Mathematisches Forschungsinstitut Oberwolfach

Report No. 34/2020

DOI: 10.4171/OWR/2020/34

Mathematical Logic: Proof Theory, Constructive Mathematics (hybrid meeting)

Organized by
Samuel R. Buss, La Jolla
Rosalie Iemhoff, Utrecht
Ulrich Kohlenbach, Darmstadt
Michael Rathjen, Leeds

8 November – 14 November 2020

Abstract. The Workshop 'Mathematical Logic: Proof Theory, Constructive Mathematics' focused on proofs both as formal derivations in deductive systems as well as on the extraction of explicit computational content from given proofs in core areas of ordinary mathematics using proof-theoretic methods. The workshop contributed to the following research strands:

- Interactions between foundations and applications.
- Proof mining.
- Constructivity in classical logic.
- Modal logic and provability logic.
- Proof theory and theoretical computer science.
- Structural proof theory.

Mathematics Subject Classification (2010): 03Fxx.

Introduction by the Organizers

The workshop *Mathematical Logic: Proof Theory, Constructive Mathematics* was held November 8-14, 2020 in a hybrid format due to the Corona pandemic. It had 12 participants at the Oberwolfach Institute and 45 virtual participants who were connected via ZOOM. The program consisted of 31 talks of 30-40 minutes.

The purpose of the workshop was

To promote the interaction between the foundations of mathematics and applications to mathematics as done for example in the field of 'proof mining'. P. Pinto,

N. Pischke and A. Sipoş talked about applications of proof mining in the context of convex optimization and ergodic theory, while A. Nicolae reported on recent uses of proof theory in the context of geodesic geometry and the 'Lion-Man' game. P. Oliva presented effective bounds for convergence theorems from probability theory whereas T. Powell gave a quantitative analysis of some classical Tauberian theorems. Applications of proof theory in the context of algebra were reported in talks by T. Coquand, F. Ferreira, H. Lombardi, P. Schuster and D. Wessel. Talks on the interplay between foundational research in the context of reverse mathematics and core mathematics where given by A. Freund and A. Weiermann, who spoke about the strength of generalized forms of Goodstein's theorem, and by S. Sanders, who studied the uncountability of $\mathbb{R}$ in the context of higher order reverse mathematics. V. Brattka's talk investigated the Weihrauch complexity of discontinuous problems in analysis. On the more foundational side, M. Baaz discussed the issue of simplicity of proofs and the possibility of condensations of proofs and the use of axioms and rules by names and B. Afshari explored the connection between infinitary proofs, proofs with induction and cyclic proofs. B. van den Berg gave a new approach to specifying the computational content of the extensionality axiom in the language of finite types. R. Kahle gave an 'extended predicative' approach to introduce a Mahlo universe 'from below'. Y. Cheng discussed formal versions of Gödel's incompleteness theorems in the context of Robinson's theory R and R-like globalisers of theories. L. Kołodziejczyk studied Π^1_1-conservativity over collection principles and solved a problem of H. Towsner.

To explore connections between proof theory, constructive formal systems and computer science. M. Fujiwara's talk investigated the strength of different forms of the fan principle in the context of intuitionistic reverse mathematics. I. van der Giessen presented new admissibility results for rules in intuitionistic provability logics. S. Negri studied the proof theory of infinitary intuitionistic logic and its embedding into infinitary modal logic S4. A. Akbar Tabatabai discussed the BHK-interpretation as a spectrum of interpretations leading to different logics. M. E. Maietti proposed 'Minimalist Foundation' as a predicative foundation for constructive mathematics. On the applied side, A. Miquel discussed the connection between implicative algebras as a generalization of complete Heyting algebras and Krivine realizability. H. Schwichtenberg used a realizability technique to extract formally verified algorithms operating on stream representations of real numbers such as Gray code from proofs in constructive analysis.

To investigate further the connections between logic and computational complexity. E. Jeřábek discussed the formalizability of algorithms for iterated multiplication; he showed, with a delicate and intricate argument, that the theory VTC^0 for TC^0-computability can prove the correctness of the Hesse-Allender-Barrington algorithm. J. Krajíček's talk explored connections between propositional complexity and proof search algorithms, and proposed a method for comparing the strength of proof systems that is not sensitive to easily recognized sets of hard tautologies. I. Oitavem's talk gave recursion theoretic definitions of the counting class #P; her definitions were based on Cook-Bellantoni style safe-normal recursive definitions and can be extended to higher levels of the #P hierarchy.

Workshop (hybrid meeting): Mathematical Logic: Proof Theory, Constructive Mathematics

Table of Contents

Vasco Brattka
The Discontinuity Problem 1699

Anton Freund (joint with Juan Pablo Aguilera, Michael Rathjen and Andreas Weiermann)
Goodstein's theorem meets reverse mathematics 1701

Matthias Baaz
Note on the Benefit of Proof Representations by Name 1703

Andreas Weiermann (joint with Juan Pablo Aguilera, Anton Freund, Michael Rathjen)
What's so special about the Ackermann function and ATR_0*?* 1704

Emil Jeřábek
Iterated multiplication in VTC^0 1705

Leszek Kołodziejczyk (joint with Marta Fiori Carones, Tin Lok Wong, and Keita Yokoyama)
Conservativity over collection principles and a problem of Towsner 1707

Adriana Nicolae (joint with Ulrich Kohlenbach, Genaro López-Acedo)
A quantitative analysis of a discrete version of the lion and man game . 1709

Fernando Ferreira
Nilpotency: an algebraic experiment in proof mining 1710

Paulo Oliva (joint with Rob Arthan)
Quantitative Borel-Cantelli Lemmas, Erdős-Rényi Theorem and Kochen-Stone Theorem 1711

Yong Cheng (joint with Fedor Pakhomov)
Robinson's theory R *and a* R*-like Globaliser for c.e. theories* 1713

Sara Negri (joint with Matteo Tesi)
On the proof theory of infinitary logic 1716

Amir Akbar Tabatabai
On the Logical Shadow of the Explicit Constructions 1718

Iris van der Giessen (joint with Rosalie Iemhoff)
Admissibility in some intuitionistic provability logics 1720

Helmut Schwichtenberg (joint with Franziskus Wiesnet)
Proof and computation with infinite data 1722

Makoto Fujiwara
The decidable fan theorem in constructive and classical reverse mathematics 1724

Pedro Pinto (joint with Ulrich Kohlenbach)
Quantitative translations for viscosity approximation methods 1725

Maria Emilia Maietti
On minimality of the Minimalist Foundation 1727

Sam Sanders (joint with Dag Normann)
On the uncountability of $\mathbb{R}$ 1729

Thomas Powell
Quantitative Tauberian Theorems 1730

Peter Schuster (joint with Daniel Wessel)
Resolving finite indeterminacy 1731

Daniel Wessel (joint with Peter Schuster)
Radical theory of Scott-open predicates 1733

Andrei Sipoş
Two recent results in proof mining 1735

Nicholas Pischke (joint with Ulrich Kohlenbach)
Quantitative results for equilibrium problems 1737

Benno van den Berg (joint with Robert Passmann)
Converse extensionality and apartness 1738

Jan Krajíček
Proof search problem 1739

Isabel Oitavem (joint with Reinhard Kahle, Ugo dal Lago)
Towards #P 1741

Alexandre Miquel
Implicative algebras: completeness results 1743

Henri Lombardi
Geometric theories for constructive algebra 1744

Bahareh Afshari
Infinitary Proofs 1747

Thierry Coquand
Constructive remarks about the Theory of Central Simple Algebras 1748

Reinhard Kahle (joint with Anton Setzer)
Mahloness and Partial Functions 1749

Abstracts

The Discontinuity Problem

Vasco Brattka

There is a simplest discontinuous function $\mathsf{LPO}:\mathbb{N}^\mathbb{N}\to\{0,1\}$, which is the test for the zero sequence, i.e., the characteristic function of the set $\{0^\mathbb{N}\}$, also known as *limited principle of omniscience.* In fact, a function $F:\subseteq\mathbb{N}^\mathbb{N}\to\mathbb{N}^\mathbb{N}$ is discontinuous, if and only if LPO is continuously Weihrauch reducible to F [6, Lemma 8.2.6].

However, there are many discontinuous and hence non-computable multi-valued problems $f:\subseteq\mathbb{N}^\mathbb{N}\rightrightarrows\mathbb{N}^\mathbb{N}$ to which LPO is not reducible. Examples are the *intermediate value theorem* IMT or *weak Kőnig's lemma* WKL [3]. Hence, it is natural to ask the following question [1, Open Problem 5.9].

Question 1 (Schröder 2018)**.** *Is there a simplest discontinuous multi-valued problem $f:\subseteq\mathbb{N}^\mathbb{N}\rightrightarrows\mathbb{N}^\mathbb{N}$ in terms of continuous Weihrauch reducibility?*

More generally, by a *problem* $f:\subseteq X\rightrightarrows Y$ we mean a multi-valued map on represented spaces X,Y that admits a realizer. We call a problem *continuous*, if it has a continuous realizer and *computable* or *solvable*, if it has a computable realizer.

So far, the literature on Weihrauch complexity has known the *non-computability problem* $\mathsf{NON}:\mathbb{N}^\mathbb{N}\rightrightarrows\mathbb{N}^\mathbb{N},p\mapsto\{q\in\mathbb{N}^\mathbb{N}:q\not\leq_{\mathrm{T}}p\}$ and the *all-or-co-unique choice problem* $\mathsf{ACC}_\mathbb{N}$ (also known as $\mathsf{LLPO}_\mathbb{N}$) as the two most simple (but incomparable) discontinuous problems [4, 3].

We claim that the problem

$$\mathsf{DIS}:\mathbb{N}^\mathbb{N}\rightrightarrows\mathbb{N}^\mathbb{N},p\mapsto\{q\in\mathbb{N}^\mathbb{N}:\mathsf{U}(p)\neq q\}$$

is the simplest "natural" such problem, where $\mathsf{U}:\subseteq\mathbb{N}^\mathbb{N}\to\mathbb{N}^\mathbb{N}$ is a universal computable function. Indeed, DIS is a common lower bound of NON and $\mathsf{ACC}_\mathbb{N}$. Our claim is witnessed by a number of further results.

Theorem 1. *A problem $f:\subseteq X\rightrightarrows Y$ is effectively discontinuous if and only if $\mathsf{DIS}\leq_{\mathrm{W}}^* f$.*

Here $\leq_{\mathrm{W}}^*$ denotes the continuous version of Weihrauch reducibility and f is called *effectively discontinuous* if there is a continuous function $D:\mathbb{N}^\mathbb{N}\to\mathbb{N}^\mathbb{N}$ that witnesses discontinuity of f in the sense that for every potential realizer Φ_p of f the value $D(p)$ is an input for f on which f is not correctly realized by Φ_p. Here Φ denotes some standard representation of (certain) continuous functions $F:\subseteq\mathbb{N}^\mathbb{N}\to\mathbb{N}^\mathbb{N}$ with the property that $\Phi_p(q)=\mathsf{U}\langle p,q\rangle$.

The theorem above shows that DIS is at least the simplest effectively discontinuous problem in terms of Weihrauch reducibility. The theorem can be proved in Zermelo-Fraenkel set theory ZF with the axiom of dependent choice DC. If one adds the axiom of determinacy AD [5], then one can go further than that.

Theorem 2. *In* $\mathsf{ZF}+\mathsf{DC}+\mathsf{AD}$ *every problem* $f:\subseteq\mathbb{N}^{\mathbb{N}}\rightrightarrows\mathbb{N}^{\mathbb{N}}$ *is either continuous or effectively discontinuous.*

Hence, in $\mathsf{ZF}+\mathsf{DC}+\mathsf{AD}$ the problem DIS is actually the simplest discontinuous problem on Baire space. However, with the full axiom of choice AC it is easy to construct counterexamples to this claim.

Example 1. *In* $\mathsf{ZFC}=\mathsf{ZF}+\mathsf{AC}$ *there exists an (even parallelizable) total discontinuous problem* $f:\mathbb{N}^{\mathbb{N}}\rightrightarrows\mathbb{N}^{\mathbb{N}}$ *that is not effectively discontinuous.*

ZFC and $\mathsf{ZF}+\mathsf{DC}+\mathsf{AD}$ are known as alternative but incompatible axiomatic settings [5]. Hence, it is actually a matter of the axiomatic setting of how "natural" DIS appears as a simplest unsolvable problem.

Independent of the axiomatic setting, DIS happens to have a number of further very interesting properties, among those the following.

Theorem 3. $\widehat{\mathsf{DIS}}\equiv_{\mathrm{sW}}\mathsf{NON}$.

That is, the *parallelization* $\widehat{\mathsf{DIS}}$ of DIS is equivalent to the non-computability problem, which leads to the suggestive slogan that "non-computability is the parallelization of discontinuity". In fact, studying the discontinuity problem reveals further insights into the nature of the relation between continuity and computability.

One further relation between the discontinuous problems mentioned here is that it turns out that DIS is the summation of $\mathsf{ACC}_{\mathbb{N}}$. Here *summation* is a newly introduced interior operator in the Weihrauch lattice that plays a dual rôle to parallelization (and corresponds to the question mark operator ? from linear logic in the same sense as parallelization corresponds to the bang operator !). Hence, the three weakest discontinuous problems discussed here, $\mathsf{DIS},\mathsf{ACC}_{\mathbb{N}}$ and NON are surprisingly all related to each other in a purely algebraic way.

A preprint with all the main results stated here is available at [2].

References

[1] Measuring the Complexity of Computational Content: From Combinatorial Problems to Analysis (Dagstuhl Seminar 18361). Technical Report 9, Dagstuhl, Germany, 2019.

[2] V. Brattka. The Discontinuity Problem. *arXiv* 2020. `https://arxiv.org/abs/2012.02143`

[3] V. Brattka, G. Gherardi, and A. Pauly. Weihrauch complexity in computable analysis. In V. Brattka and P. Hertling, editors, *Handbook of Computability and Complexity in Analysis.* Springer, 2020. (to appear).

[4] V. Brattka, M. Hendtlass, and A. P. Kreuzer. On the uniform computational content of computability theory. *Theory of Computing Systems*, 61(4):1376–1426, 2017.

[5] Y. N. Moschovakis. *Descriptive Set Theory*, volume 155 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, Rhode Island, second edition, 2009.

[6] K. Weihrauch. *Computable Analysis.* Springer, Berlin, 2000.

Goodstein's theorem meets reverse mathematics

Anton Freund

(joint work with Juan Pablo Aguilera, Michael Rathjen and Andreas Weiermann)

Goodstein's theorem is famous as a concrete result about natural numbers that cannot be proved in Peano arithmetic. As such, it provides a natural example for the incompleteness phenomenon from Gödel's theorem.

In Goodstein's original formulation, his theorem did, in fact, involved universal quantification over infinite sets. Kirby and Paris managed to avoid this quantification, so that their independence result falls into the realm of first-order arithmetic (see [3] for references and discussion). Our new work [2] adds a variant of Goodstein's theorem that entails the existence of infinite sets and can thus be studied within reverse mathematics. This more abstract perspective has the advantage that it allows for very general results. Furthermore, we find it illuminating to have a spectrum of related results that range from the concrete (Kirby and Paris) over an intermediate realm (Goodstein's original work) to the rather abstract.

To describe our approach in some detail, we consider a non-decreasing function $b:\mathbb{N}\to\mathbb{N}$ ("base change") and a family $c=(c_i)_{i\in\mathbb{N}}$ of strictly increasing functions ("coefficient changes")

$$c_i:\{0,\dots,b(i)-1\}\to\{0,\dots,b(i+1)-1\}.$$

The simplest instance of our general result is concerned with Goodstein sequences $G^2_{b,c,m}(0),G^2_{b,c,m}(1),\dots$ that have start value $G^2_{b,c,m}(0):=m<2^{b(0)}$ and satisfy

$$\begin{aligned}&G^2_{b,c,m}(i+1):=2^{c_i(n_0)}+\dots+2^{c_i(n_k)}-1\\ &\text{for}\quad G^2_{b,c,m}(i)=2^{n_0}+\dots+2^{n_k}\quad\text{with}\quad b(i)>n_0>\dots>n_k.\end{aligned}$$

Note that the exponential notation in this example is non-hereditary, in contrast to Goodstein's original theorem. In view of the latter, it is natural to ask whether we always reach $G^2_{b,c,m}(i)=0$ for some $i\in\mathbb{N}$. The answer is negative, as $b(i):=2+i$, $c_i(n):=n+1$ and $m:=3$ lead to $G^2_{b,c,m}(i)=2^{i+1}+2^0$. To analyze the situation, we recall that the original theorem does not involve coefficient changes, which amounts to setting $c_i(n):=n$. For this definition of c_i, one obtains functions

$$e_i:\{0,\dots,b(i)-1\}\to X\quad\text{with}\quad e_{i+1}\circ c_i=e_i$$

by setting $X:=\mathbb{N}$ and $e_i(n):=n$. Indeed, this characterizes $\mathbb{N}$ as the direct limit over the functions c_i, as all natural numbers lie in the image of some e_i. In contrast, the direct limit that arises from $b(i)=2+i$ and $c_i(n)=n+1$ is given by $X=\{-n\,|\,n\in\mathbb{N}\}$. This is witnessed by $e_i(n):=-1-i+n$, since we have

$$e_{i+1}\circ c_i(n)=-1-(i+1)+n+1=e_i(n).$$

The point is that our example of a Goodstein sequence that does not reach zero leads to an ill founded limit, while Goodstein's original construction is associated with the well founded limit $\mathbb{N}$. This suggests an "extended Goodstein theorem", in which the limit over the c_i is always well founded and any countable well order can be obtained as such a limit. There is a relatively simple condition on b and

$c = (c_i)_{i\in\mathbb{N}}$ that ensures this property and does not refer to the limit explicitly (see [2]). When that condition is satisfied, we call (b, c) a Goodstein system. We can now state the simplest instance of our general result in reverse mathematics:

Theorem 1 ([2]). *The following are equivalent over RCA_0:*

(1) The extended Goodstein theorem for the binary notation: For any Goodstein system (b, c) and $m < 2^{b(0)}$, we have $G^2_{b,c,m}(i) = 0$ for some $i \in \mathbb{N}$.

(2) The Turing jump of any set exists (i. e., arithmetical comprehension holds).

The crucial idea of the proof is to extend the binary notation from natural numbers (which can be seen as finite orders $n = \{0, \ldots, n-1\}$) to arbitrary linear orders: For any such order X, let

$$2^X := \{\langle x_0, \ldots, x_{k-1}\rangle \mid x_0, \ldots, x_{k-1} \in X \text{ and } x_0 >_X \cdots >_X x_{k-1}\}$$

be the set of finite descending sequences in X, ordered lexicographically. It is known that statement (2) in the theorem above is equivalent to the assertion that 2^X is a well order whenever the same holds for X. The latter is equivalent to statement (1), as we show in [2].

The assertion that $X \mapsto 2^X$ preserves well orders is an example of a well ordering principle. In the literature, one can find many equivalences between such principles and important set existence axioms from reverse mathematics (see [2] for a list of references). This suggests a vast generalization of our result. However, there is one important caveat: Many well ordering principles map natural numbers to transfinite ordinals (consider $\alpha \mapsto \varepsilon_\alpha$). These will not induce Goodstein sequences of natural numbers. In [2], well ordering principles that do map natural numbers to initial segments of $\mathbb{N}$ (and have some other natural properties) are called Goodstein dilators. More precisely, we use the term "Goodstein dilator" for suitable transformations of natural numbers. If D is such a transformation, we obtain a transformation $X \mapsto \overline{D}(X)$ of arbitrary linear orders by taking direct limits. Each Goodstein dilator D gives rise to a Goodstein sequence $G^D_{b,c,m}(0), G^D_{b,c,m}(1), \ldots$ (see [2] for details). We can now state the promised general result:

Theorem 2 ([2]). *In RCA_0 one can prove that the following are equivalent for any Goodstein dilator D:*

(1) The extended Goodstein theorem for D: For any Goodstein system (b, c) and any start value $m \in D(b(0))$, we have $G^D_{b,c,m}(i) = 0$ for some $i \in \mathbb{N}$.

(2) The extension $X \mapsto \overline{D}(X)$ of D preserves well orders.

Theorem 1 is a straightforward instance, assuming the known result on $X \mapsto 2^X$. Let us point out that Abrusci, Girard and van de Wiele [1] have also considered general Goodstein sequences relative to dilators. However, they have not allowed coefficient changes, which means that their results stay in the "concrete" rather than the "abstract" realm.

In addition to Theorem 1, we have established a much more impressive instance of Theorem 2, which exhibits a Goodstein principle that is equivalent to arithmetical transfinite recursion. The crucial challenge was to slow down the Veblen hierarchy of normal function to a transformation of natural numbers. Amazingly, the slowed-down Veblen hierarchy turns out to be the Ackermann function. This part of our work has been presented in a talk by A. Weiermann at the same workshop (see his abstract in this report). Full details for all results can be found in [2].

References

[1] V. Michele Abrusci, Jean-Yves Girard and Jaques van de Wiele, *Some uses of dilators in combinatorial problems, part I*, Logic and Combinatorics (Stephen Simpson, ed.), Contemporary Mathematics, vol. 65, American Mathematical Society, 1987, pp. 25–53.

[2] Juan P. Aguilera, Anton Freund, Michael Rathjen and Andreas Weiermann, *Ackermann and Goodstein go functorial*, preprint available as `arXiv:2011.03439`, 2020, 36 pp.

[3] Michael Rathjen, *Goodstein's theorem revisited*, Gentzen's centenary: The quest for consistency (Reinhard Kahle and Michael Rathjen, eds.), Springer, 2015, pp. 229–242.

Note on the Benefit of Proof Representations by Name

Matthias Baaz

The up to date most profound revolution in mathematics has been the introduction of the axiomatic method by David Hilbert [4]. Its most important concept is the atomistic concept of proof: A proof is a sequence of formulas $A_1 \dots A_n$ such that for all i

- A_i is an instance of an axiom or
- A_i follows from $A_{j_1} \dots A_{j_k}$ by application of a rule.
- A_n is the result of the proof.

