CCC 2017
Continuity, Computability, Constructivity - From Logic to Algorithms

Inria – LORIA, Nancy

26-30 June 2017

Abstracts

On the commutativity of the powerspace monads [⋆]

Matthew de Brecht

Graduate School of Human and Environmental Studies
Kyoto University, Japan
matthew@i.h.kyoto-u.ac.jp

We present results concerning the upper and lower powerspace monads on the category of topological spaces. In particular, we show that the monads commute on a certain class of topological spaces, which includes all quasi-Polish spaces. We will also discuss how this relates with the upper and lower powerlocales. (This is based on joint work with Tatsuji Kawai).

[⋆] This work was supported by JSPS Core-to-Core Program, A. Advanced Research Networks and by JSPS KAKENHI Grant Number 15K15940.

Hybrid Semantics for Higher-Order Store

Bernhard Reus

University of Sussex
bernhard@sussex.ac.uk

Proving soundness of type systems or program logics gets rather involved when the programming language in question uses code pointers. In this case one also uses the terms *general references* and *higher-order store*, respectively. The dynamic allocation of memory cells can be modelled elegantly by Kripke semantics, which unfortunately gets contaminated by mixed-variant recursive definitions required to model higher-order stores. This recursion is a consequence of the fact that a store can contain programs which are in turn store transformers.

Reasoning about such recursive structures in the context of Kripke models is difficult as properties of high-order store are necessarily also to be defined by recursion. The challenge is to come up with well-defined definitions that also give rise to useful reasoning principles.

The issues involved will be demonstrated using a logic for imperative programs based on *Separation Logic* which is a Hoare-style logic introduced by Reynolds and OHearn that allows one to express the absence of aliasing and to specify *memory footprints* of programs. This permits local reasoning w.r.t. heaps. To deal with the complex recursive definitions mentioned above, complete ultrametric spaces, step-indexing, or a *hybrid* (mixed) version of both can be employed. It will be explained why the hybrid approach turned out to be particularly well suited for the program logic devised.

Many of the findings presented are the result of a collaboration with Lars Birkedal, François Pottier, Jan Schwinghammer, Hongseok Yang and others.

Point-free Descriptive Set Theory and Algorithmic Randomness

Alex Simpson

University of Ljubljana, Slovenia

I shall report on an ongoing programme of work, whose further development is part of the RISE Computing with Infinite Data project. Some of the initial results have been obtained in joint work with Antonin Delpeuch (University of Oxford).

It is possible to give a simple point-free treatment of the Borel hierarchy from descriptive set theory. This supports, for example, point-free formulations of results related to category and measure. From a classical perspective, such results mainly amount to a reformulation of standard theory. Nevertheless, the point-free treatment has the added benefit of amenability to a constructive development. Not only does this allow the computational content of theorems to be extracted, but, perhaps more interestingly, the constructive theory also opens up the possibility of a novel approach to algorithmic randomness.

Sequentially locally convex QCB-spaces and Complexity Theory

Matthias Schröder

TU Darmstadt, Germany

We study sequentially locally convex QCB-spaces. They are defined as vector spaces which carry a QCB-topology such that the convergence relation is induced by a family of seminorms. Moreover we discuss Co-Polish spaces and their role in Type-2 Complexity Theory. Co-Polish Hausdorff spaces allow for a *Simple Complexity Theory* in the sense that one can measure time complexity in terms of a *discrete* (rather than a continuous) parameter on the input and the desired output precision. The duals of separable metrisable locally convex spaces formed in the category QCB turn out to be sequentially locally convex Co-Polish spaces.

Concurrent program extraction

Ulrich Berger[1] and Hideki Tsuiki[2]

[1] Department of Computer Science, Swansea University
[2] Graduate School of Human and Environmental Studies, Kyoto University

In constructive logic and mathematics the meaning of a proposition is defined by describing how to prove it, that is, how to construct evidence for it. This is called the Brouwer-Heyting-Kolmogorov interpretation. For example,

- evidence for a conjunction, $A \wedge B$, is a pair (d, e) where d is evidence for A and e is evidence for B,
- evidence for a disjunction, $A \vee B$, is a pair (i, d) where i is 0 or 1 such that if $i = 0$ then d is evidence for A and if $i = 1$ then d is evidence for B,
- evidence for an implication, $A \to B$, is a computable procedure that transforms evidence for A into evidence for B.

Formalising this interpretation of propositions and the corresponding constructive proof rules leads to a method of program extraction from constructive proofs: From every constructive proof of a formula one can extract a program that computes evidence for it. The extracted programs are functional and possibly higher-order and can be conveniently coded in programming languages such as ML, Haskell or Scheme.

If one attempts to develop program extraction into a method of synthesising 'correct-by-construction' software, one realizes that one misses out an indispensable element of modern programming: *Concurrency*, that is, the composition of independently executing computations.

Our work is an attempt to fill this gap. We present an extension of constructive logic by a new formula construct $\mathbf{S}_n(A)$ with the following BHK interpretation:

- Evidence for $\mathbf{S}_n(A)$ is tuple of at most n computations running concurrently, at least one of which terminates, and each of which, if it terminates, computes evidence for A.

It turns out that the operator $\mathbf{S}_n$ becomes useful only in conjunction with a strong form of implication, $A \,\|\, B$, to be read 'A restricted to B'. The BHK interpretation of restriction is as follows:

- Evidence for $A \,\|\, B$ is a computation a such that
  - if there is evidence for B, then a terminates;
  - if a terminates, then it does so with a result that provides evidence for A.

We present proof rules for $\mathbf{S}_n(A)$ and $A \,\|\, B$ and give examples of proofs that give rise to concurrent extracted programs. Somewhat surprisingly, the two operators validate a concurrent version of the Law of Excluded Middle,

$$\frac{A \,\|\, B \quad A \,\|\, \neg B}{\mathbf{S}_2(A)}$$

Indeed, assuming evidence a for $A \parallel B$ and b for $A \parallel \neg B$, one obtains evidence for $\mathbf{S}_2(A)$ by executing a and b concurrently.

The first example of a proof with concurrent computational content is concerned with infinite Gray code, an extension of the well-known Gray code for integers to a representation of the real numbers, introduced by Tsuiki [3]. One can prove that the (coinductive) predicate characterising this representation implies a concurrent version of the predicate characterising the signed digit representation and extract from this a concurrent program that translates infinite Gray code into signed digit representation. The extracted program is the same as the one given in [3].

The second example is about finding in a non-zero vector of real numbers an entry that is apart from zero. A concurrent program solving this problem can be extracted from a proof in the new logic. This can be further used to prove the invertibility of non-singular quadratic matrices and hence to extract a program for matrix inversion using a concurrent version of Gaussian elimination.

Currently, program extraction in this extended logic is done informally and the extracted programs are implemented in a concurrent extension of Haskell. It is future work to integrate the concurrent proof rules in a suitable interactive proof system (for example, Minlog) and to implement the corresponding program extraction procedure to make it fully automatic.

Prior to this work, a (non-concurrent) program translating an intensional version of infinite Gray code into signed digit representation has been extracted from a proof implemented in the Minlog system [1]. A precursor of our logical system is presented in [2]. It allows for the extraction of non-determinism and concurrent programs, however, without control over the number of threads, that is, processes running concurrently at the same time.

Acknowledgements

This work was supported by the International Research Staff Exchange Scheme (IRSES) Nr. 612638 CORCON and Nr. 294962 COMPUTAL of the European Commission, the JSPS Core-to-Core Program, A. Advanced Research Networks and JSPS KAKENHI Grant Number 15K00015.

The latest results were obtained while the authors were visiting the University of Canterbury, Christchurch, New Zealand, in April 2017. We are grateful to Douglas Bridges and Hannes Diener and the Mathematics Department of UC for hosting our visits which were part of the CORCON project.

References

1. U. Berger, K. Miyamoto, H. Schwichtenberg, and H. Tsuiki. Logic for Gray-code computation. In *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, Ontos Mathematical Logic 6. de Gruyter, 2016.
2. Ulrich Berger. Extracting Non-Deterministic Concurrent Programs. In *CSL 2016*, volume 62 of *LIPIcs*, pages 26:1–26:21, 2016.
3. H. Tsuiki. Real Number Computation through Gray Code Embedding. *Theoretical Computer Science*, 284(2):467–485, 2002.

ERA: Applications, Analysis and Improvements [⋆]

Franz Brauße[1], Margarita Korovina[2], and Norbert Müller[1]

[1] Abteilung Informatikwissenschaften, Universität Trier, Germany
[2] A.P. Ershov Institute of Informatics Systems, Novosibirsk, Russia

In a cooperation between Trier and Novosibirsk, we are working in several directions within the framework of exact real arithmetic (ERA). We report on work in progress aiming at further cooperations, in particular with participants of the CCC workshop 2017 in Nancy, and with particpants of the EU project CID in general.

The following overlapping topics are of interest to us: application of ERA with an emphasis on SMT solving, analysis of ERA w.r.t. computational complexity, and improvements of ERA software using sophisticated internal representations.

Interface iRRAM is a software library [7] making it easy to perform correct computations with real numbers. To ensure sufficient precision of intermediate values within the computation, the library makes use of exceptions which are a control flow mechanism, non-portable to languages besides C++. Therefore it is challenging to implement an interface providing access to features of iRRAM (e.g. real function computation, arbitrary precision approximations to reals, limits of real sequences) to other languages like Java.

We currently explore two ways to design such an interface:

- Interpreter approach: An extended Real Random Access Machine is simulated using iRRAM and can be used via a simple text oriented interface.
- Oracle approach: In this approach, *your-favourite-programming-language* uses iRRAM's functions as black boxes. This can be achieved by exposing (a subset of) iRRAM's Application Programming Interface in a language-independent way by means of the LLVM Intermediate Language [8,5].

  Going further, one such instance can be seen as a node in a computation graph allowing for continuous input and output edges akin oracles. We attempt to provide such a graph running parallel iRRAM instances at once.

Complexity We propose representations of reals and $C[0,1]$ corresponding to iRRAM's internal computations. To analyze complexity in the framework of Kawamura and Cook [3], we discover a correspondance of these representations to that introduced in [2]. This correspondance provides a way to reason about complexity of iRRAM computations on specific inputs.

[⋆] The research leading to these results has received funding from the DFG grant WERA MU 1801/5-1 and the DFG/RFBR grant CAVER BE 1267/14-1 and 14-01-91334. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 731143.

SMT solver We are working on an SMT solver, targeting automatic verification of problem instances formulated in first order language over real numbers.

Our main goal is to integrate numerical and symbolic approaches for continuous constraint solving. We made a few steps into that direction: our solver `ksmt` supports problems in SMT-LIB v2.5 format [1], features a CDCL-style SAT solver and via point-oriented conflict resolution [4] solves problems with linear constraints using rational arithmetic. We are currently working on interval-based bound propagation and conflict resolution, incorporating exact real arithmetic and supporting non-linear constraints.

Taylor models Taylor models, proposed by Makino and Berz [6], are multivariate polynomials with real (or rather double precision) coefficients enhanced with an error interval. The parameters denote unknown values in the interval $[-1, 1]$ and allow to express functional dependencies between different Taylor models that share those parameters which encode error information.

The iRRAM implementation of Taylor models currently is restricted to polynomials of degree one. We are experimenting with several strategies to keep linearity under multiplication and, recently, division. Further goals are

- extension to nonlinear versions (models as well as elementary operations),
- analysis of the computational complexity,
- general improvement of ERA derived from Taylor models.

References

1. C. Barrett, P. Fontaine, and C. Tinelli. The SMT-LIB Standard: Version 2.5. Technical report, Department of Computer Science, The University of Iowa, 2015. Available at http://www.smtlib.org.
2. F. Brauße and F. Steinberg. A minimal representation for continuous functions. https://arxiv.org/abs/1703.10044, 2017. preprint.
3. A. Kawamura and S. Cook. Complexity theory for operators in analysis. *ACM Trans. Comput. Theory*, 4(2):5:1–5:24, May 2012.
4. K. Korovin, N. Tsiskaridze, and A. Voronkov. Conflict resolution. In *Principles and Practice of Constraint Programming - CP 2009, 15th International Conference, CP 2009, Lisbon, Portugal, September 20-24, 2009, Proceedings*, pages 509–523, 2009.
5. LLVM language reference manual. http://llvm.org/docs/LangRef.html. Accessed on 08.05.2017.
6. K. Makino and M. Berz. Higher order verified inclusions of multidimensional systems by taylor models. *Nonlinear Analysis: Theory, Methods & Applications*, 47(5):3503 – 3514, 2001. Proceedings of the Third World Congress of Nonlinear Analysts.
7. N. T. Müller. The iRRAM: Exact arithmetic in C++. *Lecture notes in computer science*, 2991:222–252, 2001.
8. J. Zhao, S. Nagarakatte, M. M. K. Martin, and S. Zdancewic. Formalizing the LLVM intermediate representation for verified program transformations. In *Proceedings of the 39th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2012, Philadelphia, Pennsylvania, USA, January 22-28, 2012*, pages 427–440, 2012.

σ-locales and Booleanization in Formal Topology

Francesco Ciraulo

Department of Mathematics
University of Padua

It is well known that the complemented elements of a Heyting algebra H form a Boolean subalgebra of H. It is likewise well know that

$$B(H) = \{x \in H \mid x = --x\} = \{-x \mid x \in H\}$$

is a Boolean algebra as well, although joins in $B(H)$ differ from those in H. And if H is complete, than $B(H)$ is complete as well. In fact $B(H)$ is a quotient rather than a subalgebra of H. The mapping $x \mapsto --x$ defines a lattice epimorphism from H to $B(H)$. In case H is complete, this become an epimorphism of frames.

From the point of view of the categories of locales, this means that every locale L contains a Boolean sublocale $B(L)$, which can be characterized as the smallest dense sublocale of L (note that an arbitrary "intersection" of dense sublocales is dense).

Giovanni Sambin has recently introduced the notion of an *overlap algebra*, which can be understood as a "positive" alternative to a complete Boolean algebra (i. e. with no explicit requirement about complements). A first advantage of his approach is that powersets are examples of overlap algebras (in fact they are precisely the atomic ones) even if one works with intuitionistic logic, although they are not Boolean constructively [3, 4].

It has recently turned out [2] that overlap algebras arise as the smallest *strongly dense* sublocales (in the sense of [5]) of overt locales. No choice principle is used in the proof of such a result; and by classical logic the usual characterization of $B(L)$ is recovered.

The same statement can be given a predicative interpretation by substituting a formal topology $(S, \lhd, \mathsf{Pos})$ in place of an overt locale L. In this framework, overlap algebras can be characterized as those formal topologies for which the following condition holds

$$(\forall x \in S)[\,\mathsf{Pos}(a \wedge x) \Rightarrow \mathsf{Pos}(U \wedge x)] \implies a \lhd U \tag{1}$$

for every $a \in S$ and $U \subseteq S$. By classical logic such a condition can be seen as expressing subfitness of the lattice (co-frame) L^{op}.

The construction of $B(L)$ from L can be mimicked in the case of σ-locales [6]. In that case, $B(L)$ is still the smallest dense σ-sublocale of L; however, it is not Boolean any longer, in general. The σ-locales constructed in this way are called *d-reduced* ("d" for "dense") by Madden.

Our aim is to give a positive account of d-reduced σ-locales. In order to obtain this, we work with σ-locales which are *overt* (in a suitable sense). The positivity predicate Pos of an overt σ-locale L is then used to define a positive version of the *codense* congruence relation on L [6], which corresponds to the smallest dense σ-sublocale $B(L)$ of L. Actually, because of the positive nature of our definition, the notion of density involved here is intuitionistically stronger than the usual one.

Time permitting, we will discuss two further points:

- the relationship between $B(L)$ and $Ran(\mu)$, the smallest σ-sublocale of L of full measure [7], provided that μ is a finite measure on L, and L is fitted (the idea is that a full measure σ-sublocale of L must be dense in some sense);
- a predicative version of a classical result by Banaschewski [1] in the framework of formal topology (here some form of the axiom of countable choice becomes unavoidable).

