedirect.com/science/article/pii/S0168007209000050, computation and Logic in the Real World: CiE 2007
2. Holický, P., Ponomarev, S.P., Zajj́ček, L., Zelený, M.: Structure of the set of continuous functions with Luzins's property (N). Real Analysis Exchange **24**(2), 635–656 (1998), http://www.jstor.org/stable/44152986
3. Miller, J.S., Yu, L.: On initial segment complexity and degrees of randomness. Transactions of the AMS **360**, 3193–3210 (2008). https://doi.org/10.1090/S0002-9947-08-04395-X
4. Saks, S.: Hafner Publishing Company. Theory of the Integral (1937)

Acknowledgement

We are grateful to the organizers of the Oberwolfach Seminar 1802 *Computability Theory*, during which the inception of the presented work took place.

Push and pull protocols on finite graphs[*]

András Pongrácz[0000−0002−2771−8974]

Voting protocols, such as the push and the pull protocol, are designed to model the behavior of people during an election. These processes are also used to study social models of interaction, distributed computing in peer-to-peer networks, and to describe how viruses or rumors spread in a community.

Given a finite connected graph $G = (V, E)$ and a function $f : V \to \{0, 1\}$ (which represents the opinion of the vertices), the standard push protocol works as follows. We pick a vertex u uniformly at random, and then we choose one of its neighbors v uniformly at random, and change the opinion of v to $f(u)$. In order to avoid idle rounds, the discordant version of this protocol was defined: in that case, the vertex v is chosen randomly among those neighbors of u whose opinion differ from $f(u)$. The process halts when all vertices have the same opinion, i.e., f is constant. It is well-known that such a consensus is reached in a finite number of rounds with probability 1, and in fact the expected value of the runtime is finite.

We provide an asymptotic formula for the expected runtime of such protocols on cycle graphs and paths, and the probability for each consensus to win in the end, in terms of the initial opinion of the vertices. It was shown that the expected runtime is $\beta\rho + O(n^{3/2})$, where $n = |V|$, and β and ρ are the number of vertices with opinions 0 and 1, respectively. This expected runtime is quadratic in n at worst. If the initial state is not too complex, then the probability of each opinion to win is close to the proportion of vertices with that opinion in the initial state.

The method can be used to estimate the expected runtime of joint Drunkard walks on cycle graphs and paths, as well. The expected runtime on star graphs is also discussed in the talk.

Finally, we analyse the continuous variant of these processes where the opinion is a function $f : V \to [0, 1]$, and obtain that the possible outcome of the election is a fractal on the unit interval.

[*] The author has been supported by the EFOP-3.6.2-16-2017-00015 project, which has been supported by the European Union, co-financed by the European Social Fund, by the National Research, Development and Innovation Fund of Hungary, financed under the FK 124814 and PD 125160 funding schemes, the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, and by the ÚNKP-18-4 New National Excellence Program of the Ministry of Human Capacities.

The complexity of non-trivial homomorphisms between torsion-free abelian groups

Meng Che Ho, Dino Rossegger, Luca San Mauro

We investigate the complexity of homomorphisms between computable torsion free abelian groups. We define the *homomorphism spectrum* of computable (torsion-free abelian) groups G_1 and G_2 to be the set of Turing degrees computing non-trivial homomorphisms between all computable copies of G_1 and G_2. More formally, given G_1 and G_2, let I and J be their respective index sets. Then the homomorphism spectrum of G_1 and G_2 is

$$Sp(G_1, G_2) = \bigcap_{(H_1,H_2)\in I\times J} \{deg(X) : \exists f : H_1 \to H_2 \; ker(f) \neq H_1 \,\&\, X \geq_T f\}.$$

If $Sp(G_1, G_2)$ contains a least degree $\mathbf{d}$, we call $\mathbf{d}$ the *degree of homomorphism* of G_1 and G_2. We investigate the structure of homomorphism spectra. Our main results are as follows.

Theorem 6. *Every degree of homomorphism is hyperarithmetic.*

Theorem 7. *Every homomorphism spectrum contains either all degrees or is meagre.*

Theorem 8. *There are computable torsion-free abelian groups G_1, G_2 with $Sp(G_1, G_2) \cap \mathbf{HYP} = \emptyset$.*

Theorem 9. *For every computable $\alpha \geq 2$, $\mathbf{0}^{(\alpha)}$ is a degree of homomorphism of torsion-free abelian groups.*

Punctual equivalence relations and their punctual complexity

Luca San Mauro

This is joint work with N. Bazhenov and A. Sorbi.

The complexity of equivalence relations received much attention in the recent literature. The main tool for such endeavour is the following reducibility: given equivalence relations R and S on ω, R is *computably reducible* to S if there is a computable function $f : \omega \to \omega$ that injectively maps R-classes to S-classes. The study of c-degrees is by now fairly developed (see, e.g., [1]).