As such a sequence may contain arbitrary redundant subsequences not related to the result it is maybe more rewarding to deal with tree-like proofs, where the predecessor node / successor node relation determines the rule applications and all formulas in the proof are connected to the result. Tree-like proofs (a variation of Hilbert's concept) are the basis of proof theory since Gentzen [3], as long as proof theory is concerned with the transformation of concrete proofs. The reason is that tree-like proofs allow for regularity in a simple way (regularity is the unique use of eigenvariables). The disadvantage is of course that the same intermediary result might have two different subproofs if it is used twice in parallel.

No scientific revolution is however complete and global concepts of proofs persist. There are concepts where a global criterion for the soundness of the result exists, but subproofs may be unsound. In this note it is shown, that the proof representation by the names of axioms and rules as in Bourbaki (e.g. [2]) constitutes such a global concept: Abstract cut-elimination on the proof representation allows for a soundness proof of the result. The existence of a proof underlying a given representation is however undecidable, therefore the representation by names might be non-recursively simpler.

The optimal representation of proofs is a fundamental topic in mathematics and logic c.f. Hilbert's unpublished 24^{th} problem (the 24^{th} problem asks for the development of a criterion for the simplicity of proofs). Most simplifications of proofs are based on proof macros governed by meta-rules, as in MacLane's thesis

[5][1]. Such simplifications are proportional abbreviations and adhere to Hilbert's stepwise concept of proof. They are frequently used in mathematics in connection with explicit definitions, for example the integral is handled as an object.

Global representations of proofs as in this note allow for much stronger condensations of proofs. The complication is that external soundness criteria have to be employed. The representation in [1] leads to a more than elementary abbreviation of cut-free proofs. The representation in this note leads to a more than recursive abbreviation of proofs with cut.

References

[1] J.P. Aguilera, M. Baaz, *Unsound Inferences Make Proofs Shorter*, J. Symb. Log. **84(1)** (2019), 102–122.

[2] N. Bourbaki, *General Topology: Chapters 1–4* **18**, Springer Science & Business Media (2013).

[3] G. Gentzen, *Untersuchungen über das logische Schließen. I*, Mathematische Zeitschrift **39(1)**, Springer (1935), 176–210.

[4] D. Hilbert, *Grundlagen der Geometrie*, Teubner (1899).

[5] S. Mac Lane, *Abgekürzte Beweise im Logikkalkül*, Hubert (1934).

What's so special about the Ackermann function and $\mathbf{ATR_0}$?

Andreas Weiermann

(joint work with Juan Pablo Aguilera, Anton Freund, Michael Rathjen)

Let us define the Ackermann function as usual. So put $F_0(n) := n + 1$ and by recursion let $F_{a+1} := F_a^{n+1}(n)$ where the upper index denotes the number of iterations of the previously defined function F_a. It is well known that the function $a, b, c \mapsto F_a^b(c)$ is not primitive recursive. We show first that the function $a, b, c \mapsto F_a^b(c)$ acts like a dilator on numbers. Therefore this function extends uniquely to a function from linear orders to linear orders. In fact it becomes a functor which preserves direct limits and pull backs. Moreover it can be shown that this functor preservers well foundedness and so we see that the Ackermann function extends to a dilator.

The question is how strong the latter insight is from the viewpoint of reverse mathematics and the answer is provided by the following result.

Theorem 1. *We show that over the system* RCA_0 *the following assertions are equivalent.*

(1) The Ackermann function extends to a dilator.
(2) The binary Veblen function is a dilator.
(3) ATR_0.

Here RCA_0 and ATR_0 refer to the standard systems of reverse mathematics.

This result can be combined with results shown in the presentation by Anton Freund to show the following application to Goodstein principles.

[1] The author is grateful to the anonymous referee for the hint to MacLane's thesis which contains one of the few explicit discussions of proof macros with the corresponding rules in logic.

Theorem 2. *We show that over the system* RCA_0 *the following assertions are equivalent.*

(1) The extended Goodstein theorem holds for the Ackermann function.
(2) ATR_0.

References

[1] J. P. Aguilera, A. Freund, M. Rathjen, A. Weiermann *Ackermann and Goodstein go functorial*, https://arxiv.org/abs/2011.03439

Iterated multiplication in VTC^0

Emil Jeřábek

The underlying theme of this talk is *feasible reasoning* about the elementary integer arithmetic operations $+$, $\times$, $\leq$: what properties of these operations can be proven using only concepts whose complexity does not exceed that of $+$, $\times$, $\leq$ themselves? To make such questions formal, we can associate to any well-behaved complexity class C a theory of arithmetic T that "corresponds" to C, typically meaning that the provably total computable functions of T are the C-functions, and that T can reason with C-concepts: it proves induction, comprehension, minimization, or similar schemata for formulas that express C-predicates.

In our case, the right complexity class is (DLOGTIME-uniform) TC^0: the elementary arithmetic operations are computable in TC^0, and $\times$ is even TC^0-complete under AC^0 Turing-reductions. While TC^0 is easily seen to include $+$, $\times$, $-$, and iterated addition $\sum_{i<n} X_i$, it is much harder to show that it includes integer *division* and *iterated multiplication* $\prod_{i<n} X_i$, which was proved by Hesse, Allender, and Barrington [3], building on [1, 2]. The basic idea of [1] is to compute $\prod_i X_i$ in the *Chinese remainder representation* (*CRR*), i.e., modulo a sequence of small primes $\vec{m}$, and then reconstruct the result in binary from CRR; the main problem in getting the complexity down to fully uniform TC^0 is to devise an efficient CRR reconstruction procedure.

The basic theory corresponding to TC^0 is VTC^0, a Zambella-style two-sorted bounded arithmetic; a natural question (attributed to A. Atserias in [6]) is whether the theory can formalize TC^0 division and iterated multiplication algorithms. More precisely, we ask if VTC^0 proves the division axiom

$$(DIV) \qquad \forall X > 0\, \forall Y\, \exists Q\, \big(QX \leq Y < (Q+1)X\big),$$

and an axiom *IMUL* stating the existence of iterated products $\prod_{i<n} X_i$ satisfying the defining recurrence $\prod_{i<0} X_i = 1$, $\prod_{i<n+1} X_i = X_n \prod_{i<n} X_i$.

We know that $VTC^0 + IMUL$ proves DIV, and by [4], it is fairly powerful: it proves binary-number quantifier-free induction (*IOpen*), and even minimization for *RSUV* translations of Σ^b_0 formulas in Buss's language.

The argument in [3] does not just consist of a single algorithm—it has a complex structure with several interdependent parts:

(1) Show that $\prod_i X_i$ is in $\mathrm{TC}^0(\mathrm{pow})$, using CRR reconstruction. Here, pow denotes the function $a^r \bmod m$ with all inputs in unary, m prime.
(2) Show that $\prod_i X_i$ with polylogarithmically small input is in AC^0, by scaling down part (1).
(3) Show that pow is in AC^0 using (2), and plug it into (1).

However, what truly makes the formalization of [3] difficult is that the analysis of the algorithms suffers from "chicken or egg" problems (which came first, the chicken or the egg?):

- The proof of soundness of the CRR reconstruction procedure in part (1) heavily relies on iterated products and divisions: e.g., it refers to the product of primes from the CRR basis. But in VTC^0, we need the soundness of CRR reconstruction to define such iterated products in the first place.
- The analysis of the pow algorithm in part (3) refers to various modular powers, and even relies on Fermat's little theorem $a^{m-1} \equiv 1 \pmod{m}$. However, the latter cannot be stated, let alone proved, without having a means to define modular exponentiation in the first place.
- In part (1), the reduction of iterated modular multiplication $\mathrm{imul}(\vec{a}, m) = \prod_i a_i \bmod m$ (m prime) to pow relies on cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$, difficult to prove in bounded arithmetic. What makes this a chicken-or-egg problem is that the cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$ is in fact provable in $VTC^0 + \mathit{IMUL}$.

Despite these challenges, VTC^0 proves *IMUL* (specifically, the soundness of a variant of the algorithm from [3]), as recently shown in [5]. The formalization follows the basic outline above, adjusted to overcome the difficulties:

- Part (1) is formalized using imul as a primitive instead of pow, to postpone the issue of cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$: i.e., we prove *IMUL* in $VTC^0(\mathrm{imul})$. We get around chicken-or-egg problems by developing many low-level properties of CRR in $VTC^0(\mathrm{imul})$. This is the most technical part of the formalization.
- For part (2), polylogarithmic cuts of models of V^0 are models of *VNL*.
- We avoid the chicken-or-egg problems in part (3) by modifying the pow algorithm. We obtain a result of independent interest that there is a Δ_0 definition of pow (even for nonprime moduli) whose defining recurrence is provable in $I\Delta_0 + \mathit{WPHP}(\Delta_0)$.
- The results so far imply that *IMUL* is equivalent to the totality of imul, and to the cyclicity of $(\mathbb{Z}/m\mathbb{Z})^\times$. Paying attention to the size of parameters in this circle of implications, we can make progress on each turn using a partial formalization of the structure theorem for finite abelian groups. This allows to set up a final proof of *IMUL* in VTC^0 by induction.

Consequently, the results of [4] also apply to VTC^0.

References

[1] P. Beame, S. Cook, H. Hoover, *Log depth circuits for division and related problems*, SIAM Journal on Computing **15** (1986), no. 4, 994–1003.

[2] A. Chiu, G. Davida, B. Litow, *Division in logspace-uniform NC^1*, RAIRO – Theoretical Informatics and Applications **35** (2001), no. 3, 259–275.

[3] W. Hesse, E. Allender, D. Mix Barrington, *Uniform constant-depth threshold circuits for division and iterated multiplication*, Journal of Computer and System Sciences **65** (2002), no. 4, 695–716.

[4] E. Jeřábek, *Open induction in a bounded arithmetic for* TC^0, Archive for Mathematical Logic **54** (2015), no. 3–4, 359–394.

[5] E. Jeřábek, *Iterated multiplication in VTC^0*, arXiv:2011.03095 [cs.LO], 2020, 57 pp.

[6] P. Nguyen, S. Cook, *Theories for TC^0 and other small complexity classes*, Logical Methods in Computer Science **2** (2006), no. 1, article no. 3, 39 pp.

Conservativity over collection principles and a problem of Towsner

Leszek Kołodziejczyk

(joint work with Marta Fiori Carones, Tin Lok Wong, and Keita Yokoyama)

RCA_0 stands for the fragment of second-order arithmetic axiomatized by Δ^0_1 comprehension and Σ^0_1 induction. This is the usual base theory considered in reverse mathematics.

In [4], Towsner showed that for every $n \geq 1$, it is a Π_2-complete computational problem to decide whether a given Π^1_2 sentence ψ is Π^1_1-conservative over $\mathrm{RCA}_0 + \mathrm{I}\Sigma^0_n$ (here $\mathrm{I}\Sigma^0_n$ stands for Σ^0_n induction). He also asked whether the result is still true if Σ^0_n induction is replaced by the Σ^0_n collection principle, $\mathrm{B}\Sigma^0_n$. Recall that $\mathrm{B}\Sigma^0_n$ lies (strictly) between $\mathrm{I}\Sigma^0_{n-1}$ and $\mathrm{I}\Sigma^0_n$ in strength.

As stated, the question makes sense mainly for $n \geq 2$, because RCA_0 already contains $\mathrm{I}\Sigma^0_1$ as an axiom, so $\mathrm{RCA}_0 + \mathrm{B}\Sigma^0_1$ is simply RCA_0. To make also the case $n = 1$ meaningful, we replace RCA_0 with the weaker base theory RCA^*_0, which contains $\mathrm{B}\Sigma^0_1$ (and an axiom guaranteeing the totality of exponentiation) instead of $\mathrm{I}\Sigma^0_1$. Thus, we consider the following slight generalization of the question from [4].

Question. Given fixed $n \geq 1$, is the set

$$\{\psi \in \Pi^1_2 : \mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_n + \psi \text{ is } \Pi^1_1\text{-conservative over } \mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_n\}$$

Π_2-complete?

We show that the answer to this question is positive, but "barely so". More precisely, we obtain the following result.

Theorem. *For each $n \geq 1$:*

(a) *The set $\{\psi \in \Pi^1_2 : \mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_n + \psi$ is Π^1_1-conservative over $\mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_n\}$ is Π_2-complete.*

(b) *The set $\{\psi \in \Pi^1_2 : \mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_n + \neg\mathrm{I}\Sigma^0_n + \psi$ is Π^1_1-conservative over $\mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_n + \neg\mathrm{I}\Sigma^0_n\}$ is a consistent recursively axiomatized theory; in particular, it is recursively enumerable.*

To prove part (a) of the Theorem, we make use of so-called *cardinality principles*. The principle $\mathrm{C}\Sigma^0_n$ says that there is no number a for which there exists a Σ^0_n-definable injection from the entire natural number universe into $\{0,\dots,a\}$. We have the following:

Lemma. *For every* $n,k \geq 1$*:*

(i) $\mathrm{RCA}^*_0 + \mathrm{I}\Sigma^0_n + \neg\mathrm{C}\Sigma^0_{n+1}$ *is* Π^1_1*-conservative over* $\mathrm{RCA}^*_0 + \mathrm{I}\Sigma^0_n$*,*
(ii) $\mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_n + \neg\mathrm{I}\Sigma^0_n + \vdash \mathrm{C}\Sigma^0_k$*.*

Part (i) of the Lemma is an immediate consequence of some results of [4]. A proof of part (ii) was first described in [2]. The only proofs of (ii) that we know are model-theoretic. They are based on the idea, known from e.g. [3, 1], that models of $\mathrm{B}\Sigma^0_n + \neg\mathrm{I}\Sigma^0_n$ have "many" automorphisms. On the other hand, the existence of a witness to $\neg\mathrm{C}\Sigma^0_k$ (for whatever k) puts some nontrivial restrictions on the kinds of automorphism that a model may have.

Using the Lemma, we prove that, given a Π_2 arithmetical sentence $\forall x\, \exists y\, \delta(x,y)$, the Π^1_2 (in fact, Σ^1_1) statement

$\neg\mathrm{I}\Sigma^0_n \vee \big($"there exists a such that $\forall x \leq a\, \exists y\, \delta(x,y)$
and there exists a Σ^0_{n+1} injection from the set of all numbers into $[0,a]$"$\big)$

is Π^1_1-conservative over $\mathrm{RCA}^*_0 + \mathrm{I}\Sigma^0_n$ exactly if $\forall x\, \exists y\, \delta(x,y)$ is true.

The proof of part (b) of the Theorem also makes use of some model-theoretic methods, including expansions, saturation properties, and an isomorphism argument. Part (b) has a particularly striking form for $n = 1$: we show that a Π^1_2 sentence ψ is Π^1_1-conservative over $\mathrm{RCA}^*_0 + \mathrm{B}\Sigma^0_1 + \neg\mathrm{I}\Sigma^0_1$ if and only if $\mathrm{WKL}^*_0 + \neg\mathrm{I}\Sigma^0_1 \vdash \psi$, where WKL^*_0 extends RCA^*_0 by Weak König's Lemma.

As a byproduct of the proof of (b) for $n = 1$, we obtain an intriguing result about *restricted* Σ^1_1 formulas, i.e. formulas of the shape $\exists Y\, \forall x\, \exists y\, \delta(X,Y,x,y)$ (here δ is bounded and X is a free second-order variable). Namely, if $\sigma(X)$ is restricted Σ^1_1, then there exists an arithmetical formula $\alpha(X,Z)$ such that WKL^*_0 proves the following: for any sets X and Z, if some instance of $\mathrm{I}\Sigma^0_1$ with Z as the only second-order parameter fails, then $\sigma(X) \leftrightarrow \alpha(X,Z)$.

Note that, for example, "X is not a well-order" is a restricted Σ^1_1 formula. It follows that in models of WKL^*_0 in which induction fails for some lightface Σ^0_1 formula, being a well-order is an arithmetical property.

References

[1] Richard Kaye. Model-theoretic properties characterizing Peano arithmetic. *J. Symb. Log.*, 56(3):949–963, 1991.

[2] Leszek Aleksander Kołodziejczyk, Katarzyna W. Kowalik, and Keita Yokoyama. How strong is Ramsey's theorem if infinity can be weak?, 2020. Preprint, available at arXiv:2011.02550.

[3] Roman Kossak. On extensions of models of strong fragments of arithmetic. *Proc. Amer. Math. Soc.*, 108(1):223–232, 1990.

[4] Henry Towsner. On maximum conservative extensions. *Computability*, 4(1):57–68, 2015.

A quantitative analysis of a discrete version of the lion and man game

Adriana Nicolae
(joint work with Ulrich Kohlenbach, Genaro López-Acedo)

The lion and man problem, which goes back to R. Rado, is one of the most challenging pursuit-evasion games. In the inspiring book *Littlewood's Miscellany* [5] it is described as follows:

> *A lion and a man in a closed circular arena have equal maximum speeds. What tactics should the lion employ to be sure of his meal?*

The same book also contains a detailed discussion of the solution to this problem. Several variants of this game, both continuous and discrete, with applications in different fields such as robotics, biology, or random processes, have appeared in the literature.

In this talk, based on an interplay of ideas and techniques from logic and geometric analysis, we studied a discrete-time equal-speed pursuit-evasion game with an ε-capture criterion (in the sense that the pursuer gets within a distance less than ε to the evader). The domain X of our game is a geodesic space. Initially, the lion and the man are located at two points in X, L_0 and M_0, respectively. One fixes a positive upper bound D on the distance the lion and the man may jump. After n steps, the lion moves from the point L_n to the point L_{n+1} along a geodesic from L_n to M_n, that is $d(L_n, M_n) = d(L_n, L_{n+1}) + d(L_{n+1}, M_n)$, such that its distance to L_n equals $\min\{D, d(L_n, M_n)\}$. The man moves from the point M_n to any point $M_{n+1} \in X$ which is within distance D. Given a metric space, we say that the lion wins if $\lim_{n\to\infty} d(L_{n+1}, M_n) = 0$ for any pair of sequences $(L_n), (M_n)$ that satisfy the previous metric conditions for any $D > 0$. Otherwise the man wins.

In [1], a similar game is introduced for the particular case of uniquely geodesic spaces, so that the movement of the lion is completely determined by the movement of the man. The authors prove that in the setting of nonpositively curved bounded domains the lion always wins. Further advances in this problem were made, among others, in [6], where a characterization of compactness of the domain in terms of the success of the lion was obtained in complete, locally compact, strongly convex geodesic spaces. The main ingredient in the proof of this result is the fact that strongly convex spaces satisfy the betweenness property. However, none of these results provides any information on the speed of convergence towards 0 of the sequence $(d(L_{n+1}, M_n))$.

We focused in this talk on a quantitative uniform version of the aforementioned betweenness property and on its role in the analysis of the considered game. This allows the weakening of the topological and geometric hypotheses that ensure the success of the lion and the extraction of a rate of convergence for the sequence $(d(L_{n+1}, M_n))$ that only depends on a modulus quantifying the uniform betweenness property. Namely, the main result, stated in a purely metric setting, shows that, under the assumption of boundedness and uniform betweenness for the domain, the lion always wins. The result can be applied, e.g., in all uniformly convex normed spaces, CAT(κ) spaces (of sufficiently small diameter for $\kappa > 0$), or compact uniquely geodesic spaces satisfying the betweenness property, but also in some particular nonuniquely geodesic spaces. The obtained rate of convergence provides an explicit bound on the number of steps to be taken for an ε-capture.

The ideas that led to our results (which can be found in [4]) have their roots in proof mining. By 'proof mining' we mean the logical analysis, using proof-theoretic tools, of mathematical proofs with the aim of extracting relevant information hidden in the proofs. This new information can be both of quantitative nature, such as algorithms and effective bounds, as well as of qualitative nature, such as uniformities in the bounds or weakening of the premises. A comprehensive reference for proof mining is the book [2] (see also [3] for a recent survey).

References

[1] S. Alexander, R. Bishop, R. Ghrist, *Total curvature and simple pursuit on domains of curvature bounded above*, Geom. Dedicata **149** (2010), 275–290.

[2] U. Kohlenbach, *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*, Springer Monographs in Mathematics, Springer, Berlin-Heidelberg, 2008.

[3] U. Kohlenbach, *Proof-theoretic Methods in Nonlinear Analysis*, In: Proc. ICM 2018, B. Sirakov, P. Ney de Souza, M. Viana (eds.), Vol. 2, pp. 61-82. World Scientific 2019.

[4] U. Kohlenbach, G. López-Acedo, A. Nicolae, *A uniform betweenness property in metric spaces and its role in the quantitative analysis of the "Lion-Man" game*, Pacific J. Math. (accepted).

[5] J. E. Littlewood, *Littlewood's Miscellany* (ed: B. Bollobás), Cambridge University Press, Cambridge, 1986.

[6] G. López-Acedo, A. Nicolae, B. Piątek, *"Lion-Man" and the fixed point property*, Geom. Dedicata **202** (2019), 69–80.

Nilpotency: an algebraic experiment in proof mining

Fernando Ferreira

An element of a commutative ring with identity which lies in every prime ideal is nilpotent. This is a well-known result whose proof uses Zorn's lemma. A weakening of this fact is amenable to a proof mining analysis with the bounded functional interpretation, using bounded collection (instead of Zorn's lemma). We formulate a quantitative version of this weakening and obtain an explicit bound. We present an application.

Our proof mining analysis is the *leitmotif* for some comments and observations on the methodology of computational extraction. We emphasize that the formulation of quantitative versions of ordinary mathematical theorems is of *independent interest* from proof mining metatheorems. We also notice that, under the present type of analysis, the full result is not amenable to a quantitative analysis.

References

[1] F. Ferreira, *Injecting uniformities into Peano arithmetic*, Annals of Pure and Applied Logic **157** (1990), 122–129.

[2] P. Engrácia and F. Ferreira, *Bounded functional interpretation with an abstract type.* In: *Contemporary Logic and Computing*, editor A. Rezuş, pp. 87–112, College Publication, 2020.

[3] F. Ferreira, *Bounds for indexes of nilpotency in commutative ring theory: a proof mining approach*, to appear in The Bulletin of Symbolic Logic.