References

1. Banaschewski B., *The frame envelope of a σ-frame*, Quaestiones Mathematicae (1993).
2. F. C., *Overlap Algebras as Almost Discrete Locales*, submitted (available on arXiv).
3. F. C. and G. Sambin, *The overlap algebra of regular opens*, J. Pure Appl. Algebra (2010).
4. F. C. and M. E. Maietti and P. Toto, *Constructive version of Boolean algebra*, Logic Journal of the IGPL (2012).
5. P. T. Johnstone, *A constructive "Closed subgroup theorem" for localic groups and groupoids*, Cahiers Topologie Géom. Différentielle Catég. (1989).
6. Madden J. J., *k-frames*, J. Pure Appl. Algebra (1991).
7. Simpson A., *Measure, randomness and sublocales*, Ann. Pure Appl. Logic (2012).

Rigorous Function Calculi

Pieter Collins

Maastricht University

Almost all problems in applied mathematics deal with spaces of real-valued functions on Euclidean domains in their formulation and solution, representing dependencies on parameters, time- and space-dependent solutions, or distributions of random variables. There are many function spaces used in mathematics, each appropriate for particular problems, including spaces of continuous, differentiable and analytic functions, piecewise-continuous, measurable and integrable functions, and both bounded and unbounded domains.

In this talk, I will outline a programme (Work Package 9 of CID) for developing abstractions of these function spaces within formalisms of computable analysis, and providing concrete implementations enabling efficient rigorous computation. The goal is to give practitioners in the areas of e.g. hybrid systems, stochastic systems and partial differential equations access to the tools needed to develop rigorous solution methods with guaranteed error bounds and arbitrary accuracy. Further, by specifying appropriate abstract data types, it will be possible to pass functions as first-class objects from one computational process to another, allowing the creation of integrated computational work-flows.

First implementations of such a function calculus for continuous and differential functions are contained in the C++ package Ariadne [1] for reachability analysis of hybrid systems and in the Haskell package AERN (Approximating Exact Real Numbers) [2], and in the talk I will first explain the ideas and approach used by Ariadne: Abstract classes specifying pure virtual methods for computable operations are provided to give implementation-independent interfaces. A distinction is made between *effective* representations of functions, which provide sufficient information to evaluate the function arbitarily accurately, and *validated/verified* representations, which allow evaluation up to some error tolerance. Concrete computations are performed using Taylor polynomial models [3] with uniform error bounds, which were introduced for the rigorous numerics package COSY Infinity [4], and can be instantiated in Ariadne with both double-precision and multiple-precision rounded arithmetic. However, the framework is flexible enough to allow other function models, such as polynomials represented in Bernstein or Chebyshev bases. Applying the tool to the study of hybrid systems also requires functionality for solving differential equations to compute the continuous dynamics $\dot{\phi}(x,t) = f(\phi(x,t))$, and algebraic equations to find crossing times $g(\phi(x,\tau(x)) = 0$.

The main approach of the programme will be to first clean-up the abstractions and concrete types provided by Ariadne, if possible providing language-neutral specifications, and then extend with new functionality. In the second part of the talk, I will give an overview of the planned functionality, and how it could be implemented.

The abstractions for the important classes of real function spaces arising in mathematics should be defined in terms of core computable operations supported. The continuous functions support evaluation, differentiable functions support symbolic and automatic differentiation, and analytic functions support power series and convergence rates. The measurable and integrable functions needed for stochastic processes do not support evaluation, but can be effectively defined using completion constructions [5]. Sobolev spaces, which are important for the solution of partial differential equations, could be defined in terms of weak derivatives and function norms. For nondeterministic systems such as differential inclusions, and systems defined with piecewise-continuous functions, types of set-valued functions are also required. Finally, concrete implementations of these types will be given, ideally with both simple, easily verified algorithms, and with more complex, efficient algorithms. For example, we may with to base implementations of continuous functions over a bounded box on Fourier series [6] in order to solve partial differential equations using Galerkin methods [7].

References

1. Pieter Collins, Davide Bresolin, Luca Geretti, and Tiziano Villa. Computing the evolution of hybrid systems using rigorous function calculus. In *Proceedings of the 4th IFAC Conference on Analysis and Design of Hybrid Systems*, 2012.
2. Jan Duracz, Amin Farjudian, Michal Konečný, and Walid Taha. Function interval arithmetic. In *Mathematical Software–ICMS 2014*, pages 677–684. Springer, 2014.
3. K. Makino and M. Berz. Taylor models and other validated functional inclusion methods. *Int. J. Pure Appl. Math*, 4(4):379–456, 2003.
4. K. Makino and M. Berz. COSY Infinity Version 9. *Nuclear Instruments and Methods*, A558:346–350, 2006.
5. Bas Spitters. Constructive algebraic integration theory. *Ann. Pure Appl. Logic*, 137(1-3):380–390, 2006.
6. S. Day, O. Junge, and K. Mischaikow. A rigorous numerical method for the global analysis of infinite-dimensional discrete dynamical systems. *SIAM Journal on Applied Dynamical Systems*, 3(2):117–160, 2004.
7. Piotr Zgliczyński and Konstantin Mischaikow. Rigorous numerics for partial differential equations: the kuramoto-sivashinsky equation. *Found. Comput. Math.*, 1(3):255–288, 2001.

Ramsey actions and Gelfand duality

Willem L. Fouché

Department of Decision Sciences,
School of Economic Sciences
University of South Africa, Pretoria

If G is a Hausdorff topological group, we write $C_{rub}(G)$ for the commutative C^*-algebra with an identity element based on the bounded (complex-valued) functions on G which are right-uniformly continuous. Thus a function $f : G \to \mathbb{C}$ belongs to $C_{rub}(G)$, iff it is bounded and for every $\epsilon > 0$, there is some symmetric neighbourhood V of the identity element of G (meaning that $V = V^{-1}$), such that:

$$s^{-1}t \in V \Longrightarrow |f(s) - f(t)| < \epsilon.$$

The Gelfand dual of $C_{rub}(G)$ is denoted by $\varGamma_G$, which is a compact Hausdorff space.

We shall refer to fixed points of the action of G on $\varGamma_G$ as *Ramsey characters.*

To motivate this terminology, let as look at the following different way of looking at the oldest result in Ramsey theory. In a way, we present a dynamical C^*-algebraic reformulation of this result. But first we must introduce some terminology.

Let η be the Cantor order. This means it is an example of a countable model of the first order properties of the structure $(\mathbb{Q}, \leq)$. Write S_∞ for the symmetry group of a countably infinite set. Without loss of generality, we may assume that the countable infinite set on which S_∞ acts is coded by the natural numbers $\mathbb{N}$. As such we can view S_∞ as a subset of $\mathbb{N}^\mathbb{N}$. We topologise $\mathbb{N}^\mathbb{N}$ by imposing the discrete topology and then a product topology. The resulting space is frequently referred to as the Baire space . We topologise S_∞ via encodings to view S_∞ as embedded thus

$$S_\infty \subset \mathbb{N}^\mathbb{N}.$$

As such it is a closed subgroup of the Baire space $\mathbb{N}^\mathbb{N}$. Write $\texttt{Aut}\ \eta$ for all the symmetries of η. We can naturally view $\texttt{Aut}\ \eta$ as a subgroup of S_∞. In fact $\texttt{Aut}\ \eta$ is a closed but not open subgroup of S_∞.

We have, writing $G = \texttt{Aut}\ \eta$, that $\varGamma_G$ is a Stonean space. Indeed, (see [7])

$$C_{rub}(G) \simeq C(\varprojlim_{H <_o G} \beta(G/H)),$$

and hence, by Gelfand duality, we have the topological homeomorphism

$$\varGamma_G \simeq \varprojlim_{H <_o G} \beta(G/H).$$

Here $H <_o G$ means that H is an open subgroup of G and for a discrete space D , we write $\beta(D)$ for the Stone-Čech compactification of D.

Oldest Ramsey Theorem. *For natural numbers r, n, k there is a natural number N , such that for any r-colouring χ of the k-subsets of $[N] := \{1, \dots, N\}$,* *there is a a n-subset A of $[N]$ such that χ assumes a constant value on all the k-subsets of A.*

A case can be made for the statement that this classical finitary Ramsey theorem can be expressed, in the context of C^*-algebras as

Theorem 1. *Let $\mathtt{Aut}(\eta)$ be the topological symmetry group of the Cantor order η. Write C for the C^*–algebra of right-uniformly continuous functions on $\mathtt{Aut}\ \eta$. Then there is a Gelfand character χ on C such that*

$$\sigma\chi = \chi,$$

for all $\sigma \in \mathtt{Aut}\ \eta$.

In particular, $G = \mathtt{Aut}\ \eta$ admits a Ramsey character.

In this project we explore the extent to which such a Ramsey character is "random" or could be constructively expressed. This work is a continuation of what can be found in [3], [4] and [5].

The theorem expresses, in a different language, that the action of the group $G = \mathtt{Aut}\ \eta$ on any compact Hausdorff space admits a fixed point. In other words, $G = \mathtt{Aut}\ \eta$ is an extremely amenable group. ([8], [7].) The arguments in [8] provide an attractive way for deriving Ramsey's theorem from the extreme amenability of $\mathtt{Aut}\ \eta$.

The envisaged goal of this project is to understand dynamical versions of Ramsey theorems in a constructive and/or effective topological and probabilistic context. Some precursors of this can be found in [1], [2] and [6].

References

1. Andreas Blass. Prime ideals yield almost maximal ideals. *Fund. Math*, 127: 57-66, 1987.
2. Thierry Coquand. Constructive topology and combinatorics. *Lecture Notes in Computer Science*, 613: 159-164, 1992.
3. W. L. Fouché. Symmetry and Ramsey degrees of finite relational structures. *J. Comb. Theory A*, 85:135-147, 1997.
4. W. L. Fouché. Algorithmic randomness and Ramsey properties of countable homogeneous structures. WoLLIC2012, *Lecture Notes in Computer Science*, 7456:246-256, 2012.
5. W. L. Fouché. Martin-Löf randomness, invariant measures and countable homogeneous structures. *Theory of Computing Systems*, 52:65-79, 2013.
6. P. Freyd All topoi are localic, or Why permutation models prevail. *J Pure Appl Alg*, 46:49-58, 1987.
7. E. Glasner and B. Weiss. The universal minimal system for the group of homeomorphisms of the Cantor set. *Fund. Math.* 176:277-289,2003.
8. A. S. Kechris, V. G. Pestov, and S. Todorcevic. Fraïssé limits, Ramsey theory, and topological dynamics of automorphism groups. *Geometric And Functional Analysis*, 15:106–189, 2005.

Geometric Lorenz attractors are computable

Daniel S. Graça[1], Cristóbal Rojas[2], and Ning Zhong[3]

[1] Universidade do Algarve, Portugal
& SQIG/Instituto de Telecomunicações, Portugal
[2] Universidad Andres Bello, Chile
[3] University of Cincinnati, U.S.A.

The study of the long term behavior of a system has long attracted a significant amount attention in the scientific community. However, although significant advances were made by mathematicians like Poincaré, the discovery of *strange attractors* were only made in the 1960s, with the advent of the digital computer, where numerical simulations were used to provide new insights on the asymptotic behavior of several classes of systems. A celebrated result (the Poincaré-Bendixson theorem) shows that for flows in space of dimension less than 3, the flow can only converge to limit sets constituted by fixed points or periodic orbits. However not much was known on what happened on higher dimensions. In 1963 E. N. Lorenz [3] studied the following system (the Lorenz system)

$$\begin{cases} x' = \sigma(y - x) \\ y' = \rho x - y - xz \\ z' = xy - \beta z \end{cases} \tag{1}$$

where σ, β, and ρ are parameters, as a simplified model of atmosphere convection in an attempt to understand the unpredictable behavior of the weather. Lorenz's original numerical simulations, where the parameters were given by $\sigma = 10$, $\beta = 8/3$, and $\rho = 28$, suggested that for any typical initial condition, the system would eventually tend to a limit set with a rather complicated structure, which was more complex than a fixed point or a periodic orbit – the *Lorenz (strange) attractor*. Moreover, the dynamics on this attractor seemed to magnify small errors very rapidly, rendering impractical to numerically simulate an individual trajectory for an extended period of time.

The Lorenz system became a landmark in the modern paradigm of the numerical study of chaos: instead of studying trajectories individually, one should study the limit set of a typical orbit, both as a spatial object and as a statistical distribution [4]. However, proving the existence of the Lorenz attractor in a rigorous fashion turned out to be no easy task; indeed, the problem was listed in 1998 by Smale as one of the eighteen unsolved problems he suggested for the 21st century [5].

In 1979, based on the behavior observed in the numerical simulations of (1), several authors like Afraimovich, Bykov, and Shil'nikov [1], and Guckenheimer and Williams [2] proposed a class of models for the Lorenz system, the geometric Lorenz models, whose flow satisfies a certain list of geometric properties intended to capture the observed numerically simulated behavior in the Lorenz system. In particular, they proved that any such flow must contain a strange attractor, which supports a unique invariant probability distribution that describes the limiting statistical behavior of almost any initial condition. The strange attractor contained in a geometric Lorenz flow is called the geometric Lorenz attractor.

Using a combination of normal form theory and rigorous numerics, Tucker [6] provided, in 2002, a formal proof of the existence of the Lorenz attractor by showing that the Lorenz system behaves like a geometric Lorenz models. Since a geometric Lorenz model supports a strange attractor, so does the Lorenz system (1).

Here we will examine the computability of geometric Lorenz attractors and their physical measures. In particular we will prove the following result.

Main Theorem. *For any geometric Lorenz flow, if the data defining the flow (i.e. the right-hand side of* (1)*) is computable, then its attractor is a (inner and outer) computable subset of* $\mathbb{R}^3$*. Moreover, the physical measure supported on this attractor is a computable probability measure.*

References

1. V. S. Afraimovich, V. V. Bykov, and L. P. Shil'nikov. On the appearence and structure of the lorenz attractor. *Dokl. Acad. Sci. USSR*, 234:336–339, 1977.
2. J. Guckenheimer and R. F. Williams. Structural stability of lorenz attractors. *Publ. Math. IHES*, 50:59–72, 1979.
3. E. N. Lorenz. Deterministic non-periodic flow. *J. Atmos. Sci.*, 20:130–141, 1963.
4. J. Palis. A global view of dynamics and a conjecture on the denseness of finitude of attractors. *Astérisque*, 261:339 – 351, 2000.
5. S. Smale. Mathematical problems for the next century. *Math. Intelligencer*, 20:7–15, 1998.
6. W. Tucker. A rigorous ode solver and smale's 14th problem. *Found. Comput. Math.*, 2(1):53–117, 2002.

A Variant of EQU in which Open and Closed Subspaces are Complementary without Excluded Middle

Reinhold Heckmann

AbsInt Angewandte Informatik GmbH
Science Park 2, D-66123 Saarbrücken, Germany
heckmann@absint.com

Summary: The category EQU of equilogical spaces (taken as partial equivalence relations (PERs) on prime-algebraic lattices) is Cartesian closed even in an intuitionistic set theory, but without excluded middle EM, open and closed subspaces cannot be shown to be complements of each other. On the other hand, open and closed sublocales are complementary even without EM, but it is not easy to embed the category of locales into a Cartesian closed category. Here we combine the two approaches and define a variant of EQU with PERs on the *double-duals* of prime-algebraic lattices. The resulting category EQU2 is Cartesian closed and has complementary open and closed subspaces even without EM.

General idea: We work in an intuitionistic set theory (with powersets). We first consider the category PAL of prime-algebraic lattices and Scott-continuous functions, which has set-indexed products $\prod_{i \in I} L_i$ and exponentials $[L \to M]$. An important example is $\Sigma = \mathcal{P}\mathbf{1}$ ordered by '$\subseteq$'. With EM, Σ has exactly two elements 0 and 1, but without EM, we have to reckon with more elements. Nevertheless, Scott-continuous functions $s : \Sigma \to \Sigma$ are uniquely determined by their values on 0 and 1. They preserve binary meets and inhabited joins.

A possible incarnation of EQU has objects $X = (L_X, \sim_X)$ where L_X is in PAL and '$\sim_X$' is a PER on the points of L_X. Morphisms $f : X \to Y$ are those Scott-continuous $f : L_X \to L_Y$ that preserve the respective PERs ($a \sim_X b \Rightarrow f a \sim_Y f b$). Two morphisms $f, g : X \to Y$ are considered as equal ($f \simeq g$) if they map self-related points to related results ($a \sim_X a \Rightarrow f a \sim_Y g a$). (Without choice, one should not form equivalence classes, but change the notion of equality.) PAL can be embedded into EQU by mapping L to $(L, =_L)$. EQU has set-indexed products $\prod_{i \in I} X_i$, exponentials $[X \to Y]$, and equalizers. Open and closed subspaces of X can be defined from morphisms $p : X \to \Sigma$ as $\mathrm{O}(p) = \{a \in L_X \mid p\,a = 1\}$ and $\mathrm{C}(p) = \{a \in L_X \mid p\,a = 0\}$, yet without EM, it is not possible to prove that $\mathrm{O}(p)$ and $\mathrm{C}(p)$ are complements of each other, nor that the union of two closed subspaces is closed (since $\mathrm{C}(p) \cup \mathrm{C}(q) = \mathrm{C}(p \wedge q)$ cannot be shown).