In order to compare the complexity of equivalence relations which are computable, researchers considered also feasible variants of computable reducibility, such as the *polynomial-time reducibility* investigated in [2].

In this work, we explore **Peq**, the degree structure generated by *primitive recursive reducibility* on *punctual* equivalence relations (i.e., primitive recursive equivalence relations with domain ω).

We characterize **Peq**. In contrast with all other known degree structures on equivalence relations – and to our surprise – **Peq** has much structure, being a dense distributive lattice.

References

1. U. Andrews, A. Sorbi, *Joins and meets in the structure of Ceers*, forthcoming in ***Computability***
2. S. Gao, C. Ziegler, *On Polynomial-Time Relation Reducibility*, ***Notre Dame Journal of Formal Logic***, 58(2):271–285, 2017

Looking for trees in phylogenetic networks

Charles Semple

Phylogenetic networks are a particular type of rooted, acyclic digraph and are used in computational biology to represent the non-treelike evolutionary history of extant species. Non-treelike processes in evolution include lateral gene transfer and hybridisation. Although evolution is not necessarily treelike at the species-level, at the level of genes, we typically assume treelike evolution. Thus phylogenetic networks are often viewed as an amalgamation of gene trees (phylogenetic trees representing the evolutionary history of single genes). From this viewpoint, one of the most well-studied computational problems concerning phylogenetic networks is that of deciding whether or not a network embeds a given tree. In this talk, I will describe this problem, variations of it, and some recent results.

The open and clopen Ramsey theorems in the Weihrauch lattice

Manlio Valenti[1]

Recently [1] studied the strength, from the point of view of Weihrauch reducibility, of different principles (comparability of well-orderings, perfect tree theorem, open determinacy on Baire space) that are known to be equivalent to ATR_0. We are now considering the strength of the open and clopen Ramsey theorems (which are special cases of the Galvin-Prikry theorem). The open Ramsey theorem says that the open subsets of the space $[\mathbb{N}]^{\mathbb{N}}$ are Ramsey, i.e. for each open set P

$$(\exists H \in [\mathbb{N}]^{\mathbb{N}})\,([H]^{\mathbb{N}} \subset P \vee [H]^{\mathbb{N}} \cap P = \emptyset)$$

We say that a homogeneous solution H lands in P if $[H]^{\mathbb{N}} \subset P$, and we say that H avoids P if $[H]^{\mathbb{N}} \cap P = \emptyset$. The clopen Ramsey theorem is the restriction of the open Ramsey theorem to clopen sets. They are both known to be equivalent to ATR_0. Notice that the existence of a homogeneous solution that lands in the set does not prevent the existence of another solution that avoids it. This is not the case with open determinacy and the perfect tree theorem, where only one of the alternatives can hold. There are several (non-equivalent) ways of extracting multivalued functions from these principles. For the open Ramsey theorem we can distinguish between five versions:

weak versions: given an open set with no solutions that avoid it (resp. land in it), find a solution that lands in it (resp. avoids it);

strong versions: given an open set with some solution that lands in it (resp. avoids it), find a solution that lands in it (resp. avoids it);

full version: given an open set, find a homogeneous solution for it (which may either land in it or avoid it).

The same multivalued functions can be defined for the clopen Ramsey theorem. Not all of these formulations are equivalent from the point of view of Weihrauch reducibility. We establish their relative strength and compare them with the (multivalued) functions studied in [1], including $\mathsf{C}_{\mathbb{N}}^{\mathbb{N}}$ and $\mathsf{UC}_{\mathbb{N}}^{\mathbb{N}}$ (resp. choice and unique choice on the Baire space).

This is joint work with Alberto Marcone.

References

1. Kihara, T., Marcone, A., Pauly, A.: Searching for an analogue of ATR_0 in the Weihrauch lattice. Submitted. https://arxiv.org/abs/1812.01549 (2018)

First steps towards computable frame theory

Arno Pauly[1][0000−0002−0173−3295], *Zhifeng Matthew Ye*[1]

A *frame* abstracts from the structure of open sets of a topological space, it is a distributive lattice with arbitrary joins and finite meets. In the field of point-free topology, it was demonstrated that much of topology can be carried out without invoking spaces of points at all, and only working with frames and frame-homomorphisms.

From the perspective of synthetic topology [4], the definition of a frame is not quite right, though. Instead of finite meets and arbitrary joins, we should be asking for compact meets and overt joins. We could then carry out frame theory internally to whatever cartesian closed category we were already working in. In this level of generality, even defining what we want a frame to be is not without challenge. If we restrict to quasi-Polish spaces [1], we could use results by de Brecht and Kawai [2] to overcome these challenges. Working in domain theory, several related results were obtained in [7].