Quantitative Borel-Cantelli Lemmas, Erdős-Rényi Theorem and Kochen-Stone Theorem

Paulo Oliva
(joint work with Rob Arthan)

Let $(A_i)_{i=1}^{\infty}$ be an infinite sequence of events in a probability space $(\mathcal{S}, \mathcal{E}, P)$. The Borel-Cantelli lemma is a classical result in probability theory, relating the convergence or divergence of the sum $\sum_{i=1}^{\infty} P[A_i]$ with the probability of the event "A_i infinitely often", which is defined as follows:

$$A_i \text{ i.o.} = \bigcap_{n=1}^{\infty} \bigcup_{i \geq n} A_i$$

(i.e., $\omega \in \mathcal{S}$ happens infinitely often in $(A_i)_{i=1}^{\infty}$ if for all n there exists an $i \geq n$ such that $\omega \in A_i$).

The Borel-Cantelli lemma (see, for example, [2]) is normally presented in two parts. The first part says that when the sum $\sum_{i=1}^{\infty} P[A_i]$ converges, then A_i almost never occurs infinitely often:

Theorem 1 (First Borel-Cantelli Lemma)**.** *Let $(A_i)_{i=1}^{\infty}$ be an infinite sequence of events such that $\sum_{i=1}^{\infty} P[A_i] < \infty$. Then $P[A_i \textit{ i.o.}] = 0$.*

The second part says that when $\sum_{i=1}^{\infty} P[A_i]$ diverges, and when the A_i are mutually independent, then A_i almost always occurs infinitely often:

Theorem 2 (Second Borel-Cantelli Lemma)**.** *Let $(A_i)_{i=1}^{\infty}$ be an infinite sequence of mutually independent events such that $\sum_{i=1}^{\infty} P[A_i] = \infty$. Then $P[A_i \textit{ i.o.}] = 1$.*

In [3], Kochen and Stone presented a result that generalises the Second Borel-Cantelli Lemma in two directions: *(i)* it gives a lower bound on $P[A_i \text{ i.o.}]$ when the A_i are not mutually independent and *(ii)* it can be used to show that the assumption of mutual independence in the original lemma can be weakened to pairwise independence. We formulate this generalisation following Yan [4]:

Theorem 3 (Kochen-Stone)**.** *Let $(A_i)_{i=1}^{\infty}$ be an infinite sequence of events such that $\sum_{i=1}^{\infty} P[A_i] = \infty$. Then*

$$(1) \qquad P[A_i \textit{ i.o}] \geq \limsup_{n \to \infty} \frac{(\sum_{k=1}^{n} P[A_k])^2}{\sum_{i,k=1}^{n} P[A_i A_k]}$$

Erdős and Rényi [1] gave a result that is intermediate between the second Borel-Cantelli lemma and the Kochen-Stone theorem. Like the Kochen-Stone theorem it implies that the assumption of mutual independence in the second Borel-Cantelli lemma can be weakened to pairwise independence. Erdős and Rényi applied their theorem to the study of generalised Cantor expansions for real numbers.

Theorem 4 (Erdős-Rényi Theorem)**.** *Let* $(A_i)_{i=1}^{\infty}$ *be an infinite sequence of events such that* $\sum_{i=1}^{\infty} P[A_i] = \infty$ *and*

$$\liminf_{n\to\infty} \frac{\sum_{i,k=1}^{n} P[A_i A_k]}{(\sum_{k=1}^{n} P[A_k])^2} = 1 \tag{2}$$

Then $P[A_i \ i.o] = 1$*.*

In this talk I present the result of joint work with Rob Arthan on the following "quantitative" versions of the above theorems.

Theorem 5 (First Borel-Cantelli Lemma – Quantitative Version)**.** *Let* $(A_i)_{i=1}^{\infty}$ *be an infinite sequence of events. Assume that* $(\sum_{i=1}^{m} P[A_i])_{m=1}^{\infty}$ *converges with a rate of convergence* $\phi\colon \mathbb{N} \to \mathbb{N}^+$*, i.e. that for all* $l \geq 0$ *and* $m > \phi(l)$

$$\sum_{i=\phi(l)}^{m} P[A_i] \leq \frac{1}{2^l}$$

Then the sequence $(P[\bigcup_{i=1}^{m} A_i])_{m=1}^{\infty}$ *converges with the same rate, i.e. for all* $l \geq 0$ *and* $m > \phi(l)$

$$P\left[\bigcup_{i=\phi(l)}^{m} A_i\right] \leq \frac{1}{2^l}$$

Theorem 6 (Second Borel-Cantelli Lemma – Quantitative Version)**.** *Let* $(A_i)_{i=1}^{\infty}$ *be an infinite sequence of events which are mutually independent. Assume that the sequence* $(\sum_{i=1}^{n} P[A_i])_{n\in\mathbb{N}^+}$ *diverges with rate* $\omega\colon \mathbb{N}^+ \to \mathbb{N}^+$*, i.e. for all* N

$$\sum_{i=1}^{\omega(N)} P[A_i] \geq N$$

then, for all n *and* N*,*

$$P\left[\bigcup_{i=n}^{\omega(n+N-1)} A_i\right] \geq 1 - e^{-N}$$

Theorem 7 (Erdős-Rényi Theorem – Quantitative Version)**.** *Let* $(A_i)_{i=1}^{\infty}$ *be an infinite sequence of events. Let* $\omega\colon \mathbb{N}^+ \to \mathbb{N}^+$ *be such that for all* N

$$\left(\sum_{i=1}^{\omega(N)} P[A_i]\right) \geq N \tag{3}$$

and let $\phi\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ be such that

$$\forall l, n\left(\phi(l,n)\geq n \wedge \frac{\sum_{i,k=1}^{\phi(l,n)} P[A_iA_k]}{(\sum_{i=1}^{\phi(l,n)} P[A_i])^2}\leq 1+\frac{1}{2^l}\right) \tag{4}$$

Define $n_1=\phi(1,1)$ and, for $k>1$, $n_k=\phi(k,\max(n_{k-1},k))$. Then, for all n and l

$$P\left[\bigcup_{i=n}^{n_m} A_i\right]\geq 1-\frac{1}{2^l} \tag{5}$$

where $m=\max(\omega(2n), l+3)$.

Theorem 8 (Kochen-Stone Theorem – Quantitative Version)**.** *Let $(A_i)_{i=1}^{\infty}$ be an infinite sequence of events. Let $\omega\colon \mathbb{N}^+\to\mathbb{N}^+$ be such that for all N*

$$\left(\sum_{i=1}^{\omega(N)} P[A_i]\right)\geq N$$

Then, for all m and l and $g\colon \mathbb{N}^+\to\mathbb{N}^+$ such that $g(i)>i$, for all i, there exists an $n>m$ such that

- *$n\leq g^{(2^{l+1})}(\max(\omega(2^{l+2}\sum_{i=1}^{m} P[A_i]), m))$, and*
- *for all $j\in[n,g(n)]$*

$$P\left[\bigcup_{i=m+1}^{n} A_i\right]+\frac{1}{2^l}\geq\frac{(\sum_{i=1}^{j} P[A_i])^2}{\sum_{i,k=1}^{j} P[A_iA_k]} \tag{6}$$

References

[1] Pál Erdős and Alfréd Rényi. On Cantor's series with convergent $\sum 1/q_n$. *Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Math.*, 2:93–109, 1959.

[2] W. Feller. *An Introduction to Probability Theory and Its Applications. I. Third Edition.* John Wiley and Sons, Inc., 1968.

[3] S. Kochen and C. Stone. A note on the Borel-Cantelli lemma. *Ill. J. Math.*, 8:248–251, 1964.

[4] Jia-An Yan. A simple proof of two generalized Borel-Cantelli lemmas. In Michel Émery and Marc Yor, editors, *In memoriam Paul-André Meyer. Séminaire de probabilités XXXIX*, volume 1874 of *Lecture Notes in Mathematics*, pages 77–79. Springer, 2006.

Robinson's theory R and a R-like Globaliser for c.e. theories

Yong Cheng

(joint work with Fedor Pakhomov)

Robinson's theory **R** is introduced by Tarski, Mostowski and Robinson in [4].

Definition 1 (Tarski, Mostowski and Robinson)**.** *Robinson's theory* **R** *consists of schemes* Ax1-Ax5 *in the language $\{\mathbf{0},\mathbf{S},+,\times,\leq\}$ where $\leq$ is a primitive binary relation symbol and $\overline{n}=\mathbf{S}^n\mathbf{0}$ for $n\in\mathbb{N}$:*

Ax1: $\overline{m}+\overline{n}=\overline{m+n}$;
Ax2: $\overline{m}\times\overline{n}=\overline{m\times n}$;

Ax3: $\overline{m} \neq \overline{n}$, *if* $m \neq n$;
Ax4: $\forall x(x \leq \overline{n} \to x = \overline{0} \vee \cdots \vee x = \overline{n})$;
Ax5: $\forall x(x \leq \overline{n} \vee \overline{n} \leq x)$.

The notion of interpretation, originally introduced by Tarski, Mostowski and Robinson in [4], provides us with a method for comparing the strength of theories in different languages.[1] Let T be a recursively axiomatizable consistent theory. We say that $\mathsf{G1}$ *holds for* T if for any recursively axiomatizable consistent theory S, if T is interpretable in S, then S is incomplete (see [2]). We show that $\mathsf{G1}$ holds for T if and only if T is essentially undecidable (see [2]). We know that $\mathbf{R}$ is essentially undecidable and hence $\mathsf{G1}$ holds for $\mathbf{R}$. A natural question is: can we find a theory T such that $\mathsf{G1}$ holds for T and $T \lhd \mathbf{R}$?

Theorem 2 (Cheng, [2])**.** *For any recursively inseparable pair $\langle A, B\rangle$, there is a r.e. theory $U_{\langle A,B\rangle}$ such that $U_{\langle A,B\rangle} \lhd \mathbf{R}$ and $\mathsf{G1}$ holds for $U_{\langle A,B\rangle}$.*

It is natural to examine the structure $\mathsf{D} = \{S : S \lhd \mathbf{R}$ and $\mathsf{G1}$ holds for theory $S\}$. It is open whether $\langle \mathsf{D}, \lhd\rangle$ is well founded (or is it that for any $S \in \mathsf{D}$, there is $T \in \mathsf{D}$ such that $T \lhd S$)? However, the answer for the structure $\overline{\mathsf{D}} = \{S : S <_T \mathbf{R}$ and $\mathsf{G1}$ holds for theory $S\}$ is known.

Theorem 3 (Cheng, [2])**.** *The structure $\overline{\mathsf{D}}$ is not well founded. I.e. there is no minimal theory below $\mathbf{R}$ w.r.t. Turing reducibility such that $\mathsf{G1}$ holds for it.*

For a consistent theory T, we say $\mathsf{G2}$ holds for T if $T \nvdash \mathbf{Con}(T)$. Pudlák shows that there is no consistent r.e. theory S such that $(\mathbf{Q} + \mathbf{Con}(S)) \unlhd S$. A natural question is whether $\mathsf{G2}$ holds for $\mathbf{R}$. Since $\mathbf{Con}(\mathbf{R})$ is a Π^0_1 sentence, by the MRDP theorem, $\mathbf{Con}(\mathbf{R})$ is equivalent to $\forall x(P_1(x) \neq P_2(x))$ for some polynomials P_1 and P_2 over $\mathbb{N} \setminus \{0\}$. If we equate $\mathbf{Con}(\mathbf{R})$ with $\forall x(P_1(x) \neq P_2(x))$, we can show that $\mathbf{R} \nvdash \mathbf{Con}(\mathbf{R})$.

The following is a joint work with Fedor Pakhomov in [3].

Definition 4 (Interpretations of models)**.** *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be countable first-order languages. Suppose U is a $\mathcal{L}_1$-theory, $\mathfrak{N}$ is a $\mathcal{L}_1$-model and $\mathfrak{M}$ is a $\mathcal{L}_2$-model. An interpretation τ of U in $\mathfrak{M}$ consists of $\mathfrak{M}$-definable set $D_\tau \subseteq |\mathfrak{M}|$ (the domain of interpretation), $\mathfrak{M}$-definable set $P^\tau \subseteq (D_\tau)^n$ for each n-ary predicate symbol P from $\mathsf{Sgn}(U)$, and $\mathfrak{M}$-definable function $f^\tau : (D_\tau)^n \to D_\tau$ for each n-ary function symbol f from $\mathsf{Sgn}(U)$ such that $(D_\tau, \langle P^\tau | P \in \mathsf{Sgn}(U)\rangle, \langle f^\tau | f \in \mathsf{Sgn}(U)\rangle) \models U$. Similarly, we can define that τ is an interpretation of $\mathfrak{N}$ in $\mathfrak{M}$ if $(D_\tau, \langle P^\tau | P \in \mathsf{Sgn}(\mathfrak{N})\rangle, \langle f^\tau | f \in \mathsf{Sgn}(\mathfrak{N})\rangle) \cong \mathfrak{N}$.*

We require D_τ to be a definable set in $\mathfrak{M}$ in the above Definition. Depending on what exactly we consider to be a definable set we will get different notions of interpretations. We say τ is one-dimensional if $D_\tau \subseteq |\mathfrak{M}|$; we say τ is multi-dimensional if $D_\tau \subseteq |\mathfrak{M}|^n$ for some $n \in \omega$; we say τ is piece-wise multi-dimensional if D_τ is a

[1] Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be countable first-order languages. Let U be an $\mathcal{L}_1$-theory and T be an $\mathcal{L}_2$-theory. We write $T \unlhd U$, if T is interpretable in U; we write $T \lhd U$ if T is interpretable in U, but U is not interpretable in T.

disjoint union $A_1 \sqcup A_2 \sqcup \cdots \sqcup A_n$ of definable sets $A_1 \subseteq |\mathfrak{M}|^{i_1}, \cdots, A_n \subseteq |\mathfrak{M}|^{i_n}$; we say τ is a factor interpretation (piece-wise multi-dimensional with definable equality) if D_τ is $(A_1 \sqcup A_2 \sqcup \cdots \sqcup A_n)/\sim$, where $A_1 \subseteq |\mathfrak{M}|^{i_1}, \cdots, A_n \subseteq |\mathfrak{M}|^{i_n}$ are definable sets and $\sim$ is a definable equivalence relation on $A_1 \sqcup A_2 \sqcup \cdots \sqcup A_n$. In this work, we consider interpretations in most general sense (piece-wise multi-dimensional interpretations with definable equality).

Definition 5 (Interpretations of theories)**.** *Let $\mathcal{L}_1$ and $\mathcal{L}_2$ be countable first-order languages. Let U be an $\mathcal{L}_1$-theory and T be an $\mathcal{L}_2$-theory. An interpretation of U in T is an uniformly defined family of interpretations $\langle \tau_\mathfrak{M} : \mathfrak{M} \models T \rangle$ where $\tau_\mathfrak{M}$ is an interpretation of U in $\mathfrak{M}$ for any $\mathfrak{M} \models T$. Here, "uniformly defined" means that the corresponding components of all $\tau_\mathfrak{M}$ should be definable sets/functions given by the same formula in all $\mathfrak{M} \models T$.*

Definition 6 (Globaliser of a c.e. theory)**.** *A globaliser of a c.e. theory T is a c.e. theory U such that for any c.e. theory S, S is locally interpretable in T if and only if S is interpretable in U.*[2]

Visser shows that the theory R is a globalizer of EQ (the theory of pure equality). A natural question is: does any c.e. theory has a globaliser? The answer is positive. Pakhomov and Visser recently show that for any c.e. theory T, there is a globaliser $G(T)$ of T. However, the globaliser $G(T)$ of T constructed in this theorem is very abstract and not an analogue of Robinson's theory R.

The motivation of our work is to construct a concrete globaliser of c.e. theories that is a natural analogue of Robinson's theory R. The theory $\mathcal{R}(T)$ we construct, a natural analogue of Robinson's theory R, is a weak set theory with urelements. The general idea is to generalize Robinson's theory R to the case with urelements. The theory $\mathcal{R}(T)$ corresponds to constructible sets $L(\mathfrak{M}, \omega)$ over structures $\mathfrak{M} \models T$ in the same way as R corresponds to natural numbers.

Now, we first define the constructible hierarchy over $\mathfrak{M}$ via Gödel's operations $\mathcal{F}_1(x, y), \cdots, \mathcal{F}_N(x, y)$.[3] Define $\mathsf{L}(\mathfrak{M}, 0) = |\mathfrak{M}|$, $\mathsf{L}(\mathfrak{M}, \alpha + 1) = \mathsf{L}(\mathfrak{M}, \alpha) \cup \{\mathsf{L}(\mathfrak{M}, \alpha)\} \cup \{\mathcal{F}_i(x, y) : 1 \leq i \leq N \text{ and } x, y \in \mathsf{L}(\mathfrak{M}, \alpha) \cup \{\mathsf{L}(\mathfrak{M}, \alpha)\}\}$ and $\mathsf{L}(\mathfrak{M}, \lambda) = \bigcup_{\alpha<\lambda} \mathsf{L}(\mathfrak{M}, \alpha)$ for limit λ (see [1]). This gives us the same class of constructible sets: $\mathsf{L}(\mathfrak{M}) = \bigcup_{\alpha \in \mathsf{On}} \mathsf{L}(\mathfrak{M}, \alpha)$. Further, we will use well-founded linear preorder $\leq_\mathsf{L}$ on $\mathsf{L}(\mathfrak{M}, \omega)$ that is $x \leq_\mathsf{L} y \Leftrightarrow \forall n(y \in \mathsf{L}(\mathfrak{M}, n) \to x \in \mathsf{L}(\mathfrak{M}, n))$.

Now, we define the theory $\mathcal{R}(T)$. WLOG, we assume that T is a c.e. theory with finite predicate-only signature. The signature of $\mathcal{R}(T)$ consists of all predicates from $\mathsf{Sgn}(T)$, predicate $x \in y$, constant Ur, binary functions $\mathcal{F}_1, \cdots, \mathcal{F}_N$ for Gödel operations, unary function $\mathcal{E}$,[4] and binary predicate $\leq_\mathsf{L}$. Terms $\underline{\mathsf{L}_0} = \mathsf{Ur}$ and $\underline{\mathsf{L}_{n+1}} = \mathcal{E}(\underline{\mathsf{L}_n})$ denote finite levels of constructible hierarchy.

[2] We say a theory T is locally interpretable in a theory U if any finite sub-theory T' of T is interpretable in U.

[3] For the definition of $\mathcal{F}_1(x, y), \cdots, \mathcal{F}_N(x, y)$, we refer to [1] and [3].

[4] The intended interpretation for $\mathcal{E}$ is $\mathcal{E} : b \mapsto b \cup \{b\} \cup \{\mathcal{F}_i(x, y) \mid 1 \leq i \leq N,\ x, y \in b \cup \{b\}\}$.

Definition 7. *For each n we denote as $\underline{\mathsf{L}_n}$ the term $\mathcal{E}^n(\mathsf{Ur})$. The axioms of $\mathcal{R}(T)$ are:*

(1) T^{Ur}*, i.e. relativizations to* Ur *of all axioms of* T*;*

(2) $R(x_1, \ldots, x_n) \to x_1 \in \mathsf{Ur} \wedge \ldots \wedge x_n \in \mathsf{Ur}$*, for predicate symbols* R *from the signature of* T*;*

(3) $x \in \mathsf{Ur} \to y \notin x$*;*

(4) $x \notin \mathsf{Ur} \wedge y \notin \mathsf{Ur} \wedge \forall z(z \in x \leftrightarrow z \in y) \to x = y$ *(Extensionality);*

(5) $x \in \underline{\mathsf{L}_{n+1}} \leftrightarrow x \in \underline{\mathsf{L}_n} \vee x = \underline{\mathsf{L}_n} \vee \bigvee\limits_{1 \le i \le N} \exists y, z(x = \mathcal{F}_i(y, z) \wedge (y \in \underline{\mathsf{L}_n} \vee y = \underline{\mathsf{L}_n}) \wedge (z \in \underline{\mathsf{L}_n} \vee z = \underline{\mathsf{L}_n}))$*, for all* n *(defining axioms for* $\underline{\mathsf{L}_{n+1}}$*);*

(6) Series of axioms $\mathcal{F}_i\text{-}\mathsf{Def}_n$*, for natural* n *and* $1 \le i \le N$*, stating that* $\mathcal{F}_i(x, y)$ *works on* $x, y \in \underline{\mathsf{L}_n}$*;*

(7) $x \in \underline{\mathsf{L}_n} \wedge y \le_{\mathsf{L}} x \to \bigvee\limits_{m \le n} y \in \underline{\mathsf{L}_m}$*, for all natural* n*;*

(8) $x \in \underline{\mathsf{L}_n} \to y \le_{\mathsf{L}} x \vee x \le_{\mathsf{L}} y$.

We prove the following main theorem that generalizes the well known theorem that R is a globaliser of EQ.

Theorem 8 (Cheng and Pakhomov, [3])**.** *For any c.e. theory* T*, the theory* $\mathcal{R}(T)$ *is a globaliser of* T*.*

References

[1] Jon Barwise, *Admissible sets and structures: An approach to definability theory,* Perspectives in Mathematical Logic Volume 7, Berlin: Springer-Verlag, 1975.

[2] Yong Cheng, *Finding the limit of incompleteness I*, Accepted and to appear in The Bulletin of Symbolic Logic, Doi: 10.1017/bsl.2020.09, see arXiv:1902.06658v2, 2020.

[3] Yong Cheng and Fedor Pakhomov, *A* R*-like Globaliser for c.e. theories*, preprint, 2020.

[4] Alfred Tarski, Andrzej Mostowski and Raphael M. Robinson, *Undecidabe theories*, Studies in Logic and the Foundations of Mathematics, North-Holland, Amsterdam, 1953.

On the proof theory of infinitary logic

Sara Negri
(joint work with Matteo Tesi)

Our first aim is to obtain a sequent calculus with good structural and analytical properties for intuitionistic infinitary logic, i.e., intuitionistic logic extended with countable disjunctions and conjunctions. Existing calculi [5, 6] have restrictions on the rules of implications and infinitary conjunction that make the respective rules non-invertible.