With locales, the situation is different: Even without EM, it is possible to show that open and closed sublocales are complements and that the join of two closed sublocales is closed. The reason is that locales are defined via opens, which offer additional structure compared with points. On the other hand, it is hard to embed the locales into a decent CCC because of the contravariant nature of the opens.

The basic idea for our category EQU2 is to use neither points nor opens, but second-order opens (opens of opens) because these are covariant again. For a prime-algebraic lattice L, let $\Omega L = [L \to \Sigma]$ and $\Omega^2 L = [\Omega L \to \Sigma]$. This Ω^2 is the object part of the double-dualization monad with unit $\eta_L : L \to \Omega^2 L$, where $\eta_L\, x\, u = u\, x$. The image of η_L in $\Omega^2 L$ consists exactly of those $A : \Omega L \to \Sigma$ that preserve finite meets and arbitrary joins (sobriety).

The first idea is to define the objects of EQU2 as $(L, \approx)$ where $\approx$ is a PER on $\Omega^2 L$. Yet this does not work; to obtain Cartesian closure, the domain of the PER has to be restricted. The appropriate domain is the set $L^\bullet \subseteq \Omega^2 L$ of *fuzzy points* of L, where a fuzzy point is a function $\Omega L \to \Sigma$ preserving binary meets and binary joins (hence inhabited joins by virtue of Scott continuity). Fuzzy points are more general than the η-images of points – they are not required to preserve empty meet and empty join. Compared with points, they have enough additional structure for making open and closed subspaces complements of each other, but are still sufficiently similar to points so that Cartesian closure can be proved.

Fuzzy points: Every $\eta\, x$ $(x \in L)$ is in $L^\bullet$ (points are special fuzzy points). Every constant function $K : \Omega L \to \Sigma$ is in $L^\bullet$. For $s : \Sigma \to \Sigma$ and $A \in L^\bullet$, $s \circ A \in L^\bullet$. For $A \in L^\bullet$, let the "range" $\rho A : \Sigma \to \Sigma$ be $\rho A = \lambda b^\Sigma.\, A(\mathsf{K} b)$ where $\mathsf{K} b$ is the constant function $\lambda x^L.\, b \in \Omega L$. For $f : L \to M$, $\Omega^2 f : \Omega^2 L \to \Omega^2 M$ cuts down to $f^\bullet : L^\bullet \to M^\bullet$, and $f^\bullet(s \circ A) = s \circ f^\bullet A$ and $\rho(f^\bullet A) = \rho A$.

Objects of EQU2: $(L, \approx)$ where L is in PAL and $\approx$ is a PER on $L^\bullet$ such that (1) $A \approx B \Rightarrow \rho A = \rho B$; (2) For all $s : \Sigma \to \Sigma$, $A \approx B \Rightarrow s \circ A \approx s \circ B$; (3) For all constant $K \in L^\bullet$, $K \approx K$; (4) For all $M \subseteq [\Sigma \to \Sigma]$ that are jointly monic (i.e., $(\forall m \in M.\, m\, a = m\, b) \Rightarrow a = b$), we have $(\forall m \in M.\, m \circ A \approx m \circ B) \Rightarrow A \approx B$. Properties (1) and (2) are needed to get Cartesian closure while (3) and (4) are needed to make open and closed subspaces complementary.
Notation: $|(L, \approx)| = \{a \in L \mid \eta\, a \approx \eta\, a\}$; $\|(L, \approx)\| = \{A \in L^\bullet \mid A \approx A\}$.

Morphisms $f : X \to Y$ where $X = (L_X, \approx_X)$ and $Y = (L_Y, \approx_Y)$ are continuous functions $f : L_X \to L_Y$ with $A \approx_X A' \Rightarrow f^\bullet A \approx_Y f^\bullet A'$. Two morphisms $f, g : X \to Y$ are considered equal $(f \simeq g)$ iff for all A in $\|X\|$, $f^\bullet A \approx_Y g^\bullet A$.

Points: The global points $x : \mathbf{1} \to X$ correspond to the elements of $|X|$. Since equality of EQU2 morphisms is based on $\|X\|$ instead of $|X|$, EQU2 cannot be shown to be well-pointed (in contrast to PAL and EQU).

Product: $\prod_{i \in I}(L_i, \approx_i) = (\prod_{i \in I} L_i, \approx)$ where $A \approx A'$ iff $\rho A = \rho A'$ and for all i in I, $\pi_i^\bullet A \approx_i \pi_i^\bullet A'$. For inhabited I, the condition $\rho A = \rho A'$ is redundant, and for empty I (terminal object), $\rho A = \rho A'$ is equivalent to $A = A'$.

Exponential: $L_{[Y \to Z]} = [L_Y \to L_Z]$ and $H \approx_{[Y \to Z]} H'$ iff ($\rho H = \rho H'$ and $B \approx_Y B' \Rightarrow H \cdot B \approx_Z H' \cdot B'$) where for $H \in [L_Y \to L_Z]^\bullet$ and $B \in L_Y^\bullet$, $H \cdot B = \lambda w^{\Omega L_Z}.\, H(\lambda h^{[L_Y \to L_Z]}.\, B(w \circ h))$.

Embedding of PAL into EQU2 as a full subcategory by $L \mapsto (L, =_{L^\bullet})$. In particular, Σ can be considered as an EQU2 object. The embedding preserves products and exponentials.

Subspaces: A subspace of $X = (L, \approx)$ is a subset $S \subseteq \|X\|$ such that (1) $A \in S$ & $A \approx B \Rightarrow B \in S$; (2) For all $s : \Sigma \to \Sigma$, $A \in S \Rightarrow s \circ A \in S$; (3) For all constant $K \in L^\bullet$, $K \in S$; (4) For all $M \subseteq [\Sigma \to \Sigma]$ that are jointly monic, $(\forall m \in M.\, m \circ A \in S) \Rightarrow A \in S$. Every subspace S of X induces a space $X|_S = (L, \approx_S)$ where $A \approx_S B$ iff $A \approx B$ and $A \in S$ (and $B \in S$).

The least subspace $\bar{\emptyset}$ is the set of constant functions in $L^\bullet$ and the greatest subspace is $\|X\|$ itself. The subspaces form a *frame* with inhabited meet being intersection ($\bigwedge_{i \in I} S_i = \bigcap_{i \in I} S_i$) and inhabited join being $\bigvee_{i \in I} S_i = \mathcal{M}\,(\bigcup_{i \in I} S_i)$, i.e., union, which has properties (1)–(3), followed by a closure operator $\mathcal{M}$ to achieve (4). (In contrast, sublocales form a coframe, not a frame.)

Equalizer: For $f, g : X \to Y$, $\mathrm{E}(f,g) = \{A \in \|X\| \mid f^{\bullet}A \approx_Y g^{\bullet}A\}$ is a subspace of X, and $X|_{\mathrm{E}(f,g)}$ is the equalizer of f and g.

Special case $Y = \varSigma$: $\approx_{\varSigma}$ is equality in $\varSigma^{\bullet}$, and $f^{\bullet}A =_{\varSigma^{\bullet}} g^{\bullet}A$ iff $A f =_{\varSigma} A\, g$.

Open and closed subspaces: For $p : X \to \varSigma$, let $\mathrm{O}(p) = \mathrm{E}(p, \mathsf{K}1) = \{A \in \|X\| \mid A\, p = A\,(\mathsf{K}1)\}$ and $\mathrm{C}(p) = \mathrm{E}(p, \mathsf{K}0) = \{A \in \|X\| \mid A\, p = A\,(\mathsf{K}0)\}$.

Theorem. *$\mathrm{O}(p)$ and $\mathrm{C}(p)$ are complements, i.e., $\mathrm{O}(p) \cap \mathrm{C}(p) = \bar{\emptyset}$ and $\mathrm{O}(p) \vee \mathrm{C}(p) = \|X\|$.*

Proof (sketch). If $A \in \mathrm{O}(p) \cap \mathrm{C}(p)$, then $A\, p = A\,(\mathsf{K}0) = A\,(\mathsf{K}1)$, so A is constant, hence in $\bar{\emptyset}$.
For any $A \in \|X\|$, let $s_0, s_1 : \varSigma \to \varSigma$ be given by $s_0\, a = a \vee A\, p$ and $s_1\, a = a \wedge A\, p$. Then $(s_0 \circ A)\, p = A\, p \vee A\, p = A\, p$ and $(s_0 \circ A)\,(\mathsf{K}0) = A\,(\mathsf{K}0) \vee A\, p = A\, p$, whence $s_0 \circ A \in \mathrm{C}(p) \subseteq \mathrm{O}(p) \vee \mathrm{C}(p)$. Likewise, $s_1 \circ A \in \mathrm{O}(p) \subseteq \mathrm{O}(p) \vee \mathrm{C}(p)$. Property (4) gives $A \in \mathrm{O}(p) \vee \mathrm{C}(p)$ ($\{s_0, s_1\}$ is jointly monic because $a \vee c = b \vee c \;\&\; a \wedge c = b \wedge c \;\Rightarrow\; a = b$ in any distributive lattice).

Further properties. $\mathrm{O}(\mathsf{K}1) = \|X\|$, $\mathrm{O}(p \wedge q) = \mathrm{O}(p) \cap \mathrm{O}(q)$, $\mathrm{O}(\bigvee_{i \in I} p_i) = \bigvee_{i \in I} \mathrm{O}(p_i)$, $\mathrm{C}(\mathsf{K}1) = \bar{\emptyset}$, $\mathrm{C}(p \wedge q) = \mathrm{C}(p) \vee \mathrm{C}(q)$, $\mathrm{C}(\bigvee_{i \in I} p_i) = \bigcap_{i \in I} \mathrm{C}(p_i)$.
So the join of two closed subspaces is closed.

Duality of upper and lower powerlocales on locally compact locales

Tatsuji Kawai

Dipartimento di Matematica, Università di Padova

In locale theory (i.e. point-free topology), a powerlocale of a locale is a construction whose points form a certain class of sublocales of the original locale. In this work, we study interaction between the following three powerlocale constructions on a locally compact locale X:

1. Upper powerlocale $\mathrm{P_U}(X)$, whose points are compact fitted (or saturated) sublocales of X,
2. Lower powerlocale $\mathrm{P_L}(X)$, whose points are overt weakly closed sublocales of X,
3. Scott topology $\mathbb{S}^X$, whose points are open sublocales of X (namely elements of X).

Here, $\mathbb{S}^X$ is the exponential of a locally compact locale X over the Sierpinski locale $\mathbb{S}$, and this construction is only possible on locally compact locales.

Johnstone and Vickers [1] showed that the upper and lower powerlocale constructions commute. Moreover, Vickers [2] showed that the composition of upper and lower powerlocale construction coincides with taking Scott topology twice, which is called the double powerlocale construction $\mathbb{P}(X)$. Thus, so far we have $\mathrm{P_U}(\mathrm{P_L}(X)) \cong \mathrm{P_L}(\mathrm{P_U}(X)) \cong \mathbb{S}^{\mathbb{S}^X} = \mathbb{P}(X)$.

Our main result says that three powerlocale constructions commute in a mixed way.

Theorem 1. *If X is a locally compact locale, then*

$$\mathrm{P_U}(\mathbb{S}^X) \cong \mathbb{S}^{\mathrm{P_L}(X)}, \qquad \mathrm{P_L}(\mathbb{S}^X) \cong \mathbb{S}^{\mathrm{P_U}(X)}.$$

The above result is obtained in a purely point-free way and does not rely on the spatiality of locally compact locales.

This work is based on joint work with Matthew de Brecht (Kyoto University, Japan) and Steve Vickers (The University of Birmingham, UK).

References

1. P. T. Johnstone and S. Vickers. Preframe presentations present. In A. Carboni, M. Pedicchio, and G. Rosolini, editors, *Category Theory*, volume 1488 of *Lecture Notes in Mathematics*, pages 193–212. Springer Berlin Heidelberg, 1991.
2. S. Vickers. The double powerlocale and exponentiation: A case study in geometric reasoning. *Theory Appl. Categ.*, 12(13):372–422, 2004.

Average case complexity for Hamiltonian dynamical systems *

Akitoshi Kawamura[1], Holger Thies[1], and Martin Ziegler[2]

[1] The University of Tokyo, Japan
[2] KAIST, Republic of Korea

A Hamiltonian system is a dynamical system where the evolution over time is described by $2n$ first order ordinary differential equations of the form

$$\dot{q} = \frac{\partial H}{\partial p}, \quad \dot{p} = -\frac{\partial H}{\partial q} \tag{1}$$

for a smooth real-valued function $H(t, q, p)$ called the *Hamiltonian*. The state of the system is a point (q, p) in *phase space* with vectors $q, p \in \mathbb{R}^n$ called the *position* and *momentum*, respectively, and $t \in \mathbb{R}$ is the *time*. Hamiltonian systems are widely used in physics to describe the motion of mechanical systems. An important property of Hamiltonian systems is given by Liouville's theorem: The measure of a subset of phase space remains constant over time.

Given an initial condition q_0, p_0 for time t_0 and assuming H is analytic in a neighborhood of (t_0, q_0, p_0) the initial value problem (1) has a unique, analytic solution $\varphi : \mathbb{R} \to \mathbb{R}^{2n}$ defined on some neighborhood of t_0. If H is additionally polynomial time computable, φ is also a polynomial time computable real function [3].

We consider the problem of simulating the motion of a given Hamiltonian system on some fixed time interval $[0, T]$, i.e., given initial conditions q_0, p_0 at time 0 taken from some fixed compact subset of initial conditions and some $t \in [0, T]$, compute $q(t)$.

One problem is that the solution might not exist up to T due to singularities on the real line. On the other hand, if there are no real singularities in $[0, T]$ then the algorithm to solve the initial value problem can be iterated until the desired time is reached. The computational complexity, however, depends heavily on the location of the *complex* singularities, as they determine the number of iterations necessary. It is therefore for many systems impossible to bound the worst-case complexity independently from the initial condition. Nonetheless, the solution might not have complex singularties close to the real line for most initial values, allowing efficient computation *on average*.

Average case complexity for real functions was recently introduced by Schröder, Steinberg and Ziegler [5]. In this talk we give an application of the theory to the problem of simulating Hamiltonian dynamical systems. We focus on the famous n-body problem and some of its variations. The classical n-body problem describes the motion of n particles with masses $m_1, \ldots, m_n$ under their mutual gravitational attraction either in 2 or 3 dimensions. It can be written in Hamiltonian form (1)

* The authors thank the Japan Society for the Promotion of Science (JSPS), Core-to-Core Program (A. Advanced Research Networks) for supporting the research.

with Hamiltonian

$$H(q,p) = \sum_{i=1}^{n} \frac{\|p_i\|^2}{2m_i} - \sum_{1 \leq i \leq j} \frac{m_i m_j}{\|q_i - q_j\|} \tag{2}$$

with $q, p \in \mathbb{R}^{2n}$ for the planar and $q, p \in \mathbb{R}^{3n}$ for the spatial case. The Hamiltonian (2) is polynomial time computable and analytic in a neighborhood of any initial value and does not depend explicitly on the time t, i.e., the value of the Hamiltonian for a given initial value is constant over time. We call it the *system energy.*

It is well known that for $n \geq 3$ the problem does not have an analytical solution. Thus, the only possible approach to predict the motion in general is numerical simulation. For the special case of $n = 3$ and non-zero angular momentum there is a way to continue the solution beyond the singularities by a convergent power series due to Sundman [6], theoretically allowing to simulate the motion up to any time for all initial conditions. This solution is, however, not practical as the series converges extremely slowly [1]. On the other hand, Saari [4] showed that for $n \leq 4$ the subset of initial values leading to singularities has Lebesgue measure zero.