Our goal is, however, to work in the category of represented spaces [5]. A sufficiently abstract approach should let us replace *compact* and *overt* by their counterparts relativized to some endofunctor, and thereby obtain generalizations of spaces of pointclasses (along the lines of [6, 3]). Here, however, we will present the first steps along this journey.

References

1. de Brecht, M.: Quasi-Polish spaces. Annals of Pure and Applied Logic **164**(3), 354–381 (2013)
2. de Brecht, M., Kawai, T.: On the commutativity of the powerspace constructions. arXiv 1709.06226 (2017)
3. de Brecht, M., Pauly, A.: Noetherian Quasi-Polish spaces. In: Goranko, V., Dam, M. (eds.) 26th EACSL Annual Conference on Computer Science Logic (CSL 2017). LIPIcs, vol. 82, pp. 16:1–16:17. Schloss Dagstuhl (2017). https://doi.org/10.4230/LIPIcs.CSL.2017.16, http://drops.dagstuhl.de/opus/volltexte/2017/7698
4. Escardó, M.: Synthetic topology of datatypes and classical spaces. Electronic Notes in Theoretical Computer Science **87** (2004)
5. Pauly, A.: On the topological aspects of the theory of represented spaces. Computability **5**(2), 159–180 (2016). https://doi.org/10.3233/COM-150049, http://arxiv.org/abs/1204.3763
6. Pauly, A., de Brecht, M.: Descriptive set theory in the category of represented spaces. In: 30th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). pp. 438–449 (2015). https://doi.org/10.1109/LICS.2015.48
7. Schalk, A.: Algebras for Generalized Power Constructions. Ph.D. thesis, TU Darmstadt (1993)

Acknowledgement

We are grateful to Matthew de Brecht for inspiring discussion and helpful comments.

Finitary infinite pigeonhole principle and Ramsey's theorem in reverse mathematics

Keita Yokoyama[⋆]

Terrence Tao's finitary infinite pigeonhole principle and its variants are studied in the context of reverse mathematics by Gaspar and Kohlenbach [1]. Pelupessy [2] generalize this principle to infinite Ramsey's theorem. In this talk, we answer the question on the "faithful finitization" of infinite pigeonhole principle posed in [1] and study the strength of related principles.

References

1. Jaime Gaspar and Ulrich Kohlenbach. On Tao's "finitary" infinite pigeonhole principle. *J. Symbolic Logic*, 75(1):355–371, 2010.
2. Florian Pelupessy. On "finitary" ramsey's theorem, 2015. Available at https://arxiv.org/abs/1508.02013.

[⋆] This work is partially supported by JSPS KAKENHI (grant numbers 19K03601 and 15H03634) and JSPS Core-to-Core Program (A. Advanced Research Networks).

Inverse Lyndon words and Inverse Lyndon factorizations of words

Paola Bonizzoni[1], *C. De Felice*[2], *R. Zaccagnino*[2], *R. Zizza*[2]

Abstract

Lyndon words were introduced as *standard lexicographic sequences*, and then used in the context of the free groups. A Lyndon word is a word which is strictly smaller than each of its proper cyclic shifts for the lexicographical ordering. A famous theorem concerning Lyndon words asserts that any nonempty word factorizes uniquely into a nonincreasing product of Lyndon words, called its Lyndon factorization. This theorem provides an example of a factorization of a free monoid. There are several results which give relations between Lyndon words, codes and combinatorics of words. More recently these words found a renewed theoretical interest and several variants of them have been studied and related to the combinatorial and algorithmic properties of *necklaces*, that are powers of Lyndon words, and their prefixes or *prenecklaces*. The Lyndon factorization has recently revealed to be a useful tool also in string processing algorithms, that has not been completely explored and understood. This is due also to the fact that it can be efficiently computed. In [1] we introduce variants of the Lyndon factorization, called inverse Lyndon factorizations. Their factors, named inverse Lyndon words, are in a class that strictly contains anti-Lyndon words, that is Lyndon words with respect to the inverse lexicographic order. A word w may have several inverse Lyndon factorizations, but we prove that any nonempty word w admits a canonical inverse Lyndon factorization, named ICFL(w), that maintains the main properties of the Lyndon factorization of w: it can be computed in linear time, it is uniquely determined, and it preserves a compatibility property for sorting suffixes. In particular, the compatibility property of ICFL(w) is a consequence of another result: any factor in ICFL(w) is a concatenation of consecutive factors of the Lyndon factorization of w with respect to the inverse lexicographic order.

References

1. P. Bonizzoni, C. De Felice, R. Zaccagnino, R. Zizza, Inverse Lyndon words and Inverse Lyndon factorizations of words, Advances in Applied Mathematics, 101, pp. 281-319.