Often, the methods of labelled deduction allow to overcome such difficulties. However, the labelled calculus for (finitary) intuitionistic propositional logic [1] internalizes Kripke semantics, that does not have a viable infinitary generalization for intuitionistic logic. In fact, Kripke frames correspond to Alexandroff topologies, i.e. topologies closed under infinitary intersections, and thus validate the infinitary distributivity property

$$\bigwedge_{k>0}(P_k \vee Q) \to \bigwedge_{k>0} P_k \vee Q$$

which is not intuitionistically valid [3].

We introduce a neighbourhood semantics for infinitary intuitionistic logic which simplifies the neighbourhood semantics for (finitary) intuitionistic logic introduced in [2]: in fact, we consider neighbourhood frames which contain the unit and are closed under supersets and *finite*, rather than infinite, intersections. The latter condition maintains validity of the finite distributivity law, but does not entail validity of its infinitary version.

By internalizing neighbourhood semantics along the lines of [4] we obtain a labelled sequent calculus, called $G3I_\omega$, for intuitionistic infinitary logic. The calculus fully meets our desiderata, i.e., height-preserving admissibility of weakening and contraction as well as cut admissibility and invertibility of all the rules. The calculus also presents intuitionistic logic as an extension rather than as a restriction of classical logic.

Completeness of the new semantics is proved both indirectly, through equivalence with a complete topological semantics, and directly, through the labelled calculus: in fact, invertibility of the rules permits a Tait-Schütte-Takeuti-style completeness proof via the construction of a neighbourhood countermodel for a non-terminating branch in a failed proof-search tree.

Finally, we present an infinitary version of the modal logic $S4$, and introduce an infintary extension of the Gödel-McKinsey-Tarski translation from intuitionistic logic into $S4$ [1]. The translation is proved to be sound, in the sense that if a formula is a theorem of intuitionistic infinitary logic, then its translation is a theorem of the infinitary $S4$ system. The converse direction, namely faithfulness of the translation, is proved by induction on the height of derivations in the labelled calculus for infinitary modal logic $G3S4_\omega$ based, likewise, on neighbourhood semantics.

References

[1] R. Dyckhoff, S. Negri, *Proof analysis in intermediate logics*, Archive for Mathematical Logic **51** (2012), 71–92.

[2] M. Moniri, F. S. Maleki , *Neighborhood semantics for basic and intuitionistic logic*, Logic and Logical Philosophy **24** (2015), 339–355.

[3] M. Nadel, *Infinitary intuitionistic logic from a classical point of view*, Annals of Mathematical Logic **14** (1978), 159–191.

[4] S. Negri, *Proof theory for non-normal modal logic: The neighbourhood formalism and basic results*, IfCoLog Journal of Logics and their Applications **4** (2017), 1241–1286.

[5] S. Negri, *Geometric rules in infinitary logic*, in Arnon Avron on Semantics and Proof Theory of Non-Classical Logics, Outstanding Contributions to Logic, Springer, in press.

[6] M. Rathjen, *Remarks on Barr's theorem: Proofs in geometric theories*, In D. Probst and P. Schuster (eds) *Concepts of Proof in Mathematics, Philosophy, and Computer Science*, Series: Ontos Mathematical Logic 6, De Gruyter (2016), 347–374.

On the Logical Shadow of the Explicit Constructions

Amir Akbar Tabatabai

> "*It is equally stupid and simple to consider mathematics to be just an axiom system as it is to see a tree as nothing but a quantity of planks.*" L.E.J. Brouwer

In the intuitionistic tradition, mathematics has been considered as an incomplete story of our mental constructions and logic as the collection of the story's universal laws is nothing but a distorted incomplete shadow of the real mathematics. This role is clearly far from the foundational role that logic is usually believed to play. In the work we present here, we try to address this Brouwerian extrinsic interpretation of logic.

To formalize this interpretation, we have to first formalize the following two ingredients. First, the *constructions* that mathematics is supposed to be based on and then the *interpretation* that translates the logical formulas into the realm of the previously fixed constructions. For the former, there are many reasonable choices to make, including the computable functions formalized inside the standard model or HA, the set-theoretical functions in IZF or CZF, the terms in Martin Löf type theory or the morphisms in some strong enough categories such as locally Cartesian closed categories or toposes. In this talk and for the sake of simplicity, we set the functions in IZF as our fixed notion of construction. For the interpretations, though, we apparently have no choice but the canonical candidate of the BHK interpretation. However, we believe that the BHK interpretation is not a singular specific interpretation, but a name for a spectrum of different interpretations leading to different logics. Let us explain more, by introducing the two ends of the spectrum: The Heyting and the Brouwer interpretations:

Definition 1. *A Heyting interpretation is a map that assigns two sets $[A]_0$ and $[A]_1$ to any propositional formula A, such that:*

- *$[p]_1$ and $[\bot]_1$ are inhabited, $[p]_0 \subseteq [p]_1$, for any atomic formula p and $[\bot]_0 = \emptyset$,*
- *$[A \wedge B]_1 = [A]_1 \times [B]_1$ and $[A \wedge B]_0 = \{(x, y) \in [A \wedge B]_1 \mid x \in [A]_0 \wedge y \in [B]_0\}$,*
- *$[A \vee B]_1 = [A]_1 + [B]_1$ and $[A \vee B]_0 = \{(i, x) \in [A \vee B]_1 \mid (i = 0 \to x \in [A]_0) \wedge (i = 1 \to x \in [B]_0)\}$,*
- *$[A \to B]_1 = [B]_1^{[A]_1}$ and $[A \to B]_0 = \{f \in [A \to B]_1 \mid \forall x \in [A]_0\; f(x) \in [B]_0\}$.*

The sets $[A]_0$ and $[A]_1$ informally refer to the sets of the actual and possible constructions for A, respectively. A Brouwer interpretation is defined exactly in the same way, except for the disjunction case that is defined by: $[A \vee B]_1 = \|[A]_1 + [B]_1\|$, where $\| - \|$ is the propositional truncation, i.e., $\|X\| = \{x \in \{0\} \mid \exists y \in X\}$ and $[A \vee B]_0 = \{x \in \{0\} \mid \exists y \in [A]_0 \vee \exists y \in [B]_0\}$.

Given a construction for a disjunction, Heyting interpretation provides the complete information of the proved disjunct and the construction used for that proof. On the polar opposite side, the Brouwer interpretation uses the propositional truncation to collapse all the possible information in the construction, except probably its mere existence and hence no non-trivial information remained in a proof of a disjunction in this interpretation. This difference in the disjunction case is where the aforementioned spectrum enters the scene. Briefly, based on different amount of information that we assume a construction of a disjunction stores, we can develop different BHK interpretations.

Standing anywhere in the mentioned spectrum, it is also possible to restrict ourselves to a subclass of the interpretations to see how different conditions on the constructions lead to different logics. To have some examples, let us introduce the following classes of interpretations. An interpretation is called:

- **Markov**, if $\neg\neg\exists x \in [p]_0 \to \exists x \in [p]_0$, for any atomic formula p,
- **Kolmogorov**, if $[p]_1$ is an external finite set and $\neg\neg(x \in [p]_0) \to (x \in [p]_0)$, for any atomic formula p,
- **Proof-irrelevant**, if the condition that $[p]_0$ is inhabited implies $[p]_0 = [p]_1$, for any atomic formula p, i.e., if p has an actual proof, then all of its possible proofs are actual.

With the appropriate notions of construction and interpretation, we are ready to formalize what we mean by the theory and the logic of a calculus of constructions:

Definition 2. *Let $\mathcal{C}$ be a definable class of Heyting interpretations. By the $\mathcal{C}$-Heyting theory of* IZF*, denoted by $\mathbf{T}^H_{\mathcal{C}}(\mathsf{IZF})$, we mean the set of all propositional formulas A such that $\mathsf{IZF} \vdash \forall[-] \in \mathcal{C}\ \exists x \in [A]_0$, and by $\mathbf{L}^H_{\mathcal{C}}(\mathsf{IZF})$, we mean the set of all propositional formulas A such that $\sigma(A) \in \mathbf{T}^H_{\mathcal{C}}(\mathsf{IZF})$, for any propositional substitution σ. Similarly, define $\mathcal{C}$-Brouwer theory and logic of* IZF*, denoted by $\mathbf{T}^B_{\mathcal{C}}(\mathsf{IZF})$ and $\mathbf{L}^B_{\mathcal{C}}(\mathsf{IZF})$, respectively.*

Theorem 3. *Using M, K and PI to refer to the classes of Markov, Kolmogorov and proof-irrelevant interpretations, respectively, we have:*

- *(Brouwerian Constructivism)* $\mathbf{T}^B(\mathsf{IZF}) = \mathbf{T}^B_{PI}(\mathsf{IZF}) = \mathbf{L}^B_{MPI}(\mathsf{IZF}) = \mathbf{L}^B_K(\mathsf{IZF}) = \mathsf{IPC}$ *and* $\mathbf{T}^B_{MPI}(\mathsf{IZF}) = \mathsf{IPC} + \{\neg\neg p \to p \mid p \textit{ is an atom}\}$.
- *(Heyting's Constructivism)* $\mathbf{T}^H(\mathsf{IZF}) \supseteq \mathsf{KP}$*, where* $\mathsf{KP} = \mathsf{IPC} + (\neg A \to B \vee C) \to (\neg A \to B) \vee (\neg A \to C)$*. Therefore,* $\mathbf{T}^H(\mathsf{IZF}) \neq \mathsf{IPC}$ *and* $\mathbf{T}^H_{PI}(\mathsf{IZF}) = \mathsf{INP}$*, where* $\mathsf{INP} = \mathsf{IPC} + (A \to B \vee C) \to (A \to B) \vee (A \to C)$ *for any $\vee$-free formula A.*
- *(Russian Constructivism)* $\mathbf{L}^H_{MPI}(\mathsf{IZF}) = \mathbf{L}^H_K(\mathsf{IZF}) = \mathsf{ML}$*, where* ML *is Medvedev logic and* $\mathbf{T}^H_{MPI}(\mathsf{IZF}) = \mathsf{KP} + \{\neg\neg p \to p \mid p \textit{ is an atom}\}$.

Admissibility in some intuitionistic provability logics

Iris van der Giessen
(joint work with Rosalie Iemhoff)

In this talk I present ongoing work on the admissibility of two intuitionistic provability logics; intuitionistic Gödel-Löb logic (iGL) and strong Löb logic (iSL). Both logics have a close connection to the (unknown!) provability logic of Heyting Arithmetic. The logics are well-understood in terms of sequent calculi and semantics. Our goal is to understand the structure of all inferences of these logics in terms of their admissible rules. The bad news is that the current methods that we tried so far are not sufficient to establish nice results for iGL. The very good news is that for iSL we establish a full description of its admissible rules.

Classically, Gödel-Löb logic GL admits a provability interpretation for Peano Arithmetic, but it is an open problem what the provability logic of Heyting Arithmetic is. Logic GL consists of classical modal logic K extended by the Gödel-Löb axiom $\Box(\Box A \to A) \to \Box A$. iGL is obtained by restricting GL to intuitionistic propositional tautologies and iSL is iGL plus the completeness principle $A \to \Box A$. Logic iGL is sound with respect to the provability logic of Heyting Arithmetic, but not complete. In [10] it is shown that iSL is the provability logic of an extension of Heyting Arithmetic that has a link with slow provability. In addition, iSL plays an important role in the Σ_1-provability logic for Heyting Arithmetic [1].

Logics iGL and iSL are natural intuitionistic counterparts of GL for semantic and proof-theoretic reasons. The Kripke semantics for iGL is a natural combination of intuitionistic propositional logic and modal logic where the modal relation has the classical GL properties: transitive and conversely well-founded [9]. The completeness principle in iSL corresponds to the strong condition that the modal relation is a subset of the intuitionistic relation. In [4] and [5], single-conclusion sequent calculi for iGL and iSL have been developed. For these calculi the papers provide non-trivial syntactic proofs of cut-elimination, termination and Craig interpolation.

In this talk we explore iGL and iSL in terms of admissible rules. Admissible rules are those rules under which the set of theorems of a logic is closed. In other words, adding such a rule to a logic, does not change the set of formulas that can be derived in that logic. For example, the rule $\Box A/A$ is admissible in many normal modal logics, including iGL and iSL. Admissible rules are interesting to study, because they give insight in the structure of all possible inferences in a logic. In addition, adding an admissible rule to a system may give shorter proofs. Our goal is to provide nice descriptions of all admissible rules in iGL and iSL.

An important ingredient to reach the goal is the connection between so-called projective formulas and the extension property of Kripke models. Projective formulas are important in the study of admissible rules, because for those formulas, admissibility and derivability coincide. The extension property is a useful semantic characterization for projective formulas in many logics. Ghilardi establishes this correspondence for IPC and transitive classical modal logics such as GL [2, 3]. We have established the same result for iSL. The problem for iGL is still open.

Very recently, we have established a full description of the admissible rules for iSL (not yet published). We describe the admissible rules in terms of a proof system for the admissible rules of iSL. We use the same strategy from Iemhoff and Metcalfe [7], who provide Gentzen-style proof systems for admissibility for IPC and several modal logics such as GL. These proof systems consist of rules that reason about rules. This in contrast to the well-known sequent calculi for logics that reason about formulas. In this sense, proof systems for admissibility can be considered to reason about objects 'one level higher'. Such proof systems are very useful in obtaining decidability and complexity results for admissibility. In order to prove soundness and completeness with respect to admissibility in iSL, we use the connection between projective formulas and the extension property.

Admissible rules are usually described in terms of a basis. A basis is a set of admissible rules that derive all other admissible rules in the logic. For example, Iemhoff [6] shows that the so-called Visser rules form a basis for the admissible rules for IPC. Jeřábek [8] defines so-called modal Visser rules for classical modal logics including GL. We strongly conjecture that we can extract a basis from our proof system for admissibility for iSL that is a kind of fusion of the Visser rules for IPC and the modal Visser rules for GL. Also in this sense we can say that iSL is a natural intuitionistic version of GL.

For iGL we expect that more tools are needed in order to give a description of all admissible rules. All we know is that the admissible rules in iSL are admissible in iGL, but there are examples of rules that are admissible in iGL but not in iSL.

References

[1] M. Ardeshir and M. Mojtahedi, *The Σ_1-provability logic of HA*, Annals of Pure and Applied Logic **169**(10) (2018), 997–1043.

[2] S. Ghilardi, *Unification in intuitionistic logic*, The Journal of Symbolic Logic **64**(2) (1999) 859–880.

[3] S. Ghilardi, *Best solving modal equations*, Annals of Pure and Applied Logic **102**(3) (2000) 183–198.

[4] I. van der Giessen and R. Iemhoff, *Sequent calculi for intuitionistic Gödel-Löb logic*, Notre Dame Journal of Formal Logic, accepted for publication.

[5] I. van der Giessen and R. Iemhoff, *Proof theory for intuitionistic strong Löb logic*, arXiv (2020) `arXiv:2011.10383 [math.LO]`.

[6] R. Iemhoff, *On the admissible rules of intuitionistic propositional logic*, The Journal of Symbolic Logic **66**(1) (2001) 281–294.

[7] R. Iemhoff and G. Metcalfe, *Proof theory for admissible rules*, Annals of Pure and Applied logic **159**(1–2) (2009) 171–186.

[8] E. Jeřábek, *Admissible rules of modal logics*, Journal of Logic and Computation **15**(4) (2005) 411–431.

[9] T. Litak, *Constructive modalities with provability smack*. In: G. Bezhanishvili, ed., Leo Esakia on Duality in Modal and Intuitionistic Logics. Outstanding Contributions to Logic **4** (2014), 179–208.

[10] A. Visser and J. Zoethout, *Provability logic and the completeness principle*, Annals of Pure and Applied Logic **170**(6) (2019), 718-753.

Proof and computation with infinite data

Helmut Schwichtenberg
(joint work with Franziskus Wiesnet)

Real numbers in the exact (as opposed to floating-point) sense can be defined as Cauchy sequences (of rationals, with modulus). However, for computational purposes it is better to see them as coded by "streams" of signed digits $\{1, 0, -1\}$. A variant stream representation is the so-called "binary reflected" or Gray-code [8, 13]. Apart from being practically more useful, the stream view turns real numbers into "infinite data" and hence objects of type level 0. As a consequence the type level of other concepts in constructive analysis [4] is lowered by one, which simplifies matters considerably.

Our overall goal is to obtain formally verified algorithms (given by terms in our language) operating on stream represented real numbers. Given an informal idea of how the algorithm should work, there are two methods how this can be achieved.

(I) Formulate (using corecursion) the algorithm in the term language of a suitable theory, and then formally prove that this term satifies the specification;

(II) Find a formal existence proof M (using coinduction) for the object the algorithm is supposed to return. Then apply a proof theoretic method ("realizability") to extract M's computational content as a term (involving corecursion) in the term language of the underlying theory. The verification is done by a formal soundness proof of the realizability interpretation. The extraction of the computational content and the verification are automatic.

A general advantage of (II) over (I) is that one does not need to begin with a detailed formulation of the algorithm, but instead can stay on a more abstract level when proving the (existential) specification. In mathematics we know how to organize proofs, for instance by splitting them into lemmas or on occasion make use of more abstract concepts. In short, mathematical experience can help to find a well-structured algorithmic solution.

Method (I) was employed in [5] using Coq, and method (II) in [2, 9, 3] using Minlog[1].

We will work with constructive existence proofs in the style of [4], but in such a way that we can switch on and off the availability of input data for the constructions implicit in the proof [1]. In the present context this will be applied to real numbers as input data: we do not want to make use of the Cauchy sequence for the constructions to be done, but only the computational content of an appropriate coinductive predicate to which the real number is supposed to belong to. We consider division of real numbers as a non-trivial case study; it has been dealt with in [5] using method (I). Based on the algorithmic idea in [5], we employ

[1] http://minlog-system.de.

method (II) to extract signed digit and Gray code based stream algorithms for division from proofs that the reals are closed under division (under some obvious restrictions). In comparison with [9, 3] we have the following contributions.

- The central soundness theorem [10, p.340] is treated as a "meta" theorem w.r.t. realizability. It only deals with "object proofs" not involving realizability predicates, which is a reasonable restriction under practical aspects. We use axioms stating that every computationally relevant formula is *invariant* under realizability, formally $A \leftrightarrow \exists_z(z \mathbf{r} A)$. Such axioms already appear in [7] under the name (A-r) "to assert is to realize". A proof of this soundness theorem is given, where the need of invariance axioms is clearly visible.
- Instead of viewing the real numbers as abstractly given objects with all the necessary properties assumed as axioms we now use concrete real numbers (Cauchy sequences with moduli). The difficulty here is that for all real functions and predicates compatibility with the defined real equality has to be proven[2]; this is sometimes referred to as the "setoid hell". This problem can of course be avoided by dealing with real numbers axiomatically, as in [9, 3]. However, for the task of fully verified software reliance on such an axiom system is problematic, and needs to be backed by a careful analysis of the axiom system. This is what we essentially do.
- As already said, based on an algorithmic idea in [5] we extract stream algorithms for real division from proofs. However, to turn this idea into a formal proof for concrete real numbers was a non-trivial task. As a benefit from the necessary organization into a sequence of lemmas we obtain a relatively easy analysis of the "look-ahead", i.e., how far we have to look into the argument streams to obtain the n-th digit of the result stream.

References

[1] U. Berger. Program extraction from normalization proofs. In M. Bezem and J. Groote, editors, *Typed Lambda Calculi and Applications*, volume 664 of *LNCS*, pages 91–106. Springer Verlag, Berlin, Heidelberg, New York, 1993.

[2] U. Berger. From coinductive proofs to exact real arithmetic. In E. Grädel and R. Kahle, editors, *Computer Science Logic*, volume 5771 of *LNCS*, pages 132–146. Springer Verlag, Berlin, Heidelberg, New York, 2009.

[3] U. Berger, K. Miyamoto, H. Schwichtenberg, and H. 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.

[4] E. Bishop. *Foundations of Constructive Analysis*. McGraw-Hill, New York, 1967.

[5] A. Ciaffaglione and P. D. Gianantonio. A certified, corecursive implementation of exact real numbers. *Theoretical Computer Science*, 351:39–51, 2006.

[6] Y. L. Ershov. Model C of partial continuous functionals. In R. Gandy and M. Hyland, editors, *Logic Colloquium 1976*, pages 455–467. North-Holland, Amsterdam, 1977.

[7] S. Feferman. Constructive theories of functions and classes. In K. M. M. Boffa, D. van Dalen, editor, *Logic Colloquium 78*, volume 97 of *Studies in Logic and the Foundations of Mathematics*, pages 159–224. North-Holland, Amsterdam, 1979.

[2] Files `nat.scm`, `pos.scm`, `int.scm`, `rat.scm`, `rea.scm` in the directory `minlog/lib`

[8] P. D. Gianantonio. An abstract data type for real numbers. *Theoretical Computer Science*, 221(1-2):295–326, 1999.

[9] K. Miyamoto and H. Schwichtenberg. Program extraction in exact real arithmetic. *Mathematical Structures in Computer Science*, 25:1692–1704, 2015.

[10] H. Schwichtenberg and S. S. Wainer. *Proofs and Computations.* Perspectives in Logic. Association for Symbolic Logic and Cambridge University Press, 2012.

[11] D. Scott. Outline of a mathematical theory of computation. Technical Monograph PRG–2, Oxford University Computing Laboratory, 1970.

[12] D. Scott. Domains for denotational semantics. In E. Nielsen and E. Schmidt, editors, *Automata, Languages and Programming*, volume 140 of *LNCS*, pages 577–613. Springer Verlag, Berlin, Heidelberg, New York, 1982.

[13] H. Tsuiki. Real number computation through Gray code embedding. *Theoretical Computer Science*, 284:467–485, 2002.

[14] F. Wiesnet. Konstruktive Analysis mit exakten reellen Zahlen. Master's thesis, Mathematisches Institut der Universität München, 2017.

[15] F. Wiesnet. Introduction to Minlog. In K. Mainzer, P. Schuster, and H. Schwichtenberg, editors, *Proof and Computation*, pages 233–288. World Scientific, 2018.

The decidable fan theorem in constructive and classical reverse mathematics

Makoto Fujiwara

In this workshop, I gave a talk about my recent work [1] on constructive reverse mathematics (cf. [2]) with respect to the decidable fan theorem, which plays an important role in constructive mathematics.