While Saari's result guarantees that the simulation is possible for almost all initial conditions, we need a stronger result to bound the computational complexity. We define an ε-collision as a state of the system where two particles have distance less than ε to each other. If the initial values are chosen such that no ε-collision occurs in $[0, T]$, the number of steps can be bounded in terms of ε which in turn induces a bound on the overall complexity. We thus want the measure of the set of initial conditions leading to an ε-collision in some fixed time interval tend to 0 for $\varepsilon \to 0$. While at first this may seem like a simple generalization of Saari's theorem, the ideas in Saari's proof can not be applied directly and to our best knowledge no such result is known so far. Indeed, without the time restriction the statement is false even for the three body problem [8].

As a first step, we consider a slightly modified version of the problem, the planar circular restricted three body problem. Two massive particles move on a fixed circular orbit in the plane and a third, massless particle is influenced by their gravitational forces. Although this problem is much easier than the original problem, it still can not be solved analytically [2] and has been studied for more than 200 years due to its numerous applications [7].

Our main result is that for initial values with bounded position and energy the subset of initial conditions leading to an ε-collision at some time $t \in [0, 1]$ has Lebesgue measure bounded by a function proportional to $\sqrt{\varepsilon}$ and thus indeed tends to 0 for $\varepsilon \to 0$. We further use this result to show that simulating the planar circular restricted three body problem for finite time is polynomial time computable on average. We compare our results with numerical simulations and discuss possible extensions of our ideas to the general n-body problem and other Hamiltonian systems as well difficulties that arise.

References

1. D. Beloriszky. Application pratique des méthodes de M. Sundman à un cas particulier du problème des trois corps. *Bulletin Astronomique*, 6(2):417–434, 1930.

2. Michel Hénon. *Generating families in the restricted three-body problem*, volume 52. Springer Science & Business Media, 2003.
3. Bernd Moiske and Norbert Th Müller. Solving initial value problems in polynomial time. In *Proc. 22 JAIIO - PANEL '93, Part 2*, pages 283–293, Buenos Aires, 1993.
4. Donald G. Saari. A global existence theorem for the four-body problem of Newtonian mechanics. *Journal of Differential Equations*, 26(1):80–111, October 1977.
5. Matthias Schröder, Florian Steinberg, and Martin Ziegler. Average-Case Bit-Complexity Theory of Real Functions. In *Mathematical Aspects of Computer and Information Sciences*, pages 505–519. Springer, Cham, November 2015.
6. Karl F. Sundman. Mémoire sur le problème des trois corps. *Acta Mathematica*, 36(0):105–179, 1913.
7. Victor Szebehely. Theory of orbits. The restricted problem of three bodies. *New York: Academic Press*, 1967.
8. Lei Zhao. Quasi-periodic Almost-collision Orbits in the Spatial Three-Body Problem. *arXiv:1308.2484 [math]*, August 2013. arXiv: 1308.2484.

The Perfect Tree Theorem and Open Determinacy

Takayuki Kihara[1] and Arno Pauly[2]

[1] Nagoya University, Japan
kihara@i.nagoya-u.ac.jp
[2] Université libre de Bruxelles, Belgium
Arno.M.Pauly@gmail.com

At the Dagstuhl seminar *The Perfect Tree Theorem and Open Determinacy* [2], Marcone raised the question which Weihrauch degree(s) correspond to the principle ATR_0 in reverse mathematics. Candidates discussed were closed choice (denoted $\mathrm{C}_{\mathbb{N}^\mathbb{N}}$) or unique closed choice (denoted $\mathrm{UC}_{\mathbb{N}^\mathbb{N}}$) on Baire space (as studied in [1]). Two theorems were suggested as starting points for this exploration:

Theorem (Perfect Tree Theorem). If $T \subseteq \mathbb{N}^{<\omega}$ is a tree such that $[T]$ is uncountable, then T has a perfect subtree.

We recall that tree is called *perfect*, if any vertex in the tree has at least two incomparable descendents. Any perfect subset of $\mathbb{N}^\mathbb{N}$ arises as the set of infinite paths through a perfect tree, and for any perfect tree T we find $[T]$ to be perfect. The Perfect Tree Theorem in particular implies that the continuums hypothesis holds if restricted to closed sets.

Theorem (Open determinacy). Consider a two-player infinite sequential game with moves from $\mathbb{N}$. Let the first player have an open winning set. Then one player has a winning strategy.

We find that the Weihrauch degrees of these theorems depend on the way they are interpreted as computational problems, and they do so in the same pattern:

Theorem 1. *The following are Weihrauch equivalent*[3]*:*

1. $C_{\mathbb{N}^\mathbb{N}}$
2. *Given a tree $T \subseteq \mathbb{N}^{<\omega}$ is a tree such that $[T]$ is uncountable, find a perfect subtree of T.*
3. *Given an open game with moves from $\mathbb{N}$ such that Player 2 has a winning strategy, find a winning strategy.*

Theorem 2. *The following are Weihrauch equivalent:*

1. $UC_{\mathbb{N}^\mathbb{N}}$
2. *Given a tree $T \subseteq \mathbb{N}^{<\omega}$ such that $[T]$ is non-empty and countable, find a sequence $(p_n)_{n\in\mathbb{N}}$ satisfying:*
$$[T] = \{p_n \mid n \in \mathbb{N}\}$$
3. *Given an open game with moves from $\mathbb{N}$ such that Player 1 has a winning strategy, find a winning strategy.*

[3] The equivalence of 1 and 2 was already noted by Brattka and Marcone.

Theorem 3. *The following problems are strictly harder than* $C_{\mathbb{N}^\mathbb{N}}$*:*

- *Given a tree* T *such that* $[T]$ *is non-empty, find a subtree* T' *and a sequence* $(p_n)_{n\in\mathbb{N}}$ *such that either* T' *is perfect or* $[T] = \{p_n \mid n \in \mathbb{N}\}$*.*
- *Given an open game with moves from* $\mathbb{N}$*, find a Nash equilibrium.*

The latter shows that games with moves from $\mathbb{N}$ behave very differently compared to games with finitely many moves. In [3] it was shown that for games with finitely many moves and winning sets from the finite levels of the difference hierarchy, there always is a player such that the promise that this player wins does not reduce the Weihrauch degree of the problem to find a winning strategy.

It seems like a tempting conjecture that the two problems in Theorem 3 might be equivalent, but proving this seems to be beyond our current reach.

References

1. Vasco Brattka, Matthew de Brecht & Arno Pauly (2012): *Closed Choice and a Uniform Low Basis Theorem. Annals of Pure and Applied Logic* 163(8), pp. 968–1008, doi:`10.1016/j.apal.2011.12.020`.
2. Vasco Brattka, Akitoshi Kawamura, Alberto Marcone & Arno Pauly (2016): *Measuring the Complexity of Computational Content (Dagstuhl Seminar 15392). Dagstuhl Reports* 5(9), pp. 77–104, doi:`http://dx.doi.org/10.4230/DagRep.5.9.77`. Available at `http://drops.dagstuhl.de/opus/volltexte/2016/5686`.
3. Stéphane Le Roux & Arno Pauly (2015): *Weihrauch Degrees of Finding Equilibria in Sequential Games.* In Arnold Beckmann, Victor Mitrana & Mariya Soskova, editors: *Evolving Computability*, *Lecture Notes in Computer Science* 9136, Springer, pp. 246–257, doi:`10.1007/978-3-319-20028-6_25`.

Towards Certified Algorithms for Exact Real Arithmetic

Sunyoung Kim[1], Gyesik Lee[2], Sewon Park[3], and Martin Ziegler[3]

[1] Dept. of Math., Yonsei Univ.
[2] Dept. of Comp. Sci. and Eng., Hankyong Nat'l Univ.
[3] School of Computing, KAIST

In this extended abstract we introduce our research plan. The main goal of the research is to develop/extend libraries and tools supporting development of certified algorithms for Exact Real Arithmetic(ERA). This project would require at least the following points:

(1) Research on foundations of computing with continuous data:
We have to give a logical foundation for the formalization of the structure of real numbers as computable abstract axiomatized data type. It would be a necessary basis for the semantics of an extension of some imperative object-oriented programming language can be provided.

(2) Research on tools supporting ERA:
There are several tools supporting ERA among which iRRAM [1] seems to be most realistic and fast. Moreover, there have been many reports demonstrating its feasibility such as [4] and [2]. There has even started to certify library of IRRAM [3]. However, one needs to go much further to reach the feasibility and soundness of iRRAM and its library.

(3) Development of libraries for computable reals in a theorem prover:
In [2], the authors demonstrates how to certify some ERA algorithms written using iRRAM. For that purpose, they use Hoare logic. We believe that it is possible to extend their idea in several directions. One of them is to (semi-)automatize the certification process. This idea is partially realized in [3] which we believe could be extended and automatized.

References

1. Norbert Th. Müller. The iRRAM: Exact Arithmetic in C++. In *Computability and Complexity in Analysis*, pages 222–252. Springer, Berlin, Heidelberg, 2001.
2. Norbert Th. Müller, Sewon Park, Norbert Preining, and Martin Ziegler. On Formal Verification in Imperative Multivalued Programming over Continuous Data Types. *CoRR*, 2016. arXiv: 1608.05787.
3. Norbert Th. Müller and Christian Uhrhan. Some Steps into Verification of Exact Real Arithmetic. In *NASA Formal Methods*, number 7226 in Lecture Notes in Computer Science, pages 168–173. Springer, 2012.
4. Norbert Th. Müller and Martin Ziegler. From Calculus to Algorithms without Errors. In *Mathematical Software – ICMS 2014*, number 8592 in Lecture Notes in Computer Science, pages 718–724. Springer, 2014.

Decidability in Symbolic-Heap System with Arithmetic and Arrays

Daisuke Kimura[1] and Makoto Tatsuta[2]

[1] Toho University, Japan
[2] National Institute of Informatics, Japan

A symbolic-heap system is a fragment of separation logic, and characterizes only shapes of heaps by abstraction. It is useful for memory error checking in software verification. The truth of entailments in this system is known to be decidable. Extensions of the symbolic-heap systems with arithmetic and arrays have been actively studied recently. These extensions enable us to handle arrays of programming languages as well as pointer arithmetic in a symbolic-heap system. This talk proves the decidability of entailment checking in a symbolic heap system of separation logic with Presburger arithmetic and arrays. It is proved by translating this problem into a formula in Presburger arithmetic and using the decidability of Presburger arithmetic.

Types for safe and efficient exact computation

Michal Konečný and Eike Neumann

Aston University, Birmingham, United Kingdom
{m.konecny,neumaef1}@aston.ac.uk

AERN2[1] is a set of Haskell packages for programming exact numeric computation with the dual focus on demonstrably correct code and efficient execution. AERN2 also aims to be a playground for easy experimenting with various concepts and algorithms of computable analysis and real complexity theory. We report how the AERN2 types facilitate flexible choice of optimised evaluation strategies for Cauchy sequences, safe mixing of types in expressions without explicit conversions and safely using partial operations, detecting errors at compilation and ruling out run-time exceptions, infinities and not-a-numbers (NaNs).

Computing enclosures of exact values

Numerical computation usually involves values of various types, not only numbers such as integers, dyadics, rationals, real and complex numbers, but also vectors, matrices, closed real intervals, continuous, differentiable or analytic real functions, infinite sequences and various types of subsets of $\mathbb{R}^n$. Some of these values are finite (i.e. they form discrete spaces, e.g. $\mathbb{Q}$) and some are infinite (i.e. they form uncountable spaces, e.g. $\mathbb{R}$). Infinite values are typically approximated by finite values, e.g. a real number is often approximated by a fairly small dyadic interval that contains this number. We call such a set that approximates an exact infinite value an **enclosure**. For an enclosure of a value in a metric space, we define the accuracy of the enclosure in terms of its diameter. An infinite value is often approximated by a sequence of enclosures whose intersection is the value and whose diameter converges to 0.

AERN2 provides interval arithmetic using type `MPBall` of balls with dyadic centres and double-precision radii. Exact real number computation is provided in two ways:

- Cauchy sequences: A value of type `CauchyReal` encapsulates a function from `Accuracy` to `MPBall`. Arithmetic on these values usually works in 2 passes: the accuracy requirement is passed top-down to determine sufficient accuracies of all operands and constants and then the resulting enclosures are combined bottom-up to give an enclosure of the resulting real number.
  There are various **evaluation strategies** for computing enclosures for accuracy queries, including:
  - Caching of the best enclosure so that it can be reused in subsequent queries.
  - Querying and evaluating several Cauchy reals in parallel.

[1] https://github.com/michalkonecny/aern2

Each evaluation strategy is given as a different Arrow [1]. A real number computation can be written in an **arrow-generic** way so that the same program can be evaluated with different strategies, e.g. with or without caching, in parallel or sequentially.

- Iterative evaluation: An `MPBall` computation is repeated with increasing precision until the accuracy of the result is sufficient. The result is a `CauchyReal` but it is not computed from other `CauchyReal`s. This is similar to the main mode of exact real computation in the iRRAM C++ library.

We compare the performance of these two methods using several common benchmarks. With the caching evaluation strategy, the two methods have similar speed of execution, but the caching of `CauchyReal` approximations causes this method to take more memory than iterative evaluation. We also benchmark the benefit of parallel evaluation in exact Fast Fourier Transform (FFT).

AERN2 also provides several representations of continuous unary real functions using enclosures that are based on polynomials. We have compared their performance in [2].

Types for expressions with mixed types and partial operations

In a typical numerical computation, numerical expressions tend to mix values of different types with automatic conversions and type-based dispatch for different implementations of common operations (e.g. integer, rational, floating-point, matrix multiplications). An incorrect application of a partial operation such as division or square root either throws an exception or returns a not-a-number (NaN) value. Consider the following expressions:

```
-2 * (k/n) * pi * complex_i                                  (1)
integrateOverDom (dyadicInterval (-1,1)) (sin(10*f))         (2)
```

Here `k` and `n` are integers, forming the rational `k/n`, which is multiplied by an integer on one side and a real number on the other, and finally the resulting real number is multiplied by a complex number. Moreover, the expression (1) has no value for $n = 0$. In the second expression, `f` has to be an integrable unary function which is defined on the interval $[-1, 1]$.

Dynamically typed languages such as Matlab and Python would let us implement these expressions very conveniently, automatically converting the integers to rationals and then converting the result of the fraction to a real etc. Nevertheless, without static types the programmer gets little help in checking the correctness of the expressions and one usually ends up executing tests and debugging many exceptions and one still does not get much assurance that no exceptions will occur when the code is deployed. These problems get only worse when introducing more advanced numerical types, such as real functions.

On the other hand, statically typed languages such as ML and Haskell detect most type mismatches early (e.g. as soon as the code is saved in the editor), while they infer the most general types for expressions. Moreover, these languages have the potential to deal properly with partial operators, although this is rarely done. The downside is that these languages usually restrict the mixing of types in expressions and therefore expressions tend to include explicit type conversions.

AERN2 overrides many of the Haskell defaults so that numerical expressions allow Matlab-style mixing of values of different types in operators while maintaining early detection of type mismatches during compilation. In essence, types of expressions are consistently derived bottom-up using multi-parameter type classes and associated type functions. For example, the expression `sin(10*f)` is valid if `f` is of a type `t` that satisfies the constraints `CanMulBy t Integer` and `CanSinCos t` and its type is `SinCosType t`. In the default Haskell numerical type hierarchy, this expression would require `Floating t`. AERN2 types such as `MPBall` and `CauchyReal` satisfy `Floating` and thus can be used also with the traditionally type-checked Haskell numerical expressions.

Partial operators have return type using an "error" monad. Let us denote this monad `E` for short. For instance, we could have `(/) :: a -> b -> E c` and `sqrt :: c -> E d`. Nevertheless, this solution does not compose well as, for instance `\x y -> sqrt(x/y) :: a -> b -> E (E c)`. To get rid of the nested `E`, we could use monadic `join :: E(E t) -> E t` but this would clutter the expressions. AERN2 gives type-generic partial operations a more convenient type similar to, for instance, `(/) :: a -> b -> EnsureE c` and `sqrt :: c -> EnsureE d`, where `EnsureE (E t) = (E t)` and `EnsureE t = E t` otherwise. As the type function `EnsureE` is idempotent, there is no need to add `join`.

References

1. J. Hughes. Generalising monads to arrows. *Science of computer programming*, 37(1-3):67–111, 2000.
2. M. Konečný and E. Neumann. Representations for feasibly approximable functions. In *Proceedings of the Thirteenth International Conference on Computability and Complexity in Analysis (CCA 2016)*, pages 27–29, 2016.

Partial Computable Functions: Analysis and Complexity

Margarita Korovina[1] and Oleg Kudinov[2]

[1] A.P. Ershov Institute of Informatics Systems, SbRAS, Novosibirsk,
rita.korovina@gmail.com,
[2] Sobolev Institute of Mathematics, SbRAS, Novosibirsk
kud@math.nsc.ru

Classical computability theory has a long term tradition to study partial computable functions. While the class of effective topological spaces, in particular computable Polish spaces, is one of the main objects for investigation in the Effective Descriptive Set Theory (EDST) the class of partial computable functions $\mathcal{PCF}$ over effective topological spaces has not been deeply investigated yet. We report on ongoing research addressing natural problems related to partial computability.

$\mathcal{PCF}_{\mathcal{XY}}$ We fix the definition of a partial computable function [4] in the settings of effectively enumerable spaces is motivated by the following observations. It is well-known that in the domain–theoretic framework a partial computable real function is effectively continuous on its domain and the domain is a $\Pi_2^0[\mathbb{R}]$ in the effective Borel hierarchy [7] (see also [3]). On the computable Polish spaces this definition agrees with several known approaches to partial computability [12, 1, 2]. We show that the class $\mathcal{PCF}$ of partial computable functions over effectively enumerable spaces is closed under composition.

Weak separability for majorant–computability We perform comparative analysis of partial computability in frameworks of different approaches, in particular $\mathcal{PCF}_{\mathcal{X}\mathbb{R}}$ and the majorant computable real-valued functions $\mathcal{MC}_{\mathcal{X}\mathbb{R}}$ [5]. Thus, an effectively enumerable topological space $\mathcal{X}$ satisfies the weak separability property of the effectively open subsets if and only if $\mathcal{PCF}_{\mathcal{X}\mathbb{R}} = \mathcal{MC}_{\mathcal{X}\mathbb{R}}$. It is worth noting that the Baire, Cantor spaces and the real numbers satisfies the separability property of the effectively open subsets It will be challenging to establish whether all computable Polish spaces satisfy this property.

Index sets for $\mathcal{PCF}_{\mathcal{XY}}$ over computable Polish spaces We give a characterisation of partial computability in terms of classical enumeration operators (see e.g. [9]). Then based on this characterisation we show the existence of the principal computable numbering of $\mathcal{PCF}_{\mathcal{XY}}$ for computable Polish spaces. This allows us to study the complexity of index sets of important problems in computable analysis such as function equality and root verification. It turns out that for some problems the corresponding complexity does not depend on the choice of a computable Polish space while for other ones the corresponding choice plays a crucial role. For example, the problem of function equality is Π_1^1-complete for any $\mathcal{X}$ and $\mathcal{Y}$ while the complexity of totality problem of partial computable real-valued functions on $\mathcal{X}$ differs from space to space e.g. for $\mathcal{X} = \mathbb{R}$ totality problem is Π_2^0–complete whereas for $\mathcal{X} = \mathcal{N}$ it is Π_1^1–complete.

Descriptive complexity of $\mathcal{PCF}$ images First we show the existence of a partial computable surjection between any computable Polish space and any effectively enumerable topological space with point recovering. Using this result we prove that for any computable Polish spaces $\mathcal{X}$ and $\mathcal{Y}$, the images of partial computable functions $f : \mathcal{X} \to \mathcal{Y}$ are exactly Σ_1^1–subsets of Y in the effective Lusin hierarchy on $\mathcal{Y}$. These results give a rise on next ensuing research directions:

- Investigations of bounds on the descriptive complexity of the images of total computable functions over computable Polish spaces. We make a conjecture that bounds will be different for particular classes of computable Polish spaces. For example, it is easy to see that for the total computable real functions, the images range over intervals of special kind.
- Generalisations of EDST on computable Polish spaces to EDST on the wider class of effective topological spaces. One of the promising candidates could be effectively enumerable topological spaces with point recovering.

References

1. Gregoriades, V., Kispeter, T., Pauly, A.(2014) A comparison of concepts from computable analysis and effective descriptive set theory. *Mathematical structures in computer science* (submitted to) http://arxiv.org/abs/1403.7997
2. Hemmerling A. (2002) Effective metric spaces and representations of the reals, *Theor. Comput. Sci.* **284** (2), pages 347-372.
3. Hemmerling A. (1999) On approximate and algebraic computability over the real numbers, *Theor. Comput. Sci.* **219** (1-2), pages 185223.
4. Korovina, M. V. and Kudinov, O. V. (2016) Complexity for partial computable functions over computable Polish spaces. *Mathematical structure in Computer Science.* DOI: 10.1017/S0960129516000438, Published online: 19 December 2016.
5. Korovina, M. V. and Kudinov, O. V. (2016) Computable Elements and Functions in Effectively Enumerable Topological spaces. *Mathematical structure in Computer Science.* DOI: 10.1017/S0960129516000141, Published online: 23 June 2016.
6. Korovina, M. V. and Kudinov, O. V. (2008) Towards Computability over Effectively Enumerable Topological Spaces. *Electr. Notes Theor. Comput. Sci.* **221**, 115–125.
7. Korovina, M. V. and Kudinov, O. V. (1999) Characteristic Properties of Majorant-Computability over the Reals. In *Proc. CiE'98, Lecture Notes in Computer Science* **1584**, 188–203. Springer-Verlag.
8. Moschovakis, Y. N. (2009) *Descriptive set theory.* North-Holland, Amsterdam.
9. Rogers, H. (1967) *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, New York.
10. Spreen, D. (1998) On Effective Topological Spaces. *J. Symb. Log.* **63** (1), 185–221.
11. Selivanov., V. (2015) Towards the Effective Descriptive Set Theory. *Lecture Notes in Computer Science* **9136**, 324–333. Springer.
12. Weihrauch, K. (1993) Computability on Computable Metric Spaces. *Theor. Comput. Sci.* **113** (1), 191–210.

The Computational Content of the Constructive Kruskal Tree Theorem

Dominique Larchey-Wendling

LORIA – CNRS

Abstract. We present a Coq mechanization of an inductive proof of Kruskal's tree theorem on Well Quasi Orders and we discuss the computational content of that theorem.

Well Quasi Orders (WQO) are an important class of quasi orders (reflexive and transitive relations) which moreover satisfy the property of being well:

> A binary relation R over set/type X is *Well* if any infinite sequence $s : \mathbb{N} \to X$ contains a good pair, i.e. $i < j$ such that $R(s_i, s_j)$

But there are numerous classically equivalent characterizations of that property, see [1] for instance. WQO are stable under several constructs as exemplified by Dickson's lemma, the finite sequence theorem, Higman's lemma, Higman's theorem and Kruskal's tree theorem. Nachum Dershowitz decisively used Kruskal's tree theorem in Computer Science to show the termination of *recursive path orderings.* But WQOs can be used to show termination properties in a much larger contexts, see [5] for instance.

The Kruskal tree theorem states that the class of WQOs is stable under the tree homeomorphic embedding:

If $\leq$ is a WQO then `embed_tree_homeo`($\leq$) is a WQO.

One particular case of that theorem is Vazsonyi's conjecture: in every infinite set S of undecorated finite trees, there is a pair $t_1 \neq t_2 \in S$ of trees such that t_1 embeds into t_2. Solving that conjecture was certainly one of the main motivations behind the tree theorem.

There are many classical proofs of the tree theorem, including J.B. Kruskal's original proof. Among them, the most well known is the "short proof" of Crispin Nash-Williams based on the *minimal bad sequence* argument. That proof typically uses the excluded middle and the axiom of choice. It has been implemented in Isabelle/HOL by Christian Sternagel [3].

Contrary to classical proofs, there are few instances of intuitionistic proofs for Kruskal's tree theorem. Some require the assumption that the ground relation is decidable (e.g. [1, 2]). Veldman's [4] is the only published proof that does not require that decidability property, but it requires *Brouwer's thesis.* Moreover, no intuitionistic proof had been mechanized before.

The difficulty behind instuitionistic/constructive proofs of Kruskal's tree theorem is that proofs based on the *minimal bad sequence* argument typically uses the excluded middle and the axiom of choice. According to Veldman [4], Kruskal's original proof was much more intuitionistic in spirit. But it is also much longer. Another important obstacle is the following: the several classically equivalent definitions of the notion of WQO are (for most of them) not intuitionistically equivalent. Hence, the statement of the theorem depends (intuitionistically) on the choice of a particular definition of WQO, mostly of the Well property.

The inductive and type theoretical proof we have developed shows that a suitable intuitionistic formulation of Well is the notion of *Almost Full relation* as defined by Thierry Coquand [5] (there is also an intuitionistically equivalent formulation in terms of *Bar inductive predicates*). Hence, we prove the following inductive Kruskal tree theorem:

If a relation R is almost full then so is `embed_tree_homeo`(R)

From that theorem, we can intuitionistically derive Vazsonyi's conjecture: we keep the full power of Kruskal's theorem in that intuitionistically formulation.

Our proof follows the pattern of Veldman's [4] intuitionistic proof but the intuitionistic set-theoretic context is replaced by inductive type theory. As we use Coquand inductive formulation of almost full relation as a substitute of the well property, the *Brouwer's thesis* axiom used by Veldman is not necessary anymore: our proof is *axiom free*. We discuss the computational content of the almost full predicate and of the intuitionistic Kruskal tree theorem.

References

1. Jean Goubault-Larrecq. A Constructive Proof of the Topological Kruskal Theorem. In *Mathematical Foundations of Computer Science 2013 - 38th International Symposium, MFCS 2013, Klosterneuburg, Austria, August 26-30, 2013. Proceedings*, volume 8087 of *Lecture Notes in Computer Science*, pages 22–41. Springer, 2013.
2. Monika Seisenberger. *On the Constructive Content of Proofs*. PhD thesis, July 2003.
3. Christian Sternagel. Certified Kruskal's Tree Theorem. *J. Formalized Reasoning*, 7(1):45–62, 2014.
4. Wim Veldman. An intuitionistic proof of Kruskal's theorem. *Arch. Math. Log.*, 43(2):215–264, 2004.
5. Dimitrios Vytiniotis, Thierry Coquand, and David Wahlstedt. Stop When You Are Almost-Full - Adventures in Constructive Termination. In *Interactive Theorem Proving - Third International Conference, ITP 2012, Princeton, NJ, USA, August 13-15, 2012. Proceedings*, volume 7406 of *Lecture Notes in Computer Science*, pages 250–265. Springer, 2012.

Fractal Intersections and Products via Algorithmic Dimension

Neil Lutz*

Rutgers University
njlutz@rutgers.edu

Abstract. Algorithmic dimensions quantify the algorithmic information density of individual points and may be defined in terms of Kolmogorov complexity. This work uses these dimensions to bound the classical Hausdorff and packing dimensions of intersections and Cartesian products of fractals in Euclidean spaces. This approach shows that a known intersection formula for Borel sets holds for arbitrary sets, and it significantly simplifies the proof of a known product formula. Both of these formulas are prominent, fundamental results in fractal geometry that are taught in typical undergraduate courses on the subject.

Classical fractal dimensions, among which *Hausdorff dimension* [9] is the most important, refine notions of measure to quantitatively classify sets of measure 0. In 2000, J. Lutz [10] showed that Hausdorff dimension can be simply characterized using betting strategies called *gales*, and that this characterization can be *effectivized* in order to quantitatively classify non-random infinite data objects. This *effective Hausdorff dimension* and other, related *algorithmic dimensions* have been applied to multiple areas of computer science and have proven especially useful in algorithmic information theory [8, 15, 5].

The connection between algorithmic and classical dimensions has more recently been exploited in the other direction, i.e., to apply algorithmic information theoretic methods and intuition to classical fractal geometry (e.g., [16, 1]). A *point-to-set principle* of J. Lutz and N. Lutz [11] characterizes the classical Hausdorff dimension of any set in $\mathbb{R}^n$ in terms of the algorithmic dimensions of its individual points.

In the same work, J. Lutz and N. Lutz showed that this principle gives rise to a new, pointwise technique for dimensional lower bounds, and, as a proof of concept, used this technique to give an algorithmic information theoretic proof of Davies's 1971 [4] theorem stating that every Kakeya set in $\mathbb{R}^2$ has Hausdorff dimension 2. This bounding technique has since been used by N. Lutz and Stull [12] to make new progress on a problem in classical fractal geometry by deriving an improved lower bound on the Hausdorff dimension of generalized Furstenberg sets, as defined by Molter and Rela [14].

The same algorithmic dimensional technique is applied in this work to bound the dimensions of intersections and products of fractals. Most significantly, we

* Research supported in part by National Science Foundation Grant 1445755.

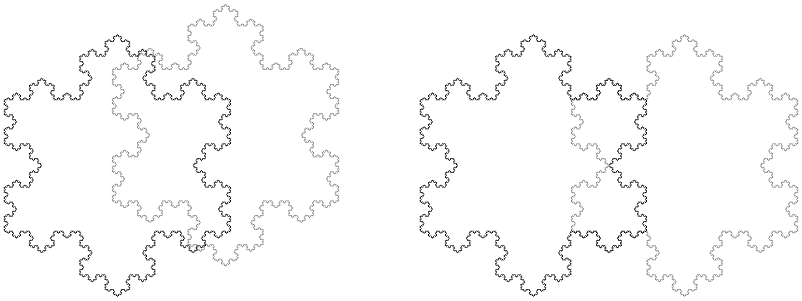

Fig. 1. Let E and F each be Koch snowflakes, which have Hausdorff dimension $\log_3 4 \approx 1.26$. Left: For almost all z, the intersection $E \cap (F + z)$ has Hausdorff dimension at most $2 \log_3 4 - 2 \approx 0.52$. Right: For a measure zero set of translations, the Hausdorff dimension of the intersection may be as large as $\log_3 4$. Note that Koch curves are Borel sets, so the new generality given by Theorem 1 is not required for this example.

extend the following intersection formula, previously shown to hold when E and F are Borel sets [6], to arbitrary sets E and F.[1]

Theorem 1 *For all* $E, F \subseteq \mathbb{R}^n$*, and for almost every* $z \in \mathbb{R}^n$, $\dim_H(E \cap (F + z)) \leq \max\{0, \dim_H(E \times F) - n\}$*, where* $F + z = \{x + z : x \in F\}$.

This approach also yields a simplified proof of the following known product formula for general sets.

Theorem 2 (Marstrand [13]) *For all* $E \subseteq \mathbb{R}^m$ *and* $F \subseteq \mathbb{R}^n$, $\dim_H(E) + \dim_H(F) \leq \dim_H(E \times F)$.

We use symmetric arguments to derive the known corresponding statements about *packing dimension* [18, 7], a formulation of fractal dimension that was developed independently by Tricot [18] and Sullivan [17] and is dual to Hausdorff dimension. These results are included here to showcase the versatility of this technique and its ability to capture the exact duality between Hausdorff and packing dimensions.

References

1. Verónica Becher, Jan Reimann, and Theodore A. Slaman. Irrationality exponent, Hausdorff dimension and effectivization. 2016.
2. Christopher J. Bishop. Personal communication, April 27, 2017.
3. Christopher J. Bishop and Yuval Peres. *Fractals in Probability and Analysis.* Cambridge University Press, 2017.
4. R. O. Davies. Some remarks on the Kakeya problem. *Proceedings of the Cambridge Philosophical Society*, 69:417–421, 1971.
5. Rod Downey and Denis Hirschfeldt. *Algorithmic Randomness and Complexity.* Springer-Verlag, 2010.

[1] This result is closely related to the Marstrand Slicing Theorem, as stated in the excellent recent book by Bishop and Peres [3]. The proof given there assumes that a set is Borel, but this assumption was inadvertently omitted from the theorem statement [2].