In constructive mathematics, it is widely-known that the decidable fan theorem $\mathrm{FAN_D}(\mathrm{T}_{01})$ for the complete binary tree $\{0,1\}^*$ is equivalent to the general decidable fan theorem $\mathrm{FAN_D}$ (cf. Section 4.7.5 of [3]). On the other hand, in the context of classical reverse mathematics (cf. [4]), König's lemma KL, a sort of contrapositive of $\mathrm{FAN_D}$, is strictly stronger than weak König's lemma WKL which is a sort of contrapositive of $\mathrm{FAN_D}(\mathrm{T}_{01})$. This seemingly paradoxical situation occurs because the countable (unique) choice is accepted in constructive mathematics (cf. Section 4.1.6 of [3]) but only the restricted version $\mathrm{QF\text{-}AC}^{0,0}$ is contained in the base theory $\mathsf{RCA_0}$ of classical reverse mathematics.

To figure out the proper relation between $\mathrm{FAN_D}$, $\mathrm{FAN_D}(\mathrm{T}_{01})$, KL and WKL, we investigated the interrelation between these principles over the intuitionistic counterpart $\mathsf{EL_0}$ (containing only $\mathrm{QF\text{-}AC}^{0,0}$) of $\mathsf{RCA_0}$. For each $\mathrm{P} \in \{\mathrm{FAN_D}, \mathrm{FAN_D}(\mathrm{T}_{01}), \mathrm{KL}, \mathrm{WKL}\}$, let dn-P denote the variant of P where the double negation $\neg\neg$ is inserted in front of the conclusion of P. Then we showed that dn-$\mathrm{FAN_D}$ and dn-$\mathrm{FAN_D}(\mathrm{T}_{01})$ are equivalent to dn-KL and dn-WKL respectively over $\mathsf{EL_0}$ augmented with the double negation shift principle for function quantifiers restricted to formulas of Σ^0_1 form:

$$\forall f^{\mathbb{N}\to\mathbb{N}} \neg\neg\exists y^{\mathbb{N}} A_{\mathrm{qf}}(f,y) \to \neg\neg\forall f^{\mathbb{N}\to\mathbb{N}} \exists y^{\mathbb{N}} A_{\mathrm{qf}}(f,y),$$

where A_{qf} is quantifier-free. From these results, it turns out that some countable choice principle is necessary to derive $\mathrm{FAN_D}$ from $\mathrm{FAN_D}(\mathrm{T}_{01})$. For the purpose of characterizing the choice principle which is necessary and sufficient for deriving

$\mathrm{FAN_D}$ from $\mathrm{FAN_D(T_{01})}$, we introduced a choice principle $\mathrm{BT_{fb}}$ which is defined in terms of some notions on countable trees, and showed that KL is equivalent to WKL plus $\mathrm{BT_{fb}}$ over $\mathsf{EL_0}$ plus some additional induction principles. In addition, $\mathrm{FAN_D}$ is derived from $\mathrm{FAN_D(T_{01})}$ plus $\mathrm{BT_{fb}}$ over $\mathsf{EL_0}$. On the other hand, it is still open whether $\mathrm{FAN_D}$ derives $\mathrm{BT_{fb}}$ constructively without using strong countable choice principles. See [1] for more details.

According to the outcome of our investigation, the equivalents of $\mathrm{FAN_D}$ in constructive (reverse) mathematics can be classified into some different classes if one works over a constructive theory containing only weak countable choice principles (e.g. $\mathsf{EL_0}$ or $\mathsf{HA}^\omega + \text{QF-AC}^{1,0}$). At the end of this talk, I illustrated this phenomenon in a concrete study of the uniform continuity theorem [5], which is from my joint work with Tatsuji Kawai.

References

[1] M. Fujiwara, *König's lemma, weak König's lemma, and the decidable fan theorem*, submitted, 2020.

[2] H. Ishihara, *Constructive reverse mathematics: compactness properties*, In: *From sets and types to topology and analysis*, volume **48** of Oxford Logic Guides, pages 245–267, Oxford Univ. Press, Oxford, 2005.

[3] A. S. Troelstra and D. van Dalen, *Constructivism in mathematics, An introduction*, Vol. I, volume 121 of Studies in Logic and the Foundations of Mathematics. North Holland, Amsterdam, 1988.

[4] S. G. Simpson. *Subsystems of second order arithmetic*, Perspectives in Logic. Cambridge University Press, Cambridge, second edition, 2009.

[5] M. Fujiwara and T. Kawai, *Decidable fan theorem and uniform continuity theorem with continuous moduli*, submitted, 2020.

Quantitative translations for viscosity approximation methods

Pedro Pinto
(joint work with Ulrich Kohlenbach)

Proof mining is a research program that employs proof theoretical tools to obtain additional information from mathematical results ([1]). Its techniques have been applied successfully to many areas of Mathematics with special focus on Nonlinear Analysis. One well known strongly convergent algorithm in Fixed Point Theory is due to Halpern [2]. Let X be a Banach space and C a nonempty, closed and convex subset. Consider T a nonexpansive map on C (i.e. $\|T(x)-T(y)\| \leq \|x-y\|$ for all $x, y \in C$), and $(\alpha_n) \subset [0,1]$ a sequence of real numbers. With u (the anchor point), and x_0 given points in C, the Halpern iteration is defined recursively by

$$\text{(H)} \qquad x_{n+1} := \alpha_n u + (1-\alpha_n)T(x_n).$$

The strong convergence of the Halpern iteration towards a fixed point of T has been extensively studied and was generalized in several different ways. Introduced by Moudafi [3], the viscosity approximation method is one such generalization in which the anchor point of the iteration is replaced by a strict contraction map, i.e. by a map ϕ satisfying $\forall x, y \in C(\|\phi(x) - \phi(y)\| \leq r\|x - y\|)$, for some $r \in [0, 1)$,

$$\text{(vH)} \qquad x_{n+1} := \alpha_n \phi(x_n) + (1 - \alpha_n)T(x_n).$$

The study of these iterations is highly relevant with applications in many practical optimization problems. In [4], Suzuki showed that the convergence of the generalized viscosity version (vH) can be reduced to the convergence of the original iteration (H). In such strong convergence results, one usually looks for metastability rates, i.e. a function $\varphi : (0, \infty) \times \mathbb{N}^{\mathbb{N}} \to \mathbb{N}$ satisfying

$$(1) \qquad \forall \varepsilon > 0 \forall f \in \mathbb{N}^{\mathbb{N}} \exists n \leq \varphi(\varepsilon, f) \forall i, j \in [n, f(n)] \ (\|x_i - x_j\| \leq \varepsilon)\,,$$

or for Cauchy rates (the particular case where the rate of metastability does not depend on the counterfunction f). The quantitative analysis of Suzuki's result concerns the analysis of a $\Pi^0_3 \to \Pi^0_3$ statement and its proof-theoretical interpretation translates classically (via a negative translation) into a transformation of a rate of metastability for the original iteration into a metastability rate for the viscosity version. Such quantitative transformation is explicitly extracted and, furthermore, the analysis reveals that one of Suzuki's conditions was superfluous. Moreover, the quantitative result largely also holds in a geodesic setting. These qualitative improvements point to the success of Proof mining in the generalization of proofs. By an inspection of the quantitative proof it is possible to see that the counterfunction f does not play any special role (beyond the one inherited from the metastability hypothesis). Hence, if we begin with a Cauchy rate for the Halpern iterations, the quantitative transformation will output also a Cauchy rate for the viscosity versions. This entails that Suzuki's arguments are essentially constructive which was not obvious a priori. This is in line with previous observations by Kohlenbach (e.g. in [5]) that by interpreting a proof (even a constructive one) in a classical way one obtains stronger results without any loss of information. Some examples of applications are given: instantiating our result with metastability rates for Halpern style iterations (from [6][7][8][9]) one obtains metastability rates for the corresponding viscosity version.

Lastly, we discuss a particular instance where it is possible to obtain a Cauchy rate for the Halpern iteration (H). A modulus of uniqueness for being a fixed point of a map $T : C \to C$ is a function $\omega : (0, \infty) \to (0, \infty)$ satisfying

$$(2) \qquad \forall \varepsilon > 0 \forall x, y \in C \ (\|x - T(x)\|, \|y - T(y)\| \leq \omega(\varepsilon) \to \|x - y\| \leq \varepsilon)\,.$$

In many cases, one can obtain rates of convergence ρ for $\|x_n - T(x_n)\| \to 0$, usually called rates of asymptotic regularity. It is well-known that in those situations, a modulus of uniqueness ω entails the existence of a Cauchy rate for (x_n):

$$(3) \qquad \forall \varepsilon > 0 \forall i, j \geq \rho(\omega(\varepsilon)) \ (\|x_i - x_j\| \leq \varepsilon)\,.$$

In [10], Gwinner introduced the following notion of a uniform accretive operator (here $A = \mathrm{Id} - T$, for T a nonexpansive map on C): there is a strictly increasing function $\varphi : [0, \infty) \to \mathbb{R}$ such that $\lim_{t\to\infty} \varphi(t) = \infty$ and for all $x, y \in C$

$$(4) \qquad \exists j \in J(x - y) \left(\langle A(x) - A(y), j\rangle \geq (\varphi(\|x\|) - \varphi(\|y\|)) \cdot (\|x\| - \|y\|) \right),$$

where J is the normalized duality map of X. Under this assumption, in the setting of uniformly convex Banach spaces, we extract a modulus of uniqueness from Gwinner's uniqueness proof. Using a rate of asymptotic regularity from [11], we finish the talk with an application of this result to obtain a Cauchy rate for the Halpern iteration (and thus also for the viscosity version) when $\alpha_n = \frac{1}{n+1}$.

References

[1] U. Kohlenbach, *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*, Springer Monographs in Mathematics. Springer-Verlag Berlin Heidelberg, 2008.

[2] B. Halpern, *Fixed points of nonexpanding maps*, Bulletin of the American Mathematical Society, **73**(6): 957-961, 1967.

[3] A. Moudafi, *Viscosity approximation methods for fixed-points problems*, Journal of Mathematical Analysis and Applications, **241**(1): 46-55, 2000.

[4] T. Suzuki, *Moudafi's viscosity approximations with Meir-Keeler contractions*, Journal of Mathematical Analysis and Applications **325**(1): 342-352, 2007.

[5] U. Kohlenbach, *Gödel's functional interpretation and its use in current mathematics*, In: Kurt Gödel and the Foundations of Mathematics. Horizons of Truth. Baaz, M. et al. (eds.), Cambridge University Press, New York, pp. 361-398, 2011.

[6] U. Kohlenbach and A. Sipoş, *The finitary content of sunny nonexpansive retractions*, Communications in Contemporary Mathematics, **23**(1): 1950093 (63pp), 2021.

[7] U. Kohlenbach and L. Leuştean, *Effective metastability of Halpern iterates in CAT(0) spaces*, Advances in Mathematics, **231**(5): 2526-2556, 2012.

[8] F. Ferreira, L. Leuştean and P. Pinto, *On the removal of weak compactness arguments in proof mining*, Advances in Mathematics, **354**: 106728 (55pp), 2019.

[9] P. Pinto, *A rate of metastability for the Halpern type Proximal Point Algorithm*, (submitted) arXiv:1912.12468, 2019.

[10] J. Gwinner, *On the convergence of some iteration processes in uniformly convex Banach spaces*, Proceedings of the American Mathematical Society, **71**(1): 29-35, 1978.

[11] U. Kohlenbach, *On quantitative versions of theorems due to F.E. Browder and R. Wittmann*, Advances in Mathematics, **226**(3): 2764-2795, 2011.

On minimality of the Minimalist Foundation

Maria Emilia Maietti

We here report some open issues and related results regarding the minimality of the Minimalist Foundation among relevant foundations for constructive and classical mathematics.

The Minimalist Foundation (**MF**) is a predicative foundation for constructive mathematics ideated in joint work with G. Sambin in [MS05] and completed to a two-level system in [Mai09].

MF consists of two levels with an interpretation of one into the other: an *intensional level* suitable as a base for a proof-assistant and for the extraction of computational contents from proofs, an *extensional level* formulated in a language close to that of ordinary mathematics, and an interpretation of the extensional level in the intensional one by means of a quotient completion (see [Mai09]).

A key feature of **MF** is that both its intensional and extensional levels consist of type systems extending versions of Martin-Löf's type theory with a primitive notion of propositions in such a way that propositions are *proof-irrelevant* at the extensional level and *proof-relevant* at the intensional one, and choice principles including the axiom of unique choice, even in the form of a rule as those valid in Heyting arithmetics, are not generally valid (see [Mai17]).

MF was called *minimalist* in [MS05] because it was intended to constitute a common core among the most relevant constructive and classical foundations for mathematics in the literature.

The two level structure of **MF** is crucial to establish its compatibility with other foundations at the most appropriate level: the intensional level of **MF** can be easily interpreted in intensional theories such as those formulated in type theory, for example Martin-Löf's type theory or Coquand-Huet's Calculus of Inductive Constructions, while its extensional level can be easily interpreted in extensional theories such as those formulated in axiomatic set theory, for example Aczel's constructive set theory **CZF** or those formulated in category theory as topoi. It is worth noting that all the mentioned interpretations preserve the meaning of propositions and of their set theoretic constructors.

Since the intensional level of **MF** is interpretable in first order fragment of Martin-Löf's type theory with one universe or in Feferman's theory of non-iterative fixpoints $\widehat{ID_1}$ in [Fef82] as shown in [IMMS18], then clearly **MF** is *predicative* in the sense of Feferman.

The intuitionistic version of the arithmetic comprehension axiom system $\mathbf{ACA_i}$ can be interpreted in both levels of **MF** by preserving the meaning of propositions and of its axioms. The same happens for the classical version **ACA** within **MF+EM** namely **MF** extended with the law of excluded middle. But **MF** appear to be stronger than $\mathbf{ACA_i}$ since it validates induction principles which allow to define the inductively generated formal topology of Cantor space and that of Dedekind real numbers.

It is still an open problem to establish the exact proof-theoretic strength of **MF** and of its classical version **MF+EM**.

In particular to establish the predicativity of **MF+EM** is an important issue to discriminate **MF** among other foundations. Indeed most relevant foundations for constructive mathematics, such as Martin- Löf's type theory and Aczel's **CZF**, becomes impredicative with the addition of the principle of excluded middle.

In our talk we want to shed some lights about this open problem by showing that in the extensional level of **MF+EM** real numbers defined as Dedekind sections, or as equivalence classes of Cauchy functional relations, do not form a set in accordance with Weyl's approach to foundation of mathematics. The same model reveals that the power-collection of the natural numbers is not a set there, too.

The proof of this theorem consists in interpreting the extensional level of the two-level system **MF+EM** in the quasi-topos of assemblies [van08] within Hyland's Effective topos [Hyl82], by interpreting propositions as strong monomorphisms, sets as countable assemblies and power-collections as the quasi-topos power-objects.

From this model we can deduce that real numbers both defined as Dedekind sections or as equivalence classes of Cauchy functional relations do not form a set in the extensional level of **MF**, too.

Instead Bishop real numbers defined as equivalence classes of regular sequences represented by lambda terms do form a set both in **MF** and in **MF+EM** and in the mentioned model these are interpreted as computable real numbers.

References

[Fef82] S. Feferman. Iterated inductive fixed-point theories: application to Hancock's conjecture. In *Patras Logic Symposion*, pages 171–196. North Holland, 1982.

[Hyl82] 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.

[IMMS18] H. Ishihara, M.E. Maietti, S. Maschio, and T. Streicher. Consistency of the intensional level of the Minimalist Foundation with Church's thesis and axiom of choice. *Archive for Mathematical Logic*, 57(7-8):873–888, 2018.

[Mai09] M. E. Maietti. A minimalist two-level foundation for constructive mathematics. *Annals of Pure and Applied Logic*, 160(3):319–354, 2009.

[Mai17] M.E. Maietti. On choice rules in dependent type theory. In *Theory and Applications of Models of Computation - 14th Annual Conference, TAMC 2017, Bern, Switzerland, April 20-22, 2017, Proceedings*, pages 12–23, 2017.

[MS05] 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.

[van08] J. van Oosten. *Realizability. An introduction to its categorical side.* Elsevier, 2008.

On the uncountability of $\mathbb{R}$

Sam Sanders
(joint work with Dag Normann)

The uncountability of $\mathbb{R}$ states that there is no injection (or bijection) from $\mathbb{R}$ to $\mathbb{N}$. Central as this statement may be to mathematics and its foundations, it has hitherto not been studied from a logical or computational point of view in detail.

We provide an overview of the state-of-the-art in higher-order arithmetic with results from [2], including the following:

First of all, the uncountability of $\mathbb{R}$ is hard to prove, the reals claimed to exist hard to compute (Kleene S1-S9), in that full second-order arithmetic comes to the fore, as has been established for the uncountable Heine-Borel theorem and the gauge integral. Thus, a new level of *simplicity* has been reached since [1].

Secondly, the previous item merely indicates that the 'normal' scale based on comprehension and discontinuous functionals is not the right scale for measuring the logical and computational strength of the uncountability of $\mathbb{R}$. Indeed, we introduce the 'non-normal scale' in which the latter is among the weakest principles (both logical and computational). In other words, a new level of *conceptual clarity* has been reached since [1].

Thirdly, exploring the ‘non-normal’ scale, we observe that many theorems of ordinary mathematics imply the uncountability of $\mathbb{R}$, including ‘pre-set theory’ results like Arzela’s convergence theorem for the Riemann integral. The same holds for relative computability in the sense of Kleene (S1-S9). In other words, a new level of *comprehensiveness* has been reached since [1].

Fourth, formulating ‘countable set’ based on ‘injection to $\mathbb{N}$’, we show that the Bolzano-Weierstrass theorem for countable sets of reals in [0,1] is highly explosive: combining it with the Suslin functional, i.e. higher-order Π^1_1-comprehension, one obtains Π^1_2-comprehension, In other words, a new level of *explosive power* has been reached since [1].

References

[1] D. Normann, S. Sanders, *On the mathematical and foundational significance of the uncountable*, Journal of Mathematical Logic, (2019), https://doi.org/10.1142/S0219061319500016.

[2] D. Normann, S. Sanders, *On the uncountability of* $\mathbb{R}$, Submitted, https://arxiv.org/abs/2007.07560.

Quantitative Tauberian Theorems

Thomas Powell

Tauberian theory compares different methods of summability. The earliest Tauberian theorem (due to and named after A. Tauber [1]) states that if the Abel sum of a series exists, and moreover the coefficients are of the order $o(1/n)$, then the series itself converges to its Abel sum. Tauber’s theorem has been significantly generalised, and has given rise to a whole research area dedicated to theorems of this type [2].

In this talk, I discussed proof theoretic aspects of Tauberian theorems, in particular the prospect of applying techniques from proof theory to obtain quantitative versions of these theorems. I first gave an account of some preliminary work along these lines [3], where simple “finitizations” of Abel’s and Tauber’s theorem via Gödel’s Dialectica interpretation [4] are given. I then presented some work–in–progress aimed at giving a proof theoretic account of the famous Littlewood [5] and Hardy-Littlewood [6] Tauberian theorems. To conclude, I listed some open questions, including the following:

1. Can proof theoretic methods like the Dialectica interpretation be applied to produce new “remainder theorems” in Tauberian theory which don’t have any precedent in the literature?
2. Are there abstract quantitative metatheorems (in the sense of the *proof mining* program) which unify and generalise groups of closely related Tauberian theorems?

I hope to make some progress on these questions in the future.

References

[1] A. Tauber, *Ein Satz aus der Theorie der unendlichen Reihen*, Monatshefte für Mathematik und Physik **8** (1897), 273–277.

[2] J. Korevaar, *Tauberian Theory: A Century of Developments*, Grundlehren der mathematischen Wissenschaften (2004), Springer-Verlag.

[3] T. Powell, *A note on the finitization of Abelian and Tauberian theorems*, Mathematical Logic Quarterly **66(3)** (2020), 300–310.

[4] K. Gödel, *Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes*, dialectica **12** (1958), 280–287.

[5] J. E. Littlewood, *The converse of Abel's theorem on power series*, Proceedings of the London Mathematical Society **s2-9** (1911), 434–448.

[6] G. H. Hardy and J. E. Littlewood, *Tauberian theorems concerning power series and Dirichlet's series whose coefficients are positive*, Proceedings of the London Mathematical Society **s2-13** (1914), 174–191.

Resolving finite indeterminacy

Peter Schuster
(joint work with Daniel Wessel)

Abstract algebra abounds with ideal objects and the invocations of transfinite methods, typically Zorn's Lemma, that grant those object's existence. Put under logical scrutiny, ideal objects often serve for proving the semantic conservation of additional non-deterministic sequents, that is, with finite but not necessarily singleton succedents. By design, dynamical methods in algebra [2, 4, 9] allow to eliminate the use of ideal methods by shifting focus from semantic model extension principles to syntactical conservation theorems, which move has enabled Hilbert's Programme for modern algebra.

A paradigmatic case, which to a certain extent has been neglected in dynamical algebra proper, is Krull's Lemma for prime ideals. A particular form of this asserts that a multiplicative subset of a commutative ring contains the zero element if and only if the set at hand meets every prime ideal. Prompted by Kemper and Yengui's novel treatment of valuative dimension [3], the authors of the present note together with Yengui have recently put Krull's Lemma under constructive scrutiny [7]. This development has eventually helped to unearth the underlying general phenomenon [8]: Whenever a certificate is obtained by the semantic conservation of certain additional non-deterministic axioms, there is a finite labelled tree belonging to a suitable inductively generated class which tree encodes the desired computation.