6. Kenneth. J. Falconer. *Fractal Geometry: Mathematical Foundations and Applications.* Wiley, first edition, 1990.
7. Kenneth J. Falconer. Sets with large intersection properties. *Journal of the London Mathematical Society*, 49(2):267–280, 1994.
8. Xiaoyang Gu and Jack H. Lutz. Dimension characterizations of complexity classes. *Computational Complexity*, 17(4):459–474, 2008.
9. Felix Hausdorff. Dimension und äusseres Mass. *Mathematische Annalen*, 79:157–179, 1919.
10. Jack H. Lutz. The dimensions of individual strings and sequences. *Information and Computation*, 187(1):49–79, 2003.
11. Jack H. Lutz and Neil Lutz. Algorithmic information, plane kakeya sets, and conditional dimension. In *Proceedings of the 34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8–11, 2017, Hannover, Germany*, pages 53:1–53:13, 2017.
12. Neil Lutz and D. M. Stull. Bounding the dimension of points on a line. In TV Gopal, Gerhard Jaeger, and Silvia Steila, editors, *Theory and Applications of Models of Computation: 14th Annual Conference, TAMC 2017, Bern, Switzerland, April 20-22, 2017, Proceedings*, pages 425–439, 2017.
13. John M. Marstrand. Some fundamental geometrical properties of plane sets of fractional dimensions. *Proceedings of the London Mathematical Society*, 4(3):257–302, 1954.
14. Ursula Molter and Ezequiel Rela. Furstenberg sets for a fractal set of directions. *Proc. Amer. Math. Soc.*, 140:2753–2765, 2012.
15. Andre Nies. *Computability and Randomness.* Oxford University Press, Inc., New York, NY, USA, 2009.
16. Jan Reimann. Effectively closed sets of measures and randomness. *Annals of Pure and Applied Logic*, 156(1):170–182, 2008.
17. Dennis Sullivan. Entropy, Hausdorff measures old and new, and limit sets of geometrically finite Kleinian groups. *Acta Mathematica*, 153(1):259–277, 1984.
18. Claude Tricot. Two definitions of fractional dimension. *Mathematical Proceedings of the Cambridge Philosophical Society*, 91(1):57–74, 1982.

Computing Absolutely Normal Numbers in Nearly Linear Time

Jack Lutz[1] and Elvira Mayordomo[2]

[1] Department of Computer Science, Iowa State University, Ames, IA 50011 USA
lutz@cs.iastate.edu
[2] Departamento de Informática e Ingeniería de Sistemas, Instituto de Investigación en Ingeniería de Aragón, Universidad de Zaragoza, 50018 Zaragoza, SPAIN
elvira@unizar.es

In 1909 Borel [3] defined a real number α to be *normal* in base b ($b \geq 2$) if, for every $m \geq 1$ and every length-m sequence w of base-b digits, the asymptotic, empirical frequency of w in the base-b expansion of α is b^{-m}. Borel defined α to be *absolutely normal* if it is normal in every base $b \geq 2$. (This clearly anticipated the fact, proven a half-century later, that a real number may be normal in one base but not in another [5, 13].) The recent book [4] provides a good exposition of the many aspects of current research on normal numbers.

The work reported here [11] concerns a relatively new problem, namely, the complexity of *efficiently* computing a real number that is provably absolutely normal. Sierpinsky [14], Lebesgue [10], and Turing [15, 1] gave very inefficient constructions of absolutely normal numbers, but it was only in 2013 that Becher, Heiber, and Slaman [2] published an algorithm that computes an absolutely normal number in polynomial time. Specifically, this algorithm computes the binary expansion of an absolutely normal number x, with the nth bit of x appearing after $O(n^2 f(n))$ steps for any computable unbounded nondecreasing function f. (Unpublished polynomial-time algorithms for computing absolutely normal numbers were also announced independently by Mayordomo [12] and Figueira and Nies [7, 8] at about the same time.)

In this work we present a new algorithm that provably computes an absolutely normal in nearly linear time. Our algorithm computes the binary expansion of an absolutely normal number x, with the nth bit of x appearing after $O(n\text{polylog}(n))$ steps. The term "nearly linear time" was introduced by Gurevich and Shelah [9]. In that paper they showed that, while linear time computability is very model-dependent, nearly linear time is very robust. For example, they showed that random access machines, Kolmogorov-Uspensky machines, Schoenhage machines, and random-access Turing machines share exactly the same notion of nearly linear time.

The novelty of our algorithm is its use of the Lempel-Ziv parsing algorithm to achieve its nearly linear time bound. For each base $b \geq 2$, we use a martingale (betting strategy) that employs the Lempel-Ziv parsing algorithm and is implicit in the work of Feder [6]. This base-b Lempel-Ziv martingale succeeds exponentially when betting on the successive digits of the base-b expansion of any real number that is not normal in base b. Our algorithm simultaneously computes and diagonalizes against (limits the winnings of) a martingale that incorporates efficient proxies of all these martingales, thereby efficiently computing a real number that is normal in every base.

References

1. V. Becher, S. Figueira, and R. Picchi. Turing's unpublished algorithm for normal numbers. *Theoretical Computer Science*, 377:126–138, 2007.
2. V. Becher, P. A. Heiber, and T. A. Slaman. A polynomial-time algorithm for computing absolutely normal numbers. *Information and Computation*, 232:1–9, 2013.
3. E. Borel. Sur les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27(1):247–271, 1909.
4. Y. Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193. Cambridge University Press, 2012.
5. J. W. S. Cassels. On a problem of Steinhaus about normal numbers. *Colloquium Mathematicum*, 7:95–101, 1959.
6. M. Feder. Gambling using a finite state machine. *IEEE Transactions on Information Theory*, 37:1459–1461, 1991.
7. S. Figueira and A. Nies. Feasible analysis and randomness. Manuscript, 2013.
8. S. Figueira and A. Nies. Feasible analysis, randomness, and base invariance. *Theory of Computing Systems*, 56:439–464, 2015.
9. Y. Gurevich and S. Shelah. Nearly linear time. In *Proceedings of the First Symposium on Logical Foundations of Computer Science*. Springer, 1989.
10. H. Lebesgue. Sur certaines demonstrations d'existence. *Bull. Soc. Math. de France*, 45:132–144, 1917.
11. J. H. Lutz and E. Mayordomo. Computing absolutely normal numbers in nearly linear time. Technical Report arXiv:1611.05911, arXiv.org, 2016.
12. E. Mayordomo. Construction of an absolutely normal real number in polynomial time. Manuscript, 2013.
13. W. M. Schmidt. On normal numbers. *Pacific J. Math*, 10(2):661–672, 1960.
14. W. Sierpinski. Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'une tel nombre. *Bull. Soc. Math. France*, 45:125–132, 1917.
15. A. M. Turing. A note on normal numbers. In J. Britton, editor, *Collected Works of A.M. Turing: Pure Mathematics*, pages 117–119. North Holland, 1992.

On real numbers in the Minimalist Foundation

Maria Emilia Maietti

Dipartimento di Matematica, Università di Padova
via Trieste 63, 35121 Padova (Italy)
maietti@math.unipd.it

It is well known that the classical different characterizations of real numbers may no longer be equivalent in a constructive foundation due to the absence of choice principles including countable choice.

We will show that this is even more true in the Minimalist Foundation, for short **MF**, ideated in [8] in joint work with Giovanni Sambin and completed into a two-level formal system in [2], due to its strictly predicative nature which makes it compatible with the most relevant classical and constructive foundations in the literature.

We recall that the two-level structure of **MF** includes: an *intensional level* suitable as a base for a proof-assistant to formalize its proofs and extract their computational contents, an *extensional level* formulated in a language as close as possible to that of ordinary mathematics and, finally, an *interpretation of the latter in the former* by means of a quotient model showing that the extensional level has been obtained by abstraction from the intensional one according to Sambin's forget-restore principle in [11].

Both levels of **MF** are represented as a dependent type theory in the style of Martin-Löf's one, respectively in [9, 4]. In particular it is worth noting that the intensional level of **MF** provides a *predicative* (and of course still *constructive*) version of the Calculus of Inductive Constructions on which the French proof-assistant Coq is based.

It should be clear from the described two-level structure that to build a model of the extensional level of **MF** is enough to build a model for its intensional level. Hence, by building a model for the intensional level of **MF**, we show that in the extensional level of **MF** the collection of real numbers as Dedekind sections or as Cauchy sequences in terms of functional relations *do not form a set* but only a collection. This is contrary to what happens in the model with other descriptions of real numbers such as Bishop's regular Cauchy sequences defined as suitable typed-terms. The key point is that typed-terms between natural numbers are interpreted as computable sequences while the interpretation of number-theoretic functional relations also includes non-computable ones.

Our model is placed within the subcategory of assemblies of Hyland's Effective Topos [1]. In particular it makes use of suitable properties of their boolean quasi-topos structure studied in joint work with Fabio Pasquali and Giuseppe Rosolini by employing the categorical notion of elementary quotient completion in [7, 6] (which was introduced to study the properties of the quotient model used in **MF**).

The fact that real numbers do not form a set in the extensional level of **MF** is related to the fact that both the axiom of unique choice and the axiom of choice, even restricted to relations on natural numbers, are not valid in both levels of **MF**, as one can show directly by also using Streicher's model in [10].

As shown in [3] this fact is in turn related to the fact that the rule of choice and the rule of unique choice are also not generally valid in both levels of **MF**.

In particular the non validity of the rule of unique choice implies that the representation of computable functions via typed terms of the intensional level of **MF** is strictly stronger than their strong representation via functional relations.

From these facts we conclude that in order to extract programs from proofs in **MF**, in particular about real numbers, we need to interpret its intensional level in a realizability model like that in [5], or in a stronger theory validating at least the rule of unique choice like Martin-Löf's type theory in [9].

References

1. J. M. E. Hyland. The effective topos. In *The L.E.J. Brouwer Centenary Symposium (Noordwijkerhout, 1981)*, volume 110 of *Stud. Logic Foundations Math.*, pages 165–216. North-Holland, Amsterdam-New York,, 1982.
2. M. E. Maietti. A minimalist two-level foundation for constructive mathematics. *Annals of Pure and Applied Logic*, 160(3):319–354, 2009.
3. M.E. Maietti. On choice rules in dependent type theory. In *International Conference on Theory and Applications of Models of Computation*, pages 12–23. Springer, 2017.
4. P. Martin-Löf. *Intuitionistic Type Theory. Notes by G. Sambin of a series of lectures given in Padua, June 1980.* Bibliopolis, Naples, 1984.
5. M.E. Maietti and S. Maschio. A predicative variant of a realizability tripos for the minimalist foundation. *IfCoLog Journal of Logics and their Applications*, special issue Proof Truth Computation, 2016.
6. M. E. Maietti and G. Rosolini. Elementary quotient completion. *Theory and Applications of Categories*, 27(17):445–463, 2013.
7. M. E. Maietti and G. Rosolini. Quotient completion for the foundation of constructive mathematics. *Logica Universalis*, 7(3):371–402, 2013.
8. M. E. Maietti and G. Sambin. Toward a minimalist foundation for constructive mathematics. In L. Crosilla and P. Schuster, editor, *From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics*, number 48 in Oxford Logic Guides, pages 91–114. Oxford University Press, 2005.
9. B. Nordström, K. Petersson, and J. M. Smith. *Programming in Martin-Löf's Type Theory, an introduction.* Oxford University Press, 1990.
10. T. Streicher. Independence of the induction principle and the axiom of choice in the pure calculus of constructions. *Theoretical Computer Science*, 103(2):395–408, 1992.
11. G. Sambin and S. Valentini. Building up a toolbox for Martin-Löf's type theory: subset theory. In G. Sambin and J. Smith, editors, *Twenty-five years of constructive type theory, Proceedings of a Congress held in Venice, October 1995*, pages 221–244. Oxford U. P., 1998.

A stratified pointfree definition of probability via constructive natural density

S. Maschio

University of Padova, Italy

Although Kolmogorov's axiomatic approach to probability is now considered standard, it has some disadvantages, in particular it is generally not very informative about how to concretely assign a probability to an event. There are at least other three historically relevant approaches to probability: one is Bernoulli's and Laplace's classical approach (shortly $\frac{\text{favourable cases}}{\text{possible cases}}$), the second is the frequentist approach (the probability is the limit of frequencies of success in a sequence of iterated trials), the third is de Finetti's subjective approach. These four paradigms overlap, but unfortunately don't coincide.

Here we give a constructive (à la Bishop, [1]) account of the frequentist approach, by means of natural density ([4]) and then we try to propose a general definition of probability structure, being authentically abstract and pointfree, but at the same time containing some information about the procedure for "concretely" assigning the probability. Such a structure can be presented in a type-theoretical framework, such as the Minimalist Foundation in [3, 2] and essentially consists of three layers: there is a Heyting algebra $\mathcal{P}$, which must be understood as the algebra of all *potential events.* $\mathcal{P}$ contains a Boolean subalgebra $\mathcal{B}$ which must be understood as the algebra of the events for which an evaluation of probability can be easily given (one could call these events *regular* or *deterministic*). In between these two algebras there is a third structure $\mathcal{E}$, the set of *actual events*, on which a probability is defined (which coincides with the evaluation on events in $\mathcal{B}$).

This shape can be recognized in the following two examples from classical mathematics. The first is the definition of a uniform probability measure on a bounded interval $[a, b]$ of the real line: first one assigns a probability to intervals (and hence to Borel subsets in $\mathcal{B}([a, b])$). Then one defines an outer measure on all potential events in $\mathcal{P}([a, b])$ and finally carves Lebesgue measurable sets (the actual events) out of $\mathcal{P}([a, b])$ using Caratheodory construction. The second example is the following: suppose one already has a Kolmogorov probability space $(\Omega, \mathcal{B}, \mathbb{P})$. One can consider fuzzy sets $f : \Omega \to [0, 1]$ as potential events and can define actual events as those which are integrable, extending $\mathbb{P}$ by defining $\mathbb{P}(f)$ as $\int_\Omega f\, d\mathbb{P}$.

Let us consider now a constructive account of the frequentist approach via natural density. A sequence of trials can be represented as a sequence

$$x_n \in \{0, 1\}\, [n \in \mathbb{N}^+]$$

For every such a sequence $\underline{x}$ one can define a sequence $\Phi(\underline{x})$ of rational numbers

$$\Phi(\underline{x})(n) := \frac{\sum_{j=1}^{n} x_n}{n}$$

i. e. the sequence of success rates in the first n trials.
We then define an *actual event* as a pair $(\underline{x}, \alpha)$ where $\underline{x}$ is a sequence of trials and

α is a strictly increasing sequence of natural numbers such that

$$|\Phi(\underline{x})(\alpha(n)+k) - \Phi(\underline{x})(\alpha(n)+h)| < \frac{1}{n} \qquad \left[n \in \mathbb{N}^+, k \in \mathbb{N}, h \in \mathbb{N}\right]$$

It is an immediate consequence of the previous condition that for every such an event $(\underline{x}, \alpha)$ the sequence $\Phi(\underline{x}) \circ \alpha$ is a Bishop real and that for every pair $(\underline{x}, \alpha)$, $(\underline{y}, \beta)$ of events with $\underline{x} = \underline{y}$, one has that $\Phi(\underline{x}) \circ \alpha$ and $\Phi(\underline{y}) \circ \beta$ are equal Bishop reals. Hence one can define a function $\mathbb{P}$ from the set of events to Bishop reals as $\mathbb{P}(\underline{x}, \alpha) := \Phi(\underline{x}) \circ \alpha$. This gives rise to a constructive account of frequentist probability. If we write $\underline{x} \in \mathcal{E}$ as a shorthand for "*there exists α such that $(\underline{x}, \alpha)$ is an event*", one can constructively prove that the following rules are satisfied:

$$\frac{}{\underline{0} \in \mathcal{E}} \qquad \frac{}{\mathbb{P}(\underline{0}) =_{\mathbb{R}} 0} \qquad \frac{\underline{x} \in \mathcal{E}}{\neg \underline{x} \in \mathcal{E}} \qquad \frac{\underline{x} \in \mathcal{E}}{\mathbb{P}(\neg \underline{x}) =_{\mathbb{R}} 1 - \mathbb{P}(\underline{x})}$$

$$\frac{\underline{x} \in \mathcal{E} \qquad \underline{y} \in \mathcal{E} \qquad \underline{x} \wedge \underline{y} = \underline{0}}{\underline{x} \vee \underline{y} \in \mathcal{E}} \qquad \frac{\underline{x} \in \mathcal{E} \qquad \underline{y} \in \mathcal{E} \qquad \underline{x} \vee \underline{y} \in \mathcal{E} \qquad \underline{x} \wedge \underline{y} \in \mathcal{E}}{\mathbb{P}(\underline{x} \vee \underline{y}) + \mathbb{P}(\underline{x} \wedge \underline{y}) =_{\mathbb{R}} \mathbb{P}(\underline{x}) + \mathbb{P}(\underline{y})}$$

$$\frac{\underline{x}' \leq \underline{x} \qquad \underline{x}' \in \mathcal{E} \qquad \underline{x} \in \mathcal{E}}{\mathbb{P}(\underline{x}') \leq_{\mathbb{R}} \mathbb{P}(\underline{x})} \qquad \frac{\underline{x}' \leq \underline{x} \qquad \underline{x} \in \mathcal{E} \qquad \mathbb{P}(\underline{x}) = 0}{\underline{x}' \in \mathcal{E}}$$

If $\underline{\rho}$ and $\underline{\pi}$ are finite lists of 0s and 1s, one can define a sequence of trials $[[\underline{\rho}, \underline{\pi}]]$ as the sequence of trials which begins with $\underline{\rho}$ and then consists of a periodic repetition of $\underline{\pi}$. Such sequences can be understood as representing regular events or events which can be evaluated following the classical approach (up to a finite number of errors). They form a boolean algebra $\mathcal{B}$ included in $\mathcal{E}$ on which the probability coincides with the probability given by the classical approach to $\underline{\pi}$, i. e. $\mathbb{P}(\mathsf{exp}(\underline{\alpha}, \underline{\pi})) = \frac{\sum_{i=1}^{\ell(\pi)} \pi_i}{\ell(\underline{\pi})}$.

In this constructive example we can recognize the three layers structure. We can hence propose a notion of *probability structure* as a triplet $(\mathcal{P}, \mathcal{E}, \mathcal{B})$ where $\mathcal{P}$ is a Heyting algebra, $\mathcal{B}$ is a Boolean subalgebra and $\mathcal{B} \subseteq \mathcal{E} \subseteq \mathcal{P}$ for which the rules above for $\mathcal{E}$ are satisfied. Both the previous examples satisfy these rules.

References

1. E. Bishop and D. S. Bridges. *Constructive analysis.* Springer, 1985.
2. M. E. Maietti. A minimalist two-level foundation for constructive mathematics. *Annals of Pure and Applied Logic*, 160(3):319–354, 2009.
3. M. E. Maietti and G. Sambin. Toward a minimalist foundation for constructive mathematics. In L. Crosilla and P. Schuster, editor, *From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics*, number 48 in Oxford Logic Guides, pages 91–114. Oxford University Press, 2005.
4. Ivan Niven. The asymptotic density of sequences. *Bull. Amer. Math. Soc.*, 57(6):420–434, 11 1951.

Isomorphism and Classification for Countable Structures

Russell Miller[⋆]

Queens College – C.U.N.Y., 65-30 Kissena Blvd.
Queens NY 11367 USA
Graduate Center of C.U.N.Y., 365 Fifth Avenue
New York, NY 10016 USA

The *Isomorphism Problem* for computable structures is well-known in computable model theory: for a particular class $\mathfrak{D}$ of computable structures, each given by an index e for the characteristic function φ_e of its atomic diagram, the Isomorphism Problem is the set of those pairs (e_0, e_1) such that the structures with indices e_0 and e_1 are isomorphic. In many cases, this problem is Σ^1_1-complete, which is as hard as it can possibly be: this holds when $\mathfrak{D}$ is the class of all computable graphs, for example, or all computable groups, or all computable fields. These results were discovered mainly by Friedman and Stanley in [4], although others have enriched them since then as well. Different classes of computable structures have simpler isomorphism problems. For computable equivalence structures, the isomorphism problem is Π^0_4-complete, as it is for for computable torsion-free abelian groups, while for computable subfields of the algebraically closed field $\overline{\mathbb{Q}}$, it is Π^0_2-complete. Details appear in [1–3, 5].

Here we investigate what happens when we drop the requirement that the structures be computable. Our structures will all still be countable, with domain ω, but instead of naming a structure by the characteristic function of its atomic diagram (or by an index for that function), we will treat the atomic diagram itself as the structure, viewing it as a real number, i.e., as an element of Cantor space 2^ω. The classes $\mathfrak{D}$ of interest to us will now include the class of all countable torsion-free abelian groups with domain ω, for example, or the class of all equivalence structures with domain ω, or similar classes. (An *equivalence structure* consists of nothing more than an equivalence relation E on the domain, in the language with E and equality.) Such a class $\mathfrak{D}$ defines a certain subclass of Cantor space, and we identify $\mathfrak{D}$ with that subclass. The subclass itself is not usually an open set; its complexity is usually determined by the complexity of the axiom set (if any) for structures in $\mathfrak{D}$, such as the axioms for torsion-free abelian groups. In some cases, these axioms may be $\mathcal{L}_{\omega_1\omega}$ sentences: the class of all subfields of $\overline{\mathbb{Q}}$, for example, is defined by the axioms for a field of characteristic 0 along with the (infinitary Π_2) statement that every element satisfies some polynomial over $\mathbb{Q}$.

A class $\mathfrak{D}$, still viewed as a subclass of 2^ω, inherits the subset topology from 2^ω. Considering the isomorphism problem for $\mathfrak{D}$, we then examine the quotient $\mathfrak{D}/\cong$, in which elements of $\mathfrak{D}$ defining isomorphic structures are identified. $\mathfrak{D}/\cong$ now bears the quotient topology relative to $\mathfrak{D}$: a subset $\mathcal{U}$ of $\mathfrak{D}/\cong$ is a set of $\cong$-classes,

[⋆] The author was supported by Grant # DMS – 1362206 from the N.S.F., and by grants from the PSC-CUNY Research Award Program and the Queens College Research Enhancement Fund.

and it is open in $\mathfrak{D}/\cong$ if and only if its union is an open subset of $\mathfrak{D}$. This means that, for $\mathcal{U}$ to be open, every element $\mathcal{A}$ of an $\cong$-class in $\mathcal{U}$ must have an initial segment σ (that is, a finite fragment of the atomic diagram of $\mathcal{A}$) such that all elements of $\mathfrak{D}$ extending σ belong to $\cong$-classes in $\mathcal{U}$. We write $\mathcal{U}_\sigma$ for the subset of 2^ω containing all extensions of σ, and refer to $\mathcal{U}_\sigma \cap \mathfrak{D}$ as a *neighborhood* of $\mathcal{A}$ within $\mathfrak{D}$. Likewise, $(\mathcal{U}_\sigma \cap \mathfrak{D})/\cong$ is a neighborhood of the $\cong$-class of $\mathcal{A}$ in $\mathfrak{D}/\cong$.

The challenge now is to recognize $\cong$ on $\mathfrak{D}$ as one of the standard Borel equivalence relations on 2^ω or on ω^ω, up to homeomorphism. Often this dictates the addition of certain definable predicates to the language, and we regard these predicates as providing a classification of $\mathfrak{D}$ up to isomorphism. For example, for the class $\mathfrak{Alg}_0$ of subfields of $\overline{\mathbb{Q}}$ (with domain ω), we can add, for each $n > 1$, an n-ary relation R_n defined by

$$R_n(a_0, \dots, a_{n-1}) \iff (\exists x)\ x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

(It is equivalent to add a list of those $p \in \mathbb{Q}[X]$ which have a root in the field.) The class $\mathfrak{Alg}_0^*$ of subfields of $\overline{\mathbb{Q}}$ in this expanded language, modulo isomorphism, is homeomorphic to the equality relation on Cantor space itself: there is a computable function (of type 2, i.e., given by a Turing functional) mapping $\mathfrak{Alg}_0^*/\cong$ bijectively onto 2^ω, for which the inverse is also computable. Since computable functions are continuous, this is a homeomorphism. The intriguing aspect is that the reduct $\mathfrak{Alg}_0/\cong$, back in the plain language of fields, is not homeomorphic to equality on 2^ω: the $\cong$-class of $\mathbb{Q}$ itself is contained in no open set except the entire space, whereas the $\cong$-class of $\overline{\mathbb{Q}}$ is contained in every nonempty open set. This reflects the primality of $\mathbb{Q}$ and the universality of $\overline{\mathbb{Q}}$ in $\mathfrak{Alg}_0$, and leads us to conclude that the relations R_n are essential to a nice classification of $\mathfrak{Alg}_0$ up to isomorphism. We plan to discuss the situation for other classes $\mathfrak{D}$ in which isomorphism is an arithmetic relation; these include the class of finite-branching trees, that of torsion-free abelian groups, that of algebraically closed fields of characteristic 0, and that of equivalence structures on ω.

References

1. W. Calvert; The isomorphism problem for classes of computable fields, *Archive for Mathematical Logic* **43** (2004), 327–336.
2. W. Calvert, D. Cummins, J.F. Knight, & S. Miller; Comparing classes of finite structures, *Algebra and Logic* **43** (2004), 365–373.
3. W. Calvert & J.F. Knight; Classification from a computable viewpoint, *Bulletin of Symbolic Logic* **12** (2006), 191–218.
4. H. Friedman & L. Stanley; A Borel reducibility for classes of countable structures. *Journal of Symbolic Logic* **54** (1989), 894–914.
5. J.F. Knight, S. Miller, & M. Vanden Boom; Turing computable embeddings. *Journal of Symbolic Logic* **72** 3 (2007), 901–918.

Nonstandard Analysis, Computability Theory, and metastability

Dag Normann[1] and Sam Sanders[2]

[1] Department of Mathematics, The University of Oslo,
P.O. Box 1053, Blindern N-0316 Oslo, Norway
dnormann@math.uio.no
[2] Munich Center for Mathematical Philosophy,
LMU Munich, Germany
sasander@me.com

Abstract. We discuss a new connection between Nonstandard Analysis and computability theory, pioneered in [10], based on the following two intimately related topics.

(T.1) A basic property of *Cantor space* $2^{\mathbb{N}}$ is *Heine-Borel compactness*: Any open cover of $2^{\mathbb{N}}$, has a *finite* sub-cover. A natural question is: *How hard is it to compute such a finite sub-cover*? We make this precise by analysing functionals that given $g : 2^{\mathbb{N}} \to \mathbb{N}$, output $\langle f_0, \dots, f_n\rangle$ in $2^{\mathbb{N}}$ such that the neighbourhoods defined from $\overline{f_i}g(f_i)$ for $i \leq n$ cover $2^{\mathbb{N}}$. The *special* and *weak* fan functionals are central objects in this study and exhibit *extreme* computational hardness.

(T.2) A basic property of $2^{\mathbb{N}}$ in *Nonstandard Analysis* is Abraham Robinson's *nonstandard compactness*, i.e. that every binary sequence is 'infinitely close' to a *standard* binary sequence. We analyse the strength of this nonstandard compactness property in the spirit of *Reverse Mathematics*, which turns out to be intimately related to the computational properties of the special and weak fan functionals.

We connect the topics (T.1) and (T.2) to mainstream mathematics by deriving the special fan functional from *slight* variations of Tao's notion of *metastability* ([13]). Based on the latter observation, we establish that many mathematical theorems naturally have 'metastable versions' which involve functionals of extreme computational hardness. We also discuss exceptions, like the *infinite pigeon hole principle*, whose metastable versions stay within Gödel's T.

Metastability, nonstandard compactness, and the special fan functional

Introduction

We introduce the *special fan functional* Θ and sketch its surprising properties, including its connection to Tao's *metastability* ([13]) and *nonstandard compactness* as in *Robinson's theorem* ([4]*p. 42). We use Kleene's schemes S1-S9 ([7]) as our notion of computability.

As to history, Θ was introduced in [11]*§3, and its computational properties are studied in [10, 9]. Intuitively speaking, Θ computes a cover for Cantor space, i.e.

on input $g : 2^{\mathbb{N}} \to \mathbb{N}$, Θ outputs $\langle f_0, \dots, f_n \rangle$ in $2^{\mathbb{N}}$ such that the neighbourhoods defined from $\overline{f_i}g(f_i)$ for $i \leq n$ cover $2^{\mathbb{N}}$, as follows:

$$(\forall T^1 \leq_1 1, g^2)\big[(\forall \alpha^1 \in \Theta(g))(\exists n \leq g(\alpha))(\overline{\alpha}n \not\in T) \to (\exists k^0)(\forall \beta^1 \leq_1 1)(\overline{\beta}k \not\in T)\big], \tag{$\mathsf{SCF}(\Theta)$}$$

where T^1 is a variable reserved for trees. Any functional Θ satisfying $\mathsf{SCF}(\Theta)$ is called a *special fan functional*, i.e. this functional is not unique. Despite its simple definition, *no type two functional can compute any* Θ, while the functional $\exists^3$ corresponding to full second-order arithmetic can compute a functional Θ. The combination of any Θ and the 'arithmetical comprehension' functional $\exists^2$ computes a realiser for ATR_0, the fourth 'Big Five' system of Reverse Mathematics (See [12]*V).

Furthermore, the combination of any Θ and the Suslin functional S^2, which corresponds to the fifth 'Big Five' system Π^1_1-CA_0 ([12]*VI), computes Gandy's *Superjump* ([3]). The combination $\Theta + S^2$ exists at the level of Π^1_2-CA_0, the outer limits of ordinal analysis, and proves the consistency of Π^1_1-CA_0, by way of foundational result, as Θ yields a conservative extension of PRA.

The previous results suggest that Θ is an interesting object of study in computability theory. As it happens, Θ was first discovered in [11] by applying the proof translation from [14] to the *nonstandard compactness* of Cantor space, which is the nonstandard counterpart of *weak König's lemma*. Hence, there is a fundamental connection between the Reverse Mathematics of Nonstandard Analysis and (higher-order) computability theory. Surprisingly, we can also connect Θ to the mathematical mainstream, Tao's notion of *metastability* in particular. To this end, we study the 'textbook' example of metastability involving the unit interval from [1]*§1.

Example 1 (Metastable convergence) The monotone convergence theorem (MCT) states that *any non-decreasing sequence in the unit interval converges to a limit*; such a sequence is hence a *Cauchy sequence* for which the usual 'epsilon-delta' definition (for a sequence $a_{(\cdot)}$ of reals) is as follows:

$$(\forall \varepsilon >_{\mathbb{R}} 0)\underline{(\exists N^0)(\forall n^0, m^0 \geq N)}(|a_n - a_m| \leq \varepsilon). \tag{1}$$

Given classical logic, (1) is equivalent to the following 'metastable' version:

$$(\forall \varepsilon >_{\mathbb{R}} 0, F)\underline{(\exists M^0)}(\forall n, m \in [M, F(M)])(|a_n - a_m| \leq \varepsilon). \tag{2}$$

While these two formulas are equivalent, their computational behaviour is quite different: On one hand, there is no computable way of obtaining an upper bound on N^0 in the usual definition (1). On the other hand, an upper bound for M^0 as in (2) is given by $F^{\lceil \frac{1}{\varepsilon} \rceil + 1}(0)$, which is the result of iterating F for $\lceil \frac{1}{\varepsilon} \rceil + 1$-many times and then evaluating at 0. In particular, M^0 as in (2) is one of the values in the finite sequence $\langle 0, F(0), F(F(0)), \dots, F^{\lceil \frac{1}{\varepsilon} \rceil + 1}(0) \rangle$. Thus, we obtain:

$$(\exists \theta^{(0\times 1)\to 0^*})(\forall k^0, F, a_{(\cdot)} \in I([0,1]))(\exists M \in \theta(k, F))(\forall n, m \in [M, F(M)])(|a_n - a_m| \leq \tfrac{1}{k}) \tag{3}$$

where '$a_{(\cdot)} \in I([0,1])$' means that $a_{(\cdot)}$ is a non-decreasing sequence in $[0,1]$.

In Example 1, we observed a 'computational' advantage of metastability (2) over (1): By introducing F as in (2), we reduce the underlined pair of quantifiers of the form '$\exists\ \forall$' in (1) to the underlined '$\exists$' quantifier in (2) as the universal quantifier (involving n, m) in (2) is bound by $F(M)$, and hence may be neglected. Thanks to this reduction in quantifier complexity, there is a finite sequence $\theta(k, F)$ which is *independent of the sequence* $a_{(\cdot)}$ as in (3), i.e. we also obtain *highly uniform* computational information. This *metastability trade-off* has been observed in general:

> Whereas in general noneffective proofs of convergence statements [...] might not provide a (uniform) computable rate of convergence, highly uniform rates of metastability can under very general conditions always be extracted using tools from mathematical logic [...]. ([6]*p. 1090)

In the next section, we investigate whether this trade-off can be made for a slight variation of (1) and (2) involving the definition of *limit convergence* instead of the definition of *Cauchy sequence* (1).

Metastability and the monotone convergence theorem

In this section, we introduce $\mathsf{MCT}_{\mathsf{meta}}$, which derives from MCT by applying the metastability trade-off to a *slight* variation of (1), namely the definition of *limit convergence*. We study the computational behaviour of $\mathsf{MCT}_{\mathsf{meta}}$, which turns out to be surprisingly *different* from (3). In particular, Θ emerges from $\mathsf{MCT}_{\mathsf{meta}}$.