Recall that a *consequence relation* on a set S is a relation $\rhd$ between finite subsets[1] and elements of S, which is *reflexive, monotone* and *transitive*:

$$\frac{U \ni a}{U \rhd a}\ (\mathrm{R}) \qquad \frac{U \rhd a}{U, V \rhd a}\ (\mathrm{M}) \qquad \frac{U \rhd b \quad U, b \rhd a}{U \rhd a}\ (\mathrm{T})$$

[1] We understand a set to be *finite* if it can be written as $\{ a_1, \dots, a_n \}$ for some $n \geq 0$.

where the usual shorthand notations are in place. The *ideals* of a consequence relation are the subsets $\mathfrak{a}$ of S *closed* under $\rhd$ in the sense that if $\mathfrak{a} \supseteq U$ and $U \rhd a$, then $a \in \mathfrak{a}$. If U is a finite subset of S, then its *closure* is an ideal:

$$\langle U \rangle = \{\, a \in S \mid U \rhd a \,\}$$

A decisive aspect of our approach is the notion of a regular set for certain non-deterministic axioms over a fixed consequence relation, where by a *non-deterministic axiom* on S we understand a pair (A, B) of finite subsets of S. A subset $\mathfrak{p}$ of S is *closed* under (A, B) if $A \subseteq \mathfrak{p}$ implies $\mathfrak{p} \between B$, where the latter is to say that $\mathfrak{p}$ and B have an element in common.

Let $\mathcal{E}$ be a set of non-deterministic axioms over $\rhd$. A *prime ideal* is an ideal of $\rhd$ that is closed under every element of $\mathcal{E}$. For instance, if $\rhd$ denotes deduction, and $\mathcal{E}$ consists of all pairs $(\emptyset, \{\, \phi, \neg\phi \,\})$ for sentences ϕ, then the (prime) ideals are exactly the (complete) theories.

A subset R of S is *regular* with respect to $\mathcal{E}$ if, for all finite subsets U of S and all $(A, B) \in \mathcal{E}$,

$$\frac{(\forall b \in B)\ \langle U, b \rangle \between R}{\langle U, A \rangle \between R}$$

Abstracted from the multiplicative subsets occurring in Krull's Lemma, regular sets haved proved the right concept for our *Universal Prime Ideal Theorem*:

Proposition 1 (**ZFC**). *A subset R of S is regular if and only if for every ideal $\mathfrak{a}$ we have $R \between \mathfrak{a}$ precisely when $R \between \mathfrak{p}$ for all prime ideals $\mathfrak{p} \supseteq \mathfrak{a}$.*

Regular sets further account for the constructive version of Proposition 1. To this end, given an ideal $\mathfrak{a}$, we next define a collection $T_{\mathfrak{a}}$ of *finite* labelled trees such that the root of every $t \in T_{\mathfrak{a}}$ be labelled with a finite subset U of $\mathfrak{a}$, and the non-root nodes with elements of S. The latter will be determined successively by consequences of U along the elements of $\mathcal{E}$.

We understand paths, which necessarily are finite, to lead from the root of a tree to one of its leaves. Given a path π of $t \in T_{\mathfrak{a}}$, we write $\pi \rhd a$ whenever $U, b_1, \ldots, b_n \rhd a$ where U labels the root of t and $b_1, \ldots, b_n$ are the labels occurring at the non-root nodes of π.

Definition. *Let $\mathfrak{a}$ be an ideal. We generate $T_{\mathfrak{a}}$ inductively according to the following rules:*

(1) For every finite $U \subseteq \mathfrak{a}$, the trivial tree (i.e., the root-only tree) labelled with U belongs to $T_{\mathfrak{a}}$.

(2) If $(A, B) \in \mathcal{E}$ and if $t \in T_{\mathfrak{a}}$ has a path π such that $\pi \rhd a$ for every $a \in A$, then add, for every $b \in B$, a child labelled with b at the leaf of π.

We say that $t \in T_{\mathfrak{a}}$ terminates *in $R \subseteq S$ if for every path π of t there is $r \in R$ such that $\pi \rhd r$.*

Our *Constructive Universal Prime Ideal Theorem* works in (a fragment of) Constructive Zermelo–Fraenkel set theory **CZF** :

Proposition 2 (**CZF**). *A subset R of S is regular if and only if for every ideal $\mathfrak{a}$ we have $R \between \mathfrak{a}$ precisely when there is a tree $t \in T_{\mathfrak{a}}$ which terminates in R.*

We thus uniformise many instances of the dynamical method and generalise the universal proof-theoretic conservation criterion offered before [6], which by Scott–style entailment relations [1] unifies numerous phenomena, e.g. [5].

References

[1] Jan Cederquist and Thierry Coquand. *Entailment relations and distributive lattices.* In Samuel R. Buss, Petr Hájek, and Pavel Pudlák, editors, *Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998*, volume 13 of *Lect. Notes Logic*, pages 127–139. A. K. Peters, Natick, MA, 2000.

[2] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. *Dynamical method in algebra: Effective Nullstellensätze.* Ann. Pure Appl. Logic **111** (2001), 203–256.

[3] Gregor Kemper and Ihsen Yengui. *Valuative dimension and monomial orders.* J. Algebra **557** (2020), 278–288.

[4] Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*, volume 20 of *Algebra and Applications*. Springer Netherlands, Dordrecht, 2015.

[5] Sara Negri, Jan von Plato, and Thierry Coquand. *Proof-theoretical analysis of order relations.* Arch. Math. Logic **43** (2004), 297–309.

[6] Davide Rinaldi, Peter Schuster, and Daniel Wessel. *Eliminating disjunctions by disjunction elimination.* Indag. Math. (N.S.) **29** (2018), 226–259. Communicated first in Bull. Symb. Logic **23** (2017), 181–200.

[7] Peter Schuster, Daniel Wessel, and Ihsen Yengui. *Dynamic evaluation of integrity and the computational content of Krull's lemma.* 2019. Preprint.

[8] Peter Schuster and Daniel Wessel. *Resolving finite indeterminacy: A definitive constructive universal prime ideal theorem.* In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '20, pages 820–830, New York, NY, USA, 2020. Association for Computing Machinery.

[9] Ihsen Yengui. *Constructive Commutative Algebra. Projective Modules over Polynomial Rings and Dynamical Gröbner Bases*, volume 2138 of *Lecture Notes in Mathematics.* Springer, Cham, 2015.

Radical theory of Scott-open predicates

Daniel Wessel
(joint work with Peter Schuster)

Let R be a commutative ring with 1, and let $\mathfrak{a} \subseteq R$ be an ideal of R. The Jacobson radical $\mathrm{Jac}(\mathfrak{a})$ of $\mathfrak{a}$ is widely known as the set of all ring elements that belong to *every* maximal ideal of R containing $\mathfrak{a}$. Assuming the axiom of choice, this receives a well-know description in first-order terms, viz.

$$\mathrm{Jac}(\mathfrak{a}) = \{\, a \in R \mid (\forall b \in R)(\, 1 \in \langle a, b\rangle \to 1 \in \langle \mathfrak{a}, b\rangle) \,\},$$

which is used to define the Jacobson radical in constructive algebra [5].

Here is our motivating question: Can we find a syntactical counterpart to maximality principles such as those ascribed to Teichmüller [10] and Tukey [11], in a manner similar to how the Jacobson radical—in its computationally meaningful form—relates to Krull's maximal ideal theorem [4]? Our challenge is thus to solve the following analogy:

$$\frac{\text{Jacobson}}{\text{Krull}} \sim \frac{\textbf{?}}{\text{Teichmüller-Tukey}} .$$

Passing from ideals of R to elements of a complete lattice L, while replacing comaximality (i.e., the property of a set of ring elements to generate 1) with a fixed (but arbitrary) Scott-open subset O of L, we are led to a closure operator j,

$$jx = \bigvee \{\, a \in L \mid (\forall b \in L)(\, a \vee x \in O \to b \vee x \in O \,)\,\},$$

related forms and instances of which had previously been considered on distributive lattices [2], complete multiplicative lattices [3], quantales [1], and frames [9].

Key features of this j can be isolated by defining, inductively, an auxiliary relation $\sqsubseteq$,

$$\frac{x \leq y}{x \sqsubseteq y} \qquad \frac{y \in O}{x \sqsubseteq y} \qquad \frac{x \sqsubseteq y \vee a \quad (\forall b \in O_a)\, x \sqsubseteq y \vee b}{x \sqsubseteq y}$$

where $O_a = \{\, b \in L \mid a \vee b \in O \,\}$. The principal ideals generated by j-fixed elements of L can be described in terms of $\sqsubseteq$. In fact, for every $x, y \in L$,

$$x \sqsubseteq y \quad \text{if and only if} \quad x \leq jy.$$

Upon introducing (once again inductively) a certain class of labelled binary trees, appropriately adapting our termination principles [7, 8] by way of $\sqsubseteq$, we are able to pin down the computational import of a powerful separation principle equivalent to the axiom of choice, and obtain a new reading of the Teichmüller-Tukey Lemma.

McCabe's short proof of Zariski's lemma [6] is an exemplary, concrete application. Rather than showing a certain ring element a to be in every maximal ideal, and thus to argue that $1 + a$ be a unit, we show, towards the same conclusion, that every path of a corresponding tree generates the required data. Incidentally, this sheds new light on Yengui's backtracking method [12].

References

[1] Bernhard Banaschewski and Marcel Erné. *On Krull's separation lemma.* Order **10** (1993), 253–260.

[2] Thierry Coquand, Henri Lombardi, and Claude Quitté. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs.* Publications Mathématiques de Besançon. Algèbre et Théorie des Nombres (2006), 57–100.

[3] Marcel Erné. *Prime ideal theory for general algebras.* Appl. Categ. Structures **8** (2000), 115–144. Papers in honour of Bernhard Banaschewski (Cape Town, 1996).

[4] Wolfgang Krull. *Idealtheorie in Ringen ohne Endlichkeitsbedingung.* Math. Ann. **101** (1929), 729–744.

[5] Henri Lombardi and Claude Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*, volume 20 of *Algebra and Applications*. Springer Netherlands, Dordrecht, 2015.

[6] John McCabe. *A note on Zariski's lemma.* Amer. Math. Monthly **83** (1976), 560–561.

[7] Peter Schuster and Daniel Wessel. *Resolving finite indeterminacy: A definitive constructive universal prime ideal theorem.* In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '20, pages 820–830, New York, NY, USA, 2020. Association for Computing Machinery.

[8] Peter Schuster and Daniel Wessel. *The computational significance of Hausdorff's Maximal Chain Principle.* In Marcella Anselmo, Gianluca Della Vedova, Florin Manea, and Arno Pauly, editors, *Beyond the Horizon of Computability. 16th Conference on Computability in Europe*, volume 12098 of *Lect. Notes Comput. Sci.*, pages 239–250. Springer, 2020. Proceedings, CiE 2020, Fisciano, Italy, June 29–July 3, 2020.

[9] Harold Simmons. *A curious nucleus.* J. Pure Appl. Algebra **214** (2010), 2063–2073.

[10] Oswald Teichmüller. *Braucht der Algebraiker das Auswahlaxiom?* Deutsche Math. **4** (1939), 567–577.

[11] John W. Tukey. *Convergence and Uniformity in Topology*, volume 2 of *Ann. Math. Studies.* Princeton University Press, Princeton, 1940.

[12] Ihsen Yengui. *Making the use of maximal ideals constructive.* Theoret. Comput. Sci. **392** (2008), 174–178.

Two recent results in proof mining

Andrei Sipoş

We present two case studies that belong to the research program of *proof mining*, which aims to analyze proofs in mainstream mathematics using proof-theoretic tools in order to reveal information which may not be immediately apparent and which is most often of a quantitative nature (a comprehensive monograph is [5], while a recent survey is [6]). For example, if a theorem states that a given sequence converges, one would want to extract a rate of convergence for the sequence. However, frequently, such a rate cannot be extracted using proof mining, not because of any limitation in the techniques, but simply because such a rate may not be uniform or may even be uncomputable. In this case, the next best thing is to analyze the (classically but not constructively) equivalent version of it, called "metastability" by Terence Tao (at the suggestion of Jennifer Chayes), expressed as

$$\forall \varepsilon \; \forall g : \mathbb{N} \to \mathbb{N} \; \exists N \; \forall i, j \in [N, N + g(N)] \; d(x_i, x_j) \leq \varepsilon$$

and tries to extract a "rate of metastability", i.e. a bound on the N depending on ε, g and possibly some other parameters of the problem.

Our first result (from the paper [9]) concerns the extraction of such rates of metastability for Picard, Mann and Ishikawa iterations of continuous functions on the unit interval $[0,1]$. Some work had already been done by Jaime Gaspar in his PhD thesis [4], where he analyzed a theorem due to Hillam, which states that if $f : [0,1] \to [0,1]$ is continuous, $x \in [0,1]$ and $\lim_{n\to\infty}(f^n x - f^{n+1}x) = 0$, then the sequence $(f^n x)$ converges. We first closed this circle of ideas, analysing more general versions of this due to Franks/Marzec and Rhoades, which do not depend on that asymptotic regularity assumption, thus extracting unconditional rates of metastability. Then, we analyzed another result due to Borwein/Borwein [2], which states that if $L > 0$, $f : [0,1] \to [0,1]$ is L-Lipschitz and (x_n), $(t_n) \subseteq [0,1]$

be such that for all n, $x_{n+1} = (1-t_n)x_n + t_n f(x_n)$, if there is a $\delta > 0$ such that for all n,

$$t_n \leq \frac{2-\delta}{L+1},$$

then the sequence (x_n) converges. The argument in the proof posed a significant challenge – it had not been so far analyzed using proof mining techniques. We managed to extract a rather complex rate of metastability for this kind of iteration, depending on ε, g and the δ above.

Our second result (from the paper [10]) concerns the extraction of rates of metastability for the mean ergodic theorem. The classical mean ergodic theorem due to von Neumann and Riesz had been previously analyzed proof-theoretically by Avigad, Gerhardy and Towsner [1] and by Kohlenbach and Leuştean [7]. What we do is to analyzed a later proof of Riesz's [8] that uses an argument which can be readily applied to a generalization of it to multiple commuting operators (sometimes attributed to Dunford [3]). This generalization states that if X is a uniformly convex Banach space, $d \geq 1$ and $T_1, \ldots, T_d : X \to X$ are commuting linear operators such that for each l and for each $x \in X$, $\|T_l x\| \leq \|x\|$, then for any $x \in X$, the sequence (x_n), defined, for any n, by

$$x_n := \frac{1}{(n+1)^d} \sum_{k_1=0}^{n} \ldots \sum_{k_d=0}^{n} T_1^{k_1} \ldots T_d^{k_d} x$$

is convergent. We managed to extract a rate of metastability for this sequence that depends, in addition to ε and g, on d, an upper bound b for $\|x\|$ and a modulus of uniform convexity η for X.

References

[1] J. Avigad, P. Gerhardy, H. Towsner, *Local stability of ergodic averages*, Trans. Amer. Math. Soc. **362** (2010), no. 1, 261–288.

[2] D. Borwein, J. Borwein, *Fixed point iterations for real functions*, J. Math. Anal. Appl. **157** (1991), no. 1, 112–126.

[3] N. Dunford, *An ergodic theorem for n-parameter groups*, Proc. Natl. Acad. Sci. U.S.A. **25** (1939), 195–196.

[4] J. Gaspar, *Proof interpretations: theoretical and practical aspects*, PhD Thesis, TU Darmstadt, 2011.

[5] U. Kohlenbach, *Applied proof theory: Proof interpretations and their use in mathematics*, Springer Monographs in Mathematics, Springer, 2008.

[6] U. Kohlenbach, *Proof-theoretic methods in nonlinear analysis*, in: B. Sirakov, P. Ney de Souza, M. Viana (eds.), *Proceedings of the International Congress of Mathematicians 2018 (ICM 2018)*, Vol. 2 (pp. 61–82). World Scientific, 2019.

[7] U. Kohlenbach, L. Leuştean, *A quantitative mean ergodic theorem for uniformly convex Banach spaces*, Ergodic Theory Dynam. Systems **29** (2009), 1907–1915.

[8] F. Riesz, *Another proof of the mean ergodic theorem*, Acta Univ. Szeged. Sect. Sci. Math. **10** (1941), 75–76.

[9] A. Sipoş, *Rates of metastability for iterations on the unit interval*, arXiv:2008.03934 [math.CA], 2020.

[10] A. Sipoş, *A quantitative multi-parameter mean ergodic theorem*, arXiv:2008.03932 [math.DS], 2020.

Quantitative results for equilibrium problems

Nicholas Pischke
(joint work with Ulrich Kohlenbach)

I present a recent application [7] of proof mining (see [4] for a recent survey and [3] for the main textbook reference) to algorithmic solutions of the equilibrium problem in convex optimization. Equilibrium problems arise as abstractions of many interesting mathematical results: the famous Nash-equilibrium in non-cooperative games, the classical variational inequality problem, saddle point problems, convex minimization problems, fixed point problems and many more can be phrased as special equilibrium problems (see [2]).

In the abstraction considered here, equilibrium problems take the form of

Problem 1. For a closed and convex set $C \subseteq \mathbb{R}^N$ and a function $f : C \times C \to \mathbb{R}$ with $f(x, x) = 0$ for all $x \in C$, find a $u \in C$ with

$$f(u, y) \geq 0 \text{ for all } y \in C.$$

In [1], H. Iiduka and I. Yamada introduced an algorithm for approximating solutions of the above problem (modulo additional requirements on f) for the particular instance of C being the set of fixed-points of a firmly nonexpansive mapping T and proved its convergence. The algorithm follows a general scheme for solving equilibrium problems presented in [2] by first reducing the equilibrium problem to a convex feasability problem and then solving that using subgradient-approximations for the metric projections of the involved convex sets in combination with a hybrid steepest descent method defined (only in the context of variational inequality problems) in [9].

I present two quantitative versions of their convergence result which were obtained by a proof-theoretic analysis of the respective proof using recent quantitative results on the convergence of Fejér monotone sequences [5, 6] (which also originated from the proof mining program). While the first result is only an explicit rate of metastability (in the sense of Tao [8]), under mild quantitative assumptions on the input parameters, the second result even gives a rate of convergence under a respectively strong "metric regularity" assumption.

References

[1] H. Iiduka and I. Yamada. A subgradient-type method for the equilibrium problem over the fixed point set and its applications. *Optimization*, 58(2):251 – 261, 2009.

[2] A. Iusem and W. Sosa. Iterative algorithms for equilibrium problems. *Optimization*, 52(3):301 – 316, 2003.

[3] U. Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics.* Springer Monographs in Mathematics. Springer-Verlag Berlin Heidelberg, 2008.

[4] U. Kohlenbach. Recent progress in proof mining in nonlinear analysis. *IFCoLog Journal of Logics and their Applications*, 10(4):3361 – 3410, 2017.

[5] U. Kohlenbach, L. Leuştean, and A. Nicolae. Quantitative Results on Fejér Monotone Sequences. *Communications in Contemporary Mathematics*, 20(2), 2018.

[6] U. Kohlenbach, G. López-Acedo, and A. Nicolae. Moduli of regularity and rates of convergence for Fejér monotone sequences. *Israel Journal of Mathematics*, 232:261 – 297, 2019.

[7] N. Pischke and U. Kohlenbach. Quantitative analysis of a subgradient-type method for equilibrium problems. *ArXiv e-prints*, 2020. arXiv, math.OC, 2008.06900.

[8] T. Tao. *Structure and Randomness: Pages from Year One of a Mathematical Blog*, chapter Soft analysis, hard analysis, and the finite convergence principle. American Mathematical Society, Providence, RI, 2008.

[9] I. Yamada and N. Ogura. Hybrid Steepest Descent Method for Variational Inequality Problem over the Fixed Point Set of Certain Quasi-nonexpansive Mappings. *Numerical Functional Analysis and Optimization*, 25(7,8):619 – 655, 2004.

Converse extensionality and apartness

Benno van den Berg
(joint work with Robert Passmann)

Following Kreisel one of the main concerns of proof theory has become the extraction of hidden computational information from proofs. For this purpose Gödel's Dialectica interpretation (combined with negative translation, if necessary) has proven itself to be indispensable. Indeed, within proof mining functional interpretations of various kinds have become a sophisticated and flexible tool for extracting additional qualitative and quantitative information from proofs.

One of the hardest principles to interpret using a functional interpretation is the principle of function extensionality. This principle, which says that two functions are equal if they yield the same output on the same input, is pervasive in mathematics. But it has proven difficult to interpret using the Dialectica interpretation, the reason being that the Dialectica interpretation requires one to interpret a stronger form of extensionality, which we have dubbed *converse extensionality*:

$$\mathsf{CE}_n: \quad \exists X\, \forall \Phi^{n+2}\, \forall f, g\, \big(\, \Phi f \neq_0 \Phi g \to f(X\Phi f g) \neq_0 g(X \Phi f g)\,\big).$$

As shown by Howard (see [1]), CE_0 cannot be witnessed in the term model of Gödel's T and CE_1 is unprovable in Zermelo-Fraenkel set theory (without choice). This has often been taken as an indication that a computational interpretation of function extensionality is well-nigh impossible.

Together with Robert Passmann, we have started to investigate whether the situation is really that hopeless. Our idea is that by a suitable enrichment of data it might still be possible to interpret (fragments of) converse extensionality. For this we are looking at Brouwer's notion of *apartness*.

Brouwer's idea was that equality might not be a primitive concept and could be defined as the negation of a strong notion of inequality called apartness. The paradigmatic example is the real numbers, where two reals r and s are apart when there are disjoint intervals with rational endpoints I_1 and I_2 such that $r \in I_1$ and $s \in I_2$. Equality of real numbers can then be defined as not being apart.

Our first step is the observation (see also [2]) that on all the finite types equality can indeed be defined as the negation of a suitable notion of apartness. But that means that one may require functionals f of type $\sigma \to \tau$ to come equipped with additional data that explains how from evidence that fx and fy are apart one obtains evidence that x and y are apart. Our initial results do indeed suggest that by enriching functionals with this data one may interpret certain forms of converse extensionality, although the results are not (yet) as strong as we had hoped.

To formulate the results that we have obtained so far, we use the notion of a typed combinatory algebra (tca), basically a model of Gödel's T. We show that from every tca (including the term model of Gödel's T) one can define a new tca, which we have dubbed the *apartness types*. By using modified realizability over these apartness types one can interpret CE_0. This shows (*pace* Howard) that it might still be possible to interpret CE_0 using terms from Gödel's T. To interpret stronger principles (CE_1 and higher) we currently have to use tcas which satisfy suitable continuity principles.

We feel that stronger results should be possible by employing our methods. Indeed, at the workshop several interesting suggestions were made which we hope to be able to explore soon.

References

[1] A.S. Troelstra. *Metamathematical investigation of intuitionistic arithmetic and analysis*, Lecture Notes in Mathematics, Vol. 344, Springer-Verlag, Berlin-New York, 1973.

[2] A.S. Troelstra and D. van Dalen. *Constructivism in mathematics. Vol. II*, Studies in Logic and the Foundations of Mathematics, volume 123, North-Holland Publishing Co., Amsterdam, 1988.

Proof search problem

Jan Krajíček

Propositional proof complexity is linked with SAT solving by interpreting the run of a complete SAT algorithm that fails to find a satisfying assignment for φ as a *proof* that $\neg\varphi$ is a tautology. Often such an "abstract" proof system is equal to (or close to) a standard proof system as is R (resolution). Various technical results (and lower bounds, in particular) known in proof complexity for the proof system can then be interpreted as results about the original algorithm. That is, proof complexity contributes to the *analysis of SAT algorithms.*

This seems to be too narrow and proof complexity ought to attempt to precisely formalize and to answer some of the outstanding informal problems. These include:

(1) How do you compare two proof search algorithms and is there an optimal way to search for propositional proofs?

(2) Why it does not seem to be particularly helpful to search for proofs in stronger proof systems?

(3) How is it possible that real-world algorithms (SAT or automated theorem proving) perform well even for very long formulas while we have exponential lower bounds for the associated proof systems?

Basic notions of proof complexity as are propositional proof systems and simulations and p-simulations among them, can be found in [1]. The fundamental problems are the NP vs. coNP problem, asking whether for some proof system P is the length-of-proof function

$$s_P(\tau) := \min\ (|w| \mid\ w \text{ is a } P\text{-proof of } \tau\ )$$

bounded by $|\tau|^{O(1)}$, and the optimality problem: Is there a proof system that is maximal in the quasi-ordering induced by (p-)simulation? The optimality problem relates to a number of questions in a surprisingly varied areas and there are quite a few relevant statements known (cf. [1, Chpt.21]).

We define a *proof search algorithm* to be a pair (A, P), where P is a proof system and A is a deterministic algorithm such that $A(\tau)$ is a P-proof of τ, for all tautologies τ. We note two statements:

Lemma *For any fixed proof system P there is A such that (A, P) is time-optimal among all (B, P); it has at most polynomial slow-down:*

$$time_A(\tau)\ \le\ time_B(\tau)^{O(1)}\ .$$

Let (A_P, P) denote some proof search algorithm time-optimal among all (B, P).

Theorem *Let P be any proof system containing R and having the property that for some $c \ge 1$, for every τ and every τ' obtained from τ by substituting constants for some atoms it holds $s_P(\tau') \le s_P(\tau)^c$.*

Then P is p-optimal iff (A_P, P) is time-optimal among all proof search algorithms (B, Q).

The proof of the non-trivial if-direction uses the fact that for any Q there is a *p-time construable sequence* of tautologies

$$\langle Ref_Q \rangle_n\ ,\ n \ge 1$$

such that if it is feasible to construct P-proofs of these formulas then P p-simulates Q.

Another context where *easy sequences of hard formulas* appear are length-of-proofs lower bounds: whenever we can show that Q is stronger than P we can demonstrate it on such a sequence.

I would like to have a definition of a quasi-ordering on proof search algorithms that does not declare (B, Q) stronger only because B will recognize a simple sequence of formulas that have short Q-proofs but long P-proofs. The idea is that we compare proof search algorithms only on *special test sets T* that do not contain easy to recognize sets of tautologies. Having such a notion, we put

Definition *Define that (A, P) is as good as (B, Q), denoted by $(A, P) \succeq (B, Q)$, iff for all test sets T:*

$$time_A(\tau)\ \le\ time_B(\tau)^{O(1)}\ \ for\ all\ \ \tau \in T\ .$$

In [1, Sec.21.5] I took test sets to be of the form TAUT $\setminus H$ with $H \in$ P/*poly*, allowing to disregard those easy sequences of hard formulas. But maybe one ought to disallow all such easy sets at the same time, and to declare a set easy if it is computable in sub-exp-time $2^{o(n)}$ rather than in p-time. Such “subexp-time-immune” subsets of TAUT can be constructed by a diagonalization process but there are also candidates that are more transparent, constructed from conjectured proof complexity generators: tautologies in such test sets express that a string is outside of the range of a suitable map.

An open problem is whether for some natural test sets there is (A, P) that is $\succeq$-maximal among all proof search algorithms. It would be interesting if some such $\succeq$ allowed for an unconditional affirmative answer and if the proof system P would be one of the weaker proof systems (this would offer answers to informal problems 1 and 2 mentioned above).

While we have easy sequences of hard formulas for various proof systems they are in a sense rather rare (e.g. combinatorial principles or reflection principles). This can be an explanation why real life algorithms solve problems of huge size (cf. informal problem 3 above): the formulas are instances from easy to describe sets and such sets of hard formulas are rare.

Slides from the talk are available at:
`www.karlin.mff.cuni.cz/~krajicek/talk-proofsearch-mfo-11-20.pdf`

References

[1] J. Krajíček, *Proof complexity*, Encyclopedia of Mathematics and Its Applications, Vol. **170**, Cambridge University Press, (2019).

Towards #P

Isabel Oitavem
(joint work with Reinhard Kahle, Ugo dal Lago)

1. Introduction

We give recursion-theoretic characterizations of the counting class $\#P$. This is done in the style of Bellantoni and Cook's safe recursion, and it takes $\#P$ into the context of implicit computational complexity. Namely, it relates $\#P$ with the implicit characterization of *FPtime* [1] and *FPspace* [4], by exploiting the features of the tree-recursion scheme of *FPspace*.

The class $\#P$ was introduced by Valiant [5] as the class of functions which count the number of accepting computations of non-deterministic Turing machines working in polynomial time. For this class, Wagner [7] introduced a hierarchy of counting functions by allowing queries to functions of the previous level. Vollmer and Wagner [6] gave a characterization of $\#P$ which uses a closure under a SUM operator.

2. Two implicit approaches to #P

We consider functions defined over 0-1 words. Thus by addition $(+)$ and product $(\cdot)$ we mean the word representation of the usual addition and product functions over natural numbers. Moreover, we follow the notation introduced in [1], where functions have two sorts of input positions: normal and safe — $f(\bar{x}; \bar{y})$.

Let ST_0 be the input-sorted characterization of *FPtime* given by Bellantoni and Cook, rephrased over 0-1 words. Based on [4], *FPspace* can be described as the closure of *FPtime* under sorted composition and sorted tree-recursion. One writes *FPspace* $= [ST_0; \mathsf{SC}, \mathsf{STR}]$, where $f = \mathsf{SC}\,[\mathsf{g}, \bar{\mathsf{r}}, \bar{\mathsf{s}}]$ if $f(\bar{x};\bar{y}) = g(\bar{r}(\bar{x};); \bar{s}(\bar{x};\bar{y}))$, and $f = \mathsf{STR}\,[\mathsf{h}]\,(\mathsf{g})$ if

$$\begin{aligned} f(p,\epsilon,\bar{x};\bar{y}) =& g(p,\bar{x};\bar{y}) \\ f(p,zi,\bar{x};\bar{y}) =& h(p,zi,\bar{x};\bar{y}, f(p0,z,\bar{x};\bar{y}), f(p1,z,\bar{x};\bar{y})), \text{ with } i \in \{0,1\}. \end{aligned}$$

We define $ST_1 = [ST_0; \mathsf{SC}_0, \mathsf{STR}\,[+]]$, where $\mathsf{SC}_0\,[\mathsf{g}, \bar{\mathsf{r}}, \bar{\mathsf{s}}]$ is $\mathsf{SC}\,[\mathsf{g}, \bar{\mathsf{r}}, \bar{\mathsf{s}}]$ with the proviso $\bar{r}, \bar{s} \in ST_0$, and $f = \mathsf{STR}\,[+]\,(\mathsf{g})$ if

$$\begin{aligned} f(p,\epsilon,\bar{x};\bar{y}) =& g(p,\bar{x};\bar{y}) \\ f(p,zi,\bar{x};\bar{y}) =& +(; f(p0,z,\bar{x};\bar{y}), f(p1,z,\bar{x};\bar{y})), \text{ with } i \in \{0,1\}. \end{aligned}$$

The main result is: $\#P = ST_1$ — see [3]. This is an implicit characterization of $\#P$ that establishes the closure of the class under a certain 'level' of composition. This is a sensitive issue since $\#P$ is not known to be closed under composition. A similar technique is used in [2] to approach NP. Concerning recursion, the $\mathsf{STR}\,[+]$ scheme corresponds, in this context, to the SUM operator used by Vollmer and Wagner in [6]. However, the $\mathsf{STR}\,[+]$ scheme gives us the possibility to extend the class of step functions. Instead of taking only + as step function in the tree-recursion scheme, one can enlarge the class of step functions without leaving $\#P$. This is a feature that reflects the robustness of the characterization, and that we do not see in approaches based on the SUM operator.

Of course that step functions are expected to be aligned with the implicit characterization of *FPspace* mentioned above. In particular, they should respect the bounding lemma given in [4]. Thus, only functions satisfying $|h(;u,v)| \leq max(|u|,|v|) + k$, for some constant k, are considerable. Notice that the addition (+) satisfies it, but multiplication $(\cdot)$ does not. There are also some other constraints that one has to keep in mind. Namely, that recursion generalizes composition and, again, $\#P$ is not known to be closed under composition.

Let Affine denote the set of all affine functions of arity 2 (over 0-1 words), i.e. functions $h(;u,v) = a \cdot u + b \cdot v + c$ with $a, b, c \in \{0,1\}^*$. Considering $\mathsf{STR}\,[\mathsf{Affine}]$ the scheme $\mathsf{STR}\,[\mathsf{h}]$ with $h \in \mathsf{Affine}$ one has that:

$$\#P = [ST_0; \mathsf{SC}_0, \mathsf{STR}\,[\mathsf{Affine}]]\,.$$

For instance, if f is defined by $\mathsf{STR}\,[\mathsf{Affine}]$ with step function $h(;u,v) = a\cdot u + b\cdot v + c$ and base function g, one has that $f(\epsilon, 11) = a \cdot a \cdot g00 + a \cdot b \cdot g01 + b \cdot a \cdot g10 + b \cdot b \cdot g11 + a \cdot c + b \cdot c + c$. Notice that, in this sum, the number of factors in the coefficients of the g's is always 2 (i.e. the length of the recursion input). Actually, the coefficients correspond to the arguments of the g's — a for 0 and b for 1, meaning that one has $a \cdot a \cdot g00$, $a \cdot b \cdot g01$, etc. The proof of the result above uses the known closure of $\#P$ under addition (+), numeric product $(\cdot)$ and conditional (provided that the decision condition is polytime).

3. Conclusion

We characterize $\#P$ implicitly, in a recursion-theoretic manner. We address the issue of closure under composition, by allowing a certain 'level' of composition within the class. Moreover, we consider a variation of the tree-recursion scheme illustrating the robustness of the approach. The present characterization of $\#P$ can be extended to all levels of the polynomial hierarchy of the counting functions and to the hierarchy itself, see [3]. Recursion-theoretic approaches also yield a base for proof-theoretic ones, and there is ongoing work in this direction.

References

[1] S. Bellantoni and S. Cook, *A new recursion-theoretic characterization of the poly-time functions*, Computational Complexity **2** (1992), 97–110.

[2] I. Oitavem, *A recursion-theoretic approach to NP*, Annals of Pure and Applied Logic **8** (2011), 661–666.

[3] R. Kahle, U. dal Lago and I. Oitavem, *Implicit recursion-theoretic characterizations of counting classes*, manuscript.

[4] I. Oitavem, *Characterizing PSPACE with pointers*, Mathematical Logic Quarterly **54(3)** (2008), 317–323.

[5] L. G. Valiant, *The complexity of computing the permanent*, Theoretical Computer Science, **8** (1979), 189–201.

[6] H. Vollmer and K. Wagner, *Recursion theoretic characterizations of complexity classes of counting functions*, Theoretical Computer Science, **163** (1996), 245–258.

[7] K. Wagner, *Some observations on the connection between counting and recursion*, Theoretical Computer Science, **47** (1986), 131–147.

Implicative algebras: completeness results

Alexandre Miquel

Implicative algebras [3] are a generalization of complete Heyting algebras intended to factorize the model-theoretic constructions underlying forcing and realizability, both in intuitionistic and classical logic. Each implicative algebra induces a (**Set**-based) tripos [2, 4, 5], using a very general construction that encompasses the construction of all forcing triposes (both intuitionistic and classical), all classical realizability triposes (in the sense of Krivine [6]) and all intuitionistic realizability triposes built from partial combinatory algebras [2].

In this talk, we show that actually, each (**Set**-based) tripos is (isomorphic to) an implicative tripos, whose underlying implicative algebra can be constructed from the generic predicate of the source tripos using domain-theoretic techniques à la Engeler [1]. From this result, we deduce in particular that all classical (**Set**-based) triposes are (isomorphic to) Krivine triposes.

We conclude the talk by discussing possible generalizations of the above result to the framework of first-order theories without equality.

References

[1] E. Engeler. *Algebras and combinators.* Algebra Universalis, 13(1):389–392, 1981.

[2] J. M. E. Hyland, P. T. Johnstone, and A. M. Pitts. *Tripos theory.* In Math. Proc. Cambridge Philos. Soc., Vol. 88, p. 205–232, 1980.

[3] A. Miquel. *Implicative algebras: a new foundation for realizability and forcing.* Mathematical Structures in Computer Science, 30(5):458–510, 2020.

[4] A. M. Pitts. *The theory of triposes.* PhD thesis, University of Cambridge, 1981.

[5] A. M. Pitts. *Tripos theory in retrospect.* Math. Struct. Comp. Sci. 12(3):265–279, 2002.

[6] T. Streicher, *Krivine's classical realisability from a categorical perspective.* Math. Struct. Comp. Sci. 23(6):1234–1256, 2013.

Geometric theories for constructive algebra

Henri Lombardi

Plan:
1) General aims
2) Historical perspective
3) Finitary dynamical theories as purely computational machineries
4) Extensions of dynamical theories

1) General aims

Two slogans of Henri Poincaré criticizing the Zermelo formal system.

- Never lose sight of the fact that every proposition concerning infinity must be the translation, the precise statement of propositions concerning the finite.
- Avoid nonpredicative classifications and definitions.

a) Hilbert's program for algebra

a1) To give a constructive semantic for existential theorems in algebra. E.g., the algebraic closure of an arbitrary discrete field: we replace the classical (static) algebraic structure given via Zorn's lemma, by a dynamical algebraic structure.

a2) To decipher abstract algebraic proofs leading to concrete results.

b) To use a framework where algebra becomes purely computational, without logic, as in Goodstein Recursive Arithmetic.

c) To give a constructive version of the classical approach of geometric theories.

d) To give a constructive version of Grothendieck toposes and their "equivalence" with geometric theories

2) Historical perspective

See the references in chronological order.
Sources of inspirations are also Kreisel unwindings and Kreisel NCI.
The book [11] contains some chapters using dynamical evaluation. In fact, many parts of the book are directly inspired by dynamical algebra.

3) Finitary dynamical theories as purely computational machineries

A coherent theory is a first order formal theory whose axioms have all the geometric form

$$(1) \qquad \forall \underline{x}\ \big(C \implies \exists\, \underline{y^1}\, D_1 \ \vee\ \cdots\ \vee\ \exists\, \underline{y^m}\, D_m\big) \qquad m \geq 0$$

where C and D_j's are *conjunctions of atomic formulae*, $\underline{y^j}$'s are lists of variables (possibly empty), $\underline{x}$ are other variables (possibly empty). An empty disjunction on the right can be replaced by $\bot$ (False).

The corresponding dynamical theory is much simpler. Axioms are viewed as computational rules. An axiom as (1) is used as a dynamical rule (2):

$$(2)\ \ \Gamma \vdash \textsf{\textbf{Introduce}}\ \underline{y^1}\ \textsf{\textbf{such that}}\ \Delta_1\ \textsf{\textbf{op}}\ \cdots\ \textsf{\textbf{op}}\ \textsf{\textbf{Introduce}}\ \underline{y^m}\ \textsf{\textbf{such that}}\ \Delta_m$$

Conjunctions of atomic formulae C, D_1, ..., D_m in (1) are replaced by lists of atomic formulae Γ, Δ_1, ..., Δ_m.

The meaning of **op** is: open branches of computations.

The meaning of **Introduce** $\underline{y^1}$ **such that** ... is: introduce fresh variables.

Theorems are valid deduction rules. A dynamical proof is given by a computational tree. At each of the leaves, one disjunct $\Delta_i(\underline{x}, \underline{t^i})$ is proved (terms $\underline{t^i}$ with only $\underline{x}$ variables replace the variables $\underline{y^i}$)

If $\mathcal{T}$ is a (finitary) dynamical theory, a dynamic algebraic structure of type $\mathcal{T}$ is given by generators and relations. It is seen as an incompletely specified algebraic structure.

Examples

Commutative rings (purely equational theory). An arbitrary commutative ring can be seen as a dynamic algebraic structure for any one of the following theories.

Without zero-divisor ring.

Integral domain. Not the same as the previous one.

Ring with a prime ideal (relation with Krull's theorem).

Local ring.

Residually discrete local ring. Not the same as the previous one.

Discrete ordered field.

Real closed field.

Natural deduction

A dynamical theory can be seen as a weak form of natural deduction: only conjunctions, disjunctions and existential quantifier. No place for quantifier $\forall$ or connector $\Rightarrow$.

4) Extensions of dynamical theories

Intuitively equivalent theories (definitions by name)

(1) Adding abbreviations.
(2) Adding connectors: disjunction, conjunction, existential quantifier.
(3) Adding terms: in case of unique existence.

(4) Adding sorts (as in Bishop set theory): subsort, quotient sort, finite product sort, finite disjoint union sort.

This changes neither valid rules nor constructive models. Is this the same thing as constructive Morita equivalence?

Adding TEP $\Leftrightarrow$ adding classical logic.
For adding classical logic, it is sufficient to add conjunctions, disjunctions, existential formulae and, for each predicate P an opposite predicate Q with the two suitable axioms.

$\textsf{In-not}_P \ \vdash P \ \textsf{op} \ Q$ $\qquad\qquad$ $\textsf{El-not}_P \quad P \textsf{,} Q \vdash \bot$

Fundamental theorem: adding classical logic gives a conservative extension.

Skolemisation.

Skolemisation gives a conservative extension [12]. Weak form of choice.

Simultaneous collapses.
This is a constructive form of extensions theorems in classical mathematics.

Theories proving the same Horn rules.
This is a constructive form of representation theorems in classical mathematics.

References

[1] Paul Lorenzen, *Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen*, Math. Z. **58** (1953), 15–24. url: `http://eudml.org/doc/169331`

[2] Stefan Neuwirth, *Lorenzen's reshaping of Krull's Fundamentalsatz for integral domains (1938-1953)*, in: Paul Lorenzen–Mathematician and Logician: Proceedings of the conference (Constance, 8-9 March 2018). Under the dir. of Gerhard Heinzmann and Gereon Wolters. In press, arXiv:2007.08625. Springer, 2021

[3] Harvey Friedman. *Classically and intuitionistically provably recursive functions.* In Scott, D. and Müller, G. Editors, Higher set theory, Volume 699 of Lecture Notes in Mathematics, Springer Verlag (1978), 21–28.

[4] D5: Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields.* In Caviness B.F. (Ed.) EUROCAL '85. Lecture Notes in Computer Science 204, 289–290. Springer (1985).

[5] Fred Richman, *Non trivial uses of trivial rings*, Proc. Amer. Math. Soc. **103** (1988), 1012–1014.

[6] L. *Effective real Nullstellensatz and variants*, in: Effective Methods in Algebraic Geometry. Eds. Mora T., Traverso C.. Birkhäuser (1991). Progress in Math. No 94 (MEGA 90), 263–288.

[7] Cederquist J., Coquand T., *Entailment relations and distributive lattices*, in: Logic Colloquium '98 (Prague). T. 13. Lect. Notes Log. Assoc. Symbol. Logic, Urbana, IL, (2000), 127–139

[8] Coste M., L., Roy M.-F., *Dynamical method in algebra: Effective Nullstellensätze*, Annals of Pure and Applied Logic **111** (2001), 203–256. (arXiv:1701.05794)

[9] L. *Dimension de Krull, Nullstellensätze et évaluation dynamique*, Math. Z. **242** (2002), 23–46.

[10] Coquand T., L. *A logical approach to abstract algebra. A survey*, Math. Struct. in Comput. Science **16** (2006), 885–900.

[11] L., Quitté C. *Commutative algebra: constructive methods.* Translated from the French (Calvage & Mounet, 2011, revised and extended by the authors) by Tania K. Roblot. Algebra and Applications No 20. Springer (2015).

[12] Marc Bezem, Thierry Coquand *Skolem's Theorem in Coherent Logic* Fundam. Inform. (2019)

Infinitary Proofs

Bahareh Afshari

In the traditional Hilbertian view, objects that exhibit non-finitary behaviour are 'ideal' and permitted only in intermediate steps towards results governing 'concrete' finitary objects. The 'concrete' proofs are, however, hard to construct. Making the right choice amongst non-deterministic inference rules and correctly identifying cut-formulas pose challenges in proof search. A more serious hurdle, that befalls even analytic systems, is the presence of induction axioms. With the problem of (induction) invariant generation being intractable, the quest for finitary proof systems and the endeavour to automatically (or semi-automatically) construct proofs go their separate ways.

Infinitary proofs, owing to their intuitive semantics, have helped break barriers in the proof theory and treatment of logics formalising inductive and co-inductive concepts. They can be broadly placed in two categories. ω-proofs, also known as *infinitely wide proofs*, are well-founded derivation trees that allow infinite branching. In contrast, *infinitely long proofs* are ill-found (finitely branching) tree derivations where infinite branches are permitted as long as they follow the unfolding pattern characterising the validity of the fixed point semantics involved. Lying strictly between finitary and infintary proofs, and displaying many of the advantages of both formalisms, are *cyclic proofs*: proof trees whose infinite expression is strictly confined to periodic or repeating patterns, thereby permitting finite representations.