We shall consider, instead of the definition of Cauchy sequence as in (1), the following definition of 'limit with rate of convergence' for $x_{(\cdot)} \in I([0,1])$:

$$\underline{(\exists x^1 \in [0,1], g^1)(\forall k^0, N^0)}(N \geq g(k) \to |x - x_N| \leq \tfrac{1}{k}), \tag{4}$$

Now, it is well-known that the limit x and rate of convergence g as in (4) are not computable from the sequence $x_{(\cdot)}$ (See [12]*§1.9). Hence, let us modify the underlined quantifier pair in (4) in the same way as in metastability in (2).

$$(\forall G^2)\underline{(\exists x^1 \in [0,1], g^1)}(\forall k^0, N^0 \leq G(x, g))(N \geq g(k) \to |x - x_N| \leq \tfrac{1}{k}), \tag{5}$$

In the same way as for (1) and (2), we have reduced the underline pair of quantifiers in (4) to the underlined quantifier in (5) as the bounded quantifier (involving k, N) in (5) again 'does not count'.

Now let us write down the associated version of (3) as follows:

$$\begin{aligned}(\exists M^{2\to 1^*})(\forall G^2, x_{(\cdot)}^{0\to 1})\big[&(\forall n^0)(0 \leq x_n \leq x_{n+1} \leq 1) \qquad (\mathsf{MCT}_{\mathsf{meta}})\\ &\to (\exists x^1, g^1 \in M(G))(\forall k, N \leq G(x, g))(N \geq g(k) \to |x - x_N| \leq \tfrac{1}{k})\big],\end{aligned}$$

which expresses that a 'metastable' limit and rate of convergence can be computed by M, and this *independently of the choice* of sequence $x_{(\cdot)}$, as suggested by the metastability trade-off. Thus, $\mathsf{MCT}_{\mathsf{meta}}$ is just (3) but with 'metastability' as in (2) replaced by 'metastable limit' as in (5). A natural question is then: Is the functional from $\mathsf{MCT}_{\mathsf{meta}}$ equally elementary as θ from (3)?

Now, that classically equivalent definitions behave differently in constructive or computable mathematics, is well-known. In this vein, the functional from $\mathsf{MCT}_{\mathsf{meta}}$ turns out to have quite strange computability theoretic properties, akin to the special fan functional, as we establish in the next theorems. Let $\mathsf{MCT}_{\mathsf{meta}}(M)$ be $\mathsf{MCT}_{\mathsf{meta}}$ with the leading existential quantifier removed and let μ^2 be Feferman's search operator ([2]) which yields a conservative extension of ACA_0.

Theorem 2 (ZFC) *A functional M satisfying $\mathsf{MCT}_{\mathsf{meta}}(M)$ can be computed from $\exists^3$ or $\Theta + \mu^2$. No type two functional can compute such a functional M. Any functional M as in $\mathsf{MCT}_{\mathsf{meta}}(M)$ computes Θ via a term of Gödel's T.*

Hence, $\exists^2$ cannot compute M from $\mathsf{MCT}_{\mathsf{meta}}$. However, by definition, $\mathsf{MCT}_{\mathsf{meta}}$ is at least as strong as the Big Five system ACA_0, and the former has quite strange Reverse Mathematics properties in the sense of Kohlenbach's *higher-order Reverse Mathematics* as in [5].

Theorem 3 $\mathsf{RCA}_0^\omega + (\mu^2)$ *proves* $(\exists\Theta^3)\mathsf{SCF}(\Theta) \leftrightarrow \mathsf{MCT}_{\mathsf{meta}}$ *while* $\mathsf{RCA}_0^\omega + \mathsf{WKL}$ *does not.*

Let UATR be ATR_0 where a functional computes the set obtained via transfinite recursion.

Theorem 4 $\mathsf{RCA}_0^\omega + (\exists\Theta)\mathsf{SCF}(\Theta)$ *proves* $\mathsf{UATR} \leftrightarrow (\mu^2)$ *while* $\mathsf{RCA}_0^\omega + \mathsf{WKL}$ *does not.*

Recall that a small number of equivalences in Reverse Mathematics are known to require a base theory *stronger* than RCA_0 and Hirschfeldt has asked whether there are more such equivalences (See [8]*§6.1). The previous theorem provides an affirmative, though perhaps unexpected, answer.

References

1. Jeremy Avigad, Edward T. Dean, and Jason Rute. A metastable dominated convergence theorem. *J. Log. Anal.*, 4, 2012.
2. Jeremy Avigad and Solomon Feferman. Gödel's functional ("dialectica") interpretation. pages 337–405, 1998.
3. R. O. Gandy. General recursive functionals of finite type and hierarchies of functions. *Ann. Fac. Sci. Univ. Clermont-Ferrand No.*, 35:5–24, 1967.
4. Albert E. Hurd and Peter A. Loeb. *An introduction to nonstandard real analysis*, volume 118 of *Pure and Applied Mathematics.* Academic Press Inc., 1985.
5. Ulrich Kohlenbach. Higher order reverse mathematics. pages 281–295, 2005.
6. Ulrich Kohlenbach and Angeliki Koutsoukou-Argyraki. Rates of convergence and metastability for abstract cauchy problems generated by accretive operators. *J. Math. Anal. Appl.*, 423(2):1089–1112, 2015.
7. John Longley and Dag Normann. *Higher-order Computability.* Theory and Applications of Computability. Springer, 2015.
8. Antonio Montalbán. Open questions in reverse mathematics. *Bull. Symbolic Logic*, 17(3):431–454, 2011.
9. Dag Normann and Sam Sanders. Nonstandard analysis, computability theory, and metastability. *In preparation*, 2017.

10. Dag Normann and Sam Sanders. Nonstandard analysis, computability theory, and their connections. *Submitted, Available from arXiv: https://arxiv.org/abs/1702.06556*, 2017.
11. Sam Sanders. The gandy-hyland functional and a hitherto unknown computational aspect of nonstandard analysis. *Submitted, Available from: http://arxiv.org/abs/1502.03622*, 2015.
12. Stephen G. Simpson. *Subsystems of second order arithmetic*. Perspectives in Logic. CUP, 2 edition, 2009.
13. Terence Tao. *Structure and randomness*. American Mathematical Society, Providence, RI, 2008. Pages from year one of a mathematical blog.
14. Benno van den Berg, Eyvind Briseid, and Pavol Safarik. A functional interpretation for nonstandard arithmetic. *Ann. Pure Appl. Logic*, 163(12):1962–1994, 2012.

The Minimalist Foundation and its impact on the working mathematician

Giovanni Sambin

Dipartimento di Matematica “Tullio Levi Civita”
University of Padova

Mathematics, in my view, is a human creation, obtained through a process of abstraction of mathematical concepts from reality. It is a result of evolution rather than the description of an absolute truth independent of us. Its effectiveness and objectivity are reached through a dynamic interaction between abstraction and application to reality. I have been developing such a perspective on mathematics, called *Dynamic Constructivism*, both in the actual development of mathematics [8] and its foundations [4–7] for over 25 years.

To obtain some metamathematical results (normalization, program-extraction, realizability interpretation) we have introduced a specific formal system called Minimalist Foundation (MF) [3, 1], which corresponds well to dynamic constructivism.

So, adopting dynamic constructivism in practice means doing mathematics in MF, or equivalently adhering to the following four principles.

1. Cultivate pluralism in mathematics and foundations. Different styles in abstraction, which means different foundations, produce different kinds of mathematics and should be respected. In particular, constructivism does not coincide with constructivization of classical mathematics; at least half of the work is to find proper definitions, corresponding to a different way of abstracting.

MF is compatible with the most relevant foundations (constructive type theory, calculus of construction, internal theory of toposes, axiomatic set theory, both classical and constructive, Feferman’s explicit mathematics) in the sense that each of them is obtained as an extension of MF.

2. Accept open notions and incomplete theories. Since the construction of mathematics is a never-ending process and nothing is given in advance, whatever makes the assumption that such a process can be blocked is rejected, such as a fixed universes of all sets, or of all subsets, or of all propositions.

Contrary to the common view, the fact that many notions are open-ended, intrinsically incomplete is not a limitation but a source of a more relaxed view and a deeper understanding. For instance, consistency of MF becomes a theorem, contrary to the case of axiomatic set theory ZFC.

3. Preserve all conceptual distinctions (no reductionism). When mathematics ceases to exist by itself, all its achievements (not only theorems or solutions to problems but also definitions, intuitions, conceptual distinctions, etc.) are the result of human struggle and thus become precious and must be kept, without reducing all to a single notion, like that of set.

As a consequence, many more primitive notions than usual are kept on stage. In particular, we will have the notions of set, collection and proposition, also in their form under assumptions (which produce the notions of operation, subset, relation, function, etc.).

4. Preserve all different levels of abstraction. It is a fact of life that communication can have different levels of reference, which in mathematics means the distinction between language and metalanguage, and different levels of abstraction, such as the computational, set-theoretic and algebraic modes.

For instance, intensional aspects live together with extensional ones, in the sense that MF has two levels of abstraction. The extensional level is as close as possible to the practice of constructive mathematics, while the intensional level admits a realizability interpretation [2]. The two levels are linked in accordance with the forget–restore principle, as proved in [1].

Contrary to common expectations (which push towards the strongest foundational theories possible), adopting MF has shown to be sufficient to do mathematics. It is even more interesting, and unexpected, that the actual development of topology over MF (see [8]) has revealed several deep structures which went unnoticed before and which will be listed and illustrated in second part of the actual talk.

In particular, it will be shown that absence of axiom of choice (and hence the distinction between operation and function) allow to conceive choice sequence (or streams) as ideal points of a pointfree Baire space.

References

1. M. E. Maietti. A minimalist two-level foundation for constructive mathematics. *Ann. Pure Appl. Logic*, 160(3):319–354, 2009.
2. M. E. Maietti and S. Maschio. An extensional Kleene realizability model for the Minimalist Foundation. In *20th International Conference on Types for Proofs and Programs, TYPES 2014*, pages 162–186, 2014.
3. M. E. Maietti and G. Sambin. Toward a minimalist foundation for constructive mathematics. In L. Crosilla and P. Schuster, editor, *From Sets and Types to Topology and Analysis: Practicable Foundations for Constructive Mathematics*, number 48 in Oxford Logic Guides, pages 91–114. Oxford University Press, 2005.
4. G. Sambin. Per una dinamica nei fondamenti. In G. Corsi and G. Sambin, editors, *Nuovi problemi della logica e della filosofia della scienza*, pages 163–210. CLUEB, Bologna, 1991.
5. G. Sambin. Steps towards a dynamic constructivism. In P. Gärdenfors, J. Wolenski, and K. Kijania-Placek, editors, *In the scope of Logic, Methodology and Philosophy of Science*, volume 1 of *Synthese Library 315*, pages 263–286. Kluwer, 2002.
6. G. Sambin. Two applications of dynamic constructivism: Brouwer's continuity principle and choice sequences in formal topology. In M. van Atten, P. Boldini, M. Bourdeau, and G. Heinzmann, editors, *One Hundred years of Intuitionism (1907-2007). The Cerisy Conference*, pages 301–315. Birkhäuser, 2008.
7. G. Sambin. Real and ideal in constructive mathematics. In P. Dybjer, S. Lindström, E. Palmgren, and G. Sundholm, editors, *Epistemology versus Ontology, Essays on the Philosophy and Foundations of Mathematics in honour of Per Martin-Löf*, volume 27 of *Logic, Epistemology and the Unity of Science*, pages 69–85. Springer, 2012.
8. G. Sambin. *Positive Topology and the Basic Picture. New structures emerging from constructive topology.* Oxford University Press, to appear.

Computing with infinite data via proofs

Helmut Schwichtenberg

LMU Munich, Germany

A real number can be represented as a Cauchy sequence $(a_n)_n$ of rationals together with a Cauchy modulus M satisfying

$$|a_n - a_m| \leq \frac{1}{2^p} \quad \text{for } n, m \geq M(p).$$

Arithmetical operations on real numbers x, y are defined by

	c_n	$L(p)$
$x + y$	$a_n + b_n$	$\max\bigl(M(p+1), N(p+1)\bigr)$
$-x$	$-a_n$	$M(p)$
$\|x\|$	$\|a_n\|$	$M(p)$
$x \cdot y$	$a_n \cdot b_n$	$\max\bigl(M(p+1+p_y), N(p+1+p_x)\bigr)$
$\frac{1}{x}$ for $\|x\| \in_q \mathbb{R}^+$	$\begin{cases} \frac{1}{a_n} & \text{if } a_n \neq 0 \\ 0 & \text{if } a_n = 0 \end{cases}$	$M(2(q+1)+p)$

where 2^{p_x} is the upper bound of x provided by the Archimedian property.

A computationally more interesting representation of real numbers is to view them as streams of signed digits $\mathrm{Sd} := \{-1, 0, 1\}$. The first task then is to define the arithmetical operations on these infinite data. This can be done directly, but it is a non-trivial task; see Wiedmer [7] and Ciaffaglione & di Gianantonio [4]. Here we consider an alternative, where the stream algorithms are extracted from proofs via realizability. Advantages are (i) that we can deal with mathematics (a constructive extension of real analysis) rather than computer science, and (ii) that (in case one uses a proof assistant to generate formal machine checked proofs) we can automatically verify the extracted programs.

For simplicity we work in the interval $[-1.1]$ (hence take the average function $\frac{x+y}{2}$ instead of addition) and consider proofs of

$$\begin{aligned}
&\forall^{\mathrm{nc}}_{x,y}(x, y \in {}^{\mathrm{co}}I \to \frac{x+y}{2} \in {}^{\mathrm{co}}I), \\
&\forall^{\mathrm{nc}}_{x,y}(x, y \in {}^{\mathrm{co}}I \to x \cdot y \in {}^{\mathrm{co}}I), \\
&\forall^{\mathrm{nc}}_{x,y}(x, y \in {}^{\mathrm{co}}I \to \frac{1}{4} \leq y \to \frac{x}{y} \in {}^{\mathrm{co}}I).
\end{aligned}$$

Here ${}^{\mathrm{co}}I$ is the greatest fixed point of an operator

$$\Phi(X) := \{\, x \mid \exists^{\mathrm{r}}_{d,x'}(d \in \mathrm{Sd} \land x' \in X \land x = \frac{x'+d}{2}) \,\}$$

satisfying the axiom

$$X \subseteq \Phi({}^{\mathrm{co}}I \cup X) \to X \subseteq {}^{\mathrm{co}}I \qquad \text{(coinduction)}.$$

A witness of the proposition $x \in {}^{\mathrm{co}}I$ then is a stream representing x, and consequently the computational content of the three proofs will be stream algorithms for the respective arithmetical operations. Notice that the reals x, y are not needed as input data of the algorithms; we therefore use the non-computational $\forall^{\mathrm{nc}}$ universal quantifier to bind them. For the average function such algorithms were informally obtained by Berger and Seisenberger [1] and formally by Miyamoto and Schwichtenberg [5]. Multiplication has been formally dealt with in Schwichtenberg [6]. The present paper reports on joint work with Hideki Tsuiki and Franziskus Wiesnet concerning division.

References

1. Ulrich Berger and Monika Seisenberger. Proofs, programs, processes. In F. Ferreira et al., editors, *Proceedings CiE 2010*, volume 6158 of *LNCS*, pages 39–48. Springer Verlag, Berlin, Heidelberg, New York, 2010.
2. Ulrich Berger, Kenji Miyamoto, Helmut Schwichtenberg, and Hideki Tsuiki. Logic for Gray-code computation. In D. Probst and P. Schuster, editors, *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, pages 69–110. De Gruyter, 2016.
3. Alberto Ciaffaglione. *Certified Reasoning on Real Numbers and Objects in Co-inductive Type Theory*. PhD thesis, Universita‘ degli Studi di Udine, Dipartimento di Matematica e Informatica, 2003.
4. Alberto Ciaffaglione and Pietro Di Gianantonio. A certified, corecursive implementation of exact real numbers. *Theoretical Computer Science*, 351:39–51, 2006.
5. Kenji Miyamoto and Helmut Schwichtenberg. Program extraction in exact real arithmetic. *Mathematical Structures in Computer Science*, 25:1692–1704, 2015.
6. Helmut Schwichtenberg. Logic for exact real arithmetic. To be submitted to the Proceedings of the workshop Mathematics for Computation, Niederaltaich, 2017.
7. Edwin Wiedmer. Computing with infinite objects. *Theoretical Computer Science*, 10: 133–155, 1980.