Cyclic proofs can often be translated into ω-proofs. The latter provide a transparent account of the interworking of logical systems which have an inherent infinitary nature such as fixed point logics. However, much like ill-founded proofs, ω-proofs are computationally unattractive. For example, interpolation is frequently provable via induction over the cut-free derivations in a finitary system, an approach which is helpless in the context of infinitary proofs but which has been shown to be feasible in some cyclic proof systems.

We discussed known and open results regarding the the connection between infinitary proofs, proofs with induction axioms, and cyclic proofs.

Constructive remarks about the Theory of Central Simple Algebras

Thierry Coquand

I presented work in progress, part of several discussions with Henri Lombardi and Stefan Neuwirth, which can also be seen as the research program of developing systematically the theory of central simple algebras from a constructive point of view. We are aware only of the previous work 1982 of Richman on this topic (which is reproduced in his joint book on constructive algebra [3]). The main difficulty which is pointed there is that one basic fundamental result of Wedderburn is not valid constructively. This result states that any central simple algebra is a matrix algebra over a division algebra. To explain more the situation and this difficulty, it is convenient to go back at the original proof 1907 by Wedderburn of this result. One main step there was that if a given nonzero element is not regular, then we can find a non trivial idempotent in a constructive way. In general however, it is not possible to decide if there is a non zero element which is not regular and we cannot proceed further constructively. This is the main difficulty, and to develop the theory of central simple algebra seems impossible without having such a result.

This difficulty is actually reminiscent of the problem of *existence of the algebraic closure* of a field in constructive mathematics. In general it is not possible to decide if a given polynomial is irreducible or not, and without having this, it seems impossible to proceed further. The (recent) solution to this problem is the method of *dynamic algebra* [2], which has two different sources. One source comes from computer algebra [1]. The idea there is to proceed *as if* a given polynomial is irreducible and introduce a formal root. When proceeding further in a proof/computation we have to compute an inverse, and we can either find the inverse or discover a non trivial divisor of the polynomial. We replace then the polynomial by this factor and proceed further. The other source of dynamical methods is to use suitable sheaf models, going back to ideas from Joyal, Mulvey, Reyes, Wraith.

The main point of my presentation is that we can follow the *first* approach in the context of central simple algebras. We proceed as if the given algebra is a division algebra, and when we have to compute an inverse in a proof/computation for a *given* element, we *either* find the inverse *or* we find a non trivial idempotent. In the later case, we can write the algebra A as a matrix algebra over a simpler algebra B. We then proceed by replacing the given algebra A by the simpler algebra B. (It should be noted that it is not clear at this stage if the *second* approach using sheaf models can apply here; we seem to need some kind of "non commutative" space for this.)

Using these ideas, we can get a "dynamic" version of Wedderburn 1907 result and start to develop the theory of central algebra. It is remarkable that most other basic results hold in a *non* dynamic way: for instance the fact that the dimension of a central algebra is always a square, or Skolem-Noether theorem that states that any automorphism is an inner automorphism. We can also provide a dynamic version of the result that a central simple algebra is a "twisted" form of a matrix algebra: we can find a separable extension over which the algebra becomes a matrix algebra. It is then possible to define the reduced norm and trace of an element, using constructive Galois theory.

We illustrate these ideas by providing a constructive reading of a recent simple proof (which uses the axiom of choice) by Karim Becher of a corollary of the famous Merkurjev theorem: for any central simple algebra of exponent 2 becomes a matrix algebra by a sequence of quadratic extension (over a field of caracteristic $\neq 2$). We replace the use of the axiom of choice by lexicographic induction over sequence of natural numbers. Defining a sequence $n_1, \dots, n_p$ to be *admissible* if we can split the given algebra by a sequence of formal extension of respective degree $n_1, \dots, n_p$ we show that if a sequence $\sigma, N, 2, \dots, 2$ is admissible with $N > 2$, we can find another admissible sequence of the form $\sigma, m_1, \dots, m_l$ with $m_1, \dots, m_l$ all $< N$.

Since there is a cohomological interpretation of the Brauer group over a given field, we hope to connect this work with recent constructive sheaf models of univalent type theory available at `arxiv.org/abs/1912.10407`.

References

[1] Jean Della Dora, Claire Discrescenzo and Domique Duval. *About a new method for computing in algebraic number fields.* EUROCAL 1985, pp 289-290.

[2] Henri Lombardi and Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini.* Calvage & Mounet, Paris, 2012.

[3] Ray Mines, Fred Richman and Wim Ruitenburg. *A Course in Constructive Algebra.* Springer, 1988.

Mahloness and Partial Functions

Reinhard Kahle

(joint work with Anton Setzer)

Mahlo cardinals were introduced 1911 by Paul Mahlo [1, 2]. The recursive analogue of a Mahlo cardinal is a recursively Mahlo ordinal: an admissible ordinal κ is a *recursively Mahlo ordinal*, if for all $f : M \to M$, which are M-recursive with parameters in M, there exists an admissible $\kappa < M$ such that $\forall \alpha < \kappa . f(\alpha) < \kappa$.

The analysis for the theory KPM by Michael Rathjen [3, 4, 5] and a corresponding subsystem of analysis [6] was an important step in the development of impredicative proof theory. Anton Setzer introduced in [7] a Mahlo universe in Martin-Löf type theory to give it a constructive underpinning. In Explicit Mathematics, Mahloness was formalized first in a metapredicative setting by Jäger and Strahm [8]. The impredicative version $\mathsf{T}_0(\mathsf{M})$ was studied by Jäger and Studer [9]; see also [10].

Explicit Mathematics is a formal framework introduced by Solomon Feferman [11, 12] to formalize Bishop-style constructive mathematics. It comprises a two sorted language, *individuals* (combinatory logic plus additional constants) and *types* (i.e., collections of individuals). Types are *named* by individuals. *Universes* are collections of names with certain closure properties. In $\mathsf{T}_0(\mathsf{M})$ a Mahlo universe is given in an axiomatic way, expressing the approriate closure conditions for functions f from names to names.

We will work in Explicit Mathematics, but introduce a Mahlo universe "from below". Given a part of the Mahlo universe already constructed, we will add to this collection names for subuniverses closed under functions f. The key difference between this approach compared to the axiomatic approach above is that we will not assume that f is a total function from names to names, but we will assume that it is total on the *subuniverse* which should be closed under f.

Thus, we start with the following situation: v is the part of the universe already constructed; u the potential subuniverse to be closed under f. u contains with b also $f\,b$; although c is in u, $f\,c$ may not (yet) be in v and u. Let $\mathsf{sub}(a,f,v)$ be a name for u (see Figure 1).

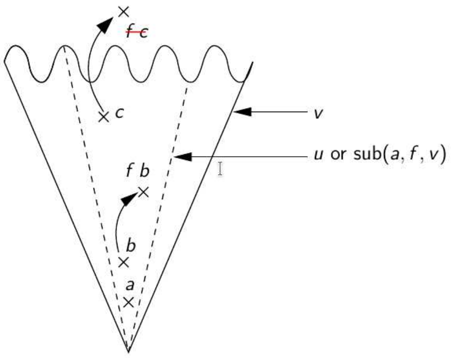

Figure 1

After adding more names to v, we may reach the situation in the left part of Figure 2, where $\mathsf{sub}(a,f,v)$ is closed under f:

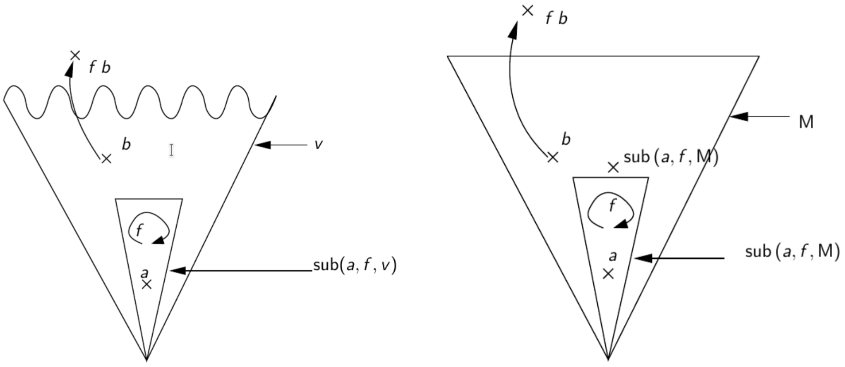

Figure 2

How f operates outside $\mathsf{sub}(a, f, v)$ does not matter: for $b \mathrel{\dot{\in}} v$ we may have $f\,b \mathrel{\dot{\notin}} v$.

Closed (sub)universes are independent of v, in the sense that an enlargement of v will not change their extension. Also, an enlargement of v also does not influence the closure property of $\mathsf{sub}(a, f, v)$ under f. This gives our approach a predicative character. Thus, we call our approach *extended predicative*.

Eventually, the Mahlo universe is obtained by enlarging a potential Mahlo universe v and $\mathsf{sub}\,(a, f, v)$ in parallel up to the stage that $\mathsf{sub}\,(a, f, v)$ is closed under f (and, of course, doing this for all a and f), as illustrated in the right part of Figure 2. So, when $\mathsf{sub}\,(a, f, \mathsf{M})$ is closed under f, then the name $\mathsf{sub}\,(a, f, \mathsf{M})$ is added to M. *But its addition to* M *doesn't affect the reason for originally adding it to* M.

A formal presentation of the corresponding theory can be found in [13], but a more detailed elaboration of the theory and its features is still work in progress.

This includes the possibility to obtain a *least Mahlo universe* by adding an appropriate induction principle. A corresponding principle appears to be problematic for $\mathsf{T}_0(\mathsf{M})$, as the quantifier in the "induction step" has to range over arbitrary functions, not only those which are total from names to names. Also, in Martin-Löf type theory, which is also based on total functions, the addition of an induction principle for Mahlo doesn't make sense.

Partial functions are essential for this induction principle, as total functions will range over too few functions to permit leastness of the Mahlo universe. But we used already partial functions in the predicative construction of the subuniverses, which are constructed by f's which might not be total outside the subuniverse.

That is the reason to use Explicit Mathematics as framework instead of Martin Löf type theory, where all functions need to be total. This is due to the underlying *Curry-Howard-correspondence* which matches functions with proofs.

To mimic our account to Mahloness in Martin-Löf type theory, one would have to answer the puzzling question (see also [14]):

What could be *partial proofs*?

References

[1] Paul Mahlo. Über linear transfinite Mengen. *Berichte über die Verhandlungen der Königlich Sächsischen Gesellschaft der Wissenschaften zu Leipzig. Mathematisch-Physische Klasse*, 63:187 – 225, 1911.

[2] Paul Mahlo. Zur Theorie und Anwendung der ρ_0-Zahlen. *Berichte über die Verhandlungen der Königlich Sächsischen Gesellschaft der Wissenschaften zu Leipzig. Mathematisch-Physische Klasse*, 64:108 – 112, 1912.

[3] Michael Rathjen. Proof-theoretical analysis of KPM. *Arch. Math. Log.*, 30:377 – 403, 1991.

[4] Michael Rathjen. Collapsing functions based on recursively large cardinals: A well-ordering proof for KPM. *Archive for Mathematical Logic*, 33:35–55, 1994.

[5] Kurt Schütte. Zur Beweistheorie von KPM. In R. Kahle and M. Rathjen, editors, *The Legacy of Kurt Schütte*, pages 469–481. Springer, 2020.

[6] Michael Rathjen. The recursively Mahlo property in second order arithmetic. *Mathematical Logic Quarterly*, 42:59–66, 1996.

[7] Anton Setzer. Extending Martin-Löf type theory by one Mahlo-universe. *Archive for Mathematical Logic*, 39:155–181, 2000.

[8] Gerhard Jäger and Thomas Strahm. Upper bounds for metapredicative Mahlo in explicit mathematics and admissible set theory. *Journal of Symbolic Logic*, 66(2):935–958, 2001.

[9] Gerhard Jäger and Thomas Studer. Extending the system T_0 of Explicit Mathematics: the limit and Mahlo axioms. *Annals of Pure and Applied Logic*, 114(1–3):79–101, 2002.

[10] Gerhard Jäger. Metapredicative and explicit Mahlo: a proof-theoretic perspective. In René Cori, Alexander Razborov, Stevo Todorčević, and Carol Wood, editors, *Logic Colloquium 2000*, Lecture Notes in Logic, pages 272 – 293. A K Peters. Association for Symbolic Logic, 2005.

[11] Solomon Feferman. A language and axioms for explicit mathematics. In J. Crossley, editor, *Algebra and Logic*, volume 450 of *Lecture Notes in Mathematics*, pages 87–139. Springer, 1975.

[12] Solomon Feferman. Constructive theories of functions and classes. In M. Boffa, D. van Dalen, and K. McAloon, editors, *Logic Colloquium 78*, pages 159–224. North–Holland, Amsterdam, 1979.

[13] Reinhard Kahle and Anton Setzer. An extended predicative definition of the Mahlo universe. In R. Schindler, editor, *Ways of Proof Theory*, pages 315–340. Ontos Verlag, 2010.

[14] Reinhard Kahle. Is there a “Hilbert Thesis”? *Studia Logica*, 107(1):145–165, 2019.

Reporter: Anton Freund

Participants

Dr. Bahareh Afshari
Computer Science and Engineering
Department
University of Gothenburg
41296 Göteborg
SWEDEN

Amir Akbar Tabatabai
Department of Philosophy
Utrecht University
Janskerkhof 13
3512 BL Utrecht
NETHERLANDS

Prof. Dr. Matthias Baaz
Institut für Diskrete Mathematik und
Geometrie
Technische Universität Wien
Karlsplatz 13
1040 Wien
AUSTRIA

Prof. Dr. Arnold Beckmann
Department of Computer Science
Swansea University
Bay Campus
Swansea SA1 8EN
UNITED KINGDOM

Prof. Dr. Lev D. Beklemishev
Steklov Mathematical Institute of
Russian Academy of Sciences
8, Gubkina St.
119 991 Moscow GSP-1
RUSSIAN FEDERATION

Dr. Ulrich Berger
Department of Computer Science
Swansea University
Bay Campus
Crymlyn Burrows, Skewen
Swansea SA1 8EN
UNITED KINGDOM

Dr. Roberta Bonancina
Carl Friedrich von Weizsäcker-Zentrum
Universität Tübingen
Keplerstrasse 2,
72076 Tübingen
GERMANY

Prof. Dr. Vasco Brattka
Institut für Theoretische Informatik,
Mathematik und Operations Research
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85577 Neubiberg
GERMANY

Prof. Dr. Samuel Buss
Department of Mathematics
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
UNITED STATES

Prof. Yong Cheng
School of Philosophy
Wuhan University
Hubei
Wuhan 430072
CHINA

Prof. Dr. Thierry Coquand
Department of Computer Science
Chalmers University of Technology
and University of Göteborg
41296 Göteborg
SWEDEN

Prof. Dr. Fernando Ferreira
Departamento de Matemática
FCUL - Universidade de Lisboa
Campo Grande, Ed. C6, Piso 2
1749-016 Lisboa
PORTUGAL

Dr. Anton Freund
Fachbereich Mathematik
Technische Universität Darmstadt
Schlossgartenstraße 7
64289 Darmstadt
GERMANY

Dr. Makoto Fujiwara
Department of Mathematics
School of Science and Technology
Meiji University
Higashi-mita 1-1-1, Tama-ku
Kawasaki-shi 214-8571
JAPAN

Prof. Dr. J. Martin E. Hyland
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Prof. Dr. Rosalie Iemhoff
Department of Philosophy and Religious
Studies
Utrecht University
Janskerkhof 13
3512 BL Utrecht
NETHERLANDS

Prof. Dr. Hajime Ishihara
School of Information Science
Japan Advanced Institute of Science
and Technology
1-1 Asahidai, Nomi
Ishikawa 923-1292
JAPAN

Prof. em. Dr. Gerhard Jäger
Institut für Informatik
Universität Bern
Neubrückstrasse 10
3012 Bern
SWITZERLAND

Dr. Emil Jeřábek
Institute of Mathematics of the Czech
Academy of Sciences
Žitná 25
115 67 Praha 1
CZECH REPUBLIC

Prof. Dr. Joost Joosten
Departamento de Filosofia
Universitat de Barcelona
Montalegre, 6
08001 Barcelona, Catalonia
SPAIN

Prof. Dr. Reinhard Kahle
Theorie und Geschichte der
Wissenschaften
Universität Tübingen
Keplerstr. 2
72074 Tübingen
GERMANY

Dr. Takayuki Kihara
Graduate School of Informatics
Nagoya University
1, Furo-cho, Chikusa-ku
Nagoya 464-0814
JAPAN

Prof. Dr. Ulrich W. Kohlenbach
Fachbereich Mathematik
Technische Universität Darmstadt
Schlossgartenstraße 7
64289 Darmstadt
GERMANY

Dr. Leszek Kolodziejczyk
Institute of Mathematics
University of Warsaw
ul. Banacha 2
02-097 Warszawa
POLAND

Dr. Antonina Kolokolova
Department of Computer Science
Memorial University of Newfoundland
St. John's NL A1B 3X5
CANADA

Prof. Dr. Jan Krajicek
Faculty of Mathematics and Physics
Charles University
Sokolovska 83
186 75 Praha 8
CZECH REPUBLIC

Prof. Dr. Laurentiu Leustean
University of Bucharest
36-46 Mihail Kogălniceanu Bd, Sector 5
050107 Bucharest
ROMANIA

Prof. Dr. Henri Lombardi
Département de Mathématiques
Université de Franche-Comté
16, route de Gray
25030 Besançon Cedex
FRANCE

Prof. Dr. Maria Emilia Maietti
Dipartimento di Matematica
Università di Padova
Via Trieste, 63
35121 Padova
ITALY

Prof. Dr. Alexandre Miquel
Instituto de Matematica y Estadistica
Facultad de Ingenieria
Julio Herrera y Reissig 565
Montevideo 11300
URUGUAY

Prof. Sara Negri
Department of Philosophy
University of Helsinki
P.O. Box 24
00014 University of Helsinki
FINLAND

Dr. Takako Nemoto
School of Information Science
Japan Advanced Institute of Science
and Technology
1-1 Asahidai, Nomi
Ishikawa 923-1292
JAPAN

Dr. Adriana Nicolae
Faculty of Mathematics and Computer
Science
Babes-Bolyai University
No. 1 Mikhail Kogalniceanu Street
400084 Cluj-Napoca
ROMANIA

Prof. Dr. Dag Normann
Department of Mathematics
University of Oslo
P. O. Box 1053 - Blindern
0316 Oslo
NORWAY

Dr. Isabel Oitavem
Departemento de Matematica
Universidade Nova de Lisboa
2829-516 Caparica
PORTUGAL

Dr. Paulo Oliva
School of Electronic Engineering and
Computer Science
Queen Mary College
University of London
Mile End Road
London E1 4NS
UNITED KINGDOM

Dr. Pedro Pinto
Fachbereich Mathematik
Technische Universität Darmstadt
Schlossgartenstraße 7
64289 Darmstadt
GERMANY

Nicholas Pischke
Fachbereich Mathematik
Technische Universität Darmstadt
Schlossgartenstraße 7
64289 Darmstadt
GERMANY

Dr. Thomas Powell
Dept. of Computer Science
University of Bath
Claverton Down
Bath BA2 7AY
UNITED KINGDOM

Prof. Dr. Pavel Pudlak
Institute of Mathematics, Czech
Academy of Sciences
Zitna 25
115 67 Praha
CZECH REPUBLIC

Prof. Dr. Michael Rathjen
School of Mathematics
University of Leeds
Leeds LS2 9JT
UNITED KINGDOM

Dr. Sam Sanders
Fachbereich Mathematik
Technische Universität Darmstadt
Schlossgartenstraße 7
64289 Darmstadt
GERMANY

Prof. Dr. Peter M. Schuster
Dipartimento di Informatica
Università di Verona
Strada le Grazie 15
37134 Verona
ITALY

Prof. Dr. Helmut Schwichtenberg
Mathematisches Institut
Ludwig-Maximilians-Universität
München
Theresienstrasse 39
80333 München
GERMANY

Dr. Monika Seisenberger
Department of Computer Science
Swansea University
Singleton Park
Swansea SA2 8PP
UNITED KINGDOM

Dr. Andrei Sipos
Department of Computer Science
University of Bucharest
Academiei 14
010014 Bucharest
ROMANIA

Prof. Dr. Thomas Strahm
Institut f. Informatik & Angewandte
Mathematik
Universität Bern
Neubrückstr. 10
3012 Bern
SWITZERLAND

Prof. Dr. Thomas Streicher
Fachbereich Mathematik, AG Logik
Technische Universität Darmstadt
Schlossgartenstraße 7
64289 Darmstadt
GERMANY

Dr. Neil Thapen
Institute of Mathematics of the AV CR
Zitna 25
115 67 Praha 1
CZECH REPUBLIC

Dr. Benno van den Berg
FNWI
Institute of Logic, Language & Computation
University of Amsterdam
P.O. Box 94242
1090 GE Amsterdam
NETHERLANDS

Iris van der Giessen
Department of Philosophy and Religious Studies
Utrecht University
Janskerkhof 13
3512 BL Utrecht
NETHERLANDS

Prof. Dr. Albert Visser
Department of Philosophy and Religious Studies
Utrecht University
Janskerkhof 13
3512 BL Utrecht
NETHERLANDS

Prof. Dr. Andreas Weiermann
Vakgroep Wiskunde
Universiteit Gent
Gebouw S8 top floor Wing A
Krijgslaan 281
9000 Gent
BELGIUM

Dr. Daniel Wessel
Dipartimento di Informatica
Università di Verona
Strada le Grazie 15
37134 Verona
ITALY

Dr. Chuangjie Xu
Mathematisches Institut
Ludwig-Maximilians-Universität München
Theresienstr. 39
80333 München
GERMANY

Dr. Keita Yokoyama
School of Information Sciences
Japan Advanced Institute of Science and Technology
1-1 Asahidai, Nomi
Ishikawa 923-1292
JAPAN

Prof. Dr. Yang Yue
Department of Mathematics
National University of Singapore
S17, 10 Lower Kent Ridge Road
Singapore 119076
SINGAPORE